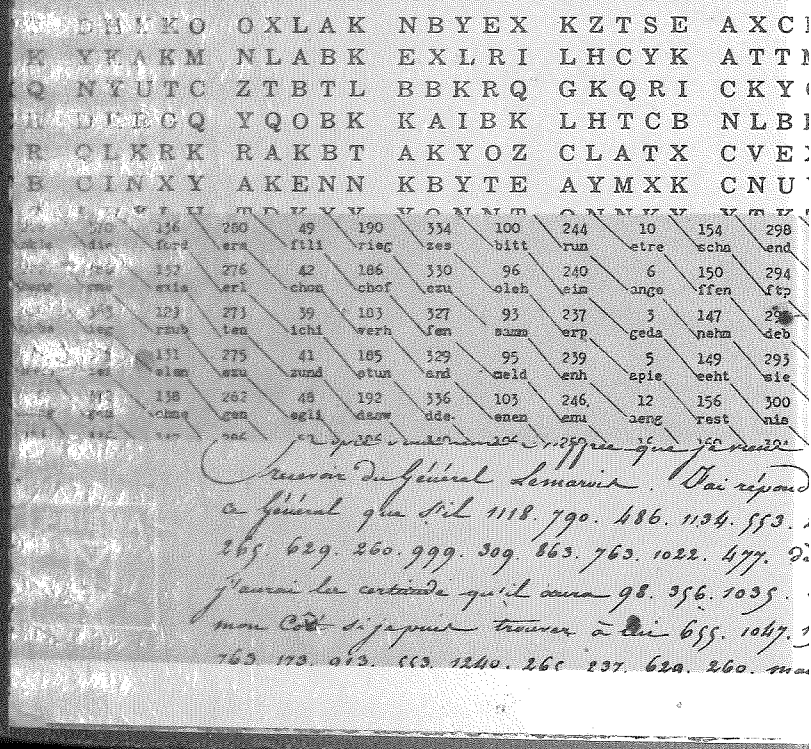
Rickard Sandler:

# Chiffer



800 31 27 5797 D1

AXIELL

*Rickard Sandler · Chiffer*

RICKARD SANDLER

# CHIFFER

*En bok om litterära och historiska hemligskrifter*

BOKFÖRLAGET PRISMA STOCKHOLM

Omslag av Bo Berndal

© 1943, 1965 Rickard Sandler

Detta är en av författaren översedd och utvidgad nyutgåva av hans 1943 hos Wahlström & Widstrand utkomna bok "Chiffer". Helt nyskrivet är slutkapitlet "Ett svenskt diplomatchiffers ändalykt".

Uppsala Stadsbibliotek
Signum Af
Acc. ut 3
Dat. 17/3 -65
Kat. L
Inb. samb.
Omb.

Gummessons Boktryckeri AB, Falköping 1965

# Innehåll

Förord till första upplagan . . . . . 7
1. Les compagnons du Silence . . . . . 9
2. Ett Napoleonchiffer före Leipzig . . . . . 14
3. Edgar Allan Poes guldscarabé . . . . . 24
4. Mannen med järnmasken . . . . . 28
5. Farliga börssiffror . . . . . 42
6. Le petit chiffre de Napoléon . . . . . 49
7. Mathias Sandorfs kryptogram . . . . . 57
8. Napoleons Hamburginstruktion . . . . . 65
9. Ortegas bekännelse . . . . . 73
10. En depesch till furst Metternich . . . . . 82
11. Balzacs olösliga kryptogram . . . . . 90
12. Marskalk Davouts rapport . . . . . 92
13. Tårta på tårta . . . . . 107
14. PQR — ett tyskt cirkulärtelegram från första världskriget . . . . . 112
15. En genial experts kamp mot rutinen . . . . . 140
16. Ett svenskt diplomatchiffers ändalykt . . . . . 155
Använd litteratur . . . . . 171

# Förord till första upplagan

Jag måste beundra mina förläggares mod att utge detta arbete, en politikers förströelse på lediga stunder. Den lilla kretsen av fackmän skall finna dessa chifferstudier puerilt enkla, för den stora läsekretsen blir de otillgängliga redan genom att texterna genomgående och avsiktligt är på främmande språk. De flesta kommer att lägga arbetet tillbaka på bokhandelsdisken som odrägligt tungläst och svårbegripligt. Det är egentligen författarens kamrater chifferamatörerna, som kan väntas ha nöje och behållning av denna bok. Hur många de är återstår att se.

Några av dessa studier har varit publicerade i Göteborgs Handels- och Sjöfartstidning. Det ur Bernadotteska familjearkivet hämtade chiffret (12) publiceras efter av H. M. Konungen meddelat tillstånd. Jag har docenten Torvald Höjer att tacka för detta intressanta studieobjekt och krigsarkivet för ett annat, i samma undersökning använt. Arbeten, ur vilka upplysningar eller chiffermaterial hämtats, är anförda i slutet av boken.

Tryckfelen bleve antagligen ännu fler, om jag besvärat förlaget med upprepade korrekturavdrag. För chifferlösare bör det vara en extra krydda att upptäcka dem.

*Författaren*

# 1. Les compagnons du Silence

En roman av Paul Féval har titeln Les compagnons du Silence. Vad kumpanerna hade för sig har i detta sammanhang föga intresse. Det kan räcka att nämna, att de sinsemellan hade ett lösenord hämtat ur en strof av Fiorvavente. Det löd: amici alliegre andiamo alla pena. Något som inte riktigt tålde dagsljuset hade de i varje fall för sig. I romanen förekommer åtskilliga chiffer. De är alla fabricerade efter en tämligen enkel substitutionsmetod. Ett mycket kort sådant skall här analyseras. Det ger exempel dels på hur man genom ett mycket enkelt trick kan försvåra det första inträngandet i chiffrets system, dels också hur ofantligt chifferlösning underlättas, om chiffreringen sköts så, att de olika orden tydligt är åtskilda.

Den korta chiffertexten, vars innehåll för övrigt ingalunda avslöjar någon hemlighet, ser ut så här:

I3R A6 A I4A5I2RI4A5I2 IL2NM2I2 CI2 DRA5M2 A2NA4O I4A5I2 RI2 A2I2A4 II2M2O RA A2NI3 I3R A6 A I4A5I2RI4A5I2 IL2NM2I2 CI2 DRA5M2 A3NI3A4 I4A5I2 RI2 IL2AA4MNA3 II2M2O RA INA3M2II3I2A3II2 EA5 OA4AI3AO4I2

Vad man nu vid en systemanalys först tar sig för är att räkna antalet förekommande tecken för att kunna bedöma, om de utgör beståndsdelar av ett alfabet, vare sig det är äkta eller ett substituerat. Räknar man nu bokstäver för sig och siffror för sig, finner man, att chiffret innehåller tio olika bokstäver och fem olika siffror. Man erhåller följande frekvensstatistik:

| | | | |
|---|---|---|---|
| I | 38 | N | 7 |
| A | 30 | O | 5 |
| 2 | 30 | L | 3 |
| 4 | 11 | C | 2 |
| R | 10 | D | 2 |
| 3 | 10 | 6 | 2 |
| M | 8 | E | 1 |
| 5 | 7 | | 166 |

Först lägger man märke till att 15 är ett bra litet antal bokstäver på en text av 166. Men ännu orimligare är frekvensfördelningen. Tre högfrekventa tecken når över 30, dvs. 20 % eller däröver. Sedan faller frekvensen abrupt ner till omkring 10, dvs. tredjedelen därav. Det finns inget språk som uppvisar en dylik frekvensfördelning. Här har man att närmast tänka sig franska eller möjligen italienska, men i vardera fallet skulle man ha en mycket utpräglad topp för bokstaven e och därefter ett avsevärt språng nedåt. Det tycks av detta uppenbart att om man tar bokstäver och siffror var för sig, så kommer man över huvud ingen vart. Och på denna lilla begynnelsesvårighet skulle en oerfaren chifferlösare kanske ge upp.

Efter detta negativa utfall får man närmast se efter, om tecknen låter sig kombinera. Måhända hör siffrorna ihop med en bokstav, den föregående eller den efterföljande. Man har naturligtvis iakttagit, att tecknen är sammanförda i grupper som kanske kan bilda ord. Ingen av dessa grupper inleds med en siffra, och i det fall då ett enda tecken ser ut att bilda ett ord är det fråga om en bokstav. Alltså försöker man sig på att sammanföra varje förekommande siffertecken med föregående bokstav i den föreställningen att $A^1$, $A^2$, $A^3$ utgör skilda bokstäver. Därigenom erhålls följande nya version, vari från början en särskilt märklig upprepning är markerad med halvfet stil:

**$I^3$ R $A^6$ A $I^4$ $A^5$ $I^2$ R $I^4$ $A^5$ $I^2$ I $L^2$ N $M^2$ $I^2$ C $I^2$**
**D R $A^5$ $M^2$ $A^2$ N $A^4$ O $I^4$ $A^5$ $I^2$ R $I^2$ $A^2$ $I^2$ $A^4$ I $I^2$ $M^2$ O**
**R A $A^2$ N $I^3$ $I^3$ R $A^6$ A $I^4$ $A^5$ $I^2$ R $I^4$ $A^5$ $I^2$ I $L^2$ N $M^2$ $I^2$**
**C $I^2$ D R $A^5$ $M^2$ $A^3$ N $I^3$ $A^4$ $I^4$ $A^5$ $I^2$ R $I^2$ I $L^2$ A $A^4$ M N $A^3$**



**$II^2M^2O$ R A I N $A^3$ $M^2$ I $I^3$ $I^2$ $A^3$ I $I^2$ E $A^5$**
**O $A^4$ A $I^3$ A O $^4$ $I^2$**

Nu finner man att för det första antalet enskilda tecken stigit till tjugo samtidigt som totalantalet sjunkit till 104. Detta ser ju vida rimligare ut. Och ännu bättre artar det sig, om man iakttar frekvensfördelningen, som nu är denna:

| | | | |
|---|---|---|---|
| $I^2$ | 18 | O | 5 |
| R | 10 | $A^3$ | 4 |
| $A^5$ | 8 | $A^2$ | 3 |
| I | 8 | $L^2$ | 3 |
| N | 7 | $A^6$ | 2 |
| $M^2$ | 7 | C | 2 |
| A | 6 | D | 2 |
| $I^3$ | 6 | M | 1 |
| $A^4$ | 5 | E | 1 |
| $I^4$ | 5 | $O^4$ | 1 |
| | | | 104 |

Nu visar tecknet $I^2$ en så exakt normalfrekvens som man kan begära, om man antar språket vara franska och $I^2$ betyda e. Frekvensen faller genast och fullt normalt för nästa tecken och hela frekvenskurvan har ett normalt utseende.

Vi arbetar vidare från denna förutsättning och fäster oss nu närmast vid den halvfeta repetitionen $I^4$ $A^5$ $I^2$ som förekommer sex gånger. Tecknet $I^4$ förekommer endast i denna sammanställning. Detta förhållande, frekvensen och förutsättningen $I^2 = e$ gör att man måste förmoda, att trigrammet just är den förträffliga inkörsport vid fransk forcering som que utgör. Vi iakttar vidare, att det fjärde "ordet" innehåller detta trigram två gånger åtskilda av en enda bokstav, R. Det finns i franskan ett enda ord, som då kan komma i fråga. Fjärde ordet kan icke vara annat än quelque och R = l. Nu skall vi dra nytta av den speciella fördel som en uppdelning på ord innebär. Chiffret börjar med tre "ord", av vilka två är enbokstaviga. Franskan har blott två ord av den typen, vilka därjämte har den egenheten att de förekommer i en bestämd ordningsföljd och

brukar föregås just av ett tvåbokstavigt ord. Chiffrets början före quelque kan därför utan vidare avläsas, och tillräcklig bekräftelse ger f. ö. bokstaven R=l. Den välkända frasen är helt enkelt il y a. Härigenom har vi alltså funnit ytterligare $I^3$=i, $A^6$=y, A=a. Sätter vi nu in dessa tolkningar får chiffret följande utseende:

$I^3$ R $A^6$ A $I^4$ $A^5$ $I^2$ R $I^4$ $A^5$ $I^2$ I $L^2$ N $M^2$ $I^2$ C $I^2$
i l y a q u e l q u e e e

D R $A^5$ $M^2$ $A^2$ N $A^4$ O $I^4$ $A^5$ $I^2$ R $I^2$ $A^2$ $I^2$ $A^4$ $I^2$ $M^2$ O
l u q u e l e e e

R A $A^2$ N $I^3$ $I^3$ R $A^6$ A $I^4$ $A^5$ $I^2$ R $I^4$ $A^5$ $I^2$ I $L^2$ N $M^2$ $I^2$
l a i i l y a q u e l q u e e

C $I^2$ D R $A^5$ $M^2$ $A^3$ N $I^3$ $A^4$ $I^4$ $A^5$ $I^2$ R $I^2$ I $L^2$ A $A^4$ M N $A^3$
e l u i q u e l e a

I $I^2$ $M^2$ O R A I N $A^3$ $M^2$ I $I^3$ $I^2$ $A^3$ I $I^2$ E $A^5$
e l a i e e u

O $A^4$ A $I^3$ A $O^4$ $I^2$
a i a e

Detta artar ju sig bra. Lösningen kan icke gärna vara långt borta. Den naturligaste fortsättningen på inledningsfrasen "il y a quelque" vore ju "chose" och i själva verket slutar ordet efter frasen på e och innehåller fem bokstäver. Det tvenne gånger upprepade självständiga "que" tyder på en komparation och andra ordet före que är *.lus,* vilket sannolikast borde vara plus. Insätts även dessa värden får chiffret följande utseende:

$I^3$ R $A^6$ A $I^4$ $A^5$ $I^2$ R $I^4$ $A^5$ $I^2$ I $L^2$ N $M^2$ $I^2$ C $I^2$
i l y a q u e l q u e c h o s e e

D R $A^5$ $M^2$ $A^2$ N $A^4$ O $I^4$ $A^5$ $I^2$ R $I^2$ $A^2$ $I^2$ $A^4$ I $I^2$ $M^2$ O
p l u s o q u e l e e c e s

R A $A^2$ N $I^3$ $I^3$ R $A^6$ A $I^4$ $A^5$ $I^2$ R $I^4$ $A^5$ $I^2$ I $L^2$ N $M^2$ $I^2$
l a o i i l y a q u e l q u e c h o s e



C $I^2$ D R $A^5$ $M^2$ $A^3$ N $I^3$ $A^4$ $I^4$ $A^5$ $I^2$ R $I^2$
e p l u s o i q u e l e

I $L^2$ A $A^4$ M N $A^3$ I $I^2$ $M^2$ O R A I N $A^3$ $M^2$ I $I^3$ $I^2$ $A^3$ I $I^2$
c h a o c e s l a c o s c i e c e

E $A^5$ O $A^4$ A $I^3$ A $O^4$ $I^2$
u a i a e

Vad som nu återstår är lätt att gissa. Att C betyder d följer direkt av sammanhanget. Orden $A^2$ N $A^4$ O och $A^2$ $I^2$ $A^4$ ger fort och fer. Därmed blir fortsättningen: C'est la foi. Sedan följer utan vidare: Il y a quelque chose de plus noir que le — —. Det ord som här skall följa blir tydligen charbon. Och detta svartare än kol c'est la conscience — — —. Svårigheten är här slutet, som nu innehåller . *u traia . e* . Efter sammanhanget att döma borde det gälla la conscience du, men i så fall föreligger här ett skrivfel, E i stället för C. Men vems samvete gäller det. Här har olyckligtvis två bokstäver blivit omkastade, varigenom ordet ser helt obegripligt ut. Den riktiga läsarten är O $A^4$ A $I^3$ O $A^4$ $I^2$, vilket ger betydelsen traître.

Ser man nu efter vilket alfabet som använts, finner man att det är följande:

a b c d e f g h i j k l m n o p q r s t u v w x y z
A M I C $I^2$ $A^2$ $L^2$ $I^3$ R $A^2$ N D $I^4$ $A^4$ $M^2$ O $A^5$ $A^6$

Alltså har alfabetet helt enkelt tillverkats av lösenordet genom att de upprepade bokstäverna i detsamma försetts med nummer i chifferalfabetet. Bortser man från numreringen läser man ju med vissa luckor i alfabetet:

A M I C I A . L I . . R . A N D I A M O A . . A

Klarar man bara den första och den sista svårigheten är detta chiffer i själva verket så lätt, att det av en i franska tränad person med lite sinne för forcering bör kunna lösas i huvudet, vilket jag övertygat mig om.

# 2. Ett Napoleonchiffer före Leipzig

Några dagar före slaget vid Leipzig sände generalmajor Berthier vid Napoleons högkvarter till marskalk Augereau, hertigen av Castiglione, två chiffrerade depescher. De innehöll samma order i två varianter. Varför så skedde är ej bekant. Måhända har vederbörande efter avsändandet av den i chiffer längre varianten ansett det nödvändigt att skicka en ny, som kunde dechiffreras mycket snabbt. Bägge depescherna är avfattade på en blandning av klart språk och chiffer, vilket vid denna tidpunkt ofta förekom. Dessa båda omständigheter måste, såsom här nedan skall visas, ha gjort depeschen till ett lätt byte för en av de franska trupprörelserna intresserad motståndare, ifall ett uppsnappande skett. Därom är *nu* intet bekant. Men fallet ägnar sig förträffligt för att visa vilka utmärkta hållpunkter för att lösa ett meddelande i hemlig skrift, som ovarsamhet, brådska eller okunnighet om forceringsmöjligheterna här åstadkommit.

Så här ser de båda depeschvarianterna ut. Till en början förefaller de nog så ogenomskinliga, även den som innehåller ett stort antal klart utskrivna ord.

I

L'empereur ordonne que vous vous portiez le plus tôt possible 167 138 169 106 171 15 117 avec son infanterie sa cavallerie et son artillerie en ne laissant 15 164 138 169 176 166 35 138 169 81 que ce que Sa Majesté a désigné pour 106 78 son principal but sera de rester 107 87 176 169 53 52 106 171 15 117 et de chasser 117 167 156 169 145 171 115 167 68 qui manoeuvrent dans 20 176 131 75 vous pouvez vous rendre en droite ligne 156 169 40 35 138 169 81 167 138 169 87 53 91



II

L'empereur ordonne que 175 138 167 164 90 138 167 152 169 145 53 166 117 13 137 103 157 176 152 167 134 37 117 174 169 106 171 15 117 15 132 6 175 176 126 48 164 153 126 32 50 175 176 126 25 68 94 106 122 171 115 176 15 164 138 169 166 35 138 169 81 136 20 173 138 53 171 107 87 82 131 15 52 134 81 94 137 90 138 169 106 51 169 116 168 115 175 176 126 137 148 115 6 119 156 96 3 176 177 146 52 169 82 131 169 107 92 126 52 167 23 53 35 138 6 61 167 52 106 171 39 53 50 52 6 72 167 177 169 117 167 137 22 145 171 115 167 68 154 107 94 138 164 126 115 176 16 115 167 20 176 131 67 126 6 14 145 175 138 167 152 138 132 166 164 90 138 167 126 115 23 126 68 23 159 92 53 93 81 94 137 22 6 90 35 138 169 81 174 169 119 53 115 15

Denna senare depesch innehåller ju uteslutande siffror utom de tre inledande orden "l'empereur ordonne que". Man kan fråga sig varför inte även dessa ord chiffrerats. Då hade den lika början inte fallit i ögonen. Det kan tänkas, att dessa ord i klar text skall ögonblickligen fästa uppmärksamheten på att det är en kejsarens befallning meddelandet innehåller och därmed påskynda behandlingen. I varje fall kan detta icke räcka till för att bestämma identiteten av de båda, som vi kan inbilla oss, uppfångade meddelandena. Men det framgår av en jämförelse med de i depesch I förekommande sifferserierna. I denna är helt naturligt just på de punkter som gäller orderns materiella innehåll klartexten avbruten av chiffer, som döljer den verkliga innebörden till synes effektivt, fastän de klara orden ej är mindre än 48 på ett totalantal av, som det skall visa sig, 70.

Lägger man de båda depescherna vid sidan av varann och går igenom sifferserien, finner man så många, relativt långa, identiska serier av siffror, att det icke kan råda tvivel om ej bara att samma chiffer använts utan att det är fråga om ett och samma meddelande. Detta framgår av den uppställning som följer.

I

L'empereur ordonne que *vous vous portiez le plus tôt possible* 167 138 **169 106** **171 15 117** avec son infanterie sa cavallerie et son artillerie en ne laissant **15** **164 138 169** 176 **166 35 138 169 81** *que ce que Sa Majesté a désigné pour* **106** 78 *son principal but sera de rester*

107 87 176 169 53 **52 106 171** 15 117 et de chasser **117 167** 156 169 **145 171 115 167 68** *qui manoeuvrent dans* **20 176** **131** 75 *vous pouvez vous rendre en droite ligne*

156 169 40 **35 138 169 81** 167 138 **169** 87 **53** 91

II

L'empereur ordonne que 175 138 167 164 90 138 167 152 169 145 53 166 117 37 103 157 176 152 167 134 37 117 174 **169 106** **171 15 117** 15 132 6 175 176 126 48 164 153 126 32 50 175 176 126 25 68 94 106 122 171 115 176 **15 164 138 169 166 35 138 169 81** 136 20 173 138 53 171 107 87 82 131 15 52 134 81 94 137 90 138 169 **106** 51 169 116 168 115 175 176 126 137 148 115 6 119 156 96 3 176 177 146 52 169 82 131 169 107 92 126 52 167 23 53 35 138 6 61 167 **52** **106 171** 39 53 50 52 6 72 167 177 169 **117 167** 137 22 **145 171** **115 167 68** 154 107 94 138 164 126 115 176 16 115 167 **20 176** **131** 67 126 6 145 175 138 167 152 138 132 166 164 90 138 167 126 115 23 126 68 23 159 92 53 93 81 94 137 22 6 90 **35 138 169** **81** 174 **169** 119 **53** 115 15

Då chiffret innehåller en högsta siffra av 177, kan förmodas, att siffrorna betyder både bokstäver (kanske flera tecken för de vanligare) och stavelser samt måhända även hela ord. Under denna förutsättning tycks intet osannolikt föreligga, om klartextpartierna till sitt omfång jämförs med de motstående sifferserierna. Hade man icke den vägledning chiffer I kan ge, skulle chiffer II få anses skäligen svårlöst.

Upprepningar ger alltid god hjälp vid chifferlösning. Hur är det med de olika siffrornas frekvens? Redan i chiffer I förekommer påfallande många repetitioner, såsom 169 ej mindre än 7 gånger. Detta tecken kommer också näst högst i chiffer II, men maximum har 138 med 12 förekomster medan 169 har 11. Man kunde då gissa att något av dessa tecken betyder e, franskans vanligaste bokstav. Detta håller dock inte streck, direkt kan frekvensen ej med säkerhet utnyttjas. En frekvens-



tabell är i varje fall bra att ha. Den blir så här, upp till 4 förekomster i ch. II.

| | ch. II | ch. 1 |
|---|---|---|
| 138 | 12 | 5 |
| 169 | 11 | 7 |
| 167 | 9 | 4 |
| 126 | 9 | — |
| 176 | 8 | 3 |
| 115 | 8 | 1 |
| 53 | 6 | 2 |
| 6 | 6 | — |
| 175 | 5 | — |
| 164 | 5 | 1 |
| 137 | 5 | — |
| 171 | 5 | 3 |
| 15 | 5 | 3 |
| 52 | 5 | 1 |
| 90 | 4 | — |
| 117 | 4 | 3 |
| 106 | 4 | 3 |
| 94 | 4 | — |
| 81 | 4 | 1 |

I följande uppställning är alla repeterade siffror utmärkta med ett =.

Det gäller nu att finna ett användbart uppslag för att få ett första insteg i chiffret. Ett sådant är att med hjälp av det kortaste inskjutna klartextstycket söka betydelsen av dess siffermotsvarighet eller några tecken däri. Titta alltså på den lilla frasen "et de chasser" som i bägge chiffren efterföljs av samma siffergrupper 117 167. Eftersom 7 chiffertecken ersätter den lilla frasen med 11 bokstäver, är det tydligt, att här förekommer rena bokstavstecken. Sätt in *ser* i chasser på de tre närmast före upprepningen stående siffrorna, dvs. 167 177 169. s e r Av dessa är 167 och 169 högfrekventa, vilket passar bra för s och r. Däremot ser det mindre lyckat ut med 177 (förekommande 2

ggr) som beteckning för e. Bäst därför pröva före ett införande i chiffertexten. En god möjlighet ger ch. I, vari de första chiffertecknen är 167 138 169. Samma serie återkommer f. ö. alldeles i slutet av samma chiffer. Beaktas klartextens innehåll i början av ch. I, kan ingen tvekan råda om att sifferserien betyder *sur*. Alltså 138 = u. Om detta proberas på de första chiffertecknen i ch. II, erhålls 175 138 167, vilket (se ch. I) tydligen är att läsa som *vous*. Men vous är ju upprepat, och därav erhålls direkt en annan representation av samma ord, nämligen 164 90 138 167. Bägge dessa beteckningar för vous finns f. ö. en gång till i chiffret. Av detta följer vidare 152 = po samt 174 = su. Med dessa värden insatta erhåller chiffret följande utseende:

| I | II |
|---|---|
| L'empereur ordonne que vous | L'empereur ordonne que 175 138 |
| vous portiez le plus tôt | 167 164 90 138 167 152 169 145 53 |
| possible | 166 117 137 103 157 176 152 167 |
| 167 138 169 106 171 15 | 134 37 117 174 169 106 171 15 |
| 117 avec son infanterie sa caval- | 117 15 132 6 175 176 126 48 164 |
| lerie et son artillerie en ne lais- | 153 126 32 50 175 176 126 25 68 |
| sant 15 164 | 94 106 122 171 115 176 15 164 |
| 138 169 176 166 35 138 169 81 | 138 169 166 35 138 169 81 136 |



| | |
|---|---|
| que ce que Sa Majes- | 20 173 138 53 171 107 87 82 131 |
| té a désigné pour | 15 52 134 81 94 137 90 138 169 |
| 106 78 son principal | 106 51 169 116 168 115 175 176 |
| but sera de rester | 126 137 148 115 6 119 156 96 3 |
| | 176 177 146 52 169 82 131 169 |
| 107 87 | 107 92 126 52 167 23 53 35 138 |
| 176 169 53 52 106 171 15 117 et | 6 61 167 52 106 171 39 53 50 52 |
| de chasser 117 167 156 169 | 6 72 167 177 169 117 167 137 22 |
| 145 171 115 167 68 qui ma- | 145 171 115 167 68 154 107 94 |
| noeuvrent dans | 138 164 126 115 176 16 115 167 |
| 20 176 131 75 vous pouvez | 20 176 131 67 126 6 145 175 138 |
| vous rendre en droite | 167 152 138 132 166 164 90 138 |
| ligne | 167 126 115 23 126 68 23 159 92 |
| 156 169 40 35 138 | 53 93 81 94 137 22 6 90 35 138 |
| 169 81 167 138 169 87 53 91 | 169 81 174 169 119 53 115 15 |

Ännu skönjs emellertid föga av orderns verkliga innehåll. Ett litet bidrag ger jämförelsen mellan 15 132 6, som bör motsvara "avec" i början, och 132 166 mot slutet där det gäller att fylla ut frasen "vous pou*vez* vous", vilket ger 15=a, 132 =ve, 6=c, 166=z. Början "vous vous por*tiez*" kan nu fyllas ut då 145 53 måste motsvara *tie,* antingen 145=ti, 53=e eller också 145=t, 53=ie, varav det förra lätt prövas ge riktigare resultat. Chiffermotsvarigheten till frasen "avec son infanterie sa cavallerie" etc. innehåller en upprepning 175 176 126 (vilken också återkommer längre fram). Den enda repetition i frasen, som faller i ögonen är "son", men den kan det ej vara, då chifferserien börjar med 175=vo. En förnuftig mening blir det endast om man antar att varianten II har i stället för "son" ordet "votre", som skulle gå bra, förslagsvis sålunda

175 176 126.
vo t re

Nära slutet kommer då en utfyllnad av *"rendre"* med 115=n, 23=d. Detta ger omedelbart 16=da i "dans" samt utfyllnaden av "*chas*ser" med 72=has. Nu kan också två viktiga ortnamn identifieras, nämligen vurzburg (med t i ch. I) samt sista ordet jena eller iena, allt med tanke på de faktiska omständigheterna kring depeschen. Därmed har man 81=g samt 87 och 119=i (j), slutligen 91=na (i ch. I). Med

6 90 35 138 169 81
c o · u r g

klarnar nu även "coburg". De singuljära förekomsterna 48, 32, 25 visar sig vara beteckningar för resp. "infanterie", "cavallerie", "artillerie". I det skick, vari chiffret nu presenterar sig, är stora delar läsbara:

| I | II |
|---|---|
| L'empereur ordonne que vous | L'empereur ordonne que 175 138<br>vo u |
| vous portiez le | 167 164 90 138 167 152 169 145 53<br>s v o u s po r ti e |
| plus tôt possible | 166 117 137 103 157 176 152 167<br>z t po s |
| 167 138 169 106 171 15 117<br>s u r a | 134 37 117 174 169 106 171 15 117<br>su r a |
| avec son infanterie sa cavallerie | 15 132 6 175 176 126 48 164 153<br>a ve c vo t re inf. v ot |



et son artillerie en ne laissant

15 164
a v

138 169 176 166 35 138 169 81
u r t z b u r g

que ce que Sa Majes-

té a désigné pour

106 78 son principal

but sera de rester

107 87
i

176 169 53 52 106 171 15 117 et
t r e a

de chasser 117 167 156 169
s r

145 171 115 167 68 qui ma-
ti n s

noeuvrent dans

20 176 131 75 vous pouvez
t

vous rendre en droite

ligne

156 169 40 35 138
r co b u

169 81 167 138 169 87 53 91
r g s u r i e na

126 32 50 175 176 126 25 68
re cav. et vo t re art.

94 106 122 171 115 176 15 164
n t a v

138 169 166 35 138 169 81 136
u r z b u r g

20 173 138 53 171 107 87 82 131
u e i

15 52 134 81 94 137 90 138 169
a g o u r

106 51 169 116 168 115 175 176
r n vo t

126 137 148 115 6 119 156 96 3
re n c i

176 177 146 52 169 82 131 169
t e r r

107 92 126 52 167 23 53 35 138
s d e b u

6 61 167 52 106 171 39 53 50 52
c s e et

6 72 167 177 169 117 167 137 22
chas s e r s

145 171 115 167 68 154 107 94
ti n s

138 164 126 115 176 16 115 167
u v re n t da n s

20 176 131 67 126 6 145 175 138
t c ti vo u

167 152 138 132 166 164 90 138
s po u ve z v o u

167 126 115 23 126 68 23 159 92
s re n d re d

53 93 81 94 137 22 6 90 35 138
e g c o b u

169 81 174 169 119 53 115 15
r g su r i e n a

Analysen kan nu knappast behöva detaljeras. En svårighet är måhända ett återstående ortnamn, nämligen

106 171 15 117,
la sa - a - le

vilket entydigt bestäms av andra grupper. I fullständig lösning får chiffret detta utseende:

| I | II |
|---|---|
| L'empereur ordonne que vous | L'empereur ordonne que 175 138<br>vo u |
| vous portiez le | 167 164 90 138 167 152 169 145 53<br>s v o u s po r ti e |
| plus tôt possible | 166 117 137 103 157 176 152 167<br>z le p lus to t po s |
| 167 138 169 106 171 15<br>s u r la sa a | 134 37 117 174 169 106 171 15<br>si b le su r la sa a |
| 117 avec son infanterie sa<br>le | 117 15 132 6 175 176 126 48 164<br>le a ve c vo t re inf. v |
| cavallerie et son artillerie en | 153 126 32 50 175 176 126 25 68<br>ot re cav. et vo t re art. en |
| ne laissant 15 164<br>a v | 94 106 122 171 115 176 15 164<br>ne la is sa n t a v |
| 138 169 176 166 35 138 169 81<br>u r t z b u r g | 138 169 166 35 138 169 81 136<br>u r z b u r g que |
| que ce que Sa Majes- | 20 173 138 53 171 107 87 82 131<br>ce q u e sa ma j es te |
| te a désigné pour | 15 52 134 81 94 137 90 138 169<br>a de si g ne p o u r |
| 106 78<br>la garnison | 106 51 169 116 168 115 175 176<br>la ga r ni so n vo t |
| son principal but | 126 137 148 115 6 119 156 96 3<br>re p ri n c i pa l bu |
| sera de rester | 176 177 146 52 169 82 131 169<br>t e st de r es te r |
| 107 87<br>ma i | 107 92 126 52 167 23 53 35 138<br>ma it re de s d e b u |
| 176 169 53 52 106 171 15 117 et<br>t r e de la sa a le | 6 61 167 52 106 171 39 53 50 52<br>c he s de la sa al e et de |
| de chasser 117 167 156 169<br>le s pa r | 6 72 167 177*169 117 167 137 22<br>c has s e r le s p ar |
| 145 171 115 167 68 qui ma-<br>ti sa n s en. | 145 171 115 167 68** 154 107 94<br>ti sa n s en. qui ma ne |
| noeuvrent dans | 138 164 126 115 176 16 115 167<br>u v re n t da n s |
| 20 176 131 75 vous pou-<br>ce t te direction | 20 176 131 67 126 6 145*** 175 138<br>ce t te di re c ti vo u |

* Uppenbarligen en variant för e.
** Tydligen förkortning av ennemis.
*** Här saknas en grupp för (ti)on.



| | |
|---|---|
| vez vous rendre en | 167 152 138 132 166 164 90 138<br>s po u ve z v o u |
| droite ligne | 167 126 115 23 126 68 23 159 92<br>s re n d re en d ro it |
| 156 169 40 35 138<br>pa r co b u | 53 93 81 94 137 22 6 90 35 138<br>e li g ne p ar c o b u |
| 169 81 167 138 169 87 53 91<br>r g s u r i e na | 169 81 174 169 119 53 115 15<br>r g su r i e n a |

Huruvida denna depesch blev tagen och löst av Napoleons allierade motståndare är som sagt icke känt. Vad man vet är, att man från rysk sida berömt sig av att kunna läsa de i den napoleonska armén använda chiffren. Sålunda har kejsar Alexander 1814 vid en middag i kretsen av franska marskalkar, enligt vad som förtäljs i marskalk Macdonalds Souvenirs, utbrett sig över den ryska dechiffreringstjänstens lösande av franska chiffer under Napoleons ryska kampanj. Han hade därvid uttryckligen bestritt, att detta berodde på att ryssarna kommit i besittning av nyckeln (eller koden) till chiffren. Som framgår av den givna analysen hade det i vart fall varit en skäligen lätt sak att forcera det Napoleonchiffer som använts på sätt som i exemplet från Leipzigslaget varit fallet.

# 3. Edgar Allan Poes guldscarabé

I Edgar Allan Poes Sällsamma historier finns det en, som handlar om en guldscarabé med gåtfulla tecken. På scarabén fann man mellan en dödskalle och ett lamm en besynnerlig inskription, antagligen något slags chiffer. Det såg ut så här:

53 ÷ ÷ † 305 ) ) 6ˣ ; 4826 ) 4 ÷ . ) ; 806ˣ ; 48 † 8q60 ) ) 85 ; I ÷ ( ; : ÷ˣ 8 † 83 ( 88 ) 5ˣ † ; 46 ( ; 88ˣ 96ˣ ? ; 8 )ˣ ÷ ( ; 485 ) ; 5 ˣ † 2 : ˣ ÷( ; 4956ˣ 2 ( 5ˣ = 4 ) 8q8ˣ ; 40 69285 ) ; ) 6 † 8 ) 4 ÷ ÷ ; I( ÷9 ; 48081; 8 : 8 ÷ I ; 48 † 85 ; 4 ) 485 † 528806ˣ 81 ( ÷9 ; 48 ; ( 88 ; 4 (÷? 34 ; 48 ) 4 ÷ ; I6I ; : I88 ; ÷? ;

Denna ramsa ser ut som ett sammelsurium men döljer kanske något hemligt meddelande. Om det verkligen är ett chiffer, är första frågan: på vilket språk? I Poes historia sägs, att teckningen av lammet gav en vägledning. Lammet kunde betyda en viss kapten Kidds signatur (kid på engelska = lamm), och vad man visste om kapten Kidd gjorde det inte troligt, att han kunde ha avfattat ett chiffer på annat språk än engelska. Den hypotesen må då tills vidare få antas. Men hur sen komma nån vart med alla dessa hopgyttrade tecken, siffror, bokstäver, skiljetecken och vad allt som finns där. Alla dessa tecken, ja — men hur många är de då? Ser man noga efter finner man i själva verket inte mer än 19. Sammanlagda antalet tecken understiger något 200. De 19 kan mycket väl vara bokstäver i det engelska alfabetet. Intrycket av besynnerliga räkneoperationer med x och parenteser är måhända avsett att vilseleda?

Men för att få någon reda i röran är det bäst att inte se dem i det hopgyttrade skick de först presenterar. Det blir också lättare då att iaktta upprepningar, som kan ha intresse. Vi får då följande bild, där vissa repetitioner av tre eller flera tecken är



understrukna: bland dem är särskilt att märka ett 7 ggr upprepat trigram ; 4 8. Dessa teckens frekvens är: 8 – 33, ; – 26, 4 – 19. Då e är den vanligaste bokstaven i engelskan och the det vanligaste trigrammet, kan vi försöka införa dessa tolkningar.

5 3 ÷ ÷ † 3 0 5 ) ) 6 ˣ ; 4 8 2 6 ) 4 ÷ . ) 4 ÷ ) ; 8 0 6 ˣ
t h e h h t e
; 4 8 † 8 q 6 0 ) ) 8 5 ; I ÷ ( ; : ÷ ˣ 8 † 8 3 ( 8 8 ) 5 ˣ †
t h e e e t t e e e e
; 4 6 ( ; 8 8 ˣ 9 6 ˣ ? ; 8 ) × ÷ ( ; 4 8 5 ) ; 5 ˣ † 2 : ˣ ÷
t h t e e t e t h e t
( ; 4 9 5 6 ˣ 2 ( 5 ˣ = 4 ) 8 q 8 ˣ ; 4 0 6 9 2 8 5 ) ; ) 6
t h h e e t h e t
† 8 ) 4 ÷ ÷ ; I ( ÷ 9 ; 4 8 0 8 I ; 8 : 8 ÷ I ; 4 8 † 8 5 ;
e h t t h e e t e e t h e e t
4 ) 4 8 5 † 5 2 8 8 0 6 ˣ 8 I ( ÷ 9 ; 4 8 ; ( 8 8 ; 4 ( ÷ ?
h h e e e e t h e t e e t h —
3 4 ; 4 8 ) 4 ÷ ; I 6 I ; : I 8 8 ; ÷ ? ;
h t h e h t t e e t t

De dubbla 8:orna behöver icke chockera, då ee förekommer ofta i engelska. Att th framträder på ytterligare ett par ställen utom i the ökar bara trovärdigheten, likaså de många förekomsterna av typen e . e. Men vissa partier ser onekligen konstiga ut. Vad kan det bli av thet . eeth? En trigramrepetition, som borde kunna hjälpa en bit vidare, är $\begin{matrix} 8\ 5\ ), \\ e\ .\ t \end{matrix}$ då ett av de vanliga trigrammen är ent. Men det för vilse och måste uppges. Om vi återgår till frågetecknet nyss, kan man tänka sig något annat än r i tomrummet? I så fall fick vi följande the tree thr . . . h, kan det sista utfyllas annorlunda än through?

Därmed skulle vi ha funnit beteckningarna (= r, ÷ = o, ? = u, 3 = g. En fyrtalig upprepning $\begin{matrix} ˣ\ ÷\ (\ ;\ 4 \\ .\ o\ r\ t\ h \end{matrix}$ ger oss ytterligare ett av de mest frekventa tecknen, x bör rimligen vara = n.

Det ser verkligen skäligen obegripligt ut fortfarande, trots att så många grupper är införda. Som förekomsten av ÷ visar, är även bokstaven o dubbelskriven två ggr. Den ävenledes två ggr dubbelskrivna ), som har hög frekvens, måste då vara en högfrekvent konsonant, sannolikast s. Om dessa vinster tillgodogörs, får chiffret nedanstående utseende:

```
5 3 ÷ ÷ † 3 0 5 ) ) 6 x ; 4 8 2 6 ) 4 ÷ . ) 4 ÷ ) ; 8 0 6 x
. . o o . g . . . . . n t h e . . s h o . s h o s t e . . n
; 4 8 † 8 q 6 0 ) ) 8 5 ; I ÷ ( ; : ÷ x 8 † 8 3 ( 8 8 ) 5 x †
t h e . e . . . s s e . t . o r t . o n e . e g r e e s . n .
; 4 6 ( ; 8 8 x 9 6 x ? ; 8 ) x ÷ ( ; 4 8 5 ) ; 5 x † 2 : x ÷
t h . r t e e n . . n u t e s n o r t h e . s t . n . . . n o
( ; 4 9 5 6 x 2 ( 5 x = 4 ) 8 q 8 x ; 4 0 6 9 2 8 5 ) ; ) 6
r t h . . . n . r . n . h s e . e n t h . . . . e . s t s .
† 8 ) 4 ÷ ÷ ; I ( ÷ 9 ; 4 8 0 8 I ; 8 : 8 ÷ I ; 4 8 † 8 5 ;
  e s h o o t . r o . t h e . e . t e . e o . t h e . e . t
4 ( 4 8 5 † 5 2 8 8 0 6 x 8 I ( ÷ 9 ; 4 8 ; ( 8 8 ; 4 ( ÷ ?
h s h e . . . . e e . . n e . r o . t h e t r e e t h r o u
3 4 ; 4 8 ) 4 ÷ ; I 6 I ; : I 8 8 ; ÷ ? ;
g h t h e s h o t . . . t . . e e t o u t
```

En lättillgänglig tolkning erbjuder sviten

```
; 4 6 ( ; 8 8 x 9 6 x ? ; 8 )
t h . r t e e n . . n u t e s
```

vilket ger 6=i samt 9=m. Av de vanligare bokstäverna saknas nu alltjämt a, likaså d. De finns bägge i det upprepade trigrammet $\begin{matrix} 5^{x}\dagger, \\ .\,n\,. \end{matrix}$ and, vari n:et redan är känt. Repetitionen $\begin{matrix} I(\div 9 \\ .\,r\,o\,m \end{matrix}$ ger oss I=f. Återstående tecken kan nu icke vålla svårighet. Då alla är införda ser chiffret ut sålunda:

```
5 3 ÷ ÷ † 3 0 5 ) ) 6 x ; 4 8 2 6 ) 4 ÷ . ) 4 ÷ ) ; 8 0 6 x
a g o o d g l a s s i n t h e b i s h o p s h o s t e l i n
```



```
; 4 8 † 8 q 6 0 ) ) 8 5 ; I ÷ ( ; : ÷ x 8 † 8 3 ( 8 8 ) 5 x †
t h e d e v i l s s e a t f o r t y o n e d e g r e e s a n d
; 4 6 ( ; 8 8 x 9 6 x ? ; 8 ) x ÷ ( ; 4 8 5 ) ; 5 x † 2 : x ÷
t h i r t e e n m i n u t e s n o r t h e a s t a n d b y n o
( ; 4 9 5 6 x 2 ( 5 x = 4 ) 8 q 8 x ; 4 0 6 9 2 8 5 ) ; ) 6
r t h m a i n b r a n c h s e v e n t h l i m b e a s t s i
† 8 ) 4 ÷ ÷ ; I ( ÷ 9 ; 4 8 0 8 I ; 8 : 8 ÷ I ; 4 8 † 8 5 ;
d e s h o o t f r o m t h e l e f t e y e o f t h e d e a t
4 ( 4 8 5 † 5 2 8 8 0 6 x 8 I ( ÷ 9 ; 4 8 ; ( 8 8 ; 4 ( ÷ ?
h s h e a d a b e e l i n e f r o m t h e t r e e t h r o u
3 4 ; 4 8 ) 4 ÷ ; I 6 I ; : I 8 8 ; ÷ ? ;
g h t h e s h o t f i f t y f e e t o u t
```

Vad som i detta fall vållat särskild omak är klartextens egendomliga innehåll. Den är så pass svårläst även efter lösningen, att den kanske bör återges som en vanlig text med orden skilda åt. Den lyder alltså:

a good glass in the bishops hostel in the devils seat fortyone degrees and thirteen minutes northeast and by north main branch seventh limb east side shoot from the left eye of the deaths head a bee line from the tree through the shot fifty feet out.

Den som sen är nyfiken på sammanhanget, får gå till Edgar Poes bok. Här gäller det endast chifferlösningen.

# 4. Mannen med järnmasken

## I

I en volym av Grimbergs Världshistoria läser man i en not följande:

Den hemlighetsfulla statsfången på Ludvig XIV:s tid, som alltid måste bära en svart sammetsmask för ansiktet, när han lämnade sin cell, förvandlades i folkfantasin till "mannen med järnmasken". I fem år — till sin död 1703 — satt han i Bastiljen. Hypoteserna om vem fången var är legio. Voltaire påstod, att han var oäkta son till drottning Anna av Österrike. Andra författare gjorde honom till en tvillingbror till Ludvig XIV, vilken skulle ha spärrat in honom till undvikande av tronföljdsstrider. Den hypotesen blev allmänt gängse genom Dumas d. ä:s roman Vicomte de Bragelonne år 1848. Men både denna och en mängd andra sägner avlivades tjugo år därefter av Topin, som framlade starka skäl för att den mystiske fången varit den mantuanske ministern Mattioly, som straffades på detta sätt, därför att han hade förrått ömtåliga statshemligheter.

Grimberg har sålunda ansett saken färdig med Marius Topins undersökning, på sin tid belönad med Franska akademins historiepris. Och Grimberg behövde sannerligen inte ta illa vid sig, om ett arbete förbigått honom i detta ämne, som ställer hela frågan i ny belysning. Det är mycket möjligt, att här åsyftade arbete föga uppmärksammats utanför den lilla kretsen av kryptointresserade. Ty i detta arbete är lösningen av järnmaskens gåta bokstavligen en chifferlösning.

Mannen med järnmasken är en skapelse av Voltaire. Den legendariska figuren, som åstadkommit så många gissningar och sysselsatt så många lärda herrars skarpsinne — det uppges över femtitalet före Topin — är tillkommen i Voltaires "Siècle de Louis XIV", publicerad 1751. Hans inspirationskälla var en allegorisk berättelse — eller nyckelroman på nutidsspråk — som utkom i Amsterdam 1746 under titeln "Mémoires secrets pour



servir à l'histoire de Perse". Efter en sedvänja som florerade särskilt under Mazarins regim uppträder personerna däri under fingerade namn.

Berättelsen är i huvuddrag denna: Prins *Cha-Abas* hade som sin mest älskade favorit en indiska och fick med henne sonen *Giafer*. Denne uppfostrades som prins. Men tronföljare var en annan son, *Sephi-Mirza*. Honom kunde *Giafer*, som var en härskarnatur, aldrig fördra. Han visade tronföljaren öppet sitt förakt och satte därmed sin fader på svåra prov i valet mellan auktoritetens krav och den faderliga ömheten. *Giafer* glömde sig slutligen därhän, att han gav *Sephi-Mirza* en örfil. Efter detta fruktansvärda brott kunde straffet icke utebli. *Cha-Abas* sammankallade sitt kronråd, som mot en röst förordade dödsstraff. Men en av rådsmedlemmarna föreslog för att lindra faderns smärta en utväg, som denne accepterade. *Giafer* skulle sändas till armén, som stod vid gränsen till *Feldraan*. Där skulle spridas det ryktet, att den unge prinsen fått pesten. Så skulle han fingeras död och begravas med all ståt men i hemlighet överföras till citadellet på ön *Ormus* för att där sluta sina dagar. Så skedde, och alla försiktighetsmått vidtogs för hemlighetens bevarande. Kommendanten på *Ormus* serverade prinsen egenhändigt måltiderna. En gång tog denne sig för att med kniven gravera sitt rätta namn på baksidan av en assiett. Den kom i händerna på en slav, som för att visa sin plikttrohet lämnade den till kommendanten. Han belönades härför med att omedelbart avlivas. Prins *Giafer* stannade flera år i *Ormus*, men han flyttades till *Ispahan*, då kommendanten fått denna förnämligare plats och ingen mer borde invigas i hemligheten. Både i *Ormus* och i *Ispahan* var den försiktighetsåtgärden föreskriven, att vid varje tillfälle då den höge fången måste utsättas för andras blickar skulle han bära en mask. Flera trovärdiga personer påstår sig ha mer än en gång sett denne maskerade fånge och har berättat, att han duade kommendanten, vilken å sin sida visade honom den högsta respekt.

Ja, detta är underlaget för legenden. Den innehåller den signifikativa masken, men det är inte alls tal om någon järnmask. Den har Voltaire själv hittat på som en extra krydda. På så vis har "mannen med järnmasken" gått till eftervärlden. I

Voltaires version blir han en av Louis XIV:s efterlämnade statshemligheter. *Cha-Abas* är solkonungen själv. Indiskan är M:lle de la Vallière. *Giafer* deras son Comte de Vermandois. *Sephi-Mirza* är le Dauphin. *Feldraan* är Flandern. *Ormus* är ön Sainte-Marguerite och citadellet i *Ispahan* är Bastiljen. Men underligt nog förvandlas den maskerade fången hos Voltaire till en alltsen födelsen hemlighållen bror till Louis XIV.

Det anses allmänt vara ostridigt, att det i slutet av 1600-talet funnits en maskerad fånge i Frankrike, som omgavs med extra sekretess. Han har vistats först på fästningen Pignerol, sen på ön Sainte-Marguerite och har slutat sina dagar i Bastiljen. Ett dödsbevis av 19 november 1703 för en Bastiljfånge, i beviset kallad Marchioly, har i diskussionen ansetts vara det sista autentiska aktstycket om den okände. Topin har använt namnlikheten som stöd för sin tes.

Vem var han då? I den stora historiska litteratur, som växt upp kring den lockande gåtan, frånsett det stoff den givit till åtskilliga romaner, figurerar bl. a. Louis XIV:s hypotetiske tvillingbroder, hans son med de la Vallière, drottning Anna av Österrikes presumerade illegitime ättling hertigen av Beaufort, Monmouth, ambassadören Mattioly, giftblandaren Oldendorf m. fl.

Ingen tolkning — före den som det här refereras till — torde vara värd större respekt än den som Grimberg anfört, Marius Topins. Men respekten har icke räckt för att låta mannen med järnmasken vila i frid. I en 1893 utkommen volym "Le masque de fer, Révélation de la Corréspondance chiffrée de Louis XIV" har tvenne författare, Emile Burgaud — som torde svara för den historiska undersökningen — och commandant Bazeries, måhända det märkligaste geni på kryptografins område som Frankrike ägde vid denna tid, tagit upp problemet till fullständig revision. De anser sig på starka grunder ha kunnat kreera en alldeles ny men ingalunda någon särskilt romantisk kandidat till "järnmasken". Enligt dem var denne en general de Bulonde, som ådragit sig Louis XIV:s vrede genom att häva belägringen av Coni under kriget mot Savoyen 1691. Med all säkerhet skulle denne person icke riskera eftervärldens nyfikenhet, om icke järnmasken fångat fantasin på ett så fascinerande sätt. Volymen redovisar tämligen omständligt en mängd omständigheter och aktstycken till stöd för sin tes. Huvuddokumentet är emellertid ett av Bazeries forcerat brev i chiffer från krigsministern Louvois till Catinat, kommenderande generalen för Piemontarmén. Bazeries insats i denna historiska undersökning hör till de märkligaste tingen i kryptografins historia. Den innebar nämligen att Le grand chiffre de Louis XIV, som vid denna tid användes och som förut trotsat alla försök till tydning blev så fullständigt forcerat att Bazeries kunnat publicera hela codelistan i det nämnda arbetet.



Frånsett det intresse själva "mannen med järnmasken" alltjämt kan erbjuda är det sålunda fråga om en av de stora bragderna på det kryptografiska området. Och det är ur den synpunkten Burgaud—Bazeries arbete här presenteras.

Något bör dock vara nämnt om den övriga bevisningen, vilken i grundlighet lämnar föga övrigt att önska.

Vad först angår Topins mantuanske ambassadör avlivas denne som järnmask genom att författarna visar, att han dött på Sainte-Marguerite, innan järnmasken överfördes därifrån till Bastiljen. I ett brev från fängelsedirektören meddelas nämligen, att en fånge som hade betjänt med sig avlidit. Och firman B.—B. anser sig kunna fastslå, att Mattioly var den ende därvarande statsfånge, som inspärrats tillsammans med sin lakej.

Genom utdrag ur Bastiljens registratur leds i bevis, att den maskerade fånge som inkom den 18 sept. 1698, av forskarna allmänt erkänd som identisk med järnmasken, var en förutvarande fånge på Pignerol. I detalj genomgår författarna dessa statsfångars öden. Det uppvisas dokumentariskt, att fyra fångar från Pignerol 1694 överförts till Sainte-Marguerite, men endast en av dem, "järnmasken", åtföljde den berömde guvernören Saint Mars, då denne övertog Bastiljen (märk här likheten med Amsterdam-historien). Att generalen de Bulonde arresterades och fördes till Pignerol efter Coni-affären är ett klart historiskt faktum, bl. a. innehöll Gazette de France strax efter denna affär en utförlig relation om saken. Författarna anser sig kunna effektivt motbevisa möjligheten att han senare frigivits. Kungens stora missnöje med generalens uppförande vid Coni är dokumen-

terat liksom den vikt Louis XIV lade vid denna orts besättande. En skrivelse från en kunglig funktionär Barbezieux till guvernör Saint Mars på Sainte-Marguerite läggs i bevisföringen särskild vikt vid på grund av vissa förut icke uppmärksammade överstrykningar i texten, ur vilka framtolkas, att skrivelsen ursprungligen innehållit frasen "de ce g$^{al}$" (= général, i analogi med M$^{al}$, maréchal) men ändrats av diskretionsskäl till "vostre ancien prisonnier". Det enda aktstycke, i vilket förekommer namn på en av Saint Mars fångar från Pignerol, i korrespondensen mellan Sainte-Marguerite och Versailles, innehåller namnet Nesmonde, vilket tolkas som förklädnad för Bulonde. Ett argument, som slående erinrar om Topins Marchioly—Mattioly, och icke kan få högre halt i korrespondensen från Sainte-Marguerite än i dödsbeviset från Bastiljen.

Mycket mer skulle kunna relateras ur denna del av arbetet, men de mest relevanta argumenten torde nu vara nämnda.

Emellertid. Intet av de aktstycken, som bevisligen kan hänföras till generalen de Bulonde innehåller någonting direkt om hans mask. Och det är ju därpå det hänger. Med en strängt reserverad hållning till författarfirmans argumentering kan man säga, att vederbörande lyckas bra — liksom åtskilliga av föregångarna — att kullstörta andras hypoteser. För egen del har de kunnat på ett sammanhängande och icke-motsägande sätt visa, hur alla kända omständigheter låter sig väl förena med hypotesen de Bulonde. Men detta är ju ingen positiv bevisföring. Allt hänger som sagt till sist på masken. Kunde det bara visas, att deras general blev dömd att bära mask då han bortdömdes till Pignerol, då och först då vore beviskedjan sluten.

Detta är vad Bazeries anser sig ha gjort genom dechiffreringen av Louvois chifferdepesch till Catinat. Men den kräver sitt eget utrymme, denna järnmaskmysteriets pièce de résistance.

## II

Den depesch från Louvois, som tillskrivs avgörande betydelse för bestämmandet av järnmaskens identitet, var avsänd till kommenderande generalen Catinat och hade det innehåll, som framgår av nedanstående. Däri har endast för läsarens bekvämlighet



de chiffergrupper som i aktstycket förekommer tre eller fler gånger särskilt utmärkts genom fet stil.

Versailles le 8 juillet 1691.

A Monsieur le Lieutenant Général de Catinat, Commandant en Chef de l'Armée du Piémont.

Monsieur.

L'ordinaire m'a rendu les lettres que vous avez pris la peine de m'écrire le 1er de ce mois.

**434 88 289 260** 326 **52** 164 **198 449** 119 **553** 47 548
526 **501 337** 251 **149 579 70** 31 453 585 405 **68** 42 25
**172 580 93 553** 77 242 496 521 565 461 **9 273** 320 404
**91 493 34 282 255** 97 508 **405** 24 484 **97 68** 285 **172**
**24** 477 **34 194** 455 **517 52 70** 22 222 509 269 131 551
**159** 38 **47** 354 **154 124 194 200** 60 414 22 448 **222**
488 475 348 115 314 302 **289** 193 24 422 **9** 215 **461**
547 **99 52 255** 466 **117 34** 216 150 **260** 405 471 **181**
170 **145** 127 **74** 238 **434 84** 187 **73 117 116** 120 **252**
313 **579 97 79** 246 **9** 233 **171 167** 92 **200 64 159 548**
363 407 **565** 480 151 **276** 83 374 **52** 26 **84** 284 **149**
500 573 347 **172 93** 469 **96 300** 91 **493** 42 **282 255**
**34 273** 24 **84** 574 305 522 206 **194** 88 192 **55 9** 385
**337 402 116 73 276 34** 566 390 **70** 520 544 311 417
214 **154** 22 **419** 13 122 570 129 **64** 159 **145** 339 89
248 437 146 17 136 230 298 **167 34 145** 461 229 **181**
**402 116 580 276** 436 **68** 75 141 **145** 327 204 565 **96**
**97 79 501 174** 450 125 **579** 81 **124 9** 514 292 561 345
**553** 186 **200** 330 309 359 **68** 23 412 565 **34** 566 **289**
152 467 121 **300** 323 **93** 574 **198** 382 403 522 **93** 318
**469 434 26** 585 **337** 55 **115** 191 324 574 503 **24** 487
8 290 415 **42 145** 416 **255 181 34 70** 209

Je suis, Monsieur, votre très humble et très affectionné serviteur.

*Louvois*

Själva texten utgörs helt av chiffer. Inalles förekommer 291 grupper, varav 128 är singuljära. Ett stort antal är repeterade

två gånger. Av själva texten framgår, i vilken utsträckning flerfaldiga repetitioner förekommer. Ingen grupp är upprepad mer än 6 gånger, gruppen 34, och två andra, 9 och 145, förekommer 5 gånger. Fyra repetitioner uppvisar grupperna 24, 53, 70, 93, 97, 255 och 565.

Detta är inget material att angripa med stora förhoppningar, då chiffret tydligen omfattar bortåt 600 grupper (den högsta i detta dokument förekommande är 585). Bazeries skulle heller icke ha kunnat prestera någon säker tolkning, om han endast haft detta material till förfogande. Han vidgår detta själv utan vidare genom sin i ett bihang till det i det föregående refererade arbetet publicerade redogörelse för chiffrets forcering.

Innan ordet lämnas åt honom själv i den delen, må emellertid ett par anmärkningsvärda saker konstateras, som iakttas vid en noggrann genomgång av chiffertexten. Den innehåller ett par längre upprepningar, fastän ej exakt identiska. Det ena paret är

91 493 34 282 255 97
91 493 42 282 255 34

Det andra:

402 116 73 276
402 116 580 276

Högst sannolikt är, att betydelsen av de i vartdera paret ingående chifferserierna är densamma. Men därmed vet vi ju inte vilken.

Det material som stod till Bazeries förfogande bestod av 7 chifferdepescher, tvenne sända av Louvois och fem med Louis XIV själv som avsändare. Av detta material har jag endast haft en mindre del under ögonen, de båda av Louvois och en av konungens. I sin helhet uppger Bazeries chiffermaterialet omfatta över 11 000 grupper, sålunda mer än fyrdubbelt det antal den nyss återgivna "järnmask"-depeschen har. En fullständig statistik visade, att vissa grupper var synnerligen högfrekventa. Sålunda förekommer gruppen 22 ej mindre än 187 ggr, gr. 124 har 185 förekomster och gr. 42 nästan lika många etc.

Men sen gäller det att bryta sig in i chiffret på någon punkt för att förmå siffrorna att börja tala själva, som Bazeries ut-



trycker saken. Han har därvid använt den metod, som fast också tidigare allmänt känd och nyttjad just genom honom fått sin särskilda berömmelse. Det är *det sannolika ordets* metod. Bazeries har antagit att i dessa chifferdepescher, vilka kunde förmodas ha ett militärt innehåll, borde ordet *l'ennemi* resp. *les ennemis* uppträda flerstädes.

En chifferlista på kanske 600 grupper bör innehålla, förutom bokstäver, siffror och skiljetecken jämväl stavelser och något mindre antal vanliga ord. Det här förutsatta sannolika ordet skulle kunna — om nu icke en särskild grupp reguljärt användes därför — avstavas eller bokstaveras som *l-en-ne-mi* eller *le-n-n-em-i* m. fl. varianter. Med stöd jämväl av frekvenserna plockade Bazeries så fram följande sekvenser, vilka samtliga väl kunde tänkas motsvara

| les | en | ne | mi | s |
|---|---|---|---|---|
| 124 | 22 | 146 | 46 | 469 |
| 124 | 22 | 125 | 46 | 574 |
| 124 | 22 | 125 | 46 | 120 |
| 124 | 22 | 125 | 46 | 584 |
| 124 | 22 | 125 | 46 | 345 |

Som synes inleds dessa serier av de tvenne mest högfrekventa grupperna. Bazeries har haft den turen — och tur är som alltid en oersättlig egenskap — att både *les* och *en*, så utomordentligt vanliga i fransk text, i Louis XIV:s grand chiffre vardera har bara en representant. Likaså och mer naturligt stavelsen *mi*. Medan *ne* i coden har 3 representanter, två brukade härovan. För *s* uppträder i dessa sekvenser 5 varianter, och hela coden har visat sig innehålla 7.

Genom denna inkörsport har Bazeries gått in i chiffret, fastän det ingenstädes handlar om les ennemis, och fått siffrorna att tala. Såsom han själv exemplifierar:

| 52 | 124 | 22 | 88 | 374 | 46 | 284 |
|---|---|---|---|---|---|---|
| . | les | en | . | . | mi | . |
| (que) | | | (-n) | (-e) | | (-s) |

Med allenast dessa grupper behärskar man nu mer än 10 % av hela chiffermassan. Man skall emellertid inte för det tro, att

det hela är så lätt avverkat som Bazeries själv framställer det.

Hur pass svårt det är att nå fram till en exakt tolkning på ett relativt litet material har jag i detta sammanhang övertygat mig om. Innan jag tagit del av originalarbetet hade jag ur en andrahandskälla kännedom både om inkörsporten *les ennemis* med därtill hörande chiffergrupper, om hela den här återgivna chiffertexten av 8 juli 1691 samt dessutom dess motsvarighet i klartext enligt Bazeries tolkning. Klartexten var emellertid separat, man kunde alltså inte se innebörden i de enskilda chiffergrupperna. Då jag i järnmaskchiffret införde grupperna från inkörsporten, gav det inalles bara 10 grupper tolkade av samtliga 291. Detta kunde i och för sig inte ge något insteg att få andra, närstående grupper knäckta. I den fullständiga översättning som följer är dessa inkörsportens grupper understrukna, så att läsaren kan döma själv.

Vidare: med ledning av den separata klartexten företog jag mig, sannerligen ej utan ansträngning, att plocka isär den, så att den kunde precis passa ihop med chiffertexten. Jag erhöll också en visserligen på några oväsentliga punkter tveksam men i det hela motsägelsefri transkription i vilken var chiffergrupp hade sig tillagd en enda, konstant betydelse. Men då jag senare fick tillgång till ytterligare ett par med samma chiffer avfattade texter och applicerade min codelista på dem, så visade sig genast att den måste innehålla bra många fel. Ty i de nya texterna uppstod flerstädes ett uppenbart sammelsurium. Till sist fann jag vid jämförelse med den av Bazeries offentliggjorda kompletta codelistan, att min mödosamt tillverkade komposition innehöll ej mindre än ett 40-tal fel däribland sådana som *da* i st. f. *it* eller *nd* i st. f. *mais*. Och man förstår vad oreda sådant kan föra med sig. Felen hänförde sig väsentligen, som naturligt är, till de singuljära förekomsterna. Och hur skulle det vara möjligt att avgöra vilken av följande två tolkningar som är den exakta:

| | | | |
|---|---|---|---|
| 145 | 339 | 89 | 248 |
| la | nuit | it | ns |
| la | nu- | da- | dans |

så länge man icke kan göra kontrollprov på annat håll?



Med all säkerhet har Bazeries haft ett styvt arbete, innan han kommit fram till den lösning som nu skall presenteras. Det har härvid sitt intresse att låta den framträda i två etapper, fast av utrymmesskäl på en gång. Låt oss anta, att arbetet fortskridit så långt, att värden kunnat fastställas på samtliga de grupper, som i Louvois depesch förekommer 3 ggr. Det är dessa som införts i den övre raden, de övriga i den undre.

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 434 | 88 | 289 | 260 | 326 | 52 | 164 | 198 | 449 | 119 | 553 | | |
| il | n | est | pas | que | | | | | avec | | | |
| | | | | necessaire | je | vous | expliqu- | e | | | | |
| 47 | 548 | 526 | 501 | 337 | 251 | 149 | 579 | 70 | 31 | 453 | 585 | 405 |
| | | | | la | | | Sa Majesté | | | | | pris |
| que- | l | des- | p | - i - | si - | r | | a | a - | p - | | |
| 68 | 42 | 25 | 172 | 580 | 93 | 553 | 77 | 242 | 496 | 521 | 565 | 461 |
| le | de | | r | avec | | | | | | | r - d - | |
| | - so - | | - d - | re | lequel | contre | vostre | o - | | | | |
| 9 | 273 | 320 | 404 | 91 | 493 | 34 | 282 | 255 | 97 | 508 | 405 | 24 |
| re | | | | | | de | | lon de | | pris | | |
| | et | sans | necessité | mon - | sieur | bu - | | a | | le | | |
| 484 | 97 | 68 | 285 | 172 | 24 | 477 | 34 | 194 | 455 | 517 | 52 | 70 | 22 |
| parti | de | le | | r | le | | de | co | | que | S.M. | en | |
| | | - ve - | | | siège | | - ni | puis - | | | | | |
| 222 | 509 | 269 | 131 | 551 | 159 | 38 | 47 | 354 | 154 | 124 | 194 | | |
| | | | | | nt | | | | | les | co - | | |
| co - | n - | no - | is - | sa - | mieux | que | personn - | e | | | | | |
| 200 | 60 | 414 | 22 | 448 | 222 | 488 | 475 | 348 | 115 | 314 | 302 | 289 | |
| n | | en | | | | | | | | | est | | |
| | se - | qu | - ces | co - | n - | no - | i - | st | aussi | combien | | | |
| 193 | 24 | 422 | 9 | 215 | 461 | 547 | 99 | 52 | 255 | 466 | 117 | 34 | 216 |
| | le | | re | d | | que | l'on | | | de | | | |
| grand | | p - | - ju - | - i | ce | | recev - | ra | | n'a - | | | |

150 260 405 471 181 170 145 127 74 238 434 84 187 73
·voir pas pris la il fa
cet - te p - - ce don - t - u - d -

117 116 120 252 313 579 97 79 246 9 233 171 167 92 200
ra ta - s r de re n
c - he - se rend - mais - t - re pe-

64 159 548 363 407 565 480 151 276 83 374 52 26 84
nt r elle e que fa
da l hy - ve - . . desir - vous -

284 149 500 573 347 172 93 469 96 300 91 493 42 282
r - re de
s - si - e - z - a - - s - te - r mon - sieur bu -

255 34 273 24 84 574 305 522 206 194 88 192 55 9 385 337
lon de le fa - s co - n re la
et - si - e - z - du - i - a

402 116 73 276 34 566 390 70 520 544 311 417 214
ta elle de S. M.
ci d Pignerol ou veu - t qu'il soit gard-

154 22 419 13 122 570 129 64 159 145 339 89 248 437 146
en nt la ne
e - fe - r - me pe - n - da - nu - it dans u -

17 136 230 298 167 34 145 461 229 181 402 116 580 276
de la d te elle
c - ha - m - b - re - i - ci - ta - d -

436 68 75 141 145 327 204 565 96 97 79 501 174 450
le la r de

et jour ayant li - be - - te se p - ro - me -
125 579 81 124 9 514 292 561 345 553 186 200 330
ne - r les re s avec
sur - m - part - t - u - n **masque**



309 359 68 23 412 565 34 566 289 152 467
le r de est
. comme gouvern - eu Pignerol a vos

121 300 323 93 574 198 382 403 522 93 318 469 434 26
re - s re il
o - r - d - vous luy envoi - e - - z s' vous

585 337 55 115 191 324 574 503 24 487 8 290 415 42
la s le de
p - - i - st ceux - ci - pour - x - e - cu - tion

145 416 255 181 34 70 209
la lon te de S. M. .
vo - -

Som synes är det inte mycket man fattar av sammanhanget, om man bara läser den övre raden

il n'est pas . que . . . . avec . . . . la . . . S. M. etc.

Men något skulle man visst få fram med blott den övre raden given.

Låt oss nu titta igen på de bägge i början observerade repetitionsparen. Den som på allvar ger sig på en uppgift sådan som Bazeries' måste förutsättas noga sätta sig in i tidsomständigheterna. Han bör känna till betydelsen av affären vid Coni och ha läst Gazette de France's relation därav, vari bl. a. omtalas, att "le Roy a envoye ordre au sieur de Catinat de faire arreter le dit sieur de Bulonde et de l'envoyer dans la citadelle de Pignerol". Han söker då efter denne Bulonde och måste fängslas av de bägge serierna

91 493 34 282 255 97
. . de . lon de
(mon sieur) (bu)
91 493 42 282 255 34
. . de . lon de

Det andra paret för tankarna till Bulondes otrevliga adressort la citadelle de Pignerol. Eller hur?

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 337 | 402 | 116 | 73 | 276 | 34 | 566 | 34 | 145 | 461 | 229 | 181 |
| la | . | ta | . | elle | de | . | de | la | d | . | te |
| | (ci) | | (d) | | | (Pignerol) | | | | (i) | |

| | | | | |
|---|---|---|---|---|
| 402 | 116 | 580 | 276 | 436 |
| . | ta | . | elle | . |
| (ci) | | (d) | | |

Och den första serien föregås omedelbart av

| | | | | | |
|---|---|---|---|---|---|
| 194 | 88 | 192 | 55 | 9 | 385 |
| co | n | . | . | re | . |
| | | (du - i) | | | |

För att ge ännu ett exempel, vad annat kan slutet vara än

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 42 | 145 | 416 | 255 | 181 | 34 | 70 | 209 |
| de | la | . | lon | te | de | S. M. | |
| | | (vo) | | | | (punkt) | |

Exaktheten i Bazeries tolkning har på ett överraskande sätt kunnat kontrolleras. Någon tid efter det Bazeries fullbordat sitt arbete påträffades i arkivet en klartext, som visade sig vara en trogen kopia av en bland de redan dechiffrerade depescherna. Beviset kan ju vara bra mot en Tomas bland historikerna. För en kryptolog är det ganska överflödigt. En tolkad chiffertext bevisar själv sin äkthet.

Men för att nu återgå till pudelns kärna, hur står det till med beviset för järnmaskens identitet? Det är sagt förut, allt hänger på masken. Och den återfinns ju i chiffret i ett oklanderligt klart sammanhang. Men tråkigt nog just den chiffergruppen, som är ensamt avgörande, kan icke verifieras. Den är singuljär. Inte bara i detta chiffer utan i hela det kända materialet är den använd bara denna enda gång. Och ännu tråkigare den kan aldrig verifieras med mindre nya texter kommer i dagen av le grand chiffre de Louis XIV.

Det måste medges, att Bazeries har sannolikheten för sig. Han anmärker själv, att det språkliga sammanhanget pekar på ett föremål och inte på en person. Eljest, kunde inte den stackars generalen få promenera "avec un sergent"? Bazeries har väl rätt i att det vore sämre franskt språkbruk. Men tvivlet, en gång väckt, frågar: varför ska just ordet *masque* ha en speciell grupp i ett chiffer om blott 600 grupper? Då det till på köpet visar sig, att gruppen använts bara en enda gång. Förutsågs det behovet av den expert, som tillverkade coden? Tänk om det i stället här hade chiffrerats *ma-s-que,* då hade saken varit absolut klar. Man tittar efter vad det är för ord som i coden fått särgrupper och finner då vid sidan av ordet *masque* också *manque* och *marque,* inte heller särdeles vanliga kan man tycka. Ordförekomsten i listan väcker överhuvud så pass förundran, att ens undran över *masque* dämpas. Så t. ex. kan man väl också finna det konstigt att i detta lilla chiffer inrymma en speciell grupp för orten Pignerol. Coden innehåller 10 ortnamn och nästan alla i de trakter som berörs av fälttåget mot Savoyen. Var kanske detta chiffer avsett just därför? En fråga utan svar.

Med allt resonerande kommer man inte över det faktum, att masken icke kan med visshet verifieras. Fastän bevisningen som helhet är starkt övertygande, kan skeptikern alltid få plats ändå för ett litet frågetecken. Som kryptografisk bedrift kommer Bazeries arbete i alla fall att stå sig. Och skulle det lilla frågetecknet också stå sig, skulle Grimberg ha kunnat känna sig ännu mer obesvärad av att en not i hans Världshistoria blivit på detta sätt attackerad.

# 5. Farliga börssiffror

Det berättas från förra världskriget. Och är inte historien exakt sann, så har den så många släktingar av äkta börd, att den kan berättas ändå. Handlingen är förlagd till London. Ett nummer av Berliner Tageblatt lämnades till granskning av en expert på hemlig skrift. Det misstänktes innehålla något dolt meddelande av vikt. Förmodligen var mottagaren av numret någon figur, som vederbörande hade skäl att hålla under observation.

En sak innehöll tidningen, som var tydligt förmärkt med rödpenna. Det gällde en med stora rubriker uppslagen tysk seger. Men experten tillskrev inte det förstrukna någon undermening. Det kunde ju helt enkelt skylta som motivet för numrets avsändande. Han forskade alltså vidare. Till sist hittade han på affärssidan något han fäste sig vid. Bland den mängd sifferuppgifter som förekom i börsmeddelandena visade sig vissa vara diskret förprickade med en liten punkt under siffran. Inte mindre än 222 siffror hade ett sådant märke.

Dem skrev experten upp i ordningsföljd och fick då fram följande sifferserie:

1 8 5 6 2 9 5 9 3 7 6 9 3 6 7 4 1 8 7 4 2 2 7 4 2 5 5 5
3 7 5 4 2 8 6 9 4 3 6 7 3 5 6 2 2 1 6 6 2 6 7 0 3 5 6 7 3
7 5 8 3 9 6 9 3 2 4 4 3 2 6 8 2 9 7 9 3 6 6 3 4 1 6 3 3 1
7 4 2 5 5 9 2 8 6 8 3 2 7 7 8 1 1 9 6 6 2 3 6 3 2 8 7 6 2
9 6 5 3 2 7 6 3 1 6 0 2 5 6 1 3 6 8 0 2 2 7 6 1 7 2 2 7 6
2 2 7 2 4 2 7 4 2 5 6 3 3 1 6 1 3 5 5 9 1 8 5 8 4 2 5 6 4
2 6 7 1 8 7 9 2 3 6 9 3 8 7 2 3 7 6 2 3 6 6 3 2 4 6 8 1 8
6 6 5 3 2 4 7 3 2 6 7 6 3 9 6 1 2 1 6 6

Frågan var nu, om den förprickning som gett upphov till denna rad av siffror verkligen haft till mening att överbringa



något hemligt meddelande. Den kryptografiske författare, ur vars arbete själva historien är hämtad, beskriver rätt omständligt de olika prov experten gjorde för att utröna om sifferserien kunde vara uppbyggd på något känt chiffersystem.

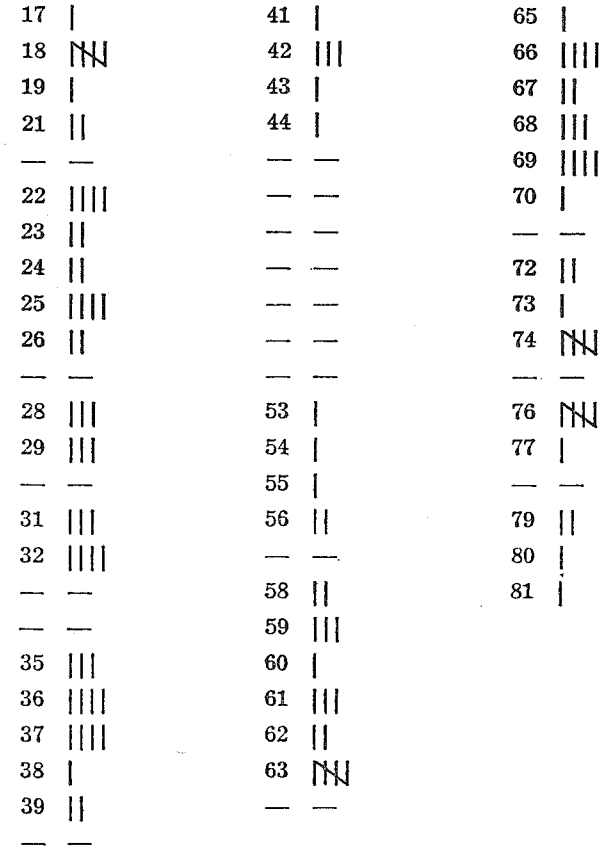
Han delar upp ramsan i 5-siffergrupper och diskuterar möjligheten av en lexikoncode. Han tar siffrorna tre och tre och undersöker de uppkommande grupperna både som de är och efter en addition av de tre siffrorna i var grupp. Han uppdelar i 2-siffergrupper och begrundar därvid också alternativet att grupperna kan representera flera olika alfabet. Han kommer i alla dessa prov till negativt resultat. Tills han får en fruktbar idé genom iakttagelsen, att vid uppdelning två och två ingen grupp är lägre än 17, ingen högre än 81. Därmed kommer han det använda systemet på spår.

Här skall emellertid en betydligt enklare och mera direkt väg beträdas. Den undersökning som anbefaller sig själv förrän man provar mera komplicerade system är uppdelningen i 2-siffergrupper. De enskilda 10 siffrorna kan ju icke i något språk bilda ett alfabet. Men 2-siffergrupperna 00—99 räcker till 4 olika alfabet eller till multipla representationer i stor skala. Även här finns det möjlighet till många varianter. Men man bör i vart fall undersöka detta innan man börjar titta på 3-, 4-, 5-siffriga tal.

Så uppställt får det presumerade chiffret det utseende här nedan visas. Förekommande dubbeluppreprepningar är däri utmärkta med fetstil.

18 56 29 59 37 69 36 74 18 74 22 74 25 55 37 54 28 69
43 67 35 62 21 66 26 70 35 67 37 58 39 69 32 44 32 68 29
79 36 63 41 63 31 74 25 59 28 68 32 77 81 19 66 23 63 28
76 29 65 32 76 31 60 25 61 36 80 22 76 17 22 76 22 72 42
74 25 63 31 61 35 59 59 18 58 42 56 42 67 18 79 23 69 38
72 37 62 36 63 24 68 18 66 53 24 73 26 76 39 61 21 66

Till denna "text" ansluter sig följande frekvensstatistik, uppställd så att även de tomma rummen kommer till synes.




Här är nu åtskilliga iakttagelser att göra. Antalet siffertal som använts är 46. Ett enda enkelt alfabet kommer alltså icke i fråga. Men två? Här är ju att räkna med det internationella alfabetet om 26, så antalet bör räcka då säkerligen några av alfabetets bokstäver saknas i texten — om det nu finns någon sådan under siffrorna. Men se närmare efter, det stora tomrummet i mitten delar upp sifferraden i två var för sig ganska sammanhängande hälfter, den ena omspännande utrymmet 17 — 44, den andra med omfånget 53 — 81. Den undre halvan innehåller 22 an-



vända och 5 icke använda tecken. Den övre resp. 24 och 4. Bägge hälfterna ger fullt utnyttjade plats för något mer än alfabetets 26 bokstäver, de inrymmer resp. 27 och 28. Men det kan ju alltid vara något skiljetecken med?

Den ena halvan ligger som synes under 50, den andra över. Läser vi med uppmärksamheten fäst därpå nu igenom chiffertexten, är det en sak som slår en. Vartannat tal är under, vartannat över 50. Detta är genomgående med 4 undantag. Dessa undantag förekommer i siffersviterna 32 44 32; 77 81 19; 76 17 22; 66 53 24. Samtliga dessa visar sig innehålla siffror som finns i början och slutet av varje halvdel, sålunda 17 och 44 samt 53 och 81. Och alla dessa är blott en gång representerade. Kan då icke dessa ha en alldeles särskild betydelse vid sidan av alfabetet?

Vi vet visserligen icke ännu vilket språk som använts, omständigheterna talar för tyska eller engelska. Men det kommer kanske i dagen av sig själv, om vi provar det vanliga alfabetets insättande i vardera halvan för sig med uteslutande av yttersiffrorna. I den lägre halvdelen får vi då precis plats för de 26 bokstäverna. Insatta i normal ordning 18 = a, 19 = b etc. får de också naturlig frekvens. Men den övre halvdelen har ett tecken för mycket. Tvekan kan där uppstå, om man skall börja med 54 = a och utelämna även den näst sista eller utelämna två i början och låta alfabetet börja 55 = a. (Bägge dessa tal är singuljärt företrädda.) Frekvensen kan ge ledning, men eftersom språket inte är känt blir det enklare att göra ett litet prov på chiffrets början.

Låt det övre alfabetet börja med 55 = a, så erhålles av de 4 första grupperna med tillämpning varannan gång av det undre och övre alfabetet

| 18 | 56 | 29 | 59 |
|---|---|---|---|
| | b | | e |
| a | | l | |

alltså *able*. Är det alltså engelska? Fortsättningen svarar ja. Ty sen kommer

37 69 36 74 18 74 22 74 25 55 37
o t t t a
t s a e h t

eller *able to state that.*

Ja, därmed tycks saken vara klar, och det är väl bara att gå på. Men gör man det efter samma schema, så blir det ett bra konstigt sammelsurium som "konstateras". Ty efter *that* skulle då — med uteslutande av gr. 54 — komma följande, fram till gr. 44

28 69 43 67 35 62 21 66 26 70 35 67 37 58 39 69 32
o m h l p m d o
k z r d i r t v o

Nå vad betyder den ramsan kozmrhdliprmtdvoo?

Den som inte ger upp här får emellertid på andra sidan gr. 44 uppleva en överraskning. Ty fortsättningen blir

32 68 29 79 36 63 41 63 31 74 25 59 28 68 32 77 81
n y i i t e n w
o l s x n h k o

Nu har det blivit förnuft igen: *only six in the know*. Men likaväl blir man rosenrasande från 81 till 17. Där får man översättningen

blfikvlkovnfhgszev

Från 17 till 53 är allt i rätta gängor igen, avsnittet ger *every thing ready by may fourth signal.* Men sen slutar det hela med det upplysande

gsivvgdl.

Tydligt är att de ur alfabetet uteslutna siffrorna 17, 53, 44, 81 har en särskild betydelse. Men bra säreget, om det var den att skilja begripliga och obegripliga stycken. De läsliga delarna ger f. ö. icke något sammanhang enbart för sig.

En mycket enkel observation kan emellertid bringa ordning i det hela. Ett alfabet kan också läsas baklänges. Om två alfabet uppställs över varann, det ena rättvänt, det andra bakfram och



man gör utbyte mellan de rätt över varann stående bokstäverna, erhålls vad man kallar ett inverterat alfabet.

abcdefghijklmnopqrstuvwxyz
zyxwvutsrqponmlkjihgfedcba

vilket ger a = z; e = v; r = i; och vice versa.

Pröva denna invertering på slutet av första sammelsuriet

dvoo
*well*

Well, det är bara att förfara så med alla de obegripliga ramsorna. Såsom synes

k o z m r h d l i p r m t d v o o b l f i k v l k o v
*p l a n i s w o r k i n g w e l l* *y o u r p e o p l e*
n f h g s z e v g s i v v g d l
*m u s t h a v e* *t h r e e t w o*

Det var alltså något allvarligt menat med punkterna under börssiffrorna. Vad adressaten fick besked om var: *Able to state that plan is working well Only six in the know. Your people must have everything ready by may fourth Signal three two.*

Sen detta blivit uppenbart, torde det ha gått lika illa med komplotten som med adressaten.

Nu återstår att förklara systemet, som emellanåt används. Mellan två alfabet, det ena ordinärt, det andra bakfram, skjuts två rörliga remsor eller stavar med siffror att ersätta bokstäverna med. Den ena remsan är numrerad från 1 till 50, den andra har siffrorna 51—99. Då de kan ställas in som man vill, kan man erhålla ett stort antal ordnade alfabet ur vardera remsan. Man kan börja med vilken siffra som helst från 1 till 25 på den ena och från 51 till 74 på den andra. Men därjämte kan man alternativt använda det rättvända och det omvända bokstavsalfabetet. Sedan ett inom de möjliga gränserna godtyckligt läge valts för de båda sifferremsorna, kan varje bokstav erhålla 4 olika siffergrupper som representant. Figuren härnedan illustrerar hur systemet fungerar.

| A B C D E F G H I J K L M N O P Q R S T U V W X Y Z |
|---|
| . . 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 . . |
| . . 52 53 54 55 56 57 58 59 60 61 62 63 64 65 66 67 68 69 70 71 72 73 74 75 76 77 78 89 80 81 82 83 . . |
| Z Y X W V U T S R Q P O N M L K J I H G F E D C B A |

De överflödiga grupperna 17, 44, 53, 54, 81 har använts för att markera var ombyte skett mellan de bägge A B C-raderna. Att detta ombyte sker på rätt långa periodiska avstånd har emellertid underlättat systemets avslöjande. Forceringen hade blivit försvårad, om alfabeten ombytts lite hur som helst och utan markering med särskilda tal. För en mottagare som känner systemet möter avläsningen ändå ingen svårighet, bara han ser var de substituerande sifferalfabeten har sin början. Och just detta framgår f. ö. icke direkt av det här behandlade chiffret. En oförlåtlig oförsiktighet är det också att växla med sådan regelbundenhet från den ena till den andra sifferremsan. Detta är alls inte behövligt, växlingen borde även i denna del ha varit så irreguljär som möjligt. Som chiffret nu var beskaffat har avsändaren ett drygt ansvar för det öde som på sin tid drabbade Berliner Tageblatts adressat i England.



# 6. Le petit chiffre de Napoléon

Under den stora koalitionens fälttåg mot Napoleon år 1813 höll denne Danzig besatt av en garnison, rätt brokigt sammansatt av fransmän, bayrare, polacker och andra i la Grande Armée enrollerade trupper. Danzig blockerades av engelska flottan och belägrades av en kombinerad rysk-preussisk armé. Garnisonen försvarade sig hårdnackat under befäl av generalen Rapp. I början av november hade den varit innesluten i 10 månader. Då inträffade en svårartad eldsvåda som konsumerade proviant för 4 månader.

I denna situation vidtog kommendanten åtgärder för att skyndsamt underrätta Napoleon om garnisonens tröstlösa belägenhet och förbereda honom på att den snart måste ge sig, om inte undsättning kom som hävde cerneringen. Till den ändan avsände han sjövägen sin ordonnans Marnier, utrustad med en längre, till större delen i chiffer avfattad rapport om tillståndet i Dantzig, som namnet stavades på den tiden. Denna rapport är daterad 6 november och avgick med Marnier den 8:de, då denne lyckades ta sig ut ur hamnen utan att uppsnappas av de engelska örlogsmännen. Men framgången av denna äventyrliga expedition var tvivelaktig. General Rapp avsände därför några dar senare en kopia av samma depesch med en agent, som stack sig in bland en skara undan bombardemangen flyktande ortsbor och på så vis kom ut ur staden.

Intetdera exemplaret av general Rapps rapport nådde emellertid sin adressat, kejsaren. Marniers expedition blev en hel liten Östersjö-odyssé. Hans rapport, som finns i franska krigsarkivet, verkar äventyrsroman precis som den är av honom själv avfattad. Han klarar sig ut ur hamnen en klar månskensnatt, förföljs av tio engelska örlogsfartyg och räddas undan dem genom en svår storm, som tvingar dem att tänka på sin egen säkerhet. Hans lilla farkost, bemannad med en 8 man stark

heterogen besättning, två fransmän, en spanjor, två tyskar, en Danzig-bo och en som Marnier själv kvalificerar helt enkelt som kosmopolit, råkar emellertid för egen del illa ut. Stormen driver farkosten redlöst mot svenska kusten. Den strandar vid Öland och inspekteras där av svenska officerare och pastorn i "Kerglosa", vilka misstänksamt mottar beskedet, att skutan för preussisk flagg. Marnier inbjuds att dinera hos sagde pastor men finner inviten alltför betänklig. Svenskarnas förehavanden finner han tyda på onda avsikter och han bestämmer sig för det desperata företaget att gå i land med besättning, ammunition och proviant och bemäktiga sig ett fyrtorn i närheten. Men han hindras därifrån av en ny fara. Två engelska fartyg närmar sig utifrån havet. Då ger han sin besättning dubbel ranson brännvin och går själv till anfall mot det närmaste. Skutan har han lyckats göra flott under förhandlingarna med svenskarna. Hans skuta är dock i så dåligt skick, att den håller på att gå till botten under striden. Han låter sin besättning äntra fiendefartyget och gör sig till herre över detta med dess 25 man och fyra kanoner och får i detsamma se sin egen skuta gå till botten. Han lyckas segla ifrån det andra engelska fartyget men befinner sig en morgon mitt i en större engelsk konvoj, som hans nyförvärvade farkost troligen tillhört. Ingen misstänker något och han seglar lugnt med engelsmännen i fyra dar. Konvojen drivs hit och dit av stormiga vindar, är ett tag ända uppe vid Finska viken men kommer efter några dar i närheten av Bornholm. Där lyckas Marnier skilja sig från sällskapet och ankrar under skydd av batterierna vid Rönne, blir charmant mottagen av Napoleons danska allierade och kommer efter ytterligare äventyr — också vid avfärden från Bornholm förföljd, denna gång av svenska krigsfartyg som legat på vakt utanför Rönne hamn — fram till Köpenhamn. Där mottas han nådigt av danska majestätet och fortsätter via Hamburg för att överbringa sitt budskap. Men han måste vända, då han hör att krigshändelserna utvecklat sig därhän, att de allierades trupper ryckt in i Frankrike. Återkommen till Köpenhamn erfar han kejsarens abdikation och kungens intåg i Paris. Han återvänder till Paris och skriver ner sin äventyrsskildring. Men rapporten stannar hos honom. Varken kejsaren eller den tappre kommendanten i



Danzig kunde nu ha något intresse av hans mission. General Rapp och hans garnison hade kapitulerat redan den 17 november efter nya förödande bombardemang.

Hur det gick med den duplicata av rapporten som skickades med hemlig agent vet man ingenting om, mer än att varken agent eller rapport kom fram. Det sannolika är att bägge föll i händerna på Napoleons fiender. Och de bör då ha fått klart för sig hur förtvivlad ställningen var i den belägrade staden.

Verkligen? Kan man förutsätta att de var i stånd att dechiffrera rapporten? Ja, det är mycket möjligt som vi nu skall se.

Det måste för den skull bringas i läsarens erinran en sak, som tidigare här skildrats. Redan i september hade under uppmarschen till Leipzigslaget Berthier begått oförsiktigheten att sända Augereau en dubbel depesch i blandning av chiffer och klartext. Att dess hemlighet var förlorad för den som var i besittning av dess bägge varianter har här förut visats.

Illa nog kan det genmälas, men behöver den olyckan gå ut över andra chifferdepescher avfattade under helt andra omständigheter och avhandlande andra ämnen? Ja det är just den saken som nu skall undersökas.

Låt oss först förutsätta, att Rapps Danzigrapport sätts i händerna på en expert med tillgång till de dechiffrerade Leipzigdepescherna. Denne börjar då sitt arbete på den nya chiffertexten med ett högst värdefullt startkapital, nämligen den ordlista han fått ur de förra.

Dessa var ju bägge ganska korta och man kan därför tro — innan man gjort erfarenheten själv — att de inte avslöjar mycket utöver sitt eget innehåll. Ser man nu efter finner man, att de två Leipzigdokumenten ger kännedom om inalles 69 chiffergrupper och möjlighet att uppställa den preliminära codeförteckningen överst på sid. 52.

Gällde det en code om tusentals grupper vore detta resultat en mycket bra början. Men är det som här — "Le petit chiffre de Napoléon" — fråga om 200 grupper, blir effekten närmast fruktansvärd.

Vi skall pröva den på några partier av general Rapps depesch. I sin helhet är den alldeles orimligt för lång för att åter-

*Grupper kända från Leipzigdepescherna:*

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 3 | bu | 53 | e | 103 | lu | 148 | ri |
| 6 | c | 61 | he | 106 | la | 152 | po |
| 15 | a | 67 | di | 107 | ma | 153 | ot |
| 16 | da | 68 | en | 115 | n | 154 | qui |
| 20 | ce | 72 | ha | 116 | ni | 156 | pa |
| 22 | ar | 75 | direction | 117 | le | 157 | to |
| 23 | d | 78 | garnison | 119 | i | 159 | ro |
| 25 | art. | 81 | g | 122 | is | 164 | v |
| 32 | cav. | 82 | es | 126 | re | 166 | z |
| 35 | bo | 85 | h | 131 | te | 167 | s |
| 37 | b | 87 | i/j/ | 132 | ve | 168 | so |
| 39 | al | 90 | o | 134 | si | 169 | r |
| 40 | co | 91 | na | 136 | que | 171 | sa |
| 48 | inf. | 92 | it | 137 | p | 173 | q |
| 50 | et | 93 | li | 138 | u | 174 | su |
| 51 | ga | 94 | ne | 145 | ti/on/ | 175 | vo |
| 52 | de | 96 | l | 146 | ra | 176 | t |
| | | | | | | 177 | se |

ges. Här intas början, slutet och ett litet stycke inne i texten. I chiffertexten införs omedelbart de ur "ordlistan" kända betydelserna. Början ser då ut sålunda:

Danzig le 6 novembre 1813.

Sire,

J'envoye près de Votre Majesté un de mes aides de
camp pour lui rendre compte 52 106 167 119 150 15 145
de la s i — a tion
52 106 137 106 20 de 12 46 107 96 61 138 169 119 126 156
de la p la ce — — ma l he u r i r re
146 37 117 82 176 22 148 148 132 119 6 119 dans la 104
pa ra b le es t ar ri ve i c i —
119 176 76 137 126 95 62 15 138 52 138 151 de ce 111 119
i t — p re — — a u de u — — i
167 117 58 15 6 149 174 99 117 167 45 145 53 169 167 de
s le — a c — su — le s — ti e r s



121 167 19 137 137 159 161 167 119 90 94 99 115 167 50
— s — p p ro — s i o ne — n s et
134 les 22 114 53 167 de V. M. 94 106 99 176 176 68 176
si ar — e s ne la — t t en t
68 50 34 52 69 119 126 37 119 68 157 176 117 132 169 117
en et — de — i re b i en to t le ve r le
167 119 53 60 106 177 138 117 165 169 167 165 6 145 132
s i e — la se u le — r s — c ti ve
52 20 176 176 53 78 qui s'est 97 111 169 158 93
de ce t t e garnison — — r — li
177 53 par 52 110 115 81 167 et continuels 174 6 6 53 167
se e de — n g s su c c e s
82 176 de 176 62 95 94 169 par 52 110 115 81 167 et continuels
es t t — — ne r de — n g s
174 6 6 53 167 82 176 de 176 62 95 94 169 par la 4 137
su c c e s es t t — — ne r — p
145 161 131 46 53 52 134 glorieuse
ti — te — e de si
119 53 119 139 115 167 15 20 146 137 137 90 169 176
j e j — n s a ce ra p p o r t
les 53 158 176 167 de 134 150 15 145 des 176 159 138 137
e — t s si — a tion t ro u p
137 53 167 tant 9 142 90 115 115 53 176 176 53 167 que 107
p e s — — o n n e t t e ,s ma
106 52 167 et 6 149 170 117 167 20 115 176 167; 117 167
la de s c — — le s ce n t s le s
53 158 176 167:
e — t s

Att ett på detta vis ifyllt chiffer icke har många av sina hemligheter kvar bör lite var kunna se genast. Avläsningen av luckorna underlättas också av de repetitioner som uppträder bland de förut okända grupperna. Dessa upprepningar har feta siffror. Man begriper utan vidare, att det i begynnelsen liksom mot slutet är tal om *"la situation"*. Inte heller behöver man tveka mycket om att 12 betyder Danzig. Att gruppen därefter betyder *"un"* är väl också vad man närmast gissar på, fast det förvirrar

att mot slutet finna *"un-e de si glorieuse"*. Fattas det inte här en grupp, så att det blir *une défense si glorieuse?* Verkliga sammanhanget är, att i chiffersystemet ingår att låta vissa bigram samtidigt betyda en längre bokstavsgrupp eller ett ord. Vi ha 145 = *ti* eller = *tion*. I analogi 52 = *dé(fense)*.

Den irreparabla malheuren har inträffat — när? *dans la — it — pre — — au deu* — måste vara *la nu-it du premi-er au de-u-x*. Och grupperna 95 62 bekräftar, repeterade i omvänd ordning i senare delen, där de ger *de t-er-mi-ne-r*. Tidsbestämningen innehåller också *de ce — is*, vilket sista måste vara *mo-is*. Det klarar upp vad det är garnisonen gjort: *qui s'est — — r — li see*. Det blir *im-mo-r-ta-li-se-e*, med konfirmation genom upprepningar av gr. 158, på ett ställe *les e — ts = etats* och i slutet likaledes *le-s e-ta-ts*. Men vad hände vid den angivna tidpunkten? Jo, *le — a c — su — les — tiers de — s — ppro — sione — ns*. Med hjälp av upprepningar får man le ? a c-on-su-me-les ? tiers de ? s appro-vi-sione-me-ns, där man tills vidare får sätta frågetecken för grupperna 58 (= feu), 45 (= quar) och 121 (= no). Chiffret ger, icke i denna del men i sin fortsättning, fullgod bekräftelse på de inom parentes angivna tolkningarna. I fortsättningen kan man tveka, om i frasen *et si les ar — es de V. M.* skall läsas ar-m-es eller ar-mé-es, bådadera acceptabla, den förra läsarten den riktiga. Sen står det klart *ne la me-ttent en et-at* de fa-ire bientot lever le sie-ge. Chifferserien

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 117 | 165 | 169 | 167 | 165 | 6 | 145 | 132 |
| le | — | r | s | — | c | ti | ve |

är lika lustig och löslig som ett korsord, naturligtvis *pe*-r-s-*pe*-ctive. Garnisonen har odödliggjort sig genom — *ongs et continuels succès*, tydligen *l-ongs*. Den riskerar nu, att slutet ska bli la — pti — te, däri gruppen 161 (= vi) redan är bestämd; uppenbart ska man läsa *ca-p-ti-vi-te*. I slutet talas det om *malades et c — — lescents*, läs *c-on-va-lescents*, konfirmerande gr. 149 = *on*.

Besynnerligt ter sig väl — om man icke känner tidens militära språkbruk — den före *malades et convalescents* upptagna kategorin — — onnettes. Men sammanhanget pekar på vapenföra, för vilka användes termen *ba-y-onnettes*.



Utan sådana pekpinnar som de nu brukade kan läsaren tillgodogöra sig övriga partier av rapporten. De är uppställda så, att i en övre rad de från Leipzigchiffren kända gruppernas betydelse införts och i en undre de nya gruppernas tolkning.

| | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Nos | 165 | 167 | 16 | 115 | 167 | 96 | 118 | 76 | 46 | 15 | 138 | 44 | sont |
| | — | s | da | n | s | l | — | — | — | a | u | — | |
| | pe(rte) | | | | | | incendie | du | 1 | | | 2 | |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| 97 | et telle chose | 173 | 138 | 90 | 115 | 162 | 87 | 167 | 167 | 53 |
| — | | q | u | o | n | — | i | s | s | e |
| im(menses) | | | | | | pu | | | | |

| | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 69 | 87 | 126 | 63 | 117 | 167 | 126 | 76 | 87 | 177 | 115 | 176 | 106 | 52 | 15 |
| — | i | re | — | le | s | re | — | i | se | n | t | la | de(fense) | a |
| fa | | | el | | | | du | | | | | | | |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 45 | 11*) | 87 | 167 | 15 | 138 | 137 | 103 | 167 |
| — | — | i | s | a | u | p | lu | s |

Je ne dois pas finir sans faire observer à Votre Majesté

| | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| que | 106 | 78 | 94 | 177 | 40 | 114 | 152 | 177 | en parti que | 23 | 39 | 93 | 82 |
| | la | garn. | ne | se | co | — | po | se | | d | al | li | es |
| | | | | | | m | | | | | | | |

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 50 | qu'il n'y a | 52 | 73 | 146 | 115 | 4 | 122 | 136 | 106 | 44 | 2me | 67 |
| et | | de | — | ra | n | | is | que | la | — | | di(vision) |
| | | | f | | | ca | | | | (2) | | |

| | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 106 | 111 | 92 | 53 | 52 | 106 | 44 | 23me | 50 | 96 | 82 | 44 | régiments | 52 | 32 |
| la | — | it | e | de | la | — | | et | l | es | — | | | de cavallerie |
| | mo | (i) | | | | (2) | | | | | 2 | | | |

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| à peu près | 106 | 111 | 92 | 53 | 52 | 96 | 25 | 117 | 60 | 116 | 53 | 106 |
| | la | — | it | e | de | l | artillerie | le | — | ni | e | la |
| | | mo | (i) | | | | | | ge | | | |

* Uppenbart skrivfel 11 i st. f. 111; antalet månader kan ej utläsas ur denna del av chiffret.

| | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 107 | 148 | 94 | 50 | 106 | 44 | 22me | | 67 | | 174 | laquelle | je | 6 | 159 |
| ma | ri | ne | et | la | — | | | di(vision) | | sur | | | c | ro |
| | | | | | (2) | | | | | | | | | |

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 122 | 136 | 96 | 149 | 165 | 138 | 176 | 40 | 114 | 137 | 176 | 62 | |
| is | que | l | — | — | u | t | co | — | p | t | — | |
| | | | on | pe | | | | m | | | er | |

Je suis avec le plus profond respect, Sire, de Votre Majesté Impériale et Royale, le très humble et fidèle sujet.

Signé: R A P P.

Rapporten innehåller i övrigt en så dokumenterad och utförlig skildring av garnisonens och förrådens miserabla tillstånd, att den fallen i fiendehand måste övertyga vederbörande om att stadens fall borde vara en fråga om dagar, såsom också visade sig vara fallet. I sin helhet finns rapporten publicerad i *Bazeries'* arbete *Les chiffres secrets dévoilés.*

Läsaren torde efter detta vara övertygad om att Leipzigdepescherna i händerna på en person med fallenhet för chifferlösning varit alldeles tillräckliga för att göra hela coden värdelös som bevarare av sekreta ting. Med varje nytt depeschmaterial ökas lättheten och säkerheten i dechiffreringen. Enbart med här redovisade små partier ur den Rappska rapporten är man uppe i nära 100 kända grupper, dvs. hälften av Napoleons "petit chiffre".

Denna benämning antyder, att Napoleon även hade ett annat, större chiffer. Men "le grand chiffre de Napoléon" är en annan historia.



# 7. Mathias Sandorfs kryptogram

I Jules Vernes-boken om Mathias Sandorf berättas om en uppsnappad biljett, innehållande 18 bokstavsgrupper om 6 vardera och uppställda i tre kolumner. Biljetten innehöll en chiffrerad text, och det skildras i äventyrsboken, hur man också lyckats hitta det instrument, med vilket chiffreringen utförts. Det var en kvadratisk pappkartong, uppdelad i 36 rutor. Av dessa var 9 utskurna som öppna fönster. Det var vad man kallar ett raster (internationellt "grille"). Genom att på lämpligt sätt aptera detta raster på den funna chiffertexten, avläsande de bokstäver som kunde ses genom de öppna fönstren, och undan för undan vrida rastret ett kvarts varv, så att andra bokstäver framträdde, blev det möjligt att avläsa meddelandets verkliga innehåll. De utskurna fönstren var nämligen placerade på sådant vis, att öppna och täckta rutor successivt intog varandras plats vid omvridningen, utan någon dubblering. Av en textlängd om 36 bokstäver hade sålunda vid chiffrets utskrift genom fönstren samtliga bokstäver blivit återgivna i en viss omkastad ordning men heller ingen bokstav mer kommit med än den ursprungliga texten innehöll. Upprepningen tre gånger av denna procedur hade frambragt den givna chifferlängden ($36 \cdot 3 = 108$).

I Jules Vernes framställning går det hela mycket lätt. Poängen är där upphittandet av det använda rastret. Men om detta inte skett, hade man då behövt stå rådlös? Det är det vi nu ska se och tar som utgångspunkt bara själva innehållet i biljetten. Den lydde:

| | | |
|---|---|---|
| i h n a l z | z a e m e n | r u i o p n |
| a r n u r o | t r v r e e | m t q s s l |
| o d x h n p | e s t l e v | e e u a r t |
| a e e e i l | e n n i o s | n o u p v g |
| s p e s d r | e r s s u r | o u i t s e |
| e e d g n c | t o e e d t | a r t u e e |

Vad betyder nu dessa bokstäver? Till antalet är de 108. Men vilka är representerade? Kan det vara så att var bokstav är tecken för en viss annan bokstav eller är bokstäverna identiskt desamma som i det dolda originalmeddelandet, fast här omkastade i ordningsföljd? En frekvensstatistik ger omedelbart besked härom. Man finner nedanstående frekvensvärden. Från början fanns anledning tro, att meddelandet avfattats på franska. Statistiken stämmer därmed bra. Den ojämförligt vanligaste bokstaven visar sig vara e. Särskilt stor frekvens visar bland konsonanterna n, r, s, t. De i franska så gott som aldrig förekommande k och w saknas. Inga onaturligheter kan f. ö. iakttas i bokstavsfördelningen. Alltså: bokstäverna har behållit sin ursprungliga innebörd. Vi har framför oss ett omkastningschiffer.

Men efter vilken regel har omkastningen skett? Det kan ju tänkas oerhört många möjligheter. De måste dock först och främst begränsas därav, att chiffret skall vara för mottagaren läsbart på något relativt enkelt sätt. En matematisk regel, som kan hållas i minnet, eller något nyckelord. Eller, som i detta fall, användning av ett raster, som både avsändare och mottagare har i sin ägo.

| | | | |
|---|---|---|---|
| a 𝍸 I | g II | m II | t 𝍸 III |
| b – | h II | n 𝍸 IIII | u 𝍸 II |
| c I | i 𝍸 | o 𝍸 II | v III |
| d IIII | j – | p IIII | w – |
| e 𝍸 𝍸 𝍸 𝍸 II | h – | q I | x I |
| f – | l IIII | r 𝍸 IIII | y – |
| | | s 𝍸 IIII | z II |

Omkastningar plägar ofta åstadkommas genom användning av en geometrisk figur, för det mesta rektanglar. Består ett chiffer av 108 tecken, kan det tänkas, att det skett en rektangulär uppskrivning av dem, vertikalt och horisontellt efter värdena 6×18, 18×6, 3×36, 36×3, 9×12, 12×9. Då sedan varje sådan uppställning kan omkastas på flerfaldigt sätt, förstår man att det är omständligt att pröva sig fram. Men det är vad man har att göra.

Utanför dessa omkastningsmetoder faller sen de som ett raster medger. I detta fall kan rastermetoden från början misstänkas, därför att chifferlängden utgör multipel av en kvadrat (6×6×3). Och prövningen av denna möjlighet går vi nu direkt på.



En säregenhet för rasterinskrivning av en text måste framträda i chiffret. Fönstren i rastrets olika lägen kommer att te sig som spegelbilder, de fyra lägena tagna två och två. Detta medför att en bokstavsserie, som inskrivs i två motsatta rasterlägen, kommer att framstå som skriven baklänges i det ena av dessa lägen. Men nu är det ju i verkligheten inte samma bokstavsserie, som inskrivs i ett senare läge utan en ny. Men det är en sammanhängande, "äkta" serie av bokstäver. Och i en sådan bör man kunna upptäcka i språket vanligen förekommande bigram. Analysen av ett rasterchiffer kan därför, i stället för att uppställa hypoteser om rastrets möjliga konstruktion, gå ut från en uppskrivning av chiffertexten både framlänges och baklänges, under varann, och en granskning av bigrammöjligheter. Inga andra är acceptabla än de som i båda raderna ger språkligt användbara bigram. Då man träffar rätt, får man också kännedom om motsvarande fönsters placering i rastret.

Analysen utförs här först på den sista tredjedelen av chiffret. Denna innehåller nämligen ett q, något som man för fransk text icke försummar begagna. Saken är nämligen den, att bortsett från förkortningar — alltså i en fransk normaltext — ett q antingen är obevekligen följt av ett u eller också utgör sista bokstaven i det unika ordet cinq. Detta faktum kommer till riklig användning i lösning av fransk chiffertext. Det vanligaste q-trigrammet är *que*. Efter q förekommer här 3 u och än fler e. En uppställning efter anvisningen nyss ger dock inget uppmuntrande resultat. I den dubbla utskrivningen presenterar sig chiffrets sista tredjedel sålunda:

r u i o p n m t q s s l e e u a r t n o u p v g o u i t s e a r t u e e

e e u t r a e s t i u o g v p u o n t r a u e e l s s q t m n p o i u r

Om man avläser de kombinationer av *que* som i ordningsföljd kan åstadkommas i övre raden och de trigram som bildas,

om de rätt under befintliga bokstäverna läses i motsatt ordning erhåller man

| | | |
|---|---|---|
| que mpt | que mat | que mst |
| que upt | que uat | que ust, |
| que rpt | que rat | que rst |

Gör man detsamma men börjar i undre raden, då från höger till vänster, får man de mot *q u e* svarande trigrammen i övre raden att bli m p t, e p t, r p t, m a t, u a t, r a t, m s t, u s t, r s t, u i t, r i t.

Somliga av de så erhållna nya trigrammen verkar omöjliga, andra möjliga men intet ser särskilt sannolikt ut. Emellertid kan det naturligtvis hända att de tre bokstäverna *que* icke alla blivit inskrivna vid samma inställning av rastret. Om t. ex. q inskrivits i första läget och de båda andra sen rastret vridits ett kvarts varv, kan man vid jämförelsen mellan de bägge raderna blott upptäcka motsvarigheten till *ue*. Detta är verkligen här fallet, vilket från början försvårar och gör att *que*-försöket utfaller negativt.

Det gäller därför att söka ett annat uppslag. Franskans vanligaste bigram är *es* och ett av dess vanligaste ord *est*. Ur undre raden härovan kan man kombinera fram *est* i ordningsföljd på flera sätt, men om det är en "äkta" kombination skall den ge upphov till ett rimligt trigram även baklänges i övre raden. Och dessutom på exakt motsvarande plats i de bägge andra tredjedelarna av chiffret.

För att förtydliga saken återges alla de tre fördubblade ramsorna med utsatt placering.

```
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36
i h n a l z a r n u r o o d x h n p a e e e i l s p e s d r e e d g n c
c n g d e e r d s e p s l i e e e a p n h x d o o r u n r a z l a n h i

z a e m e n t r v r e e e s t l e v e n n i o s e r s s u r t o e e d t
t d e e o t r u s s r e s o i n n e v e l t s e e e r v r t n e m e a z

r u i o p n m t q s s l e e u a r t n o u p v g o u i t s e a r t u e e
e e u t r a e s t i u o g v p u o n t r a u e e l s s q t m n p o i u r
```



Man erhåller sålunda de mot varann svarande trigrammen

| | |
|---|---|
| e s t | s i g |
| e r r | u s s |
| o u r | d e l |

En naturlig utfyllnad av *our* i första undre raden ges av *pour*. Motsvarigheterna blir då

| | |
|---|---|
| p o u r | d e l a |
| v e r r | u s s e |
| t e s t | s i g n |

Stryk nu samtliga utplockade bokstäver, så ser sista tredjedelen ut sålunda:

```
r u i o p n m ⁄ q ⁄ s l ⁄ e u a r ⁄ ⁄ o u p v ⁄ o u ⁄ t ⁄ e a r t u e
e e u t r a e ⁄ t ⁄ u o ⁄ v p u o ⁄ ⁄ r a u e ⁄ l s ⁄ q ⁄ m n p o i u
```

Av s i g n kan i övre raden bildas s i g n e och s i g n a l. Det förra ger i undre raden v t e s t, det senare o u t e s t, vilket senare föredras, då det som synes kan fyllas ut till t o u t e s t.

Prövas bokstäverna i motsvarande plats i de bägge andra dubbelraderna får man, i den första

s e n v e r r  u s s e l e v

och i den andra

s s e p o u r  d e l a h o n

Ännu är det inte mycket begripligt, men intet har framkommit som är språkligt oformligt. I den andra dubbelraden kan en fortsättning sökas, som bättrar på intrycket. Det är ganska få bokstäver som följer efter sekvensen s e n v e r r och bland dem är e z acceptabla. Då har man

| | |
|---|---|
| t o u t  e s t  p r | e r  s i g n a l q |
| s e n v e r r e z | t o u s  s e  l e v e |
| s s e  p o u r  l i | c e  d e  l a  h o n |

Nu har vi sökt placera 9 bokstäver i var rad. Men fler finner vi ej på denna väg, ty fler står ej att finna i detta rasterläge. Ett raster 6×6 innehåller 36 rutor och bland dem 9 fönster. Det är vid kringvridningen i de fyra lägena som genom dem har inskrivits samtliga bokstäver rastret kan rymma i var utskrift. Det q som följer på s i g n a l har t. ex. sin fortsättning (q)u e i nästa rasterläge.

Men vi kan, efter bokstävernas platser i rummen 9, 12, 16, 19, 24, 27, 29, 32, 36, numera bestämma rastrets utseende. Det måste se ut som nedanstående.

| | | | | | |
|---|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 | 6 |
| 7 | 8 | 9 | 10 | 11 | 12 |
| 13 | 14 | 15 | 16 | 17 | 18 |
| 19 | 20 | 21 | 22 | 23 | 24 |
| 25 | 26 | 27 | 28 | 29 | 30 |
| 31 | 32 | 33 | 34 | 35 | 36 |

Om det vrids i kvarts varv erhålls dessa 4 successiva lägen, och därmed kan övriga bokstäver införas.

I

| | | | | | |
|---|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 | 6 |
| 7 | 8 | 9 | 10 | 11 | 12 |
| 13 | 14 | 15 | 16 | 17 | 18 |
| 19 | 20 | 21 | 22 | 23 | 24 |
| 25 | 26 | 27 | 28 | 29 | 30 |
| 31 | 32 | 33 | 34 | 35 | 36 |

II

| | | | | | |
|---|---|---|---|---|---|
| 6 | 12 | 18 | 24 | 30 | 36 |
| 5 | 11 | 17 | 23 | 29 | 35 |
| 4 | 10 | 16 | 22 | 28 | 34 |
| 3 | 9 | 15 | 21 | 27 | 33 |
| 2 | 8 | 14 | 20 | 26 | 32 |
| 1 | 7 | 13 | 20 | 25 | 31 |



III

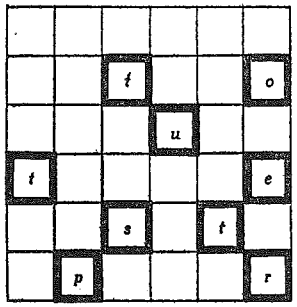
| | | | | | |
|---|---|---|---|---|---|
| 36 | 35 | 34 | 33 | 32 | 31 |
| 30 | 29 | 28 | 27 | 26 | 25 |
| 24 | 23 | 22 | 21 | 20 | 19 |
| 18 | 17 | 16 | 15 | 14 | 13 |
| 12 | 11 | 10 | 9 | 8 | 7 |
| 6 | 5 | 4 | 3 | 2 | 1 |

IV

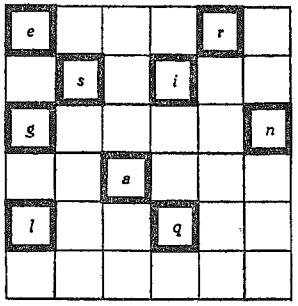
| | | | | | |
|---|---|---|---|---|---|
| 31 | 25 | 19 | 13 | 7 | 1 |
| 32 | 26 | 20 | 14 | 8 | 2 |
| 33 | 27 | 21 | 15 | 9 | 3 |
| 34 | 28 | 22 | 16 | 10 | 4 |
| 35 | 29 | 23 | 17 | 11 | 5 |
| 36 | 30 | 24 | 18 | 12 | 6 |

Resultatet kan avläsas i nedanstående figurer, som för den sista tredjedelen åskådliggör hur inskrivningen skett, och av den följande tablån över hela chiffret.

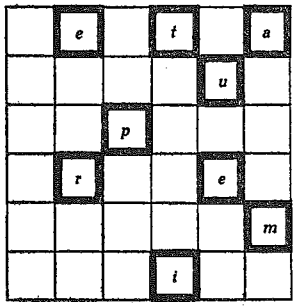
I



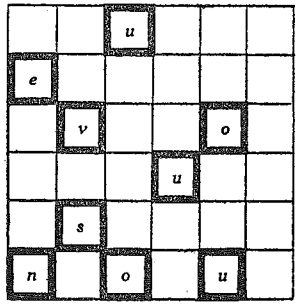

III




II



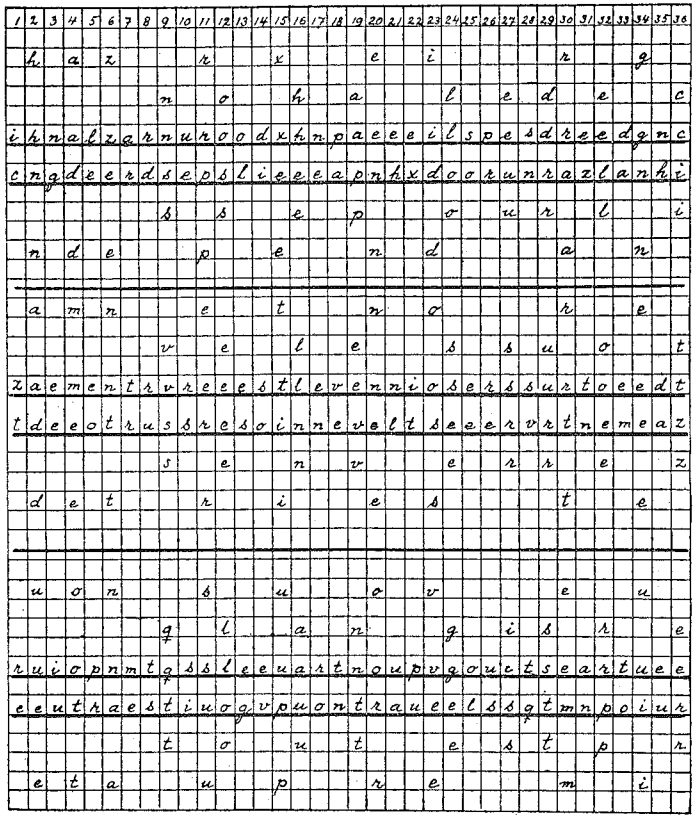

IV



Texten lyder sålunda:

*tout est pret au premier signal que vous nous enverrez de trieste tous se leveront en masse pour l'independance de la hongrie xrzah*

Slutbokstäverna kan vara avsändarens signatur eller också är de fyllnadsgods i rasterutskrivningen.



Att lösningen här gått ut från undre sista raden hänger samman därmed, att chiffret för att försvåra upptäckt tillverkats så, att texten inskrivits baklänges i rastret.



UPPSALA STADSBIBLIOTEK

# 8. Napoleons Hamburginstruktion

Le grand chiffre de Napoléon har existerat i flera varianter. Det har tydligen i flera omgångar snappats upp av fienden och därför måst ersättas. Dess allmänna struktur tycks emellertid ha bibehållits. Det består av ca 1 200 grupper för bokstäver, stavelser och ord. I en skrivelse till sin adjutant överste Bernard 2 mars 1813 säger Napoleon sig frukta, att fienden är i besittning av de chiffer, som användes under föregående kampanj. Han meddelar nu sin adjutant att han önskar nya chiffer och preciserar: Jag vill ha två slags chiffer, ett för högkvarterets korrespondens med de olika kårbefälhavarna och ett eget för min korrespondens med armébefälhavarna under den tid jag är borta.

Det är antagligen det sålunda beordrade nya kejserliga chiffret som är använt i den instruktion om åtgärder gentemot Hamburg, som på Napoleons order avsändes den 7 maj från Waldheim. Kejsaren hade nyss vunnit bataljen vid Lützen. Han beordrar nu i Waldheim Berthier, prince de Neuchâtel et de Wagram, att till marskalk Davout avsända ett chiffrerat meddelande innehållande detaljerade order om hur Hamburg och de patriotiska hamburgarna skall behandlas efter resningen mot de franska inkräktarna.

Chiffret är av stort historiskt intresse ur två synpunkter. Det tycks ovederläggligen visa, att kejsar Napoleon personligen bär hela ansvaret för den hårdhänta behandlingen av Hamburg och befriar därigenom Davout från en fläck på hans krigarära. Ur svensk synpunkt är chiffret särskilt intressant genom den instruktion Napoleon ger om attityden gentemot svenska armén, som under kronprinsen stod i Pommern. Det ger ett ytterligare belägg för att kronprinsens hållning gentemot Frankrike ännu var obestämd och att Napoleon med vetskap därom icke var benägen att bryskera saken. Den tråkiga affären med

Döbeln får härmed också sin belysning.

Någon chifferteknisk analys är här icke avsedd. Genom understrykningar har uppmärksamheten fästs på vissa karaktäristiska upprepningar. Tolkningen har gjorts av *Bazeries* i hans lilla studie *Les chiffres de Napoléon 1er pendant la Campagne de 1813*. Det arbete, som här i andra hand utförts, inskränker sig till att slå ut klartexten, som är meddelad för sig, på chiffergrupperna, vilket visserligen icke är gjort i en handvändning och i några få fall icke kan ske med full säkerhet. Jag anmärker, mera för kuriositetens skull, att den mest använda chiffergruppen 519 representerar z, som icke alls är högfrekvent men som här har blott denna enda representation. Då det här gäller en rad personliga order, blir verbformer av typen vous ferez mycket vanliga, därav gruppens ovanliga frekvens. Av 1 200 grupper är här använda 338. Chiffret är efter forcering av detta meddelande tillspillogivet. Det återges nu som historiskt dokument.

92 74 71 265 le 7 mai 1813
va - l - de - im
A Monsieur 389 491 464
le maréchal prince d' Eckmühl
Je vous ai annoncé 1168 par ma lettre du 5 la victoire
prince
complète que l'Empereur a remporté le 2 mai dans les plaines de Lutzen sur les armées Russes et Prussiennes réunies; nous continuons à poursuivre l'ennemi et probablement 292 130
nous ser -
617 49 55 641 47 279 49 71 17 1105 92 28
on - s de main a dre - s - de . le duc d'El chingen va pas -
130 14 117 385 523 197 801 915 732 137 523 14 781
se - r l el - be et mar - che - r sur be - r - li -
362 761 989 144 343 de vous faire 559 qu'il
n . l'Empereur me charge connaître
est 900 136 605 586 588 782 519 47 527
indispen sable que vous vous port - ie - z a Hambourg
que vous vous 825 782 519 71 322 791 et que vous
empar - ie - z de cette ville



334 887 841 402 519 sur le champ 693 206 1142 757
di - ri - gi - e - z le général van - da -
597 144 243 389 717 19 174 597 1010 185 704 657 1157
m - me dans le mec - k - le - m - bourg . vo - i - ci
529 1192 136 605 393 429 297 169 586 870 835 519
la conduite que vous avez a tenir . vous fe - re - z
792 18 174 1041 597 1103 929 912 984 287 527
arrêter sur le cha - m - p tous les sujets de Hambourg
685 288 872 13 680 537 389 451 349 71 29 942 237
qui ont pris du service sous le ti - tre de sen - at - eurs
287 527 185 497 912 870 593 519 613 13 769 429
de Hambourg . vous les fe - re - z tra - du - ire a
133 1177 931 503 781 235 769 197 586 870 835 519
une commis - sion mi - li - ta - ire et vous fe - re - z
172 728 74 66 732 912 907 528 401 1189 185 497 112
fu - si - l - le - r les cinq plus coup - ables . vous en -
1197 135 519 261 690 537 22 566 855 159 474 842
ver - re - z les autres sous bonne es - cor te en France
262 378 135 297 294 426 998 789 23 875 169 605 870
pour être re - ten - us dans une prison d état . vous fe -
835 519 327 389 637 903 953 135 18 419 158 821
re - z mettre le se - que - st - re sur leurs biens et
497 912 524 593 519 735 944 49 903 216 185 389 178
vous les déclare - re - z con - fi - s - qué s . le do -
641 402 73 362 969 722 814 309 49 351 1095 *)
main- e pre - n - dra possession des mai - s - ons (fo)n -
23 216 71 84 135 et cetera 810 1170 870 835 519 814 522
d - s de ter - re . vous fe - re - z des - ar -
785 1136 791 185 586 870 835 519 172 728 74 881 107
mer la ville . vous fe - re - z fu - si - l - le - r
929 912 624 71 529 389 841 288 765 853 942 657 136
tous les officiers de la le - gi - on an - se - at - i - que
413 809 474 1197 135 519 929 152 685 194 617 872 71
et vous en - ver - re - z tous ceux qui aur - ont pris de
117 962 426 787 389 841 473 474 842 262 1034 378
l emploi dans cette lé - gi - on en France pour y être

* Sannolikt fattas här en grupp med betydelsen fo.

503 49 384 619 307 566 169 810 aussitôt que 704 926
mi - s aux gal - èr - es . . vos troupes
637 617 16 229 47 886 873 843 1197 188 605 235 915
ser - ont arrivé - s a s - c - h - ver - in vous tâ - che-
835 519 1147 222 334 135 71 497 62 657 499 14 13 1168
re - z sans rien di - re de vous sa - i - si - r du prince
413 287 62 564 503 74 389 413 809 622 205 1197 135 519
et de sa fa - mi - l - le et vous l en - ver - re - z
205 842 243 133 789 23 875 891 13 873 49 596 613
en France dans une prison d état ces du - c - s ayant tra -
230 529 999 870 287 9 601 306 1118 474 973 318 519
hi la con - fe - de - ra - tion . vous en agir - e - z
71 1148 47 74 318 476 71 419 1093 1146 358 809 483
de même a l é - gard de leurs ministres . . vous ne
645 996 349 519 616 1174 44 912 406
comme - t - tre - z aucun acte d'hos tilité contre les suédois
49 286 593 953 474 996 243 1136 239 144 9 179 318
s ils re - st - en - t dans la po - me - ra - ni - e
821 524 362 996 630 287 144 968 307 702 169
et déclare - n - t vouloir de - me - ur - er tranquilles .
761 605 870 135 519 998 781 49 159 71 135 990 385 912
. vous fe - re - z une li - s - te de re - b - el - les
814 1141 481 188 710 663 13 49 71 995 857 256 59
des 15 cent in - di - vi - du s de la 30 2 division
503 781 235 769 912 528 887 915 413 685 599 93 389
mi - li - ta - ire les plus ri - ches et qui se sont le
528 338 1192 996 185 809 912 870 135 519 792 307
plus mal condui - ts . vous les fe - re - z arrêt - er
821 497 870 135 519 327 174 853 136 953 135 18 419
et vous fe - re - z mettre le se - que - st - re sur leurs
158 928 389 178 641 318 807 362 969 722 169
biens dont le do - main - e pre - n - dra possession .
787 1127 249 137 455 1096 426 74 511 744 1010
cette mesure est sur - tout nécessaire dans l Old - en - bourg
17 358 809 870 135 519 327 133 735 982 456 601 71
. . vous fe - re - z mettre une con - tri - bu - tion de
103 368 18 261 791 71 527 413 287 190 523
50 millions sur les villes de Hambourg et de Lu - be -



873 19 185 809 73 1095 279 519 814 1127 262 1136
c - k . vous pre - n dre - z des mesures pour la
593 344 601 71 322 508 197 460 301 980 421
re - parti - tion de cette somme et pour qu elle soit
849 701 67 185 586 870 135 519 410 14 929
promptement pay - e . vous fe - re - z pa - r tout
671 440 107*) 389 701 49 197 792 307 912 802 362
des a - r - le pay - s et arrêt - er les ge - n -
757 107 144 49 1194 127 179 307 476 531 821 624
da - r - me - s ca - non - ni - ers garde - côtes et officiers
197 1156 74 757 583 21 962 49 1080 774 194 680
et so - l - da - ts ou employé - s qui étant au service
384 9 325 613 230 1020 419 815 872 607 216 637 617
au - ra - ient tra - hi s leurs pro - pri - été - s ser - ont
999 944 49 136 229 169 1095 21 153 566 28 18 929
con - fi - s - qué - s . n ou - bli - ez pas sur - tout
455 261 309 288 71 527 685 638 93 338 254
toutes les mais - ons de Hambourg qui se sont mal com-
588 318 413 928 382 442 93 591 306 286
port - es et dont les intentions sont mauvaises . il
730 287 560 14 912 815 872 607 49 1147 445 473 889
faut de - place - r les pro - pri - été - s sans quoi on ne
637 9 657 996 509 309 18 71 218 701 49 17 810 809
se - ra - i - t ja - mais sûr de ce pay - s . . vous
870 135 519 440 14*) 529 560 71 527 185 605
fe - re - z a - r la place de Hambourg . vous
870 593 519 124 835 671 239 362 996 389 663 194 588
fe - re - z fai - re des po - n - ts - le - vis aux porte-
229 185 1170 870 135 519 327 814 1194 33 18 912
s . vous fe - re - z mettre des ca - nons sur les
135 597 410 361 49 593 389 1197 261 410 9 12 583 197
re - m - par - t - s re - le - ver les pa - ra - pe - ts et
809 986 135 519 133 1157 235 116 389 13 531 71
vous établi - re - z une ci - ta - del - le du côté de

* Här saknas 144 14
me - r

682 522 1010 287 450 301 1049 21 907 94 139
Ha - ar - bourg de manière que 4 ou 5 mille hommes
1034 421 47 74 264 887 71 529 239 164 1136 601 413
y soient à l ab - ri de la po - pu - la - tion et
71 929 188 873 968 931 169 358 809 870 135 519 402
de toute in - c - ur - sion . . vous fe - re - z é -
619 562 949 996 440 14*) 190 523 873 19 262 136 322
gal - e - men - t a - r Lu - be - c - k pour que cette
791 421 1109 47 74 264 887 23 133 401 71 641 17 358
ville soit aussi à l ab - ri d un coup de main . .
809 135 210 818 179 130 135 519 873 664 1005 682
vous re - or - ga - ni - se - re - z c - u - x - ha-
348 17 761 929 46 1127 1168 93 71 887 320 968
ven . . toutes ces mesures prince sont de ri - gue - ur
989 483 497 224 1136 781 523 159 23 205 405
l'Empereur ne vous laisse la li - ber - té d en mo-
334 944 307 616 185 586 287 751 519 524 14 136
di - fi - er aucune . vous de - ve - z déclare - r que
873 249 212 427 654 287 62 274 197 973 205 731
c est par ordre exprès de sa Majesté et agir en temps
534 160 813 1136 1182 958 218 1096 17 929 912
et lieux avec la pru - den - ce nécessaire . tous les
139 999 311 49 1180 378 149 221 886 71 135 704 74
hommes con - nu - s pour être che - f s de re - vo - l -
159 423 378 172 499 74 912 21 655 229 194 619
te doivent être fu - si - l - lés ou envoy - és aux gal -
307 229 169 810 580 194 144 873 19 389 597 1010 74
èr - es . . quant aux Me - c - k - le - m - bourg l
612 259 249 136 46 1168 93 30 71 1136
instruction général est que ces princes sont hors de la
985 287 74 61 15 541 362 205 730 222 224
protection de l empire mais il n en faut rien laisser
122 12 14 218 543 413 815 62 274 194 9
a - pe - r - ce - voir et probablement Sa Majesté au - ra
389 731 287 721 14 814 427 169 20 912 1168
le temps de donne - r des ordres . comme les princes



71 144 873 19 389 597 1010 170 72 996 658 238
de Me- c - k - le - m - bourg peu - ven - t ignorer nos
140 239 728 601 809 239 664 751 519 815 327 23
dis - po - si - tions vous po - u - ve - z pro - mettre d
264 210 23 929 218 365 704 664 969 205 1034 327 41
ab - or - d tout ce qu'on vo - u - dra en y mett - ant
262 835 953 887 873 601 797 74 122 815 386 601 71
pour re - st - ri - c - tion sauf l a - pro - ba - tion de
989 17 74 122 815 386 601 774 212 348 664 318
l'Empereur . l a - pro - ba - tion étant par - ven - u - e
929 599 1154 9 657 996 205 135 780 17 810 527
tout se trouve - ra - i - t en rè - gle . . Hambourg
774 205 875 71 404 605 1034 295 135 519 133
étant en état de siège vous y nomme - re - z un
150 865 870 14 144 262 205 124 1136 239 781 218
command - ant fe - r - me pour en faire la po - li - ce
17 809 205 1197 135 519 389 259 1142 757 597 144
. vous en - ver - re - z le général van - da - m - me
474 65 813 186 1055 361 782 14 259 185 286 730
en avant avec votre quar - t - ie - r général . il faut
363 883 1168 71 144 428 802 14 218 259 912 139
avoir soin prince de me - na - ge - r ce général les hommes
287 289 856 348 733 9 593 169
de guerre de - ven - ant ra - res .

Le Prince de Neuchâtel
Major Général
Signé Alexandre

Ordern om arkebusering är som synes klar. Ingen tvekan kan råda om tolkningen. Det inskärps att Davout icke har rätt att göra någon modifikation och han är bemyndigad förklara, att han handlar på kejsarens uttryckliga order. Vad angår förhållandet till svenska kronprinsen är det visserligen så, att i instruktionen "vous ne commettrez aucun acte d'hostilité contre les suédois s'ils restent dans la Pomeranie et déclarent vouloir demeurer tranquilles" gruppen 1174 för "acte d'hostilité" blott förekommer en gång, varför tolkningen icke har stöd av någon

upprepning. Men det råder icke något tvivel om att meningen måste vara riktigt återgiven.

Dessa instruktioner expedierades icke blott från Waldheim 7 maj utan även följande dag från Nossen. Endast den senare depeschen tycks ha kommit fram. Och denna kunde Davout icke dechiffrera i brist på chiffernyckel. Han meddelar i rapport till högkvarteret 11 maj från Bremen, att han just mottagit duplicatan från Nossen av ett chiffrerat brev, daterat 92, 74, 71, 265 den 7 maj, som börjar Je vous ai annoncé 1168 etc. Så meddelar han, att han blott är i besittning av ett chiffer som icke är användbart för att förstå det erhållna meddelandet, varför han skickar en adjutant att hämta det använda chiffret. Som framgår av ett senare samma dag avsänt nytt meddelande till högkvarteret anlände en kurir strax efter och medförde det. Davout slutar med att säga, att nu är alltsamman dechiffrerat, och han kommer att efter bokstaven utföra kejsarens order: "j'exécuterai à la lettre les intentions de Sa Majesté".

Samtidigt som denna episod visar, att chifferväsendet inte befann sig i bästa ordning inom la Grande armée utgör det ett ytterligare belägg på att ansvaret för grymheterna i Hamburg helt kommer på Napoleons konto.



# 9. Ortegas bekännelse

Jules Vernes smak för chiffer framträder i åtskilliga av hans äventyrsböcker. Sett med den nutida expertisens ögon förefaller hans produkter kanske en smula puerila, men för den rene lekmannen fyller de fullt ut sin uppgift att förhöja det hemlighetsfulla i äventyrsskildringen. Ett exempel på ett rasterchiffer har tidigare givits (Mathias Sandorfs kryptogram). En helt annan chiffertyp har av Jules Verne använts i historien om hur domaren Jarriquez i sista minuten räddade en oskyldig från att dömas för mord genom att dechiffrera den i verkligheten skyldiges i hemlig skrift nedlagda bekännelse.

Domaren Jarriquez hade i ett etui funnit ett gulnat papper innehållande en meningslös bokstavsramsa, som skall återges vid analysen av chiffret. Han insåg strax att det rörde sig om ett kryptogram, som måhända kunde lösa det problem han brottades med och satte i gång med all sin energi. Men efter timmar av arbete hade han inte kommit längre än till en förmodan att dokumentet var avfattat på portugisiska. Hans försök att med ledning av frekvensen i detta språk sätta in de rätta bokstäverna ledde dock, som det står i boken, till en ren kakofoni.

Efter ytterligare timmar av spekulation hade han emellertid fått korn på vad det kunde vara för system som använts. Att h var den mest använda bokstaven hade han redan vid den första undersökningen konstaterat. Nu hade han fäst sig vid att på två ställen förekom 3 h i rad. Han drog därav den slutsatsen att h icke kunde konstant betyda en viss bokstav utan måste ha flera betydelser. Detta därför, som Jules Verne berättar saken, att i inget språk förekommer det ord med tredubbling av samma bokstav.

Inom parentes anmärkt är detta att ta till ett alldeles falskt påstående, såsom just den nyss använda frasen visar: *"att ta"*. Om orden bara skrivs ihop kan man lätt få sådana fall. Och i det

papper domaren Jarriquez undersökte var bokstäverna sammanskrivna från början till slut. På en oriktig premiss byggde denne en riktig slutsats.

Han resonerade sig till att ett chiffer med denna egendomlighet (3 h i rad) borde ha kommit till genom att de ursprungliga bokstäverna medelst en viss numrering förskjutits, t. ex. så att första bokstaven förskjutits tre steg, andra bokstaven fem steg och tredje bokstaven två steg nedåt i alfabetet. Men vilken sifferserie och hur lång? Det kunde han inte komma på och förtvivlade om lösningen, då en händelse kom att fixera hans uppmärksamhet på namnet Ortega. Han fick plötsligt den idén, att det namnet kunde finnas i chiffret. Hans blickar fastnade på de sex sista bokstäverna *suvjhd*. Då han jämförde dem med *ortega* fann han, att varje bokstav i *suvjhd* i förhållande till bokstäverna i *ortega* följde efteråt i alfabetet, visserligen på olika avstånd, sålunda

| o | r | t | e | g | a |
|---|---|---|---|---|---|
| 4 | 3 | 2 | 5 | 1 | 3 |
| s | u | v | j | h | d |

Och då han prövade denna förskjutningsserie på början av chiffret fick han genast denna avslöjande ingress: Le véritable auteur du — — —. Hemligheten var röjd.

Ja, tänk så tursamt. Att komma på ordet Ortega och så finna det just i slutet av chiffret. Så mycket tur får en ordinär chifferlösare inte räkna på. Och nu skall vi se, hur man kan angripa Jules Vernes Ortegachiffer utan att vara så speciellt gynnad av omständigheterna.

Det dokument som föll i domaren Jarriquez hand hade nedanstående innehåll, vari för utrymmesbesparing några spärrningar här gjorts:

p h y j s l y d d q f d z x g a s g z z q q e h x g
k f n d r x u j u g i o c y t d x v k s b x h h u
y p o h d v y r *y m* h u h p u y d k j o x p h e *t o z* s
l e t n p m v f f o v p d p a j x h y y n o j y g g a y



m e q y n f u q l n m u l y f g s u z m q i z t l b q g y
u g s q e u b v n r c r e d g r u z b l r m x y u h q h
p z d r r g a r o k e p q x u f i v v *r p l* p h o n t h v
d d q f h q s n t z *h h h* v f e p m q *k y u u* e x k t o
g z g *k y u u* m f v i j d q d p z j q s y k *r p l* x h x q
r *y m* v k l o *h h h o t o z* v d k s p p s u v j h d

En statistik över bokstävernas förekomst ger följande bild av frekvensen:

| | | | |
|---|---|---|---|
| h 23 | g 12 | s 10 | n 8 |
| u 19 | r 12 | e 9 | t 8 |
| y 19 | v 12 | k 9 | b 4 |
| d 16 | x 12 | l 9 | i 4 |
| p 16 | z 12 | j 8 | a 3 |
| q 16 | f 10 | m 8 | c 2 |
| o 13 | | | |

Som synes är det internationella alfabetets alla bokstäver utnyttjade utom w, som är överflödigt. Redan i Jarriquez första reflektioner förekommer f. ö. den iakttagelsen. Han finner det med rätta mycket otroligt, att i en text av 274 bokstäver varje alfabetets bokstav kommit till användning. Detta talar i och för sig emot att det här skulle vara fråga om ett enkelt utbytesalfabet. Att det icke är en transposition man har framför sig visar omedelbart frekvensen för sällsynta bokstäver.

Frekvensfördelningen utesluter definitivt tanken på ett enda alfabet. Fördelningen är alldeles för jämn, för små tal i toppen och för höga i botten. Av en dylik statistik blir slutsatsen att flera alfabet kommit till användning. Men hur många?

För Jules Verne var det synbarligen obekant hur man kan bestämma detta. Numer vet man mycket väl vilken angreppspunkten är.

Användningen av flera alfabet har satts i system särskilt genom bruket av den s. k. Vigenèrerutan, uppkallad efter en fransk diplomat från 1500-talet, Blaise de Vigenère, som själv kallade sitt system det odechiffrerbara chiffret. Det troddes också allmänt till mot slutet av 1800-talet, att med omsorg gjorda chiffer

av denna art verkligen kunde motstå alla forceringsförsök. Tiden för sådana illusioner är emellertid förbi.

Vigenèrerutan innehåller 25 à 26 alfabet (utan eller med w) i en kvadratisk uppställning, som i tur och ordning börjar med a, b, c etc.

a b c d e f .....
b c d e f g .....
c d e f g h .....
d e f g h i .....
.....

Man väljer alfabeten efter ett överenskommet nyckelord och chiffrerar klartextens bokstäver en efter en med så många alfabet som nyckelordet innehåller. En variant härav, kallad Gronsfelds system, ersätter nyckelordet med en sifferserie, vilket medför att blott de tio första raderna i Vigenèrerutan kommer till användning. Efter denna metod kan man med träning både chiffrera och dechiffrera i huvudet utan att ha den kvadratiska rutan tillgänglig.

De olika varianterna av Vigenèremetoden medför en stark utjämning av frekvensen. De angreppsmöjligheter ett enkelt substitutionschiffer bjuder är bortelimínerade. Men har chiffret en viss längd i förhållande till nyckelordet eller sifferserien, uppträder i kryptotexten i alla fall upprepningar. Dessa är systemets sårbara punkt.

Det är detta vi nu skall se med Jules Verne som exempel.

I den förut återgivna chiffertexten har de repetitioner understrukits, som består av tre till fyra bokstäver. Om man räknar efter på vilket avstånd dessa upprepningar förekommer får man fram följande:

| | |
|---|---|
| k y u u | 12 = 2×6 |
| r y m | 192 = 32×6 |
| t o z | 186 = 31×6 |
| r p l | 60 = 10×6 |
| h h h | 54 = 9×6 |



Avståndssiffrorna är uppdelade i faktorer i syfte att konstatera om de innehåller någon gemensam faktor. Finns en sådan, avslöjar den antalet använda alfabet, i detta fall sex. Övriga tal härovan låter uppdela sig även i andra faktorer, men 186 innehåller primtalet 31, vilket begränsar valet till 6, 2 eller 3. Och då är det säkrast att undersöka antagandet 6 alfabet.

Känner man antalet alfabet, ställer man upp hela chiffertexten i lika många kolumner, här alltså 6. De bokstäver som då står i samma kolumn är samtliga chiffrerade med ett och samma alfabet. Man får på detta vis texten uppdelad i 6 olika substitutionschiffer, som man skulle kunna behandla precis som sådana. Men uppgiften är i själva verket här förenklad. Då alla alfabeten är ordnade, bestäms samtliga bokstävers betydelse i ett sådant alfabet så fort man kan bestämma en enda bokstavs identitet.

Chiffret får i den nya uppställningen det utseende här nedan visas. Även förekommande upprepningar av två bokstäver är därvid kursiverade.

| | | |
|---|---|---|
| *p h* y j s l | h y *y n* o j | *p h* o n t h |
| y d d q f d | y g g a y m | v d d q f h |
| z x g a s g | e q *y n* f u | q s n t z *h* |
| z z q q e h | q l n m u l | *h h* v f e p |
| x *g k* f n d | y f g s u z | *m q k y u u* |
| r x u j u g | *m q* i z t l | e x k t o g |
| i o c y t d | b q g *y u* g | z g *k y u u* |
| x *v k* s b x | s q e u b v | m f v i j d |
| h h u y p o | n r c r e d | q d p z j q |
| h d v y *r y* | g r u z b l | s y k *r p l* |
| *m* h u h p u | r m x *y u* h | x h x q *r y* |
| y d k j o x | q h p z d r | *m v k* l o *h* |
| *p h* e *t o z* | r g a r o k | *h h* o *t o z* |
| s l *e t* n p | e p q x u f | v d k s p p |
| m v f f o v | i v v *r p l* | s u v j h d |
| p d p a j x | | |

För att granska de olika alfabeten får man nu göra statistik för var kolumn. Resultatet sammanfattas sålunda:

| | I | II | III | IV | V | VI | |
|---|---|---|---|---|---|---|---|
| a | — | — | — | 3 | — | — | 3 |
| b | 1 | — | — | — | 3 | — | 4 |
| c | — | — | 2 | — | — | — | 2 |
| d | — | 7 | 2 | — | 1 | 6 | 16 |
| e | 3 | — | 3 | — | 3 | — | 9 |
| f | — | 2 | 1 | 3 | 3 | 1 | 10 |
| g | — | 4 | 4 | — | — | 4 | 12 |
| h | 5 | 9 | — | 1 | 1 | 7 | 23 |
| i | 2 | — | 1 | 1 | — | — | 4 |
| j | — | — | — | 4 | 3 | 1 | 8 |
| k | — | — | 9 | — | — | — | 9 |
| l | — | 2 | — | 1 | — | 6 | 9 |
| m | 6 | 1 | — | 1 | — | 1 | 9 |
| n | 1 | — | 2 | 3 | 2 | — | 8 |
| o | — | 1 | 3 | — | 8 | 1 | 13 |
| p | 4 | 1 | 3 | — | 5 | 3 | 16 |
| q | 4 | 5 | 2 | 4 | — | 1 | 16 |
| r | 3 | 2 | — | 4 | 2 | 1 | 12 |
| s | 4 | 1 | — | 3 | 2 | — | 10 |
| t | — | — | — | 5 | 3 | — | 8 |
| u | — | 1 | 5 | 1 | 8 | 4 | 19 |
| v | 2 | 4 | 4 | — | — | 2 | 12 |
| w | — | — | — | — | — | — | — |
| x | 3 | 3 | 2 | 1 | — | 3 | 12 |
| y | 4 | 2 | 3 | 7 | 1 | 2 | 19 |
| z | 3 | 1 | — | 4 | 1 | 3 | 12 |
| | 15 | 16 | 15 | 16 | 15 | 16 | 276 |

Det visar sig nu, att medan chiffret i sin helhet innehåller samtliga bokstäver är i de enskilda kolumnerna 15—16 bokstäver företrädda, vilket kan vara rimligt nog i textbitar av 276:6=43 bokstävers längd. I brist på annat antagande kan förutsättas, att Jules Verne skrivit franska även i chiffret. Följaktligen söker man i varje kolumn att identifiera *e*, språkets ojämförligt mest frekventa bokstav.

Med det efter uppdelningen så starkt reducerade bokstavs-



antalet vågar man nu icke vänta sig att i alla alfabet finna *e* som den mest högfrekventa bokstaven. Men om varje alfabet är ordnat finns goda kontrollmedel. Vokalerna a, e, i skall återfinnas på sina bestämda mellanrum. En högfrekvent grupp bildar r, s, t i rad. Före a bör finnas en zon med tomrum eller blott någon enstaka förekomst på platserna för x, y, z. Den i franskan icke begagnade bokstaven k skall markeras av ett tomrum. Likaså w om det är begagnat, men så är här icke förhållandet.

Utpräglade "toppar" utvisar statistiken för alfabet II, III, IV, V och VI medan I är jämnare fördelat. Man kan då starta med hypoteserna: i alf. II: h=*e*, i alf. III: k=*e*, i alf. IV: y=*e*, i alf V: o el. u=*e*, i alf. VI: h=*e*.

För alfabet II stämmer det bra. Inpassas alfabetet så, att h blir *e*, får man högfrekventa d=*a* och q=*m* samtidigt som k infaller på ett tomrum och platserna före d (=*a*) också är tomma. Men i alfabet III går det inte ihop, k=*e* strandar på att *k* (i klartextalfabetet) skulle få två representanter. Av samma grund måste i alf. V både u=*e* och o=*e* förkastas. Hypotesen för alf. IV uppvisar tomrum för *k*, men där blir stötestenen att rummen för det presumerade *a* skulle komma att intagas av *4x, 4y 4z*. För alf. VI visar sig det gjorda antagandet acceptabelt, vilket innebär att första och sjätte kolumnerna är chiffrerade med samma alfabet. För alf. I kan slutligen genast konstateras, att av de bägge mest frekventa m och h ingendera kan vara *e*. På basis av detta resonemang skulle vi alltså blott kunna sätta in tvenne klartextalfabet.

Men vi kommer ett stycke till genom iakttagelsen, att chifferbokstäverna ph är tre gånger upprepade i kol. I och II, och dessa bokstäver inleder hela texten. Är nu h=*e* i kol. II, så är det berättigat att gissa på *le* i textens början, en synnerligen vanlig inledning. Om det klartextalfabet som motsvarar p=*l* insätts i kolumn I kommer dess *e* visserligen att få en onormalt låg representation, men ingenting framträder som gör hypotesen direkt omöjlig. Vi prövar därför användningen av de tre alfabeten för kol. I, kol. II och kol. VI.

| | | |
|---|---|---|
| p h y j s l | x g k f n d | h h u y p o |
| *l e i* | *s d a* | *d e l* |
| y d d q f d | r x u j u g | h d v y r y |
| *t a a* | *n t d* | *d a u* |
| z x g a s g | i o c y t d | m h u h p u |
| *u t d* | *e l a* | *i e r* |
| z z q q e h | x v k s b x | y d k j o x |
| *u v e* | *s s t* | *t a t* |
| | | - - - - - - |

Ingenting direkt stötande framträder härvid. Det vore nu en bra fortsättning, om man någonstans kunde identifiera ett *que*. Det lyckas ej, men däremot hittar man i slutet av en chifferrad och början av nästa följande:

h d v y r y
*u*
m h u h p u

Något som kunde bli ett *qui*. Det skulle förutsätta f = *e* i kol. V. Hur det artar sig framgår här nedan:

| | | |
|---|---|---|
| p h y j s l | x g k f n d | h h u y p o |
| *l e r i* | *s d m a* | *d e o l* |
| y d d q f d | r x u j u g | h d v y r y |
| *t a e a* | *n t t d* | *d a q u* |
| z x g a s g | i o c y t d | m h u h p u |
| *u t r d* | *e l s a* | *i e o n* |
| z z q q e h | x v k s b x | - - - - - - |
| *u v d e* | *s s a t* | |

Återstoden kan nu knäckas t. ex. på de chifferrader som innehåller klartextbokstäverna

. . . . . d
e l . . s a
s s . . a t



*de l . . sass . . at,* vilket upplagt ger de l'assassinat. I de bägge kolumner, vari alfabeten icke ännu identifierats, skulle vi i så fall få i kol. III g = *e* och i kol. IV j = *e*.

Insätts dessa alfabet i chiffrets början erhålls:

| | | |
|---|---|---|
| p h y j s l | z x g a s g | x g k f n d |
| *l e v e r i* | *u t e u r d* | *s d i a m a* |
| y d d q f d | z z q q e h | r x u j u g |
| *t a b l e a* | *u v o l d e* | *n t s e t d* |

Lösningen är alltså funnen. Papperet innehöll verkligen Ortegas bekännelse: Le véritable auteur du vol des diamants et de l'assassinat des soldats qui escortaient le convoi commis dans la nuit du vingt-deux janvier milhuitcentvingtsix n'est donc pas Joan da Costa injustement condamné à mort c'est moi le misérable employé de l'administration du district diamantin oui moi seul qui signe de mon vrai nom Ortega.

Alfabetets sex a är i de olika kolumnerna företrädda av

e d c f b d

vilket innebär en numerisk förskjutning neråt i alfabetet enligt sifferserien

4 3 2 5 1 3

En dylik chiffrering kan man ju mycket väl utföra utan hjälpmedel genom att räkna på fingrarna. Sifferserien är lätt att komma ihåg. Dechiffreringen kan också göras utan tillgång till en Vigenèreruta genom att bokstav för bokstav räkna uppåt i alfabetet enligt den överenskomna sifferserien.

# 10. En depesch till furst Metternich

Sedan jag hos docenten Torvald Höjer förfrågat mig, om han under sina Bernadotte-forskningar påträffat några olösta chifferdepescher, erhöll jag från honom i början av 1941 några fotostatkopior av depescher, som han funnit i Bernadotteska familjearkivet, i Haus-, Hof- und Staatsarchiv i Wien samt i Public Record Office i London. Det engelska dokumentet måste jag omedelbart lämna åt sitt öde, det syntes mig med sina över 3 000 grupper icke erbjuda några chanser. Den ur H. M. Konungens arkiv hämtade depeschen, som sysselsatt mig länge och med slutlig framgång, är värd sin alldeles särskilda behandling. Nu tar jag upp Wien-depeschen. Den har sitt intresse som prov på hur dechiffrören sökt förhindra den nedskrivna lösningens användning som chiffernyckel och på hans misslyckande med detta.

Depeschen i fråga är sänd från den österrikiske kommissarien i nordarméns högkvarter, generalen baron Vincent, till furst Metternich och skriven i Kiel i januari 1814. Den ger intryck av att vara till större delen löst och har följande utseende:

Je dois encore ajouter à ce que les copies déjà citées de mes
Lettres vous apprenderont, mon Prince, que soit les reflexions
sur les
33 70 1001 996 34 309 756 2100 2002
595 841 907 1031 21 194 948 1198 1080
reproches qu'il s'attirait en retardant les opérations
1197 752 469 676 488 657 744 1179 58
que les Cours Impériales attendraient de lui
251 529 1044 274 929 1164 1137 437 530
ou qu'il ait attaché quelque prix aux
398 456 585 223 148 812 416 1207 57
representations que je lui ai faites depuis quelques



398 562 650 1164 1310 146 522 1106 676
jours soit qu'il soit moins obsedé par M. d
173 1164 1250 398 130 469 153 392 410
Suchtelen et Thornton le Prince royal est
361 1044 259 130 922 242 416 81 1190
absolument porté à terminer avec le Danemarck
66 14 522 173 788 794 816 153 600
et je crois pouvoir garantir la fin prochaine de
1710 3 1080 1257 1007 841 676 841 1195 78
cette longue affaire à moins d'un evènement
568 513 405 999 999 336 552 1145 21 1002
dont je n'apperçoit pas de vraisemblance
766 787 1217 769 5 1032 44 872 524
634 476 501 907 176 974 857 838 81
138 799 316 1086 239 144 672 1409 36
651 752 757 292 14 146 819 1124 895
139 524 1195 2001 980 174 709 246 44
431 138 846 288 862 923 1060 36 1135
1064 886 341 1074 1510 57 1890 1304 2

n'ayant que la réponse d'un estafette, je ne puis entrer dans des détails plus circonstanciés, mais je vous tiendrai au courant mon Prince de ce que je viens de vous faire presentir, jusqu'à ce que je puisse enfin annoncer à Votre Altesse l'entière conclusion de la paix.

Veuillez — — — — — — —

Mellan den inledande klartexten och den mellan chifferraderna inskrivna lösningen finner man alltså två rader chiffergrupper, och efter den rad, där den lösta texten upphör, följer ett större antal chifferrader utan tillhörande lösningstext, innan den avslutande klartexten tar vid. Nu är frågan: vad kan dessa chifferrader, vilka till synes icke är lösta, innehålla? Är det möjligt att angiva den saken med ledning av den dechiffrerade delen?

Det använda chiffret innehåller minst 2 100 grupper. I dokumentet har 135 grupper använts, varibland 25 är återupprepade, ingen dock mer än 3 ggr, och dessa är f. ö. blott 4. Kan

ett sådant material medge några säkra slutsatser rörande depeschens övriga innehåll?

Ja. Fastän det icke varit möjligt att exakt bestämma varje grupps betydelse, kostade det icke någon större möda att ge ett för forskningen fullt tillräckligt besked rörande innehållet.

Den mellan raderna skrivna lösningen kan tänkas avse antingen chifferraden över eller raden under texten. Vare sig dechiffrören gjort på ena eller andra sättet kan det utan svårighet konstateras, att lösningstexten icke korresponderar mot chiffergrupperna närmast över, resp. under. Klarast framträder detta genom att jämföra några chiffergrupper på rad 10—11 med texten. Där finner man den karakteristiska sammanställningen

841 676 841

åtföljd av 1195, allesamman repeterade grupper, och ett litet stycke efter dubbelgruppen

999 999

Texten ovanför kan uppenbarligen icke vara återgiven med 841 676 841, då någon motsvarande bokstavsgruppering icke finns. Texten under medger i förstone tolkningen

| 841 | 676 | 841 | 1195 |
|---|---|---|---|
| e | ven | e | ment |

I så fall skulle dubbelgruppen 999 motsvara de bägge p:na i apperçoit. Men tolkningen strandar avgjort på det i 3:e raden upprepade 676, då tolkningen *ven* omöjligt kan inpassas i den underskrivna texten.

Ytterligare observationer bestyrker, att det över huvud icke finns något sammanhang mellan texten och de chiffergrupper, som finns över eller under den. Kan det då vara så, att det som skrivits mellan raderna icke alls är någon lösning av detta chiffer? Vid genomläsning av hela depeschen, inledningen, det parti som har skenet av en tolkning och avslutningen, framgår intet, som talar emot att de tre partierna är beståndsdelar av samma depesch. Ja, man finner rent av, att inledning och tolkning kan läsas sammanhängande utan att något meningsstörande fram-



träder. Hur skall man då förstå den första, tomma chifferraden?

*Om* den mellanskrivna texten på ett eller annat vis är en översättning av chiffret, så borde man kunna i texten finna motsvarighet till den ensamstående kombinationen 841 676 841, dvs. bokstäver, stavelser eller ord, som upprepas med ett mellanrum, som upptages av blott en chiffergrupp. Texten innehåller två sådana möjligheter, nämligen *que-l-que* (f. ö. på två ställen) och *soit qu'il soit*. Hela texten utskriven med understrukna, mera karakteristiska upprepningar ser så ut:

Je dois encore ajouter à ce que les copies déjà cités de mes Lettres vous apprenderont, mon Prince, *que soit* les réflexions sur les reproches *qu'il* s'attirait en retardant les opérations *que* les Cours Impériales attendraient *de* **lui** ou *qu'il* dit attaché **quelque** prix aux representations *que* **je lui** ai faites depuis **quelques** jours, *soit qu'il soit* **moins** obsedé par M. de Suchtelen et Thornton, le prince royal est absolument porté à terminer avec le Danemarck, et **je** crois pouvoir garantir la fin prochaine *de* cette longue affaire à **moins** d'un evènement dont **je** n'apperçoit pas de vraisemblance.

Det gäller nu att se efter om texten kan placeras så i förhållande till chiffergrupperna att chiffrets upprepningar motsvaras av textens. Först må fastställas vilken av de båda tolkningarna av 841 676 841 som kan accepteras. Närmaste kontrollmöjlighet är dubbelgruppen 999. Med det första que-l-que skulle den motsvaras av de två s:en i jours soit. Men den mellanliggande texten är alldeles för lång för att vara uttryckt med de 5 chiffergrupper som finns mellan 841 och 999. För det andra que-l-que skulle 999 tolkas som t i et Thornton, även här är mellanliggande textdel osannolikt lång. Endast med soit qu'il soit blir avståndet acceptabelt till samma bägge t:n.

Nu förekommer både 841 och 676 även i början av chiffret,

2:a och 3:e raden. Deras tolkningar skall då också kunna återfinnas. Och det går, qu'il finns på två ställen, vilket även grupp 676 gör, soit finns bara en gång. Men det är i den inledande klartexten. Hur kan det hänga ihop?

Är arbetshypotesen soit qu'il soit riktig, borde det gå att placera namnet *Thornton,* förutsatt 999 = t. I dess närhet förekommer en upprepad grupp 21, som också finns på rad 2. Sannolikast tycks detta vara

| | | | | |
|---|---|---|---|---|
| *999* | 336 | 552 | 1145 | *21* |
| T | ho | r | nt | on |

Hur går det då med det första 21, som finns nära 841? Jo, efter *soit* följer i klartexten *les re flexi on s,* som innehåller stavelsen *on*

| | | | | |
|---|---|---|---|---|
| *841* | *907* | 1031 | *21* | 194 |
| soit | les | reflexi | on | s |

Den upprepade gruppen 907 kan placeras långt ner i texten, fastän med betydelsen *le,* i sammanställningen *le Danemarck* — ingenting oacceptabelt då plural ofta i en sådan chiffertyp får utläsas ur sammanhanget.

Även *moins,* efter *soit qu'il soit,* alltså gruppen 1195, tycks kunna rimligt inpassas vid gruppens upprepning mot slutet av chiffertexten.

Om detta är riktigt, skulle vi besitta de stödjepunkter för tolkningen, som framgår av efterföljande uppställning:

Je dois encore ajouter à ce que les copies déjà citées de mes Lettres vous apprenderont, mon Prince, que soit les reflexions sur les

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 33 | 70 | 1001 | 996 | 34 | 309 | 756 | 2100 | 2002 |
| 595 | **841** | **907** | 1031 | **21** | 194 | 948 | 1198 | **1080** |
| | soit | les | reflexi | on | s | | | |
| 1197 | **752** | **469** | **676** | 488 | 657 | 744 | 1179 | 58 |
| | | | qu'il | | | | | |
| 251 | 529 | **1044** | 274 | 929 | **1164** | 1137 | 437 | 530 |



| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **398** | 456 | 585 | 223 | 148 | 812 | **416** | 1207 | **57** |
| **398** | 562 | 650 | **1164** | 1310 | **146** | 522 | 1106 | **676** |
| | | | | | | | | qu'il |
| **173** | **1164** | 1250 | **398** | **130** | 469 | **153** | 392 | 410 |
| **361** | **1044** | 259 | **130** | 922 | 242 | **416** | **81** | 1190 |
| 66 | **14** | **522** | **173** | 788 | 794 | 816 | **153** | 600 |
| 1710 | 3 | **1080** | 1257 | 1007 | **841** | **676** | **841** | **1195** |
| | | | | | soit | qu'il | soit | moins |
| 568 | 513 | 405 | **999** | **999** | 336 | 552 | 1145 | **21** |
| | | | t | T | ho | r | nt | on |
| 766 | 787 | 1217 | 769 | 5 | 1032 | **44** | 872 | **524** |
| 634 | 476 | 501 | **907** | 176 | 974 | 857 | 838 | **81** |
| | | | le | | | | | |
| **138** | 799 | 316 | 1086 | 239 | 144 | 672 | 1409 | 36 |
| **651** | **752** | 757 | 292 | **14** | **146** | 819 | 1124 | 895 |
| **139** | **524** | **1195** | 2001 | 980 | 174 | 709 | 246 | 44 |
| | | moins | | | | | | |
| **431** | **138** | 846 | 288 | 862 | 923 | 1060 | **36** | 1135 |
| 1064 | 886 | 341 | 1074 | 1510 | **57** | 1890 | 1304 | 2 |

— — —

Men detta leder ju till att de första chifferraderna skulle återfinnas i klartexten, som inleder. Detta är just vad som är fallet.

Ett experiment att placera alla repeterade grupper i förhållande till texten och att mellan dem skriva ut den givna tolkningen utfaller, med några frågetecken, sålunda:

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Je | dois | encore | ajouter | à | ce | que | les | copies | déjà | citées |
| 33 | 70 | 1001 | 996 | 34 | 309 | 756 | 2100 | 2002 | | |
| de | mes | lettres | vous | apprenderont | | | mon | Prince | | |
| 595 | **841** | **907** | 1031 | **21** | 194 | 948 | 1198 | **1080** | | |
| que | soit | les | reflexi | on | s | sur | le | - | s | |
| 1197 | **752** | **469** | **676** | 488 | 657 | 744 | 1179 | 58 | | |
| re | - | pro | - | ches | qu'il | s' | a | t | t | i | r | - | a | - | i |
| 251 | 529 | **1044** | 274 | 929 | **1164** | 1137 | 437 | 530 | | |
| - | t | en | re | - | tar | - | dan | - | t | les | o | per | - | |
| **398** | 456 | 585 | 223 | 148 | 812 | **416** | 1207 | **57** | | |

at - i - o - n - s — que les Cours
Impériale - s
398 562 650 1164 1310 146 522 1106 676
at - tendraien - t d - e lui ou qu'il
173 1164 1250 398 130 469 153 392 410
ai - t — at - ta - ché quel - que prix
361 1044 259 130 922 242 416 81 1190
aux re - presen - ta - tion - s que je(?) —
66 14 522 173 788 794 816 153 600
— — lui ai fait - es depuis quel - q -
1710 3 1080 1257 1007 841 676 841 1195 78
u - e - s jour - s soit qu'il soit moins obsedé
568 513 405 999 999 336 552 1145 21 1002
par M. de e - t T - hor - n - t - on le
Suchtelen
766 787 1217 769 5 1032 44 872 524
prince royal est ab s - o - l - u - ment porté à
634 476 501 907 176 974 857 838 81
ter - miner avec le D a n e m a r c k et je(?)
138 799 316 1086 239 144 672 1409 36
— c r o i s p o u v o i r g a r a n t i r l - a
651 752 757 292 14 146 819 1124 895
fin pro - ch - ain — e de cette longue
139 524 1195 2001 980 174 709 246 44
affaire à moins d' un e - vè - ne - ment
431 138 846 288 862 923 1060 36 1135
dont — je n' a p p e r c o i t p - a - s
1064 886 341 1074 1510 57 1890 1304 2
d - e v - r - ai - s - em - bl - ance

n'ayant que la réponse d'un estafette, je ne puis entrer dans des détails plus circonstanciés, mais je vous tiendrai au courant mon Prince de ce que je viens de vous faire presentir, jusqu'à ce que je puisse enfin annoncer à Votre Altesse l'entière conclusion de la paix.

Veuillez — — — — — — —

Det är icke möjligt att exakt uppdela texten på chiffergrupperna och icke möjligt att bestämt säga med vilket textord de-



peschens chiffrerade del börjar. Men det framgår ovedersägligt av de många överensstämmelserna, att sedan inledningen skrivits i klartext har ett parti av densamma dessutom upprepats i chiffer, samt att den mellanskrivna tolkningen motsvarar chiffret ända till dess slut. Dechiffrören har för att dölja sammanhanget mellan text och chiffer börjat skriva in sin lösning några rader nedanför de chiffergrupper, som verkligen motsvarar texten och har sedan skrivit ut den så tätt att många chifferrader blir tomma mot slutet, fast de alla är tolkade. Så har framkallats det skenet, att depeschen till vissa delar är olöst, vilket icke är fallet. Depeschen innehåller ingenting utöver det tolkade partiet jämte de två klartextstyckena.

Det dubbla knep, som här använts för att dölja rätta förhållandet, räcker icke som skydd mot en analys. I senare tid har man noga aktat sig för att skriva ner lösningen på själva chiffret. Den vanliga instruktionen torde vara, att själva chiffret skall omedelbart förstöras och endast lösningen bevaras. Är man försiktig gör man f. ö. någon lätt omskrivning som icke rubbar innehållet i sak.

# 11. Balzacs olösliga kryptogram

I arbetet *La physiologie du mariage* har *Balzac* meddelat ett kryptogram om ca 3 600 tecken, vars lösning sysselsatt många utan framgång. Det sammansätts av stora och små bokstäver, siffror och alla möjliga typografiska tecken, somliga upp- och nedvända.

Ett parti av detta chiffer återges nu här nedan:

btto; qtdod ;tcas ffias scsâv sdoys cssaa dotot hacai dgbdq ,tdto gottd .ocdt mtsrd êmddP d'odo d'aêo cotaL t'ass asq's ;fltt qt;do qsdod flss; t:t-l ,dtat dotsa tbeqæ d-tod ,tdêohêhg o;odâ snsat -oâef to'uc tPdce ise,s dotno '.aos rs-ɟi ê'.it d;êvc t;.de sdta- tbmæb dLomb Nffio dbq'm to'qo dê.to b-:o: d-doq tdqod dh*ooo* 4oqtd adthd ;ada. terat æPai' dotot oêè'- tt'a- 'têdt oeaob totot aqdff ghdov 'otêo 'doe- '.bdd godho smoh, eidod oaet- :ooPd e,odt obdds deg"o ɟeqff iogié ooftd ot..á otL*od dd*roa -dood id'od ,deod odgfb odc'o ddoo' ddhff iffdd Kodff itdtq dté'o d'*ooo* tgffl hflat tqol- tbddg 'cqdd oboob o:ddt 't-do fgdêo d,odo 'oeom oPdab adomd g'*ot d-qo- 'doei oeot" d.doi 'b'og 'gPcf lhimc tda:o m,oot pdqoo goans ctd'o édo't gdtoo dtoto ttfdf fiodf fi,dd oNɟt; d,v*oo* *opdto* dodám bgo,t gddea ed*ctt* *t*,-oo ɟg,tq c.oar ciodd ,,omq td'po hodtt tæKfl dɟdv dt..g OKdgf fiede utmeb deé-ç ecf;h g.rta uxmev nieto arqfc tuvtx irnmc bç-'h :fi.r atnim duv,t ffidg éoætd odtPa doLgq od-gv ot;ff obádt rsidh ddqco t'tdo dolda daoxé z-ent micso staqr aep;g dhfi; rtaml uxcny tizni mdcc- éfq,a

*Bazeries* har gjort sig mödan att underkasta första tredjedelen av kryptogrammet sin analys. Ur hans detaljstatistik över ca 1 000 tecken kan anföras, att han funnit 55 olika tecken, varibland 2 med en frekvens om drygt 150, och att ej mindre än



6 tecken är tredubblade, vilket i franska icke kan förekomma för annan bokstav än e. Hans analys visar, att det icke kan vara vare sig ett substitutionschiffer eller ett transpositionschiffer och hans slutsats som nog är oemotsäglig blir, att det icke är fråga om något kryptogram överhuvudtaget, utan om ett grovt skämt med läsarens nyfikenhet och godtrogenhet.

"Chiffret" förekommer i den avdelning där Balzac behandlar biktens och äktenskapets inbördes förhållande. Författaren har kanske velat säga att frågan om bikten och älskaren är en odechiffrerbar fråga. Han har, menar Bazeries, helt enkelt lämnat ett par sidor blanka i sitt manuskript och sagt till sin förläggare: detta parti får ni fylla som ni vill, med stora och små bokstäver, siffror, punkter, accenter m. m., ibland placerade upp och ned, så att de bildar ett sammelsurium utan varje mening. Ett motstycke till vad en modern atonalist gjort i ett orkesterverk, där partituret på ett par sidor försetts med kompositörens anvisning: varje instrument spelar här efter godtycke. Sättaren av det Balzacska manuskriptet har måhända helt enkelt tömt ut typerna från sin kast på golvet och plockat upp dem huller om buller.

Ett enkelt sätt att producera ett litterärt chiffer och ett litteraturhistoriskt problem.

# 12. Marskalk Davouts rapport

*Ur Bernadotteska familjearkivet*

Den förut omnämnda depeschen ur H. M. Konungens arkiv, som jag erhållit för forcering av docent Torvald Höjer, är en rapport avsänd av Davout från Ratzeburg den 6 nov. 1813 till kejsaren. Napoleon tycks aldrig ha erhållit den. Att den hamnat i det Bernadotteska arkivet måste innebära, att den snappats upp av den svenska armén. Docenten Höjer har, enligt vad han meddelat mig, gjort en förfrågan hos Archives Nationales i Paris om möjligheten att lösa depeschens chiffrerade huvuddel, men fått det beskedet att detta ansågs omöjligt.

Det är ett ovanligt vackert och tydligt utskrivet dokument, såsom syns på omstående facsimile av dess första sida. I sin helhet har det följande innehåll:

Sire,

J'ai l'honneur d'adresser à V. M. copie d'une lettre chiffrée que je viens de reçevoir du Général Lemaroix. J'ai répondu à ce Général que s'il

1118 790 486 1134 553 443 265 629 260 999 309 863 763 1022 477

dès que j'aurai la certitude qu'il aura

98 356 1035

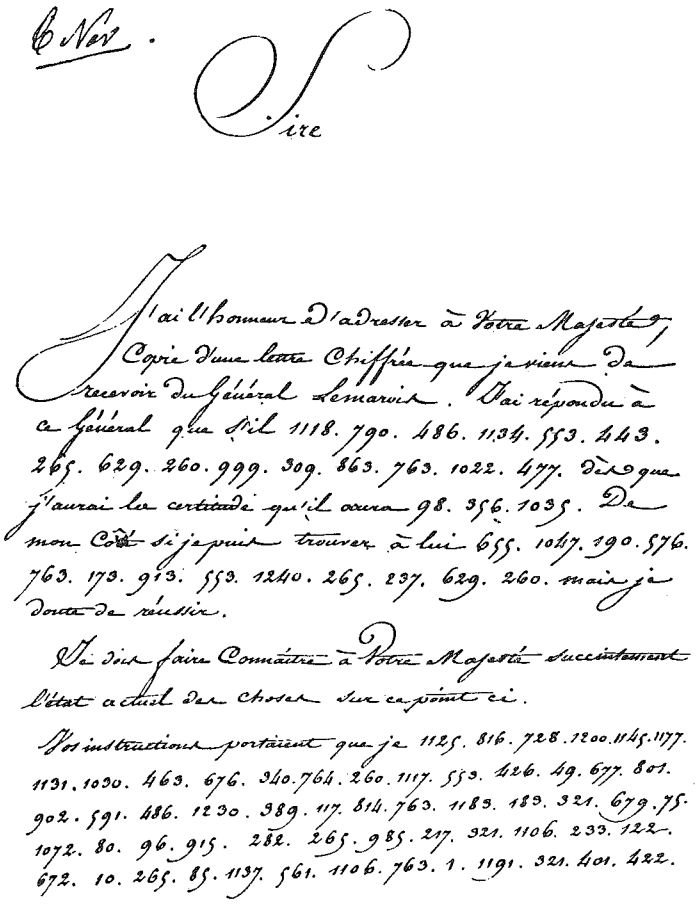
De mon côté si je puis trouver à lui 655 1047 190 576 763 173 913 553 1240 265 237 629 260 mais je doute de réussir.

Je dois faire connaître à V. M. succintement l'état actuel des choses sur ce point ci.

Vos instructions portaient que je 1125 816 728 1200 1145 1177 1131 1030 463 676 340 764 260 1117 553 426 49 677 801 902 591 486 1230 389 117 814 763 1183 183 321 679 75 1072 80 96 915 282 265 985 217 321 1106 233 122 672 10 265 85 1137 561 1106 763 1 1191 321 401 422 30 938 743 184 322 763 460 540 10 322 221 339 42 34 117 654 185 813 645 333 209 963 754 455

J'ai adressé dans le temps differents rapports à V. M. et au Major Général. J'ai la certitude que plusieurs sont parvenus. J'ai été informé qu'on avait laissé encombrer beaucoup d'éstafettes à Cassel, et qu'au moment de l'entrée des Russes on avait brûlé toutes les dépêches.





Depuis les courses des partis ennemis sur la rive gauche 516 1175 136 100 576 1020 910 197 223 18 665 486 117 969 910 197 497 1011 43 1131 902 100 363 677 627 169 912 165

M. le Comte de Chaban m'a fait connaître dernièrement 1132 115 782 577 516 132 669 251 363 950 149 169 1165 1179 139 985 731 58 731 947 1104 676 934 816 969 95 735 524 1167 10 251 363 855 128 938 1168 790 381 1131 627 985 175 11 382 363 460 432 831 210 954 117 705 381 518

265 221 103 486 420 1164 1186 909 124 760 296 54 1113 1118 597 306 412 700 793 418 333 985 469 1117 432 831 au fur et à mesure 291 895 190 54 1020 741 626 539 597 363 902 926 260 772 543 309 479 1055 169 115 118 224 659 327 564 339 671 382 985 460 539 636 115 782 Je doute qu'il adopte cette proposition. Sans cette 760 846 55 464 1117 1016 539 671 62 486 754 41 296 80 549 34 100 210 820 1104 334 985 488 1104 714 679 382 363 460 539 Le Colonel Ponthon qui est un officier d'un grand mérite a fait des travaux immenses à Hambourg; cette place peut maintenant être considerée comme forte.

En avant du faubourg St. Georges, il y a à 800 toises de la place, une première ligne que l'ennemi ne pourrait point emporter de vive force sans faire des ouvrages.

A 400 toises en avant de ce faubourg le colonel Ponthon a établé une ligne bastionnée qui prend de pair l'Alster jusqu'à l'Elbe et qui peut être considerée comme terminée à l'exception 122 1171 228 941 731 93 372 363 854 340 638 597 136 332 681 418 306 412 117 920 626 100 On fait une estacade qui prend de pair la gauche des ouvrages jusqu'au corps de place, dans l'Alster, elle sera achevée ces jours ci.

Tous les bastions et courtines du corps de place ont été relevés; cet ouvrage peut être consideré comme terminé. Sur le front d'Altona entre les rives droites de l'Alster et de l'Elbe, le chemin couvert est entrepris et va être achevé et palissadé. 265 918 309 1144 930 511 1113 812 338 956 238 902 503 1042 33 383 626 918 539 463 676 173 479 985 607 1111 172 575 990 671 214 460 431 ce qui ajoutera beaucoup à la force de la place.

On va aussi entreprendre ces jours ci quelques redoutes sur le front d'Altona à 2 ou 300 toises de la place.

Le pont de communication entre Hambourg et Harbourg est terminé. Cet ouvrage fait le plus grand honneur à M. Jousselin, Ingénieur en Chef des ponts et chaussées, homme du plus grand mérite et pour lequel je réclame les bontés de V. M.

J'ai ordonné la construction d'un camp retranché sur les hauteurs de Harbourg; il est déjà très avancé et le fort de Harbourg est fait 625 1069 773 576 757 985 654 592 191 549 1104 953 516 310

Quant à la position de l'Armée, j'occupe toujours Ratzebourg ma gauche appuyée à Travemünde et ma droite à Lauenbourg. 285 1010 11 150 902 54 136 263 184 45 135 306 677 598 1117 93 1129 1167 993 165 50 452 564 340 828 1010 600 643 1131 1044 801 497 150 259 212 963 1219 115 558 55 799 159 605 728 828 1113 905 333 363 115 748 18 115 280 731 93 1129 1117 605 577 1117 153 620 251 1135 554 963 763 1022 1140 781 18 80 45 56 636 115 45 150 Si ce bruit est vrai, ou m'en 564 655 600 1164 420, e 998 601 597 1190 265 627 363 664 990 11 964 322 479 363 136 670 426 149 162 626 810 154 636 206 740 1126 480 43 605 426 23



654 893 1069 304 237 606 connu 80 45 1125 334 33 172 217 1047 486 1100 601 332 534 518 398 43 4 957 924 115 759 594 1104 676 676 1003 54 224 928 595 10 418 4 l'harmonie est parfaite entre les troupes de V. M. et celles Danoises.

J'ai maintenant une très bonne tête de pont à Hope vis à vis de Zollenspiecker. L'ennemi s'est beaucop renforcé sur ce point par quelques régiments anglais et suédois nouvellement débarqués. On annonce aussi que le corps du Général Tanenzien qui s'était retiré sur Berlin pour se refaire se porte sur ces points ci; il a du se mettre en marche le 31 octobre ou le 1er novembre.

La meilleure harmonie règne entre Vos généraux. Je ne puis, entre autres, trop faire l'éloge du général Loison. Vous pouvez compter, Sire, que nous rivaliserons tous pour vous donner des preuves de notre amour, de notre dévouement et de notre fidélité.

Beaucoup d'emplois sont vacants dans les régiments; des mémoires de proposition ont été envoyés au Major Général et par duplicata au Ministre de la Guerre. Le Major Général ne m'a pas répondu à cause des circonstances et le Min. de la Guerre m'a annoncé en avoir fait le renvoi à Son Altesse. Ces emplois vacants étant nuisible au service de V. M. je la prie de vouloir bien m'autoriser à faire entrer en fonction d'après les mémoires de proposition que me donneront les régiments.

Je prie aussi V. M. de vouloir bien accorder un certain nombre de décorations qui seraient distribuées par des Conseils composés de Généraux à ceux des militaires qui auraient fait quelqu'action brillante.

J'ai l'honneur d'être avec le plus profond respect

De Votre Majesté

Le très humble & obéissant serviteur &

très fidèle sujet

Le Maréchal Duc d'Auerstädt

Prince d'Eckmühl

Ratzebourg le 6 novembre 1813.

Bortsett från det långa avslutande klartextpartiet utgör de i chiffertexten insprängda klartexterna en obetydlig del av innehållet. Ifall ingen ledtråd skulle gå att erhålla från annat håll, förefaller en forcering icke ha stora chanser. Då jag förut sysslat med Napoleon-chiffer var min första tanke att undersöka, om något av dessa chiffer, som jag kände till, här hade kommit till användning. Den allmänna typen är le grand chiffre.

Försök att använda kända grupper ur det chiffer som använts i Napoleons Hamburginstruktion ger rent negativa resultat. Detta under våren använda chiffer hade med säkerhet

långt före november fått utbytas mot ett nytt såsom icke längre säkert. Enligt uppgift av Bazeries användes ett annat chiffer under tiden aug.—nov., även detta efter 1 dec. utbytt mot ett annat.

All anledning fanns att probera höstchiffret, av vilket jag genom Bazeries förut citerade lilla skrift kände brottstycken genom tre olika, av Bazeries forcerade depescher.

Historien om denna forcering visar vilka egendomliga tillfälligheter som spelar in på detta område. På 90-talet upptäckte en person i Aachen att det stack fram något vitt papper ur en söndrig pärm till en Schiller-upplaga från början av århundradet. Nyfiken sprättade han upp pärmen och fann några fullskrivna papper, samtliga av Davout adresserade till kejsar Napoleon. Tre av dessa dokument var chifferdepescher. Ägaren gjorde vad han kunde för att få chiffren lösta. Men vart han vände sig blev försöken fåfänga. Så skrev han till en ättling av marskalken, general Davout, i tro att denne kanske genom familjepapperen var i besittning av chiffernyckeln. Men någon sådan fanns inte i hans papper, och han vände sig då till Bazeries. Denne förklarar att han skulle ha gått bet på uppgiften, om han inte vid undersökning i Archives nationales och Dépôt de la Guerre hade påträffat andra depescher avfattade i samma chiffer och bland dem några med lösning utskriven. Därmed lyckades han åstadkomma en nära nog komplett tolkning av de tre i Aachen funna depescherna. Dessa är, chiffer för sig och den lösta texten för sig, återgivna i Bazeries arbete som jag hade tillgång till då jag av Höjer erhöll den nu i Sverige befintliga chifferdepeschen.

Långt senare, då mitt arbete med denna redan hade framskridit tämligen bra, fick jag kännedom om att boken i Aachen gett upphov till ännu en forceringsbragd, alldeles oberoende av Bazeries. Depescherna har nämligen även tolkats på tysk sida av Willisch, chef för utrikesdepartementets chiffreringsbyrå i Berlin, enligt vad som meddelas i Hist. Jahrbuch der Görres-Gesellschaft, årg. 1896, i en artikel av Karl Wacker. Denne hade i årg. 1895 av samma tidskrift publicerat depescherna utan lösning och därvid berättat samma upptäcktshistoria som den Bazeries refererar. Forceringen hade lyckats därigenom, att ett



i svenska krigsarkivet förvarat brev från Davout till general Lemarois (kommendant för franska garnisonen i Magdeburg) ställts till Willischs förfogande. Detta brev fanns nämligen i två versioner, varav det ena i klartext tryckts i Mazade: Correspondance de Davout, medan det i Sverige befintliga till stor del var chiffrerat. Då det kunde konstateras identitet mellan de bägge versionerna fick Willisch i sin hand ett tillräckligt antal kända grupper för att kunna till största delen dechiffrera de tre Aachendepescherna. Vid en jämförelse mellan Willisch och Bazeries visar sig överensstämmelsen vara förbluffande stor. På enstaka punkter föreligger divergenser, men allt väsentligt i innehållet är lika.

Det var med Bazeries material jag angrep min uppgift. Genom analys av de fristående chiffer- och klartexterna skaffade jag mig en ordbok, så långt materialet räckte och gick att applicera den på det nya dokumentet. Det visade sig snart att ingen tvekan kunde råda om att detta var utfört i samma chiffer. Några få fullständiga ord framträdde i denna första etapp, f. ö. bokstäver och stavelser här och där, som det krävde mycken möda att sammanfoga. Det vore orimligt söka återge hur detta arbete fortskred, det såg gång på gång hopplöst ut och det var att återuppta det med nya hypoteser beträffande det stora flertalet grupper, som icke kunde erhållas ur den lilla ordbok jag hade till skänks genom Bazeries.

Då jag hade drivit det fram så långt jag kunde utan nytt material, hade depeschen följande utseende:

J'ai répondu à ce général que s'il **1118** **790** **486**
(trouve) (moyen) de
**1134** **553** **443** **265** **629** **260** **999** **309** **863**
(tir)er (sur) Hambourg je fe ra(i) (suite) à (ses)
**763** **1022** **477**
lettres de
dès que j'aurai la certitude qu'il aura
**98** **356** **1035**
les
De mon côté si je puis trouver à lui **655** **1047** **190**
(faire) pas se(r)

576 763 173 913 553 1240 265 237 629
(des) lettres de [départ] ? (sur) (ortnamn) je le fe
260 mais je doute de réussir.
ra(i)

— — — — — — — — — — — — — —

Vos instructions portaient que je 1125 816 728 1200
(ne) [sont] ? (pas) me
(devais)
1145 1177 1131 1030 463 676 340 764 260 1117
inquiet er de (s) (pas) (se) ra(i) t
553 426 49 677 801 902 591 486 1230 389(?) 117
(sur) (la) ri ve (ga) u che de (l'Elbe) (.) la
814 763 1183 183 321 679 75 1072 80 96
dernière lettre (que) (j'ai) (reçu) de V. M. (est) (du) 14
915 282 265 985 217 321 1106 233 122
(octobre) (.) je n (ai) (reçu) (aucune) (dépêche) du
(réponse)
672 10 265 85 1137 561 1106 763 1 1191
(M. Général) et je puis (même) aucune lettre (être)
321 401 422 30 938 743 184 322
(reçu) quelque (temps) (autre) (que) [tout] ? (sans)
763 460 540 10 322 221 339 42 34 117 654
lettre d (envoi) et (sans) me faire (savoir) ni la da
(connaître)
185 813 645 333 209 963 754 455
te (ni) le li (eu) (de) l expédition

— — — — — — — — — — — — — —

Depuis les courses des partis ennemis sur la rive gauche
516 1175 136 100 576 1020 910 197 223 18 665 486
la ren tre e des con tri bu (tions) et de
117 969 910 197 497 1011 43 1131 902 100 363 677
la con tri bu tion (sont) de v e n ues
627 169 912 165
pres (que) (nul) .

M. le Comte de Chaban m'a fait connaître dernièrement



1132 115 782 577 516 132 669 251 363 950 149
que le (défaut) ? al la (i) (t) (a) n avoir plus
169 1165 1179 139 985 731 58 731 947 1104 676
(que) cinq (mille) (fra) n c (s) c ai s (s)
934 816 969 95 735 524 1167 10 251 363 855 128
(e) [sont] ? con si (der) able [après] ? et a n y (voir)
(devaient) [ment] ?
938 1168 790 381 1131 627 985 175 11 382 363
(autre) (—) (moyen) (que) de pre n (dre) les fo n
460 432 831 210 954 117 705 381 518 265 221 103
d s qui étaient dans la (ban que) . je me (suis)
486 420 1164 1186 979 124 760 296 54 1113
de ter mi ne a (cette) (mesure) [et] ? (on) (a)
1118 597 306 412 700 793 418 333 985 469
(trouvé) en vi (ron) (siffra) millions (en) li n (go)
1117 432 831 au fur et à mesure 291 895 190
t s qui (quelque) ? (part) ? se(r)
54 1020 741 626 539 597 363 902 926 260 772 543 309
ont con ver ti s en n u (me) rai re i a
479 1055 169 115 118 224 659 327 564 339
mo (ins) (que) le (compte) [ne] ? s (aur) ? a (faire)
671 382 985 460 539 636 115 782 Je doute qu'il
(les) fo n d s (pour) le (défaut)
adopte cette proposition. Sans cette 760 846
(mesure) [à la] ?

55 464 1117 1016 539 671 62 486
[dernière] ? [heure] ? t (ou) s (les) (travaux) de
(jour)
754 41 296 80 549 34 100 210 820 1104 334
l (entretien) [et] du ge ni e étaient (su) s pe
(artillerie)
985 488 1104 714 679 382 363 460 539
n (du) s (manque) de fo n d s

— — — — — — — — une ligne bastionnée — — — — — — — — qui peut être considérée comme terminée à l'exception
122 1171 228 941 731 93 372 363 854 340 638 597
du che m in c ou (vert) n (étant) pas encore en

136 332 681 418 306 412 117 920 626 100 — — — —
tre (pris) sur en vi ron(s) la (sor) ti e
(moi)
265 918 309 1144 930 511 1113 812 338 956 238 902
je f a (is) (faire) a k ha u
503 1042 33 383 626 918 539 463 676 173 479 985 607
po r (ta) ti f s (s) de mo n tent
1111 172 575 990 671 214 460 431 ce qui ajoutera
pour (mettre) dans tout (les) d
beaucoup à la force de la place.

— — — — — — — — — — — — — —

— — — —— — — — — et le fort de Harbourg est fait
625 1069 773 576 757 985 654 592 191 549 1104
a [l]? (des) (bli) n da [di]? [—]? ge s
(—)
953 516 310
pour la garnison

Quant à la position de l'Armée, j'occupe toujours Ratzebourg ma gauche appuyée a Travemünde et ma droit à Lauenbourg, 285 1010 11 150 902 54 136 263 184 45
(jusqu') (ici) les danois v ont tres bien [tout]? roi
135 306 677 598 1117 93 1129 1167 993 165 50
(est) vi ve (ment)? t ou (r) (ment)? (e) . .
452 564 340 828 1010 600 643 1131 1044 801
a pas se (ici) un (sécrètaire)? de le (ga)
497 150 259 212 963 1219 115 558 55
(tion) danois [par]? [ti]? (de) (ortnamn) le deux [dernier]
799 159 605 728 828 1113 905 333 363 115 748 18
(a) (pas) se (a) ber li n le (siffra?) et
115 280 731 93 1129 1117 605 577 1117 153 620 251
le (bruit) c ou (r) t (a) (al) t (o) n (a)
(siffra)
1135 554 963 763 1022 1140 781 18 80 45
[est]? (muni) (de) lettre de (son)? (ministre)? et du roi
56 636 115 45 150 Si ce bruit est vrai on m'en
(prusse) (pour) le roi danois



564 655 600 1164 420 e 998 601 597 1190 265 627 363
a (fait) un mis? ter en je pre n
664 990 11 964 322 479 363 136 670 426 149
(ds) toutes les (précautions) ? sans mo n tre r la plus
162 626 810 154 636 206 740 1126 480 43 605
(pe) ti te (crainte)? (pour) son(t) (a)
(signe)?
426 23 654 893 1069 304 237 606 connu 80 45 1125
la da i (l) [sa]? le du roi ne
(—)
334 33 172 217 1047 486 1100 601 332 534 518
pe r (mettr) (ait) pas de (croire) (pris)? .
398 43 4 597 924 115 759 594 1104 676 676 1003
. son général en chef le prince he s (s) (s)?
54 224 928 595 10 418 4 l'harmonie est par-
on ne (peut)? (méfier) et en général
faite entre les troupes de V. M. et celles Danoises.

— — — — — — — — — — — — — —

I detta skick hade jag tillfälle att diskutera depeschen med Höjer, som gav mig värdefulla anvisningar om Davoutlitteratur. Uppgifter i *Servières* l'Allemagne française sous Napoléon Ier och i *Vigier* Davout, maréchal d'Empire om beslaget på Hamburgerbankens tillgångar gav i sak bekräftelse på det tolkade innehållet i depeschen. På flera ställen i litteraturen finns f. ö. nämnt, att Davout den 6 nov. rapporterat till kejsaren om dessa sina åtgärder. Den största överraskningen mötte emellertid i *Mazades* utgåva av Correspondance de Davout. Under nr 1480 finns där publicerad en depesch, daterad Ratzebourg 6 nov. 1813, som visar sig vara just det av mig behandlade chifferdokumentet. Något nytt historiskt stoff var sålunda med dess forcering ej bragt i dagen. Forceringsresultatet överensstämde till väsentliga stycken med det ur Davouts personliga arkiv av Mazade publicerade dokumentet. Genom denna upptäckt blev det nu möjligt att komplettera luckorna i tolkningen. Dock med ett betydelsefullt undantag. Den hos Mazade tryckta och den i Stockholm bevarade depeschen skiljer sig åt däri, att chifferdepeschen har ett helt parti som alldeles saknas i den

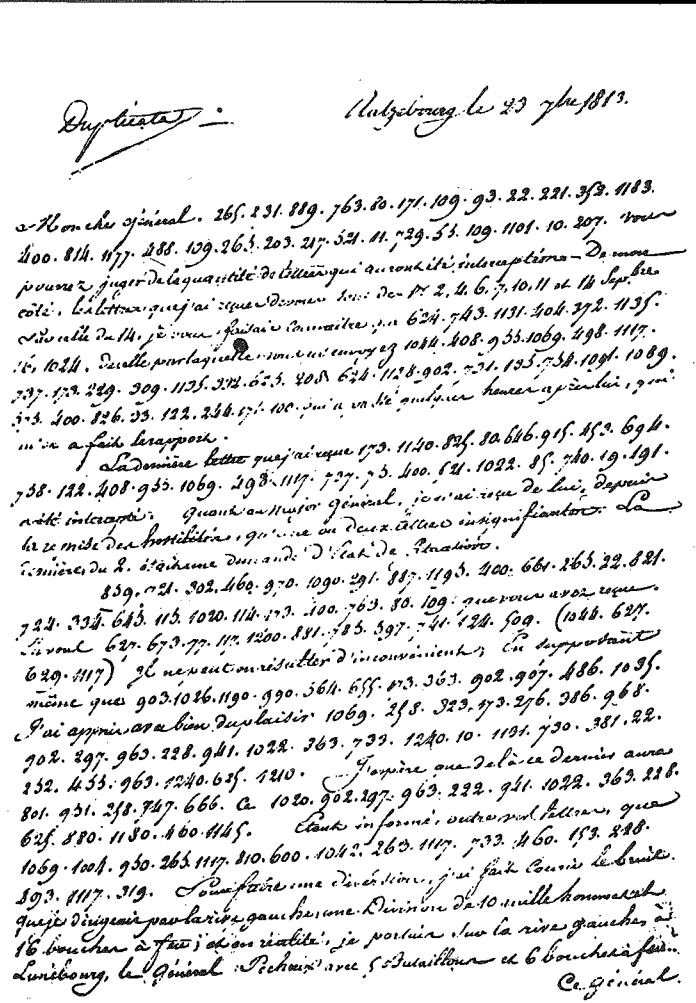
tryckta. Det är hela slutavdelningen efter klartexten: Quant à la position de l'Armée etc. I trycket följs detta stycke omedelbart av chiffrets avslutande klartext: J'ai maintenant une très bonne tête de pont à Hope etc. En mindre divergens i samma stycke är att trycket innehåller följande omdöme om danskarna: La meilleure intelligence existe entre les troupes de Votre Majesté et les troupes danoises. Le général en chef, le prince de Hesse, se conduit on ne peut mieux. Men i stället handlar hela det parti i Stockholms-depeschen, som icke återfinns hos Mazade, om danskarna, vilket den redan verkställda forceringen visat.

Detta parti om ca 150 chiffergrupper kunde alltså varken kontrolleras eller kompletteras genom fyndet hos Mazade. Det blev nu den sista etappen i forceringen att komma till rätta därmed. Det skulle inte ha lyckats, om ej ytterligare hjälpmaterial kunnat skaffas. Redan är nämnt, att den tyska lösningen av Aachen-dokumenten genomförts tack vare ett dokument i svenska krigsarkivet. Efter åtskilligt forskande har arkivet återfunnit detta. (Se facsimile.) Och det visade sig vara synnerligen värdefullt. Det kompletterade ordlistan med ett antal nya grupper. Med användning av dem kunde nu slutspurten ske. Chifferdepeschen föreligger därmed med ett par obetydliga frågetecken tolkad i sin helhet som följer:

J'ai répondu à ce général que s'il 1118 790 486
trouvait moyen de
1134 553 443 265 629 260 999 309 863 763
tirer sur Hambourg je fe - rai *honneur* a ses lettres
1022 477
de *change*
dès que j'aurai la certitude qu'il aura
98 356 1035
*touché* les *fonds*
De mon côté si je puis trouver à lui 655 1047 190 576
faire pas ser des
763 173 913 553 1240 265 237 629 260 mais
lettres de *change* sur *Magdebourg* je le fe - rai
je doute de réussir.

— — — — — — — — — — — — — —





Vos instructions portaient que je 1125 816 728 1200
ne devais pas m
1145 1177 1131 1030 463 676 340 764 260 1117 553
inquiét - er de *ce qui se* pas - se - rai - t sur
426 49 677 801 902 591 486 1230 389 117 814 763
la ri - ve ga - u - che de l'Elbe . la dernière lettre

1183 183 321 679 75 1072 80 96 915 282 265 985 217
que j'ai reçu de V. M. est du *16 août* . je n ai
321 1106 233 122 672 10 265 85 1137 561
reçu aucun *ordre* du M. Général et je puis (même) (affirmer) ?
1106 763 1 1191 321 401 422 30
aucune lettre — être reçu (sauf) ? quelques *nominations*
(seulement) ?
938 743 184 322 763 460 540 10 322 221 339
*d officiers mais* sans lettre d envoi et sans me faire
42 34 117 654 185 813 645 333 209 963 754 455
connaître ni la da - te ni le li - eu de l expédition
— — — — — — — — — — — — — —

Depuis les courses des partis ennemis sur la rive gauche
516 1175 136 100 576 1020 910 197 223 18 665 486 117
la ren - tre - e des con - tri - bu - tions et *celle* de la
969 910 197 497 1011 43 1131 902 100 363 677
con - tri - bu - tion extraordinarie sont de - v - e - n - ues
627 169 912 165
pres - que nulles .

M. le Comte de Chaban m'a fait connaître dernièrement
1132 115 782 577 516 132 669 251 363 950 149
que la *service*. al - la - *it manquer qu'il* n avait plus
169 1165 1179 139 985 731 58 731 947 1104 676 934
que cinq mille fra - n - c - s c ai - s - *se qu'il*
816 969 95 735 524 1167 10 251 363 855 128 938
devait con - si - der - able - ment et *qu'il* n y voyait d
1168 790 381 1131 627 985 175 11 382 363 460 432
autres moyens que de pre - n - dre les fo - n - d - s
831 210 954 117 705 381 518 265 221 103 486 420
qui étaient dans la ban - que . je me suis de - ter -
1164 1186 979 124 760 296 54 1113 1118 597 306
mi - ne a cette mesure et l'on a trouvé en - vi -
412 700 793 418 333 985 469 1117 432 831 au fur
ron (11?) millons en li - n - go - t s qui
et à mesure 291 895 190 54 1020 741 626 539 597
*des besoins* ser - ont con - ver - ti - s en



363 902 926 260 772 543 309 479 1055 169 115 118
n - u - me - rai - re i a mo - ins que le *commerce*
ne s *engage* à 339 671 382 985 460 539 636 115
224 659 327 564 faire les fo - n - d - s pour le
782 Je doute qu'il adopte cette proposition. Sans cette
service
760 846 55 464 1117 1016 539 671 62 486 754
mesure *sous huit jours* t - ou - s les travaux de l
41 296 80 549 34 100 210 820 1104 334 985
artillerie et du ge - ni - e *seraient?* su - s - pe - n -
488 1104 714 679 382 363 460 539
du - s *faute* de fo - n - d - s

— — — — — — — — une ligne bastionnée — — — —
— — — qui peut être considérée comme terminée à l'exception
122 1171 228 941 731 93 372 363 854 340 638 597
du che - m - in c - ou - vert n étant pas encore en -
136 332 681 418 306 412 117 920 626 100 — — — — —
tre - pris sur en - vi - ron la *moi* ti é
265 918 309 1144 930 511 1113 812 338 956 238 902
je f - a - is faire *40* a *50 bloc* - k - ha - u -
503 1042 33 383 626 918 539 463 676 173 479 985 607
s po - r - ta - ti - f - s *qui se* de - mo - n - tent
1111 172 575 990 671 214 460 431 ce qui ajoutera
pour mettre dans toutes les *places* d *armes*
beaucoup à la force de la place.

— — — — — — — — — — — — — —

— — — — — — — — et le fort de Harbourg est fait
625 1069 773 576 757 985 654 592 191 549 1104
a l exception des bli - n - da - — — ge - s
953 516 310
pour la garnison

Quant à la position de l'Armée, j'occupe toujours Ratzebourg ma gauche appuyée a Travemünde et ma droit à Lauenbourg, 285 1010 11 150 902 54 136 263 184 45
jusqu' ici les danois v - ont très bien *mais* [le] roi

135 306 677 598 1117 93 1129 1167 993 165 50 452
est vi - ve - ment t - ou - r - ment - e . . il
564 340 828 1010 600 643 1131 1044 801 497
a pas - sé ici un (sécrétaire) de lé - ga - tion
150 259 212 963 1219 115 558 55 799 159 605
danois par - ti de [ortsnamn] ? le 2 - 8 (*oct*) *il* a
728 828 1113 905 333 363 115 748 18 115 280 731
pas - sé a ber - li - n le [siffra] et le bruit c -
93 1129 1117 605 577 1117 153 620 251 1135 554 963
ou - r - t a al - t - o - *na qu'il* est muni de
763 1022 1140 781 18 80 45 56 636 115
lettre de *l'Empereur (russe)* et du roi (prusse) pour le
45 150 Si ce bruit est vrai on m'en 564 655 600 1164
roi danois a fait un mis -
420 e 998 601 597 1190 265 627 363 664 990 11
ter *(quoi) qu'il* en *(soit)* je pre - n - ds toutes les
964 322 479 363 136 670 426 149 162 626 810
(précautions) sans mo - n - tre - r la plus pe - ti - te
154 636 206 740 1126 480 43 605 426 23
(crainte) pour (10?) — *tra - hi - son* a la *(confédération)*
*(une)*
654 893 1069 304 237 606 connu 80 45 1125 334
da - i - l - *leur* le (caractère) du roi ne pe -
33 172 217 1047 486 1100 601 332 534 518 398
r - mettr - ait pas de croire *qu'il* (prend) part . .
43 4 597 924 115 759 594 1104 676 676 1003
son général en chef le prince he - s - *se se conduit*
54 224 928 595 10 418 4
on ne peut *mieux* et en général l'harmonie est parfaite
entre les troupes de V. M. et celles Danoises.

— — — — — — — — — — — — — —



# 13. Tårta på tårta

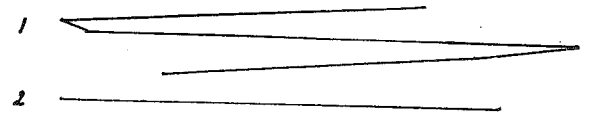
*En sockerbagares spionageförsök*

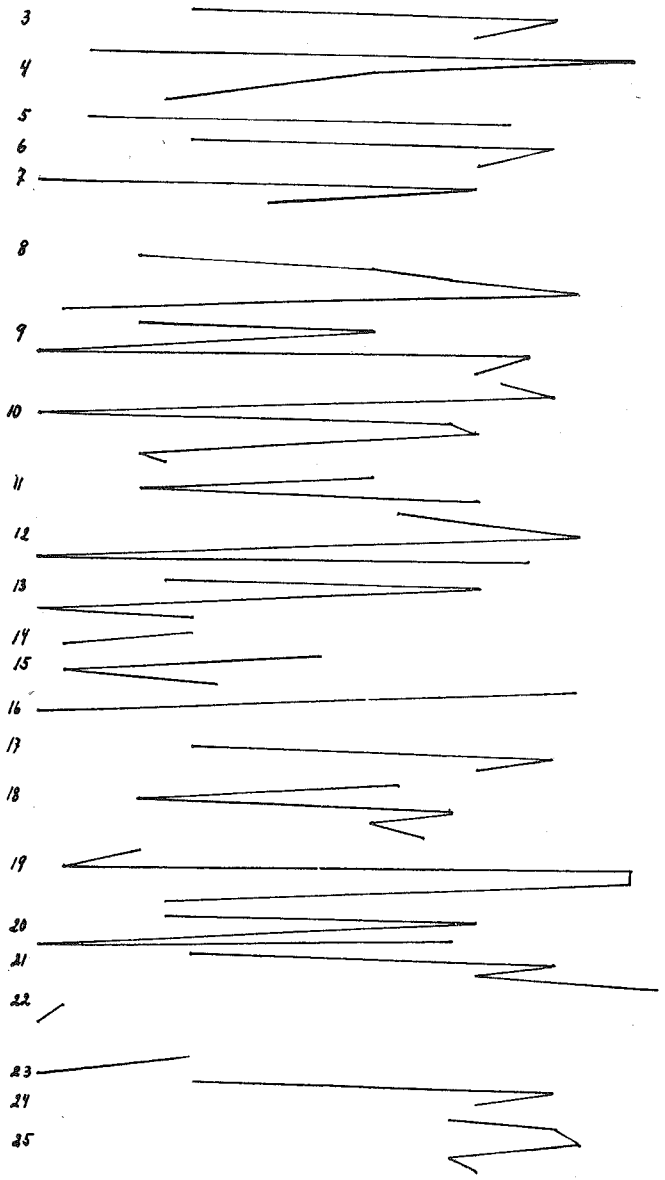
Tårta på tårta kan ha en farligare betydelse än att säga om samma sak i onödan.

I en fransk stad strax bakom fronten under första världskriget levde en sockerbagare, som hade ådragit sig kontraspionagets uppmärksamhet på grund av det intresse han visade för trupprörelser och militära angelägenheter överhuvud. Man hade också kunnat konstatera, att fienden på något vis hölls underrättad om ting som det var av vitalt intresse att dölja. Man hade länge misstänkt bagaren utan att komma på honom med något graverande. Tydligen skaffade han sig vissa informationer, men om han överbringade något till fienden och hur, hade trots minutiösa undersökningar icke kunnat ådagaläggas.

En enda sak föreföll besynnerlig i hans yrkesutövning, han brukade leverera tårta på tårta till en antikvitetshandlare i en annan stad på flera mils avstånd. Man hade flera gånger låtit hans tårta komma bort på vägen och grundligt genomforskat innanmätet utan att finna något misstänkt.

Så får en medlem av kontraspionagebyrån, som hade fantasi över den rutinmässiga nivån, idén att titta närmare på den chokladutsirning varmed varje tårta var på vanligt sätt försedd. Han företog sig att noggrant fixera de smala chokladstrimlornas utseende, läge och längd. En dag sände bagaren sin kund tre tårtor på en gång. Vid exakt avbildning på rutat papper av chokladdekoren framgick då följande teckningar, som då de ordnades under varandra, bildade nedanstående totalbild av räta och zigzag-dragna linjer. Han numrerade dem till ett antal av 25.





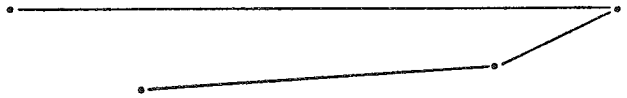



Det kunde kanske betyda 25 ord. Flera linjekombinationer befanns exakt lika; t. ex. nr 3, 6, 17, 24. Till en början trodde han att varje linje betydde en viss bokstav, men fick absolut ingen mening av sammanställningen. Då han lät ögat löpa uppifrån och ner, fäste han sig emellertid vid att många linjer började, respektive slutade på samma punkt i vertikalplanet. Han lade en linjal på teckningen och lät den glida vertikalt från ena till andra sidan och fann då, att den förvirrande mängden av linjer hade sina begynnelse- eller ändpunkter i summa 18 olika lägen. 18, det skulle just vara ett passande antal bokstäver i ett kortare meddelande. Tänk om linjernas utseende i övrigt saknade betydelse och det enda riktiga var just dessa lägen?

Man kunde ju tänka sig, att det var punkterna som betecknade bokstäverna och att orden bildades genom att hur som helst med linjer sammanbinda dessa punkter. Då skulle man just få ett sådant zigzag-mönster. Den förut anmärkta upprepningen

blev då ett ord icke om två bokstäver utan ett 3-bokstavigt ord, bestående av punkterna

Efter fåfänga tolkningsförsök utgående från att det brukade språket var franska och likaså misslyckade prov med tyska, övergick vår man till hypotesen engelska och gick in för att den påtagligaste upprepningen kunde vara engelskans vanliga the. Då borde nr 27, som innehöll ytterligare en punkt, rimligast vara them.



Nr 22 och nr 23 med två bokstäver lockade nu. Det senare "ordet" med början på t, borde då vara to

det förra, börjande på punkten o, sannolikt on eller of

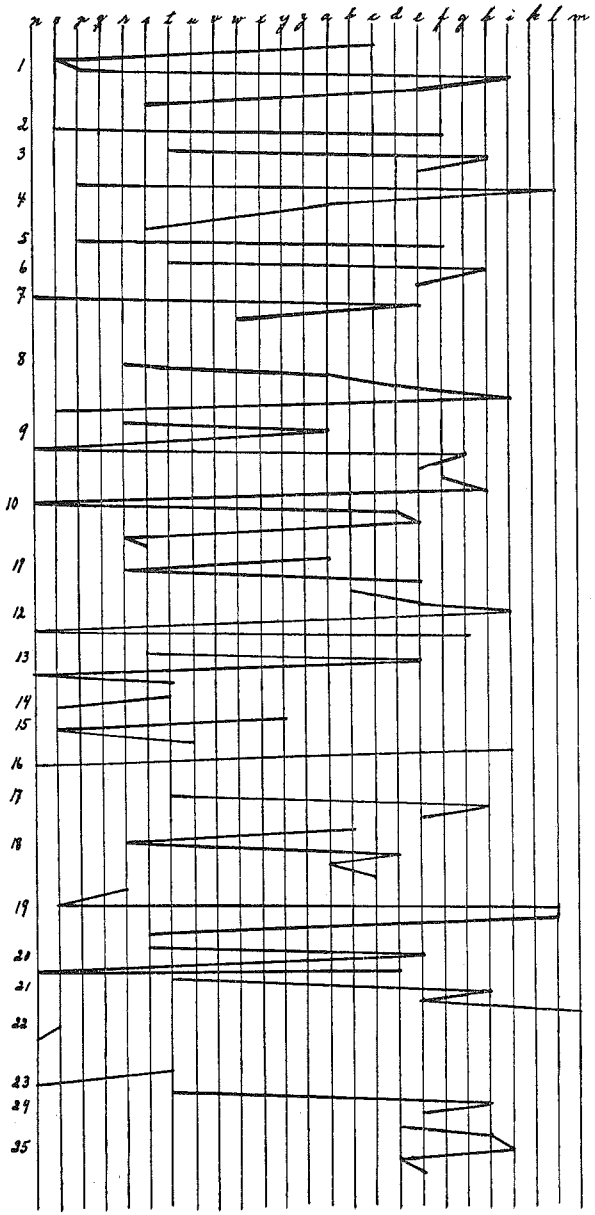
Med de förra tolkningarna skulle de båda intill varann liggande bokstäverna n och o komma att representeras av två närmast varann belägna punkter. Ja, varför inte?

Genom att lägga in vertikallinjer, som i teckningen på nästa sida, kunde forceraren avslöja hela alfabetet och därmed meddelandets innehåll:

Copies of the plans of the new radio range are being sent to you in bread rolls. Send them on to the chief.

Sen bagaren hängts, fick antikvitetshandlaren vänta på sina tårtor.





# 14. PQR — ett tyskt cirkulärtelegram från första världskriget

Det chiffermeddelande, som i det efterföljande behandlas, är ett aktstycke från första världskriget. Det är hämtat ur *Yardleys* läsvärda bok "The American black chamber" (har utkommit i svensk översättning under titeln "Amerikas svarta kammare"). Några veckor efter vapenvilan utsändes det av tyske generalkonsuln i Mexiko till alla tyska konsuler i landet, beordrande dem att förstöra alla den hemliga tjänsten berörande handlingar. Yardley upplyser att han fått det i sin hand för forcering av en i mexikanska telegrafverket placerad spion, vars uppgift var att stjäla kopior av tyska chiffermeddelanden. Detta berättas och dokumentet återges i kapitlet om Pablo Waberski, den ende tyske agent som i Amerika blev avrättad under första världskriget, ansedd för att vara den farligaste av där verksamma spioner.

Waberski hade i febr. 1918 arresterats vid gränsen till Mexiko. Det enda komprometterande han innehade var ett pappersark med chifferskrift. Detta fick Yardley ta hand om med order att dechiffrera det på en natt. Det utfördes också. Papperet visade sig vara ett av tyske ministern i Mexiko von Eckhardt utfärdat intyg att innehavaren var tysk agent och av tyska myndigheter skulle åtnjuta allt stöd. På detta fällande bevis dömdes också Waberski till döden.

Yardley talar rätt utförligt och mycket instruktivt om, med vilken metod han lyckades knäcka detta Waberski-chiffer. Han uppfordrar i samband med återgivandet av generalkonsulns stulna cirkulär sina läsare att söka forcera detta. Han anger ingenting om sitt eget tillvägagångssätt men gör den för uppgiften hugade läsaren den stora tjänsten att meddela i engelsk översättning vad cirkuläret innehöll.

En av Yardleys läsare framlägger nu här, hur han efter att ha stängt sig inne några vackra feriedagar genomförde forceringen. Då chiffret återgivits mitt i Waberski-historien och till



det yttre erinrade om det för denne ödesdigra chiffrerade papperet, kunde antas att chiffret tillhörde samma typ av omkastningschiffer. Dock visar resultatet att det var av betydligt mer komplicerad beskaffenhet än det i Yardleys bok analyserade. Den långa mödan visas bäst av den långrandiga utveckling som nu följer. Dess ursäkt må vara att åskådligt klargöra hur mycket arbete, som kan ligga bakom en kryptomans resultat.

Telegrammet är stämplat Deutsche Gesandtschaft och daterat Mexiko 10 jan. 1919. Med ett här gjort tillfogande av några understrykningar samt en numrering, visande varje bokstavs plats i chiffret, lyder det:

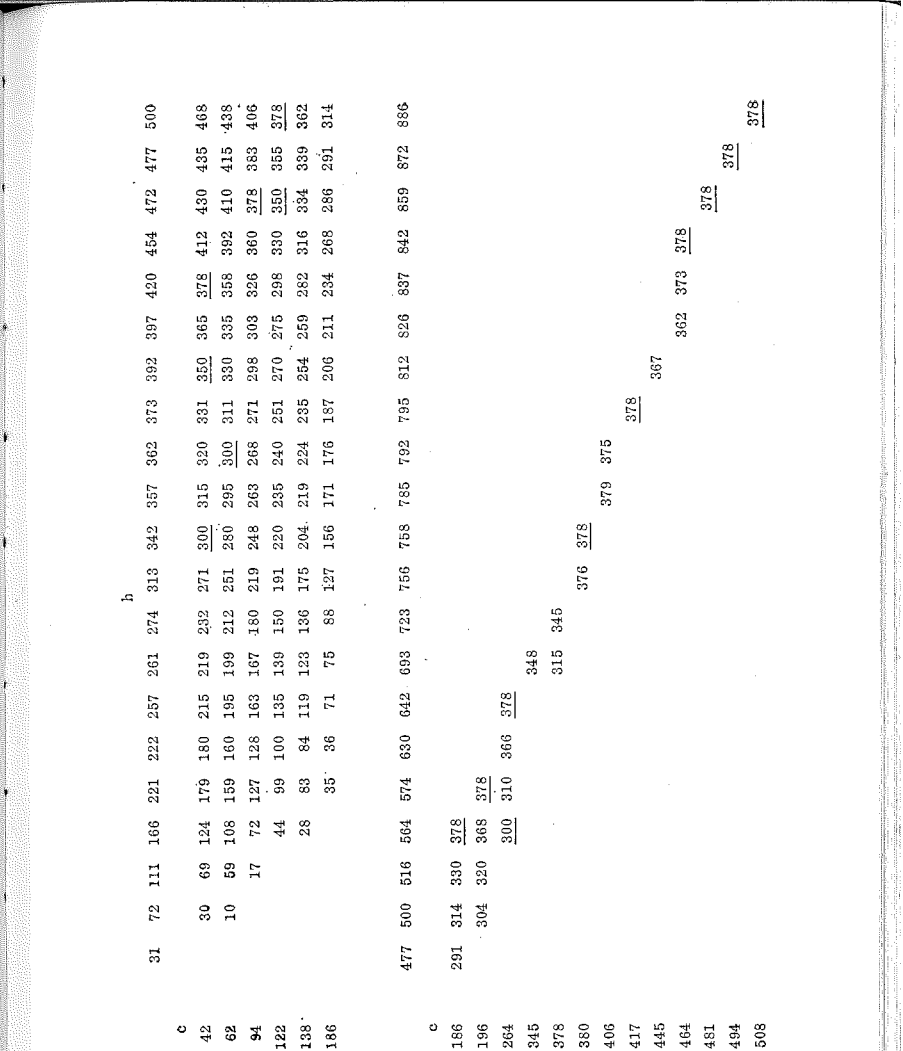
| | | | | | |
|---|---|---|---|---|---|
| 1 | nogaaaimue | 11 | saeesntraa | 21 | seienewwei |
| 31 | heuamaoeid | 41 | zedkeftedt | 51 | edgeigunri |
| 61 | eceutnninb | 71 | mhbebanais | 81 | iteaarukss |
| 91 | tdscmoorob | 101 | aeuoermotd | 111 | hzzzdibgtt |
| 121 | fceumlreri | 131 | eeoemffcea | 141 | iqeirenuef |
| 151 | drisrrbnle | 161 | enznuhbtpf | 171 | kgtineenel |
| 181 | anvescalrr | 191 | adngdceoeu | 201 | tiailuiorl |
| 211 | bkrnnoeeqe | 221 | hhananvsdf | 231 | niemineiee |
| 241 | eetreegdmp | 251 | eilsbihlnu | 261 | hodciageef |
| 271 | sttheetdbe | 281 | ugmuaudnuu | 291 | dnsfnenenn |
| 301 | umtralgtnu | 311 | rehnemenbe | 321 | mntngefsae |
| 331 | kltzedrkii | 341 | rhficnvaks | 351 | onbtguhewn |
| 361 | thitzmsrmd | 371 | lghireicsc | 381 | enpneiette |
| 391 | nhvdnvhbvn | 401 | nrsnecnemn | 411 | ngepniceuh |
| 421 | eortsgesie | 431 | eneonfiend | 441 | wnpkcevemd |
| 451 | isrhwlften | 461 | amucnosazr | 471 | ahelnehiln |
| 481 | crseamilnb | 491 | eutceszrth | 501 | rsaeoszclx |
| 511 | mneouhslcu | 521 | nmenenefae | 531 | eckerglnra |
| 541 | bgfireubli | 551 | roznnsseuz | 561 | csthpusica |
| 571 | ufohunnbdn | 581 | betfmmcirt | 591 | unfrnsrbna |
| 601 | dsukouiust | 611 | bmgdreninu | 621 | lusneadash |
| 631 | scecfaonen | 641 | ehsmnrgoot | 651 | erzruierne |
| 661 | incneinfee | 671 | etgstnbika | 681 | zeugdednkr |
| 691 | ibhideeree | 701 | aeuneinzet | 711 | dendaoerea |
| 721 | ighueuoanu | 731 | uzasruoddi | 741 | eeemcutiee |

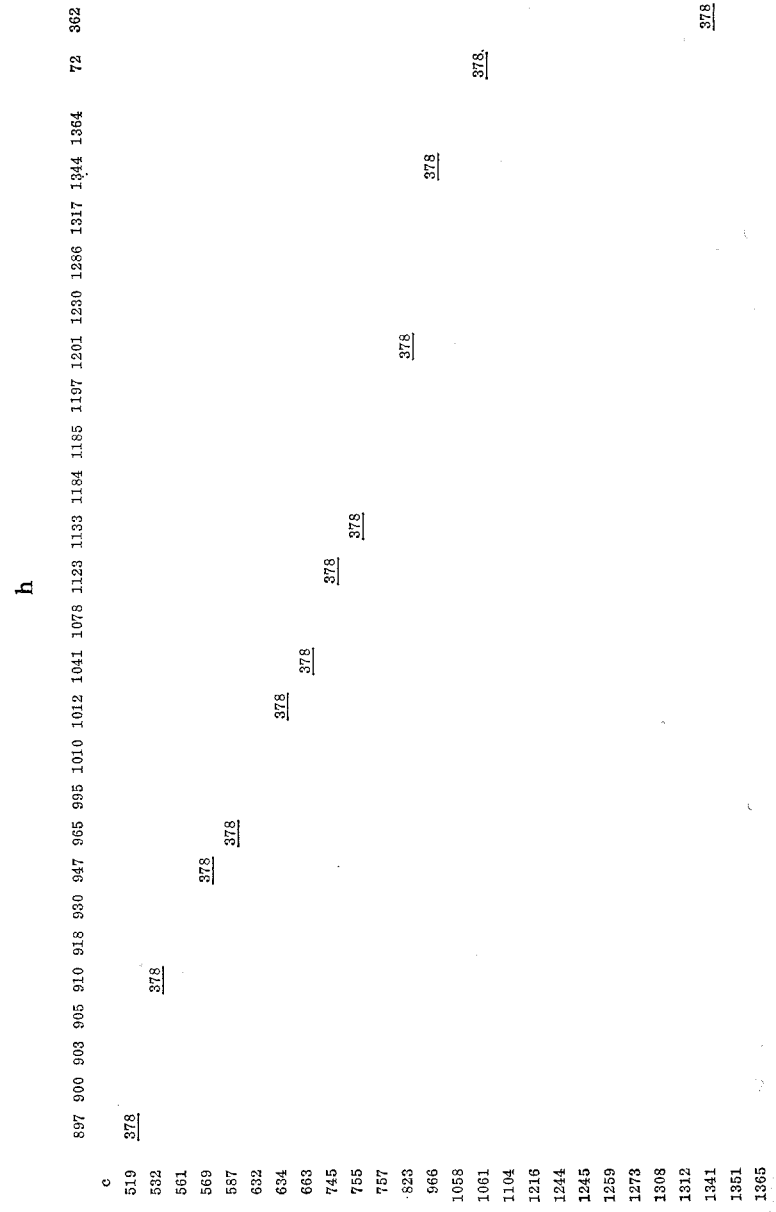
| | | | | | |
|---|---|---|---|---|---|
| 751 | teanchchdd | 761 | igrrrrrnso | 771 | esiereerde |
| 781 | emiehdeade | 791 | nhdthmnosm | 801 | elolmeennd |
| 811 | rhktendend | 821 | uockehaete | 831 | eresfjhouk |
| 841 | fhbmkttemn | 851 | ledsetuehl | 861 | enimliaern |
| 871 | ehzeuesesg | 881 | snmeuhaimd | 891 | rrensahikh |
| 901 | rahdhennjh | 911 | osesedfhin | 921 | meerneaseh |
| 931 | udzsgifmri | 941 | uoisoehsna | 951 | deitfeebsa |
| 961 | ekamhceant | 971 | eaoabeunou | 981 | flrnneizua |
| 991 | nfpbhmnfon | 1001 | gusdiporth | 1011 | fhrsmdndrl |
| 1021 | tmaurrwini | 1031 | ulnezsknts | 1041 | hdrsdbbnip |
| 1051 | osedlsuctb | 1061 | ctidafsaue | 1071 | ttunwirhbr |
| 1081 | ngnedumiis | 1091 | veurakklne | 1101 | enrcmtdtea |
| 1111 | nsinleimgr | 1121 | iehnlemnlg | 1131 | gkhegdatee |
| 1141 | eaaeegtero | 1151 | arusrelari | 1161 | graenutnbi |
| 1171 | eeikdnspni | 1181 | ribhhpkuze | 1191 | tkfseshdne |
| 1201 | haravntsee | 1211 | ipreicseuu | 1221 | emozusmudh |
| 1231 | ipitnndark | 1241 | nalccssgle | 1251 | ursttrlecp |
| 1261 | irbdnsaend | 1271 | recoeteian | 1281 | mdtnnheamt |
| 1291 | ntzeomtier | 1301 | nukwmttcke | 1311 | ucebdihtnf |
| 1321 | eswgowgeen | 1331 | notzreasnu | 1341 | caahngbeil |
| 1351 | ceernsnrta | 1361 | lgghcue | | |

Chiffrets transpositionstyp och språket är lätta att fastställa. Frekvensen ger klart utslag. Det använda språket är tyska. Någon invecklad transposition har använts.

Det gäller nu att se, om den metod Yardley använt för Waberski-chiffret, nämligen sammanknytningen av bokstäverna *c* och *h* kan användas även i detta fall. Det är nämligen så att i tyska c nästan undantagslöst efterföljs av antingen och mestadels h eller k. Har nu i den verkliga texten bokstäverna splittrats efter någon matematisk regel, är det värt undersökning, om i chiffret avstånden mellan olika c och h uppvisar något mera allmänt förekommande avståndstal. Om dessa bägge bokstäver blivit skilda åt på ett visst bestämt avstånd, bör det samma gälla andra, ursprungligen sammanhängande bokstäver. Man ställer därför upp alla c och alla h med nummerplatsen angiven i en horisontell och en vertikal kolumn och räknar ut samtliga av-








ståndstal, varvid får iakttas att hela tiden räkna åt samma håll, dvs. räkna till slutet och börja från början igen, enär ett c som nu står nära slutet mycket väl hänger ihop med ett h, som kommit i början av chiffret. Av vidstående sammanställning framgår en klar överlägsenhet för avståndet 378.

Reflektioner till siffran *378*. Antaget att det är fråga om ett transpositionschiffer av rektangeltyp, så kan redan nu förmodande göras om rektangelns utseende.

$$378 = 2 \cdot 3 \cdot 3 \cdot 3 \cdot 7$$

De möjliga rektangeltyperna blir: 6·63, 18·21, 54·7, 14·27, bland vilka den första och tredje kan utmönstras som ohanterliga. Rektangeln torde vara antingen 18·21 eller 14·27 med företräde för den förra som den bekvämare. Avgörande prov först då det kunnat påvisas en regelbundenhet i orddelarnas avstånd efter antingen 14- eller 18-sammansättningar.

Hela bokstavschiffret uppdelas nu efter avståndet 378 i kolumner om resp. 4 och 3 bokstäver. Varje orddel får här sitt linjenummer, som i fortsättningen används.

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 1 | n | s | c | g | 146 | e | n | a | n | 291 | d | e | b |
| 2 | o | c | h | d | 147 | n | e | h | m | 292 | n | e | n |
| 3 | g | e | d | a | 148 | u | n | d | d | 293 | s | e | i |
| 4 | a | n | d | t | 149 | e | e | h | t | 294 | f | t | p |
| 5 | a | p | i | e | 150 | f | f | e | n | 295 | n | k | o |
| 6 | a | n | g | e | 151 | d | a | n | n | 296 | e | s | s |
| 7 | i | e | r | e | 152 | r | e | n | h | 297 | n | t | e |
| 8 | m | i | r | a | 153 | i | e | j | e | 298 | e | n | d |
| 9 | u | e | r | a | 154 | s | c | h | a | 299 | n | b | l |
| 10 | e | t | r | e | 155 | r | k | o | m | 300 | n | i | s |
| 11 | s | t | r | e | 156 | r | e | s | t | 301 | u | k | u |
| 12 | a | e | n | g | 157 | b | r | e | n | 302 | m | a | c |
| 13 | e | n | s | t | 158 | n | g | s | t | 303 | t | z | t |
| 14 | e | h | o | e | 159 | l | l | e | z | 304 | r | e | b |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 15 | s v e r | 160 | e n d e | 305 | a u c |
| 16 | n d s o | 161 | e r f o | 306 | l g t |
| 17 | t n i a | 162 | n a h m | 307 | g d i |
| 18 | r v e r | 163 | z b i t | 308 | t e d |
| 19 | a h r u | 164 | n g n i | 309 | n d a |
| 20 | a b e s | 165 | u f m e | 310 | u n f |
| 21 | s v e r | 166 | h i e r | 311 | r k s |
| 22 | e n r e | 167 | b r e n | 312 | e r a |
| 23 | i n d l | 168 | t e r u | 313 | h i u |
| 24 | e r e a | 169 | p u n k | 314 | n b e |
| 25 | n s e r | 170 | f b e w | 315 | e h t |
| 26 | e n m i | 171 | k l a m | 316 | m i t |
| 27 | w e i g | 172 | g i s t | 317 | e d u |
| 28 | w c e r | 173 | t r e t | 318 | n e n |
| 29 | e n h a | 174 | i o h c | 319 | b e w |
| 30 | i e d e | 175 | n z u k | 320 | e r i |
| 31 | h m e n | 176 | e n d e | 321 | m e r |
| 32 | e n a u | 177 | e n z u | 322 | n e h |
| 33 | u n d i | 178 | n s s c | 323 | t a b |
| 34 | a g e n | 179 | e s g e | 324 | n e r |
| 35 | m e n b | 180 | l e i b | 325 | g u n |
| 36 | a p h i | 181 | a u f d | 326 | e n g |
| 37 | o n d e | 182 | n z m i | 327 | f e n |
| 38 | e i t e | 183 | v c r h | 328 | s i e |
| 39 | i c h i | 184 | e s i t | 329 | a n d |
| 40 | d e m k | 185 | s t u n | 330 | e z u |
| 41 | z u n d | 186 | c h o f | 331 | k e m |
| 42 | c h o n | 187 | a p i e | 332 | l t i |
| 43 | d e s s | 188 | l u s s | 333 | t d i |
| 44 | k o m p | 189 | r s o w | 334 | z e s |
| 45 | e r e n | 190 | r i e g | 335 | e n v |
| 46 | f t l i | 191 | a c h o | 336 | d d e |
| 47 | t s o r | 192 | d a s w | 337 | r a u |
| 48 | e g l i | 193 | n u n g | 338 | k o r |
| 49 | d e m b | 194 | g f a e | 339 | i e a |
| 50 | t s e h | 195 | d o d e | 340 | i r k |
| 51 | e i e h | 196 | c h e n | 341 | r e k |



| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 52 | d e n p | 197 | e u i n | 342 | h a l |
| 53 | g e n k | 198 | o n t o | 343 | f i n |
| 54 | e n d u | 199 | e n f t | 344 | i g e |
| 55 | i e r z | 200 | u b e z | 345 | c h e |
| 56 | g o h e | 201 | t d e r | 346 | n u n |
| 57 | u n k t | 202 | i n b e | 347 | v e r |
| 58 | n f t k | 203 | a b s a | 348 | a u c |
| 59 | r i e f | 204 | i e a s | 349 | k o m |
| 60 | i e n s | 205 | l t e n | 350 | s a t |
| 61 | e n d e | 206 | u f k u | 351 | o n d |
| 62 | e d e s | 207 | i m a c | 352 | n u t |
| 63 | e w n h | 208 | o m m a | 353 | b u e |
| 64 | u n d d | 209 | r c h a | 354 | t z a |
| 65 | t p u n | 210 | l i c h | 355 | g a n |
| 66 | n k o e | 211 | b r e n | 356 | u s s |
| 67 | n o c h | 212 | k t a b | 357 | h r i |
| 68 | i e k a | 213 | r u n g | 358 | e u n |
| 69 | n v e r | 214 | n n t e | 359 | w o l |
| 70 | b e h a | 215 | n f e i | 360 | n d e |
| 71 | m m a v | 216 | o r a l | 361 | t d i |
| 72 | h d e n | 217 | e n o c | 362 | h i m |
| 73 | b i t t | 218 | e s a e | 363 | i e g |
| 74 | e s e s | 219 | q r b e | 364 | t e r |
| 75 | b r e e | 220 | e b e r | 365 | z e i |
| 76 | a h r e | 221 | h n u n | 366 | m m e |
| 77 | n w e i | 222 | h a n s | 367 | s c h |
| 78 | a l s p | 223 | a d o n | 368 | r u n |
| 79 | i f f r | 224 | n s u r | 369 | m t l |
| 80 | s t j e | 225 | a u f t | 370 | d i e |
| 81 | i e h i | 226 | n k l a | 371 | l e m |
| 82 | t n o c | 227 | v o r l | 372 | g e n |
| 83 | e a u s | 228 | s u n g | 373 | h t l |
| 84 | a m k e | 229 | d i n g | 374 | i e g |
| 85 | a u f u | 230 | f u e h | 375 | r a g |
| 86 | r c h u | 231 | n s i c | 376 | e n k |
| 87 | u n b e | 232 | i t z u | 377 | i c h |
| 88 | k o m m | 233 | e b u e | 378 | c h e |

| | | | |
|---|---|---|---|
| 89 | s s k o | 234 | m m a |
| 90 | s a t z | 235 | i g n |
| 91 | t z t u | 236 | n d f |
| 92 | d r e s | 237 | e r p |
| 93 | s a m m | 238 | i e b |
| 94 | c h n u | 239 | e n h |
| 95 | m e l d | 240 | e i m |
| 96 | o l e h | 241 | e n n |
| 97 | o n d i | 242 | e u f |
| 98 | r e s p | 243 | t l o |
| 99 | o h e i | 244 | r u n |
| 100 | b i t t | 245 | e s g |
| 101 | a l u n | 246 | e n u |
| 102 | e n e n | 247 | g e s |
| 103 | u c h d | 248 | d a d |
| 104 | o r l a | 249 | m d i |
| 105 | e s e r | 250 | p a p |
| 106 | r e n k | 251 | e s o |
| 107 | m a i n | 252 | i h r |
| 108 | o m m a | 253 | l s t |
| 109 | t i l l | 254 | s c h |
| 110 | d l i c | 255 | b e f |
| 111 | h n a c | 256 | i c h |
| 112 | z b e s | 257 | h f r |
| 113 | z e r s | 258 | l a s |
| 114 | z u n g | 259 | n o m |
| 115 | d t e l | 260 | u n d |
| 116 | i c h e | 261 | h e n |
| 117 | b e z u | 262 | o n d |
| 118 | g s e r | 263 | d e r |
| 119 | t z u s | 264 | c h l |
| 120 | t r e t | 265 | i s t |
| 121 | f t s t | 266 | a m m |
| 122 | c h e r | 267 | g n a |
| 123 | e r s l | 268 | e r u |
| 124 | u s g e | 269 | e g r |
| 125 | m a s c | 270 | f o r |



| | | | |
|---|---|---|---|
| 126 | l e n p | 271 | s o w |
| 127 | r o m i | 272 | t t i |
| 128 | e s e r | 273 | t e n |
| 129 | r z u b | 274 | h r i |
| 130 | i c h d | 275 | e z u |
| 131 | e l a n | 276 | e r l |
| 132 | e x i s | 277 | t u n |
| 133 | o m m a | 278 | d i e |
| 134 | e n d e | 279 | b e z |
| 135 | m e r n | 280 | e r s |
| 136 | f o r d | 281 | u n k |
| 137 | f u e r | 282 | g e n |
| 138 | c h n e | 283 | m i t |
| 139 | e s s c | 284 | u n s |
| 140 | a l s o | 285 | a c h |
| 141 | i c h e | 286 | u n d |
| 142 | q u i t | 287 | d e r |
| 143 | e n k e | 288 | n i s |
| 144 | i m h i | 289 | u n d |
| 145 | r e r a | 290 | u f b |

Redan från början kan från denna sammanställning antecknas dels vissa sannolika orddelar, dels vissa bokstavsramsor, som företer ett besynnerligt utseende.

Som exempel på sannolika orddelar kan nämnas: linje 4 andt, 8 mira, 23 indl, 27 weig, 34 agen, 57 unkt (p—?), 61 ende, 169 punk(—t?), 208 omma (k—?) och många andra.

Som egendomliga orddelar kan antecknas: linje 1 nscg, 46 ftli, 80 stje, 86 rchu, 91 tztu, 121 ftst, 178 nssc, 194 gfae, 197 euin, 219 qrbe.

Vidare må antecknas, att c 1061 och c 1351, som skall höra till h 72 och h 362 ger följande uppslag:

| | | |
|---|---|---|
| linje 305 och 72 | auc h/den | avstånd 145 |
| linje 217 och 362 | e/noc h/im | avstånd 145 |

Försök att kombinera andra slut-c:n med begynnelse-h:n ger inget säkert utslag.

Avståndet 145 används nu som arbetshypotes. Det ger prima vista ett antal sammansättningar, som ser möjliga ut, t. ex. 35 men/b leib 180, 53 gen/k onto 198, 71 mma/v oral 216, 73 bitt e/sae 218, 161 erfo lgt 306, 132 exis tun 277, 215 n/fei nde 360, 269 egr aphi 36, 323 t/ab satz 90, 343 fin dlic (h?) 110.

Bland orddelar att observera torde man lägga märke till sådana som kan misstänkas vara bitar av "komma" eller "punkt". Några dylika må antecknas jämte möjliga kompletteringsdelar:

| | | | | |
|---|---|---|---|---|
| 71 | mma\|v | jfr | 295 | nko |
| 88 | komm | » | 101 | alun, 34 agen |
| 108 | omma | » | 106 | renk, 341 rek, 376 enk |
| 133 | omma | » | 40 | demk, 53 genk, 58 nftk |
| 155 | rkom | » | 125 | masc |
| 208 | omma | » | 175 | nzuk, 340 irk (samt föreg.) |
| 234 | mma | » | 89 | ssko |
| 349 | kom | » | 234 | mma |

Att rester av "komma" tycks förekomma oftare än av "punkt" är i och för sig naturligt. Direkt ger ej heller dessa sammanställningar något säkert uppslag, men de bör i fortsättningen observeras, då de undan för undan kommer till nytta. Bland annat bör de kunna avslöja andra avståndssiffror för orddelarnas förskjutning än den antecknade siffran 145. Sannolikheten talar för att ett större antal sådana förekommer. För att komma dem på spåren gäller det nu att djärvt angripa ordbitarna för att kombinera dem i detta puzzle. Mera ovanliga bokstavskombinationer kan därvid först angripas.

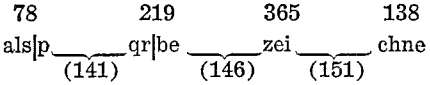
Det gäller att vinna "insteg" i chiffret någonstans. Och vi får göra upprepade försök. Några utgångspunkter har vi i kombinationerna på avstånd 145, bland dem i främsta rummet de bägge hophäktade ch-sammanställningarna *auc hden* och *enoc him*. Andra är misstänkta *komma-* och *punkt*-tecken. Slutligen bör vi djärvt gripa oss an med några orddelar med egendomligt utseende.

1) Tag t. ex. *219 qrbe,* hur kan ett ord innehålla bokstäverna



qrb i följd eller hur skall den bokstavsföljden kunna uppdelas på två ord? Detta verkar otroligt, och det leder tanken in på möjligheten att det icke alls är fråga om ord i vanlig mening. Kan det gälla en beteckning, för vilken vissa bokstäver använts, qr kommer ju i alfabetisk följd. Låt oss nu uppsöka qrbe i den stora kolonnlistan. Låt ögat genomlöpa den bredvidstående kolonnen för att efterforska någon sammansättningsmöjlighet. Där finns några steg lägre *78 alsp*. Sammanställt med föregående ger det en alfabetisk bokstavsföljd *pqr,* föregånget av ett *als,* vilket passar bra, ifall pqr är en beteckning för något (vad kan vi tills vidare ej känna). Alfabetsviten efterföljs i 219 av (qr) *be.* En blick på kolonnen höger om ger en förträfflig avslutning. Ett steg lägre står *365 zei,* vilket indikerar just beteckning, förutsatt det går att finna en fortsättningsdel i verbet *be-zei-chnen.* I kolonnen till vänster uppenbarar sig tvenne linjer med kombinationen *chn.* Det är *94 chnu* samt *138 chne,* av vilka den senare ges företräde. Gör man sig möda se efter, skall man f. ö. finna att i hela chiffret ingen mer linje har bokstavsföljden *chn.*

Nu har vi en första liten serie av orddelar och kan börja studera avstånden (härefter angivna inom parentes under och emellan resp. linjer).




Vi får fram avståndstalen 141, 146, 151, vilka alla håller sig kring förut observerade siffra 145. Om verbformen nu är fullständig (1 pers. sing.) eller skall kompletteras med *n* . . . eller *t* . . . vet vi ej. En blick på motstående och närstående linjer i 5:e kolonnen visar förekomsten av båda de senare möjligheterna men också att en annan fortsättningskombination finns 3 steg lägre än *138 chne,* nämligen *286 und,* avståndet är 148, vilket blott antecknas till minnes.

2) Vi får göra ingrepp på annat håll och välja *142 quit,* vilket omedelbart ger anledning söka en komplettering för att få substantivet Quit-tung eller verbet quit-tieren. Vi begagnar samma mekaniska metod att betrakta linjerna i bredvidstående

kolonn några steg uppåt och nedåt. För verbformen finner vi inget belägg i närheten, för substantivet erbjuder sig en möjlighet, dock först 10 steg högre, nämligen *277 tun*. Dess användbarhet hänger på att en linje *g* . . . står att finna, som kan häktas vid. Nu finns det inte någon vidstående kolonn att betrakta, då chifferlinjerna ju slutar med 378. Här må inskjutas, att man bör räkna avstånden bara i *en* riktning, framåt eller bakåt, eljest blir det lätt villervalla och misstag. Avstånden räknas sålunda hela tiden i riktning från kolonnlinjernas början mot slutet, varefter man räknar från början igen. Ett avstånd av 145 från 217 (som vi nu utgick från) blir alltså 277 + 145 − 378 = 44, de linjer som befinner sig på avståndet 145 återfinns med kolonnsystemets uppställning i kolonn 1. Den först tänkbara möjlighet vi i denna kolonn träffar vid sökande uppåt och nedåt är *53 genk*. Detta ger en plural av substantivet i *Quit-tun-genk* jämte början av ett nytt ord. En stor tur är att denna komplettering ger sig direkt ur vidstående linje, redan antecknad bland dem som med avståndstalet 145 ger brukbara ordbitar. Vi får alltså serien:

| 142 | 277 | 53 | 198 |
|---|---|---|---|
| quit (135) | tun (154) | gen\|k (145) | onto |

De nu funna avståndstalen är emellertid genomgående andra än de till förra serien hörande.

3) Vi tar en ny uppslagsända: linje *8 mira*. Osökt går tanken till något admirabelt eller, ännu enklare och troligare (det är ju fråga om ett krigschiffer, som kan innehålla militära termer) till Admiral. Vi söker den föregående kompletteringsdelen. Vi går nu bakåt, då utgångspunkten hör till de 145 första, har vi att söka kring 378 − 8 − 145 = 225, alltså i kolonn 5, efter en orddel . . *ad*. En sådan (och bara en inom 20 steg uppåt och nedåt) finns, nämligen *248 dad*. Vi får därmed:

| 248 | 8 |
|---|---|
| d\|ad (138) | mira |



med ännu ett nytt avståndstal. Försöket att finna en efterföljande komplettering efter samma metod slår alldeles fel, om vi söker kring 153 i kolonn 2. Vi får gå i den ena riktningen ända till *126 lenp*, som ej kan användas. I andra riktningen har vi tämligen nära *159 llez* och längre bort *180 leib* samt *188 luss*, ingendera tycks användbar. Vi får underkasta oss att se genom kolonnsystemets alla linjer, där finns ytterligare 6, som börjar med l. Bland dem har en redan tilldragit sig uppmärksamhet vid provandet av 145 som avståndstal, och denna linje ger dessutom bland dem alla en omedelbart begriplig fortsättning. Det är *253 lst*, vilken kan kombineras med *20 abes* (kolonn 1). Därmed får vi

| 248 | 8 | 253 | 20 |
|---|---|---|---|
| d\|ad (138) | mira | (245) l\|st (145) | abes |

Är tolkningen riktig finns det alltså avståndstal, som icke alla håller sig kring 145 som hittills. Här återfinner vi visserligen det kända talet 145 men i en helt annan serie än förut. Då gissningsmöjligheterna för ögonblicket här tycks uttömda, gör vi försök på annat håll.

4) Vi väljer *132 exis*. Det enda i chiffret förekommande x:et uppträder i en symtomatisk kombination, här måste man tänka i första hand på Existenz eller existieren. Kombinationen på avstånd 145 med *277 tun* är mindre tillfredsställande, men i närheten (kolonn 5) finns *273 ten*, som passar bättre och föranleder letande efter en linje som börjar med z . . och en sådan finns på behörigt avstånd i kolonn 1, nämligen *41 zund* och nästan mitt emot i kolonn 2 en ytterligare kombination, *192 dasw*. Alltså

| 132 | 273 | 41 | 192 |
|---|---|---|---|
| exis (141) | ten (146) | z\|und (151) | das\|w |

Betrakta nu avståndstalen i denna serie och jämför med den först framkomna *pqr*-serien. Samma avståndstal i samma ord-

ning. Härmed en första säker antydan om en regel i puzzlets virrvarr.

5) Så prövar vi också de bägge ch-sammanfogningarna:

305 72
auc h|den

ger inte mycket i och för sig. Detta kan tämligen lätt utbyggas bakåt på alldeles samma sätt som förut genom att överse vidstående linjer i kolonn bredvid. Vi erhåller:

16 151 305 72
nd|so dann auc h|den
(135) (154) (145)

Nu har vi erhållit identiskt samma serie avståndstal som i *quit*-serien.

Ett försök att utvidga:

217 362
e|noc h|im
(145)

utfaller negativt till en början. Vi har blott avståndstalet 145 som utgångspunkt. Detta tal finns redan i två serier: *quit*-serien och *mira*-serien. Men om man söker utvidga den nya kombinationen bakåt, blir resultatet obegripligt vare sig man tillämpar den ena eller andra serien:

a) 306 63 217 362
lgt tpun e|noc h|im
(135) (154) (145)

b) 212 350 217 362
ktab sat e|noc h|im
(138) (245) (145)

Båda ger idel frågetecken i fråga om sammanhanget men vi får en iakttagelse på köpet.



tpun 63 tycks kunna häktas ihop med 212 ktab vilket i sin tur mycket väl kan hänga ihop med sat 350 Avstånden är här:

63 212 350
t|pun kt|ab sat
(149) (138)

vilket ger oss ett nytt avståndstal (149) och ett gammalt (138) men i en annan serie. Skall vi ideligen upptäcka nya distanssiffror utan att komma fram till någon regel? Det gäller att hålla på, tills avståndsserien börjar upprepa sig, så att säga biter sig själv i svansen.

För att komma därhän skall vi nu ställa upp våra resultat överskådligt (se tablå på sid. 128) och efter den principen, att identiska serier av distanstal kommer under varann i de olika raderna. Utrymmet tas till så, att ett 20-tal orddelar får plats bredvid varann. Vi har att hålla oss till rektangelsiffrorna 14, 18, 21, 27 och hoppas att inte behöva gå till den högsta siffran, innan vi funnit regelmässigheten. F. ö. har vi att fortsätta med att utprobera nya kombinationer, utbygga dem framåt och bakåt och jämföra resultaten i fråga om distanstalen.

Antecknas må, att ett försök att redan nu häkta ihop de tre funna distansserierna utfaller negativt: alltså efter serien 141, 146, 151 låta omedelbart följa 135, 154, 145 och därefter 138, 245, 145. Tillräckligt att anföra vilken obegriplig ramsa det blir, om man bygger ut *pqr*-serien med *quit*-serien, och likaså om denna senare förlängs med *mira*-seriens avståndstal.

a) 78 219 365 138 273 49 194
alsp qrbe zei chne ten demb gfae
(141) (146) (151) (135) (154) (145)

b) 142 277 53 198 336 203 348
quit tun genk onto dde absa auc
(135) (154) (145) (138) (245) (145)

Det gäller alltså att finna nya distanstal, på förhand kan man inte veta hur många. Redan nu är tydligt, att talet 145 uppträder åtminstone två gånger i serie, varför det är förmånligt använda dess kombinationsmöjligheter ytterligare. Så har vi också *komma*- och *punkt*-tecknen.

6) *359 woll* kan möjligen höra samman med *126 lenp* (se föreg.). Vi prövar bakåt bägge de serier, som slutar med distanstalet 145. Det visar sig, att *mira*-serien är oanvändbar.

| 354 | 114 | 359 | 126 |
|---|---|---|---|
| tza | zung | wol | lenp |
| (138) | (245) | (145) | |

Däremot ger den andra serien ett acceptabelt resultat bakåt och kan dessutom förlängas ett steg framåt genom antagandet att det avslutande p i 126 är en beståndsdel i *punkt* (se föreg.). Vi får nämligen:

| 70 | 205 | 359 | 126 | 281 |
|---|---|---|---|---|
| beha | lten | wol | len\|p | unk |
| (135) | (154) | (145) | (155) | |

Fortsättningen framåt bör ju bildas av en linje som börjar med t (för komplettering av *punkt*). Söker vi kring 48 (kolonn 1) på avståndet 145, finner vi närmast *47 tsor* och *50 tseh*. Ingendera vågar vi utan vidare placera. Mycket längre bort finns *17 tnia* och *65 tpun,* av vilka den sista förkastas (tillhör *punkt*-kombinationen, två punkter kan ej komma alldeles efter varann). Då chiffret inalles innehåller ett 20-tal orddelar med t som begynnelsebokstav, är rikedomen väl stor för att våga en gissning utan ytterligare vägledning. Men ett nytt avståndstal har erhållits, förlängande *quit*-serien sålunda:

135, 154, 145, *155*

Därav skall vi i sinom tid använda oss. Nu söker vi flera nya uppslagsändar. Resultatet införs på sin särskilda rad.

7) Ett misstänkt, lustigt *komma* har vi i kombinationen *89 ssko, 234 mma* (se föreg.). Vi prövar de bägge distansserier, i

vilka 145 ingår, förkastar *mira*-serien (härefter tycks onödigt införa vid proven framkommande felresultat, läsaren kan göra proven själv efter vad som tidigare utvecklats) och behåller med tvekan och mycken undran det resultat, som den nyss utvidgade *quit*-serien ger. Det ser så ut:

| 178 | 313 | 89 | 234 | 11 |
|---|---|---|---|---|
| nssc | hiu | ss\|ko | mma | stre |
| (135) | (154) | (145) | (155) | |

Bokstavsramsan nsschiuss förefaller orimlig. Skulle vi vara på villospår? Ingår måhända 145 i ännu en tredje serie, den vi inte ännu kommit på? Innan vi ger upp den nu antecknade tolkningen, lockar emellertid sista orddelen till gissning. Om *stre* är början av ett ord, ligger nära att tänka på *streng* eller därmed besläktat ord. Då vi söker på vanligt sätt, finner vi i bredvidstående kolonn 2, två steg lägre, dvs. på avstånd 147 linjen *158 ngst,* vilket ger superlativen av *streng*. Detta kräver någon utfyllnad. Tanken går gärna till "strängaste tystlåtenhet" eller något dylikt. En möjlig komplettering ger kolonn 3 i *296 ess,* och då kan man gissa på stre-ngst-es/s-chwe-igen. Bokstavsföljden *chw* finns emellertid som början ingenstans i chiffret. Men man finner i kolonn 1 en karakteristisk beståndsdel i *27 weig,* som skulle kunna kombineras med *254 sch* (avstånd 151). Men då finns det ett s för mycket i *296 ess* och vi får ge upp denna kombination. I alla fall uppteckna vi resultatet:

| 11 | 158 | 296 | |
|---|---|---|---|
| stre | ngst | es\|s | ? |
| (147) | (138) | | |

och inför det tillsammans med den konstiga utbyggnaden bakåt, fastän med stor tvekan, på sin rad. Om det ligger något i tolkningen, är resultatet viktigt, ty det ger ytterligare två distanstal, 147 och 138, det senare har vi redan upptecknat som det första i *mira*-serien. Kan det vara identiskt samma 138, så att vi nu kan fortsätta med *mira*-serien? Det ser mycket illa ut, ty fortsättningen ges då av *163 zbit,* en meningslös ramsa *es/s-zbit.*

8) En kombination som lockar är *269 egr + 36 aphi* med avståndet 145. Redan från början gissar man på något som har med "telegrafi" (på tyska —graphie) att göra. Ett försök med den senast funna serien (*mira* är icke användbar) ger följande, som är värt sin egen rad:

| 358 | 115 | 269 | 36 | 191 | 338 | 98 |
|---|---|---|---|---|---|---|
| e\|un | d\|tel | egr | aphi | acho | kor | resp |
| (135) | (154) | (145) | (155) | (147) | (138) | |

Detta skulle ge ett förträffligt stöd åt den nyss ventilerade tolkningen; bara inte det förargliga *acho* fanns och om s stod i st. f. a, var saken ju klar. Men detta kan knappast vara en felaktig tillfällighet. För första gången inställer sig den misstanken, kan inte en bokstav vara felskriven? Vi skall i fortsättningen få flera anledningar att ställa den frågan. Den upptecknade tolkningen pekar avgjort på fortsättningen (korresp)-ondenz. Men inga av de funna avståndstalen hjälper fram till detta resultat. Ett snabbt öga kan emellertid lätt övertyga sig om att *onde* verkligen finns i 37, men på vilket avstånd? Siffran 317, överstigande allt vi hittills funnit. — Vi går vidare.

9) Bland *punkt*-kombinationerna finns ingen med distansen 145. Däremot förekommer andra nu funna avståndstal. Så t. ex. 294 ftp + 57 unkt, distans 141. Låt oss pröva *pqr*-serien härpå. Vi får:

| 294 | 57 | 203 | 354 |
|---|---|---|---|
| tt\|p | unkt | absa | tz\|a |
| (141) | (146) | (151) | |

Detta utfaller bra. Efter punkten kommer ny avdelning (Absatz), fortsättningen ligger i dunkel. Men kanske är nu något att hitta i andra riktningen. Vi måste gissa, med utgångspunkt från att *ft* utgör slutet av ett ord, t. ex. något på nft (Zukunft), aft (det finns många). Vid jämförelse mellan kolonnerna 2 och 3 fäster vi oss vid *154 scha,* som mycket bra passar ihop. Vad för *scha-ft* i så fall? Telegrammets natur gör det alls ej osannolikt, att det är fråga om Gesandt-schaft. Och verkligen, i kolonn 1, några steg högre upp, finner vi *4 andt*. Finns då möjligen även

*ges,* som resterar? Det gäller att komma ihåg att vi nu går bakåt, vi söker i kolonn 5 och finner där en linje (en enda) som passar, *247 ges*. Detta ger ett stort framsteg, vi får nu serien:

| 247 | 4 | 154 | 294 | 57 | 203 | 354 |
|---|---|---|---|---|---|---|
| ges | andt | scha | ft\|p | unkt | absa | tz\|a |
| | (135) | (150) | (140) | (141) | (146) | (151) |

och därmed är pqr-serien utbyggd med på en gång tre nya distanstal. Serien är nu:

135, 150, 140, 141, 146, 151.

10) Ett prov görs med utgångspunkt från *155 rkom* sammanställt med *302 mac*. Avståndet är 147. Den siffran finns i den förlängda *quit*-serien. Resultatet blir i det hela acceptabelt så när som på det obegripliga slutet:

| 322 | 74 | 233 | 378 | 155 | 302 | 62 |
|---|---|---|---|---|---|---|
| n\|ch | iffr | ebue | che | r\|kom | ma\|c | edes |
| | (135) | (154) | (145) | (155) | (147) | (138) |

Längre går det inte nu att komma härmed.

Så har det fortgått. Med utgångspunkt från andra förbindelsemöjliga orddelar har brottstycken av ytterligare 11 rader knåpats ihop. För att spara utrymme och då metoden nu tillräckligt demonstrerats, antecknar jag här blott, att den 21:a raden gav följande långa serie, som innehåller de flesta distanstalen:

| 87 | 229 | 364 | 136 | 276 | 39 |
|---|---|---|---|---|---|
| unbe | ding | t\|er | ford | erl | ich\|i |
| | (142) | (135) | (150) | (140) | (141) |

| 185 | 336 | 106 | 241 | 17 | |
|---|---|---|---|---|---|
| st\|un | d\|de | ren\|k | enn | tnia | |
| (146) | (151) | (148) | (135) | (154) | (145) |

| 162 | 317 | 86 | 224 |
|---|---|---|---|
| nahm | e\|du | rch\|u | nsur. |
| | (135) | (147) | (138) |



Här finns ett påtagligt bokstavsfel, kenntnisnahme, eljest klart.

Det återstår ett drygt arbete, för vilket här icke kan redogöras, för att inpassa återstående orddelar så, att alla raderna blir kompletta och kan förbindas med varandra. Det försvåras särskilt av den ymniga förekomsten av bokstavsfel. Men det lyckas och då visar sig att distanstalen bildar en cyklisk serie med samma tal under varann i alla rader, utom i ett kolumnmellanrum, språngstället, där växlande tal uppträder. I detta stadium ser chiffret ut som tablån på nästa uppslag utvisar.

Nu kan chiffret helt avläsas, bara man vet var början är. Det har avsändaren gett i handom genom att avsluta med ordet schluss, som återfinnes nära slutet av rad 6. Omedelbart därefter finner man början: bitte . . .

Lösningen blir alltså:

bitte saemtliche mit dem krieg zusammenhaengenden komma vor allem also die auf den goheimdienst und den dienst der vertreter unseres general- und admiralstabes klammer auf ueber die existens und das wirken dieser vertreter ist jetzt und fuer alle zukunft komma auch nach friedenschiuss komma strengstes stillschweigen zu bewahren klammer zu bezueglichen kemma in ihren haenden befindlichen und in zukunft noch an sie gelangenden papiere komma deren aufbewahrung nicht unbedingt erforderlich ist und deren kenntnianahme durch unsere noch immer nach dem besitze solchen papiere strebenden feinde fuer uns kompromittierend oder auch nur unangenehm sein koennte komma scfort sorgfaeltig und restlos verbrennen und hie asche zerschlagen punkt absatz es gehoeren hierzu bezonders listen registerabreehnungen quittungen kontobuecher und so weiter sowie auch die betreffende briefliche und telegraphiacho korrespondenz mit dieser gesandtschaft punkt absatz ausgenommen bleiben vorlaeufig noch die jetzt noch im benutzung befindlichen chiffrebuecher komma cedes und goheimachrift stichwcerter und anweisungen komma deren durchaus sicherer bewnhrung ganz besonders aufmerksamkeit zu schenken ist punkt absatz bitte die hinsichtlich der schon verhandenen papiere erfolgte ausfuehrung dieses auftrages schriftlich offen melden und so dann auch den vorliegenden scgenannten verbrennungserlass verbren-

| | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| rad 15 ← | 1 | 117 | 267 | 31 | 166 | 316 | 78 | 219 | 365 | 138 | 286 | 43 | 197 | 342 | 119 | 266 | 26 | 361 | 128 | 279 | rad 6 → |
| | | bezu | gna | hmen | hier | mit | alsp | qrbe | zei | chne | und | dess | euin | hal | tzus | amm | enmi | tdi | eser | bez | |
| | | (150) | (142) | (135) | (150) | (140) | (141) | (146) | (151) | (148) | (135) | (154) | (145) | (155) | (147) | (138) | (335) | (145) | (151) | | |
| rad 16 ← | 2 | 351 | 123 | 265 | 22 | 172 | 312 | 75 | 221 | 372 | 142 | 277 | 53 | 198 | 353 | 122 | 260 | 271 | 38 | 189 | rad 8 → |
| | | ond | ersl | ist | enre | gist | era | bree | hnun | gen | quit | tun | genk | onto | bue | cher | und | sow | eite | rsow | |
| | | (150) | (142) | (135) | (150) | (140) | (141) | (146) | (151) | (148) | (135) | (154) | (145) | (155) | (147) | (138) | (11) | (145) | (151) | | |
| rad 17 ← | 3 | 99 | 249 | 13 | 148 | 298 | 60 | 201 | 347 | 120 | 268 | 25 | 179 | 324 | 101 | 248 | 8 | 253 | 20 | 171 | rad 4 → |
| | | ohei | mdi | enst | undd | end | iens | tder | ver | trst | eru | nser | esge | ner | alun | dad | mira | lst | abes | klam | |
| | | (150) | (142) | (135) | (150) | (140) | (141) | (146) | (151) | (148) | (135) | (154) | (145) | (155) | (147) | (138) | (245) | (145) | (151) | | |
| rad 3 ← | 4 | 171 | 321 | 85 | 220 | 370 | 132 | 273 | 41 | 192 | 340 | 97 | 251 | 18 | 173 | 320 | 80 | 91 | 263 | 9 | rad 7 → |
| | | klam | mer | aufu | eber | die | exis | ten | zund | dasw | irk | ondi | eso | rver | tret | eri | stje | tztu | ndf | uera | |
| | | (150) | (142) | (135) | (150) | (140) | (141) | (146) | (151) | (148) | (135) | (154) | (145) | (155) | (147) | (138) | (11) | (145) | (151) | | |
| rad 14 ← | 5 | 225 | 375 | 139 | 274 | 46 | 186 | 327 | 95 | 246 | 16 | 151 | 305 | 72 | 227 | 374 | 134 | 1 | 146 | 297 | rad 15 → |
| | | auft | rag | esso | hri | ftli | chof | fen | meld | enu | ndso | dann | auc | hden | vorl | ieg | ende | nseg | enan | nte | |
| | | (150) | (142) | (135) | (150) | (140) | (141) | (146) | (151) | (148) | (135) | (154) | (145) | (155) | (147) | (138) | (245) | (145) | (151) | | |
| rad 1 ← | 6 | 279 | 51 | 193 | 328 | 100 | 240 | 3 | 149 | 300 | 70 | 205 | 359 | 126 | 281 | 50 | 188 | 73 | 218 | 369 | rad 17 → |
| | | bez | eieh | nung | sie | bitt | eim | geda | eeht | nis | beha | lten | wol | lenp | unk | tsch | luss | bitt | esae | mtl | |
| | | (150) | (142) | (135) | (150) | (140) | (141) | (146) | (151) | (148) | (135) | (154) | (145) | (155) | (147) | (138) | (263) | (145) | (151) | | |
| rad 4 ← | 7 | 9 | 159 | 301 | 58 | 208 | 348 | 111 | 257 | 30 | 178 | 313 | 89 | 234 | 11 | 158 | 296 | 109 | 254 | 27 | rad 11 → |
| | | uera | llez | uku | nftk | omma | auc | hnac | hfr | iede | nssc | hiu | ssko | mma | stre | ngst | ess | till | soh | weig | |
| | | (150) | (142) | (135) | (150) | (140) | (141) | (146) | (151) | (148) | (135) | (154) | (145) | (155) | (147) | (138) | (191) | (145) | (151) | | |
| rad 2 ← | 8 | 189 | 339 | 103 | 238 | 10 | 150 | 291 | 59 | 210 | 358 | 115 | 269 | 36 | 191 | 338 | 98 | 37 | 182 | 333 | rad 9 → |
| | | rsow | iea | uchd | ieb | etre | ffen | deb | rief | lich | eun | dtel | egr | aphi | acho | kor | resp | onde | nzmi | tdi | |
| | | (150) | (142) | (135) | (150) | (140) | (141) | (146) | (151) | (148) | (135) | (154) | (145) | (155) | (147) | (138) | (317) | (145) | (151) | | |
| rad 8 ← | 9 | 333 | 105 | 247 | 4 | 154 | 294 | 57 | 203 | 354 | 124 | 259 | 35 | 180 | 335 | 104 | 242 | 235 | 2 | 153 | rad 10 → |
| | | tdi | eser | ges | andt | scha | ftp | unkt | absa | tza | usge | nom | menb | leib | env | orla | euf | ign | ochd | ieje | |
| | | (150) | (142) | (135) | (150) | (140) | (141) | (146) | (151) | (148) | (135) | (154) | (145) | (155) | (147) | (138) | (371) | (145) | (151) | | |
| rad 9 ← | 10 | 153 | 303 | 67 | 202 | 352 | 114 | 255 | 23 | 174 | 322 | 79 | 233 | 378 | 155 | 302 | 62 | 289 | 56 | 207 | rad 19 → |
| | | ieje | tzt | noch | inbe | nut | zung | bef | indl | iohc | neh | iffr | ebue | che | rkom | mac | edes | und | gohe | imac | |
| | | (150) | (142) | (135) | (150) | (140) | (141) | (146) | (151) | (148) | (135) | (154) | (145) | (155) | (147) | (138) | (227) | (145) | (151) | | |

| | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| rad 7 ← | 11 | 27 | 177 | 319 | 46 | 226 | 366 | 129 | 275 | 48 | 196 | 331 | 107 | 252 | 29 | 176 | 314 | 343 | 110 | 261 | rad 20 → |
| | | weig | enzu | bew | ahre | nkla | mme | rzub | ezu | egli | ohen | kem | main | ihr | enha | ende | nbe | fin | dlic | hen | |
| | | (150) | (142) | (135) | (150) | (140) | (141) | (146) | (151) | (148) | (135) | (154) | (145) | (155) | (147) | (138) | (29) | (145) | (151) | | |
| rad 21 ← | 12 | 135 | 285 | 49 | 184 | 334 | 96 | 237 | 5 | 156 | 304 | 61 | 215 | 360 | 137 | 284 | 44 | 127 | 272 | 45 | rad 13 → |
| | | mern | ach | demb | esit | zes | oleh | erp | apie | rest | reb | ende | nfei | nde | fuer | uns | komp | romi | tti | eren | |
| | | (150) | (142) | (135) | (150) | (140) | (141) | (146) | (151) | (148) | (135) | (154) | (145) | (155) | (147) | (138) | (83) | (145) | (151) | | |
| rad 12 ← | 13 | 45 | 195 | 337 | 94 | 244 | 6 | 147 | 293 | 66 | 214 | 349 | 125 | 270 | 47 | 194 | 332 | 325 | 92 | 243 | rad 16 → |
| | | eren | dode | reu | chnu | run | ange | nehm | sei | nkoe | nnte | kom | masc | for | tsor | gfae | lti | gun | dres | tlo | |
| | | (150) | (142) | (135) | (150) | (140) | (141) | (146) | (151) | (148) | (135) | (154) | (145) | (155) | (147) | (138) | (371) | (145) | (151) | | |
| rad 18 ← | 14 | 81 | 231 | 373 | 130 | 280 | 42 | 183 | 329 | 102 | 250 | 7 | 161 | 306 | 83 | 230 | 368 | 307 | 74 | 225 | rad 5 → |
| | | ichi | nsic | htl | ichd | ers | chon | verh | and | enen | pap | iere | erfo | lgt | eaus | fueh | run | gdi | eses | auft | |
| | | (150) | (142) | (135) | (150) | (140) | (141) | (146) | (151) | (148) | (135) | (154) | (145) | (155) | (147) | (138) | (317) | (145) | (151) | | |
| rad 5 ← | 15 | 297 | 69 | 211 | 346 | 118 | 258 | 21 | 167 | 318 | 88 | 223 | 377 | 144 | 299 | 68 | 206 | 199 | 244 | 117 | rad 1 → |
| | | nte | nver | bren | nun | gser | las | sver | bren | nen | komm | adon | ich | imhi | nbl | ieka | ufku | enft | ige | bezu | |
| | | (150) | (142) | (135) | (150) | (140) | (141) | (146) | (151) | (148) | (135) | (154) | (145) | (155) | (147) | (138) | (371) | (145) | (151) | | |
| rad 13 ← | 16 | 243 | 15 | 187 | 292 | 64 | 204 | 345 | 113 | 264 | 34 | 169 | 323 | 90 | 245 | 14 | 152 | 55 | 200 | 351 | rad 2 → |
| | | tlo | sver | bren | nen | undh | ieas | che | zers | chl | agen | punk | tab | satz | esg | ehoe | renh | ierz | ubez | ond | |
| | | (150) | (142) | (135) | (150) | (140) | (141) | (146) | (151) | (148) | (135) | (154) | (145) | (155) | (147) | (138) | (281) | (145) | (151) | | |
| rad 6 ← | 17 | 369 | 141 | 283 | 40 | 190 | 330 | 93 | 239 | 12 | 160 | 295 | 71 | 216 | 371 | 140 | 278 | 181 | 326 | 99 | rad 3 → |
| | | mtl | iche | mit | demk | rieg | ezu | samm | enh | aeng | ende | nko | mmav | oral | lem | also | die | aufd | eng | ohei | |
| | | (150) | (142) | (135) | (150) | (140) | (141) | (146) | (151) | (148) | (135) | (154) | (145) | (155) | (147) | (138) | (281) | (145) | (151) | | |
| rad 19 ← | 18 | 63 | 213 | 355 | 112 | 264 | 24 | 165 | 311 | 84 | 232 | 367 | 143 | 288 | 65 | 212 | 350 | 163 | 308 | 81 | rad 14 → |
| | | ewnh | rung | gan | zbes | ond | erea | ufme | rks | amke | itzu | soh | enke | nis | tpun | ktab | sat | zbit | ted | iehi | |
| | | (150) | (142) | (135) | (150) | (140) | (141) | (146) | (151) | (148) | (135) | (154) | (145) | (155) | (147) | (138) | (191) | (145) | (151) | | |
| rad 10 ← | 19 | 207 | 357 | 121 | 256 | 28 | 168 | 309 | 77 | 228 | 376 | 133 | 287 | 54 | 209 | 356 | 116 | 145 | 290 | 63 | rad 18 → |
| | | imac | hri | ftst | ich | wcer | teru | nda | nwei | sung | enk | omma | der | endu | rcha | uss | iche | rera | ufb | ewnh | |
| | | (150) | (142) | (135) | (150) | (140) | (141) | (146) | (151) | (148) | (135) | (154) | (145) | (155) | (147) | (138) | (29) | (145) | (151) | | |
| rad 11 ← | 20 | 261 | 33 | 175 | 310 | 82 | 222 | 363 | 131 | 282 | 52 | 187 | 347 | 108 | 263 | 32 | 170 | 19 | 164 | 315 | rad 21 → |
| | | hen | undi | nzuk | unf | tnoc | hans | ieg | elan | gen | denp | apie | rek | omma | der | enau | fbew | ahru | ngni | eht | |
| | | (150) | (142) | (135) | (150) | (140) | (141) | (146) | (151) | (148) | (135) | (154) | (145) | (155) | (147) | (138) | (227) | (145) | (151) | | |
| rad 20 ← | 21 | 315 | 87 | 229 | 364 | 136 | 276 | 39 | 185 | 336 | 106 | 247 | 17 | 162 | 317 | 82 | 224 | 217 | 362 | 135 | rad 12 → |
| | | eht | unbe | ding | ter | ford | erl | ichi | stun | dde | renk | enn | tnia | nahm | edu | rchu | nsur | enoc | him | mern | |
| | | (150) | (142) | (135) | (150) | (140) | (141) | (146) | (151) | (148) | (135) | (154) | (145) | (155) | (147) | (138) | (371) | (145) | (151) | | |

nen komma don ich in hinblich auf kuenftige bezugnahmen hiermit als pqr bezeichne und dessen inhalt zusammen mit dieser bezeichnung sie bitte im gedaechtnis behalten wollen punkt sehluss.

Antalet bokstavsfel är som syns så stort, att det skulle varit utomordentligt svårt att utan efterforskande av metoden lista ut orddelarnas sammanhang.

Här skulle man nu kunna stanna. Men den intellektuella nyfikenheten driver en att fråga, efter vilken metod har detta transpositionschiffer utskrivits och lösts. Det förefaller ändå ganska otympligt, att därvid skulle ha använts denna besvärliga serie av stora distanstal. All anledning finns att anta att en vida enklare metod är i fråga, vilken resulterar i de höga avståndstalen. Om vi antar såsom skett redan i början, att det är fråga om transposition av en skrift utskriven i en rektangel, kan givetvis vid en förskjutning i både horisontell och vertikal led produkten ge höga avståndstal, även om själva förskjutningarna är betydligt enklare.

Denna del av uppgiften är väl så intressant. Men det blir för omständligt att ge en detaljredogörelse, hur man ur lösningen kan rekonstruera det använda tillvägagångssättet vid chiffreringen. Här må endast antydningar ges.

Eftersom distanstalsserien är avslutad med 18 intervaller, kan det nu sägas bestämt, att här använts rektangeln 18·21, såsom misstänktes.

För att uppspåra metoden — och förrän vi känner den, är uppgiften icke fullt löst — kan vi nu utgå från den stora första tablån över de 378 linjerna och skriva upp dem i en rektangel 18·21 genom att låta de 18 första linjerna med deras nummer komma i följd i en första kolumn och fortsätta tills vi fyllt 21 kolumner. Nu vet vi ju vilka linjer som hör ihop och borde kunna lista ut enligt vilken metod de särats från varandra. Omedelbart kan vi icke finna ut detta. Första orddelen *73 bitt* återfinns i kolumn V överst, dess fortsättning har vi i kolumn XIII rad 2, men sedan följer inte nästa ordbit i rad 3, vi hittar den först i rad 9, kolumn XXI. Och den därpå följande i kol. VIII, rad 15 osv.



För att få fram hurudant tillvägagångssättet har varit tar vi fram den tablå II, ur vilken lösningen kunde avläsas, och placerar in den riktiga texten i orddelar i den ordning de förekommer i den nyss ifyllda nya tablån, varvid kolumnerna betecknas med latinska och raderna med vanliga siffror, alldeles som vi nyss började med. Med ledning av tablå II håller vi emellertid i sär de olika raderna för att se efter, om någon bestämd enklare regelmässighet i linjernas följd och därmed i förskjutningen av deras ursprungliga ordning kan påvisas, som är lika för de olika raderna.

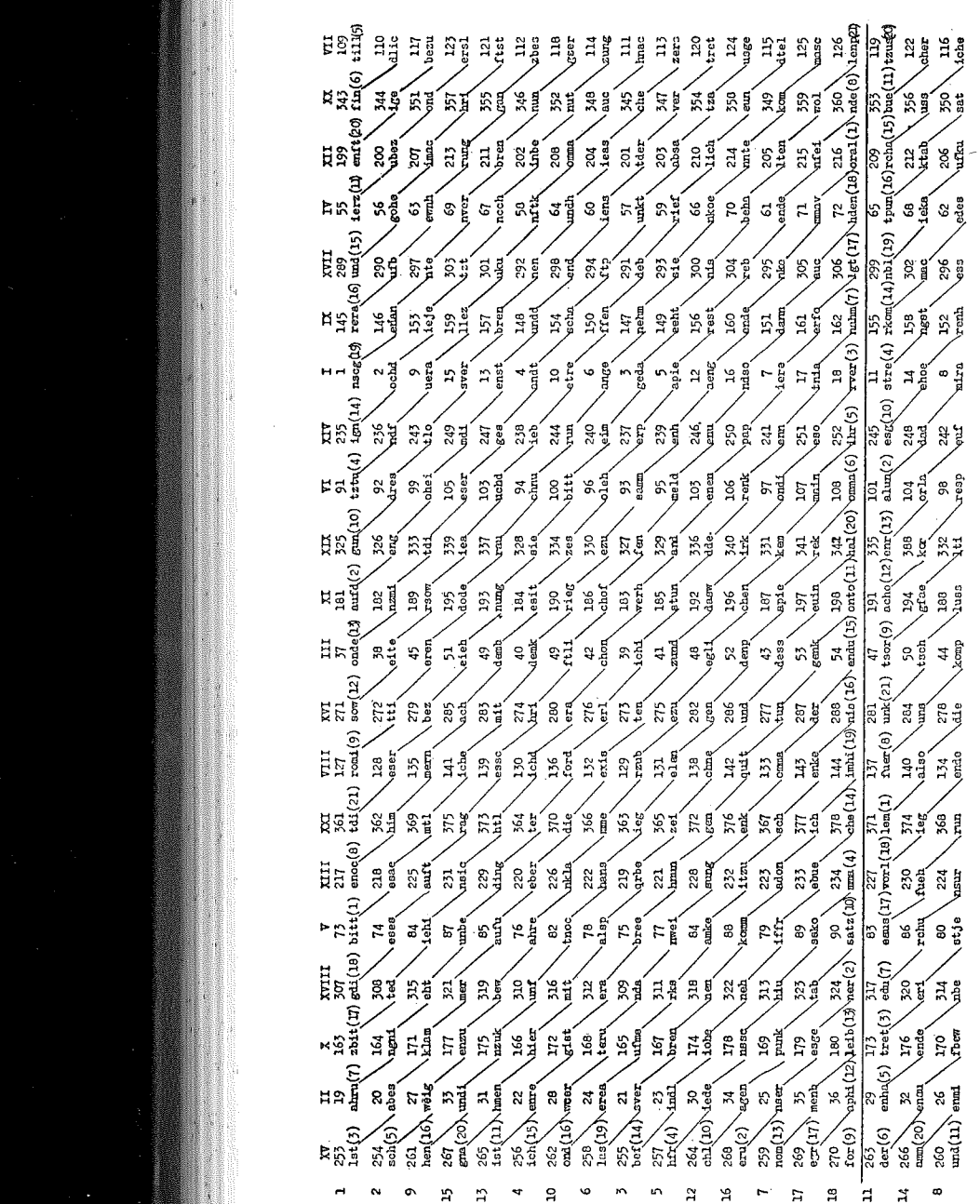
En detaljanalys av distanstalen utvisar nu, att de uppkommit genom att både rader och kolumner flyttats om efter ett visst system, som framgår av tablån på nästa sida.

Däri kan chiffret avläsas med början på rad 1 i kolumn V, där vi har *73 bitt*. Det gäller bara att läsa diagonalt. Men textföljden bryts då efter rad 18. Hela den understa avdelningen skall skjutas ett steg ytterligare, så att fortsättningen på diagonalen från kol. V *bitt* till kol. XII *oral* är att finna i kol. XXI. Nu kan varje diagonalrad komplett läsas. Vad som återstår är hopknytningen dem emellan. Var skall man fortsätta, sen man läst en diagonal till slut? Genom siffrorna 1, 2 etc. kan läsaren se hur det är gjort, men efter vilken regel?

Om detta är i själva verket mycket litet att säga, fast det på sin tid beredde den som skriver detta långvarigt grubbel. Alla försök att finna en bestämd regel slog slint. Till sist klarnade sammanhanget inför denna reflektion: en regel skall tjäna en bestämd uppgift, är regelmässigheten onödig motverkar den ändamålet, som är att chiffret skall vara läsbart av adressaten men helst icke av obehöriga. Här behövs i själva verket ingen regel alls. Med de kompletta diagonaltexterna är det så pass lätt för den som känner metoden att finna fortsättningen, att man kan placera fortsättningen på rad 1 i vilken kolumn som helst och fortsätta tills man fyllt hela rektangeln.

Detta förklarar de regellöst växlande distanstalen vid språngstället. Att vissa tal återkommer ett par gånger är ej underligt, då möjligheterna är begränsade.

Vi står alltså inför ett fall, där regellösheten är den bästa metoden. Och detta skulle gälla generellt, i fråga om tryggheten



mot forcering, om det ej motverkades av det praktiska behovet att göra chiffret läsbart — och relativt lätt läsbart — för den rätte mottagaren.

Den i förevarande chiffer använda metoden kan nu återges som följer:

1) En rektangel 18 rader·21 kolumner (räcker för 1134—1512 bokstäver i grupper om 4 eller 3).

2) Raderna omgrupperade: de två första orubbade, sedan ordningsföljd 9, 15, 13, 4, 10, 6, 3, 5, 12, 16, 7, 17, 18, 11, 14, 8.

3) Kolumnerna omgrupperade: II, V, VIII, XI, XIV, XVII, XX, dvs. var tredje orubbad, övriga förskjutna med 8, sålunda II, X, XVIII etc.

4) De tre sista radernas ordgrupper är förskjutna i sidled, så att närmast högre kolumn inträder, alltså under XV inträder efter linje 18 kolumn XVI.

5) Texten börjar i kolumn V och är skriven diagonalt med förskjutning en plats horisontalt och vertikalt hela rektangeln igenom. Valet av begynnelseordets kolumn i varje 18-grupp är godtyckligt.

6) Sedan texten utskrivits sålunda omgrupperas rektangeln med linjer och kolumner i normal ordningsföljd.

7) Chiffret utskrives genom att ta bokstäverna i vertikal ordningsföljd hela rektangeln igenom och uppdela dem i grupper om 10 bokstäver.

# 15. En genial experts kamp mot rutinen

Namnet *Bazeries* har flera gånger i det föregående mött läsaren. På sin tid var han antagligen Frankrikes mest geniale kryptolog. Fastän han som militär själv tillhörde skrået fick han föra en långvarig och för det mesta fåfäng kamp mot rutinen på området. Den vanliga historien om de militära topparnas konservatism och naturliga olust inför nydanande impulser.

Nu för tiden är chiffermaskiner allmänt i bruk, både i militär och diplomatisk tjänst. Så var det icke på Bazeries tid. Han hade 1891 presenterat krigsdepartementet en enkel kryptografisk apparat, som han konstruerat, lätt att sköta i fråga om både chiffrering och dechiffrering och som icke erfordrade hemlighållande av konstruktionen. Bazeries fick beröm vid demonstrationen men avslag i fråga om dess antagande.

Han säger själv i en skrift som han senare tillställde departementet, att han av samtal med generalstabsofficerare fått veta, att generalstaben icke ville veta av något annat system än ett sådant, som bara krävde penna och papper och som lätt kunde behållas i minne utan någon skriftlig anteckning. Bazeries beslöt att finna ut ett dylikt system och presenterade det några år senare, i en skrivelse av 1898 till samma departement.

Han bilägger för prövningen av systemet tre kryptogram — av vilka det är onödigt att här återge mer än ett, det kortaste — och säger, att han inte vill smickra sig med att ha tillverkat ett olösligt chiffer; men om dessa tre kryptogram motstår forcering, så är det kanske ändå den förgäves sökta lösningen av problemet.

Ur hans meddelande kan följande utdrag förtjäna återges: Systemet har den fördelen, att det lurar forceraren i fråga om den använda metoden. Vissa kryptografiska knep har använts för att dölja den. Dock är den så enkel, att den just därigenom bevarar sin hemlighet. Den är i användning lika snabb som nå-



got känt och använt system. Varje kryptogram är gjort med olika nyckel, en nyckel, som avsändaren väljer godtyckligt utan att i förväg meddela den åt mottagaren. Med ett ord, kryptogrammet bär sin nyckel med sig.

För övrigt, säger Bazeries, har jag inte sagt mitt sista ord, ty genom att modifiera denna metod, med bevarande av dess ursprungliga idé, kunde man kanske komma fram till att inte alls behöva frukta dess avslöjande. Men fullt så säker som i fråga om sin chifferapparat säger sig Bazeries icke vara.

Nummer 2 av de medsända proven innehöll detta:

40 grupper.

| | | | |
|---|---|---|---|
| D E G S C | L M L H Y | O S K S A | U Q O L Q |
| U A O S H | H Y S A E | M Q S H S | H Q O N D |
| S B Q C X | O L L U U | S L D S K | C C Q C S |
| B S N K S | X C T I O | N D D S K | Q T N A O |
| S C G X D | M N G Q D | L X L Y R | O M C H Q |
| Q D S S C | T M X O S | H Y T Q Y | S L C S K |
| O G X M S | H T B J N | E O L Q Q | S O A O J |
| X N R S Q | R S M S H | Q K Y C O | M R O S A |
| Y H X S K | O R Q C L | M S N O M | Q S C H X |
| R H S Y A | O S K B L | B A O S H | N D Q T T |

Sedan kommissionen för militär kryptografi granskat Bazeries memorandum utan att ha lyckats forcera de medsända kryptogrammen, anmodades han att meddela sin metod, vilket han gjorde i ett nytt memorandum, varur här meddelas det väsentliga, fastän med den ändringen, att tillämpning sker just på det nyss återgivna provchiffret.

Det gäller att chiffrera ett meddelande, som börjar:

le ministre des affaires étrangères à reçu l'avis officiel de la levée du blocus de Cuba.

Först väljs en nyckel för substitution. Nyckeln består av två godtyckligt valda bokstäver. Genom att använda deras ordningsnummer i alfabetet erhålles ett tal, som begagnas för substitutionsalfabetet.

Man väljer t. ex. DE = 45 = quarantecinq. Därav bildas en kvadrat om 25 bokstäver med alfabetet skrivet horisontellt. Vid

sidan därav bildar man en annan kvadrat av det normala alfabetet, skrivet vertikalt och gör substitutionen genom att byta ut varje bokstav i klartexten (representerad av den normala alfabetkvadraten) mot den i motsvarande ruta av substitutionskvadraten befintliga bokstaven.

Alltså: av q u a r(a)n t e c i(nq) bildas alfabetet Q, U, A, R, N, T, E, C, I, B, D, F, G, H, etc.

| Substitutionskvadrat | Normalt alfabet |
|---|---|
| Q U A R N | A F K P U |
| T E C I B | B G L Q V |
| D F G H J | C H M R X |
| K L M O P | D I N S Y |
| S V X Y Z | E J O T Z |

Första operationen vid chiffreringen blir då:

| | | | | | | |
|---|---|---|---|---|---|---|
| l e m | i n i | s t r | e d e | s a f | f a i | r e s |
| C S G | L M L | O Y H | S K S | O Q U | U Q L | H S O |
| e t r | a n g | e r e | s a r | e c u | l a v | i s o |
| S Y H | Q M E | S H S | O Q H | S D N | C Q B | L O X |
| f f i | c i e | l d e | l a l | e v e | e d u | b l o |
| U U L | D L S | C K S | C Q C | S B S | S K N | T C X |
| c u s | d e c | u b a | | | | |
| D N O | K S D | N T Q | | | | |

Ett sådant chiffer vore lätt att forcera. Men nu vidtar en ytterligare operation av transpositionsnatur. Kryptogrammet är uppdelat i trancher om tre bokstäver och i varje sådan grupp kastar man om bokstävernas ordning, så att kryptotexten blir G S C-L M L-H Y O-S K S-U Q O-L Q U-O S H-H Y S-E M Q osv.

Forceringen försvåras ytterligare genom insättande av ett godtyckligt antal nollor (bokstäver, som saknar betydelse och vid dechiffreringen stryks). De insätts enligt konventionen, att om första bokstaven i en tregrupp är vokal, så är denna en nolla. Då första bokstaven i substitutionskryptot, efter tranchernas omkastning, blir en vokal, är det följaktligen nödvändigt in-



sätta en extra vokal som nolla, annars bortfaller en bokstav ur klartexten.

De två bokstäver, som bildar nyckeln, sätts först och kryptotexten utfylls till jämna 5 grupper, vilket genom bruket av nollor blir mycket lätt. Det är bra att i texten ange antalet grupper, ty då kan dechiffrering ske, även om vid telegrafering någon bokstav skulle falla bort.

Vid dechiffreringen avskiljs först de två bokstäver, som bildar nyckeln, och substitutionsalfabetet uppställs. Den övriga texten uppdelas i trancher om tre bokstäver, med iakttagande av att de vokaler, som är nollor, stryks.

Alltså:

D E G S C L M L H Y O S K S (A) U Q O L Q U (A) O S H H Y S

Sen sker omkastning till
CSGLMLOYHSKSOQUUQLHSOSYH och dechiffrering sker med de två kvadraterna
l e m i n i s t r e d e s a f f a i r e s e t r etc. (resten är nu ytterst lätt att lösa).

Efter att ha lämnat denna redogörelse tillägger Bazeries:

Emellertid, med en liten modifikation hoppas jag åstadkomma, att metoden icke kan avslöjas. Den metoden skall jag senare göra bekant. Nu skulle det vara nyttigt, om dechiffrörerna försökte att med kännedom om min metod forcera det nya kryptogram, som följer härefter. Om det står emot forceringsförsök, så är det ett verkligt odechiffrerbart system för en var som icke besitter nyckeln.

Det nya kryptogrammet, som strax skall återges, består av 43 grupper och är försett med en vägledande rubrik: diversenotis, tagen ur en tidnings polisnyheter.

Icke heller detta kryptogram kunde generalstabens experter knäcka, trots upplysningarna. Men Bazeries erhöll så småningom följande besked från vederbörande: "Det har konstaterats, att metoden icke erbjöd erforderliga garantier i säkerhet för att kunna accepteras."

Hur kan detta förlikas, frågar till sist Bazeries, med det faktum att experterna icke kunde lösa det nya chiffret heller? Mystère!

Mysteriet stannade icke vid detta fiasko för 1890-talets franska rutinexpertis. Bazeries gjorde aldrig, av okänd anledning, bekant hur han tillverkat det sist presenterade chiffret. Från slutet på 90-talet har detta chiffer varit en knäckfråga för hela världens experter och amatörer på forcering. Dess motståndskraft räckte dryga 40 år. Först under senare år har en lösning presterats av en amerikan, som 1938 under signaturen *Candela* utgav en ytterst intressant publikation över detta Bazeries berömda olösta militärchiffer.

Historien om hur han gick till väga skall nu i sammandrag berättas.

Fait divers pris, dans un journal, aux nouvelles judiciaires.
43 groupes. L M P C X B R L S Q H F M H H C B H K X
C M S H Q B C U P M C C V F S A K F L M V G S R X
F C V B R S N X F T K K R R N D D Q G H Q X N L M
H F S V K R F S N I C R V K B A K V G N V C S G C
N R S M M C H P B K H F Q U C F U N X B V I G V T
K H K R O D N R N B M R K F G G N C M C K S V H N
G S G C U R K G N V K D D Q V R K O N B N L G Q T
S N K I C V U K B V I G F G C Z F H U C H S A M N
U C X F F V F C R H K B F G C X N H G Q

Ce cryptogramme, comme ceux précédemment établis, porte sa clef.

Detta var alltså problemet.

Candelas undersökning är intressant genom den utförliga redovisningen även av de misslyckade försök han gjorde att genomtränga slöjan, innan han kom in på rätt väg. Det skulle ta för stort utrymme att återge något därav, detta referat får begränsas till den rätta vägen.

Fastän en ganska enkel substitution ligger till grund för kryptogrammet, kommer man icke långt med vanliga frekvensmetoder. Den kan här vara förvriden av nollorna. Och om här också föreligger en transposition av okänd art — det erinras



om Bazeries karakteristik: en viss modifikation — fördärvas möjligheten att utnyttja bigramstatistiken i hög grad. En frekvensiakttagelse kan emellertid vem som helst göra. Det finns ingen bokstav i chiffret med en frekvens, som kan motsvara franskans e, som har ungefär dubbla frekvenstalet mot de i frekvens närmast kommande. All sannolikhet talar för att e har dubbel representation. Det högsta procenttalet har C med 10 %, därnäst K och N med drygt 8, vilket tillsammans skulle ge en god frekvenssiffra för e, men flera andra kombinationer är ur frekvenssynpunkt möjliga.

Candela redovisar en fullständig frekvensstatistik, som i fortsättningen utnyttjas, fastän den icke här återges, men han fortsätter icke sin analys på denna väg, utan han söker att direkt finna nyckeln till substitutionsalfabetet. Han utgår med stöd av Bazeries egen anvisning från att systemet är i sina grundidéer oförändrat, först en substitution med ett räkneord som nyckel — och nyckeln inlagd i chiffret — och sedan en transposition efter någon omkastningsmetod.

Han når sitt resultat genom en systematisk, skarpsinnig analys av de franska räkneorden. Man kan visserligen med dem bilda ett mycket stort antal olika nycklar. Men antalet är ingalunda obegränsat, och möjligheterna kan studeras gruppvis, varvid en utsållning undan för undan kan ske genom att studera de förekommande frekvenstalen. Han ställer upp ett schema över de franska räkneorden och konstaterar först, att deras begynnelsebokstäver kan vara

C, D, H, M, N, O, Q, S, T, V.

Obefintliga är däremot bokstäverna B, J, K, Y. Dessa måste följaktligen tillhöra den del av alfabetet, som följer efter nyckeln.

Vidare konstateras, att

V och G endast förekommer i vingt
F endast i neuf
H endast i huit
Z i onze, douze, treize, quatorze, quinze och seize.

De tänkbara nycklarna grupperar han i följande grundformer:

| | | |
|---|---|---|
| HUITC | CENT— | CINQE |
| M | D | M |
| QUARN | H | U |
| TO | I | DEUXC |
| TR | M | M |
| QUINZ | N | DIXHU |
| VINGT | O | ML |
| MILE— | Q | NE |
| C | R | SE |
| D | S | DOUZE |
| H | U | SIXCE |
| N | V | ML |
| O | NEUFC | SOIXA |
| Q | M | |
| S | ONZE— | |
| T | M | |
| U | SEIZ— | |
| V | M | |
| | SEPTC | |
| | M | |
| TREIZ | TROIS | |
| N— | | |
| NC | | |
| ND | | |
| NH | | |
| NO | | |
| NQ | | |
| NS | | |
| NU | | |

Han angriper dessa möjligheter med utgångspunkt från ett efter Bazeries system uppställt normalalfabet, där e har dubbel representation genom uteslutning av den i franskt språk obehövliga bokstaven K.



| | |
|---|---|
| AFEPU | . . . . . |
| BGLQV | . . . . . |
| CHMRX | . . . . . |
| DINSY | . . . . . |
| EJOTZ | . . . . . |

Hur skall den ännu tomma substitutionskvadraten kunna ifyllas? Det första e:t, längst ner till vänster, måste tillhöra den del av substitutionsalfabetet, som följer efter nyckeln. Med säkerhet skall i denna del finnas bokstäverna

B (5), J (0), K (8), Y (0)

med frekvenstal inom parentes. Uteslutna bland dem är J och Y, troligast är K.

Den substitutionsbokstav, som motsvarar normala A, bör finnas bland de kryptobokstäver, som har högsta frekvenstal.

A (8) = någon av C (10), K (8), N (8), F (7), V (7), H (7), R (7). Av dessa utesluts K, F, R, som icke kan börja ett franskt räkneord. De återstående undersöks i fråga om nyckelns första rad med användande av förut angivna alternativ och under jämförelse beträffande frekvens med normalalfabetets första rad.

| | | | |
|---|---|---|---|
| *N* | NEUFC | NEUFM | AFEPU |
| | 8 0 3 7 10 | 8 0 3 7 4 | 8 11 7/2 2 6 |

Granskningen visar, att N bör uteslutas.

| | | | |
|---|---|---|---|
| *V* | VINGT | AFEPU | |
| | 7 1 8 6 1 | 8 1 17/2 2 6 | |

Uteslutes likaså.

| | | | |
|---|---|---|---|
| *H* | HUITC | HUITM | AFEPU |
| | 7 3 1 1 10 | 7 3 1 1 4 | 8 11 7/2 2 6 |

Uteslutes.

| | | | |
|---|---|---|---|
| *C* | CENT | CINQ | AFEPU |
| | 10 0 8 1 | 10 1 8 3 | 8 11 7/2 2 . |

Endera av dessa passar. I så fall A=C och E=N.

Nu kan ifyllning av substitutionskvadraten börja. Om K antas vara det ena e:t, kan även J, som icke tillhör nyckeln, ges en bestämd position. Dessutom talar allt för att kvadratens sista bokstav är Y, icke Z. Ty i senare fallet vore Y (0)=T (7), vilket är osannolikt. Härmed skulle man få denna preliminära bild av de bägge kvadraterna:

| | |
|---|---|
| A F E P U | C . N . . |
| B G L Q V | . . . . . |
| C H M R X | . . . . . |
| D *I* *N* *S* Y | . . . . J |
| E J O T Z | K . . . Y |

Z tillhör därmed nyckeln. I normalkvadratens näst sista rad är de tre bokstäverna I (7), N (8), S (8) kursiverade, tre högfrekventa i rad. Vilka är deras motsvarigheter i substitutionskvadraten? De som föregår J kan vara

A B D E *F* *G* *H* I
3 4 2 0 7 6 7 1

Det syns uppenbart, att I N S motsvaras av F G H
7 8 8 7 6 7
Normalbokstaven B (4) tycks närmast representeras av B (4). A (3), som då skulle komma sist i kvadratens tredje rad, kan ej gärna företrädas av X (0). Härur skulle framgå, att både A och I tillhör nyckelordet. Emedan G ej finns i nyckeln, kan ej heller V höra dit, ty de finns bägge endast i vingt. Detta V skall inpassas mellan K och Y. Vid jämförelse med frekvenserna för J O T i normalkvadraten tycks troligast,

0 3 7

att T (7)=V (7). X måste också finnas i nyckeln. Kvadraterna ser härefter sålunda ut:



| | |
|---|---|
| A F E P U | C . N . . |
| B G L Q V | . . . . . |
| C H M R X | . . . . . |
| D I N S Y | B F G H J |
| E J O T Z | K . . V Y |

Nu kan slutas till, att varken H U I T, N E U F eller V I N G T kan finnas i nyckeln.

Däremot bör någon av z-formerna onze, douze, treize, quatorze, quinze, seize finnas där, vidare någon av x-formerna six, dix, soixante. Nyckeln bör även innehålla 14—15 bokstäver.

Nu kan man ägna sig åt de räkneord, som börjar med C E N T eller C I N Q. Vi provar först det senares tre former.

| | |
|---|---|
| A F E P U B | C I N Q E T |
| 6 0 | 0 1 |
| A F E P U B G L | C I N Q U A T E |
| 6 0 1 6 | 3 1 1 0 |
| A F E P U B G | C I N Q M L E |
| 6 0 1 | 4 2 0 |

Alla dessa alternativ osannolika, utesluts.

Återstår så de många nyckelord, som börjar med cent. Candelas uppställning ger någorlunda klart besked om den sannolikaste nyckeln vid frekvensjämförelse med normalalfabetet.

A F E P U B G L Q V C H M R X
6 0 1 6 1 1 3 0 2 6 0

C E N T
U M I L
3 4 1 2
D U X M I L
2 3 3 4 1 2
R O I S M L
7 1 1 6 4 2
Q U
3 3

I Q
1 3
S I X M L
6 1 3 4 2
S P M I
6 1 4 1
D
2
O
2
R I Z M L
7 1 0 4 2
R M I L
7 4 1 2
S I X M L
6 1 0 4 2
*S O I X A*
6 1 1 3 1
*U M L*
3 4 2
*D*
2
*R Z*
7 0

Av dessa finner Candela den sista kombinationen bäst fylla förutsättningarna. Nyckelordet skulle vara
C E N T S O I X A (N T E E T) U (N) M (I) L (L E) D (E U X C E N T T) R (E I) Z (E)=1 6 1 2 1 3.

Om nu detta tal översätts till bokstäver, får man P(16) L(12) M (13). Just dessa återfinner man i kryptots början, fastän i ordningsföljden LMP. Riktigheten av Candelas analys tycks härmed bekräftad.

Men chiffret är ju ingalunda löst med detta. Nu kan substitutionen avvecklas. Återstår att övervinna de svårigheter transpositionen och förekomsten av nollor innebär. För att översätta kryptobokstäverna till normalt alfabet används alltså



dessa bägge kvadrater, i vilka, för ytterligare belysning av överensstämmelsen, frekvenstalen är inskrivna under bokstäverna.

Substitutionskvadrat

| C | E | N | T | S |
|---|---|---|---|---|
| 10 | — | 8 | 1 | 6 |
| O | I | X | A | U |
| 1 | 2 | 4 | 1 | 3 |
| M | L | D | R | Z |
| 4 | 2 | 2 | 7 | 0 |
| B | F | G | H | J |
| 4 | 7 | 6 | 7 | — |
| K | P | Q | V | Y |
| 8 | 1 | 4 | 7 | — |

Normalkvadrat

| A | F | E | P | U |
|---|---|---|---|---|
| 8 | 1 | 17/2 | 2 | 6 |
| B | G | L | Q | V |
| — | 1 | 6 | 1 | 2 |
| C | H | M | R | X |
| 3 | — | 3 | 6 | — |
| D | I | N | S | Y |
| 4 | 6 | 7 | 7 | — |
| E | J | O | T | Z |
| 17/2 | — | 5 | 7 | — |

Om man nu med uteslutande av de tre nyckelbokstäverna söker återställa texten, erhåller man följande obegripliga ramsa:

(L M P) C X B R L S Q H F M H H C B H K X C M S H
a l d r h u o s i c s s a d s e l a c u s
Q B C U P M C C V F S A K F L N V G S R X F C V B R
o d a v j c a a t i u q e i h e t n u r l i a t d r
S N X F T K K R R N D D Q G H Q X N L M H F S V K
u e l i p e e r r e m m o n s o l e h c s i u t e
R F S N I C R V K B A K V G N V C S G C N R S M M
r i u e g a r t e d q e t n e t a u n a e r u c c
C H P B K H F Q U C F U N X R V I G V T K H K R O
a s j d e s i o v a i v e l r t g n t p e s e r b
D N R N B M R K F G G N C M C K S V H N G S G C U
m e r e d c r e i n n e a c a e u t s e n u n a v
R K G N V K D D Q V R K O N B N L G Q T S N K I C
r e n e t e m m o t r e b e d e h n o p u e e g a
V U K B V I G F G C Z F H U C H S A M N U C X F F
t v e d t g n i n a x i s v a s u q c e v a l i i
V F C R H K B F V C X N H G Q
t i a r s e d i t a l e s n o

Om nu denna besynnerliga text uppkommit genom en omkastning styckevis av texten, bör den se åtminstone betydligt naturligare ut, om man skriver om den baklänges. Det är icke att vänta en sammanhängande begriplig text, ifall omkastningen skett i brutna stycken, men orddelar och kanske hela ord bör då framträda. Det är vad som sker, som syns av nedanstående från slutet skrivna text, i vilken vissa påfallande textbitar *kursiverats*.

o n s|e l a t i|*d e s* r|a i t i *i l a v e c* q u s a v *s i x*
a n *i n g t d e* v v t *a g e e* u p o n h e d *e b e r t* o m
m e t e n e r v a n *u n e s t u e a c a e n* n i e r c d e r
*e m b r e|s e p t|n g t|r l e v i|a v o i s e d* j s *a c c u*
r e a n u a *t é n t e* q *d e t r a g e* u i r e t u i s c h
e l o s *n o m m e* r r e e p *i l e u r d t a i l r u n* t e h
i e *q u i* t a a c j v a d o s u c a l e s d a s s c i s o u
h r d *l a*

Man ser här genast ord och orddelar komma fram. Påfallande är, att man i mitten kan läsa *le vingt septembre* och i början *des relations*. På två ställen förekommer *age* i sammanställningar, ur vilka kan utläsas, på ena sidan *agé de vingt ans*, på andra sidan *agé de trente ans*. Tydligt är att omkastning skett, omväxlande för stycken om 3, 4 och 5 bokstäver. Slutet av baklängestexten (dvs. början av klartexten) tycks svårast att komma till rätta med.

Fortsätter man uppdelningen i textbitar efter samma system, som i des relations, dvs. 4, 5, 3, erhåller man:

Des r/elati/ons ecqu/iilav/ait ingt/sixan/sav upon/tagee /dev omme/ebert/hed unes/ervan/ten nier/acaen/tue

Läses dessa stycken i ordning bakifrån erhålles denna fullt sammanhängande text:

? — nier à caen tué une servante nommée berthe dupont agée de vingt six ans avec qui il avait des relations.

Det observeras att i denna del av chiffret tydligen icke använts några nollor. Om man nu går vidare på samma sätt bryts emellertid sammanhanget:

esop/rembre/cde



och sönderbryts därjämte den påfallande sammanställningen

sept/embre

Är den riktig, bör närmast före *embre* finnas en 3-bokstavsgrupp, *der*. Denna går förträffligt ihop med -nier, man erhåller sept embre der nier à caen etc. Då har i texten överhoppats ett c, kryptobokstaven M. Är den en nolla? Att vokaler icke som i Bazeries förut behandlade system här begagnas som nollor är klart redan därigenom att icke ett enda vokalmöte förekommer i hela kryptogrammet. Nu går det ett stycke vidare:

avoi/r le vi/ngt

Men det spårar strax ur:

urea/jsacc/sed

Här verkar särskilt bokstaven j främmande. Stryks den får man i stället

rean/saccu/sed

Och vidare:

de tr/enteq/uat uisc/uiret/age

Här blir fullt begripligt

age de trentequatre ans accusé d'avoir etc.

I så fall är även j = kryptobokstaven P ett nolltecken. Fortsättningen blir begriplig, om det närmast följande h stryks, då nämligen

erre/s nomm/elo tail/leurd/epi quit/tehie/r un

eller: — quitté hier un tailleur de pierres nommé lo-uis curiet agé etc.

Sålunda även h = L ett nolltecken.

Om i nästa återigen först ett j och sen ett h och ett c stryks, erhålles

ucal/vados/aac ourd/assis/esd/la

vilket ger: la cour d'assises du calvados a acquitté etc.

Härmed är hela texten dechiffrerad. Det visar sig då, att *Bazeries* i detta fall använt nollor ytterst sparsamt och som nolltecken valt just de bokstäver L, M, P som ingår i nyckeln.

*Candela*, som tydligen blivit starkt intresserad av de möjligheter *Bazeries* system inrymmer, har omarbetat det för

engelskt språkbruk, uppvisar hur de engelska räkneorden kan på motsvarande sätt användas, ger tips i fråga om forceringen av dylika kryptogram och anför en rad delvis svårknäckta exempel.

Systemet kan lika lätt apteras för svenska förhållanden. För att ge de läsare, som orkat följa framställningen ända hit, en nöt att knäcka till egen förnöjelse följer här nedan ett sådant exempel, vars lösning en systematiskt arbetande amatör bör kunna finna ut.

240 grupper.

| | | | | | |
|---|---|---|---|---|---|
| ELZYK | DHYKO | OXLAK | NBYEX | KZTSE | AXCKC |
| ICTRK | YKAKM | NLABK | EXLRI | LHCYK | ATTMY |
| TYYKQ | NYUTC | ZTBTL | BBKRQ | GKQRI | CKYCQ |
| YKREH | DKRGQ | YQOBK | KAIBK | LHTCB | NLBEM |
| XGBTR | QLKRK | RAKBT | AKYOZ | CLATX | CVEXB |
| BTTTB | CINXY | AKENN | KBYTE | AYMXK | CNUYT |
| YTRRQ | LBXLH | TDKXY | YONNT | ONNKY | YTKZY |
| TKGMT | NGBTH | KNCTB | KETNT | XEUVC | VETNZ |



# 16. Ett svenskt diplomatchiffers ändalykt

Det gäller ett äldre svenskt diplomatiskt chiffer, som sen länge icke är i bruk.

Vid regeringsskiftet våren 1936, då jag motsåg en helledig sommar, erbjöd jag mig att göra ett försök att forcera det diplomatiska chiffer som då var i bruk. En blå bok om bombardemanget av vår rödakorsambulans i Abessinien var förberedd. Dess innehåll var grundat på telegramdepescher mellan Rom och Stockholm. Mitt experiment avsåg att utröna i vad mån en dylik publikation kunde utnyttjas för att forcera den använda chiffercoden.

Till mitt förfogande ställdes ett litet antal chiffertelegram jämte för publicering avsedda blåbokstexter. Dessa kunde jag förutsätta vara i görligaste grad omskrivna i syfte att motstå forcering, då närmast från italiensk sida.

Min undersökning visade sig kräva ett drygt arbete. Att redogöra för den i dess helhet skulle kräva alltför stort utrymme. Det får räcka att summariskt illustrera hur jag gick till väga och vad resultatet blev.

Jag ger nu exempel på vad som kom fram ur min behandling av de två första telegram jag jämförde med motsvarande blåbokstexter. Det var telegrammen nr 43 och nr 1, vilka härmed presenteras. Därvid är i chiffren med v i samma chiffer förekommande repetitioner och med x i det andra chiffret iakttagna identiska chiffergrupper markerade. Därjämte är blåbokstexterna uppdelade i stycken om 6—7 ord till underlättande av jämförelsen.

Beträffande konstruktionen av chiffercoden iakttas omedelbart att samtliga chiffergrupper är 5-siffriga utan upprepning av någon siffra i varje grupp och att ingen siffergrupp har högre första siffra än 5. Det leder till slutsatsen att coden bör innehålla 2800 grupper.

*Telegram 43*

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 1 | 23914 | 02853 | 08921 | 26418 | 26879V | X26458V | 01642V |
| 2 | 23741 | 26517 | 27038 | 41935 | X04561V | 37091 | X29173V |
| 3 | 23048 | X39816 | X35046 | 06374V | 39507 | X30154V | 06374V |
| 4 | 18467 | 20973 | X19386V | 47205 | 17803V | X46980V | X37904 |
| 5 | 49570 | 12630 | 52467 | 08697V | 43965V | 06189 | 42069 |
| 6 | 24910 | X04628 | 42071 | 54120 | 50742 | 04376V | X18529V |
| 7 | X27680 | 06358 | 47058V | X34879V | = | 02358 | 39628 |
| 8 | X21783 | 41056 | 09486 | X04561V | 29371 | 43965V | 54092 |
| 9 | 01279 | X19386 | 32657V | 17402 | 38597 | X49086V | 30512 |
| 10 | 04376V | 16479V | 38740 | 18046 | 36129 | 12936 | 53780 |
| 11 | X49086V | 13976V | X02931V | X18529V | 13625 | 32854 | 49760 |
| 12 | 48076 | X51026 | 27983 | 06981 | 21830 | 18372 | 05293 |
| 13 | 19475V | 04981 | X49086V | 19378 | X29640V | 49316 | 49537V |
| 14 | 46531 | 01357 | 38279V | 31820 | 06374V | 48965V | = |
| 15 | 19475V | 40739 | 16082V | 43205 | X17924V | 12036 | 37914 |
| 16 | X26458V | 06239 | 50726 | 54281V | X34879V | 53490V | 15908 |
| 17 | X02931V | 42691 | 19530 | X29640V | 15368 | 49720V | 08569 |
| 18 | 13856 | 53962 | 07459 | 12605 | 32657V | 40892 | 40192 |
| 19 | 35209 | 24531 | X49086V | X54302 | 26357 | 43967 | 38927 |
| 20 | 18362 | X34879V | 15294 | 15432 | 48195 | 05981 | X29173V |
| 21 | 35029 | 19475V | 43015 | X15476 | 49537V | 02946V | 47058V |
| 22 | X34879 | = | 54017 | 49720V | X53940 | 54708 | 38194 |
| 23 | 26370 | 36950 | X23046 | 35607 | X19386V | 18306 | 17380 |
| 24 | 06243 | 41032 | 52349 | 28694 | 19087 | 51267 | X43071 |
| 25 | 31750 | 28017 | 08697V | 48563 | 29604 | 41638 | 29073 |
| 26 | 02637 | 16479V | 40359V | 48569 | X13950V | 17803V | X19386V |
| 27 | X17924V | 36912 | 09673 | 50236 | 19783 | 51246V | 49810 |
| 28 | 01642V | 23864 | 48653 | 12463V | 19732V | 38012 | 05748 |



| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 29 | 20195 | 36289 | X02374 | =X10476V | 19732V | 49037 | 54219 |
| 30 | X34879V | 43697 | 27584 | 10528 | X40359V | X40239 | 47205 |
| 31 | 04293 | X13807V | X46980V | 39685 | 16802 | 09457 | 24873 |
| 32 | X17924V | 28930 | X49086V | 06517 | 54281V | 13976V | X34879V |
| 33 | 40359V | 51097 | 36409 | 16748 | 04519 | 18754 | 28093 |
| 34 | 53760 | X13807V | 26879V | 10257 | X26749 | 54896 | 12463V |
| 35 | 17803V | 45289 | X31264 | X30154 | 51246V | 16082V | 08231 |
| 36 | X10476V | 38279V | X13950 | X08752 | = 06842 | 51693 | 02946V |
| 37 | 26907 | 41607 | 53490V | X10476V | 16873 | X13807V | 01396 |
| 38 | 16087 | 01936 | 41762 | 37925 | 48965V | 41026 | 35168 |
| 39 | 04736 | | | | | | |

*Telegram 43: text*

( 1) I dag blev jag uppkallad till / chefen
( 2) för den politiska avdelningen i *italienska* / utrikesministeriet för att mottaga ett muntligt / meddelande från *italienska* regeringen av
( 3) följande innehåll /:
( 4) Den verksamhet, som utövats av / de *svenska* officerarna i *Abessinien,* däribland främst / generalmajoren Virgin, bl. a. Virgins *anti-*
( 5) *italienska* / förklaringar i tidningspressen, det
( 6) å *svensk* sida / ådagalagda intresset för organiserandet av Röda / Korsverksamhet i *Abessinien*
( 7) samt framför allt / undertecknandet av ett vän-
( 8) skaps- och handels/avtal mellan *Sverige* och
( 9) *Abessinien,* vilket allt / från *italiensk* sida
(10) anses hava ett / medvetet sammanhang och en be-
(11) stämd tendens, har / hos *italienska* regeringen
(12) skapat ett / utpräglat / intryck av att *svenska* re-
(13) geringen är ovänligt / inställd till *Italien.*
(14) De åtgöranden / och anstalter från *svensk* sida,
(15) varom nu / är fråga, skulle visserligen var för
(16) sig icke givit intryck av att vara / direkt rik-
(17) tade mot *Italien* men fattas / nu såsom uttrycket
(18) för en allmän *anti-/italiensk* inställning.
(19) De kunna erhålla / mycket allvarliga följder för
(20) de *svensk-italienska* / förbindelserna.

*Telegram 1*

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 1 | 53608 | X04628 | 08653 | X04561V | X31264 | 48730 | 05372 |
| 2 | X39816 | X26517 | 13089 | X35046 | X29173 | X13950V | 38795 |
| 3 | 03124 | 16980 | 40798 | 37049 | 17428 | X37904 | X53940 |
| 4 | X54302 | 27860 | 45193 | X18529V | X21783 | 34719 | 03984 |
| 5 | 04987 | X34879V | 17956 | X43071V | 09168V | X34879V | 23716 |
| 6 | 43658 | 18640 | 39820V | X18529V | 50437 | X43071V | X40239 |
| 7 | X27680 | 09168V | 12043 | 26749 | 40936 | 08367 | 37201 |
| 8 | 48573 | 43981 | 39820V | 17483 | 18975 | 49581 | X23046 |
| 9 | 13746 | 31405 | X51026 | 27153 | X13807V | 10289 | 46591 |
| 10 | 40586 | 08367 | 35067 | X02931 | 31694V | 07432 | 41269 |
| 11 | 15074 | X13807V | X04561V | 18057 | 03549 | 49836 | X49086 |
| 12 | 40318 | 28467 | 31694V | X29640 | 19804 | X26458 | 20465 |
| | 51980 | 36450 | 32059 | 29864 | 10498 | X08752 | 13054 |
| 13 | X17924V | 29641 | 07298 | 52901 | 01354 | X19386 | X13950V |
| 14 | 15364 | 30952 | X46980V | 35089 | 51392 | 02451 | X10476 |
| 15 | 39471 | X30154 | 12953 | 16542 | 08739 | X46980V | 18349 |
| 16 | X17924V | X15476 | X02374 | 24691 | 02654 | X40359 | 07639 |
| 17 | X18529V | 09821 | | | | | |

*Telegram 1: text*

( 1)( 2) Enligt vad som meddelats mig av Su/vich *vilken*
( 3) jag på hans begäran idag / besökt har general Graziani telegraferat följande: /
( 4) I dagarna *hade italienska flygare,* såsom re-
( 5) pressalier / för att *abessinierna* stympat *italienska*
( 6) *fångar, bombarderat / abessinska trupper.* Bland an-
( 7) nat *hade* i / närheten *av* Cogoru *bombarderats* mi-
( 8) litärbefälhavaren / Ras Destas kvarter, vilket för-
( 9) lagts i / omedelbar närhet *av en svensk ambulans.* /
(10)(11) Det föreföll *som* om en bomb exploderat / invid denna *ambulans* och sårat Hylander. /
(12) Sedan jag framfört *svenska regeringens* anhållan
(13) om / införskaffande av upplysningar lovade Suvich
(14) att / omedelbart delgiva *mig* de ytterligare informa-



(15) tioner som / han kunde erhålla. Han bad *mig*
(16)(17) (att) *varna svenska regeringen* för att skänka / tilltro till meddelanden *från / abessinskt håll.* /

Om denna codelista ägde jag ingen kännedom. Jag antog att grupperna kunde betyda bokstäver, orddelar, hela ord, vissa brukliga fraser, möjligen grammatiska beteckningar. Huruvida coden innehåller ord från främmande språk var en öppen fråga. Utrymme synes finnas, närmast att gissa på är chiffergrupper ur dåtidens gängse diplomatspråk, franska.

Jämför man längden av resp. blåbokstext och telegram finner man en överraskande samstämmighet, 17—18 rader ifråga om telegram 1. Däremot är telegram 43 uppenbarligen längre än motsvarande klartext. Denna motsvaras av ungefär 22 rader i chiffret.

Den iakttagelsen kan i samband därmed göras att efter rad 22 följer 3 rader i chiffret nästan helt fria från repetitioner. Vad som därefter följer har antagligen icke medtagits i blåbokens text. Telegram 43 torde alltså vara återgivet i stympat skick.

Den naturliga metoden att vinna ett första insteg i chiffren är "det sannolika ordets" metod. Man tittar alltså efter chiffergrupper för Sverige /svensk/, Italien /italiensk/ och Abessinien /abessinsk/.

Chiffergrupper med 3 eller fler repetitioner är

i telegram 43

06374/3/ 10476/3/ 13807/3/ 17803/3/ 17924/3/
19386/4/ 19475/3/ 34879/6/ 40359/3/ 49086/5/

i telegram 1

18529/3/

Den klaraste signalen för ett sannolikt ord ger grupp 18529 näst sist i tel. 1 och näst sist också i klartexten. Gruppen bör betyda Abessinien eller adjektivformen abessinsk. Gruppens förekomst på rad 6 med motsvarighet i del 6 av klartexten styrker tolkningen och ger på köpet 2 ytterligare chiffertolkningar

39820 18529 50437
bombarderat abessinska trupper

Förekomsten på chiffrets rad 4 passar inte lika bra, i blåbokens text finner man Abessinien först i del 5, här kan en omstuvning av ordföljden ha ägt rum.

I tel. 43 har grupp 18529 två förekomster. Den på chiffrets rad 4 synes passa in på textens motsvarande del. Medan den på rad 11 i chiffret får i klartexten plats först i del 12, vilket tyder på en transkription med omkastad ordföljd.

Jag provade också från början, om någon av grupperna med de flesta repetitionerna kunde betyda Sverige, resp. svensk. Dessa grupper, 34879 och 49086, hade emellertid en sådan placering i chiffret, att resultatet vid jämförelsen med blåboken utföll negativt.

Men i det sammanhanget uppmärksammades en dubbeluppрepning i chiffret, rad 7 och 21—22 som hade sin direkta motsvarighet i klartexten del 6—7 och del 22. Detta medförde tolkningen

| 47058 | 34876 |
|---|---|
| anti - | italiensk |

Då gruppen 34879 dessutom i förra delen av tel. 43 förekommer i rad 16 och 20 ger detta

| 54281 | 34879 | | 18362 | 34879 |
|---|---|---|---|---|
| till | Italien | och | mot | Italien |

Och vidare, i tel. 1, rad 5, två förekomster. Klartexten har italiensk i del 4 och i del 5. Med viss omkastning av ordföljden synes ett par ytterligare tolkningar befogade

| 34879 | 17956 | 34879 | 23716 |
|---|---|---|---|
| italienska | fångar | italienska | flygare |

Men grupp, eller grupper, för Sverige /svensk/ saknas alltjämt. Då ingen av de undersökta visat sig passa är det antagligt, att codelistan innehåller varianter.

Klartexten har Sverige och Abessinien mycket nära varann i del 11 i frasen "undertecknande av ett vänskaps- och handelsavtal mellan Sverige och Abessinien . . ."



Gruppen närmast före 18529 /Abessinien/ är 02931, som i tel. 43 finns upprepad rad 17. I motsvarande textdel återfinnes frasen "å svensk sida". Samma grupp finns i tel. 1 rad 10, som har motsvarighet i slutet av blåbokens textdel 9 "en svensk ambulans". Vilket bör räcka för tolkningen i tel. 43

| 13976 | 02931 | 18529 |
|---|---|---|
| det | svensk- | abessinska |

vilket måste medföra att "vänskaps- och handelsavtalet" i chiffret följer efter, inte som i klartexten före "Sverige och Abessinien". Detta leder till en mer hypotetisk tolkning av närmast följande grupper

| 13625 | 32854 | 49760 | 48076 |
|---|---|---|---|
| vänskaps- | och | handels- | avtalet |

I tel. 1 ger 02931 tvenne tolkningar

| | | | |
|---|---|---|---|
| rad 10 | 35067 | 02931 | 31694 |
| | en | svensk | ambulans |

| | | |
|---|---|---|
| rad 12 | 28467 | 31694 |
| | denna | ambulans |

Det måste finnas någon variant för Sverige /svensk/ eftersom klartexten innehåller svensk på ett par ställen, där 02931 icke förekommer.

I tel. 43 har blåboken frasen "de svenska officerarna i Abessinien" i stycke 6 och "å svensk sida" i textdel 7. Den repetitionsgrupp som då kommer närmast i fråga är 43965 på rad 5, resp. 8. Detta ger följande tolkningsmöjligheter

| | | | | |
|---|---|---|---|---|
| rad 5 | 08697 | 43965 | 06189 | 42069 |
| | de | svenska | officer- | arnas |

| | | | |
|---|---|---|---|
| rad 8 | 29371 | 43965 | 54092 |
| | å | svensk | sida |

Men i tel. 1 finner man på två ställen, textdel 12 och 16, "svenska regeringen". Där passar ingen av de bägge funna grupperna för "svensk". Det kan ju vara en enda grupp som just betyder "svenska regeringen". Det passar utmärkt med grupp 17924 i början av rad 17 och kan vara acceptabelt i början av rad 14.

Tolkningar:

| | | |
|---|---|---|
| rad 14 | 17924 | 29641 |
| | Sv. regeringens | anhållan |
| rad 16—17 | 18349 | 17924 |
| | varna | Sv. regeringen |

Gruppen finns också i tel. 43, rad 15 varmed jämföres textdel 15. Det ger

| | | |
|---|---|---|
| 16082 | 43205 | 17924 |
| intryck | att | sv. regeringen |

Ordet "bombarderat" förekommer i blåbokstexten till tel. 1 i textdel 5 och 6. På första stället som nämnts omedelbart före "abessinska trupper".

Gruppen 39820 återkommer först i rad 8, vilket tyder på en omskrivning. En sannolik tolkning framkommer då:

| | | | | |
|---|---|---|---|---|
| 26749 | 40936 | 08367 | ... | 39820 |
| i | närhet | av | | bombarderat |

Gruppen 40936 återfinnes på rad 10, vilket mycket väl kan ge tolkningen

| | | | |
|---|---|---|---|
| 10289 | 46591 | 40586 | 08367 |
| i | omedelbar | närhet | av |

I delstyckena 13—14 och motsvarande rader av chiffer 43 får man ytterligare fram följande:



| | | | | |
|---|---|---|---|---|
| 19475 | 04981 | 49086 | 19378 | 29640 |
| ett | medvetet | ? | sammanhang | och |

| | | | |
|---|---|---|---|
| samt | 49537 | 46531 | 01357 |
| | en | bestämd | tendens |

Dessutom i rad och stycke 16—17 samma telegram

| | | | | | |
|---|---|---|---|---|---|
| 15908 | 02931 | 42691 | 19530 | 29640 | 15368 |
| de | svenska | åtgöranden | | och | anstalter |

Och vidare tel. 43 rad 21

| | | |
|---|---|---|
| 19475 | 43015 | 15476 |
| ett | uttryck | för |

Detta bör ge en ungefärlig föreställning om tillvägagångssättet. Den ytterligare analysen av dessa båda telegram avslöjade en del små ord såsom "mig", "som", "hade" m. m.

Dessutom kunde avslöjas att vissa grupper angav grammatiska former, t. ex. 43071 = pluralis, 13807 = imperfektum. Den så ymnigt förekommande grupp 49086 kunde aldrig ges någon säker tolkning och betraktades som en nolla.

I det skick den jämförande analysen av de bägge förut undersökta telegrammen erhållits återges de härefter. Resultat: i tel. 43 drygt tredjedelen av chiffergrupperna tolkade, i tel. 1 något mer, ungefär 40 %.

*Telegram 43*

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 1 | 23914 | 02853 | 08921 | 26418 | 26879 | 26458 | 01642 |
| 2 | 23741 | 26517 | 27038 | 41935 | 04561 *som* | 37091 | 29173 |
| 3 | 23048 | 39816 | 35046 | 06374 | 39507 | 30154 | 06374 |
| 4 | 18467 | 20973 | 19386 *s* | 47205 | 17803 | 46980 *mig* | 37904 |
| 5 | 49570 | 12630 | 52467 | 08697 *de* | 43965 *svenska* | 06189 *officer* | 42069 *arnas* |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 6 | 24910 | 04628 | 42071 | 54120 | 50742 | 04376 | 18529 *abessin* |
| 7 | 27680 | 06358 | 47058 *anti-* | 34879 *italiensk* | = | 02358 | 39628 |
| 8 | 21783 | 41056 | 09486 | 04561 *som* | 29371 *å* | 43965 *svensk* | 54092 *sida* |
| 9 | 01279 | 19386 *s* | 32657 *för* | 17402 | 38597 | 49086 *0* | 30512 |
| 10 | 04376 | 16479 | 38740 | 18046 | 36129 | 12936 | 53780 |
| 11 | 49086 *0* | 13976 *det* | 02931 *svensk-* | 18529 *italienska* | 13625 *vänskaps* | 32854 *och* | 49760 *handels* |
| 12 | 48076 *avtalet* | 51026 | 27983 | 06981 | 21830 | 18372 | 05293 |
| 13 | 19475 *ett* | 04981 *medvetet* | 49086 *0* | 19378 *sammanhang* | 29640 *och* | 49316 *0* | 49537 *en* |
| 14 | 46531 *bestämd* | 01357 *tendens* | 38279 | 31820 | 06374 | 48965 | = |
| 15 | 19475 *ett* | 40739 *utpräglat* | 16082 *intryck* | 43205 *att* | 17924 *sv. regeringen* | 12036 | 37914 |
| 16 | 26458 | 06239 | 50726 | 54281 *till* | 34879 *Italien* | 53490 *punkt* | 15908 *De* |
| 17 | 02931 *svenska* | 42691 *åtgöranden* | 19530 | 29640 *och* | 15368 *anstalter* | 49720 | 08569 |
| 18 | 13856 | 53962 | 07459 | 12605 | 32657 | 40892 | 40192 |
| 19 | 35209 | 24531 | 49086 *0* | 54302 | 26357 | 43967 | 38927 |
| 20 | 18362 *mot* | 34879 *Italien* | 15294 | 15432 | 48195 | 05981 | 29173 |
| 21 | 35029 | 19475 *ett* | 43015 *uttryck* | 15476 *för* | 49537 *en* | 02946 *allmän* | 47058 *anti-* |
| 22 | 34879 *italiensk* | = | 54017 *inställ-* | 49720 *ning* | 53940 | 54708 | 38194 |

| | | | | | | |
|---|---|---|---|---|---|---|
| 26370 | 36950 | 23046 | 35607 | 19386 | 18306 | 17380 |
| 06243 | 41032 | 52349 | 28694 | 19087 | 51267 | 43071 |
| 31750 | 28017 | 08697 | 48563 | 29604 | 41638 | 29073 |
| 02637 | 16479 | 40359 | 48569 | 13950 | 17803 | 19386 |
| 17924 | 36912 | 09673 | 50236 | 19783 | 51246 | 49810 |
| 01642 | 23864 | 48653 | 12463 | 19732 | 38012 | 05748 |
| 20195 | 36289 | 02374 | = 10476 | 19732 | 49037 | 54219 |
| 34879 | 43697 | 27584 | 10528 | 40359 | 40239 | 47205 |
| 04293 | 13807 | 46980 | 39685 | 16802 | 09457 | 24873 |
| 17924 | 28930 | 49086 | 06517 | 54281 | 13976 | 34879 |
| 40359 | 51097 | 36409 | 16748 | 04519 | 18754 | 28093 |



| | | | | | | |
|---|---|---|---|---|---|---|
| 53760 | 13807 | 26879 | 10257 | 26749 | 54896 | 12463 |
| 17803 | 45289 | 31264 | 30154 | 51246 | 16082 | 08231 |
| 10476 | 38279 | 13950 | 08752 | = 06842 | 51693 | 02946 |
| 26907 | 41607 | 53490 | 10476 | 16873 | 13807 | 01396 |
| 16087 | 01936 | 41762 | 37925 | 48965 | 41026 | 35168 |
| 04736 | | | | | | |

## *Telegram 1*

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 1 | 53608 | 04628 | 08653 | 04561 *som* | 31264 | 48730 | 05372 |
| 2 | 39816 | 26517 | 13089 | 35046 | 29173 | 13950 | 38795 |
| 3 | 03124 | 16980 | 40798 | 37049 | 17428 | 37904 | 53940 |
| 4 | 54302 | 27860 | 45193 | 18529 *abessin.* | 21783 | 34719 | 03984 |
| 5 | 04987 | 34879 *italienska* | 17956 *fångar* | 43071 *(plur.)* | 09168 *hade* | 34879 *italienska* | 23716 *flygare* |
| 6 | 43658 *i* | 18640 *dagarna* | 39820 *bombarderat* | 18529 *abessinska* | 50437 *trupper* | 43071 *(plur.)* | 40239 *punkt* |
| 7 | 27680 *Bl. a.* | 09168 *hade* | 12043 | 26749 *i* | 40936 *närhet* | 08367 *av* | 37201 |
| 8 | 48573 | 43981 | 39820 *bombarderat* | 17483 | 18975 | 49581 | 23046 |
| 9 | 13746 | 31405 | 51026 | 27153 | 13807 | 10289 *i* | 46591 *omedelbar* |
| 10 | 40586 *närhet* | 08367 *av* | 35067 *en* | 02931 *svensk* | 31694 *ambulans* | 07432 *(punkt)* | 41269 *Det* |
| 11 | 15074 *föreföll* | 13807 *(imperf.)* | 04561 *som* | 18057 *en* | 03549 | 49836 | 49086 |
| 12 | 40318 | 28467 *denna* | 31694 *ambulans* | 29640 *och* | 19804 | 26458 | 20465 |
| 13 | 51980 | 36450 | 32059 | 29864 | 10498 | 08752 | 13054 |
| 14 | 17924 *sv. regeringens* | 29641 *anhållan* | 07298 | 52901 | 01354 | 19386 | 13950 |
| 15 | 15364 | 30952 *delgiva* | 46980 *mig* | 35089 *de* | 51392 | 02451 | 10476 |
| 16 | 39471 | 30154 | 12953 *(punkt)* | 16542 *Han* | 08739 *bad* | 46980 *mig* | 18349 *varna* |
| 17 | 17924 *sv. regeringen* | 15476 *för* | 02374 | 24691 | 02654 | 40359 *meddelande* | 07639 *från* |
| 18 | 18529 *abessinskt* | 09821 *håll* | | | | | |

Till mitt förfogande hade ställts några ytterligare chiffertelegram. Med kontrollanalys tack vare dem kunde jag i det närmaste avsluta detta mitt semesterarbete innan jag kom tillbaka till Stockholm. Där begärde jag hos UD att för kontroll få ett chiffer som motsvarade ett visst meddelande i blåboken. Det jag fick visade sig emellertid vid min granskning ha ett helt annat innehåll. Då jag meddelade detta till vederbörande fick man i UD klart för sig, att det inte var mycket bevänt med deras "hemliga skrift". Coden togs också ur allmänt bruk.

Jag får avstå från redogörelse för det stort utrymme krävande avslutningsarbetet med ytterligare tolkningar och diverse korrektioner av feluppfattade grupper. Mitt slutresultat inlämnades till UD i september 1936. Det presenteras härefter i vad avser de båda telegrammen 43 och 1.

*Telegram 43*

| | | | | | | |
|---|---|---|---|---|---|---|
| 23914<br>*Chefen* | 02853<br>*för* | 08921<br>*polit.avdeln.* | 26418<br>*utrikes-<br>dept* | 26879<br>*Bu-* | 26458<br>*t-* | 01642<br>*ti* |
| 23741<br>*har* | 26517<br>*i dag* | 27038<br>*vid* | 41935<br>*samtal* | 04561<br>*som* | 37091<br>*skedde* | 29173<br>*(imperf.)* |
| 23048<br>*på* | 39816<br>*begäran* | 35046<br>*meddelat* | 06374<br>*(supinum)* | 39507<br>*han* | 30154<br>*erhållit* | 06374<br>*(sup.)* |
| 18467<br>*sin* | 20973<br>*regering-* | 19386<br>*s* | 47205<br>*uppdrag* | 17803<br>*lämna* | 46980<br>*mig* | 37904<br>*följande* |
| 49570<br>*muntliga* | 12630<br>*meddelande* | 52467<br>*(kolon)* | 08697<br>*De* | 43965<br>*svenska* | 06189<br>*officer-* | 42069<br>*arnas* |
| 24910<br>*främst* | 04628<br>*Vi-* | 42071<br>*rg-* | 54120<br>*in-* | 50742<br>*s* | 04376<br>*verksamhet* | 18529<br>*Abessinien* |
| 27680<br>*bl. a.* | 06358<br>*dennes* | 47058<br>*anti-* | 34879<br>*italienska* | = | 02358<br>*tidnings-* | 39628<br>*uttalanden* |
| 21783<br>*(plur.)* | 41056<br>*det* | 09486<br>*intresse* | 04561<br>*som* | 29371<br>*å* | 43965<br>*svensk* | 54092<br>*sida* |
| 01279<br>*ådagalagt-* | 19386<br>*s* | 32657<br>*för* | 17402<br>*organiserande* | 38597<br>*av* | 49086<br>*0* | 30512<br>*rödakors-* |
| 04376<br>*verksamhet* | 16479<br>*detta* | 38740<br>*land* | 18046<br>*och* | 36129<br>*framför allt* | 12936<br>*under-<br>teckn-* | 53780<br>*andet* |



| | | | | | | |
|---|---|---|---|---|---|---|
| 49086<br>*0* | 13976<br>*det* | 02931<br>*svensk-* | 18529<br>*abessinska* | 13625<br>*vänskaps* | 32854<br>*och* | 49760<br>*handels-* |
| 48076<br>*avtalet* | 51026<br>*vilket* | 27983<br>*allt* | 06981<br>*här* | 21830<br>*ansågs* | 18372<br>*(imperf.)* | 05293<br>*hava* |
| 19475<br>*ett* | 04981<br>*medvetet* | 49086<br>*0* | 19378<br>*sammanhang* | 29640<br>*och* | 49316<br>*0* | 49537<br>*en* |
| 46531<br>*bestämd* | 01357<br>*tendens* | 38279<br>*hade* | 31820<br>*givit* | 06374<br>*(sup.)* | 48965<br>*it. regeringen* | = |
| 19475<br>*ett* | 40739<br>*klart* | 16082<br>*intryck* | 43205<br>*att* | 17924<br>*sv. regeringen* | 12036<br>*vore* | 37914<br>*ovänlig-* |
| 26458<br>*-t* | 06239<br>*inställ-* | 50726<br>*d* | 54281<br>*till* | 34879<br>*Italien* | 53490<br>*(punkt)* | 15908<br>*Dessa* |
| 02931<br>*svenska* | 42691<br>*åtgöranden* | 19530<br>*(plur.)* | 29640<br>*och* | 15368<br>*föranstalt-* | 49720<br>*ningar* | 08569<br>*(plur.)* |
| 13856<br>*vilka* | 53962<br>*tag-* | 07459<br>*na* | 12605<br>*var* | 32657<br>*för* | 40892<br>*sig* | 40192<br>*icke* |
| 35209<br>*skulle* | 24531<br>*fattats* | 49086<br>*0* | 54302<br>*såsom* | 26357<br>*direkt* | 43967<br>*rikta-* | 38927<br>*de* |
| 18362<br>*mot* | 34879<br>*Italien* | 15294<br>*men* | 15432<br>*som* | 48195<br>*nu* | 05981<br>*betraktades* | 29173<br>*(imperf.)* |
| 35029<br>*såsom* | 19475<br>*ett* | 43015<br>*uttryck* | 15476<br>*för* | 49537<br>*en* | 02946<br>*allmän* | 47058<br>*anti-* |
| 34879<br>*italiensk* | = | 54017<br>*inställ-* | 49720<br>*ning* | 53940<br>*(cit.tn)* | 54708 | 38194 |
| 26370 | 36950 | 23046 | 35607 | 19386 | 18306 | 17380 |
| 06243 | 41032 | 52349 | 28694 | 19087 | 51267 | 43071 |
| 31750 | 28017 | 08697 | 48563 | 29604 | 41638<br>*På* | 29073<br>*förfrågan* |
| 02637<br>*huruvida* | 16479<br>*detta* | 40359<br>*meddelande* | 48569<br>*komme* | 13950<br>*att* | 17803<br>*lämna-* | 19386<br>*s* |
| 17924<br>*sv. regeringen* | 36912<br>*även* | 09673<br>*genom* | 50236<br>*beskickningen<br>i Sthlm* | 19783<br>*förklarade* | 51246<br>*(imperf.)* | 49810<br>*But-* |
| 01642<br>*-ti* | 23864<br>*att* | 48653<br>*så* | 12463<br>*icke* | 19732<br>*skulle* | 38012<br>*bli* | 05748<br>*fall-* |
| 20195<br>*-et* | 36289<br>*men* | 02374<br>*att* | = 10476<br>*han* | 19732<br>*skulle* | 49037<br>*under-* | 54219<br>*rätta* |
| 34879<br>*italienska* | 43697<br>*beskick-<br>ningen* | 27584<br>*om* | 10528<br>*ovanstående* | 40359<br>*medde-<br>lande* | 40239<br>*(punkt)* | 47205<br>*Jag* |

| | | | | | | |
|---|---|---|---|---|---|---|
| 04293 | 13807 | 46980 | 39685 | 16802 | 09457 | 24873 |
| *förbeföll* | *(imperf.)* | *mig* | *att* | *efter* | *instruktion* | *från* |
| 17924 | 28930 | 49086 | 06517 | 54281 | 13976 | 34879 |
| *sv. regeringen* | *eventuellt* | *0* | *återkomma* | *till* | *det* | *italienska* |
| 40359 | 51097 | 36409 | 16748 | 04519 | 18754 | 28093 |
| *meddelandet* | *(punkt)* | *Någon* | *närmare* | *preciser-* | *ing* | *därav* |
| 53760 | 13807 | 26879 | 10257 | 26749 | 54896 | 12463 |
| *önskade* | *(imperf.)* | *Bu-* | *tt-* | *i* | *nu* | *icke* |
| 17803 | 45289 | 31264 | 30154 | 51246 | 16082 | 08231 |
| *lämna* | *(punkt)* | *Jag* | *erhöll* | *(imperf.)* | *intryck* | *att* |
| 10476 | 38279 | 13950 | 08752 = | 06842 | 51693 | 02946 |
| *han* | *hade* | *att* | *framföra* | *det* | *i* | *allmän-* |
| 26907 | 41607 | 53490 | 10476 | 16873 | 13807 | 01396 |
| *-na* | *ordalag* | *(punkt)* | *Han* | *underströk* | *(imperf.)* | *dock* |
| 16087 | 01936 | 41762 | 37925 | 48965 | 41026 | 35168 |
| *den* | *stor-* | *a* | *vikt* | *it. regeringen* | *fäs-* | *te* |
| 04736 | | | | | | |
| *därvid* | | | | | | |

*Telegram 1*

| | | | | | | |
|---|---|---|---|---|---|---|
| 53608 | 04628 | 08653 | 04561 | 31264 | 48730 | 05372 |
| *Su-* | *vi-* | *ch* | *som* | *jag* | *på* | *dennes* |
| 39816 | 26517 | 13089 | 35046 | 29173 | 13950 | 38795 |
| *begäran* | *idag* | *besökt* | *meddelade* | *(imperf.)* | *att* | *general* |
| 03124 | 16980 | 40798 | 37049 | 17428 | 37904 | 53940 |
| *G-* | *raz-* | *ia-* | *ni* | *telegraferat* | *följande* | *(cit. tn)* |
| 54302 | 27860 | 45193 | 18529 | 21783 | 34719 | 03984 |
| *Såsom* | *repressalier* | *för att* | *abessinierna* | *(plur.)* | *st-* | *ym-* |
| 04987 | 34879 | 17956 | 43071 | 09168 | 34879 | 23716 |
| *-pat* | *italienska* | *fångar* | *(plur.)* | *hade* | *italienska* | *flyg-* |
| 43658 | 18640 | 39820 | 18529 | 50437 | 43071 | 40239 |
| *-are* | *i dagarna* | *bombarderat* | *abessinska* | *trupper* | *(plur.)* | *(punkt)* |
| 27680 | 09168 | 12043 | 26749 | 40936 | 08367 | 37201 |
| *Bl. a.* | *hade* | *man* | *i* | *närhet* | *av* | *Co-* |
| 48573 | 43981 | 39820 | 17483 | 18975 | 49581 | 23046 |
| *-go-* | *ru* | *bombarderat* | *militär-* | *befälhavare* | *Ras* | *Des-* |
| 13746 | 31405 | 51026 | 27153 | 13807 | 10289 | 46591 |
| *-tas* | *kvarter* | *vilket* | *förlagts* | *(imperf.)* | *i* | *omedelbar* |
| 40586 | 08367 | 35067 | 02931 | 31694 | 07432 | 41269 |
| *närhet* | *av* | *en* | *svensk* | *ambulans* | *(punkt)* | *Det* |



| | | | | | | |
|---|---|---|---|---|---|---|
| 15074 | 13807 | 04561 | 18057 | 03549 | 49836 | 49086 |
| *föreföll* | *(imperf.)* | *som* | *en* | *bomb* | *exploderat* | *0* |
| 40318 | 28467 | 31694 | 29640 | 19804 | 26458 | 20465 |
| *invid* | *denna* | *ambulans* | *och* | *såra-* | *t* | *Hy-* |
| 51980 | 36450 | 32059 | 29864 | 10498 | 08752 | 13054 |
| *-land-* | *er* | *(cit.-tn)* | *Sedan* | *jag* | *framfört* | *(sup.)* |
| 17924 | 29641 | 07298 | 52901 | 01354 | 19386 | 13950 |
| *sv. regeringens* | *anhållan* | *enl. telegram* | *50* | *lovade* | *S* | *att* |
| 15364 | 30952 | 46980 | 35089 | 51392 | 02451 | 10476 |
| *omedelbart* | *delgiva* | *mig* | *de* | *ytterligare* | *informationer* | *han* |
| 39471 | 30154 | 12953 | 16542 | 08739 | 46980 | 18349 |
| *kunde* | *erhålla* | *(punkt)* | *Han* | *bad* | *mig* | *varna* |
| 17924 | 15476 | 02374 | 24691 | 02654 | 40359 | 07639 |
| *sv. regeringen* | *för* | *att* | *tro* | *på* | *meddelande* | *från* |
| 18529 | 09821 | | | | | |
| *abessinskt* | *håll* | | | | | |

Den egna codelista jag hade kunnat upprätta innehöll då nära 900 chiffergrupper, dvs. nära tredjedelen av dess 2800.

På min begäran skedde en kollationering av felen i min code jämförd med den officiella. Resultatet verkade i förstone anskrämmande, ty rättelserna utgjorde drygt 300, alltså mer än tredjedelen av gruppantalet i min lista. Jag undersökte rättelselistan närmare. Kollationeringen hade helt naturligt skett rutinmässigt, så att varje avvikelse, även utan varje saklig betydelse, befanns antecknad. Jag fann bland rättelserna inalles 6 grova betydelsefel.

För att visa i vilken ringa grad mina tolkningar innebar någon saklig förvanskning av telegrammens innebörd meddelar jag nu de rättelser som avser tel. 43 förra delen och tel. 1. Min tolkning i övre raden, rättelser i undre raden. Hur lite rättelserna inverkar på sakinnehållet framgår klart. De nyss anmärkta grova betydelsefelen hänför sig till andra telegram. Beträffande dessa två är den egentligen anmärkningsvärda feltolkningen att en grupp, som jag satt 0 för, har betydelsen "representera".

*Rättelser i telegram 43, förra delen*

| | | | | | | |
|---|---|---|---|---|---|---|
| 02853 | 08921 | 23048 | 39816 | 12630 | 06189 | 42069 |
| *för* | *polit. avdeln.* | *på* | *begäran* | *meddelande* | *officer-* | *arnas* |
| *i st. f. polit* | *avdelning* | *hans* | *"* | *communication* | *plur.* | *gen.* |

| | | | | | | |
|---|---|---|---|---|---|---|
| 50742 | 06358 | 01279 | 18046 | 12936 | 53780 | 18372 |
| *s* | *dennes* | *ådagalagt* | *och* | *underteckna* | *andet* | *imperfektum* |
| *plur.* | *hans* | *visat* | *samt* | *avsluta* | *part. pres.* | *konjunktiv* |

| | | | | | | |
|---|---|---|---|---|---|---|
| 49316 | 31820 | 50726 | 15908 | 19530 | 24531 | 05981 |
| 0 | *giva* | *d* | *dessa* | *plur.* | *fattas* | *betraktas* |
| *representera* | *skänka* | *part. perf.* | *ifråga-varande* | *best. form plur.* | *verka* | *fattas* |

*Rättelser i telegram 1*

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 03124 | 16980 | 04987 | 23716 | 43658 | 40936 | 51980 | 36450 |
| *g* | *raz* | *pat* | *flyg-* | *are* | *närhet* | *länd* | *er* |
| *gr* | *az* | *at* | *flyga* | *re* | *trakt* | *län* | *der* |

Nu hade ju tolkningen av dessa två chifferdepescher stöd av blåbokstexten. Men tolkningen omfattade ju också senare delen av tel. 43, som icke medtagits i blåboken. Det har ju sitt särskilda intresse att se efter hur mycket rättelser det blev i den delen. Rättelserna är sannerligen varken många eller betydelsefulla såsom framgår av efterföljande sammanställning.

*Rättelser i telegram 43, senare delen*

| | | | | | | |
|---|---|---|---|---|---|---|
| 41638 | 29073 | 50236 | 49037 | 54219 | 54396 | 45289 |
| *på* | *förfrågan* | *beskickn. i Sthlm* | *under-* | *rätta* | *nu* | *punkt* |
| *citat slut* | *på min fråga* | *it. beskickn. i Sthlm* | *telegrafiskt* | *underrätta* | *tydligen* | *och* |

| | |
|---|---|
| 06842 | 01936 |
| *det* | *stor* |
| *detsamma* | *utomordentlig* |

I fråga om de nästan repetitionsfria raderna mellan förra och senare delen av tel. 43, vilka av mig lämnats otolkade, bekräftade kollationeringen min förmodan, att detta mellanstycke utgjordes av ett citat på franska, motsvarande sista meningen i blåbokstexten.

Det fanns inte heller efter kollationeringen någon anledning ändra mitt slutomdöme, att den använda coden i så väsentlig grad skulle bli tillspillogiven genom blåbokens publicering, att detta chiffersystem icke längre borde komma till användning. Så blev ju också resultatet.



# Använd litteratur


Bazeries *Les chiffres secrets dévoilés,* Paris 1893.

Bazeries *Les chiffres de Napoléon Ier,* Fontainebleau 1896.

Burgaud & Bazeries *Le masque de fer,* Paris 1893.

Candela *The military cipher of Commandant Bazeries,* New York 1938.

Lange et Soudart *Traité de Cryptographie,* Paris 1935.

Mansfield *One hundred problems in cipher,* London 1936.

Mazade *Correspondance de Davout,* Paris 1885.

Servières *L'Allemagne française sous Napoléon Ier,* Paris 1904.

Yardley *The American black chamber,* London 1931.
(Svensk översättning *Amerikas Svarta Kammare,* 1938)

Vigère *Davout,* Paris 1898.

*Hist. Jahrbuch d. Görres-Gesellschaft 1895—96.*

# *Ett urval Prismaböcker*

## KULTURHISTORIA

*Stig Ahlgren* Lärdom och lättsinne *7: 50*
*Marcel Brion* Dagligt liv i Wien på Mozarts och Schuberts tid *8: 50*
*Teddy Brunius* Kritikens pionjärer *8: 50*
*Jérôme Carcopino* Dagligt liv i antikens Rom *12: 50*
*Daniel-Rops* Dagligt liv i Palestina på Jesu tid *11: 50*
*Denis Diderot* Skådespelaren och hans roll *5: 50*
*A. G. Drachmann* Antikens teknik *9: 50*
*Ivar Harrie* Athenare *9: 50*
*Birger Norman* Repliker i kulturdebatten *5: 50*

## EKONOMI

*Sune Carlson* Företagsledare i arbete *9: 50*
*Stig T. L. Ericson* Vardagens ekonomi *8: 50*
*J. K. Galbraith* Överflödets samhälle *12: 50*
*Börje Kragh* Konjunkturbedömning *14: 50*
Prisma årsbok för aktieägare 1962 *inb. 16: 50*
*Robert Rock* Framgångsrika svenska företag *7: 50*
*Kurt Samuelsson* Hur vår moderna industri vuxit fram *7: 50*
*Göran Smith* Parterna på arbetsmarknaden *5: 50*
*Westerlind—Beckman* Sveriges ekonomi *6: 50*

## POLITIK, SAMHÄLLSVETENSKAP

*Axel Brusewitz* Kungamakt, herremakt, folkmakt *7: 50*
*Alan Bullock* Hitler I—III *à 8: 50*
De politiska partiernas program *6: 50*
*Arthur Koestler (red.)* Nedgång och fall? *12: 50*
*Le Corbusier* Vår bostad *8: 50*
*Ivar Lo-Johansson* Zigenare *8: 50*
*Wright Miller* Ryssarna som människor *5: 50*
*Hans Wattrang* Det kalla kriget *7: 50*
*Ernst Wigforss* Ur mina minnen *14: 50*
*George Woodcock* Anarkismen *14: 50*

## ARKEOLOGI, ETNOGRAFI, GEOGRAFI, HISTORIA

*Hans W:son Ahlmann m. fl.* Afrika *inb. 16: 50*
*Hans W:son Ahlmann m. fl.* Sovjetunionen *inb. 24: 50*
*Johannes Brøndsted* Vikingarna *8: 50*
*Sten Carlsson* Bonde — präst — ämbetsman *6: 50*
*Bengt Danielsson* Söderhavskärlek *8: 50*
*Bror Gadelius* Häxor och häxprocesser *8: 50*
*E. O. James* Gravarna berättar *9: 50*
*Hans Jägerstad* Sveriges historia i årtal *7: 50*
*Bruno Kalnins* Rysslands historia och statsskick *9: 50*
*Folke Lindberg* Hantverk och skråväsen under medeltid och äldre vasatid *12: 50*
*Einar Malm* Sitting Bull och kampen om Vilda Västern *6: 50*
*Sven Ulric Palme* Stockholms krigshistoria *6: 50*
*Karl Ploetz* Världshistorien i årtal *8: 50*
*Martin P:n Nilsson* Olympen *13: 50*
*Joseph Reither* Prisma världshistoria *8: 50*
*Robert C. Suggs* Polynesien — folk och kulturer *9: 50*
*Alf Åberg* Digerdöden *6: 50*
*Alf Åberg* Snapphanarna *6: 50*

## HANDBÖCKER

*Peter S. Hargreaves* Speak English better *5: 50*
*Samuel Karelitz* Prisma barnläkarbok *6: 50, inb. 9: 50*

*Keres-Kotov* Konsten att vinna i schack *6: 50*
*Emanuel Lasker* Sunt förnuft i schack *6: 50*
*Gert Lindner* Lilla fotoboken *7: 50*
*Iva Maasing* Sportbilar och bilsport *8: 50*
Modern engelsk-svensk ordbok *inb. 12: 50*
*H.-P. Pellaprat* Franskt kök för alla *inb. 7: 50*
Prisma uppslagsbok *inb. 12: 50*
*Jerome och Julia Rainer* Lyckliga tillsammans *6: 50*
*Reese—Watkins* Poker *5: 50*
*Brita Schlyter* Lek och leksaker *6: 50*
*Göran Smith* Arbete och ansvar *6: 50*
*Göran Smith* Service *5: 50*
*Gunnar Stahre* Vi bygger en sportstuga *6: 50*
*Arthur Steiner* Now you're talking *6: 50*
*Maj Thermaenius-Göransson* Gott och lättlagat *7: 50*
*Jan Ullén* Prisma bilhandbok I *inb. 9: 50*
*Einar Werner* Bridge på tjugo lektioner *6: 50*

## MEDICIN, BIOLOGI, RELIGION, PSYKOLOGI

*Isaac Asimov* Blodet *6: 50*
*Matts Bergmark* Farligt att förtära *12: 50*
*H. J. Eysenck* Psykologi på gott och ont *8: 50*
*H. J. Eysenck* Är ni intelligent? *12: 50*
*Munro H. Fox* Djurens personlighet *5: 50*
*Erich Franzen* Testpsykologi *5: 50*
*Robert Galambos* Nerver och muskler *5: 50*
*Donald R. Griffin* Att se med hörseln *4: 50*
*Gösta Harding* I uppväxtåren *6: 50*
*Ian M. L. Hunter* Minnet *4: 50*
*Gunnar Lundquist* Våra nerver *6: 50*
*F. L. Marcuse* Hypnos *6: 50*
*A. Stuart Mason* Hormonerna och hälsan *5: 50*
*Ragnar Numelin* Grafologin som vetenskap *5: 50*
*Erik Nyhlén* Svensk frikyrka *12: 50*
*Michael W. Ovenden* Liv på andra planeter *5: 50*
*Bengt Sjögren* Farliga djur och djur som inte finns *6: 50*
*Nathan Söderblom* Uppenbarelsereligion *7: 50*
*Robert Thomson* Tänkandets psykologi *7: 50*
*G. N. M. Tyrrell* Vid tröskeln till det okända *8: 50*
*Hans Winterstein* Sömn och dröm *5: 50*

## MATEMATIK, FYSIK, KEMI

*Irving Adler* Tänk på ett tal *4: 50*
*Louis J. Battan* Elementens raseri *4: 50*
*Bergeijk — Pierce — David* Ljudvågorna och vi *5: 50*
*Francis Bitter* Magneter *7: 50*
*George A. W. Boehm* Den nya matematiken *4: 50*
*Hermann Bondi* Världsrymdens gåtor *4: 50*
*R. L. F. Boyd* Rymdraketer och satelliter *4: 50*
*Charles V. Boys* Underverk med såpbubblor *4: 50*
*Rachel L. Carson* Havet *7: 50*
*I. Bernard Cohen* Fysikens banbrytare *5: 50*
*James A. Coleman* Relativitetsteori för alla *4: 50*
*P. J. Davis* De stora talens värld *8: 50*
*Davis — Day* Vatten — vetenskapens spegel *6: 50*
*René Dubos* Louis Pasteur och den moderna vetenskapen *4: 50*
*Albert Einstein* Om naturvetenskapen *5: 50*
*Fink — Lutyens* Bakom TV-rutan *4: 50*
*George Gamow* Tyngdkraften *5: 50*
*Donald J. Hughes* Den fantastiska neutronen *4: 50*
*Patrick M. Hurley* Hur gammal är jorden *4: 50*
*Lawrence P. Lessing* Vad är kemi? *5: 50*
*D. K. C. MacDonald* Vid absoluta nollpunkten *5: 50*
*H. W. Newton* Solens ansikte *6: 50*
*C. Stanley Ogilvy* Matematiska problem som väntar på sin lösning *8: 50*

*Alfred Romer* Den rastlösa atomen *5: 50*
*W. W. Sawyer* Räkna med nöje *6: 50*
*Åke Wallenquist* Astronomiskt lexikon *inb. 16: 50*
*Warren Weaver* Sannolikhet *13: 50*
*Victor F. Weisskopf* Vid kunskapens gränser *12: 50*
*Wilson — Littauer* I kärnfysikerns verkstad *7: 50*

*En bok om litterära och historiska hemligskrifter av Rickard Sandler*

# CHIFFER

Vid sidan av sin mångskiftande politiska och administrativa verksamhet hade utrikesministern och sedermera landshövdingen Rickard Sandler en originell hobby som han utvecklade till en specialitet. Hobbyn var chiffer, och den gjorde honom så småningom till en ofta anlitad expert, bl. a. under andra världskriget. Han skrev också en bok i ämnet, som utkom 1943 och här föreligger i av författaren bearbetad och utvidgad nyutgåva.

CHIFFER är till övervägande del uppbyggd kring autentiska fall ur diplomatins och det internationella spionagets historia, men redogör också för några berömda chifferproblem ur världslitteraturen. Under rubriker som *Ett Napoleonchiffer före Leipzig, Edgar Allan Poes guldscarabé, Farliga börssiffror, Napoleons Hamburginstruktion, En depesch till furst Metternich* och *PQR – ett tyskt cirkulärtelegram från första världskriget* beskriver Sandler med hjälp av instruktiva diagram och tabeller olika chiffersystem och forceringsmetoder.

I ett nyskrivet kapitel kallat *Ett svenskt diplomatchiffers ändalykt* får vi bevittna en uppvisning i den högre skolan som Sandler själv utförde sommaren 1936. Det gällde att utröna huruvida det dittills använda svenska diplomatchiffret var pålitligt eller ej – man befarade i det aktuella läget italiensk "insyn". Redogörelsen för hur Sandler steg för steg forcerade detta chiffer utgör en av höjdpunkterna i denna intellektuellt stimulerande och ytterst roande bok.

BOKFÖRLAGET PRISMA 9:50