CODICI CIFRATI

Arne Beurling
e la crittografia nella II guerra mondiale

Bengt Beckman

CODICI CIFRATI

Arne Beurling
e la crittografia nella II guerra mondiale

Traduzione a cura di
Clemente Ancona

Springer

Traduzione a cura di:
Clemente Ancona

Revisione Scientifica:
Renato Betti

© Bengt Beckman, 1996
Edizione originale dell'opera pubblicata da Albert Bonniers Förlag, Stockholm, Sweden
Tradotta in italiano con l'autorizzazione di Bonnier Group Agency, Stockholm, Sweden

ISBN-10 88-470-0316-4
ISBN-13 978-88-470-0316-3

Quest'opera è protetta dalla legge sul diritto d'autore. Tutti i diritti, in particolare quelli relativi alla traduzione, alla ristampa, all'uso di illustrazioni e tabelle, alla citazione orale, alla trasmissione radiofonica o televisiva, alla registrazione su microfilm o in database, o alla riproduzione in qualsiasi altra forma (stampata o elettronica) rimangono riservati anche nel caso di utilizzo parziale. La riproduzione di quest'opera, anche se parziale, è ammessa solo ed esclusivamente nei limiti stabiliti dalla legge sul diritto d'autore, ed è soggetta all'autorizzazione dell'editore. La violazione delle norme comporta le sanzioni previste dalla legge.

Springer fa parte di Springer Science+Business Media
springer.it
© Springer-Verlag Italia 2005
Stampato in Italia

L'utilizzo in questa pubblicazione di denominazioni generiche, nomi commerciali, marchi registrati, ecc. anche se non specificatamente identificati, non implica che tali denominazioni o marchi non siano protetti dalle relative leggi e regolamenti.

Progetto grafico della copertina: Valentina Greco, Milano
Fotocomposizione e impaginazione: Valentina Greco, Milano
Stampa: Signum Srl, Bollate (MI)

Indice

Introduzione all'edizione italiana VII
Premessa X
Prefazione XII

Parte 1

1. Un cifrario del XVIII secolo 3
2. La prima macchina cifrante al mondo 9
3. Damm, Hagelin e Gyldén 17
4. Intercettazione di segnali radio e analisi crittografica prima del 1939 29
5. Guerra 37
6. Entra in scena Arne Beurling 43
7. La flotta russa del Baltico 53
8. Segnali misteriosi 65
9. Telescriventi 69
10. L'analisi di Beurling 75
11. La G-Schreiber e gli "app" 89
12. Crittoanalisi sistematica 95
13. Esce di scena Gyldén, ma ricompare Beurling 105
14. La doppia trasposizione 111
15. Operazione Barbarossa 121
16. Il posto di lavoro 129
17. Contenuti 141
18. La nascita della FRA 147
19. Risultati brillanti, malgrado tutto 153
20. Regressi e fughe di notizie 161
21. L'Armata Rossa e il mare Artico 167
22. Il codice russo a doppia cifratura 171
23. Stella Polaris 175

24. Graduale calo del traffico tedesco 185
25. Borelius fa una visita ai Tedeschi 191
26. Informazioni - Ma quanto valgono? 197
27. Norvegia 201
28. Gli ultimi anni di guerra 211
29. I sistemi crittografici svedesi 215
30. Arne Beurling 1943-45 221

Parte 2

31. Arne Beurling 233
32. Attraverso gli occhi di una donna 245
33. Una magica amicizia 251

Fonti 261
Indice dei nomi 263

Introduzione all'edizione italiana

Nei primi anni della II guerra mondiale ebbe luogo uno dei fatti più clamorosi nel campo della crittografia militare, quando il matematico svedese Arne Beurling decrittò il codice che i Tedeschi utilizzavano per le comunicazioni strategiche fra Berlino ed i territori occupati in Norvegia e in Finlandia. Un'impresa paragonabile a quella del famoso codice *Enigma* – compiuta dai servizi di *intelligence* di Inghilterra e Polonia con l'apporto del noto matematico Alan Turing – seppure, a differenza di questa, rimasta segreta fino a tempi recenti. Il risultato più evidente di questo lavoro fu forse la decrittazione dei dati di invasione dell'Unione Sovietica – la cosiddetta "operazione Barbarossa" – come viene narrato nel libro.

L'autore, Bengt Beckman, dopo la guerra è stato per molti anni a capo dell'agenzia svedese di intercettazione e decifrazione (FRA) e, quando il materiale è uscito dal segreto militare, ne ha ricostruito con precisione e passione tutta la storia, dai primi risultati della *intelligence* svedese in occasione della Guerra d'Inverno russo-finlandese, alla nascita dell'agenzia stessa ed ai successi del periodo bellico. Della storia fanno parte essenziale il clima politico e la speranza che la Svezia riesca a mantenersi neutrale, il lavoro di decrittazione visto nella normalità delle attività quotidiane da parte dei dipendenti dell'agenzia, il genio isolato e scontroso di Beurling che non rivela le proprie mosse. Sullo sfondo: le vicende per noi poco note della guerra nel Baltico e nel mare del Nord.

I fatti che riguardano la decrittazione dei messaggi tedeschi sono semplici da riassumere: all'inizio della guerra, la Germania chiede di poter utilizzare i cavi telefonici in territorio svedese per le proprie comunicazioni con i paesi occupati. La Svezia acconsente e, da allora, ha a disposizione una grande quantità di messaggi riservati attraverso la regolare intercettazione del traffico delle telescriventi. Il maggior successo crittografico si manifesta presto, nell'aprile del 1940, soltanto due settimane dopo che il comando tedesco ha introdotto una nuova macchina – la *Geheimschreiber* (o *G-schreiber*) – un dispositivo che appare primitivo agli occhi di oggi ma che al tempo sembrava inespugnabile: tutti i telegrammi intercettati sono leggibili "in chiaro" dal comando svedese. Due settimane sono state sufficienti ad Arne Beurling, che partiva soltanto da una certa quantità di intercettazioni ma era a digiuno di ogni nozione relativa alle telescriventi, per emulare il dispositivo cifrante e ridurre il problema a quello di una semplice *routine* che personale appositamente addestrato, ma per altro non specializzato, può eseguire in tempi molto brevi.

Di fatto, come sempre avviene nel settore della crittografia, il successo si basava su una serie di piccoli errori commessi. Piccoli, ma imperdonabili – come l'uso ripetuto delle parole chiave – e in definitiva dipendeva dalla pigrizia e mancanza di fantasia degli operatori tedeschi, se non da incompetenza o frustrazione. Solo in qualche caso, si basava su una vera e propria attività di spionaggio. Ed è proprio in queste piccole fessure che si insinua la bravura dell'analista crittografo.

Con le vicende relative alla II guerra mondiale, la storia millenaria della crittografia conosce le manifestazioni più alte di una fase del proprio sviluppo, dopo che l'invenzione del telegrafo a metà dell'800 e più ancora l'avvento della radio avevano reso possibili comunicazioni rapide e facili, a scapito del fatto che fossero facilmente intercettabili. Il rimedio consiste nel cifrare con metodi sempre più intricati le comunicazioni esposte ad indiscrezione. In questa fase la crittografia è ancora un'arte – l'arte di trasmettere messaggi riservati. Più che un metodo riproducibile e analizzabile nelle sue regole, è una pratica che si acquisisce con l'esperienza. Si basa sulla fantasia del progettista e richiede intuito nell'analista che vuole infrangere il cifrario: non a caso Beurling non rivelerà mai la propria strategia di attacco alla *G-schreiber*. "Un mago non rivela i propri trucchi", si limita a ripetere, alquanto irritato, a chi vuole spiegazioni che forse non è in grado di dare.

Matematico raffinato, cultore di analisi complessa e di analisi armonica, Beurling si rende conto che il lavoro di decrittazione è analogo a quello che precede la dimostrazione di un teorema o la formulazione di un risultato. Per niente formalizzabile, è un lavoro che affonda le radici in una massa di dati, di sensazioni e di verifiche empiriche. Il risultato appare all'esterno, in tutto e per tutto, un atto di magia. E il libro parla anche, con linguaggio accessibile a diversi livelli, dei possibili sistemi di cifratura e sovracifratura, degli attacchi, delle osservazioni vincenti e delle strade senza sbocco, di tutto quel substrato di tentativi e prove empiriche che, quando hanno successo, fanno del lavoro di decrittazione un'impresa unica.

Dotato di forte personalità e grande ascendente, ma allo stesso tempo facilmente irritabile, Beurling è un personaggio singolare, in maniera naturale al centro di tutte le attività, dei successi come degli inevitabili contrasti che si manifestano nell'ambiente scientifico. E il libro lo segue anche nel periodo post bellico, quando si trasferisce all'*Institute for Advanced Study* di Princeton, fino alla sua scomparsa nel 1986, quasi a voler comprendere le ragioni del successo crittografico attraverso l'ulteriore esame del personaggio, o forse soltanto per far conoscere maggiormente la personalità di Beurling che, nonostante i risultati scientifici e il brillante lavoro di decrittazione in tempo di guerra, non è molto conosciuto al di fuori della Svezia.

Oggi la crittografia ha abbandonato la fase dei sistemi empirici di cifratura e decrittazione, basati sull'intuizione personale e dotati di poche regole, soprattutto di carattere statistico-combinatorio, così come nel corso del tempo ha superate altre fasi: il periodo "eroico" monoalfabetico, quando la fantasia costituiva la maggiore sorgente di imprevedibilità per l'intercettatore, poi la sistematica rinascimentale, con i primi cifrari polialfabetici, i primi congegni meccanici e i primi algoritmi, contrastata efficacemente dai metodi statistici. L'inizio del '900 presenta nuovi concetti e nuovi dispositivi, come il flusso delle chiavi generato casualmente e l'uso di macchine elettromeccaniche per il trattamento dell'informazione. Dall'inizio del '900 sorge una grande quantità di dispositivi, soprattutto a rotori, come l'*Enigma* e la stesa *G-schreiber*, che ricorrono a metodi sempre più complessi per cifrari i messaggi.

La nuova fase, quella della moderna crittografia, riguarda la nascita dell'idea di "chiave pubblica" negli anni '70. Con essa, l'antica arte di trasmettere messaggi segreti si sta facendo scienza, anche sotto l'emergenza delle necessità delle comunicazioni commerciali: oltre alle esigenze militari e diplomatiche, da sempre presenti, la crittografia coinvolge operazioni quotidianamente compiute da tutti, in ambito privato e personale. E la materia si trova oggi al crocevia, pratico e concettuale, di numerose discipline scientifiche: teoria dell'informazione, complessità computazionale, calcolo delle probabilità, teoria dei numeri, per citarne solo alcune. Investe problematiche di grande valore sociale e politico, coinvolge la nostra *privacy* e il nostro giudizio morale, ha rilevanza sul piano economico e del diritto.

Al confronto con i sistemi di cifratura odierni, quelli di cui si narra nel libro appaiono irrimediabilmente ingenui e datati, non solo alla luce delle moderne potenzialità di calcolo, ma anche delle nuove idee. Eppure, solo qualche decennio fa, per la loro analisi è stato necessario ricorrere ad un massiccio lavoro umano, continuo e sistematico, ai primi rudimentali sistemi di calcolo automatico, appositamente progettati, e all'opera insostituibile e creativa di un "mago". L'apporto umano è ancora alla base di qualsiasi impresa di questo genere. Questa ne è la storia. Una storia recente.

Renato Betti
Politecnico di Milano

Premessa

Quando scoppiò la Seconda Guerra Mondiale, il 1° settembre 1939, la Svezia aveva due pericolosi vicini. La Germania aveva già occupato l'Austria e la Cecoslovacchia e l'Unione Sovietica stava avanzando pretese territoriali sulla Finlandia e gli Stati Baltici. Una settimana prima dell'attacco della Germania alla Polonia, i due antagonisti sorpresero il mondo – che aveva sperato in un equilibrio del terrore – concordando un patto di non aggressione, il Patto Molotov-Ribbentrop. Sembrava che le due fiere unissero le loro forze.

Per motivi storici, l'URSS veniva percepita dagli Svedesi come la minaccia più immediata: la Svezia era stata in guerra con la Russia più o meno in continuazione durante il periodo 1200-1809, ed ora sembrava che l'Orso Russo si stesse preparando ad avanzare di nuovo nella nostra direzione. La Sezione Cifra del Quartier Generale dello Stato maggiore della Difesa, di recente formazione, aveva concentrato i propri sforzi sui sistemi di codifica sovietici, allo scopo di seguire le mosse della marina sovietica.

Nell'autunno del 1939 le pretese sovietiche si fecero sempre più minacciose e, quando i Finlandesi si rifiutarono di cedere, la Russia attaccò. In Svezia l'aggressione diede origine a moti d'indignazione fino ad allora raramente registrati e a manifestazioni di solidarietà. I Finlandesi tennero duro per tre mesi – la cosiddetta Guerra d'Inverno durò dal 30 novembre al 13 marzo – ma alla fine dovettero accettare severe condizioni.

In Svezia la minaccia immediata parve affievolirsi, ma il 9 aprile i Tedeschi occuparono la Danimarca e la Norvegia. I soldati svedesi da poco smobilitati dovettero riprendere servizio.

Per comunicare con Berlino, gli occupanti della Norvegia usavano cavi che passavano attraverso la Svezia, e gli Svedesi furono abbastanza indelicati da intercettare le linee. All'inizio il sistema crittografico tedesco parve troppo difficile da forzare. Tuttavia le cose cambiarono quando Arne Beurling, professore di matematica all'università di Uppsala, fu chiamato a dare una mano: per diversi anni le comunicazioni tedesche furono regolarmente decrittate.

Il governo e le forze armate svedesi avevano la possibilità di seguire lo sviluppo degli eventi, e non solo in Norvegia, da poltrone di prima fila. Venivano trasmessi regolari rapporti sui diversi teatri di guerra agli ufficiali dello Stato maggiore di stanza in Norvegia. In più, risultò che una parte della corrispondenza tra Berlino e l'ambasciata tedesca di Stoccolma era criptata con lo stesso tipo di macchina cifrante.

L'attacco tedesco all'URSS nel giugno del 1941 non giunse agli Svedesi come

una sorpresa: riuscendo a leggere i telegrammi tedeschi cifrati, ne erano a conoscenza con settimane d'anticipo. La Guerra di Continuazione tra Finlandia e Russia, per la quale in Svezia vi fu scarso entusiasmo, portò alla cooperazione tra Germania e Finlandia, con truppe tedesche stazionanti in Finlandia. Così come le truppe di stanza in Norvegia, esse usavano cavi telegrafici attraverso la Svezia e lo stesso sistema di cifratura, cosicché, di nuovo, gli Svedesi furono in grado di intercettare e decrittare le loro comunicazioni.

Per quasi tutto il resto della guerra, le truppe tedesche circondarono quasi completamente la Svezia: erano in Norvegia, in Finlandia, nel Baltico, in Polonia, in Danimarca e, ovviamente, nella stessa Germania. Questo, prima dell'avvento dei missili da crociera e degli ICBM (*Inter-Continental Balistic Missiles*, missili balistici intercontinentali), né ci si poteva aspettare aiuto da qualcuno. In Norvegia stazionavano 350.000 soldati tedeschi, la maggior parte dei quali poteva essere usata in operazioni contro la Svezia. In tale situazione, per il governo svedese fu inestimabile la possibilità di seguire i piani tedeschi: si potevano avere indicazioni di un possibile attacco con vasto anticipo.

In ogni modo, non giunsero indicazioni in tal senso, e nessun attacco ebbe luogo. Nell'inverno 1942-43 la bilancia si spostò a svantaggio dei Tedeschi. Persero 250 mila uomini a Stalingrado e, in Africa, Rommel cominciò a ritirarsi. L'esito della guerra si poteva ormai intravedere.

Al tempo stesso, verso la fine del 1942, i Tedeschi cominciarono a rendersi conto che le loro comunicazioni in cifra erano ampiamente decifrate in Svezia. Vennero allora introdotti alcuni miglioramenti nel sistema e, piano piano, venne a mancare questo spiraglio sulla macchina da guerra tedesca. Ma ormai il pericolo si era andato riducendo.

Durante la fase più critica della guerra la direzione politica e militare poté seguire i piani e le disposizioni dei Tedeschi e modificare di conseguenza la propria politica, cercando di tenere la Svezia fuori dalla guerra.

La storia della violazione del codice tedesco è narrata in dettaglio in questo libro per la prima volta.

Hans Dalberg

Prefazione

La storia dei successi crittoanalitici – quando si riescono a infrangere i sistemi di cifratura di altri paesi – è generalmente tenuta segreta. Ma con l'andar del tempo la segretezza viene gradualmente allentata, ed ora si può narrare la storia della decrittazione del sistema tedesco *Geheimschreiber* da parte di Arne Beurling.

Nel 1946, quando cominciai a lavorare per la FRA come coscritto, la guerra era ormai terminata. Qui racconterò le storie di coloro che hanno preso parte, e portato a compimento, alcune tra le più notevoli e singolari imprese crittoanalitiche mai realizzate. Inoltre, darò qualche esempio di come viene fatta l'analisi crittografica, sia a livello elementare che a livello più avanzato. Il lettore è invitato a cimentarsi personalmente con questi esempi.

Nel 1991 sono andato in pensione, dopo essere stato a capo della sezione di analisi crittografica della FRA. Le mie fonti principali sono gli archivi della FRA e gli uomini e le donne che hanno partecipato allo sforzo bellico. Alla fine del libro c'è un elenco di quelli che ho intervistato. Sono grato a tutti loro, ma vorrei esprimere dei ringraziamenti speciali a un paio di vecchi amici.

Il primo in assoluto è Carl-Gösta Borelius, morto nel 1995. Ho sfruttato a man bassa le sue memorie e i suoi appunti. Egli inoltre mi ha aiutato con materiale crittografico e tecnico durante la stesura di questo libro. Un'altra fonte di estremo valore è stato Åke Lundqvist, che ho intervistato varie volte, ripetutamente citando brani dei suoi rapporti. Sven Wäsström, il guru dei nostri servizi di *intelligence*, mi ha fornito un aiuto inestimabile nel chiarire una serie di punti oscuri. Ulla Flodkvist ha tradotto per me vari testi dal tedesco, Gunnar Blom ha contribuito con la storia di un caso di analisi crittografica, e Gunnar Jacobsson, così come molti altri, mi hanno raccontato le loro storie e i fatti relativi agli anni pionieristici del *sigint* svedese. Sono grato ad Anne-Marie Yxkull Gyllenbrand, Gertrud Nyberg-Grenander, Lennart Carleson, Erna e Lars Ahlfors. Tutti hanno conosciuto personalmente Beurling e tutti mi hanno aiutato a creare un ritratto della sua complessa personalità.

Vorrei infine ringraziare Olle Häger e Hans Villius. Il progetto di questo libro è nato durante la preparazione di un documentario TV su Arne Beurling, realizzato insieme a loro. Essi mi hanno incoraggiato e indotto a cominciare a scrivere: dopo aver letto il manoscritto, hanno contribuito con idee e opinioni, delle quali sono loro molto grato.

Bengt Beckman

Parte 1

1. Un cifrario del XVIII secolo

Alla FRA, l'agenzia svedese per le comunicazioni segrete, mi capitò di dover affrontare strani compiti, come quando nel 1988 ricevetti una lettera con quattro frasi cifrate, tratte da un diario del 1770.

Un dottorando e storico dell'università di Uppsala di nome Jan Häll aveva trovato queste frasi mentre stava conducendo una ricerca su Swedenborg[1] e seguaci. Non essendo riuscito a scoprire il sistema di cifratura, si rivolse per aiuto al Ministero della difesa e, dopo un po' di giri, la lettera approdò sul mio tavolo. Nella loro forma originaria le frasi erano le seguenti:

16 giugno: *Öpka cgplotnl utpx oyx Otolyss Otiåtigt Lmnqrt Urlayxa*
9 settembre: *Balagxa mbaljaysråa hcts*
30 settembre: *Banjöay orp cgp ora hcts*
14 ottobre: *Hctsxyl tz ora mpxt*

Al fine di rendere la presente esposizione più comprensibile, abbiamo creato un gruppo di frasi simili in lingua italiana:

VQDWHCBQ RPQUQ ULH PQKK PRAYRAWBR KLMNQR TQKBWVB

KLXXWAWHBW QHVQUQTQOW RYLHQR

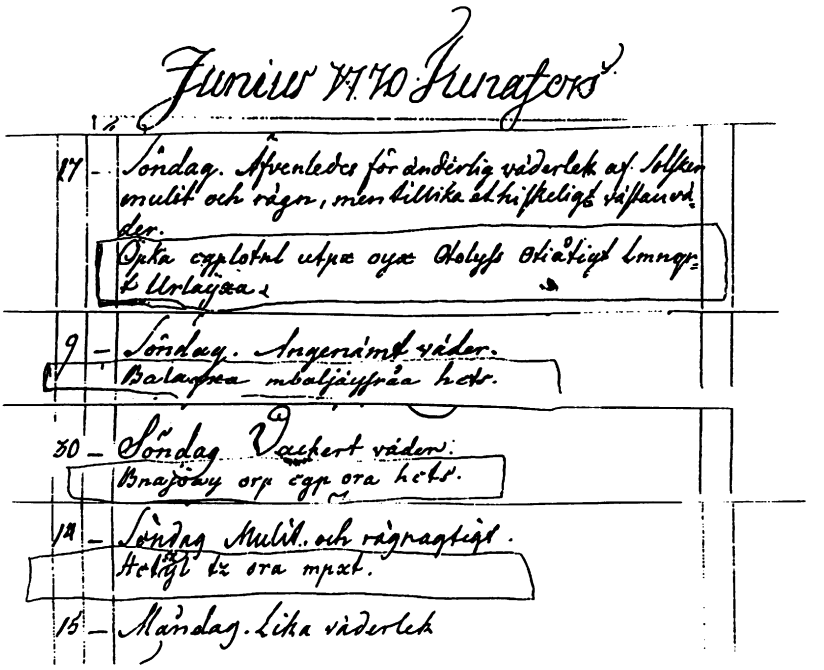
QO PQL RPQUL DWVW OR PQR RYRHQR

URCKRBR VR KLXXWAWHJR

Il diario era quello di un tal Christian Johansén e, di quest'ultimo, Jan Häll scrisse quanto segue:

"Come premessa, posso dire che Johansén presto divenne il principale allievo di Swedenborg nel XVIII secolo. Nel 1770, quando furono scritte le frasi, egli aveva 25 anni e, per la prima e ultima volta, aveva appena incontrato Swedenborg. Al tempo egli lavorava come precettore presso la casa del proprietario delle ferriere Tunafors, Hellenius. Sembra che avesse trascorso molti

[1] Emanuel Swedenborg, scienziato svedese del XVIII secolo, trasformato in mistico religioso, fondatore di una setta che portava il suo nome.



Da un diario del XVIII secolo

dei suoi giorni giocando d'azzardo, anche se allo stesso tempo anelava a condurre una vita religiosamente corretta. Nel diario si trovano poche tracce sul contenuto delle frasi, ad eccezione del fatto, abbastanza certo, che fossero di argomento religioso: tutte e quattro sono state scritte di domenica, forse in relazione a servizi ecclesiastici".

Avrei certo potuto delegare questo compito a qualche collega più giovane del mio dipartimento, ma la curiosità ebbe la meglio e il giorno stesso mi portai a casa la lettera.

Chiunque voglia mettere alla prova la propria abilità può ora interrompere la lettura e mettersi a lavorare per conto proprio. Attrezzi raccomandati sono: carta, matita, gomma e un sacco di idee.

Il sistema sembra proprio uguale a quelli assegnati come esercizio nei corsi elementari di crittografia, una semplice sostituzione di parole separate da spazi. Il primo ordine delle operazioni consiste quindi in una tavola di frequenza delle lettere:

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
4	6	2	2	0	0	0	7	0	1	7	7	1	1	3	6	17	18	0	2	5	5	11	4	3	0

La distribuzione molto irregolare delle lettere non contraddice l'ipotesi di una semplice sostituzione. La tabella indica anche che la lettera più comune della lingua italiana, la *e*, è rappresentata dalla *W*, dalla *Q* o dalla *R* e il fatto che queste lettere siano spesso in fine di parola conferma che possono stare per delle vocali.

Quando si affronta una semplice sostituzione, si può usare con vantaggio una proprietà strutturale, la ripetizione o quasi ripetizione di sequenze di lettere. In questo caso, vediamo che le sequenze *RPQU* e *KLXXWAWH* si presentano entrambe due volte, mentre *RYLHQR* e *RYRHQ* hanno tutto in comune meno la terza lettera, e anche che *PQL* e *PQR* differiscono solo per la lettera terminale. Il digramma *QR* compare quattro volte e i correlati *QO e QL* una sola, tutte in fine di parola. Si trovano anche relazioni più esotiche, ma ci accontenteremo di questi esempi.

Per cominciare, con *PQL* e *PQR*, buoni candidati potrebbero essere sostantivi come "uso/usi", oppure articoli: "mio/mia" o "tuo/tua", soprattutto se si conferma che *Q* sta per una vocale. L'accostamento *KLXXWAWH* è seguito in un caso da *BW*, e nell'altro caso da *JR*, alimentando il sospetto di una provenienza verbale con desinenze come *-ente* e *–enza* [differente/differenza], tenuto conto della doppia *XX*; i sostantivi e gli aggettivi variano tendenzialmente per la sola lettera finale, e questo potrebbe essere il caso di *RPQUQ* e *RPQUL* [onere/oneri], e gli aggettivi sono tipicamente sostantivati da *-ità* [felice/felicità] o anche *–ezza* [contento/contentezza], il cui schema non è presente. L'ipotesi verbale, includente l'assunto che *KLXXWAWH* termini con *-ente* e *–enza*, non contraddice il fatto che *e* ed *a* sono vocali ad alta frequenza.

Cosicché, la nostra prima *Ansatz* sarà:

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
r t n z e

VQDWHCBQ RPQUQ ULH PQKK PRAYRAWBR KLMNQR TQKBWVB
e n t n r r e t t e t

KLXXWAWHBW QHVQUQTQOW RYLHQR
e r e n t e n e n

QO PQL RPQUL DWVW OR PQR RYRHQR
e e n

URCKRBR VR KLXXWAWHJR
t e r e n z

Notiamo che le lettere *R* e *Q*, molto frequenti, dovrebbero rappresentare vocali. Dato che la *e* è occupata da *W*, per la combinazione *QR/QL* siamo rimasti con i suggerimenti "*ia/io*" oppure "*ia/iu*". In effetti, dalla tavola delle frequenze, il secondo caso sembra meno probabile, quindi, con *r* corrispondente a *A*, e *a* a *R*, otteniamo una prima indicazione: abbiamo a che fare con un *alfabeto a sostituzione reciproca*. Sembra difficile sfruttare tale ipotesi in questo particolare momento, cosicché per ora la lasceremo da parte e guarderemo ai risultati delle ipotesi formulate finora:

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
r t n z o i a e

VQDWHCBQ RPQUQ ULH PQKK PRAYRAWBR KLMNQR TQKBWVB
i en t i a i i on i ar areta o ia i t e t

KLXXWAWHBW QHVQUQTQOW RYLHQR
o erente in i i i e a onia

QO PQL RPQUL DWVW OR PQR RYRHQR
i io a i o e e a i a a ania

URCKRBR VR KLXXWAWHJR
a ata a o erenza

Per fare progressi, dobbiamo fare un'audace supposizione su alcune parole. Un attraente bersaglio è RPQUQ con il suo compagno RPQUL, che sembrano gridare di essere semplicemente "amico/amici". Ciò tra l'altro concorda con la lettera *P* al posto della frequente *m*.

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
r t n z o m i a c e

VQDWHCBQ RPQUQ ULH PQKK PRAYRAWBR KLMNQR TQKBWVB
i en t i amici conmi mar areta o ia i te t

KLXXWAWHBW QHVQUQTQOW RYLHQR
o erente in ici i e a onia

QO PQL RPQUL DWVW OR PQR RYRHQR
i mio ami co e e a mia a ania

URCKRBR VR KLXXWAWHJR
c a a t a a o e r e n z a

Le rimanenti lettere sono facili da immaginare: *V=d/C=t* e *K=s/Y=g* e si conferma che si tratta di una sostituzione reciproca:

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

VQDWHCBQ RPQUQ ULH PQKK PRAYRAWBR KLMNQR TQKBWVB
d i v e n u t i a m i c i c o n m i s s m a r g a r e t a s o p h i a b i s t e d t

KLXXWAWHBW QHVQUQTQOW RYLHQR
s o f f e r e n t e i n d i c i b i l e a g o n i a

QO PQL RPQUL DWVW OR PQR RYRHQR
i l m i o a m i c o v e d e l a m i a a g a n i a

URCKRBR VR KLXXWAWHJR
c a u s a t a d a s o f f e r e n z a

Notiamo che il sofferente Christian ha fatto un errore: ha scritto "agania" anziché "agonia". Ciò va tenuto in conto quando si trattano sistemi con carta e matita. L'alfabeto usato può scriversi:

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

la cui chiave mnemonica poteva facilmente essere ricordata dal nostro addolorato protagonista.

La scoperta della signorina Bistedt ebbe una sua parte nella tesi di Jan Häll, che fu pubblicata come *I Swedenborgs labyrint* [Nel labirinto di Swedenborg] (Atlantis, 1995, in svedese) sulla quale chi scrive è stato debitamente informato.

Terminologia

Molte parole in fatto di scrittura segreta derivano dalla parola greca *kriptós*, segreto. Parliamo così di *cripto* o *crittosistema*, o anche di *cripto* tout court, o di *dispositivo* o *apparato criptico* o *crittico*. *Crittologia* e *crittografia* vengono

usati quando si vuole parlare della scienza o arte della scrittura segreta. A volte crittologia è il termine più comprensivo, e crittografia si riferisce solo all'arte di mantenere segreta l'informazione. La crittologia quindi comprende la crittoanalisi, la decifrazione dei sistemi crittati, vale a dire il reperimento dell'informazione senza avere una totale conoscenza a priori del sistema usato.

Una seconda classe di termini – *cifrario*, *macchina cifrante, cifrare* – deriva dal latino *cifra*, equivalente a *zero*, (originalmente dall'arabo *sifr,* equivalente a vuoto, zero). Infine, c'è la parola *codice*, amata e impropriamente usata. Nella teoria dell'informazione, il termine *codice* è usato per qualunque sistema di rappresentazione dell'informazione, sia esso segreto o palese, come ad esempio il codice Morse o l'ASCII. In crittologia, la parola viene spesso adoperata in luogo di "cifrato" o di "criptico", benché la terminologia ortodossa ritenga che "codice" equivalga a *libro di codici* (come spiegheremo meglio più avanti), per differenziarlo da *cifratura*, vale a dire un crittogramma nel quale le lettere sono cifrate a una a una. Con le moderne tecniche di cifratura è difficile attenersi, da un punto di vista filosofico, a questa dicotomia, e noi saremo piuttosto liberali nell'usarla. L'espressione popolare per crittoanalisi, "infrangere un codice", risulta di scarso gusto per il professionista, ma è difficile da bandire dai titoli di testa dei giornali.

Una parola ambigua in fatto di crittologia è *chiave*, che può avere molteplici significati. A volte *chiave* equivale a *variabile criptica*, che è un termine indicante elementi segreti spesso cambiati in un sistema. Chiave può anche indicare il risultato intermedio del processo di cifratura – *chiave corrente*, *flusso di chiavi* - così come una parte regolare del linguaggio in frasi ed espressioni, come l'inglese *keyboard* (tastiera), o *elemento chiave,* dove "chiave" non ha alcuna connotazione crittografica.

Per sequenze di lettere, come *AB*, *XYZ* E *IJKL*, useremo le parole *digrafo, trigrafo, tetragrafo* anziché *bigramma, trigramma* ecc. *Signal Intelligence* o brevemente *sigint*, è il termine inglese adoperato per indicare le informazioni raccolte intercettando segnali e ascoltando trasmissioni via radio o via cavo.

Altri termini verranno spiegati strada facendo. Dato l'argomento di questo libro, dovremo spesso riferirci a varie istituzioni svedesi, i nomi abbreviati delle quali sono ben noti al lettore svedese. Useremo pertanto traduzioni semiufficiali – MAE per Ministero degli Affari Esteri (UD in svedese) – o ne inventeremo di nuove, per quanto possibile facilmente intelligibili – come QGSMD o Quartier Generale dello Stato maggiore della Difesa, in svedese *Försvarsstaben.*

2. La prima macchina cifrante al mondo

La prima macchina cifrante al mondo fu svedese. Essa fu presentata al re Gustavo III in una lettera del barone Frederik Gripenstierna, una figura peraltro ignota ai circoli crittografici. Una fattura della sua ditta, la Firma Charles Apelquist & Company, mostra che il prezzo era di 130 *riksdaler*.

L'apparecchio stesso e i suoi disegni sono andati smarriti. Una descrizione di questo dispositivo, contenuta in un opuscolo, fu trovata negli anni '70 nell'Archivio di Stato di Svezia: "Descrizione che illustra come una macchina cifrante, costruita dal sottoscritto, può essere usata per cifrare e decifrare" [tradotto dallo svedese]. In calce si legge: Drottningholm, 23 settembre 1786, F. Gripenstierna.

Per singolare coincidenza, Drottningholm è situata sull'isola di Lovö, sul lago Mälaren, dove ha sede la FRA, la ricordata agenzia svedese per le comunicazioni segrete, e dove lo scopritore del documento, Sven Wäsström, trascorse la maggior parte della sua vita professionale.

Altre circostanze sono ancor più singolari. Nella lettera al re, Gripenstierna fa riferimento al proprio nonno, Christofer Polhem, in questi termini: "…da me inventata secondo i principi appresi in gioventù da mio nonno…". Polhem fu un inventore prolifico. In Svezia è meglio conosciuto per via della cosiddetta serratura Pohlem, ma egli lavorò in vari settori; per esempio, giusto per nominarne alcuni: impianti di autotrasporto delle miniere, utensili per tagliare il legno, telai, apparecchi di sutura, orologi a pendolo… Senz'altro, una macchina cifrante poteva far parte del suo vasto repertorio.

Sven Wäsström ha esplorato a lungo la vasta corrispondenza di Pohlem con i sapienti europei del tempo, scoprendo che Pohlem aveva studiato l'*Abacus Numeralis*, un'opera del gesuita e studioso Kircher. In questa opera sono abbozzati i principi della macchina di Gripenstierna.

Frederik Gripenstierna ebbe un'ampia opportunità di venire a conoscenza delle idee del nonno. Dopo la morte della moglie, Pohlem si trasferì nella tenuta della famiglia Gripenstierna a Ekerö, un'altra isola del lago Mälaren, vicino a Lovö, dove visse fino al 1755. La figlia di Pohlem sposò Carl Gripenstierna, ciambellano della regina vedova Hedvig Eleonora e proprietario di Kersö, un'altra isola del lago Mälaren, molto vicina a Lovö. Carl Gripenstierna ebbe due figli; il maggiore, Frederik, nacque nel 1728, ricevette la sua baronia nel 1755 e morì nel 1804.

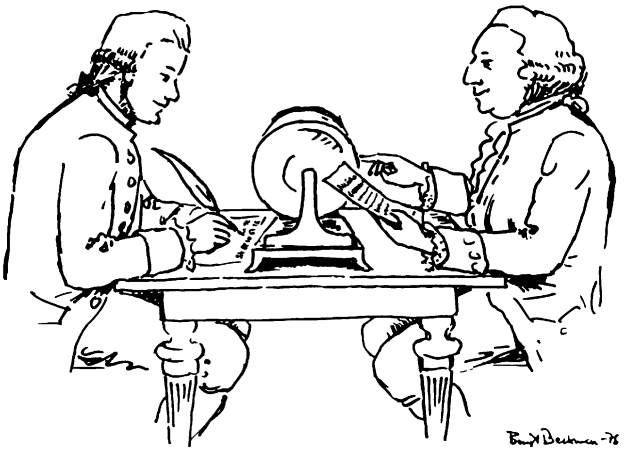
Molti indizi fanno pensare che la macchina di Gripenstierna debba in realtà chiamarsi macchina di Pohlem. Probabilmente, fu costruita in esempla-

re unico, benché per ogni genere di uso pratico ne fossero necessari almeno due. Si può affermare con sicurezza che essa non fu mai messa in opera realmente, ma spero che sia di qualche interesse lo studio del suo progetto. Sven Wäsström e l'autore di queste righe hanno tentato di farne una ricostruzione, e Boris Hagelin, della Crypto AG svizzera, ne ha costruito un modello, conservato nel museo dell'azienda.

L'idea di base del progetto non è molto complicata e può essere descritta agli addetti ai lavori come un sistema Vigenère a sostituzione non ordinata, di lunghezza finita e con periodo variabile. La *Chiffre-Maskin* era costitiuita da 57 dischi alfabetici racchiusi in un cilindro. Metà della circonferenza di ogni disco recava incise le lettere in ordine alfabetico, e l'altra metà conteneva, sempre incisi, 30 numeri compresi tra 0 e 99, disposti in totale disordine. Le lettere si potevano vedere solo attraverso uno spioncino situato da una parte del cilindro, mentre i numeri si potevano analogamente vedere attraverso un altro spioncino, sull'altra parte del cilindro.

L'apparecchio era azionato da due persone. Si introduceva il testo in chiaro, in sezioni di 57 caratteri al massimo, dalla parte delle lettere, ruotando i dischi finché le lettere giuste comparivano nello spioncino. Quindi l'altra persona registrava i numeri che comparivano nello spioncino della sua parte. Gripenstierna sottolinea il vantaggio: solo una persona vedeva il testo in chiaro. L'altra, presumibilmente il segretario del re, vedeva e registrava solo il testo cifrato.

Un'ulteriore complicazione era quella di poter lavorare con sezioni più corte di 57 caratteri. I primi dieci dischi avevano dei codici numerici di due cifre, arbitrariamente scelti, incisi sopra lo spioncino dalla parte del segretario,



e l'addetto alla cifratura poteva cominciare da uno qualsiasi di questi dischi. Per rendere possibile la decifrazione, il numero di codice del disco di partenza veniva scritto alla fine di ciascuna sezione cifrata.

Dato che il segretario leggeva da sinistra a destra, le lettere cifrate della sezione compariva all'inverso. Ciò era automaticamente corretto durante il processo di decifrazione.

Nella sua descrizione, Gripenstierna dice che la macchina contiene 1539 variazioni delle lettere "da cui discende l'innegabile impossibilità di essere mai in grado di calcolare i valori delle lettere della *Chiffre*". Il numero 1539 è il prodotto 27x57, probabilmente il numero di lettere dell'alfabeto che egli usava, moltiplicato per il numero dei dischi. L'alfabeto del testo in chiaro non è noto con esattezza, ma dagli esempi di testo dati da Gripenstierna si può supporre che fosse costituito almeno dalle lettere dell'alfabeto svedese, eccetto la X e la W, più i punti, le virgole, il punto e virgola e le spaziature.

A B C D E F G H I J K L M N O P Q R S T U V Y Z Å Ä Ö . , ; -

C'era anche uno spazio bianco, che in verità non rientrava nel processo di cifratura.

È senz'altro naturale che, in crittografia, il progettista pretenda che il proprio sistema è inviolabile, così come è naturale che il criptoanalista metta alla prova questa pretesa. Quali difficoltà doveva affrontare un criptoanalista e quali possibilità aveva di ripristinare il testo in chiaro da una *dépêche* cifrata con un simile dispositivo?

Nella macchina di Gripenstierna non c'è niente di simile ad una variabile crittologica, vale a dire nessun elemento segreto che cambi da messaggio a messaggio o da un giorno all'altro. La sicurezza risiede nel mantenere segreta la costruzione della macchina: i numeri incisi sui dischi e i numeri di codice dei primi dieci dischi. In tal modo, se da un lato si evita che l'analista abbia qualche idea sui principi progettuali della macchina, dall'altro gli si consente di avere un testo cifrato abbastanza lungo costituito, per esempio, da 100 righe.

Nel linguaggio crittografico, il sistema è un *Vigenère*, un cifrario a sostituzione con più alfabeti. Vigenère era un diplomatico francese che illustrò il suo sistema in un opuscolo del 1586.

Il compito dell'analista non è facile. Egli scopre presto che il sistema non è una semplice sostituzione, e in un secondo tempo può supporre di trovarsi alle prese con un Vigenère. Il primo ordine di operazioni da affrontare consiste nella ricerca del *periodo*, vale a dire del numero di alfabeti. Dopo un po' dovrà ammettere di aver sbagliato e cominciare a supporre che il periodo sia variabile. Studiando le ripetizioni nel testo cifrato e notando che la distanza tra que-

ste è dell'ordine di grandezza di 50, o di multipli approssimati di 50, egli comincerà a sospettare che i periodi variabili siano all'incirca di questa lunghezza. Con questo in mente, egli può *adattare*, o *mettere in fase*, sezioni del testo cifrato in relazione tra di loro. Di nuovo è aiutato dalle ripetizioni del testo, ma anche dal fatto che il numero dei digrafi (vale a dire delle combinazioni di due cifre) in ogni alfabeto non può essere maggiore di 30 (l'alfabeto, più i segni di punteggiatura). Il nostro analista potrà allora scoprire la numerazione delle sezioni e con tale conoscenza mettere in fase completamente il sistema.

A questo punto egli avrà ridotto il problema ad un comune Vigenère, che può essere attaccato compilando tabelle di frequenza dei digrafi che appaiono in ogni colonna (corrispondenti ai dischi). Il digrafo più comune in ciascuna colonna è in genere il separatore delle parole, poi seguiranno i digrafi per *a, e, n, t* ecc., ma non necessariamente nel giusto ordine. Indovinando correttamente solo alcune lettere e usando le ripetizioni trovate, potrà allora tentare di trovare brevi parole comuni da adattare alle proprie congetture. Dato che non si è ancora reso conto che le sezioni sono scritte all'incontrario, sbaglierà nelle proprie supposizioni fino a quando non troverà l'idea giusta.

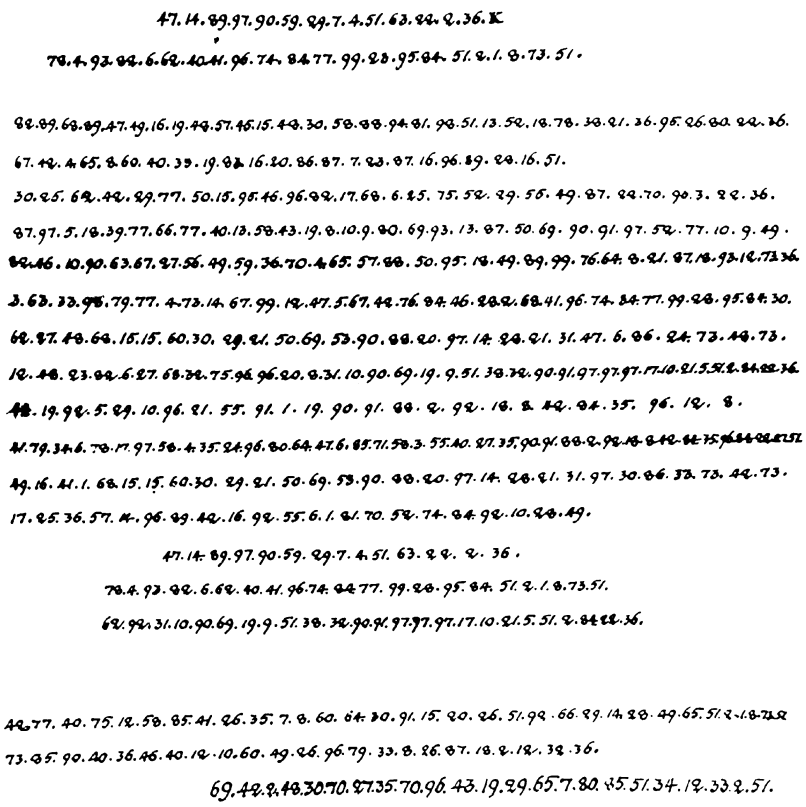
Il compito dell'analista è semplificato se dispone di un *crib*[1], o porzione di testo in chiaro, di cui egli sa che fa parte del messaggio, e se conosce o può conoscere la posizione che esso ha all'interno del messaggio. Quando le lettere del *crib*, o piuttosto i digrafi che lo rappresentano, sono trovati in altre sezioni, questa informazione può essere usata per intuire alcune parole con maggiore verosimiglianza.

L'analista viene anche aiutato dall'accesso a un consistente numero di messaggi. In questo caso per lui è più facile scoprire il sistema dei numeri di codice delle ruote iniziali.

Un analista esperto ha buone probabilità di ricostruire la maggior parte del testo disponendo di una *profondità* pari a 100: in questo caso 100 sezioni correttamente disposte in fase. In ogni caso è necessaria una buona dose d'inventiva e di intuizione linguistica, oltre a diligenza o semplice tenacia.

Più avanti è riportato il testo cifrato inviato da Gripenstierna al re. Se cercassimo di decifrarlo non andremmo molto lontano. Ma in questo caso c'è un *crib*, costituito dalla lettera di accompagnamento del messaggio, "il formato della lettera concorda con il messaggio cifrato".

[1] Nel gergo scolastico inglese può anche equivalere a *bigino,* e "to crib" sta per *copiare* (p.e. dal quaderno del compagno di banco) (n.d.t).



Lettera cifrata indirizzata al re

La lettera in chiaro:

Stormägtiste Allernådigste Konung!

Efter Allernådigste Befallning har jag nu förfärdigat en Chiffre-Clav, och som jag högeligen önskar, att den måtte vinna Eders Konglige Majestäts Nådigste Approbation; så utbeder jag mig den Nåden, att inför Eders Konglig Majestät, få den samma i underdånighet uppvisa.

Med underdånigste Zele och Soumission, har jag den nåden, att intill dödstunden framhärda,

Stormägtiste Allernådigste Konung,
Eders Konglig Majestäts,
Allerunderdånigste Tropligtigste
Tienare och undersåte
Fridric Gripenstierna.

Il fatto che il *crib* sia scritto nello svedese del Settecento è irrilevante: chiunque può cercare di ricostruire almeno una parte degli alfabeti cifrati. Si può seguire la strategia appena accennata: le righe del testo cifrato sono da leggere all'incontrario e spostate in modo che le rispettive colonne siano tutte cifrate con la semplice sostituzione definita dalla ruota corrispondente.

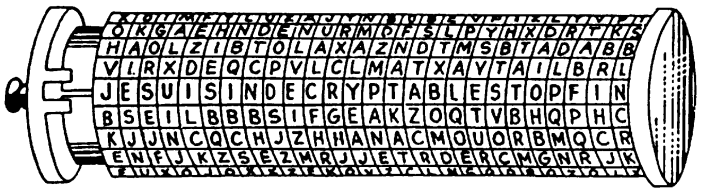
A titolo d'esempio, e di traccia, trascriviamo la prima riga del testo cifrato, con il numero di codice della ruota corrispondente (solo all'inizio il numero di codice è preceduto dalla lettera *K*) e il *crib*:

K36	*02*	*22*	*63*	*51*	*04*	*07*	*29*	*59*	*90*	*97*	*89*	*14*	*47*
	s	*t*	*o*	*r*	*m*	*ä*	*g*	*t*	*i*	*g*	*s*	*t*	*e*

Non si sa se Gripenstierna abbia scelto a caso le combinazioni a due cifre degli alfabeti cifrati, o se abbia usato un qualche tipo di algoritmo. Se il lettore riesce a ricostruire gli alfabeti delle ruote, è invitato a esprimere un'opinione, anche se, naturalmente, la lunghezza del testo riprodotto qui è troppo breve per giungere a conclusioni definitive.

Il cilindro di Bazeries

Il cilindro di Bazeries, progettato dal francese Étienne Bazeries nel 1891, è simile alla macchina di Gripenstierna, anche se un po' più raffinato. Nella sua semplicità, è un'invenzione ingegnosa. Le sue 25 ruote, contenenti ciascuno una permutazione delle lettere A-Z, ruotano intorno ad un asse comune. Il cifratore fa girare le ruote per comporre il testo in chiaro in una posizione designata, e legge il testo cifrato in un'altra posizione, scelta a caso. Il decifratore non ha bisogno di sapere quale posizione di lettura sia stata scelta; egli



"*Je suis indécryptable*" [non sono decrittabile]

semplicemente inserisce il testo cifrato nella posizione designata, quindi guarda le 25 possibili posizioni di lettura. Le lettere formeranno un testo leggibile in una sola di esse, e quello sarà il messaggio originale in chiaro. La ragione per la quale ciò è possibile sta nella notevole *ridondanza* del linguaggio: solo pochissime tra le possibili combinazioni di 25 lettere hanno senso.

Lo statista americano, poi divenuto presidente, Thomas Jefferson, aveva sviluppato un'idea simile cento anni prima, ma il suo progetto non ebbe uso immediato e finì per essere dimenticato. Esso però fu nuovamente ripreso in considerazione durante la seconda guerra mondiale: gli Americani usarono un dispositivo chiamato M-94, basato sullo stesso principio.

3. Damm, Hagelin e Gyldén

L'industria crittografica svedese ebbe inizio con i fratelli Damm. Arvid era un ingegnere tessile e Ivar un insegnante di matematica. Entrambi erano appassionati di crittografia. Poco prima della morte di Ivar, nel 1918, i fratelli pubblicarono un breve opuscolo dattiloscritto, *Kryptologins grunder* [Fondamenti della crittologia]. Secondo Arvid, l'ultima parola pronunciata dal fratello in letto di morte fu "cripto".

Arvid Damm aveva una grande quantità di idee e fece molti progetti. Nel 1918, con l'aiuto del comandante Olof Gyldén, capo del Collegio della Marina da guerra, fondò una compagnia, la AB Cryptograph. Gyldén coltivava un notevole interesse per la crittografia ed aveva antenati matematici: suo padre era il noto astronomo Hugo Gyldén, nella cui famiglia crebbe la figlia di Sofia Kovalevsky. Il figlio di Olof, Yves Gyldén, avrà una parte di primo piano nella storia della crittografia svedese.

Con la AB Cryptograph, Damm poté cominciare a sfruttare commercialmente le proprie idee; nell'arco di cinque anni furono costruiti sei diversi prototipi di macchina cifrante. Tuttavia la produzione tendeva a fermarsi a questo stadio iniziale. Le macchine risultavano inaffidabili ma, nonostante le luminose idee crittografiche contenute nel loro progetto, Damm non riusciva a venderle. Forse l'inettitudine commerciale di Damm era in qualche misura dovuta alla sua eccentricità ed al suo stile di vita *bohémien*. La storia del suo "matrimonio" illustra bene questo aspetto della sua personalità.

Damm era un accanito donnaiolo. Durante un soggiorno in Finlandia, si innamorò di un'artista da circo ungherese; dovunque il circo si spostava, lì Damm compariva. Il suo amore non fu del tutto ignorato, ma prima di cedere al suo spasimante, la principessa del circo volle che la relazione venisse formalizzata. Damm risolse il problema invitando un certo numero di amici ad un finto matrimonio, con tanto di testimoni e con uno dei convenuti travestito da prete, per la celebrazione.

In seguito, incontrata una giovane donna più attraente, Damm volle annullare il "matrimonio" in tribunale, nonostante la decisa opposizione della "moglie". Durante il processo la sordida storia venne a galla, con il racconto del falso matrimonio fatto da Olof Gyldén. Per difendersi, Damm accusò la finta moglie di spionaggio, ma l'accusa fu confutata. E naturalmente il sodalizio d'affari tra Damm e Gyldén giunse al termine.

Nel 1921 la compagnia di Damm era ormai sull'orlo della bancarotta, quando entrò in scena la famiglia Hagelin. Karl Wilhelm (Vasilevich) Hagelin

(padre di Boris, che in seguito sarebbe divenuto famoso come costruttore di macchine cifranti) era nato in Russia da genitori svedesi. Era amico stretto di Emanuel Nobel e membro di primo piano della compagnia petrolifera della famiglia Nobel a Baku. A causa della rivoluzione russa, la compagnia fu costretta a rinunciare ai propri possedimenti in Russia, così Emanuel Nobel e K.W. Hagelin si trasferirono in Svezia. Decisero allora di investire nella compagnia di Damm, sia perché erano entrambi attratti dalle innovazioni tecniche, sia perché intravedevano nuove possibilità commerciali della crittografia per la corrispondenza d'affari.

Boris Hagelin aveva allora trent'anni. Diplomato in ingegneria, pur non avendo conoscenze in fatto di crittografia, né interesse per la materia, fu inserito nella compagnia dagli investitori. Il suo compito era quello di controllare e tener d'occhio l'imprevedibile Damm, che era incline a sviluppare ingegnose ma invendibili apparecchiature.

Un ex impiegato e collaboratore di Damm, G.A. Lindbeck, ha espresso la massima ammirazione per l'intelligenza e le doti tecniche di Damm. Molti prototipi progettati da Damm sono esposti al museo della Crypto AG in Svizzera, una compagnia fondata da Boris Hagelin nei primi anni '50.

La più importante tra le invenzioni di Damm fu la B1, l'"Elettrocrittografo". Si basava su un suo brevetto del 1919 relativo a un sistema di cifratura mediante rotori. Un rotore è un dispositivo ruotante che, in ogni posizione, realizza una sostituzione semplice. La stessa idea fu sviluppata quasi contemporaneamente da Hebern negli Stati Uniti, da Koch in Olanda e da Scherbius in Germania. In un rotore, la sostituzione è realizzata con fili elettrici che collegano 26 contatti sulla parte *in chiaro* a 26 contatti sulla parte *in cifra*. Si possono immaginare i contatti come rappresentanti le lettere *A*-*Z*. Quindi, la parte in chiaro *A* è collegata alla parte in cifra *D*, per esempio, *B* a *Z* e così via. Premendo *B* su una tastiera, un impulso elettrico viene trasmesso al contatto *B* della parte in chiaro. Attraverso un filo, la corrente giunge al rotore nel punto *Z*, che è la lettera cifrata che sostituisce la *B* del testo in chiaro. Dopo che una lettera è stata cifrata, il rotore ruota, cambiando la sostituzione semplice. Dato che ci sono solo 26 posizioni, il rotore tornerà al punto di partenza dopo 26 spostamenti, in modo che la macchina, senza aggiunte speciali, eseguirà solo una sostituzione Vigenère di periodo 26. Il tocco in più sta nel montare un certo numero di ruote su un asse comune, eseguire le sostituzioni in serie, e far scattare i rotori l'uno rispetto all'altro fra i caratteri del testo. Con ciò il periodo Vigenère può essere reso molto lungo. Questo stesso principio fu usato nella macchina Enigma durante la seconda guerra mondiale.

Nel 1925 Damm si trasferì a Parigi, a quanto pare per continuare il proprio lavoro sulle macchine cifranti da telegrafia. Boris Hagelin lo sostituì allora