STORIA DELLA CRITTOGRAFIA

LE MACCHINE CIFRANTI

In ordine di esposizione:

- Sara Castellani:
  - Crittografia antica e primi cifrari storici
- Daniele Salvi:
  - Crittografia moderna, Jefferson e Lorenz
- Daniele Lozzi:
  - Enigma e Bombe di Turino
- Daniele Palladino:
  - Sigaba e Purple

1. CRITTOGRAFIA ANTICA E PRIMI CIFRARI STORICI (curato da Sara Castellani)

1.1 La storia

Per migliaia di anni re, regine e generali hanno avuto il bisogno di comunicazioni efficienti per governare i loro paesi e comandare i loro eserciti. Nel contempo, essi compresero quali conseguenze avrebbe avuto la caduta dei loro messaggi in mano ostili : informazioni preziose sarebbero state a disposizione delle nazioni rivali e degli eserciti nemici. Fu il pericolo dell' intercettazione da parte degli avversari a promuovere lo sviluppo di codici, tecniche di alterazione del messaggio destinate a renderlo comprensibile solo alle persone autorizzate.

Una delle prime tecniche di comunicazione segrete, basata sull'occultamento del messaggio, si chiama **steganografia**, dalle parole greche **steganós**, che significa coperto, e **gráphein**, che significa scrivere. Negli anni sono state impiegate in tutto il mondo innumerevoli forme di steganografia.

Uno dei metodi più bizzarri per trasmettere le informazioni segrete era utilizzato nell'antica Persia e viene raccontato da Erodoto. Esso consisteva nel rapare i capelli di uno schiavo e nel scrivergli il messaggio sulla testa. Lo schiavo si recava poi dal destinatario del messaggio dopo che gli erano ricresciuti i capelli e il messaggio era recuperato rapandoglieli nuovamente.

Nell'antica Cina si dipingeva il messaggio su striscioline di seta finissima, che venivano appallottolate e coperte di cera. Le palline erano quindi inghiottite dal messaggero. Nel XVI secolo lo scienziato italiano Giambattista Della Porta spiegò come comunicare tramite un uovo sodo, preparando un inchiostro con 30 grammi di allume in mezzo litro d'aceto, e usandolo per scrivere sul guscio. La soluzione penetra nel guscio, che è poroso, senza lasciar traccia, e tinge l'albume solidificato; quest'ultimo potrà essere letto sbucciando l'uovo.

La longevità della steganografia dimostra che essa garantisce una certa sicurezza, ma il suo punto debole è evidente : se il latore del messaggio è attentamente perquisito, è probabile che il messaggio sia scoperto; in tal caso, il nemico può farne l'uso che crede. In altre parole, la segretezza è perduta nel momento stesso dell'intercettazione. In tal caso è inevitabile che molti messaggi siano trovati.

Perciò in parallelo con lo sviluppo della steganografia si assisté all'evoluzione della crittografia, dal greco **kryptós**, che significa nascosto. La crittografia non mira a nascondere il messaggio in sé, ma il suo significato. Per rendere incomprensibile un testo, lo si altera per mezzo di un procedimento concordato a suo tempo dal mittente e dal destinatario. Questi può quindi invertire il procedimento, e ricavare il messaggio originale. Il vantaggio della crittografia è che anche se il nemico intercetta il messaggio, esso risulta incomprensibile e quindi inutilizzabile. Infatti il nemico, non conoscendo il procedimento di alterazione, dovrebbe trovare difficile, se non impossibile, ricostruire il significato.

Non tutte le società antiche svilupparono forme di crittografia. La Cina, per esempio, l'unica civiltà antica ad usare una scrittura ideografica, non ne ha mai viste. Le ragioni, a detta degli storici, sono legate alla natura prevalentemente orale delle comunicazioni.

In India, invece, forme di crittografia furono concretamente praticate. In diversi testi sacri sono presenti riferimenti a forme di scritture segrete. Nell'Artha-Sastra, un testo classico sugli affari di stato, si sottolinea l'importanza delle scritture segrete nei servizi di spionaggio. Esempi di scritture segrete sono presenti anche nel Latila-Vistara, un libro che esalta le virtù di Budda.

Anche nelle scritture cuneiforme sviluppate in Mesopotamia sono stati ritrovati esempi di crittografia. Sia presso gli Assiri che i Babilonesi, le due grosse civiltà sorte sulle sponde del Tigri, è stata rinvenuta l'usanza di sostituire le parti terminali delle parole con elementi corti e stereotipati detti colofoni. In Iraq, nel periodo finale delle scritture cuneiformi, è presente per la prima volta la sostituzione di nomi con numeri.

Anche se la steganografia e la crittografia sono discipline indipendenti, possono essere impiegate per alterare e occultare il medesimo testo, garantendo un livello di sicurezza molto più alto. Per esempio, il « ***microdot*** », cioè la riduzione di uno scritto alle dimensioni di un punto, è una forma di steganografia che ebbe largo impiego durante la seconda guerra mondiale. Tramite un procedimento fotografico, gli agenti tedeschi in America latina trasformavano una pagina scritta, precedentemente crittografata, in una macchia con un diametro inferiore al millimetro, che poteva essere nascosta nel puntino di una « i » in una comunicazione banale. Il primo microdot fu scoperto dall' FBI nel 1941 grazie a una soffiata.

1.2 Crittografia antica

Le più antiche notizie sicure sono probabilmente quelle sulla **scitala lacedemonica** , data da Plutarco come in uso dai tempi di Licurgo (IX sec a.C.) ma più sicuramente usata ai tempi di Lisandro(verso il 400 a.C.). Consisteva in un bastone su cui si avvolgeva ad elica un nastro di cuoio; sul nastro si scriveva per colonne parallele all'asse del bastone, lettera per lettera, il testo segreto. Tolto il nastro dal bastone, il testo vi risultava trasposto in modo regolare ma sufficiente per evitare la comprensione senza un secondo bastone uguale al primo.

Scitala lacedemonica

Disco di Enea

Tra il 390 e il 360 a.C. venne compilato da Enea il tattico, generale della lega arcadica, il primo trattato di cifrari il cui XXI capitolo tratta appunto di messaggi segreti. In questo viene descritto un disco sulla zona esterna del quale erano contenuti 24 fori, ciascuno dei quali era contrassegnato da una lettera disposte in ordine alfabetico. Un filo, partendo da un foro centrale, si avvolgeva

passando per i fori delle successive lettere del testo. Il destinatario del messaggio svolgeva il filo dal disco segnando le lettere da esso indicate. Il testo si doveva poi leggere a rovescio. Le vocali spesso erano sostituite da gruppi di puntini(vedi figura sopra).

Nei testi sacri, in particolare nel Vecchio Testamento, si possono ritrovare tre principali scritture segrete : l' **Atbash**, l' **Albam** e l' **Atbah**.

Il primo codice cifrato, l' **Atbash**, è stato ideato dal popolo ebraico. Esso consisteva nel capovolgere l'alfabeto, di conseguenza la prima lettera diventava l'ultima e l'ultima la prima e così per tutte le altre lettere dell'alfabeto. Usando l' attuale alfabeto ordinario, l' Atbash può essere riassunto con la seguente tabella di cifratura :

Usando il moderno alfabeto internazionale, l'Atbash può essere riassunto con la seguente tabella di cifratura:

CHIARO 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

CIFRATO 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

Utilizzando la frase **Il sole brilla** come frase chiara da cifrare il risultato sarà: **Rohlovyirooz.**

Il codice Atbash è quindi simile ma meno complesso di quello di Cesare, poichè al contrario di quest'ultimo prevede solo una possibile sostituzione.

L'Albam richiede che l'alfabeto venga diviso in due parti e che ogni lettera venga sostituita con la corrispondente dell'altra metà.

Infine, **l'Atbah**, richiede che la sostituzione soddisfi una relazione di tipo numerico. Le prime nove lettere dell'alfabeto vengono sostituite in modo tale che la somma della lettera da sostituire e della lettera sostituente risulti uguale a dieci. Per le restanti lettere dell'alfabeto deve valere una regola simile con somma pari a 28 in decimale.

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
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

Lo storico greco **Polibio** (200 ca. -118 a.C.), nelle sue Storie (Libro X) descrive un interessante metodo di cifratura. L'idea è quella di cifrare una lettera con una coppia di numeri compresi tra 1 e 5, in base ad una matrice 5x5, contenente le lettere dell'alfabeto. Ogni lettera viene rappresentata da due numeri, guardando la riga e la colonna in cui essa si trova. Per esempio, a=11 e r=42.

Inoltre, Polibio, suggeriva di mandare tanti messaggeri quanti erano i caratteri del messaggio. Questi portavano nella mano sinistra un numero di torce pari all'indice di riga e nella mano destra un numero pari all'indice di colonna. In effetti più che di un codice segreto, si tratta di un sistema di telecomunicazione, di fatto un telegrafo ottico. In tal modo il messaggio può essere trasmesso con due gruppi di cinque torce (p.es. 1,5 = una torcia accesa a destra, cinque a sinistra). Telegrafi a torce esistevano da molti secoli ed erano stati descritti da Enea il tattico intorno al 350 a.C., ma erano basati su un limitato elenco di messaggi possibili; quello di Polibio si basa invece sulla scomposizione del messaggio nelle singole lettere ed è quindi in grado di trasmettere qualsiasi messaggio.

#	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I	J
3	KQ	L	M	N	O
4	P	R	S	T	U
5	V	W	X	Y	Z

Esempio:

Quindi la frase **Attenzione agli scogli** dopo la cifratura risulterà:

1144441534552435341511223224431335223224

La sua importanza nella storia della crittografia sta nell'essere alla base di altri codici di cifratura come il Playfair chiper o il cifrario campale germanico usato nella prima guerra mondiale.

Svetonio nella Vita dei dodici Cesari, un'opera del II secolo d.C., racconta che Giulio **Cesare** usava per le sue corrispondenze riservate un codice di sostituzione molto semplice, nel quale ogni lettera del testo veniva sostituita dalla lettera che la segue di tre posti nell'alfabeto. Ad esempio la lettera A è sostituita dalla D, la B dalla E e così via fino alle ultime lettere che sono cifrate con le prime come nella tabella che segue (che fa riferimento all'odierno alfabeto internazionale).

Prendendo come esempio la frase **Auguri di buon compleanno** si otterrà il seguente messaggio cifrato:

Chiaro auguridibuoncompleanno Cifrato dxjxulglexrqfrpsohdqqr

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

Più in generale si dice codice di Cesare un codice nel quale la lettera del messaggio chiaro viene spostata di un numero fisso di posti, non necessariamente tre. Poiché l'alfabeto internazionale è composto da 26 caratteri sono possibili 26 codici di Cesare diversi dei quali uno (quello che comporta uno spostamento di zero posizioni) darà un cifrato uguale al messaggio chiaro iniziale.

Lo scrittore Robert Graves, grande studioso di storia romana e autore di una pseudo-autobiografia dell'imperatore Claudio (nei due romanzi *Io Claudio* e *Il divo Claudio*), sostiene che **Augusto** usava accanto al semplice codice di Cesare un cifrario più sicuro per le comunicazioni più delicate; sarebbe stato lo stesso Claudio a comprenderne il funzionamento dopo aver studiato le carte di Augusto. Il metodo si basa sul testo greco dell'Iliade; il testo chiaro e un brano dell'Iliade erano scritti in parallelo; ogni lettera del chiaro era confrontata con la corrispondente dell'Iliade, si calcolava la differenza tra i due caratteri e la sequenza dei numeri così calcolati costituiva il messaggio cifrato. Per decifrare era sufficiente sommare al carattere dell'Iliade il numero del

messaggio. Si tratta chiaramente di cifrario polialfabetico che precorre di 1500 anni la **tavola di Vigenere**.

Esempio:

Parola chiara:	C A S A
Posizione lettera chiara:	3 1 9 1
Parola chiave:	P E L O
Posizione lettera chiave:	16 5 12 15
Parola cifrata:	S F E P
Posizione:	19 6 5 16

In questo caso la prima lettera chiara (*C* posizione 3) verrà spostata di 16 posti (posizione della lettera chiave *P*) e si verrà a trovare in posizione 19, equivalente alla lettera *S*; allo stesso modo la seconda lettera chiara (*A* posizione 1), spostata di 5 posti (posizione della lettera chiave *E*), diventerà la lettera cifrata *F* (posizione 1+5=6), mentre la terza lettera (*S* posizione 19) spostata di 12 posti dar□9+12=31 che, superando i limiti dell'alfabeto, dovrà essere diminuita di 26 dando come risultato la lettera 5 (*E*).

Ecco un altro esempio usando come testo chiaro "Le nostre truppe in Polonia sono in rotta" crittografato usando come chiave i primi versi dell'Inferno di Dante Alighieri:

chiaro: l e n o s t r e t r u p p e i n p

chiave: n e l m e z z o d e l c a m m i n

sposta: 14 5 12 13 5 26 26 15 4 5 12 3 1 13 13 9 14

cifrato z j z b x p o t x w g s q r v w d

chiaro: o l o n i a s o n o i n r o t t a

chiave: d i n o s t r a v i t a m i r i t

sposta: 4 9 14 15 19 20 18 1 22 9 20 1 13 9 18 9 20

cifrato: s u c c a u k p j x c o e x l c u

Il messaggio crittato sarà quindi: **zjzbxpotxwgsqrvwdsuccaukpjxcoexlcu.**

Per decifrare il testo basterà compiere il processo inverso (sottrarre invece di sommare).

1.3 La crittografia fino al XVIII secolo

Verso l'anno mille compaiono i primi **alfabeti cifranti** o monografici. Essi sono usati successivamente soprattutto nelle missioni diplomatiche tra i vari staterelli europei, particolarmente da parte delle repubbliche marinare e dalla corte papale di Roma e a partire dal XIV secolo.

Negli **alfabeti cifranti** la cifratura avviene tramite alfabeto monografico, nel caso più semplice, dando ad ogni lettera dell'alfabeto, compresi a volte lo spazio e i vari segni di interpunzione, come corrispondente un segno dello stesso alfabeto, di un altro alfabeto o addirittura inventato dall'ideatore della cifra al momento. Si ottiene quindi una tabella a due colonne dove ogni segno alfabetico del testo in chiaro corrisponde biunivocamente ad uno dell'alfabeto cifrante.

Un sistema usato dall'Arcivescovo di Napoli, **Pietro di Grazia**, tra il 1363 e il 1365, é quello in cui le lettere sono cifrate con numeri o simboli speciali. La corrispondenza tra lettere e simboli o numeri per la sostituzione è fissata da una tabella. Dagli inizi del XIV secolo, per depistare i tentativi di analisi statistica delle frequenze, si iniziano ad usare più segni per cifrare le vocali, dato che queste sono molto ricorrenti in un testo. Successivamente tale tecnica viene estesa anche alle consonanti più ricorrenti. Inoltre alcune parole, utilizzate frequentemente, (Papa, et, con, quo, etc.) sono sostituite con un solo simbolo. Un primo esempio di questa cifratura fu la lettera di Michele Steno scritta nel 1411.

Lettera di Michele Steno

Leon Battista Alberti, nel suo Trattato De Cifris, introdusse il suo sistema polialfabetico che per tre secoli , seppur attribuito ad altri autori costituì il basamento dei sistemi crittografici. Esso ha proposto un disco composto di due cerchi concentrici di rame. Uno esterno fisso di diametro maggiore sul quale sono riportate le lettere dell'alfabeto in chiaro e uno interno mobile per le lettere dell'alfabeto cifrante. Il disco esterno fisso composto di 24 caselle contenenti 20 lettere latine maiuscole (inclusa la Z, con U=V ed escluse H J K W Y) ed i numeri 1 2 3 4 per il testo chiaro; e quello interno mobile, con le 24 lettere latine minuscole per il testo cifrato. Le 20 lettere maiuscole messe in ordine alfabetico; le 24 maiuscole in disordine (questa è una norma fondamentale, trascurata da molti successori dell'Alberti, senza la quale si ha una semplice generalizzazione del codice di Cesare).

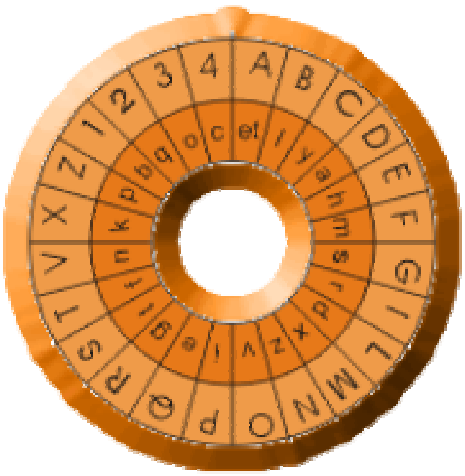
Fissata una lettera maiuscola come indice (ad es. B) si deve spostare il disco mobile interno e scrivere, come prima lettera del crittogramma, la lettera minuscola che corrisponde alla B; quindi cifrare alcune parole con la lista risultante. Quando si decide di cambiare la lista cifrante si scriverà la nuova lettera chiave in maiuscolo in modo da indicare chiaramente al corrispondente il cambio di lista. Ciò fatto, si porterà quella lettera ad affacciare l'indice B ed in questa nuova posizione si cifreranno altre parole secondo la nuova lista.

Può anche essere utilizzata una chiave diversa per ogni parola del testo in chiaro. Le lettere che di volta in volta corrispondono ai numeri 1 2 3 4 non vengono usate per la cifratura. Tutte le lettere del messaggio da cifrare sono cambiate in base all'associazione tra le lettere maiuscole e quelle minuscole.

Mittente e destinatario avevano entrambi la stessa macchinetta. Entrambi concordavano una lettera che sarebbe stata la chiave di partenza. Per crittare il messaggio, il mittente iniziava ruotando il disco interno in maniera casuale. Iniziava quindi a scrivere il testo cifrato, riportando per prima cosa la lettera sul disco piccolo in corrispondenza della chiave concordata sul disco grande. Passava quindi ad eseguire la sostituzione del testo prelevando i caratteri sul disco più piccolo in corrispondenza dei caratteri da cifrare sul disco più grande. Terminata la prima parola, ruotava di nuovo in maniera casuale il disco interno ed iniziava a scrivere la nuova parola riportando nel cifrato la lettera sul disco piccolo in corrispondenza della chiave concordata sul disco grande, seguita dalla parola le cui lettere venivano ancora sostituite dalla corrispondenza tra disco grande e disco piccolo. In questo modo, ogni parola utilizzava un proprio alfabeto di sostituzione e con tale dispositivo ne erano a disposizione 24 (ecco perchè questo sistema è classificato tra i polialfabetici). In questo modo, Leon Battista riusciva ad impedire l'analisi statistica basata sulla frequenza delle lettere da lui stesso studiata.
Interessante notare come tale dispositivo venisse utilizzato anche come piccolo nomenclatore: Leon Battista aveva stabilito un codice formato da 336 valori, combinando 1,2,3,4 in gruppi di 2, 3 e 4 cifre (11, 12, 13, 14, 21...111,112...1111,1112...). Grazie alle quattro cifre riportate nel disco più grande, era possibile cifrare il codice, rendendolo più sicuro, sebbene avesse già di per sé una certa sicurezza per l'epoca. Per cifrare tali numeri si utilizzava la stessa tecnica vista in precedenza.

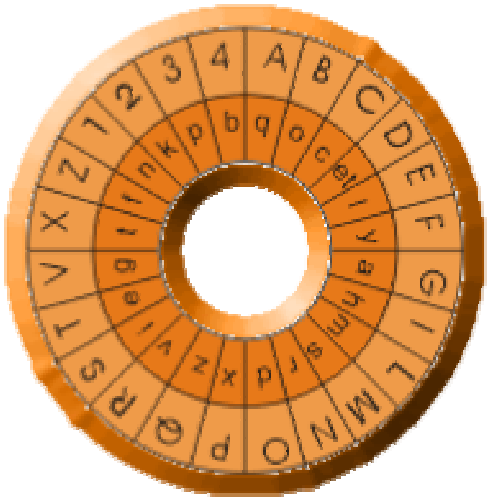
Esempio d'uso:

Mettiamo di dover cifrare la frase "Messaggio da Leon".
Iniziamo convenendo una lettera che fa da riferimento, diciamo la C.
Ruotiamo a caso il disco interno e passiamo in questa situazione, con il disco interno posizionato come in figura qua sotto.
Dato che il riferimento è la lettera C, iniziamo a scriver il messaggio indicando al destinatario come deve ruotare il suo disco interno. Per farlo iniziamo la parola cifrata con Y, e ne deriva:
Messaggio = YXHTTETSSRV

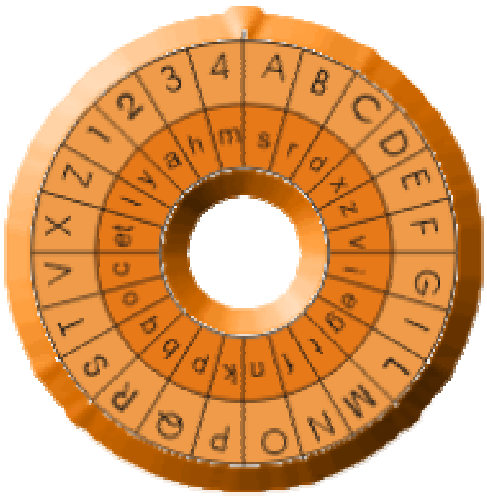


Disco dell'Alberti

Nuova rotazione casuale e cifratura della seconda parola:
Da = CETQ



Nuova rotazione e cifratura: Leon = DGZNF



Messaggio da Leon = YXHTTETSSRV CETQ DGZNF

L'unico neo consiste nel fatto che la sicurezza è affidata ad una chiave di cifratura di un solo carattere: sarebbe semplicissimo decifrare il messaggio anche senza sapere che la prima lettera di ogni parola è la chiave di cifratura, basterebbe provare per ogni parola le 24 posizioni del disco.

Per aumentare la segretezza (le lettere maiuscole costituiscono un aiuto non solo per il corrispondente ma anche per il "nemico") l'Alberti suggerisce di usare uno dei quattro numeri per segnalare il cambio di alfabeto; la lettera minuscola corrispondente al numero sarà la nuova chiave; non vi sono quindi più lettere maiuscole e la cifra risulta così molto più sicura, e decisamente superiore a quelle che la seguirono nel tempo, e in particolare alla fin troppo famosa Tavola di Vigénère. Si tratta in definitiva di una delle cifre polialfabetiche più sicure, che non ottenne il successo meritato anche per la decisione dell'Alberti di tenerla segreta (il suo trattato fu pubblicato solo un secolo più tardi a Venezia insieme ad altri suoi "opuscoli morali" e passò quasi inosservato).

Tale disco non ottenne successo anche per la decisione dell'Alberti di tenerlo segreto (il suo trattato fu pubblicato solo un secolo più tardi a Venezia insieme ad altri suoi "opuscoli morali" e passò quasi inosservato).

Il bresciano **Giovan Battista Bellaso** pubblicò tra il 1553 e il 1564 tre opere di crittologia contenenti alcuni cifrari polialfabetici di notevole interesse. L'idea su cui si basa il principale cifrario proposto dal Bellaso è quella di ricavare cinque alfabeti da una parola segreta convenuta. Le lettere dell' alfabeto vengono scritte in una tabella composta da due righe. In particolare quelle della parola segreta sono inserite nelle prime colonne intercalate sulle due righe e le rimanenti lettere dell'alfabeto vengono scritte di seguito. In questo modo si è ottenuto il primo alfabeto derivato. A partire da questo ricaviamo il secondo spostando circolarmente verso destra la seconda riga di una posizione. Applicando lo stesso procedimento al secondo alfabeto, si ricava il terzo alfabeto derivato e così via fino ad ottenerne cinque, ognuno dei quali sarà identificato da un gruppo di quattro lettere. Facendo riferimento sempre al primo alfabeto, le lettere della prima e della sesta colonna identificano il primo alfabeto derivato, quelle della seconda e della settima colonna identificano il secondo alfabeto derivato. In generale le quattro lettere che identificano l' i-esimo alfabeto sono quelle dell' i-esima e della (i + 5)-esima colonna. A questo punto si deve convenire una frase segreta; le lettere di quest' ultima servono a selezionare l' alfabeto da usare. In particolare,

presa l' i-esima lettera della parola segreta, si controlla quale dei cinque identificativi degli alfabeti la contiene. Si determina così l'alfabeto da usare per l' i-esima parola del testo in chiaro. Se il numero di lettere della frase segreta è minore del numero di parole del testo da cifrare, la frase segreta viene riapplicata ciclicamente per la selezione degli alfabeti. La cifratura si effettua sostituendo la lettera del testo in chiaro con la lettera che si trova sulla stessa colonna nell'alfabeto predeterminato.

Riportiamo a titolo di esempio il seguente: l'idea è quella di ricavare diversi alfabeti disordinati da una parola convenuta, versetto o motto (l'antenato diretto delle odierne password). Le lettere della parola segreta vengono scritte all'inizio a sinistra intercalate su due righe; le rimanenti lettere dell'alfabeto vengono scritte di seguito.

Un esempio dell'autore: data la parola chiave IOVE, il primo alfabeto derivato (alfabeto latino di 20 lettere posta V=U) è:

I O A B C D F G H L
V E M N P Q R S T X

Il secondo si ottiene spostando circolarmente la seconda riga:

I O A B C D F G H L
X V E M N P Q R S T

e così via fino ad ottenere cinque alfabeti; ognuno di questi sarà identificato da un gruppo di quattro lettere, come nella tabella a lato.

A questo punto si deve convenire un altro motto segreto, p.es OPTARE MELIORA; le lettere di quest'ultimo servono a selezionare l'alfabeto da usare.

Volendo allora cifrare la frase "Inviare truppe domani" si ha:

Chiave O P T

Chiaro I N V I A R E T R U P P E D O M A N I

Cifrato X C O X E G A A I C H H D M T D X F S

I D V Q	I O A B C D F G H L V E M N P Q R S T X
O F E R	I O A B C D F G H L X V E M N P Q R S T
A G M S	I O A B C D F G H L T X V E M N P Q R S
B H N T	I O A B C D F G H L S T X V E M N P Q R
C L P X	I O A B C D F G H L R S T X V E M N P Q

Le cifre del Bellaso sono più deboli di quella dell'Alberti perchè usano alfabeti invertiti e non del tutto arbitrari, mentre il cambio di lista non è segreto. Il Bellaso sembra comunque essere stato il primo crittologo moderno a proporre l'uso di parole chiave o versetti come chiavi di cifratura, un uso poi divenuto popolarissimo in crittografia, a partire dal cifrario di Vigenere.

Blaise de Vigenére pubblicò nel 1586 un trattato di cifrari nel quale proponeva tra gli altri un codice che ebbe grande fortuna e che è ricordato con il suo nome. Si tratta del più semplice codice di sostituzione polialfabetica, e proprio per la sua semplicità ha goduto per secoli di una grossa fama.

La forza del cifrario di Vigenére sta nell'utilizzare non uno ma 26 alfabeti cifranti per cifrare un solo messaggio. Il metodo si può considerare una generalizzazione del codice di Cesare; invece di

spostare sempre dello stesso numero di posti la lettera da cifrare, questa viene spostata di un numero di posti variabile, determinato dalle lettere della parola chiave, da concordarsi tra mittente e destinatario. La parola è detta chiave o verme, per il motivo che, essendo in genere molto più corta del messaggio, deve essere ripetuta molte volte. Di seguito viene riportata il cifrario utilizzato nei codici di Vigénère. Dal cifrario di Vigenere deriva peraltro il cifrario di Vernam, considerato il cifrario teoricamente perfetto. Il metodo si può considerare una generalizzazione del codice di Cesare; invece di spostare sempre dello stesso numero di posti la lettera da cifrare, questa viene spostata di un numero di posti variabile, determinato in base ad una parola chiave, da concordarsi tra mittente e destinatario, e da scriversi sotto il messaggio, carattere per carattere; la parola è detta verme, per il motivo che, essendo in genere molto più corta del messaggio, deve essere ripetuta molte volte sotto questo, come nel seguente esempio:

Testo chiaro - ARRIVANOIRINFORZI

Verme - VERMEVERMEVERMEVE

Testo cifrato - VVIUZVRFUVDRWAVUM

Il testo cifrato si ottiene spostando la lettera chiara di un numero fisso di caratteri, pari al numero ordinale della lettera corrispondente del verme. Di fatto si esegue una somma aritmetica tra l'ordinale del chiaro (A = 0, B = 1, C = 2 ...) e quello del verme; se si supera l'ultima lettera, la Z, si ricomincia dalla A, secondo la logica delle aritmetiche finite.

Per semplificare questa operazione il Vigénère propose l'uso della seguente tavola quadrata, composta da alfabeti ordinati spostati. Volendo ad esempio cifrare la prima **R** di ARRIVANO si individuerà la colonna della **R**, quindi si scenderà lungo la colonna fino alla riga corrispondente della corrispondente lettera del verme (qui **E**); la lettera trovata all'incrocio è la lettera cifrata (qui **V**); la seconda **R** invece sarà cifrata con la lettera trovata sulla riga della **R** di VERME, e cioé con la **I**.

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

Il vantaggio rispetto ai codici mono-alfabetici è evidente: la stessa lettera del testo chiaro non è sempre cifrata con la stessa lettera; e questo rende più difficile l'analisi statistica del testo cifrato e la decrittazione.

Chi riceve il messaggio per decifrarlo deve semplicemente usare il metodo inverso (sottrarre invece che sommare); riferendosi all'esempio di sopra si avrà:

Testo cifrato - VVIUZVRFUVDRWAVUM
Verme - VERMEVERMEVERMEVE
Testo chiaro - ARRIVANOIRINFORZI

si potrà decifrare la seconda **V** ricercandola nella riga della corrispondente lettera del verme, la **E**; la colonna dove si trova la **V** ha al primo posto in alto la lettera chiara, la **R**.

1.4 Conclusioni

Prima dell'avvento dei computers gli algoritmi crittografici erano "orientati al carattere" e consistevano fondamentalmente di due tecniche di base (anche combinate tra loro): la sostituzione di un carattere con un altro e la sostituzione di un carattere alla posizione x con un carattere alla posizione y. La sicurezza di un algoritmo crittografico basato su queste tecniche era direttamente proporzionale alla complessità di tali sostituzioni e, al contrario di quelli che sono i presupposti della crittografia moderna, tali algoritmi crittografici erano sicuri fino a quando l'algoritmo stesso rimaneva segreto.

1.5 Richiami

I **cifrari poligrafici** sono cifrari nei quali ogni lettera del testo viene dapprima scomposta in gruppi di due o più lettere o cifre che vengono poi a loro volta cifrate per sostituzione o per trasposizione. Da alcuni autori sono detti tomogrammici. Per contro i cifrari dove le lettere vengono cifrate ad una ad una si dicono **monografici**.

I ***cifrari*** **polialfabetici** si differenziano dai monoalfabetici in quanto un dato carattere del testo chiaro (p.es. la A) non viene cifrato sempre con lo stesso carattere, ma con caratteri diversi in base ad una qualche regola, in genere legata ad una parola segreta da concordare. In questo modo la sicurezza del codice dovrebbe aumentare in modo significativo; non è infatti non è più così semplice individuare le lettere del messaggio in base alla loro frequenza caratteristica di ogni lingua. Così per esempio la lettera E molto frequente in tutte le lingue non potrà più essere individuata grazie alla sua frequenza molto elevata. I **cifrari monoalfabetici** sono cifrari di sostituzione: del testo chiaro si sostituisce ogni carattere con un altro carattere (o numero) secondo una tabella prestabilita, ottenendo il testo cifrato.

Nulla: denominare un segno o un gruppo cifrante che non ha valore di lettera alfabetica nè di segno d'interpunzione, ma che si usa solo per alterare le frequenze relative delle lettere del testo.

2. Crittografia moderna, Jefferson e Lorenz

(curato da Daniele Salvi)

2.1 La crittografia dalla seconda metà del XIX secolo alla Grande Guerra

Dalla metà del XIX secolo l'uso della crittografia assume un ruolo determinante nella trasmissione di messaggi di carattere logistico e strategico. Con l'invenzione della radio i messaggi sono trasmessi anche via etere e quindi esposti molto più di prima all'intercettazione da parte del nemico; il ricorso alla crittografia diventa inevitabile, come la necessità di cifrari sempre più sofisticati. Una necessità che è ignorata in Italia dove si dovrà ottendere l'entrata in Guerra nel 1915 per rendersi conto del ritardo accumulato in campo crittografico, e porvi rimedio.
Tra i metodi usati nella Grande Guerra si possono ricordare i cifrari poligrafici:

- Playfair cipher (1854)
- Cifra campale germanica (1918)
- Il cifrario bifido di Delastelle

I cifrari poligrafici sono cifrari nei quali ogni lettera del testo viene dapprima scomposta in gruppi di due o più lettere o cifre che vengono poi a loro volta cifrate per sostituzione o per trasposizione. Da alcuni autori sono detti tomogrammici.
Per contro i cifrari dove le lettere vengono cifrate ad una ad una si dicono monografici.
Nell'Ottocento quando il principale mezzo di telecomunicazione era il telegrafo si usarono metodi basati sul *codice Morse*; venivano cifrati i punti e le linee di tale codice; di questo tipo è la *cifra Pollux.*
Altri cifrari fanno uso di una matrice quadrata nella quale vengono disposte venticinque lettere; la cifratura avviene cercando la lettera chiara nella matrice e associandole la coppia di numeri o lettere che identificano la riga e la colonna; questa coppia di cifre o lettere viene poi cifrata secondo regole più o meno complesse.
Il più antico esempio di sistema poligrafico è la *scacchiera di Polibio* che non era però un codice segreto ma piuttosto un sistema pensato per un telegrafo ottico. Molto più recenti sono il *Playfair Cypher, le cifre a scacchiera del Collon, la cifra campale germanica e il cifrario bifido di Delastelle*, tutti metodi piuttosto sicuri tanto da essere stati usati in tutte e due le guerre mondiali.
L'avvento del computer in questa seconda metà di secolo ha indebolito in modo radicale la sicurezza di questi metodi che sono ormai da considerare obsoleti.

- Cifrario Playfair

Il Playfair cipher fu inventato dal noto fisico Sir Charles Wheatstone (1802-1875), ma il nome di Playfair deriva da colui che ha divulgato nelle alte sfere governative questo metodo di cifratura. Lyon Playfair, barone di St.Andrews, mostrò per la prima volta questo sistema nel 1854 durante una cena organizzata da Lord Granville alla presenza di Lord Palmerton (1784-1865) allora ministro degli Esteri. La speranza di Playfair era quella di far utilizzare il Cipher durante la guerra di Crimea ma il sistema fu effettivamente utilizzato dall'esercito britannico solamente a partire dalla guerra Boera.

Il Cipher è ritenuto essere il primo metodo di cifratura a bigrammi.
Si usa una matrice 5 x 5 di 25 lettere che viene riempita nelle prime caselle con la parola chiave, abolendo le eventuali lettere ripetute, ed è completata con le rimanenti lettere nel loro ordine alfabetico. Si omette la W che, se necessario, potrà essere cifrata come una doppia V. Così, con la chiave computer, si otterrà la tabella a lato. L'unica lettera non presente è la Q, in quanto è la lettera che è quasi sempre seguita dalla U e quindi facilmente riconoscibile.

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

Combinato così il quadrato alfabetico di 25 caselle, la cifratura si farà tenendo conto delle regole che seguono.
Il testo in chiaro deve essere diviso in bigrammi di due lettere consecutive. Le due lettere si cercano sul quadrato e si sostituiscono con altre secondo le seguenti regole: se le due lettere chiare si trovano su una stessa riga, si prendono le due lettere che le seguono a destra; se una delle due lettere chiare si trova sulla quinta colonna a destra, si prenderà la prima lettera a sinistra della stessa riga. Se le due lettere chiare sono sulla stessa colonna, si prendono le due lettere sottostanti; se una lettera è nell'ultima riga, si prenderà la lettera che sta nella prima riga della stessa colonna; se le due lettere sono in colonne e righe diverse, si prendono le due che costituiscono un rettangolo con esse, cominciando da quella che si trova nella stessa riga della prima lettera del bigramma in chiaro; qualora il bigramma chiaro presenti due lettere uguali si cercherà di eliminare questo raddoppio, oppure di romperlo inserendo una lettera rara (k, w, x, y).
Prendendo la frase Inviare subito nuove truppe si otterrà la seguente successione di bigrammi (si noti che il raddoppio della lettera -p- è stato spezzato inserendo fra le due lettere la -y-):
IN VI AR ES UB IT ON UO VE TR UP YP E
Quindi, seguendo le regole succitate, il messaggio cifrato risultante sarà il seguente:
HQ ZF AB TK BI DB PK CM OF EA CU AY E
Questa cifra è abbastanza buona e comoda, presenta però un difetto: dato il modo di formazione del quadrato alfabetico, le lettere più frequenti della lingua si trovano sulle prime due linee, mentre quelle rare si trovano normalmente nell'ultima linea. Questo consente, in molti casi, di risalire al quadrato molto velocemente e quindi rende il messaggio facilmente decrittabile.

- Cifra campale germanica(1918)

Questo metodo di Crittografia fu usato dall'esercito tedesco nella Grande Guerra, a partire dagli inizi del 1918.
Il metodo utilizza una scacchiera simile a quella usata nel Playfair Cipher, e nel cifrario bifido di Delastelle; si sostituiscono le lettere con gruppi di due o più lettere, le quali vengono poi sottoposte a una trasposizione per la trasmissione. Si tratta quindi di un cifrario poligrafico.

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

La Cifra Campale Germanica usa, come componenti esterne alla scacchiera, lettere i cui segnali dell'alfabeto telegrafico Morse siano molto diversi tra loro (come ad esempio a, d, f, m, x) in modo da evitare errori di trasmissione radio.
Venivano usate due matrici. La prima, di 25 lettere, veniva riempita, con un procedimento simile a quello del Playfair Cipher, nelle prime caselle con la parola chiave, abolendo le eventuali lettere ripetute, ed era completata con le rimanenti lettere nel loro ordine alfabetico. Così, con la chiave alfabeto, eliminata la A che si ripete, si otterrà la tabella a lato.
Il messaggio da cifrare è: Comunicare posizione flotta.

Ora alle semplici lettere chiare vengono sostituiti bigrammi cifrati, leggendo le coordinate cartesiane nel quadrato, cioè le lettere che indicano la linea e la colonna in cui si trova la lettera da cifrare.
I bigrammi cifrati vengono poi sottoposti alla seguente trasposizione: sono innanzitutto inseriti ordinatamente nella seconda matrice, formata da una chiave mnemonica nella prima linea e da una chiave numerica nella seconda, le cui cifre corrispondono all'ordine alfabetico della lettera sovrastante.

V	E	N	E	Z	I	A
6	2	5	3	7	4	1
D	F	D	D	F	X	X
A	M	A	F	D	D	F
A	A	M	M	A	X	M
D	D	D	M	X	F	D
X	X	F	D	D	D	M
A	A	X	A	F	A	D
D	D	D	A	D	A	A
A						

Così con la chiave mnemonica Venezia si otterrà la tabella di trasposizione:
Leggendo ora per colonne a partire dalla colonna 1, il crittogramma da trasmettere sarà quindi:
XFMDMDA FMADXAD DFMMDAA XDXFDAA DAMDFXD DAADXADA FDAXDFD
Per decifrare bisogna prima di tutto scrivere il testo cifrato per colonne nella tabella di trasposizione secondo l'ordine della chiave e limitando prima il rettangolo in base al numero delle lettere del testo cifrato; quindi leggere per righe le successive coppie nella tabella di trasposizione, e quindi decifrare sulla scacchiera, con procedimento inverso a quello di cifratura.

- Il cifrario bifido di Delastelle

Il cifrario bifido di Delastelle è un cifrario poligrafico basato sulla matrice 5x5 usata per la prima volta nella scacchiera di Polibio e utilizzata anche dal Playfair Cipher e dalla cifra campale germanica.
Il metodo è dovuto a Félix-Marie Delastelle uno tra i massimi crittologi francesi del XIX secolo.
Il metodo si articola in tre passi:
Il messaggio chiaro viene spezzato in blocchi di cinque caratteri ciascuno; se l'ultimo blocco non è esattamente di cinque, gli ultimi posti sono riempiti di X.
Ogni lettera del blocco viene cifrata con due cifre e cioè con l'indice di riga e l'indice di colonna, che vengono scritte in verticale sotto la lettera chiara.
Le cifre vengono ora riscritte in orizzontale riga dopo riga ottenendo un messaggio con un numero di cifre doppio dell'originale.
A questo punto ogni coppia di numeri viene ritrasformata in lettera sempre secondo la matrice. Ne risulta il messaggio cifrato da trasmettere.
La matrice può essere quella semplice con le lettere dell'alfabeto ordinate (senza la W che può cifrarsi con una doppia V), oppure può essere ottenuta con una parola chiave come nel cifrario di Playfair.
Il Delastelle propose anche un cifrario trifido, che fa uso di una matrice tridimensionale 3x3x3, con 27 celle (ne avanza dunque una che può servire per lo spazio o per un carattere di controllo).

	1	2	3	4	5
5	S	V	X	Y	Z
2	T	E	R	A	B
3	D	F	G	H	I
4	J	K	L	N	Q

Come esempio si prenda la matrice ottenuta con la parola chiave COMPUTER, e si voglia cifrare il messaggio URGE INVIO RINFORZI che viene così composto e cifrato:
URGEI-NVIOR-INFOR-ZIXXX
12323 45312 34312 53555
53325 42523 54223 55333
Il messaggio in cifre viene ora raggruppato a due a due e riconvertito in

lettere, ottenendo così il messaggio cifrato:
12 32 35 33 25 45 31 24 25 23 34 31 25 42 23 53 55 55 53 33
O F I G B Q D A B R H D B K R X Z Z X G

2.2 Cifrario di Jefferson

Il cifrario di Jefferson prende il nome dal suo inventore Thomas Jefferson (1743-1826), uno degli autori della Dichiarazione d'Indipendenza e Presidente degli USA nel 1801-1804. Il codice è di facile utilizzo e può ancor oggi essere considerato abbastanza sicuro. Stranamente però Jefferson non lo mise mai in uso e il suo cifrario fu dimenticato fino al 1922, quando fu riscoperto e utilizzato, fino agli anni '50, dall'esercito statunitense. E nel 1890 Etienne Bazeries un crittologo francese propose l'Indecifrabile, un cifrario del tutto equivalente a quello di Jefferson.

Il codice di Jefferson è un metodo di cifratura meccanico basato su un cilindro di circa 15 cm di lunghezza e 4 cm di larghezza montato su un asse e sezionato in 36 dischi uguali (25 nella versione poi utilizzata dagli Americani, 20 nel cilindro di Bazeries). Sull'esterno di ciascuna ruota sono scritte le 26 lettere dell'alfabeto, equidistanti l'una dall'altra. L'ordine in cui sono disposte le varie lettere non corrisponde a quello naturale e varia da ruota a ruota.
Il messaggio in chiaro deve essere cifrato a blocchi di 36 lettere ciascuno (qualora l'ultimo blocco presenti meno di 36 lettere, esso deve essere completato con lettere nulle); la chiave di cifra è un numero che va da 1 a 25. Supponendo che il testo chiaro sia La missione in Polinesia è fallita e la chiave sia il numero 5, in una certa riga, non importa quale, si comporrà il messaggio in chiaro (omettendo naturalmente gli spazi); il crittogramma corrispondente andrà letto sulla quinta riga sopra quella che contiene il blocco in chiaro.

cifrato ->	5	GKRPXAFYEQYFUUAXYYEPSQYFTAELCIXVFCKZ
	4	HJQOWBHXDPXETRZYAZDORPXESZDMBHWUEBHX
	3	IBPNVCQWBOWDSQYZPACNQPWDRYCNZGVTDAGW
	2	JNOMUDLTHNVCRPXAIBBMPNVCQWBOYFUSAZFU
	1	KONLTHNVCABVNTHNVCALNVCLHXDPXETRZYDP
chiaro ->		LAMISSIONEINPOLINESIAEFALLITAXXXXXXX

La decifratura avviene con il procedimento inverso; si compone il messaggio e si legge il testo chiaro nella quinta riga sotto. Il destinatario, bastava che montasse le ruote nel cilindro usando la sequenza chiave fornita, e che ruotasse tali ruote singolarmente in modo da formare una riga con i primi 36 caratteri del messaggio cifrato. Mantenendo ora questo allineamento, analizzava cosa era scritto sulle altre 25 righe, fino a trovarne una che contenesse una frase sensata. La trascriveva e continuava a decrittare il resto del messaggio con lo stesso sistema.
Volendo poteva anche essere convenuta la distanza dalla riga composta, rispetto a quella cifrata, in modo da non doverle osservare tutte e 25 in fase di decrittazione, ma sicuramente usando la scelta casuale della riga si aumentava la sicurezza, dato che l'alfabeto di crittazione è in questo modo diverso ogni 36 caratteri all'interno dello stesso messaggio ed un crittoanalista si trova così a dover fronteggiare un nuovo sisitema di cifratura ogni 36 caratteri, invece di avere a disposizione tutto l'intero testo del messaggio.

In pratica la chiave di questo metodo è duplice: 1) un numero segreto compreso tra 1 e 25 e 2) la struttura del cilindro. Considerato che ogni ruota ha una permutazione di 26 caratteri e le permutazioni sono 26! (circa 4x1026) il numero di chiavi possibili è dell'ordine di 10 26xN, dove N è il numero di ruote, che è un numero enorme. Il livello di sicurezza è quindi molto elevato, ma con un grosso rischio: se il cilindro cade nelle mani del nemico, restano solo 25 chiavi possibili e il crittogramma può essere facilmente forzato come un cifrario di Cesare.
Il dispositivo inventato da Thomas Jefferson, allora segretario di stato, divenuto in seguito terzo presidente degli Stati Uniti, non può lasciare indifferenti gli interessati ai sistemi di crittografia: si tratta del primo esempio di una serie di macchine cifranti basate su cilindri e dischi ruotanti intorno ad un asse, la più celebre di tutte è la cosiddetta Macchina Enigma usata dai Tedeschi nella Seconda Guerra Mondiale.

Analisi:
In altre parole, il rullo altro non è che un sistema polialfabetico a sostituzione, dove:
la chiave di cifratura è composta, per ogni riga, da un alfabeto casuale (pero` solo se si usa il metodo di prelevare una riga casuale del cilindro, viceversa è fissa per tutto il messaggio).
la chiave di cifratura globale è composta dalla sequenza di inserimento delle ruote nell'asse del cilindro.
Questo sistema permette di avere una discreta sicurezza. Prendiamo in esame solo le possibilità di inserimento dei vari dischi nell'apposito asse. Riportiamo le possibilità di combinazione che si hanno in base al numero di dischi usati:

Dischi	Combinazioni
1	1
2	2
3	6
4	24
5	120
6	720
7	5040
8	40320
9	362880
10	3628800
11	39916800
12	479001600
13	6227020800
14	8.7 * 10^10
15	1.3 * 10^12
16	2.09 * 10^13
17	3.5 * 10^14
18	6.4 * 10^15
19	1.2 * 10^17
20	2.4 * 10^18
21	5.1 * 10^19
22	1.12 * 10^21
23	2.5 * 10^22
24	6.2 * 10^23
25	1.5 * 10^25
26	4.03 * 10^26
27	1.08 * 10^28
28	3.04 * 10^29
29	8.8 * 10^30
30	2.6 * 10^32
31	8.2 * 10^33
32	2.6 * 10^35
33	8.6 * 10^36
34	2.9 * 10^38
35	1.03 * 10^40
36	3.7199332 * 10^41

Il dispositivo di Jefferson, anche se nelle mani del nemico, offriva comunque una protezione di rilievo, data dall'enorme quantità di combinazioni possibili per l'assemblamento del cilindro (371 seguito da 39 zeri). Non disponendo neanche del cilindro e quindi non conoscendo la composizione di ogni singola ruota, andrebbero aggiunte alle miliardi di possibilità di assemblamento, anche tutte le possibili combinazioni date dalla disposizione casuale dei caratteri su ogni singola ruota!

Nota per programmatori:
Mentre negli utilizzi militari sono segreti anche i dispositivi che generano un messaggio, uno sviluppatore crea un software che sarà sicuramente venduto e disponibile a tutti. E` quindi bene tenere sempre a mente il concetto esposto da Kerckoffs, secondo il quale un sistema deve mantenere la sua impenetrabilità anche se l'avversario conosce nei dettagli il modo in cui il sistema si applica, purché non sia a conoscenza della chiave usata. In altre parole non è il metodo usato a dover fare la parte del leone, quanto l'impossibilità di decrittazione senza la conoscenza della chiave.

2.2 Crittografia nella I GM

La I guerra mondiale è la prima grande guerra dopo l'invenzione del telefono e della radio; questi mezzi di comunicazione se da una parte consentono una velocità di trasmissione dei messaggi praticamente istantanea, dall'altra sono irrimediabilmente esposti all'intercettazione da parte del nemico, e questo vale soprattutto per le comunicazioni radio. Catturare il corriere che recava un messaggio importante era impresa difficile e occasionale, intercettare una trasmissione radio, una volta installata una stazione di intercettazione è un gioco da ragazzi.
I primi a rendersi conto di questa nuova situazione furono i Francesi che allo scoppio della guerra disponevano già di un ben organizzato ed efficiente ufficio cifra presso il gran quartier generale dell'esercito. E sin dall'ottobre 1914 i crittanalisti francesi guidati dal Col. Cartier e dal Cap.Olivari erano in grado di decrittare i messaggi radio tedeschi. Ma il migliore crittanalista francese era un professore di paleontologia *Georges Painvin* che riuscì a decrittare la cifra campale germanica nel 1918.
Altrettanto ben preparati gli Austriaci: già nell'agosto 1914 i crittanalisti asburgici riuscivano a decrittare i radiomessaggi russi che per la verità erano solo in parte cifrati; anche quando i russi cominciarono a cifrare i loro messaggi radio il cap. Pokorny riuscì nel giro di pochi giorni a decrittarli nuovamente.
Negli altri paesi veri e propri uffici cifra furono organizzati solo dopo l'entrata in guerra.
Assolutamente impreparati erano soprattutto i Russi che all'inizio della guerra non si preoccupavano neanche di cifrare i loro messaggi radio, come avvenne durante la battaglia di Tannenberg nell'agosto 1914 quando persino gli ordini operativi venivano trasmessi in chiaro; un formidabile regalo ai Tedeschi che intercettavano tutto.
I Tedeschi comunque riuscirono a decrittare i messaggi russi anche dopo che questi ultimi iniziarono a cifrare le loro comunicazioni radio; qualche successo lo ottennero anche nei confronti dei Francesi; il principale crittanalista tedesco fu il prof. Deubner.
Capo dell'ufficio crittologico della Marina Britannica era Sir Alfred Ewing che organizzò la cosiddetta Room 40 (dal numero della sua stanza negli uffici dell'ammiragliato) dove si decrittavano migliaia di radiomessaggi della marina tedesca. Il più noto di questi messaggi fu il "telegramma Zimmermann" con il quale i Tedeschi offrivano un'alleanza ai Messicani in chiave anti-USA. Letto al Congresso degli Stati Uniti questo messaggio fu uno dei fattori che spinsero gli USA a entrare in guerra nel 1917.
Negli USA non esistendo un Ufficio Cifra federale fu promosso a tale rango il reparto crittologico dei laboratori Riverbanks di Chicago una fondazione privata di ricerca nella quale lavorava anche *William Friedmann* destinato a divenire il massimo crittologo e crittanalista USA.

Del tutto impreparati in campo crittologico erano gli Italiani che dovettero in un primo tempo appoggiarsi all'ufficio cifra francese; solo in un secondo tempo fu costituito un ufficio cifra autonomo sotto la guida di *Luigi Sacco*. All'inizio del XX secolo la crittografia in Italia, che pure vantava tradizioni di tutto rispetto (L.B.Alberti, Bellaso, Porta), aveva toccato uno dei suoi livelli più bassi; basti pensare che era ancora in uso il cifrario militare tascabile, una variante della *tavola di Vigenere* di cui da tempo era noto un metodo di decrittazione (quello del Kasiski).
All'inizio della Grande Guerra la stazione radiotelegrafica di Codroipo era in grado di intercettare i messaggi austriaci ma non di decrittarli, poichè l'Esercito Italiano non disponeva di un Ufficio Cifra! Per rimediare il Comando Supremo inviò nel luglio 1915 il cap. Sacco, comandante della stazione di Codroipo, in Francia presso il gran quartier generale di Chantilly, per cercare l'aiuto del ben organizzato ufficio cifra francese. All'inizio del 1916 il Sacco fu messo a capo di un servizio di intercettazione radio che doveva ancora passare ai Francesi i messaggi perchè fossero decrittati. Ma la collaborazione con i Francesi si rivelò insoddisfacente; i crittanalisti d'oltralpe riuscivano a decrittare molti messaggi austriaci, ma rifiutarono sempre di istruire gli Italiani sui loro metodi. Irritato da questa situazione il Sacco propose al suo superiore gen. Marchetti di creare un Ufficio Crittografico autonomo ("Se i Francesi sono riusciti in questa impresa, non vedo perchè non dovremmo riuscirci anche noi"); fu preso in parola, e incaricato di organizzare tale Ufficio.
Sotto la guida del Sacco e dei suoi collaboratori Tullio Cristofolini, Mario Franzotti, e Remo Fedi, furono forzati il cifrario campale austriaco, quello diplomatico, e quello navale. Furono forzati anche alcuni cifrari tedeschi in uso nei Balcani, p.es. il crittogramma relativo al viaggio del gen. Falkenhayn in Grecia nel gennaio 1917, episodio ricordato dal Sacco nel suo manuale di Crittografia.
Paradossalmente però ci volle la disfatta di Caporetto nel 1917 perché il Sacco riuscisse a convincere gli alti comandi italiani ad abbandonare i vecchi cifrari, che come poi si seppe venivano facilmente decrittati dagli austriaci, e di adottare quei nuovi più sicuri sistemi che avevano fino allora rifiutato perchè *troppo complicati*! Unica attenuante per questa incredibile leggerezza il fatto che gli alti comandi italiani, a differenza di quelli di altri paesi, evitarono sempre di trasmettere per radio i messaggi più importanti.
La possibilità di intercettare e decrittare i messaggi austriaci ebbe un'importanza non trascurabile nel 1918, per fronteggiare l'offensiva austriaca del Piave.
In definitiva fu proprio la Grande Guerra a far scoprire a molti Stati l'importanza della Crittografia, il cui ruolo diventerà assolutamente fondamentale nella II guerra mondiale.

Cifrario di Vernam

Nel 1917 Gilbert Vernam, impiegato della compagnia AT&T, inventò un ingegnosissimo sistema di protezione crittografica, per comunicazioni su telegrafo, dei testi codificati in binario. Egli costruì per prima cosa un dispositivo in grado di leggere contemporaneamente due nastri in input e generare a partire da essi un nastro di output tale che ciascun foro fosse generato mediante uno XOR dei due corrispondenti fori sui nastri input. Dopodiché prese un nastro su cui era perforata una sequenza di caratteri casuale ed un nastro su cui era perforato un testo reale e li passò nella sua macchina. Il risultato fu un nastro completamente inintellegibile, ovvero cifrato.
Lo schema di crittografia di Vernam è uno schema one-time pad; un tale schema richiede che :

- la chiave sia usata una sola volta (da qui il nome);
- deve essere lunga almeno quanto il testo in chiaro;
- fra i bit che compongono la chiave non deve esserci alcuna relazione;
- la chiave deve essere generata casualmente.

In pratica se il testo in chiaro è X = 0110 e la chiave è K = 1100, applicando il metodo di Vernam si ottiene il seguente testo cifrato :

$$Y = X \oplus K = 1010$$

la decifratura si ottiene nel seguente modo:

$$X = Y \oplus K = 0110$$

Notiamo che è stata applicata la stessa chiave ed è stata effettuata la stessa operazione sia per la cifratura che per la decifratura, ciò caratterizza un sistema crittografico reversibile, questo è uno dei molti aspetti notevoli del cifrario di Vernam. Per ciò che concerne la sicurezza, a tutt'oggi, questo è l'unico metodo ad essere perfetto, ossia costituisce un cifrario assolutamente indecifrabile in senso stretto.
Un cifrario si dice perfetto se, dati X il testo in chiaro e Y il cifrato corrispondente, gode della seguente proprietà:
per ogni X'e Y' risulta :
$Pr (X = X') = Pr (X = X' | Y = Y')$
La proprietà di cui sopra si chiama sicurezza perfetta. Per un cifrario che gode della sicurezza perfetta, l'indecisione nello stabilire qual è il testo in chiaro X senza conoscere il testo cifrato Y è la stessa che si ha su X conoscendo il testo cifrato Y.
Le proprietà che caratterizzano l'one-time pad sono estremamente restrittive, volendole rispettare si ottiene un sistema scomodo da usare in pratica, considerando che le ingombranti chiavi andrebbero generate in anticipo rispetto al loro uso previsto, e conservate in luogo sicuro. Sono questi i motivi per cui questo sistema non viene usato che per casi eccezionali, come la famosa hot-line tra Washington e Mosca.
Un'altro problema è che l'one-time pad è modificabile; un intruso può cambiare Y così che il messaggio M decifrato sia differente dal messaggio spedito. Non ci sono modi per il destinatario di controllare che il mittente abbia spedito proprio il messaggio ricevuto. Ci sono delle varianti che possono evitare di utilizzare delle chiavi così grandi, ma che fanno perdere la perfezione al sistema perché introducono delle dipendenze statistiche. Un esempio è quello di prendere una chiave in un grosso testo, come la Bibbia, specificando un punto di inizio qualunque, tutti i caratteri da quel punto in poi, formeranno la chiave. La dipendenza statistica è insita proprio nel fatto che le parole devono avere senso compiuto. La difficoltà per i crittoanalisti, oltre alla conoscenza della chiave (punto di inizio nel testo), sta anche nel capire qual è il testo utilizzato.
Il problema con le chiavi corte, che dunque devono essere riutilizzate ciclicamente nel corso del messaggio, è che producono, in uscita, delle regolarità statistiche che possono essere usate dai crittoanalisti per forzare il cifrario.

Il cifrario di Vigenere ha il suo tallone d'Achille nel fatto di essere un insieme di cifrari di Cesare intercalati a distanza fissa, cosa che ne rende possibile e anzi molto facile la crittanalisi, tanto più se la chiave è breve.
Ben diversa sarebbe però la situazione se la chiave avesse lunghezza infinita o, che in fondo è lo stesso, fosse lunga come il testo chiaro (o meglio come la somma di tutti i testi chiari).
È questa l'idea proposta da G.S.Vernam nel 1926; come già spiegato viene generata una chiave del tutto casuale, e dunque imprevedibile, lunga come il testo; a questo punto il chiaro e la chiave vengono "sommati" proprio come nel cifrario di Vigenere. L'unica differenza è che nel Vernam si sommano non tanto gli ordinali delle lettere da cifrare ma i singoli bit che codificano la lettera nei codici usati nelle telecomunicazioni (allora il codice Baudot, oggi il codice ASCII) con l'operazione logica XOR. Questa è simile all'addizione, ma ha il vantaggio di essere reversibile, e quindi verrà usata anche per decifrare.
In tal modo la debolezza del Vigenere è superata e anzi Claude Shannon, il padre della Teoria dell'Informazione, ha dimostrato nel 1949 che ogni cifrario "teoricamente sicuro" è un cifrario di Vernam (e viceversa). Infatti se la chiave è totalmente casuale e lunga come il testo allora il testo cifrato non contiene alcuna informazione sul testo chiaro, ed è del tutto al sicuro dagli attacchi della crittanalisi statistica.
Per avere una sicurezza assoluta non si dovrebbe mai riutilizzare la stessa chiave; se si utilizza più volte la stessa chiave infatti questa torna ad essere più breve del messaggio, o meglio della somma

di tutti i messaggi e il cifrario non è più perfetto. Per questo motivo questo tipo di cifrario viene detto a chiave non riutilizzabile.

Addizione di caratteri con il codice Baudot	
chiaro c	A T T E N Z I O N E 11000 00001 00001 10000 00110 10001 01100 00011 00110 10000
verme v	W I A P F I L K M S 11001 01100 11000 01101 10110 01100 01001 11110 00111 10100
cifrato c XOR v	00001 01101 11001 11101 10000 11101 00101 11101 00001 00100 T P W Q E Q H Q T {sp}

Perché allora non usiamo tutti questo cifrario? Il problema è che la chiave lunga come il testo deve essere preventivamente comunicata al destinatario in modo sicuro e ... qui il gatto si morde la coda, visto che non sempre è disponibile un canale sicuro di comunicazione.
I due corrispondenti dovrebbero incontrarsi periodicamente in luogo sicuro e generare una sequenza casuale lunghissima, sufficiente per un gran numero di messaggi, da utilizzare un po' alla volta. Una volta esaurita la chiave dovranno incontrarsi di nuovo, rigenerare la chiave etc.etc.
Per semplificare le cose si potrebbe pensare di generare la chiave in modo pseudo-casuale, secondo una qualche regola nota e riproducibile dal destinatario; questa idea diede luogo nel periodo tra le due guerre mondiali a una generazione di macchine cifranti, tra le quali la macchina Lorenz usata dai tedeschi nella II guerra mondiale. Ma così il cifrario non è più assolutamente sicuro, perché la chiave non è più realmente lunga come il testo, la vera chiave è la regola generatrice!. Tanto è vero che la macchina Lorenz fu forzata dagli inglesi sin dal 1941.
Nonostanti queste difficoltà il cifrario di Vernam sembra sia stato usato effettivamente negli anni della guerra fredda dai servizi segreti dell'Est e per il telefono rosso tra Washington e Mosca. Un cifrario di Vernam era anche quello trovato addosso al Che Guevara dopo la sua uccisione nel 1967.
Crittografia nella II GM

Forse in nessun altra guerra come nella II guerra mondiale la Crittografia ha svolto un ruolo di primo piano.
Gli storici potranno discutere a lungo su quanto sia stata importante per la vittora finale la superiorità alleata in questo campo; non c'è
comunque dubbio che questa superiorità sia stata schiacciante fin dai primi anni di guerra.

Il caso più noto è certo quello della macchina Enigma, usata dai tedeschi e considerata a torto inattaccabile; solo molti anni dopo la fine della guerra si seppe che in effetti già nel 1932, prima ancora che Hitler arrivasse al potere, l'ufficio cifra polacco aveva trovato il modo di forzare l'Enigma. E durante la guerra gli inglesi del progetto ULTRA continuarono a forzare sistematicamente i messaggi cifrati con l'Enigma e dal 1941 anche quelli cifrati con la più sofisticata macchina Lorenz.
Quante vittorie alleate avevano alla base questa superiorità crittografica? Difficile dare una risposta precisa, più semplice citare un paio di casi ben noti:

- Battaglia di capo Matapan: la disfatta della flotta italiana (marzo 1941) pare abbia avuto origine dal fatto che gli inglesi avevano decrittato alcuni messaggi cifrati della marina tedesca che fornivano l'esatta posizione della flotta italiana.
- Sbarco in Normandia: Eisenhower e Montgomery erano in grado di leggere tutti i messaggi degli alti comandi tedeschi, che usavano la macchina Lorenz; ebbero così conferma che Hitler aveva creduto alla falsa notizia di un imminente sbarco alleato nei pressi di Calais, e

aveva concentrato le sue migliori truppe in quella zona. Poterono quindi ordinare lo sbarco in Normandia sicuri che avrebbe incontrato ben poca resistenza.

Anche sul fronte del Pacifico gli Americani sin dal 1940, un anno prima di Pearl Harbour, avevano realizzato Magic una macchina in grado di decrittare i messaggi giapponesi cifrati con la macchina Purple. Ricordiamo due episodi certi e uno dubbio:

- Battaglia delle Midway: l'ammiraglio Isoroku Yamamoto, comandante supremo della flotta giapponese, nel maggio 1942 aveva preparato un piano per attaccare a sorpresa le isole Midway a est delle Haway, determinato com'era a infliggere una serie di duri colpi iniziali agli USA prima che la superiorità economica-industriale americana avesse il sopravvento. Ma grazie a Magic gli Americani intercettarono i piani di Yamamoto e l'Ammiraglio Nimitz, comandante della flotta USA, fu in grado di preparare la battaglia conoscendo già fin nei dettagli i piani del nemico; fece inoltre trasmettere falsi piani americani usando un cifrario che sapeva essere stato forzato dai giapponesi. L'effetto sorpresa si trasformò in un boomerang e la vittoria USA alle Midway fu quindi in buona parte dovuta alla superiorità crittologica.
- Morte dell'Amm. Yamamoto: il 14 Apr 1943 fu decrittato un messaggio che diceva che l'ammiraglio Yamamoto avrebbe visitato l'isola di Bougainville il 18 e specificava persino le ore di partenza e di arrivo e il tipo di aerei usati. L'ammiraglio Nimitz subito informato, dopo aver sentito il Presidente Roosevelt, organizzò una squadra di aerei P-38 che il 18 puntualmente intercettò e abbattè l'aereo di Yamamoto; i giapponesi persero così il loro uomo più prezioso. La morte di Yamamoto fu peraltro presentata come dovuta a un incidente e solo dopo molti anni furono rivelati i dettagli dell'episodio.
- Pearl Harbour: Gore Vidal, il noto scrittore americano, sostiene, e con lui diversi storici, che gli Americani, grazie a Magic, sapevano in anticipo anche dell'attacco di Pearl Harbour e decisero di non impedirlo; avevano infatti bisogno di un motivo forte per convincere la riluttante opinione pubblica americana della necessità di entrare in guerra e quell'attacco a tradimento dei Giapponesi fu ideale per questo scopo. Una teoria più prudente sostiene che gli Americani sapevano che il Giappone stava per attaccare, ma non sapevano dove. Certo è che al momento dell'attacco nella baia di Pearl Harbour non c'era nemmeno una portaerei e in definitiva furono affondate solo alcune navi vecchie e di importanza non fondamentale per la guerra.

E alla fine della guerra il gen. Marshall ammise che in molti casi di importanza "non vitale" gli alleati dovettero fingere di non conoscere i messaggi cifrati nemici, anche al costo di perdite umane, tale era il timore che tedeschi e giapponesi si accorgessero che i loro cifrari venivano sistematicamente decrittati.

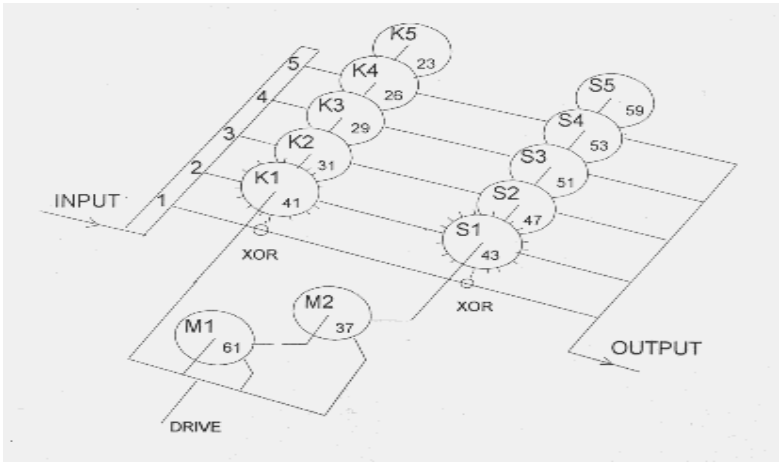
Anche l'attacco di Pearl Harbour va dunque annoverato tra questi casi? Se è così, è però ben difficile che la cosa possa mai essere confermata ufficialmente, considerato che in quell'occasione morirono circa 3000 cittadini americani.

Per quanto riguarda l'Italia non si ripeterono i successi della Grande Guerra; il gen.Sacco protagonista di quei successi, aveva per la verità progettato una macchina cifrante piuttosto complessa, un prototipo di questa era stato costruito dalle officine Nistri, ma per motivi non ben chiariti la macchina andò distrutta e non venne quindi mai usata; un episodio che ben si inserisce nell'andamento disastroso della guerra per l'Italia.

Un successo sia pur temporaneo e di natura più spionistica che crittanalitica, lo si ebbe nel 1941 quando il servizio segreto italiano riuscì a trafugare dall'ambasciata americana a Roma il cifrario "Black". Grazie a questa impresa italiani e tedeschi riuscirono per qualche tempo a decrittare i messaggi americani nel Nord Africa; e sembra che molti dei successi di Rommel fossero dovuti a queste intercettazioni; quando nel 1942 gli alleati scoprirono che i loro messaggi venivano forzati, il cifrario "Black" fu abbandonato e sostituito con la ben più sicura macchina M-138. E, che sia stato un caso o no, finirono anche i successi di Rommel in Africa.

2.3 Macchina di Lorenz

È ben noto anche fuori degli ambienti specializzati che durante la II guerra mondiale i tedeschi si affidarono per lo più alla macchina Enigma, e che questa fu forzata prima dai polacchi e poi dagli inglesi.
Meno noto è che i tedeschi usarono anche altri cifrari durante la guerra; in particolare gli alti comandi tedeschi, usarono una macchina telescrivente realizzata dalla ditta Lorenz che a differenza dell'Enigma usava 32 caratteri codificati con il codice Baudot(vedi paragrafo seguente), che era già un codice binario, nel senso che ogni carattere era codificato con 5 bit (0 o 1); la macchina si ispirava direttamente al cifrario di Vernam, considerato il cifrario perfetto.
Secondo le idee base del Vernam ogni carattere del messaggio era scomposto nei suoi 5 bit, che venivano sommati in modo binario (in pratica con un connettivo XOR) con i bit del corrispondente caratterre della chiave (detta anche sequenza oscurante).
Secondo Vernam la chiave dovrebbe essere indefinitamente lunga e del tutto casuale; a queste condizioni il Vernam è inattaccabile, ma c'è la grossa difficoltà di comunicare in modo sicuro la chiave al corrispondente. I progettisti della Lorenz pensarono di sostituire la chiave casuale con una chiave pseudo-casuale generata da un dispositivo meccanico (dodici rotori) secondo una procedura ovviamente segreta.



Struttura della macchina di Lorenz

In questo modo però il cifrario non è più inattaccabile e così fu per la macchina Lorenz che fu forzata dai crittanalisti inglesi del progetto Ultra, grazie anche a una grossa ingenuità di un cifratore tedesco; e proprio per decrittare più velocemente i cifrati Lorenz, nel 1943 nacquero i Colossi che possono considerarsi i primi veri calcolatori elettronici della storia, due anni prima dell'americano ENIAC.
I crittanalisti inglesi del progetto Ultra a Bletchley Park dopo aver forzato la macchina Enigma riuscirono anche a forzare come già accennato la macchina Lorenz usata dagli alti comandi tedeschi, e quindi di importanza ancor maggiore dell'Enigma.
Il primo successo si ebbe grazie a una grossa ingenuità di un cifratore tedesco il 30 ago 1941; questi aveva appena trasmesso un messaggio in cifra da Vienna ad Atene, quando ricevette la richiesta di ripetere il messaggio perchè non era stato ricevuto bene; il cifratore, forse per pigrizia o forse per impazienza, invece di ritrasmettere lo stesso messaggio identico, lo ritrasmise con alcune abbreviazioni (primo grave errore), dopo aver riposizionato i rotori della macchina alla stessa posizione del messaggio precedente (ancor più grave errore). Così il primo messaggio iniziava con

la parola Spruchnummer, il secondo con Spruchnr. (Spruchnummer vuol dire numero del messaggio)
Una vera manna per gli inglesi che avevano intercettato entrambi i messaggi e notato che i primi caratteri erano uguali; fu il crittoanalista John Tiltman che con un paziente lavoro riuscì alla fine a ricostruire la sequenza oscurante della Lorenz e quindi il messaggio chiaro.
Una volta ricostruita una sequenza oscurante era necessario comprendere la regola pseudo-casuale che la generava per poter rendere sistematica la decrittazione dei cifrati Lorenz; fu il chimico Bill Totte a completare questo lavoro arrivando a ricostruire completamente la struttura interna della Lorenz, che gli inglesi chiamavano in codice Tunny.
Ma decrittare a mano un cifrato Lorenz richiedeva un lavoro lungo 4-6 settimane, un tempo eccessivo in tempo di guerra. I messaggi decrittati erano spesso superati dagli eventi e di fatto inutili.
Per velocizzare le cose fu dapprima costruita una macchina elettromeccanica la Heath Robinson che però aveva problemi a mantenere la velocità di elaborazione necessaria.
Fu all'inizio del 1943 che il matematico Max Newman e l'ingegnere del Post Office Tommy Flowers ebbero l'idea di simulare le parti meccaniche con circuiti elettronici e iniziarono il progetto del Colosso, un vero e proprio calcolatore elettronico, capace di forzare la Lorenz in poche ore. Il primo Colosso, il Mark 1, fu assemblato alla fine del 1943 e pienamente operativo all'inizio del 1944. Il Colosso leggeva il testo cifrato secondo il codice Baudot, con un lettore ottico di nastri perforati alla rimarchevole velocità di 5000 caratteri al secondo.
Il testo così letto veniva confrontato con la struttura dei rotori della Lorenz alla ricerca di alcuni schemi caratteristici di questa macchina. Il testo cifrato doveva essere letto anche molte volte fino al momento in cui veniva forzato.
In pratica il Colosso applicava il metodo escogitato da Bill Tutte rendendolo molto più veloce; un cifrato che per essere forzato a mano richiedeva piu' di un mese di lavoro, veniva forzato dal Colosso in poche ore.
Da quando il primo Colosso divenne operativo(1944) acquistò grande importanza perché si stava preparando lo sbarco alleato in Francia. I messaggi decrittati mostrarono infatti agli alleati che Hitler aveva preso per buone le false notizie fatte trapelare su uno sbarco alleato a Calais, aveva concentrato le truppe in Belgio e che quindi lo sbarco in Normandia non avrebbe incontrato grossi ostacoli.
Dopo il primo furono costruiti altri nove Colossi; e nell'ultimo anno di guerra, grazie anche al fatto che gli alleati avevano sistematicamente bombardato e danneggiato le linee telefoniche tedesche costringendo i tedeschi a usare sempre di più le comunicazioni radio, quasi tutti i messaggi cifrati tedeschi venivano decrittati fornendo un vantaggio formidabile ai comandanti alleati.
Alla fine della guerra ben 63 milioni di caratteri cifrati tedeschi erano stati decrittati dai Colossi!
I Colossi furono distrutti alla fine della guerra, e solo nel 1996 ne fu ricostruito uno nel museo di Bletchley Park.
In definitiva il Colosso deve essere considerato il primo vero calcolatore elettronico della storia, precedendo di più di un anno l'americano ENIAC che viene in genere presentato come il primo computer.
Fatto è che la costruzione del Colosso era ovviamente uno dei segreti più gelosamente custoditi dai servizi segreti inglesi, e solo negli anni '70 la storia dei Colossi fu resa di pubblico dominio.
Un'ultima nota sul Colosso; contrariamente a quello che si legge su molti libri e siti web il Colosso non ha niente a che fare con la disfatta della Macchina Enigma che richiese piuttosto le Bombe dispositivi elettromeccanici molto più semplici. Il Colosso era un computer specificamente progettato per forzare la macchina Lorenz e solo per quello.

2.4 Codice Baudot

Meno noto del codice Morse, il codice Baudot fu inventato nel 1870 dal francese Emile Baudot e venne usato ampiamente nei decenni successivi per le comunicazioni telegrafiche e soprattutto per le telescriventi.
Si tratta di un codice di 32 caratteri che in qualche modo precorre gli attuali codici informatici come il codice ASCII. Ogni carattere è infatti codificato con 5 bit (o cifre binarie 0, 1), con un totale di 25 = 32 caratteri possibili; in effetti questo numero viene ad essere quasi raddoppiato con un trucco simile a quello usato dalle tastiere: ogni combinazione di bit può infatti avere due significati, il primo come lettera dell'alfabeto, il secondo come cifra o carattere speciale. Per passare da una serie all'altra vengono usati due caratteri speciali il 27 per passare da lettera a cifra, il 31 per passare da cifra a lettera.
Come si vede nella tabella a lato oltre a lettere e cifra compaiono nel codice Baudot anche alcuni codici di controllo, come {cr} che sta per carriage return [ritorno carrello] o {lf} = line feed [avanzamento linea].
Diversi cifrari nati tra le due guerre mondiali furono esplicitamente progettati in funzione del codice Baudot; così fu per il cifrario Vernam e per le macchine cifranti che realizzavano uno pseudo-Vernam come la tedesca macchina Lorenz.

3. ENIGMA E BOMBE DI TURING (curato da Daniele Lozzi)

3.1 Introduzione

Enigma era una macchina cifratrice utilizzata dal Terzo Reich negli anni precedenti e durante la Seconda Guerra Mondiale. Lo scopo per cui questa apparecchiatura era concepita era quello di rendere il più possibile sicure le comunicazioni il cui contenuto era importante tenere segreto. La macchina Enigma veniva utilizzata per "mascherare" un messaggio che un operatore telegrafico mandava ad un altro in modo che chiunque intercettasse tale messaggio non fosse in grado di sapere che cosa il messaggio stesso diceva. Quando un operatore utilizzava la macchina, egli digitava le lettere che costituivano il messaggio sulla tastiera della macchina e i meccanismi interni della stessa trasformavano quel testo in un altro apparentemente incomprensibile. La chiave di lettura era l'utilizzo della stessa macchina, opportunamente assettata, da parte di chi riceveva il messaggio cifrato.

Di seguito è presentata una breve storia dell'evoluzione della macchina cifratrice tedesca nota col nome di Enigma e di come crittoanalisti di tutto il mondo si siano impegnati a decifrare i suoi messaggi. Dapprima viene illustrato il funzionamento base della macchina, e successivamente, come nella realtà storica in cui la vicenda ha avuto luogo, si descrivono i miglioramenti tecnici apportati ad Enigma e gli espedienti usati dai crittoanalisti per risolvere i problemi da essi derivanti.

Nel 1918 l'inventore Arthur Scherbius e l'amico Richard Ritter fondarono la Scherbius&Ritter, la società dalla quale avrebbe avuto origine la macchina cifratrice Enigma. Scherbius aveva studiato ingegneria elettrica ad Hannover e mise in pratica le conoscenze così acquisite progettando un

dispositivo crittografico che corrispondeva ad una riproduzione elettromeccanica del disco cifrante di Leon Battista Alberti.

3.1.2 Funzionamento di Enigma

Fig.1: Enigma pronta all'uso.

La macchina era costituita da diversi elementi relativamente semplici se presi singolarmente, ma che costituivano insieme un potente apparato per la produzione di scritture cifrate.

La versione base del dispositivo era costituita da tre componenti collegati tra loro con fili elettrici: una tastiera per immettere le lettere del testo in chiaro; un'unità scambiatrice che cifra la lettera trasformandola nel corrispondente elemento del crittogramma; un visore con varie lampadine che illuminandosi indicano la lettera da inserire nel testo cifrato. In pratica l'operatore preme il tasto

corrispondente ad una lettera del testo in chiaro, la macchina elabora l'impulso elettrico ricevuto e fa illuminare la lampadina corrispondente alla lettera cifrata.

Fig.2: Vista dei componenti

La parte più importante della macchina è lo scambiatore che consiste in uno spesso disco di gomma attraversato da una fitta rete di fili provenienti dalla tastiera. Questi fili entrano nello scambiatore e dopo un percorso formato da vari gomiti emergono dalla parte opposta. Lo schema interno dello scambiatore determina in pratica un alfabeto cifrante utilizzabile per una semplice cifratura a sostituzione monoalfabetica.

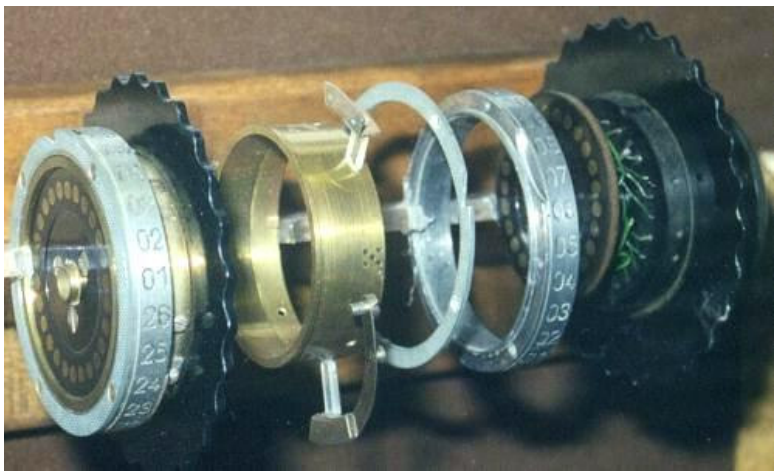


Fig.3: Struttura di uno scambiatore

Il passo successivo dell'idea di Scherbius prevedeva di far ruotare il disco dello scambiatore di un ventiseiesimo di giro dopo la cifratura di ogni lettera, facendo sì che l'alfabeto cifrante cambiasse dopo ogni lettera trasformando la cifratura monoalfabetica in una polialfabetica.

Così com'è il meccanismo presenta il problema della ripetizione che è comunemente sinonimo di cifratura debole. Per superarlo vennero introdotti un secondo e un terzo scambiatore. Il secondo compiva una rotazione parziale soltanto dopo che il primo aveva compiuto un intero giro e allo stesso modo faceva il terzo basandosi sul secondo. In questo modo la macchina di Scherbius poteva disporre di 26x26x26 = 17576 procedure di sostituzione diverse.

Un altro degli elementi del dispositivo considerato importante dallo stesso inventore era il riflessore. Esso consisteva di un disco con circuiti interni simile agli scambiatori ma che non ruotava e i fili che vi entravano riemergevano dallo stesso lato. Con tale elemento installato un segnale in ingresso alla macchina attraversava i tre scambiatori, poi passava al riflessore e veniva rimandato indietro passando nuovamente negli scambiatori, ma usando un percorso diverso.

Vediamo come nella pratica Enigma veniva usata. Innanzitutto bisogna specificare che gli scambiatori dovevano essere posizionati con un certo assetto prima di iniziare la cifratura di un messaggio e la loro posizione costituiva una vera e propria chiave. L'insieme di tali chiavi giornaliere era contenuta in un cifrario che doveva essere distribuito mensilmente a tutti gli operatori e che doveva essere, ovviamente, molto ben custodito. Gli assetti giornalieri del cifrario venivano usati per tutti i messaggi di una giornata. Per cifrare un messaggio un operatore Enigma posizionava gli scambiatori secondo la chiave giornaliera, digitava il messaggio sulla tastiera della macchina e spediva via radio il risultato al destinatario. Quest'ultimo digitava il messaggio cifrato sulla tastiera della sua macchina Enigma, sulla quale gli scambiatori erano sistemati secondo la stessa chiave giornaliera usata in precedenza, e otteneva il messaggio in chiaro. La semplicità con cui questa operazione era realizzata era dovuta proprio all'introduzione del riflessore.

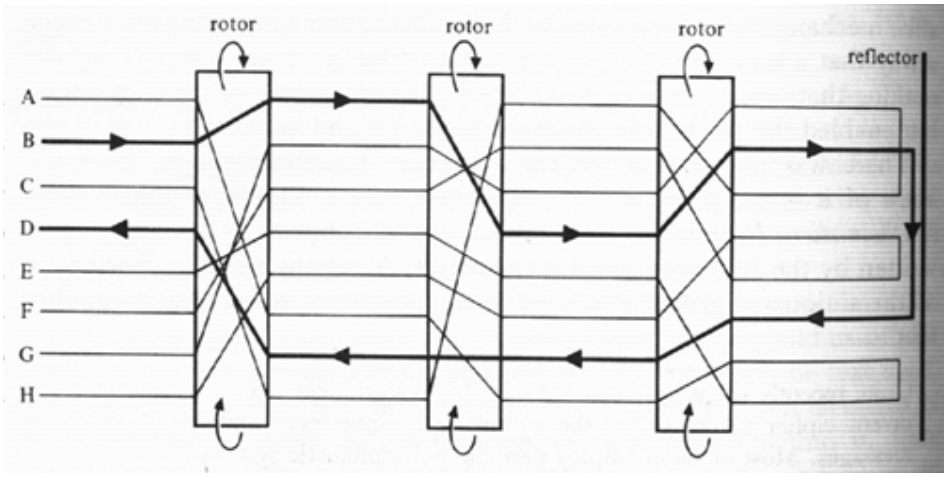


Fig.4:Schema semplificato di cifratura con un alfabeto ridotto.

La sicurezza di Enigma non era considerata la complessità della macchina stessa, ma l'elevato numero di combinazioni che un nemico avrebbe dovuto controllare per ottenere l'assetto iniziale. Infatti ammettendo di controllare una chiave al minuto e di poter lavorare giorno e notte, ci sarebbero volute due settimane per scoprire la chiave di un solo giorno. Ma questo non bastava e Scherbius decise di introdurre due nuove caratteristiche. Per prima cosa rese gli scambiatori rimovibili in modo da poterli sostituire con altri o scambiarli tra loro e questo accorgimento aumentava il numero di chiavi di un fattore pari a 6 (poiché 3 elementi intercambiabili possono essere combinati in 6 modi diversi).

La seconda caratteristica era l'inserimento di un pannello a prese multiple tra la tastiera e il primo rotore. Il pannello permetteva al mittente di inserire alcuni cavi muniti di spinotti, che avevano l'effetto di scambiare due lettere prima della loro immissione nel rotore. L'operatore di Enigma aveva a disposizione sei cavi per sei coppie di lettere, mentre le altre quattordici restavano non scambiate.

Combinando insieme tutti gli elementi fin qui osservati si può calcolare il numero di chiavi che Enigma poteva impiegare:

- Gli scambiatori (o rotori) potevano orientarsi oguno in 26 modi nel piano perpendicolare all'asse di rotazione, quindi tutti e tre generavano 26x26x26 = 17576 combinazioni;
- All'interno dell'unità cifratrice i tre scambiatori potevano essere inseriti in diverse posizioni reciproche, così riassumibili: 123, 132, 213, 231, 312, 321. Erano quindi ammesse 6 diverse posizioni reciproche dei rotori;
- Con il pannello a prese multiple i possibili abbinamenti di 12 (6x2) lettere su 26 sono moltissimi (per l'esattezza, 100 miliardi 391 milioni 791 mila 500).

Il numero totale di chiavi si ottiene moltiplicando tra loro le suddette possibilità: 17576x6x100391791500 = circa 10 milioni di miliardi!

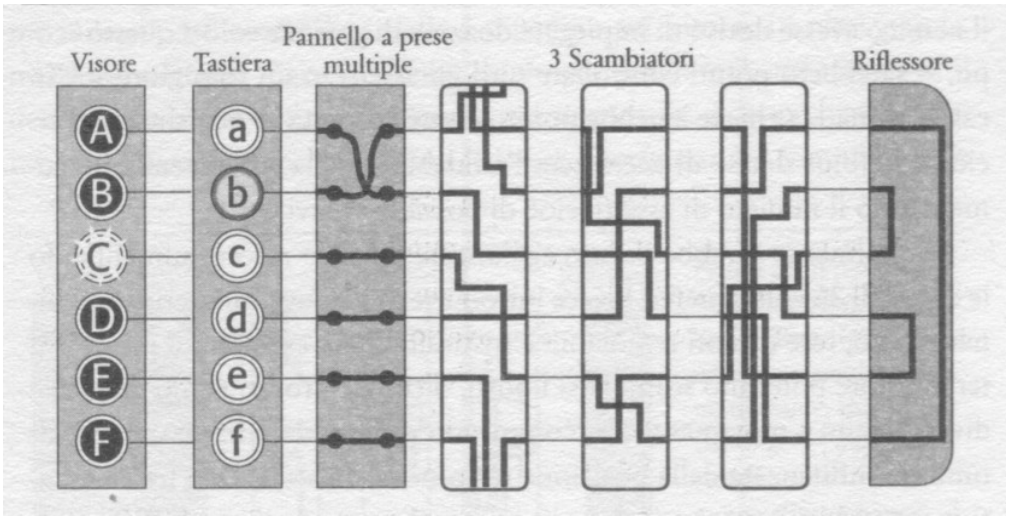


Fig.5: Schema semplificato con riflessore e pannello a prese multiple.

Nonostante fosse formata da elementi semplici, dunque, la combinazione di questi ultimi produceva una macchina cifratirce apparentemente inespugnabile. Eppure il suo inventore trovò difficoltà nel suo intento di diffonderla sul mercato sia dei privati sia degli organi governativi (come pure capitò ad altri giunti a soluzioni simili in altri Paesi), sia per il costo (20000 sterline attuali), sia perché nessuno sembrava aver colto l'importanza di una simile invenzione.

Alla fine i militari, dopo aver appreso quanto vantaggio la Regia Marina inglese avesse tratto dall'intercettazione delle comunicazioni cifrate tedesche durante la Prima Guerra Mondiale, e dopo altri episodi simili si decise ad adottare Enigma per prevenire nuovi pericoli del genere. Nel 1925 Scherbius organizzò la produzione in serie della sua invenzione e nei due decenni successivi le forze armate tedesche ne acquisirono 30000 esemplari. Questo permise loro di iniziare la Seconda Guerra Mondiale con il sistema di comunicazioni più sicuro al mondo facendo pensare che Enigma avrebbe avuto un ruolo chiave nel successo delle armate del Reich. Invece proprio Enigma fu una delle cause della loro disfatta.

3.2 Guerra ad Enigma: i crittoanalisti polacchi

Dopo i successi della Grande Guerra l'Inghilterra e i suoi alleati si sentivano sicuri della loro superiorità e l'attenzione che avevano posto nell'intercettare e risolvere i crittogrammi dei loro nemici nel passato andò man mano diminuendo fino a subire una vera e propria battuta d'arresto dopo il 1926, anno in cui cominciarono a intercettare messaggi di cui non venivano a capo. Si trattava dei primi crittogrammi prodotti da Enigma per le forze armate germaniche. Dopo qualche mese di insuccessi i crittoanalisti della Stanza 40 si diedero per vinti, seguiti dai colleghi degli uffici analoghi delle altre potenze vincitrici.
Fortunatamente una Nazione non aveva smesso di preoccuparsi dei suoi avversari che in realtà diventavano sempre più minacciosi e questa era la Polonia, stretta tra Germania e Russia. In particolare un ufficio chiamato Biuro Szyfrow, l'ufficio cifre polacco, si impegnò a raccogliere tutte le informazioni possibili sulle comunicazioni crittate tedesche e non si scoraggiò nemmeno di fronte ai messaggi apparentemente indecifrabili prodotti da Enigma.
Questo ufficio possedeva una versione commerciale della macchina, ma questo non era di nessuna utilità per risolvere le comunicazioni militari. La situazione rimase invariata fino al novembre del 1931 quando Hans-Thilo Schmidt, un impiegato dell'ufficio amministrativo preposto alle comunicazioni crittate militari, fornì ad una spia francese, il cui nome in codice era Rex, le foto di due manuali di istruzioni per la cifratrice dietro ricompensa di 10000 marchi (circa 30000 €). I servizi segreti francesi passarono, quasi senza dargli conto, queste informazioni al Biuro Szyfrow che così fu in grado di produrre una replica della versione militare di Enigma. Ma anche questo non bastava. Infatti gli utilizzatori di Enigma basavano la loro sicurezza sull'elevatissimo numero di combinazioni da controllare per trovare la chiave giornaliera in quanto la conoscenza del dispositivo da parte del nemico era già data per scontata. Inoltre per maggiore sicurezza (dato che la chiave giornaliera sarebbe stata usata per centinaia di messaggi e questo poteva facilitare il compito dei crittoanalisti nemici) venne adottata una nuova chiave per ogni messaggio, detta chiave di messaggio. Tale chiave veniva trasmessa usando l'assetto indicato dalla chiave giornaliera (nota in anticipo a tutti gli operatori perché contenuta nel cifrario) e ripetuta due volte di seguito e poi veniva usata per regolare il nuovo assetto della macchina per il singolo messaggio. Ad esempio se la chiave giornaliera era QCW e la chiave di messaggio PGH (entrambe indicano un orientamento degli scambiatori), l'operatore mittente avrebbe digitato PGHPGH come inizio del messaggio in chiaro. Cifrando il messaggio quelle lettere sarebbero diventate poniamo KIVBJE (da notare che la prima metà della stringa è diversa dalle seconda perché Enigma modificava automaticamente l'assetto degli scambiatori dopo ogni lettera). Dopo aver cifrato la chiave di messaggio l'operatore posizionava gli scambiatori su PGH e cifrava il messaggio vero e proprio. Il destinatario regolava la

macchina su QCW, la chiave giornaliera, e decifrava le prime sei lettere del messaggio ricevuto dopodiché posizionava gli scambiatori su PGH e poteva decifrare il testo del messaggio.

Fig.1: Marian Rejewski.

Ed è a questo punto che l'ingegnosità dei polacchi pose le basi per la soluzione del problema. Nonostante tradizionalmente si fosse sempre creduto che le persone più adatte per risolvere problemi di crittografia fossero i linguisti e gli umanisti, a causa della natura elettromeccanica di Enigma i responsabili del Biuro Szyfrow decisero di reclutare dei matematici. E li scelsero inoltre organizzando un corso di crittografia all'Università di Poznan, situata in una zona ex prussiana e quindi appartenuta alla Germania fino al 1918. Tra i 20 matematici selezionati il più brillante era senza dubbio il giovane Marian Rejewski (Fig.1).
Dopo un breve periodo di apprendistato Rejewski venne messo al lavoro su Enigma. Egli cercò di tradurre in termini numerici ogni aspetto del funzionamento della macchina e basò la sua strategia sul fatto che la ripetizione è nemica della sicurezza, perché crea degli schemi i quali a loro volta sono l'alimento della crittoanalisi.
La ripetizione più ovvia nei messaggi Enigma era quella della chiave di messaggio che veniva cifrata due volte di seguito all'inizio di ogni comunicazione. Questo significava che la prima e la quarta lettera erano legate strettamente alla posizione degli scambiatori così come la seconda e la quinta e la terza e la sesta. Man mano che venivano intercettati nuovi messaggi Rejewski aveva materiale per completare una tabella delle corrispondenze. Poniamo per esempio che venissero ricevuti i seguenti quattro messaggi (ne consideriamo solo le prime sei lettere):

1. L O K R G M
2. M V T X Z E
3. J K T M P E
4. D V Y P Z X

Considerando le prime e quarte lettere di ciascun esagramma crittato si poteva costruire una prima tabella:

Prima lettera: 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
Quarta lettera: P M R X

E con un sufficiente numero di messaggi in una stessa giornata la tabella avrebbe potuto essere più completa:

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

In base alle tabelle costruite il matematico polacco risalì a delle concatenazioni tra le lettere mettendo in relazione le lettere della riga superiore e quelle della riga inferiore. Tenendo conto solo della prima e quarta lettera di ogni messaggio otteneva concatenazioni simili alla seguente:

Concatenazioni:	Numero di collegamenti:
A -> F -> W -> A	3
B -> Q -> Z -> K -> V -> E -> L -> R -> I -> B	9
C -> H -> G -> O -> Y -> D -> P -> C	7
J -> M -> X -> S -> T -> N -> U -> J	7

Ovviamente questo lavoro andava ripetuto per le altre coppie di lettere dell'esagramma.
Dall'analisi di Rejewski si capiva che queste concatenazioni dipendevano in modo complesso dai collegamenti del pannello a prese multiple, dalla collocazione degli scambiatori e dal loro assetto, ma fin qui le possibilità da vagliare non apparivano ridotte e quindi il problema non cessava di esistere.
L'intuizione geniale del crittoanalista polacco fu quella di capire che gli effetti del pannello e quelli degli scambiatori sulle concatenazioni potevano essere separati. In particolare notò che il numero di collegamenti dipende esclusivamente dagli scambiatori. Infatti, tornando all'esempio precedente, supponiamo che le lettere S e G siano scambiate dal pannello a prese multiple. Se usiamo il cavetto di S e G per scambiare ad esempio T e K otteniamo:

Concatenazioni:	Numero di collegamenti:
A -> F -> W -> A	3
B -> Q -> Z -> T -> V -> E -> L -> R -> I -> B	9
C -> H -> S -> O -> Y -> D -> P -> C	7
J -> M -> X -> G -> K -> N -> U -> J	7

Notiamo che alcune lettere sono cambiate, ma il numero di collegamenti è rimasto invariato.
Grazie a questa intuizione si riuscì a ridurre in maniera molto significativa il numero di possibili combinazioni da controllare per trovare la chiave giornaliera: infatti ora bisognava scoprire non una chiave tra dieci milioni di miliardi, ma quale assetto degli scambiatori avesse generato le concatenazioni osservate. E il numero di assetti da verificare era il prodotto delle possibili collocazioni negli alloggiamenti (6) e dei possibili orientamenti (17576), quindi 105456.
Grazie alle repliche della versione militare di Enigma di cui il Biuro Szyfrow disponeva e dopo un anno di lavoro si riuscì a compilare un repertorio contenente tutte le possibili lunghezze delle concatenazioni e i relativi assetti degli scambiatori.
Questo fu uno storico passo avanti in quanto, una volta ricevuti un certo numero di messaggi Enigma, bastava osservare le prime sei lettere, costruire la tabella delle corrispondenze e controllando il repertorio si riusciva facilmente a trovare l'assetto degli scambiatori corrispondente alla chiave giornaliera. A questo punto i messaggi non erano totalmente in chiaro a causa degli scambi di lettera effettuati dal pannello a prese multiple, ma ciò non rappresentava un problema. Infatti escludendo il pannello sulle repliche della macchina una parte del messaggio (quella che conteneva lettere non scambiate dal pannello) era quasi comprensibile e perciò non risultava difficile trovare le lettere da collegare con i cavi del pannello a prese multiple.

Successivamente Rejewski riuscì a progettare, adattando alcune delle copie di Enigma a sua disposizione, un congegno che automatizzava la ricerca della chiave giornaliera controllando rapidamente le 17576 combinazioni per trovare le posizioni dei rotori degli scambiatori. Questi congegni erano chiamati "bombe" forse a causa del ticchettio prodotto durante il funzionamento e, poiché gli scambiatori potevano essere posti in sei posizioni diverse occorrevano sei "bombe" che funzionavano in parallelo. Così come Enigma aveva rappresentato l'automazione del processo di cifratura, così le "bombe" di Rejewski rappresentavano l'automatismo della decifrazione.
Un aspetto della storia che potrebbe stupire è che i crittoanalisti del Biuro Szyfrow vennero tenuti all'oscuro del fatto che ben 38 mesi di chiavi giornaliere erano già nelle mani dei servizi segreti polacchi grazie a Rex e al suo contatto Asche (Hans-Thilo Schmidt) che non smisero di incontrarsi segretamente mentre Rejewski e i suoi continuavano a lavorare sodo per decifrare i crittogrammi tedeschi con le loro sole forze. Questo avvenne perché si temeva che un giorno un'eventuale guerra avrebbe interrotto la fornitura delle chiavi giornaliere da parte delle spie e sarebbe stato necessario agire da soli.
Alla fine del 1938 i successi polacchi nel decifrare i messaggi Enigma subirono una pesante battuta d'arresto dovuta all'introduzione di nuove misure per aumentare la sicurezza della macchina. Infatti tutti gli operatori Enigma ricevettero due nuovi scambiatori e il numero di cavetti del pannello a prese multiple passò da sei a dieci. Con i nuovi scambiatori il numero delle combinazioni passava da sei a 60 il che rendeva necessaria la costruzione di altre 54 "bombe", cosa che risultava impossibile per il bilancio del Biuro Szyfrow. Inoltre con le aggiunte al pannello a prese multiple le lettere scambiate passavano da dodici e venti su ventisei portando il numero di possibili chiavi a 159 miliardi di miliardi!
La guerra sembrava sempre più inevitabile e il Terzo Reich sempre più minaccioso così si decise di rivelare i progressi fatti dal Biuro Szyfrow su Enigma, fino ad allora tenuti segreti, agli alleati più potenti e ricchi di Francia e Inghilterra e di tentare di proseguire altrove il lavoro impedendo ai tedeschi di scoprire i risultati ottenuti.

3.3 Bletchley Park

Attorno alle metà del 1939 i polacchi trasferirono il loro materiale in Inghilterra e più precisamente in un palazzo nel Buckinghamshire che si chiamava Blechley Park ed era la sede della Government Code and Cypher School (GC&CS). Qui poteva essere ospitato un numero superiore di addetti rispetto alla vecchia Stanza 40 e questi crittoanalisti (che per la prima volta vennero reclutati anche in Inghilterra tra i matematici) erano sistemati in diversi edifici appositamente realizzati detti Capanne. Esse erano numerate e ad ogni numero corrispondeva un compito diverso: la Capanna 6 era quella che si occupava della decifrazione dei messaggi Enigma. Inoltre si passò dalle duecento persone impiegate del 1939 alle circa settemila della fine del conflitto. Grazie al lavoro del Biuro Szyfrow e alla maggiore disponibilità di risorse gli uomini (e donne) di Blechley Park risolsero piuttosto rapidamente i nuovi problemi creati dall'aggiunta degli altri scambiatori e cavetti. Basti pensare che durante la Battaglia d'Inghilterra i crittoanalisti furono spesso in grado di fornire ai comandi della RAF il luogo e il momento delle incursioni tedesche e informazioni come queste erano di importanza realmente enorme per l'esito della guerra.

Fig.1: Blechley Park oggi.

Fig.2: Blechley Park nel 1939.

Partendo dalle basi fornitegli dai polacchi i crittoanalisti inglesi riuscirono a trovare anche altre scorciatoie per scoprire la chiave giornaliera che denominarono “cillies”. Un “cilly” non era una imperfezione di Enigma, ma derivava dal modo in cui veniva usata. Infatti molti operatori usavano come chiave di messaggio tre lettere adiacenti sulla tastiera oppure le iniziali di una fidanzata il che rendeva più semplice intuire la chiave stessa. Altri errori anche più gravi furono commessi ad alti livelli. I responsabili della compilazione dei cifrari cercarono di rendere le chiavi più difficili da prevedere imponendo però delle limitazioni al numero di chiavi stesse. Infatti stabilirono che nessuno scambiatore potesse occupare la stessa posizione per due giorni consecutivi e anche che ogni lettera non potesse essere scambiata con quella che la precede e la segue (ad esempio S non andava scambiata con R o T). Queste limitazioni, che a prima vista sembrano sensate, portarono ad una riduzione di oltre il cinquanta per cento del numero di disposizioni degli scambiatori e ad una notevole facilitazione per i crittoanalisti inglesi.
La ricerca di nuove scorciatoie era importante poiché Enigma continuò ad evolversi per tutta la durata della guerra e continue modifiche alle bombe o ai sistemi di decifrazione usati si resero necessarie, oltre alla collaborazione tra tutti i componenti dell’eterogeneo gruppo di Bletchley Park.


Fig.3: Alan Turing.

Tra tutti gli impiegati della CG&CS quello che diede il contributo più significativo alla sconfitta di Enigma fu Alan Turing, più noto per i suoi studi sui problemi indecidibili e sulla cosiddetta "macchina universale", anticipazione teorica dei moderni calcolatori.
Turing notò che molti dei messaggi che venivano intercettati avevano una struttura piuttosto rigida e spesso capitava che messaggi che venivano trasmessi periodicamente (come ad esempio i bollettini meteorologici) avevano le stesse parole nelle stesse posizioni fisse. L'esperienza poteva fornire indicazioni ancora più precise, come ad esempio che le prime sei lettere del secondo rigo di alcuni tipi di messaggi corrispondevano alla parola "wetter" (tempo atmosferico). Questo costituiva ciò che in gergo dei crittoanalisti viene definito un "crib", cioè un frammento del testo in chiare che può essere dedotto in base a considerazioni non crittoanalitiche. Turing era convinto di poter sfruttare i cribs per ottenere un procedimento di soluzione dei crittogrammi Enigma diverso da quello di Rejewski e che quindi permettesse di superare il pericolo che i tedeschi smettessero di ripetere la chiave di messaggio due volte. Si concentrò su un crib in particolare e anche in questo caso scoprì delle concatenazioni, ma che stavolta riguardavano le lettere del testo in chiaro e del testo cifrato nell'ambito di un crib. Nella figura è mostrato un possibile crib e la sua concatenazione.

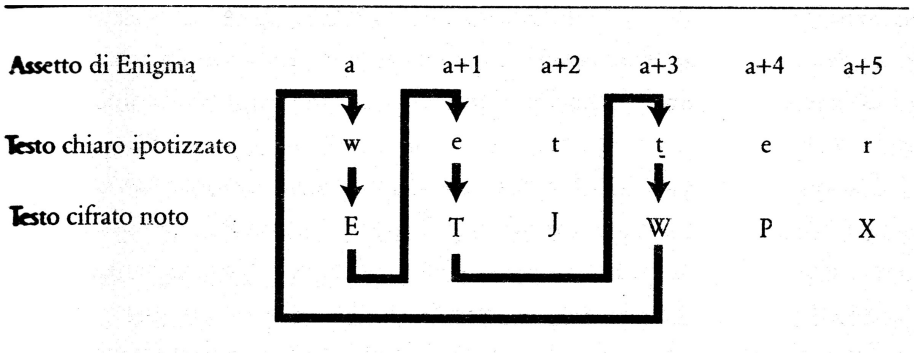


Fig.4: Uno dei "crib" di Turing con la concatenazione in evidenza.

Analizzando la concatenazione possiamo dire che:
- Nell'assetto a, Enigma cifra w come E.
- Nell'assetto a+1, Enigma cifra e come T.
- Nell'assetto a+3, Enigma cifra t come W.

Turing sviluppò tutte le implicazioni dei rapporti all'interno del ciclo e in base a questo progettò un circuito elettrico che collegava tre macchine Enigma con cavi posti tra l'input di una macchina e l'output della successiva seguendo lo schema mostrato in figura.

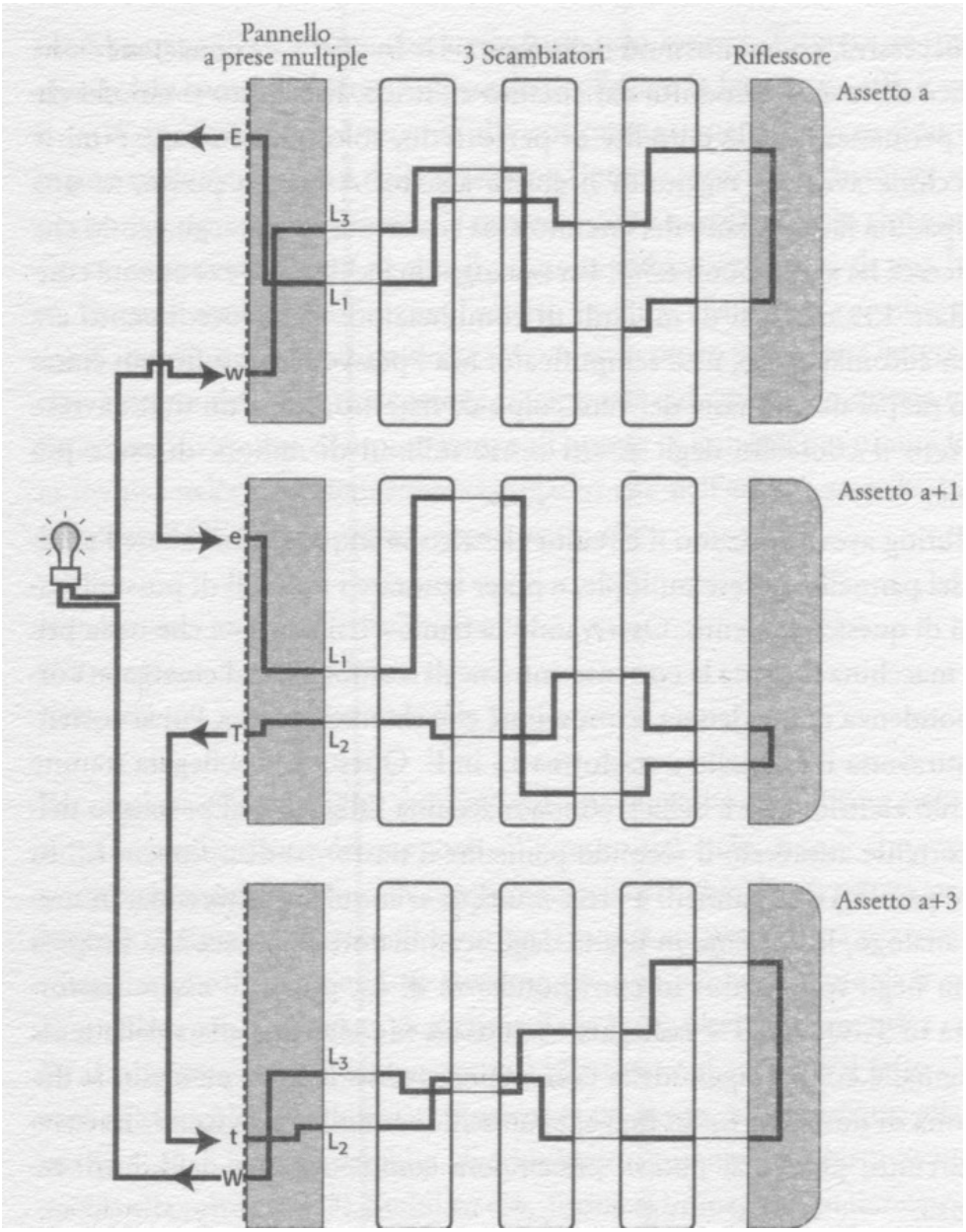


Fig.5: Schema di un circuito completo corrispondente al giusto assetto degli scambiatori.

Questo permetteva un procedimento di verifica automatizzato in quanto inserendo una lampadina nel circuito, essa si sarebbe accesa quando il corretto assetto fosse stato trovato. Osservando la figura si nota che il circuito era costruito in modo da annullare gli effetti del pannello a prese multiple e quindi bisognava solo collegare l'output del primo gruppo di scambiatori con l'input del secondo gruppo in corrispondenza di L1. Poiché questo valore non era noto era necessario collegare le 26 uscite del primo gruppo con i 26 ingressi del secondo formando 26 circuiti, ciascuno dotato di una lampadina per evidenziarne la chiusura. Alla fine, scoperto il giusto orientamento degli scambiatori, uno dei circuiti si chiudeva causando l'accensione della lampadina. Ipotizzando che gli scambiatori mutassero orientamento ogni secondo, per completare l'operazione di controllo di tutti gli orientamenti ci sarebbero volute cinque ore. Gli scambiatori, però, erano cinque e le cifratici ne contenevano tre con 60 combinazioni, quindi per controllare tutte le disposizioni erano necessari 60 gruppi di tre macchine da far lavorare in parallelo.

Risolto il problema degli scambiatori risultava più semplice determinare l'assetto del pannello a prese multiple attraverso l'uso dei crittogrammi parzialmente decifrati.
Qualcuno parve rendersi conto dell'inestimabile valore che un'intuizione del genere avrebbe avuto e perciò le 100000 sterline necessarie per costruire quelle che vennero soprannominate le "bombe di Turing" vennero rapidamente messe insieme e si potè procedere alla realizzazione al cui completamento si giunse all'inizio del 1940. Ogni bomba era composta da dodici gruppi di scambiatori Enigma collegati elettricamente. Il primo prototipo non funzionò proprio a dovere e contemporaneamente gli operatori Enigma smisero di ripetere le chiavi di messaggio, cosa che portò ad un crollo delle decifrazioni fino all'arrivo della versione migliorata delle bombe denominata "Agnus Dei". Questo dispositivo era in grado di risalire ad una chiave giornaliera in una sessantina di minuti al massimo, ma il suo funzionamento non era completamente autonomo e indipendente dal personale che lo utilizzava. Infatti aveva bisogno di partire da un crib il quale a sua volta non era altro che un'ipotesi che i crittoanalisti facevano, immaginando che una certa parola in chiaro potesse trovarsi in una certa posizione. Nel caso in cui la parola faceva parte del messaggio ma non era nella posizione ipotizzata si poteva ovviare al problema con un trucco. Nel crib seguente il testo in chiaro fa parte del crittogramma ma non si ha la sicurezza di averlo collegato alle lettere giuste.

Testo chiaro ipotetico: w e t t e r n u l l s e c h s
Porzione del crittogramma: I P R E N L W K M J J S X C P L E J W Q

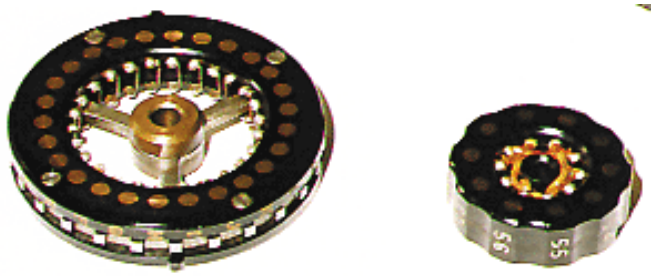
Quello che poteva aiutare in questi casi era che il riflessore di Enigma non permetteva ad una lettera di essere cifrata come se stessa (ovvero una "a" non poteva essere cifrata come "A"). Quindi nell'esempio ci deve essere un allineamento sbagliato poiché si sovrappongono una "e" in chiaro e una "E" cifrata. Le cose non cambiano spostando la prima riga di una posizione a sinistra, ma effettuando lo spostamento verso destra si trova un allineamento ammissibile e che poteva quindi essere utilizzato per la ricerca automatica della chiave giornaliera.
Grazie ai progressi fatti con le bombe i crittoanalisti di Bletchley Park ottennero anche l'appoggio incondizionato dello stesso Churchill il che permise di aumentare il numero di apparecchiature in dotazione e anche di aumentare il personale (reclutato tramite la pubblicazione sul Daily Telegraph di un cruciverba per "code-breakers").

4. SIGABA E PURPLE (curato da Daniele Palladino)

4.1 Sigaba

Il più noto crittologo americano nel XX secolo fu probabilmente William Friedman. Studiando le macchine cifranti a rotori che si erano diffuse negli anni Venti, arrivò a determinare tutti i difetti della macchina più famosa di quel periodo: Enigma.
Questa, in sintesi, non era una macchina cifrante molto complessa. Infatti il suo meccanismo di codifica era talmente

semplice che poteva essere paragonato ad un banale contatore.
Il principio di funzionamento era basato sul fatto che ad ogni scrittura di una singola lettera i rotori al suo interno giravano in modo da generare ogni volta un codice casuale per codificare l'intero messaggio.
Per questo motivo non si poteva semplicemente aumentare il numero dei rotori, con i quali codificare i vari messaggi, per essere più sicuri sull'affidabilità della macchina.
Un primo passo compiuto da W. Friedman, per arrivare alla macchina Sigaba, fu l'Elettric Cipher Machine (ECM) progettata e costruita nel 1935 insieme al suo collaboratore Frank B. Rowlett. L'ECM era una macchina elettrica che somigliava ad Enigma nella sua configurazione, l'unica differenza tra le due era una nastro metallico forato che serviva a far passare la corrente in determinati circuiti, a seconda dei fori, per codificare e decodificare i vari messaggi.
Praticamente si può considerare il nastro come la chiave di tutto, infatti doveva essere identica in tutte la sue caratteristiche per le varie macchine che volevano comunicare tra loro. Questo era considerato il punto debole per questa prima versione della macchina cifrante, infatti bastava che la chiave fosse intercettata per poter decodificare tutte le comunicazioni.
Col passare del tempo l'esercito e la marina degli Stati Uniti, dopo vani tentativi per ottenere una macchina che non potesse essere forzata, si associarono e chiesero a Friedman di studiare un nuovo modo per poter comunicare in maniera che nessuno riuscisse a decifrare i propri messaggi.
A questo punto Friedman e il suo collaboratore cercarono con successo di concludere gli studi su Enigma e di eliminare tutti i difetti e le debolezze dell'ECM, escludendo il nastro forato e facilitandone il funzionamento aggiungendo anche un dispositivo di stampa per migliorarne la comodità.
La nuova macchina fu un vero e proprio successo.
Il suo meccanismo, considerato unico, al posto del nastro forato aveva un innovativo insieme di 15 rotori che erano suddivisi nel seguente modo:



- 5 rotori per la cifratura;
- 10 per generare una sequenza pseudo-casuale che stabilisce quali rotori ruotano ad ogni passo; all'interno era presente un cablaggio segreto.

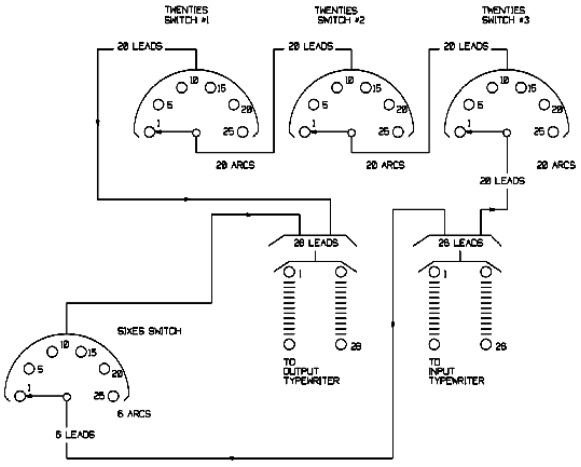
Questa macchina fu conosciuta con il nome di Sigaba. Era molto complessa nella sua struttura, ma al suo interno erano individuabili due parti ben note in precedenza, infatti si poteva dire che era formata da due macchine Enigma contemporaneamente.
Anche se l'algoritmo di cifratura può essere determinato in maniera molto semplice con un computer di oggi, non risulta esserci stata alcuna forzatura di questo gioiello nella storia della crittografia durante il periodo in cui era in uso.

4.2 PURPLE

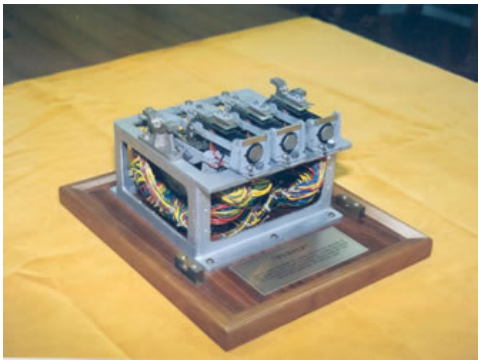
Negli anni Trenta i giapponesi vollero ideare una nuova macchina destinata alle comunicazioni di alto livello, e tali macchine furono ampiamente utilizzate nelle navi da guerra.

Studiando le varie macchine cifranti americane, tipo Enigma, arrivarono alla conclusione di utilizzare, al posto dei classici rotori destinati alla codifica dei messaggi, degli switch telefonici. In questo modo volevano confondere il funzionamento di Purple rispetto alle altre macchine.
Questi switch erano controllati da interruttori che determinavano ad ogni passo un collegamento tra un terminale di input ad uno dei 25 di output rimanenti.
Un elettromagnete fissava l'interruttore alla relativa posizione seguente tramite il passaggio di corrente. Tale procedura porta alla realizzazioni di 25 alfabeti indipendenti tra loro per la codifica dei messaggi.
I suddetti terminali sono la rappresentazione logica dell'alfabeto a 26 lettere, infatti veniva diviso in due gruppi:

- 6 lettere (AEIOUY)
- 20 lettere



Con questo tipo di struttura della macchina, i giapponesi pensarono che nessuno sarebbe riuscito a determinare il funzionamento esatto dell'algoritmo di cifratura, purtroppo per i giapponesi, Friedman riuscì a capire il procedimento con cui i vari messaggi venivano codificati. Tutto ciò avvenne dopo soli 18 mesi di studio sulla macchina da parte del miglior crittografo del XX secolo.
Il principio con cui Friedman decifrava i messaggi inviati da Purple fu poi meccanizzato e quindi costruita Magic, strumento elaborato al solo scopo di intercettare e decriptare le comunicazioni inviate dai giapponesi.
Una curiosità sulla storia di Purple fu che pur conoscendo nel dettaglio il funzionamento e i meccanismi usati nel concepire la macchina, gli americani riuscirono a costruire delle copie perfette rispetto all'originale, ma non ad impossessarsi di un esemplare costruito prettamente dai giapponesi.



L'unico pezzo di una macchina originale, rinvenuto a Berlino nel 1945 ed esistente tuttora è custodito nel Museo Crittologico Nazionale di Washington.

RIFERIMENTI TELEMATICI

Tutte le informazioni contenute nel presente documento sono reperibili nei seguenti siti web:

1. http://www.nsa.gov
2. http://www.liceofoscarini.it
3. http://www.icsm.it
4. http://www.museoscienza.org
5. http://www.dia.unisa.it
6. http://www.tonycrypt.com/Crittografia/Alberti.htm

"Quando numeri e figure non saranno più la chiave di tutte le creature, quando quelli che cantano o baciano sapranno più dei profondi eruditi, quando il mondo tornerà ad essere vita libera il vero mondo, quando poi luce e ombra si ricongiungeranno in un genuino chiarore, e quando in fiabe e poesie si riconosceranno le storie eterne del mondo, allora di fronte ad un'unica parola magica si dileguerà tutta la falsità"