Storia della crittografia e macchine cifranti

In ordine di presentazione:

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

Storia della crittografia

- Il pericolo dell' intercettazione da parte degli avversari promosse lo sviluppo di codici.
- Codici:tecniche di alterazione del messaggio destinate a renderlo comprensibile solo alle persone autorizzate.
- Steganografia: una delle prime tecniche di comunicazione segrete:
  - occultamento del messaggio (metodi bizzarri per trasmettere informazioni)
  - Perdita della segretezza nel momento dell'intercettazione.

Crittografia

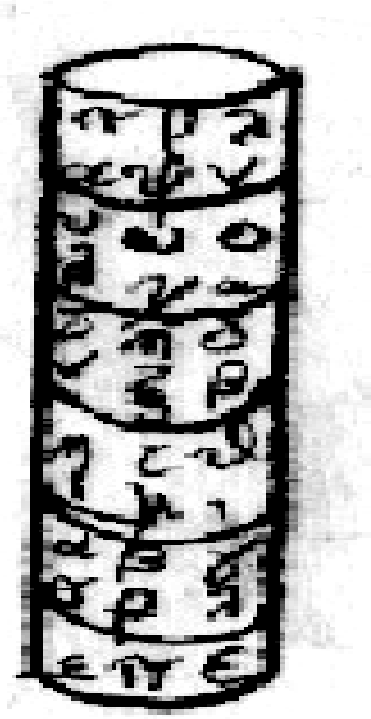
- Sviluppo parallelo della CRITTOGRAFIA dal greco *kriptos* (nascosto).
- Mira a nascondere il significato del messaggio e non il messaggio.
- Si altera il testo per mezzo di un procedimento concordato tra mittente e destinatario.
- Vantaggi(rispetto a stenografia):se il nemico intercetta il messaggio non lo comprende e quindi diventa inutilizzabile.

Crittografia e società antiche

- Non tutte le società antiche svilupparono forme di crittografia:
  - Cina (scrittura ideografica)
    - Ragioni: natura prevalentemente orale delle comunicazioni
- India: importanza delle scritture segrete nei servizi di spionaggio.
- Mesopotamia: nelle scritture cuneiformi.
- Iraq: nel periodo finale delle scritture cuneiformi prima è presente sostituzione dei nomi con i numeri.

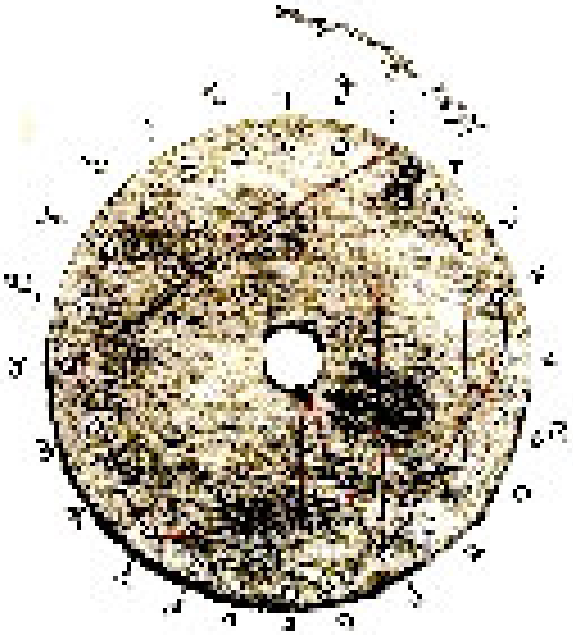
Crittografia antica

- Scitala lacedemonica: la più antica forma di crittografia (400 a. c.)negli scritti di Plutarco.
- Consisteva in un bastone in cui si avvolgeva ad elica un nastro di cuoio(algoritmo di cifratura).
- La chiave consisteva nel diametro del cilindro.
- Scrittura per colonne parallele all'asse del bastone lettera per lettera.



Disco di Enea (390-360 a.c.)

- Sulla zona esterna del disco 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.



Testi sacri(Vecchio Testamento)

- Tre principali codici cifrati:
  - Atbash
  - *Albam*
  - *Atbah*

Atbash

- Ideato dal popolo ebraico.
- 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.

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

- Frase da cifrare: **Il sole brilla**
  Frase cifrata: **Rohlovyirooz**

Albam

- Richiede che l'alfabeto venga diviso in due parti e che ogni lettera venga sostituita con la corrispondente dell'altra metà.
- Esempio:
  - 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
    - Sara → fnen

Atbah

- La sostituzione soddisfa 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.
- Esempio:
  - 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
    - La c = 3 viene sostituita con la g=7 in modo che la somma sia 10

Polibio (200 ca. -118 a.C.)

- Nelle sue Storie (Libro x)descrive un importante 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.

#	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 d'uso(Polibio)

- Esempio:

  Frase da cifrare: *Attenzione agli scogli*

  Frase cifrata:
  114444153455243534151122322443133 5223224

Vantaggi codice di Polibio

- 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.

Cifrario di Cesare(II secolo d.C.)

- Codice di sostituzione molto semplice, nel quale ogni lettera del testo veniva sostituita dalla lettera che la segue di tre posti nell'alfabeto.

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

Cifrario di Cesare

- 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.
- Sono possibili **26 codici di Cesare** diversi: poiché l'alfabeto internazionale è composto da 26 caratteri.
- Un alfabeto (quello che comporta uno spostamento di zero posizioni) darà un cifrato uguale al messaggio chiaro iniziale.

Esempio(cifrario di Cesare)

- Esempio la frase *Auguri di buon compleanno* si otterrà il seguente messaggio cifrato:

  Chiaro: auguridibuoncompleanno

  Cifrato: dxjxulglexrqfrpsohdqqr

Cifrario di Augusto

- Usava accanto al semplice codice di Cesare un cifrario più sicuro per le comunicazioni più delicate.
- Il metodo si basa sul testo greco dell'Iliade.
- Si tratta chiaramente di **cifrario polialfabetico** che precorre di 1500 anni la **tavola di Vigenére**.

Cifratura e Decifratura

- **Cifratura**:
  - 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.
- **Decifratura**:
  - Era sufficiente sommare al carattere dell'Iliade il numero del messaggio.

Esempio(cifrario Augusto)

Parola chiara:	C A S A
Posizione lettera chiara:	3 1 19 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*;
- La terza lettera (*S* posizione 19) spostata di 12 posti darà 19+12=31 che, superando i limiti dell'alfabeto, dovrà essere diminuita di 26 dando come risultato la lettera 5 (*E*).

La crittografia fino al XVIII secolo

- Compaiono i primi **alfabeti cifranti** o monografici(anno 1000).
- Alfabeto cifrante: Si ottiene una tabella a due colonne dove ogni segno alfabetico del testo in chiaro corrisponde biunivocamente ad uno dell'alfabeto cifrante(lo stesso alfabeto, un altro o inventato dall'ideatore della cifra).
- Usati successivamente soprattutto nelle missioni diplomatiche tra i vari stati europei.

Pietro Di Grazia

- Metodo usato tra il 1363 e il 1365 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. Estesa anche alle consonanti.

Il Disco di Leon Battista Alberti

- Nel suo Trattato De Cifris (circa nel 1400), introdusse il **primo codice polialfabetico**.
- Per tre secoli costituì il basamento dei sistemi crittografici.
- Introduce il concetto su cui si basa la macchina cifrante ***Enigma.***

Struttura del disco

- Disco composto di due cerchi concentrici di rame.
- Uno **esterno** fisso di diametro maggiore sul quale sono riportate le lettere **dell'alfabeto in chiaro**: composto di 24 caselle contenenti 20 lettere maiuscole in ordine lessicografico, escluse H, J, K, W, Y, al posto delle quali ci sono i numeri 1, 2, 3, 4.
- Uno **interno** mobile per le lettere dell'**alfabeto cifrante**. Il disco interno riporta le 24 lettere minuscole in maniera disordinata (la e e la t sono collassate) ed un simbolo speciale et.

Disco cifrante di Alberti

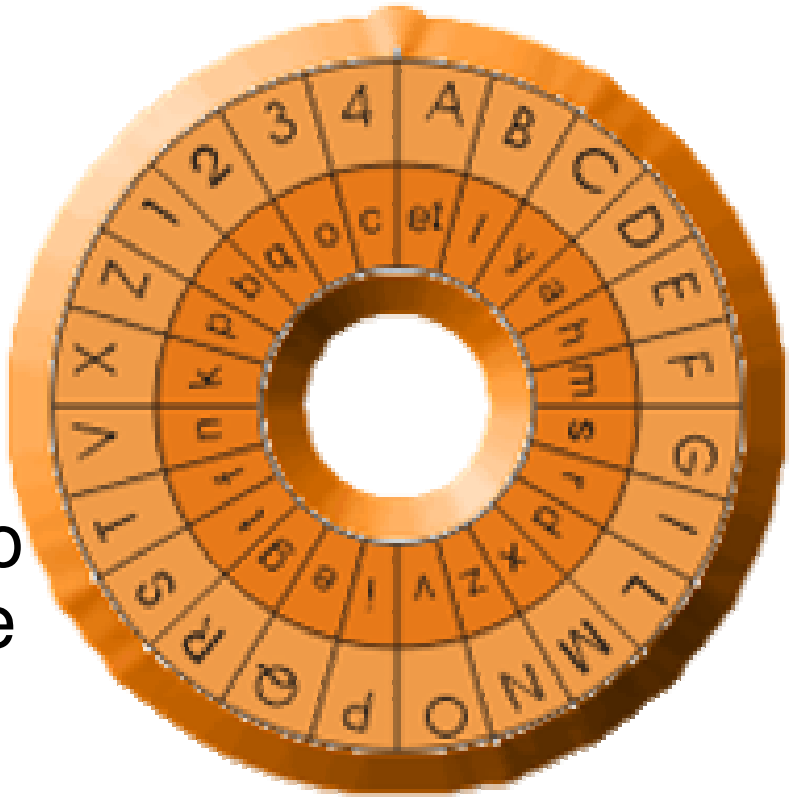
- Mittente e destinatario avevano entrambi la stessa macchinetta. Entrambi concordavano una lettera che sarebbe stata la chiave di partenza.
- Per **cifrare** il messaggio, il mittente iniziava ruotando il disco interno in maniera casuale. Iniziava quindi a scrivere il testo cifrato, riportando per prima 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.

Disco cifrante di Alberti(1)

- Terminata la prima parola, ruotava di nuovo in maniera casuale il disco interno e iterava la procedura di sostituzine.
- 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).
- Le lettere che di volta in volta corrispondono ai numeri 1,2,3,4 non vengono usate.

Esempio d'uso(1)

- Messaggio da cifrare: "Messaggio da Leon"
- Lettera chiave: C.
- Ruotiamo a caso il disco interno e passiamo alla posizione in figura.
- 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



Esempio d'uso(2)

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

Punto debole

- 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.
- Aumento segretezza reso possibile grazie all'utilizzo di uno dei quattro numeri per segnalare il cambio dell'alfabeto;la lettera minuscola corrispondente al numero sarà la nuova chiave; non vi sono quindi più lettere maiuscole.

Punti forza

- Leon Battista riusciva ad **impedire l'analisi statistica basata sulla frequenza delle lettere** da lui stesso studiata.
- 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).

Giovan Battista Bellasso

- Pubblicò tre opere di crittologia tra il 1553 e il 1564 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.

Costruzione degli alfabeti: primo alfabeto derivato

- 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.

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

Successivi alfabeti derivati

- A partire da questo ricaviamo il secondo spostando circolarmente verso destra la seconda riga di una posizione, e così via applicando lo stesso procedimento fino al quinto.
- Ognuno dei quali sarà identificato da un gruppo di quattro lettere.

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

Metodo di cifratura(1)

- 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.

Metodo di cifratura(2)

- 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.

Metodo di cifratura(3)

- La cifratura si effettua sostituendo la lettera del testo in chiaro con la lettera che si trova sulla stessa colonna nell'alfabeto predeterminato.

Esempio completo

Motto segreto, p.es OPTARE MELIORA.

Frase da cifrare: "Inviare truppe domani“.

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

Considerazioni

- 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 Vigenére.

Cifrario di Vigenére

- Blaise de **Vigenére** propose in un trattato di cifrari pubblicato nel 1586 un codice che ebbe molta fortuna e che è ricordato con il suo nome.
- Fama grazie alla semplicità del semplice codice polialfabetico.
- Punto forza: utilizzare non uno ma 26 alfabeti cifranti per cifrare un solo messaggio.
- Il metodo si può considerare una generalizzazione del codice di Cesare.
- Da tale cifrario deriva il cifrario di **Vernam**, considerato il cifrario teoricamente perfetto.

Metodo di cifratura

- 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.

Tavola di Vigenére

Tavola quadrata
composta da alfabeti ordinati spostati

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	Q
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

Conclusioni

- La sicurezza di un algoritmo crittografico basato su queste tecniche era direttamente proporzionale alla complessità di tali sostituzioni.
- Al contrario di quelli che sono i presupposti della crittografia moderna, tali algoritmi crittografici erano sicuri fino a quando l'algoritmo stesso rimaneva segreto.

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.
- in Italia dove si dovrà ottendere l'entrata in Guerra nel 1915 per rendersi conto del ritardo accumulato in campo crittografico, e porvi rimedio.

La crittografia dalla seconda metà del XIX secolo alla Grande Guerra

- Tra i metodi usati nella Grande Guerra si possono ricordare i cifrari poligrafici:
  - Playfair cipher (1854)
  - Il cifrario bifido di Delastelle
  - Cifra campale germanica (1918)

Playfair cipher

- Divulgato da Lyon Playfair doveva essere utilizzato durante la guerra di Crimea ma il sistema fu effettivamente utilizzato dall'esercito britannico solamente a partire dalla guerra Boera.
- 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.

Il cifrario bifido di Delastelle

- Il metodo è dovuto a Félix-Marie Delastelle uno tra i massimi crittologi francesi del XIX secolo.
- Cifrario poligrafico basato sulla matrice 5x5 usata per la prima volta nella scacchiera di Polibio.
- 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.

Cifra campale germanica

- Metodo di Crittografia 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.

Cifrario di Jefferson

Cifrario di Jefferson

- Inventato da Thomas Jefferson (1743-1826)
- 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).

Cifrario di Jefferson

- Il messaggio in chiaro deve essere cifrato a blocchi di 36 lettere ciascuno
- La chiave è duplice:
  - un numero “n” che va da 1 a 25
  - la struttura del cilindro
- Il crittogramma si leggerà sulla n-esima riga sopra quella con il blocco in chiaro.
- Decifratura con il procedimento inverso; si compone il messaggio e si legge il testo chiaro nella n-esima riga sotto.

Esempio

- Testo in chiaro: La missione in Polinesia è fallita
- Chiave: il numero 5
- Il crittogramma si leggerà sulla quinta riga sopra quella con il blocco in chiaro.

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

Crittografia nella I Guerra Mondiale

- Utilizzo di mezzi di comunicazione come radio e telefono esposti all'intercettazione da parte del nemico.
- Sin dall'ottobre 1914 i crittanalisti francesi erano in grado di decrittare i messaggi radio tedeschi (*Georges Painvin*).
- Gli Austriaci già nell'agosto 1914 decrittarono i radiomessaggi russi.
- I Russi non si preoccupavano neanche di cifrare i loro messaggi radio (battaglia di Tannenberg nell'agosto 1914).

Crittografia nella I Guerra Mondiale

- I Tedeschi decrittarono i messaggi russi anche dopo che questi iniziarono a cifrarli (prof. Deubner).
- Il Capo dell'ufficio crittologico della Marina Britannica, Sir Alfred Ewing, organizzò la cosiddetta Room 40 dove si decrittavano i radiomessaggi della marina tedesca (telegramma Zimmermann).
- Negli USA esisteva solo il reparto crittologico dei laboratori Riverbanks di Chicago (*William Friedmann)*.

Crittografia nella I Guerra Mondiale

- Impreparati erano gli Italiani prima appoggiati all'ufficio cifra francese, poi guidati da *Luigi Sacco*.
- All'inizio del 1916 era possibile intercettare ma non decrittare(decrittaggio ai francesi).
- Sacco crea un Ufficio Crittografico autonomo.
- Forzati il cifrario campale austriaco, navale e diplomatico, e alcuni cifrari tedeschi.

Crittografia nella I Guerra Mondiale

- Con la disfatta di Caporetto nel 1917 si abbandonarono i vecchi cifrari, che come poi si seppe venivano facilmente decrittati dagli austriaci.
- La possibilità di intercettare e decrittare i messaggi austriaci ebbe un'importanza non trascurabile nel 1918, per fronteggiare l'offensiva austriaca del Piave.

Cifrario di Vernam

- Inventato nel 1917 da Gilbert Vernam.
- Ingegnosissimo sistema di protezione crittografica, per comunicazioni su telegrafo, dei testi codificati in binario.
- Lettura contemporanea di due nastri in input e generazione di un nastro di output tale che ciascun foro fosse generato mediante uno XOR dei due corrispondenti fori sui nastri input.

Cifrario di Vernam

- 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.

Esempio

- 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:

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

Crittografia nella II Guerra Mondiale

- Ruolo di primo piano della Crittografia.
- Il caso più noto: macchina Enigma, usata dai tedeschi e considerata a torto inattaccabile.
- Forzata dall'ufficio cifra polacco e durante la guerra dagli inglesi del progetto ULTRA che dal 1941 forzarono anche quelli cifrati con la macchina di Lorenz.

Crittografia nella II Guerra Mondiale

- Vittorie alleate grazie alla superiorità crittografica:
  - **Battaglia di capo Matapan**: 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.

Crittografia nella II Guerra Mondiale

- Sul fronte del Pacifico gli Americani sin dal 1940, 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**: intercettazione dei piani dell'Amm. Yamamoto per attaccare a sorpresa le isole Midway.
  - **Morte dell'Amm. Yamamoto**: nel 1943 fu decrittato un messaggio relativo ad un viaggio di Yamamoto e fu così abbattuto il suo aereo.

Crittografia nella II Guerra Mondiale

- **Pearl Harbour** : alcune fonti affermano che gli Americani sapevano in anticipo dell'attacco di Pearl Harbour e decisero di non impedirlo. Altre sostengono che gli Americani sapevano che il Giappone stava per attaccare, ma non sapevano dove.

Crittografia nella II Guerra Mondiale

- Italia:
  - Il gen.Sacco aveva progettato una macchina cifrante, ma per motivi non ben chiariti la macchina andò distrutta.
  - Successo 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".

Macchina di Lorenz

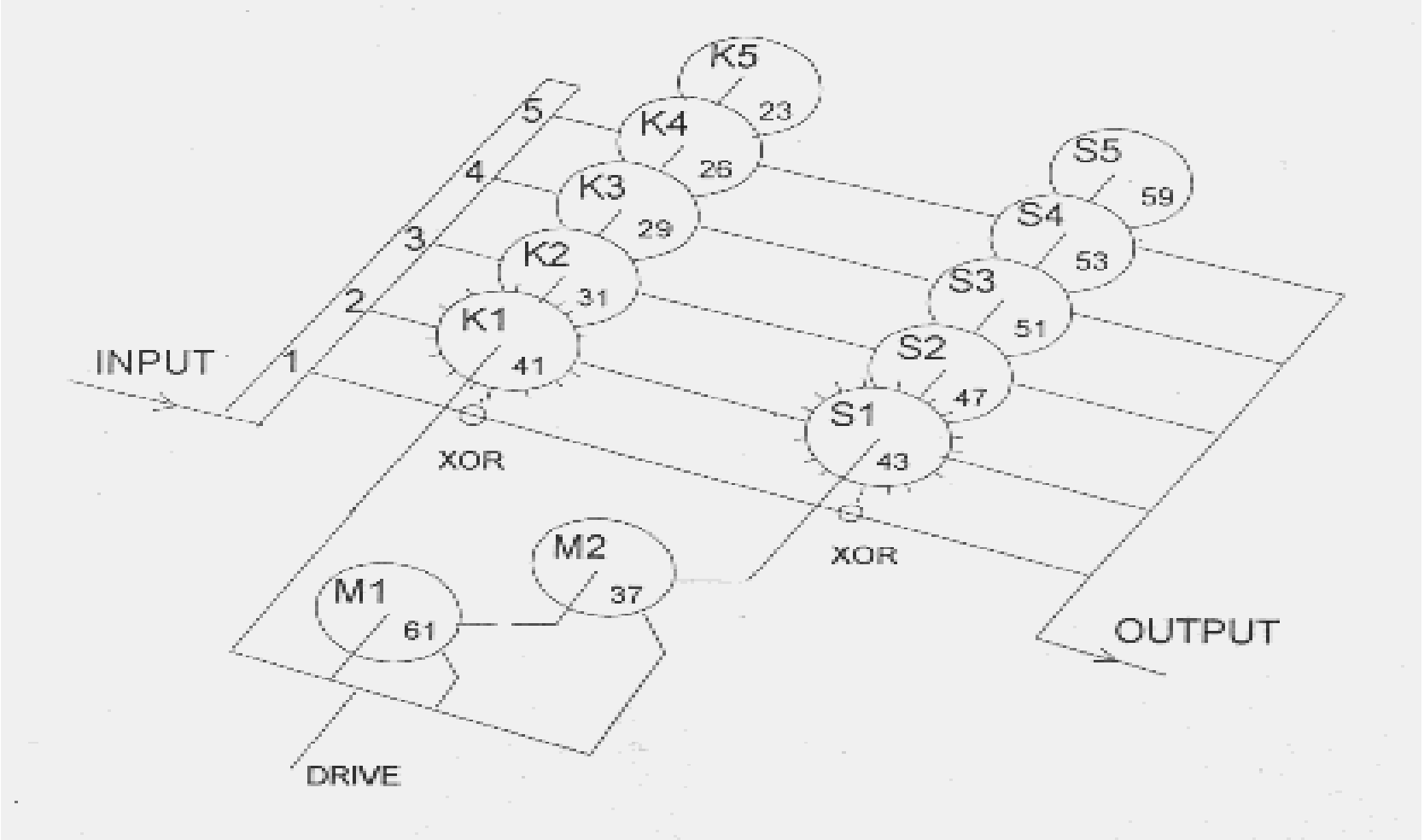
Macchina di Lorenz

- Realizzata dalla ditta Lorenz, usava 32 caratteri codificati con il codice Baudot, 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.

Macchina di Lorenz

- Sostituzione della chiave casuale (Vernam) con una chiave pseudo-casuale generata da un dispositivo meccanico (dodici rotori) secondo una procedura ovviamente segreta.
- La cifratura di Lorenz era usata per crittare le comunicazioni tra Hitler e i suoi capi di stato maggiore.
- Cifrario non più inattaccabile tanto che fu forzato dai crittanalisti inglesi del progetto Ultra

Macchina di Lorenz



Macchina di Lorenz

- Decrittaggio e forzamenti:
  - Il primo successo si ebbe grazie a una grossa ingenuità di un cifratore tedesco il 30 ago 1941
  - John Tiltman riuscì a ricostruire la sequenza oscurante della Lorenz e quindi il messaggio chiaro.
  - Bill Tutte riuscì a ricostruire completamente la struttura interna della Lorenz.

Macchina di Lorenz

- Nel 1943 nascita dei Colossi:
  - Leggevano 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.

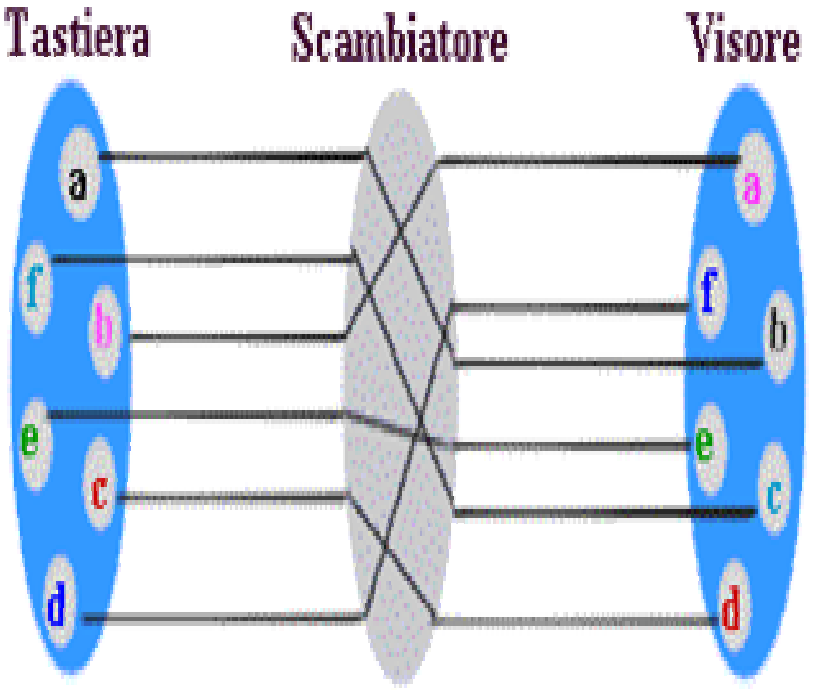
LE MACCHINE CIFRANTI: ENIGMA

SCHEDA BIOGRAFICA

- Nasce nel 1918 per mano dell'inventore tedesco Arthur Scherbius
- Scherbius aveva studiato ingegneria elettrica ad Hannover e Monaco
- Enigma nasce come versione elettromeccanica del disco cifrante dell'Alberti

SCHEMA BASE

- La versione Base del congegno di Schebius consiste in tre componenti:
- Una Tastiera
- Un'unità scambiatrice
- Un Visore con varie lampadine



PASSO 1

- Il primo passo consiste nel far ruotare il disco dello scambiatore di 1/26 di giro dopo ogni lettera battuta trasformando il cifrario da monoalfabetico a polialfabetico
- Questo metodo definisce per la macchina 26 chiavi in base alla posizione iniziale del rotore

PASSO 2

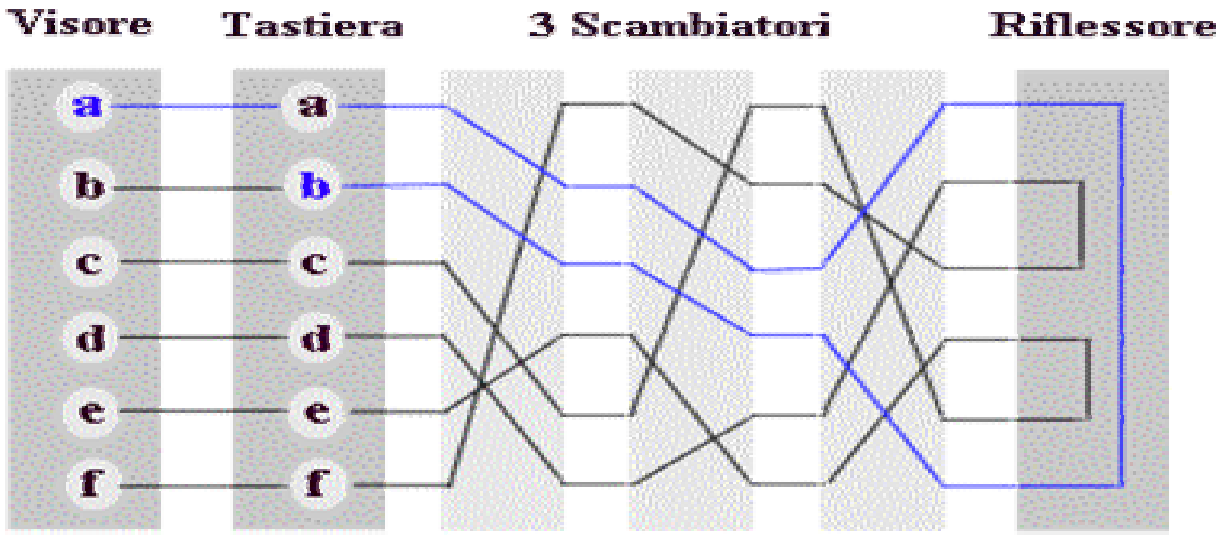
- Nel passo precedente abbiamo definito una cifratura polialfabetica con solo 26 chiavi (troppo poche)
- Si aggiunge un nuovo rotore che gira di 1/26 di giro ogni giro completo del primo rotore
- Questa nuova configurazione definisce un numero di chiavi pari a: 26 * 26 = 676

PASSO 3

- Le 676 chiavi sono ancora troppo poche
- Si aggiunge un altro rotore in cascata col secondo che porta le chiavi ad un totale di 26 * 26 * 26= 17576

PASSO 4

- Si aggiunge anche un rilessore un componente simile al rotore che non ruota ed ha entrata e uscita dallo stesso lato.
- Con questa aggiunta abbiamo il seguente schema:



PROBLEMI

- Con l'assetto attuale della macchina le chiavi sono 17576 troppo poche per scoraggiare un crittoanalista che dispone di più macchine e più aiutanti
- Per aumentare l'affidabilità occorre aumentare ancora il numero delle chiavi possibili

PASSO 5

- Si aggiunge la possibilità di permutare tra loro l'ordine dei rotori questo aumenta il numero delle chiavi di un fattore pari a 6 cioè il numero delle permutazioni possibili su tre rotori
- Il numero delle chiavi diviene: 17576 * 6

PASSO 6 (1)

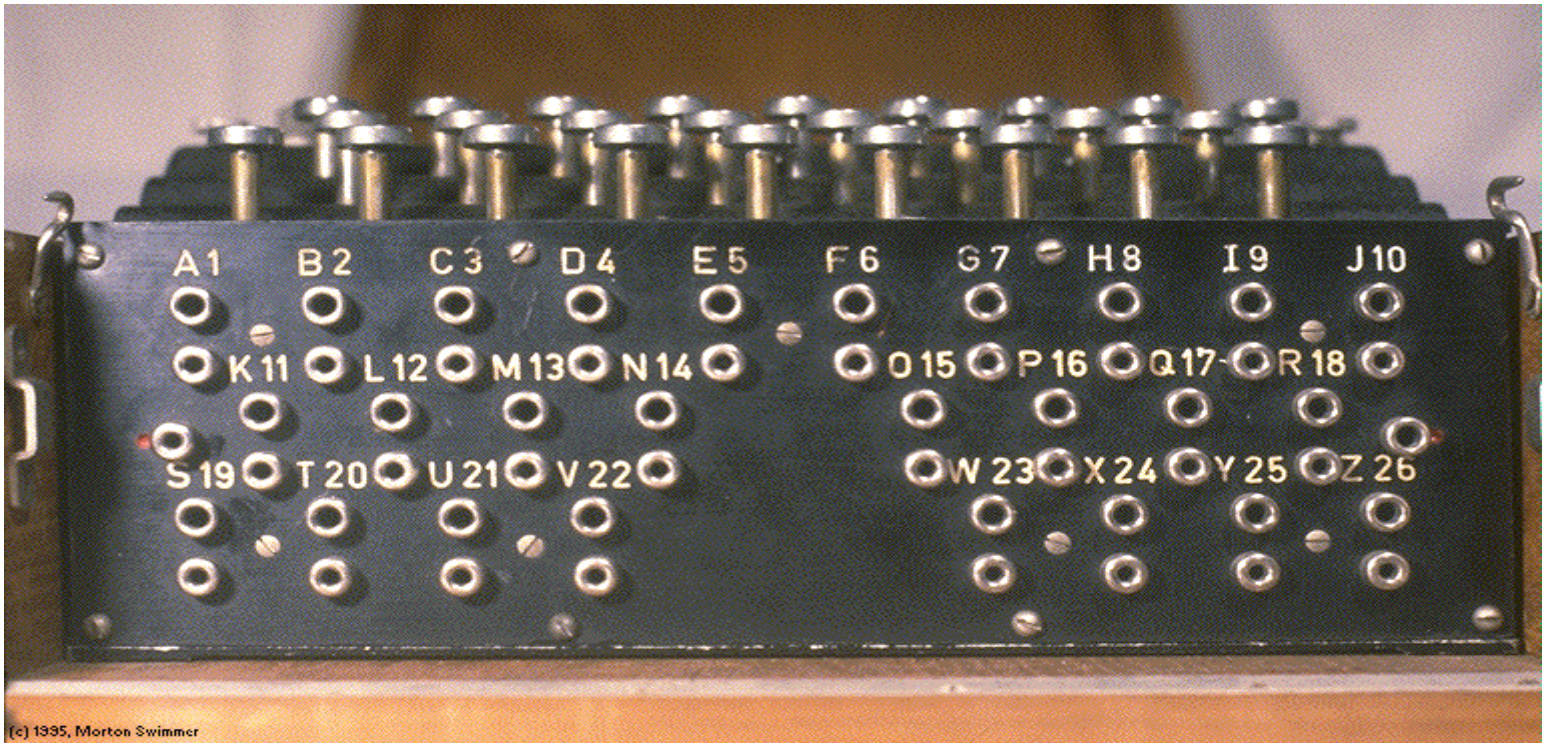
- Le chiavi sono ancora troppo poche e sarebbe quasi inutile aggiungere un altro rotore (aumento delle chiavi di un fattore pari a 26)
- Si decide di aggiungere un Pannello a Prese Multiple, tra la tastiera e il primo rotore, capace di scambiare tra loro 6 coppie di lettere prima dell'immissione nel primo rotore

PASSO 6 (2)

- Questa possibilità fa aumentare il numero di chiavi di un fattore pari a 100.391.791.500 (più di 100 miliardi), ricavati dalla formula:

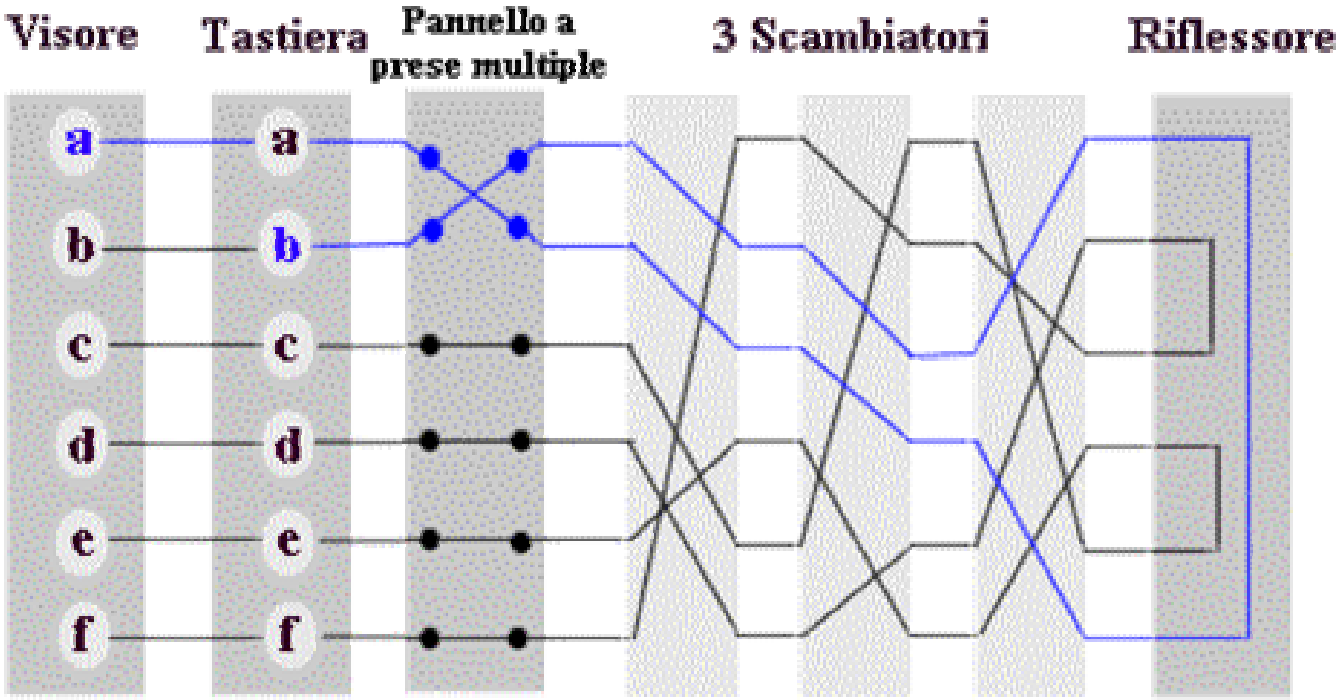
  26! / ((26 – 2p)! * p! * 2^p) dove p è il numero dei cavi

PASSO 6 (3)


A1 B2 C3 D4 E5 F6 G7 H8 I9 J10
K11 L12 M13 N14 O15 P16 Q17 R18
S19 T20 U21 V22 W23 X24 Y25 Z26
(c) 1995, Morton Swimmer

PRIMA VERSIONE ATTIVA

- Nella prima versione Enigma si presentava con il seguente schema:



FACCIAMO 2 CONTI

- Come abbiamo visto il computo totale delle chiavi della prima versione di enigma presentava un numero totale di chiavi pari a: 17576 * 6 * 100.391.791.500

  pari a:

  10.586.916.764.424.000 COMBINAZIONI
  (più di 10 milioni di miliardi)

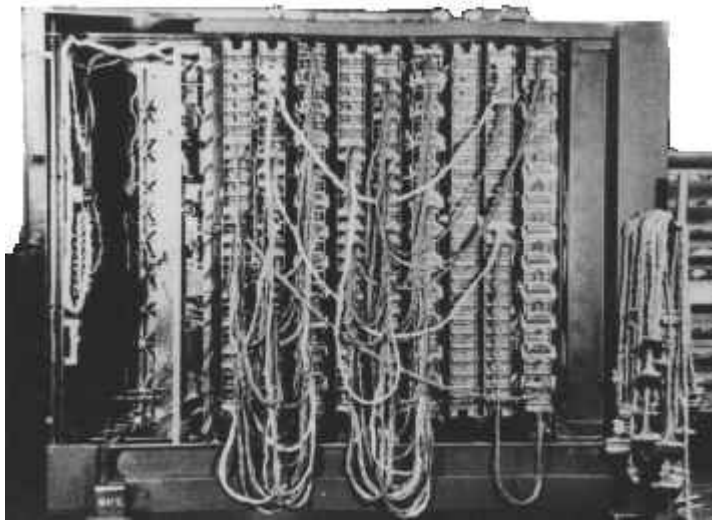
EVOLUZIONI

- Dalla metà degli anni 30 in poi il numero di chiavi disponibili per Enigma aumentò con l'aggiunta di 2 rotori le permutazioni passarono da 6 a 60, e con l'aumento dei cavi dello scambiatore da 6 a 10 il numero totale di chiavi arrivò ad un numero record di: 158.962.555.217.826.360.000 (quasi 159 miliardi di miliardi di combinazioni)

COMMENTI FINALI

- Con un simile macchinario i tedeschi si sentivano tranquilli circa la sicurezza del loro codice eppure non fu così …

LE MACCHINE CIFRANTI: LE BOMBE DI TOURING



I CRITTOANALISTI POLACCHI

- Dal 1926 in poi (anno in cui le forze germaniche iniziarono ad utilizzare Enigma) l'unica nazione che tentò di codificare il codice fu la Polonia.
- Il lavoro venne svolto all'interno del Biuro Szyfrov con la presenza di molti matematici tra cui: Marian Rejevsky

L'IDEA DI BASE

- L'idea di base di Rejewsky si basava su un errore dei tedeschi in quanto questi all'inizio di ogni messaggio ripetevano 2 volte (criptandolo con la chiave di giornata) la chiave del messaggio, e come si sa la ripetizione è nemica della crittologia

UN ESEMPIO (1)

Poniamo per esempio che venissero ricevuti i seguenti quattro messaggi
(ne consideriamo solo le prime sei lettere):

L O K R G M
M V T X Z E
J K T M P E
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:

Pr. 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
Qu 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

UN ESEMPIO (2)

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

Naturalmente lo stesso procedimento andava ripetuto per tutte le altre lettere dell'esagramma iniziale

La cosa importante è che il numero di collegamenti è indipendente dal pannello ma dipende solamente dai rotori (scambiatori) , per cui con questa analisi era possibile escludere un gran numero di configurazioni a priori, quindi si devono verificare "soltanto" 6 * 17576 = 105456 configurazioni

LA BOMBA DI REJEWSKY

- Poco dopo il matematico progettò una macchina in grado di controllare velocemente tutte le 17576 combinazioni di una data permutazioni, Rejewsky le chiamò Bombe, all'inizio ne servivano 6 ma quando vennero aggiunti gli altri 2 rotori le 60 macchine erano troppo per il governo polacco ed il tutto si trasferì in Inghilterra

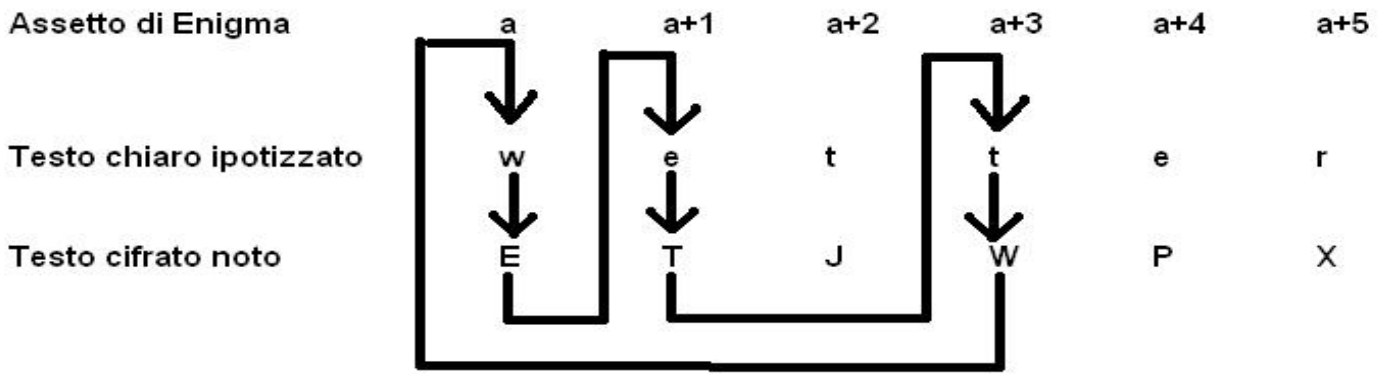
BLECHLEY PARK

- Dal 1939 in poi gli sforzi per risolvere il codice enigma si spostarono in Inghilterra presso la sede de GC&CS (Government Code & Cypher School)
- Qui erano presenti molti matematici, tra gli altri anche Alan Touring

I CRIB

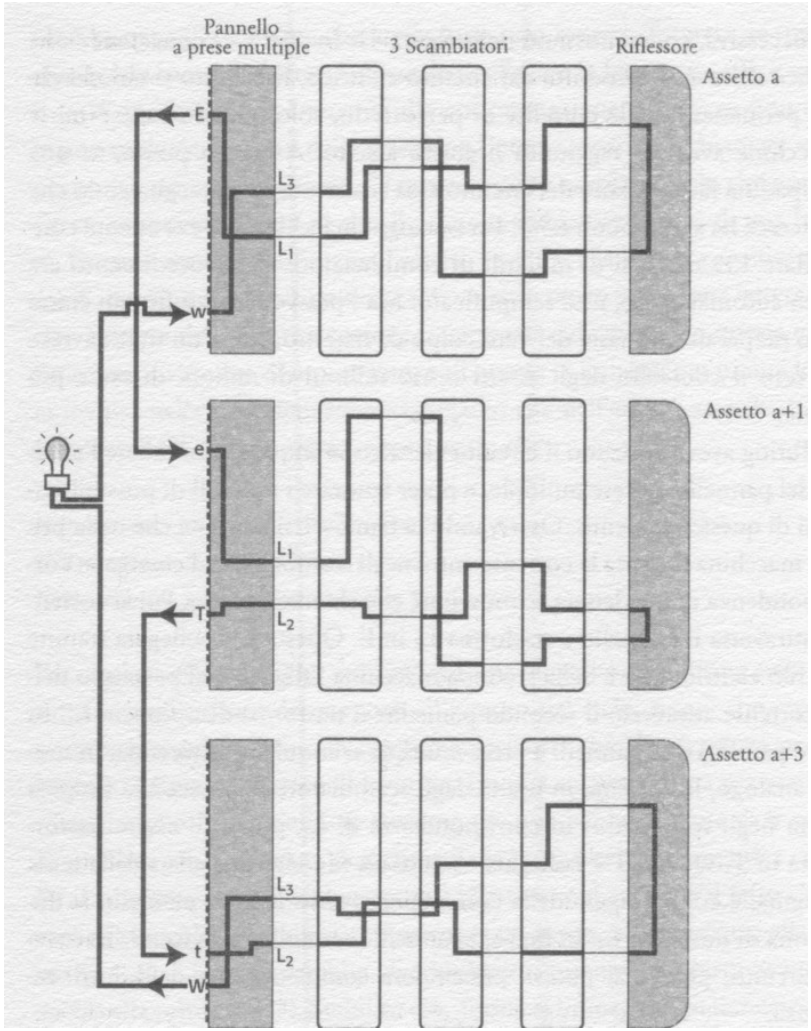
- In crittografia un Crib è una parte di codice criptato di cui si conosce il significato in chiaro
- Alan Touring sfruttò questi Crib per creare una macchina capace di trovare la configurazione esatta dei rotori in “poco tempo”

UN ESEMPIO DI CRIB



- Analizzando la concatenazione possiamo dire che :
- 1. In assetto a Enigma cifra w con E
- 2. In assetto a+1 Enigma cifra e con T
- 3. In assetto a+3 Enigma cifra t con W

LA BOMBA DI TOURING (1)

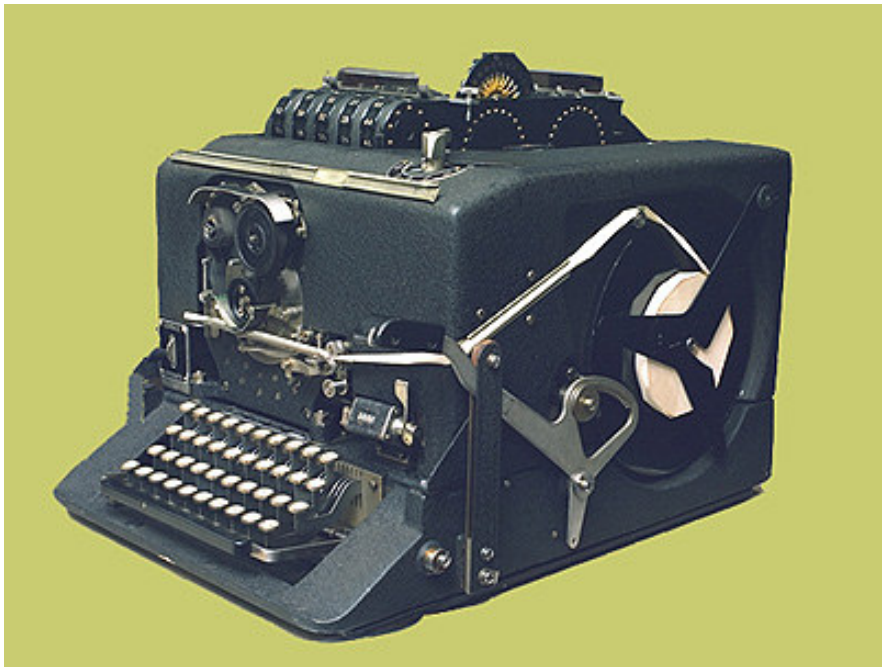


- Partendo da queste considerazioni Touring sviluppò una macchina che provava tutte le configurazioni accettabili per un dato crib in un tempo accettabile creando una sorta di macchina Enigma aperta con cui si poteva collegare l'uscita di una all'ingresso dell'altra secondo lo schema qui a fianco.

LA BOMBA DI TOURING (2)

- Naturalmente furono necessarie ben 60 bombe di Touring con una spesa complessiva di ben 100000 sterline
- Con il progresso tecnologico le bombe arrivarono a trovare la chiave giornaliera in meno di un'ora
- Questo contribuì notevolmente alla vittoria della guerra da parte degli alleati

LE MACCHINE CIFRANTI:
Sigaba



Sigaba

- William Friedman (1891-1969)
  Frank Rowlett (1908-1998)

- Evoluzione della macchina ENIGMA

- Non risulta alcuna forzatura di questa macchina nel periodo in cui era in uso

Origine di Sigaba

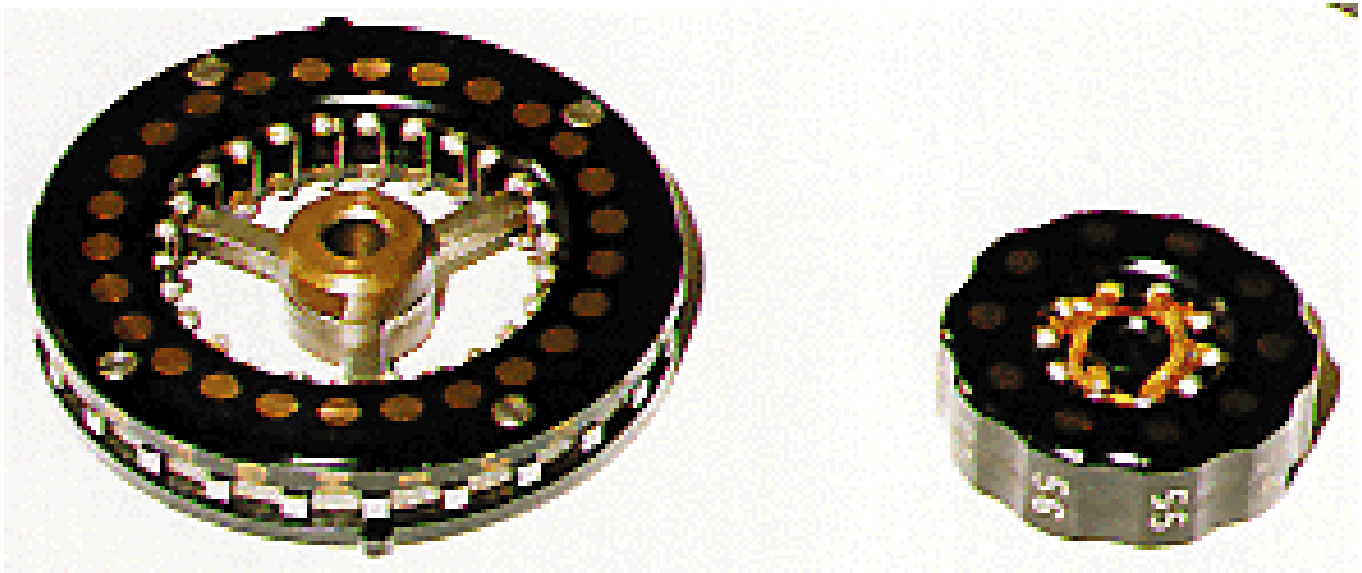
Punto debole di ENIGMA:

- Meccanismo di rotazione dei rotori (semplice contatore)
  - L'aumento di rotori non garantiva la sicurezza della macchina

Origine di Sigaba

- 1935 nascita dell'ECM (Elettric Cipher Machine):
  - Chiave: nastro metallico forato per il passaggio di corrente per determinare la posizione dei rotori

I Rotori



Svantaggi dell'ECM

- Nastro identico per tutte le macchine che comunicano
- Semplice calcolo per determinare le regolazioni potenziali dei rotori della macchina

Sviluppo dell'ECM

- 1941 esercito e marina si sono associati :
  - Creazione di un sistema crittografico unico: "SIGABA"
- Al posto del nastro perforato si sviluppa nuovo insieme di rotori più controllato (Rowlett)
- Potenziamento e semplificazione dell'utilizzo

Funzionamento di Sigaba

- Equivale a “due ENIGMA in una”
- Cablaggio interno (segreto)
- 15 rotori:
  - 5 per la cifratura
  - 10 per generare una sequenza pseudo-casuale che stabilisce quali rotori ruotano ad ogni passo
- Dispositivo di stampa che ne migliora la comodità operativa

LE MACCHINE CIFRANTI: PURPLE

Purple

- Creata dai giapponesi negli anni ’30
- Destinata alla crittografia ad alto livello
- Maggior parte delle macchine a bordo delle navi

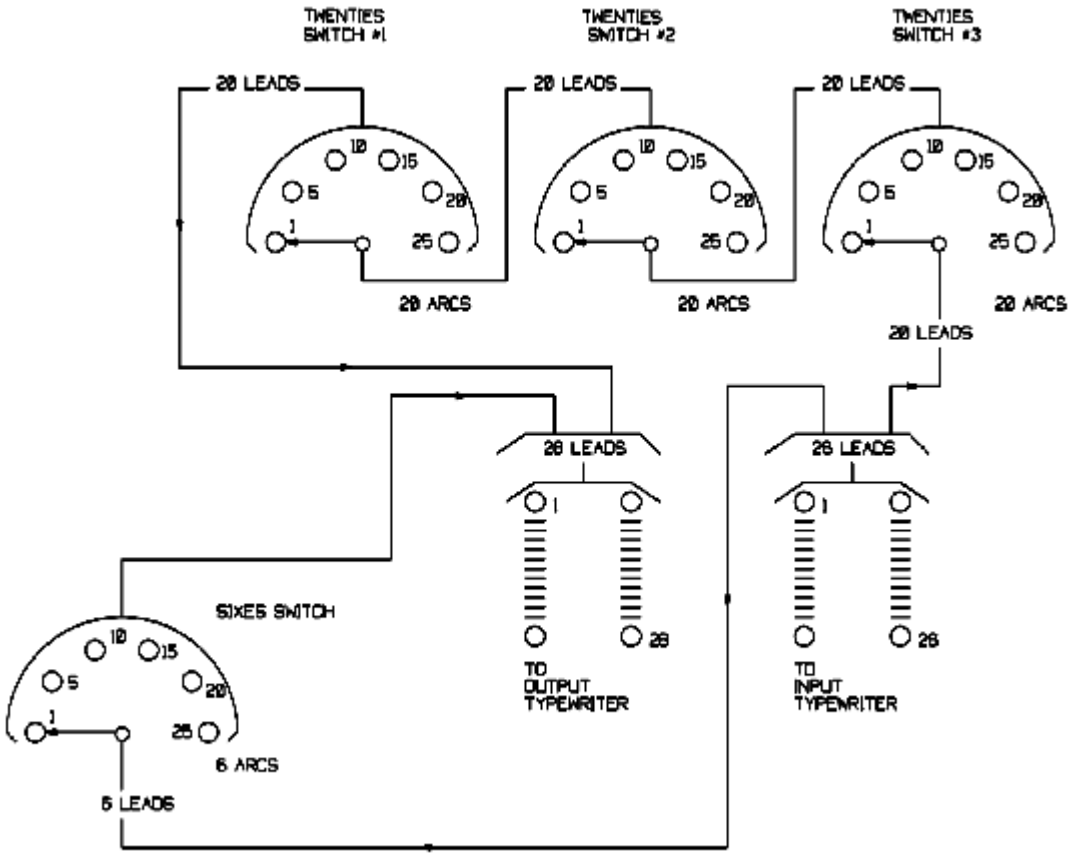
Purple

- Si supponeva inattaccabile
- Decrittata da Friedman 18 mesi dopo aver capito il principio di funzionamento (1940)
  - Metodo meccanizzato con la macchina Magic

Funzionamento di Purple

- Nuova macchina diversa da ENIGMA
  - Nessun rotore, ma switch di tipo telefonico
    - In modo da rendere meno prevedibile la rotazione dei rotori
  - Alfabeto di 26 caratteri diviso in 2 gruppi:
    - 6 lettere (AEIOUY)
    - 20 lettere

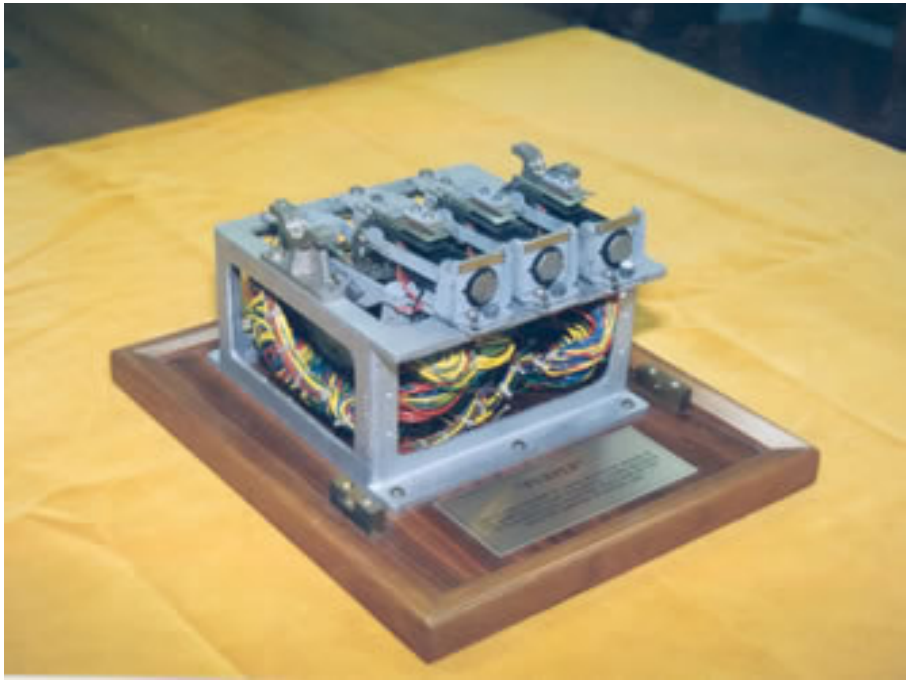
Funzionamento di Purple



Purple

- Nessun esemplare originale rimasto
- Unico frammento a Berlino nel 1945
  - (Museo Crittologico Nazionale di Washington)

Purple



Riferimenti telematici

- http://www.nsa.gov
- http://www.liceofoscarini.it
- http://www.icsm.it
- http://www.museoscienza.org
- http://www.dia.unisa.it
- 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"

(Novalis Enrico di Ofterdingen)