www

La macchina ha un input da tastiera, un meccanismo di trasformazione del simbolo pigiato (pannello frontale, rotori e pannello riflettore) e una tastiera con pulsanti illuminati in output

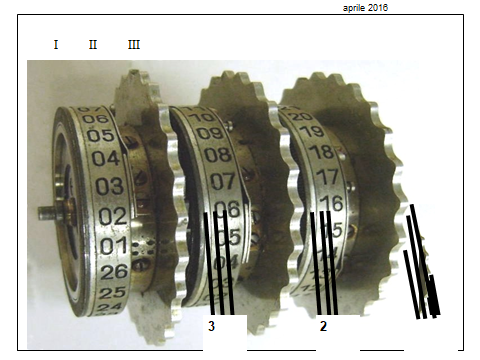


Pigiando un tasto il segnale passa per il pannello frontale dove può subire una prima trasformazione.

Alcune lettere (da 6 a 10 dipende dal modello), attraverso al pannello frontale, sono accoppiate ad altre in modo fisso mediante un cavo.

Esempio di pannello: (S,D), (F,G), (H,B), (O,P), (Z,C), (X,N)

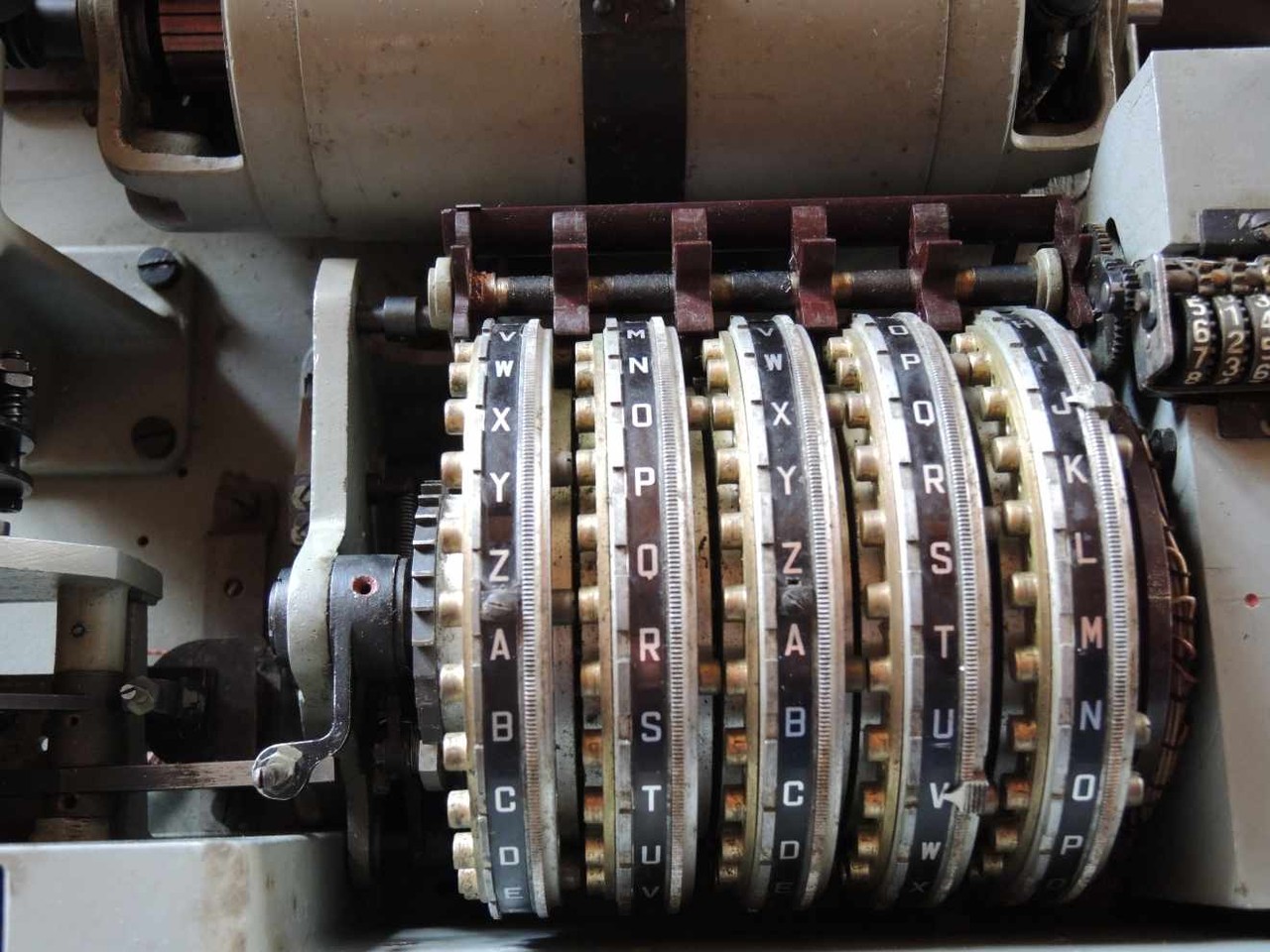
.



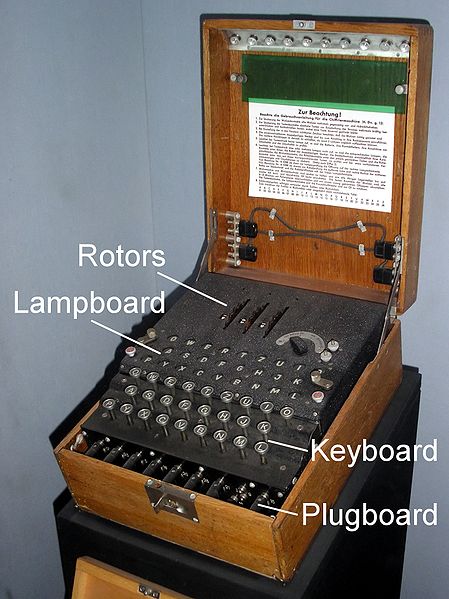


Mmm

Il segnale arriva quindi alla sequenza dei rotori (da 3 a 6 a seconda del modello); quindi un pannello riflettore fa rientrare il segnale nella sequenza dei rotori a verso invertito; quindi passando dal pannello frontale il segnale accende uno dei tasti luminosi.

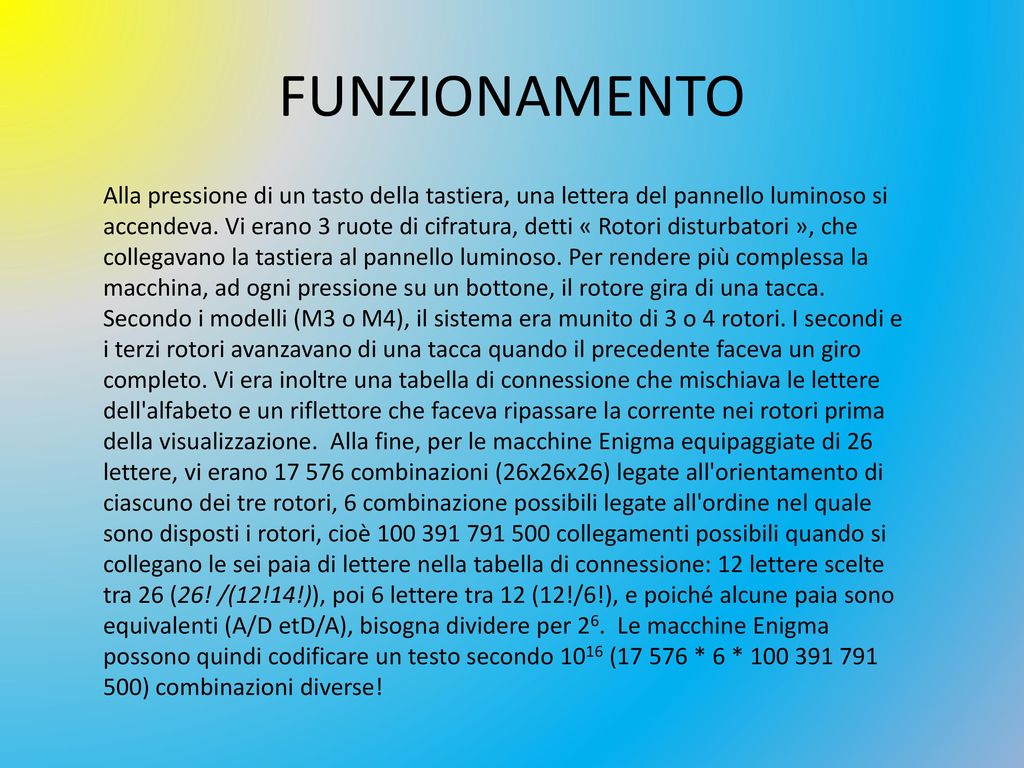




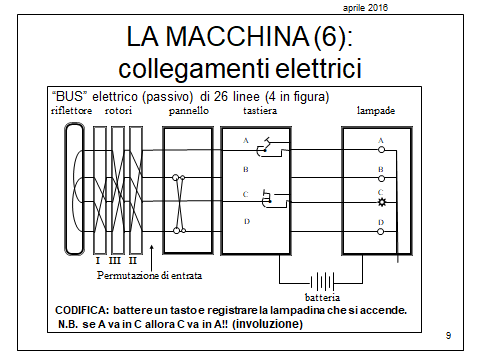


Mmm

mmm



mmm



**LA PREDISPOSIZIONE DELLA MACCHINA**

**Informazioni presenti su manuale**

**chiave del “mese”** ordine dei rotori: II I III

**chiave del “giorno”** lettere per posizionare le tacche

**pannello di commutazione**: per esempio (BD) (FK) (GZ) (ER) (TD) (W B)

**A scelta dell’operatore**

**chiave del “messaggio”** tre lettere scelte dall’operatore: A B C

**NUMERO DELLE COMBINAZIONI POSSIBILI**

disposizione dei 3 rotori 3! = 6 (60 co 3 rotori su 5)

posizionamento delle tacche 262 = 676

posizione iniziale dei 3 rotori 263 = 17576

pannello di commutazione 6 cavi 1011

numero totale di disposizioni possibili 6x262x263x1011 = 1016

**LA CODIFICA E TRASMISSIONE DEL MESSAGGIO**

PRIMA PARTE

impostazione della macchina: chiave del mese + chiave del giorno + pannello di commutazione;

scelta della chiave di messaggio (es.: ABC) e codifica della chiave di messaggio **duplicata** (es.: ABCABC → KPZDTF)

SECONDA PARTE

Riposizionamento dei rotori con la chiave del messaggio e codifica del testo del messaggio.

TERZA PARTE

Trasmissione, per telegrafo o telefono, del testo codificato con in testa la chiave di messaggio, precedentemente codificata, (duplicata).

**OPERAZIONI DI DECODIFICA**

PRIMA PARTE

Impostazione della macchina: chiave del mese + chiave del giorno + pannello di commutazione;

Decodifica dei primi 6 caratteri del messaggio cifrato per verificare la chiave del messaggio **duplicata** (es.: ABCABC → KPZDTF) posta in testa del messaggio.

SECONDA PARTE

Riposizionamento dei rotori

TERZA PARTE

Decodifica del messaggio.

**DECIFRATURA POLACCA**

Si utilizzano dispositivi virtuali (la matematica delle permutazioni e Rejevski per progettare tentativi di configurazioni) e dispositivi reali (le “bombe polacche” per simulare il funzionamento di enigma).

In una prima fase il metodo ha funzionato perché i Polacchi si sono accorti che ogni messaggio iniziava con la chiave del giorno scritta due volte! Le prime sei lettere di un messaggio iniziavano per esempio con SGKGBZ. Quindi la prima lettera del messaggio veniva trasformata prima in S e poi in G, la seconda in G e poi in B e la terza in K e poi in Z.

Questi metodi forniscono risultati soddisfacenti finché la chiave di messaggio viene trasmessa duplicata.

Con queste informazioni, con la conoscenza matematica sulle permutazioni, con lo spionaggio, con la fortuna di aver trovato una ENIGMA intatta su un sommergibile alla deriva e con l’aiuto delle *bombe*, gli alleati sono inizialmente riusciti a decrittare ENIGMA.

Vedi esempio di CODIFICA/DECODIFICA DI UN MESSAGGIO: INVOLUZIONE.

Appendice G-7

**DECIFRATURA INGLESE**

Due difficoltà: 1) non sono più trasmesse le chiavi duplicate e

2) si passa da tre a cinque dischi .

Unico attacco possibile (già realizzato con relativo successo dai polacchi negli ultimi tempi) rimane il *plain text attack*. Si ipotizzano (parti di) testi oggetto delle comunicazioni tedesche e si costruiscono sistemi che, simulando ENIGMA, ne forniscono una versione crittografata.

Obbiettivo: individuare la chiave di messaggio (configurazione dei rotori all’inizio del messaggio).

Si parte da un vincolo “matematico”: per esempio nessuna lettera può essere trasformata in se stessa; e si adotta lo stratagemma dei *crib* e del *gardening*. Si continua ad usare macchine che simulano le funzioni di ENIGMA (le bombe inglesi e Colossus).

Introduzione, alla fine del 1939, dei *crib* (termini che si ipotizza siano presenti nel messaggio, per esempio sulla meteorologia, sulle località con operazioni critiche in corso, nomi comuni nel gergo militare, ..) e del *gardening* o *planting a crib* (distribuire dei crib nei testi usati nei tentativi di simulazione).

The process used [sequential](https://en.wikipedia.org/wiki/Sequential_analysis) [conditional probability](https://en.wikipedia.org/wiki/Conditional_probability) to infer information about the likely settings of the Enigma machine.

Turing e Newmann suggeriscono la tecnica basata sui “crib”, cioè ipotizzare che il messaggio contenga qualche parola chiave (per esempio “wettervorhersage” (previsione del tempo) e fare ipotesi sulla struttura di ENIGMA verificando la comparsa di queste parole e scartando sistematicamente le ipotesi che trasformavano una lettera in se stessa. Le previsioni del tempo sull’Atlantico scritte nello stesso formato in ogni giorno sono risultate cruciali.

Il contributo di Turing in questa fase è determinante per sfruttare la parte linguistica/matematica del progetto ENIGMA; Tommy Flowers e Max Newmann sono determinanti per la costruzione di Colossus.

COLOSSUS

Colossus può essere definito come il primo calcolatore elettronico digitale programmabile; ma **Colossus non è un computer**: infatti

1 era programmato con interruttori e cavetti di collegamento e non con un programma memorizzato e

2 poteva eseguire solo calcoli di tipo combinatorio per riconoscimento di configurazioni

3 non era general purpose.

**.**

.