Crittografia con Python

Corso introduttivo
Marzo 2015

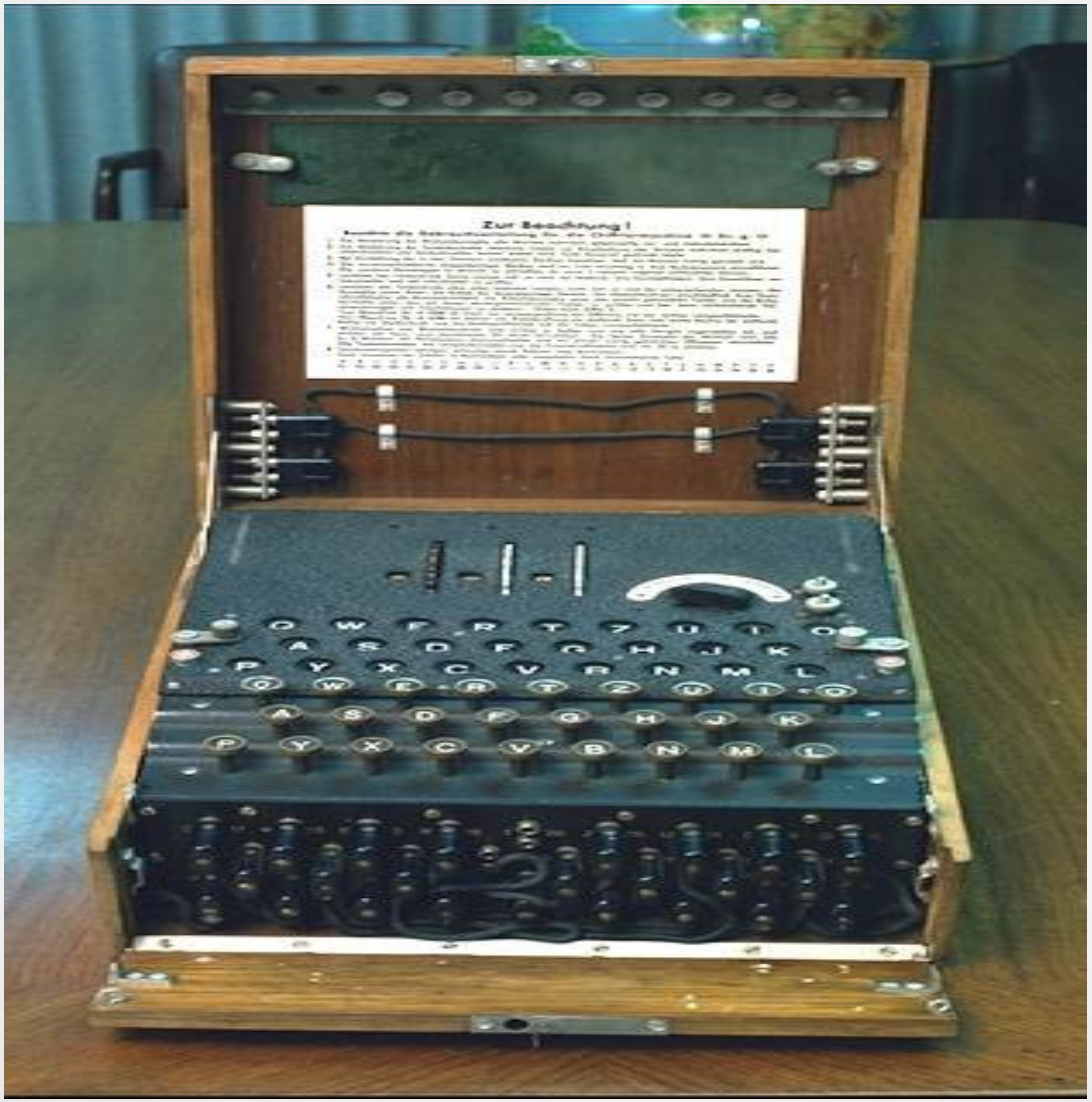
Con materiale adattato dal libro “Hacking Secret Cypher With Python”
di Al Sweigart (http://inventwithpython.com/hacking/index.html)

Prof. Alessandro Bugatti

Un esempio storico: Enigma

- Macchina usata dai Tedeschi nella Seconda Guerra Mondiale per cifrare i messaggi dell'Esercito
- Cifrario a sostituzione in cui l'alfabeto cifrante continua a cambiare (cifratura polialfabetica)

La macchina Enigma



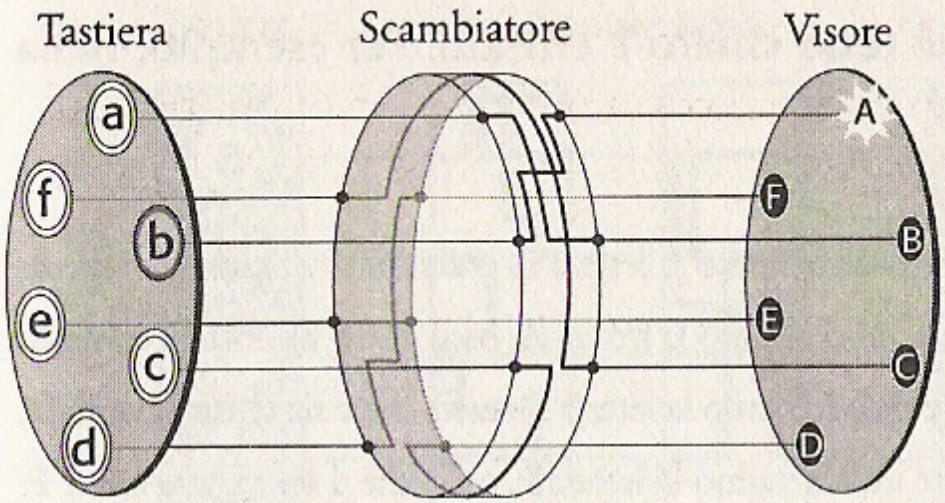
Cenni storici

- Inventata dall'inventore tedesco tedesco Arthur Scherbius nel 1918 (nello stesso periodo anche altri brevettarono idee simili)
- E' una macchina elettro-meccanica, in cui si realizza un'automazione del processo di cifratura
- Aumenta la sicurezza rispetto ai metodi precedenti

Funzionamento

- Combinazione di cifrario polialfabetico e monoalfabetico
- L'idea fondamentale è quella dei rotori scambiatori.
- Ogni rotore effettua una cifratura monoalfabetica fissa ed è costituito da un disco di gomma attraversato da fili elettrici secondo lo schema seguente

Anello scambiatore



a	→ B
b	→ A
c	→ D
d	→ F
e	→ E
f	→ C

Figura 26 Versione semplificata della macchina Enigma con un alfabeto di sei lettere. L'elemento più importante di Enigma è lo scambiatore. Digitando **b** sulla tastiera a sinistra, la corrente entra nello scambiatore, segue il percorso dei fili elettrici ed emerge in modo da illuminare la lettera **A**. In breve, **b** è crittata come **A**. Il riquadro a destra riassume il modo in cui ogni elemento dell'alfabeto di sei lettere è crittato.

I rotori

- Ad ogni pressione di un tasto il rotore effettua una rotazione di 1/26 di angolo giro, modificando così l'alfabeto cifrante
- Vengono poi utilizzati 3 rotori: ogni volta che il rotore più interno compie un giro completo quello alla sua sinistra compie 1/26 di giro e lo stesso vale per quello più esterno.
- In totale 26x26x26 alfabeti cifranti diversi, cioè

17576

Il riflessore

- Per far sì che la macchina potesse sia crittare che decrittare in maniera perfettamente simmetrica fu inserito un riflessore
- Questo non era altro che un circuito fisso che faceva tornare indietro il segnale su un altro percorso.
- In questo modo inserendo il testo cifrato si otteneva il testo in chiaro

Schema completo

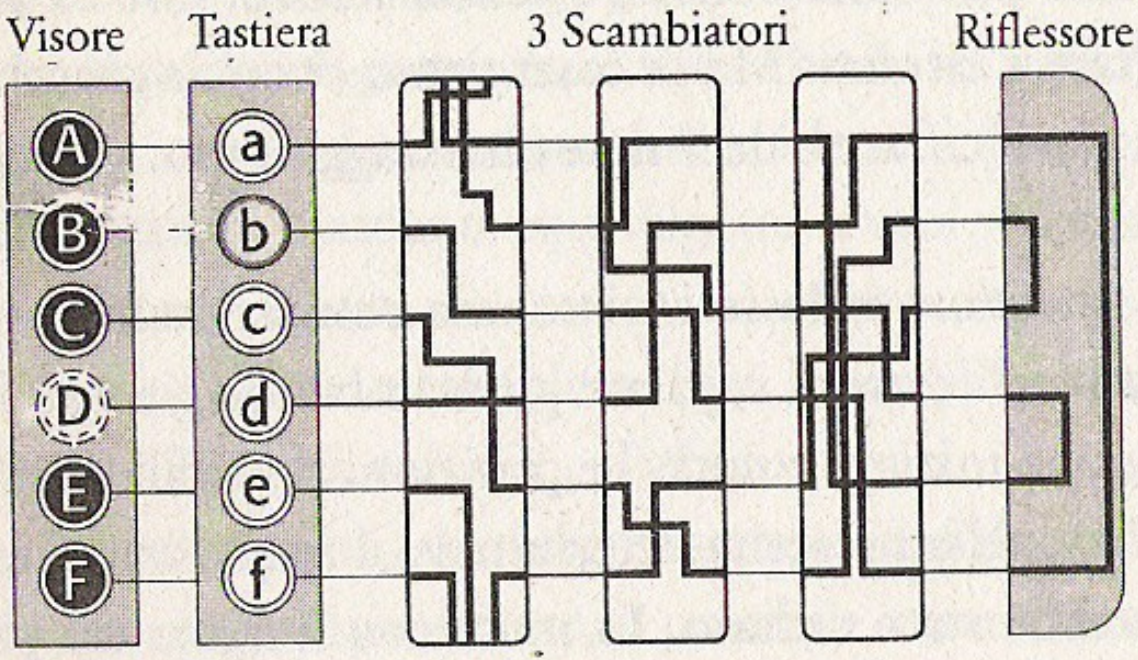


Figura 29 Il progetto di Scherbius del modello base di Enigma includeva un terzo scambiatore e un riflessore, che costringeva l'impulso elettrico ad attraversare di nuovo gli scambiatori. Con questo assetto particolare, la pressione del tasto **b** determina l'illuminazione di **D** sul visore, qui raffigurato accanto alla tastiera.

Permutazione dei rotori

- Per aumentare il numero di alfabeti cifranti viene fatto in modo che i rotori possano essere messi a piacere nei 3 alloggiamenti
- Questo genera 6 diverse possibili permutazioni di rotori, aumentando di un fattore sei il numero di alfabeti cifranti possibili

$$17576 \times 6 = 105456$$

Pannello a prese multiple

- Il numero di alfabeto cifranti è grosso ma non tale da scoraggiare la crittoanalisi per forza bruta.
- Viene aggiunto allora un pannello a prese multiple composto da 26 prese e 6 fili conduttori: ogni filo connette due prese che rappresentano due lettere in modo che vengano scambiate fra loro

Pannello a prese multiple

- I possibili modi di connettere i 6 fili tra le 26 prese sono 100.391.791.500, aumentando così decisamente il numero di alfabeti cifranti

10.586.916.764.424.000

- Perchè non avere unicamente il pannello a prese multiple che da solo dà il maggior contributo? Perchè preso singolarmente non è altro che un cifrario monoalfabetico...

Riassumendo...

- *Scambiatori*: (detti anche *Rotori*) ognuno dei tre dischi rotanti poteva orientarsi in 26 modi nel piano perpendicolare al suo asse di rotazione. Di conseguenza, erano ammesse 17.576 (26x26x26) combinazioni di orientamenti.
- *Unità cifratrice*: i tre scambiatori potevano essere inseriti nell'unità centrale in diverse posizioni reciproche, così riassumibili: 123, 132, 213, 231, 312, 321. Erano quindi ammesse 6 diverse posizioni reciproche dei rotori.
- *Pannello a prese multiple*: i possibili abbinamenti di 12 (6 x 2) lettere su 26 sono moltissimi, 100 miliardi 391 milioni 791 mila 500

Il numero totale di chiavi si ottiene moltiplicando le suddette possibilità: 17.576 x 6 x 100.391.791.500 = circa 10 milioni di miliardi...

Caratteristiche di Enigma

- La macchina originale era di dimensioni 34x28x15 cm, pesava 12 Kg e costava circa 100.000 euro attuali.
- Per utilizzarla si doveva aver la chiave, composta dalla posizione dei rotori (orientamento e disposizione) e dalla posizione delle prese.
- Si premeva un tasto e si segnava su di un foglio la lampadina accesa corrispondente

Attaccare Enigma

- Apparentemente Enigma non aveva punti deboli, in realtà uno studio accurato del meccanismo da parte di alcuni tra i più brillanti scienziati del tempo e alcuni errori nell'utilizzo permisero di violarla.
- Enigma fu adottata dall'Esercito tedesco nel 1925 e fino alla fine della guerra ne furono prodotti 30.000 esemplari.

I crittoanalisti polacchi

- Grazie al tradimento del tedesco Schmidt i francesi vennero in possesso dei piani di costruzione di Enigma e li passarono ai polacchi ritenendo non fosse possibile violare Enigma
- I servizi segreti polacchi costituirono un gruppo di crittoanalisi affidandosi a dei matematici, di cui il più brillante fu Marian Rejewski

Utilizzo di Enigma

- Ogni giorno i tedeschi utilizzavano una chiave diversa.
- Per evitare di produrre tantissimo testo cifrato con la stessa chiave veniva spedita una chiave di messaggio formata da tre lettere utilizzando la chiave giornaliera e poi il resto del messaggio era crittato con la chiave di messaggio

Errori nell'utilizzo

- La chiave di messaggio veniva ripetuta due volte all'inizio del messaggio, per evitare errori in ricezione.
- Questo era un appiglio per i crittoanalisti, in quanto sapevano che la prima e la quarta lettera erano la stessa e che i rotori la trasformavano in due lettere distanti tra loro tre movimenti del rotore.

Le concatenazioni

- Avendo a disposizione un numero sufficiente di messaggi era possibile associare ad ogni lettera dell'alfabeto la sua corrispondente tre posizioni dopo
- Esempio: se la parola in chiaro (la chiave di messaggio) fosse stata **liuliu** e dopo la cifratura fosse divenuta **gthfgy** si poteva associare la **g** con la **f**

La struttura delle concatenazioni

- Rejewski notò che c'erano delle strutture particolari che chiamò concatenazioni

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
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

- Nell'esempio precedente la A è legata alla F, la quale è legata alla W la quale è legata alla A che chiude la concatenazione

Esempio

- Scrivendo tutte le concatenazioni (anche quelle generate dalla seconda e quinta lettera e dalla terza e sesta lettera) si arriva ad avere un insieme di concatenazioni che risulta univoco e identifica una particolare chiave.
- Inoltre Rejewski notò come il pannello scambiatore non influenzi questo risultato

Raccolta delle configurazioni

- A questo punto è “sufficiente” schedare tutte le configurazioni di Enigma associandogli le concatenazioni generate.
- Questo lavoro impegnò Rejewski e i suoi aiutanti per un anno, ma alla fine le 105.456 configurazioni furono catalogate.
- In questo modo la prima versione di Enigma venne violata (il pannello scambiatore non poneva troppi problemi)

Le bombe

- Successivamente i tedeschi modificarono gli scambiatori rendendo inutilizzabile il catalogo.
- Rejewsky costruì un meccanismo (chiamato bomba) che era in grado di controllare velocemente le 17576 posizioni degli scambiatori e in due ore trovare la chiave
- Ne costruirono 6, uno per ogni disposizione dei rotori

Miglioramenti di Enigma

- Nel 1938 i tedeschi aggiunsero due nuovi rotori, così le possibili combinazioni di rotori passarono da 6 a 60.
- Inoltre i cavi per il pannello a prese multiple diventarono dieci invece che sei
- Bisognava costruire altre 54 bombe e anche dedurre i collegamenti dei due nuovi rotori

Passaggio di consegne

- Nel giugno 1939 la Polonia, attendendosi l'invasione tedesca, passò tutto il lavoro fatto su Enigma a francesi e inglesi, sia teorico che concreto (Enigma)
- Il 1 settembre 1939 la Polonia fu invasa e iniziò la Seconda Guerra Mondiale

Bletchley Park

- Gli inglesi , considerando insufficiente la stanza 40, costituirono un centro per la crittoanalisi a Bletchley Park
- Per la prima volta non furono arruolati solo linguisti e umanisti ma anche studiosi di discipline scientifiche
- Il personale passò da 200 persone all'inizio della guerra a 5000 alla fine

Altri errori

- I tedeschi fecero altri errori che resero Enigma meno sicuro:
  - cillies
  - regolarità nel posizionamento dei rotori
  - collegamenti tra le prese multiple che escludevano alcune possibilità

Alan Turing

- Nato a Londra nel 1912
- Ammesso al King's College nel 1931, ebbe modo di incontrare Russell, Whitehead, Wittgestein
- Lavorò sul teorema dell'indecibilità di Godel e nel 1937 pubblicò *On computable numbers*, il suo lavoro più significativo, nel quale introdusse il concetto di "Macchina di Turing"

Arrivo a Bletchley Park

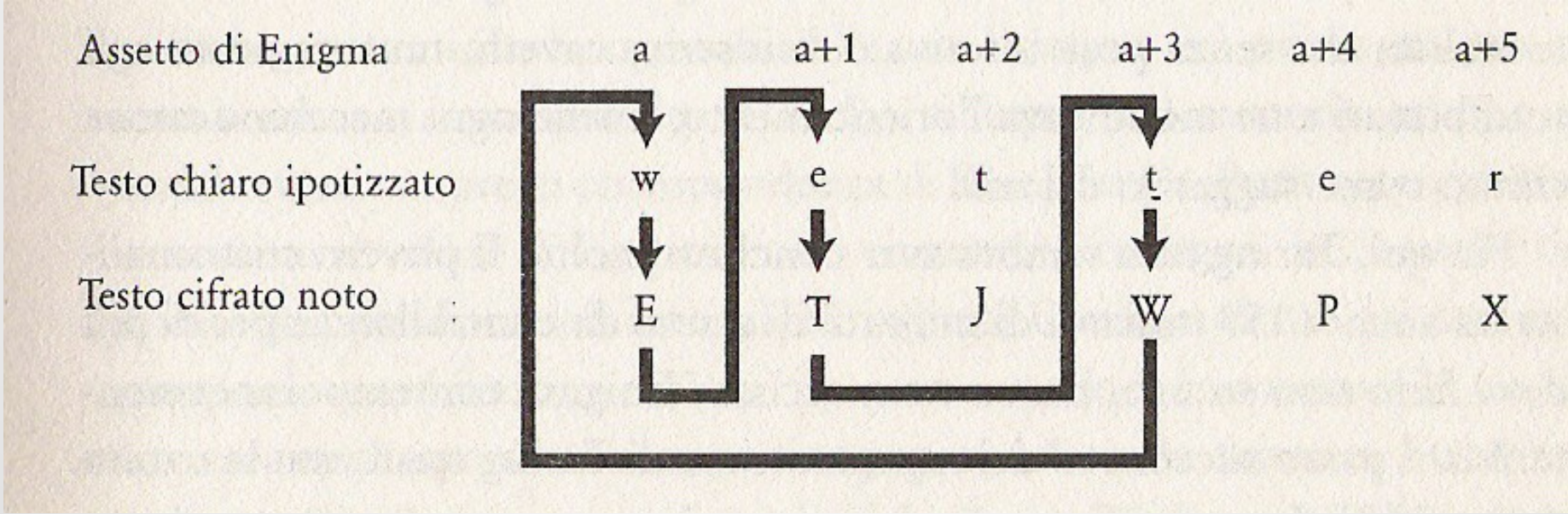
- Nel 1939 Turing arrivò a Bletchley Park e vi rimase fino alla fine della guerra
- Gli fu affidato il compito di individuare nuovi metodi che avrebbero permesso di violare Enigma anche quando i tedeschi non avessero più trasmesso due volte la chiave di messaggio

I cribs

- I cribs erano delle parole nei messaggi tedeschi di cui si riusciva a prevedere, con osservazioni esterne alla crittanalisi, il valore in chiaro
- Esempio: le comunicazioni tedesche ad una certa ora erano bollettini meteo ed era molto probabile che contenessero la parola **wetter** in una certa posizione

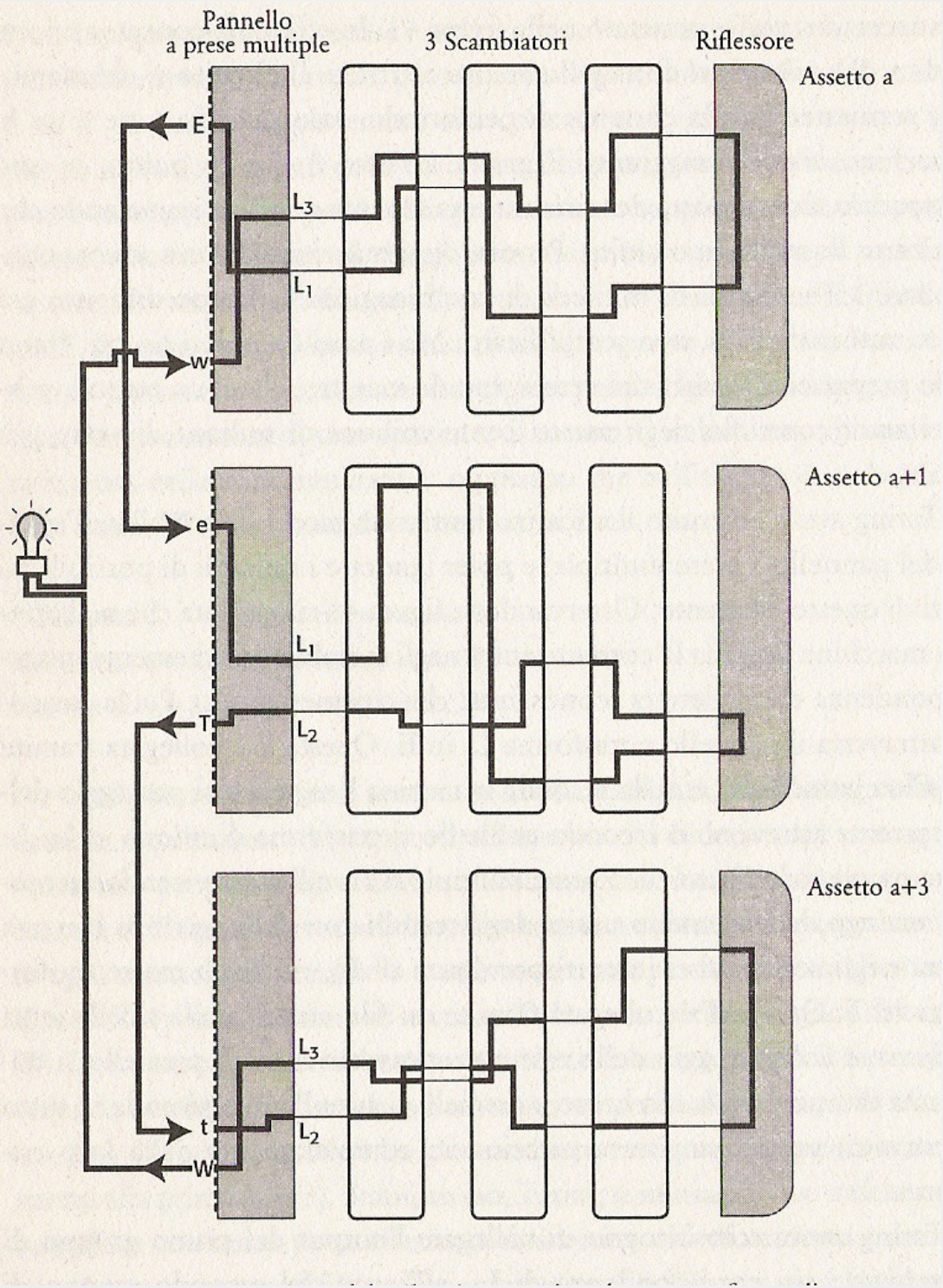
Nuove concatenazioni

- Come Rejewski anche Turing individuò delle concatenazioni create dal processo di cifratura



Le bombe di Turing

- Decise di collegare insieme tre macchine Enigma con i rotori in posizioni separate da un numero di passi indicati dalla concatenazione
- Queste avrebbero dovuto esplorare l'insieme delle possibili chiavi finchè non si fosse accesa una lampadina
- A questo punto rimaneva il problema del pannello e della posizione dei rotori


Pannello
a prese multiple
3 Scambiatori
Riflessore
Assetto a
E
L3
L1
W
Assetto a+1
e
L1
T
L2
Assetto a+3
L3
t
L2
W

Finisce la guerra

- Dopo la guerra tutti i lavori degli uffici di crittanalisi furono secretati e alle persone che vi avevano lavorato fu comandato di non parlarne con nessuno
- Turing morì suicida nel 1954, dopo aver subito una condanna per omosessualità ed essere stato sottoposto a cure ormonali forzate
- Solo molti anni dopo si seppe del suo contributo alla causa alleata