La Bomba di Turing

Indice

Introduzione

Gli inglesi, nella località segreta di **Bletchley Park**, avevano già un modello completamente funzionante della macchina Enigma (fornito dai polacchi), quindi i loro sforzi erano concentrati sul trovare, giornalmente, la corretta configurazione iniziale.
Il tipo di attacco (attacco alla frase probabile) portato alla macchina Enigma da parte di **Dillwyn Knox** e **Alan Turing** è basato sul confronto di un testo in chiaro (**crib**) e il corrispondente testo cifrato, questo confronto avrebbe escluso la maggior parte delle possibili configurazioni della macchina stessa.
Per essere in grado di decriptare un messaggio in tempi ragionevoli, Turing ideò una macchina elettrica chiamata '***bombe***', costruita da **Harold 'Doc' Keen**, che eseguiva una ricerca esaustiva tra tutte le possibili combinazioni dell'Enigma.
Un'espansione della bomba è la **tavola diagonale** inventata da **Gordon Welchman**, aggiungeva alla bomba la funzionalità dello stecker. La bomba con tavola diagonale richiedeva schemi di configurazione (**menu**) meno complessi.

Attacco alla frase probabile

Crib

Questo tipo di attacco era basato sulla conoscenza di un testo in chiaro, detto crib, e di una porzione di testo cifrato contenente il cifrato del crib. Per posizionare correttamente il crib sul suo testo cifrato si sfruttava la proprietà della macchina Enigma di non cifrare mai un carattere con se stesso.

Supponiamo di avere come crib:

```
WETTERVORHERSAGEBISKAYA
```

e la seguente porzione di testo cifrato:

```
QFZWRWIVTYRESXBFOGKUHQBAISEZ
```

iniziamo la ricerca sovrapponendo i due frammenti di testo e controllando tutte le coppie di lettere formate:

```
WETTERVORHERSAGEBISKAYA
QFZWRWIVTYRESXBFOGKUHQBAISEZ
             ^
```

questa configurazione non è corretta poiché la S è cifrata con se stessa, si procede spostando il crib di una posizione:

```
 WETTERVORHERSAGEBISKAYA
QFZWRWIVTYRESXBFOGKUHQBAISEZ
       ^   ^           ^
```

neppure questo accoppiamento è corretto per la V, la E e la A

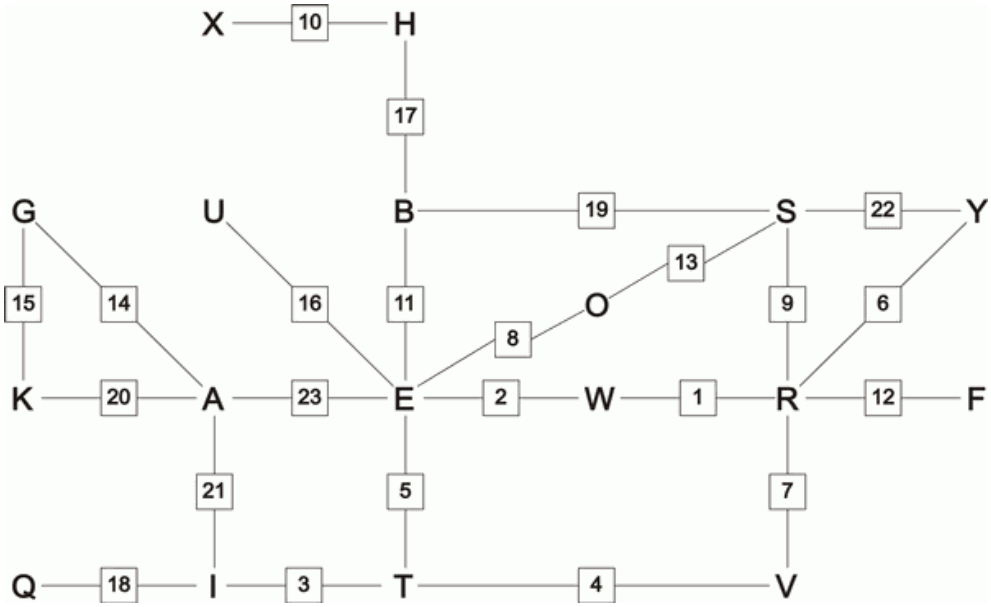
```
  WETTERVORHERSAGEBISKAYA
QFZWRWIVTYRESXBFOGKUHQBAISEZ
          ^
   WETTERVORHERSAGEBISKAYA
QFZWRWIVTYRESXBFOGKUHQBAISEZ
   ^                   ^
    WETTERVORHERSAGEBISKAYA
QFZWRWIVTYRESXBFOGKUHQBAISEZ
```

quest'ultima configurazione sembra accettabile. A questo punto numeriamo le varie coppie formate:

```
      1 2 3 4 5 6 7 8 9...                    ...23
      W E T T E R V O R H E R S A G E B I S K A Y A
      R W I V T Y R E S X B F O G K U H Q B A I S E
```

Menu

Una volta ottenuta una coppia crib-cifrato si può tracciare un grafico che conserva tutte le proprietà del testo, questo grafico è detto menu.



In questo menu è possibile notare che AGK così come AEIT formano un ciclo, questo ciclo è alla base del lavoro degli inglesi.

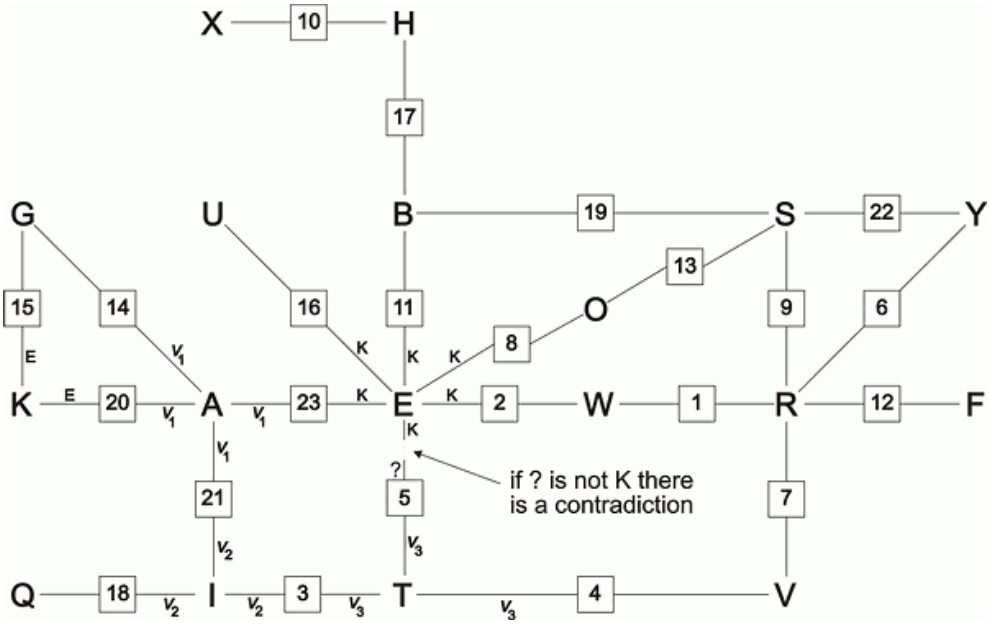
La crittazione dell'Enigma era basata su tre passi fondamentali:

I. scambio dello stecker
II. crittazione dei rotori e del riflettore
III. scambio dello stecker

Prendiamo in esame il loop E-A-I-T:

1. E supponiamo che sia scambiata dallo stecker in K, K verrà cifrata (dai rotori) in v1 e v1 infine scambiata in A
2. A è scambiata dallo stecker in v1 (come da passo 1), v1 cifrata in v2 quindi scambiata in I
3. I scambiata in v2 cifrata in v3 scambiata in T
4. T è scambiata in v3, v3 sarà cifrata in v4 e se v4 non corrisponde a K (che sarebbe scambiata dallo stecker in E) la nostra ipotesi iniziale sarebbe errata e, di conseguenza, la corrente configurazione dei rotori sarebbe da scartare

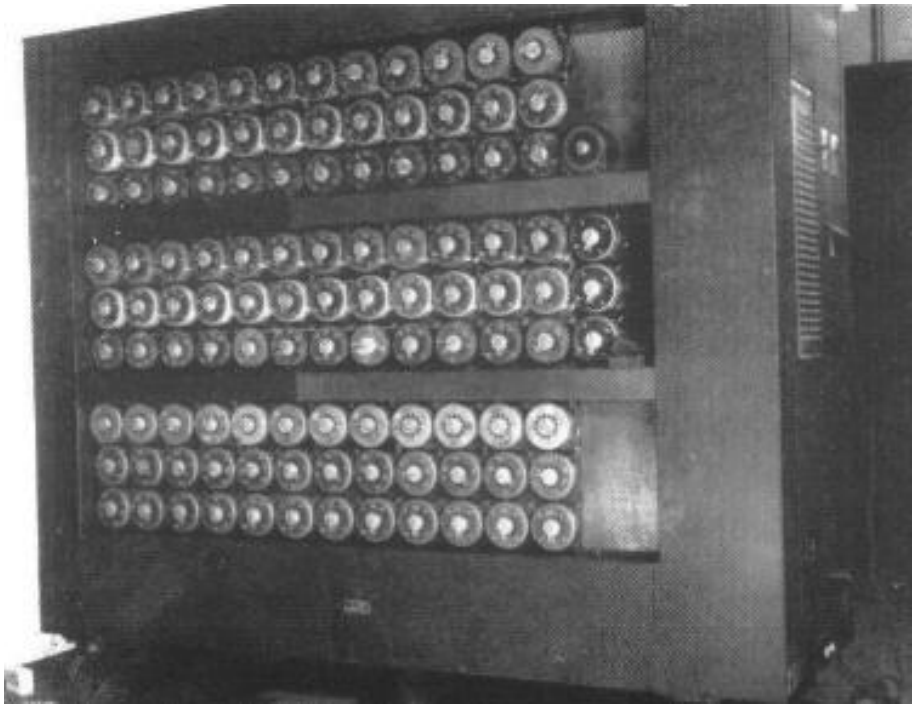
se escludiamo il lavoro dello stecker sappiamo che K è cifrato in v1, v1 cifrato in v2, v2 cifrato in v3 e v3 cifrato in K, sempre che la nostra ipotesi iniziale sia corretta.

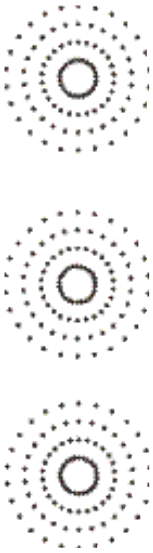


La bomba

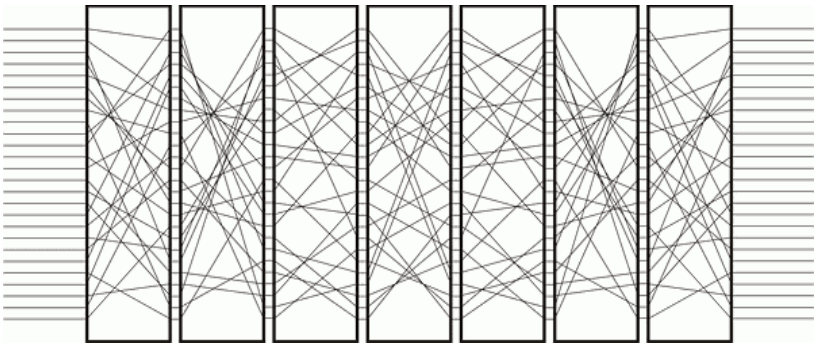
Descrizione della bomba

La bomba era una macchina capace di cercare la combinazione corretta dei rotori tra tutte le combinazioni possibili. Era un armadio di una tonnellata di peso diviso in tre batterie ciascuna contenente dodici colonne di tre tamburi ciascuna. Ogni tamburo rappresentava un rotore, quindi ogni tripletta una intera macchina enigma. La fila superiore di tamburi di ciascuna batteria ruotava ad una velocità di 120 rpm (fila corrispondente ai rotori veloci) , la fila media ruotava ad ogni rivoluzione completa della prima fila e la fila inferiore ad ogni rivoluzione completa della seconda fila.





Nella fila veloce di tamburi entravano 26 fili (ognuno corrispondente ad una lettera dell'alfabeto), ed eseguiva la permutazione del primo rotore. La prima fila era collegata con la seconda che eseguiva la permutazione del secondo rotore, la seconda fila era collegata con la terza che eseguiva la permutazione del terzo rotore quindi lo scambio del riflettore e nuovamente la permutazione del terzo rotore. Dal terzo rotore il segnale elettrico risaliva e subiva nuovamente le permutazioni del secondo e del primo rotore, infine usciva dal primo tamburo. Il tutto è così schematizzabile:

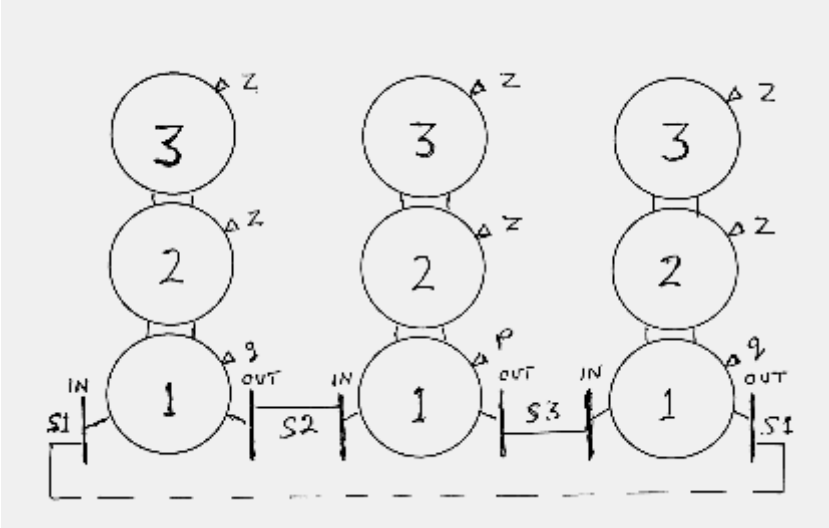


Un esempio

Da una coppia crib-cifrato del tipo:

```
abcdefghijklmnopq
JYCQRPRYDEMCJMRSR
SPRUCHNUMMERXEINS
......|........||
```

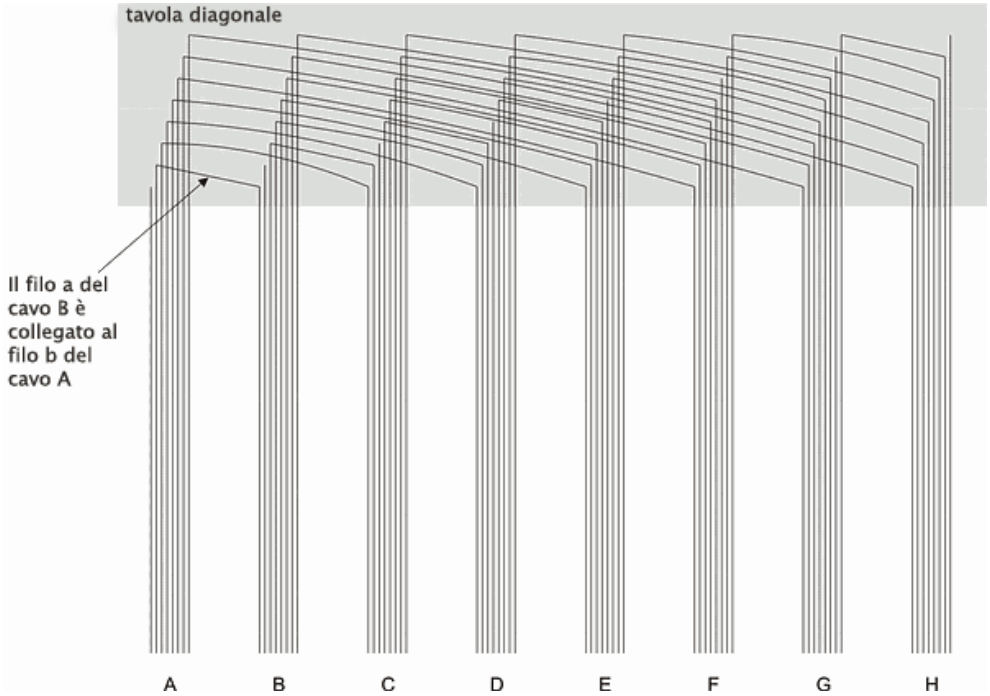
si nota il ciclo RN (posizione g) NS (posizione p) SR (posizione q). Escludendo lo stecker abbiamo R cifrato dalla prima tripletta di tamburi in N, N cifrato dalla seconda tripletta in S, e S cifrato nuovamente in R. Se il ciclo è permanente (l'uscita è connessa all'ingresso) allora la nostra configurazione è corretta.



Da notare nel disegno di Turing è la disposizione dei tamburi la fila superiore (lenta) e l'intermedia sono sempre impostate a Z mentre la prima fila (tamburi veloci) è impostata prima a G poi a P quindi a Q in accordo alla numerazione (stavolta in lettere) assegnata all'accoppiamento crib-cifrato. Le prime due file non cambiano lettera poiché la il secondo rotore girava una volta ogni 26 mentre il terzo rotore una volta ogni 26^2, quindi erano considerati totalmente statici.

La tavola diagonale

Un'importante espansione della bomba è dovuta a Gordon Welchman, l'ideatore della tavola diagonale. La tavola diagonale forniva una schematizzazione dello stecker e si basava sul principio di reciprocità di quest'ultimo, se A è scambiato con B, B verra sempre stato scambiato con A.



La tavola diagonale aveva come ingresso 26 cavi (ognuno per ogni lettera dell'alfabeto), ciascun cavo contenente 26 fili anch'essi corrispondenti ad una lettera dell'alfabeto. Come si vede dalla figura se il filo b del cavo A è collegato con il filo a del cavo B vuol dire che la A è scambiata dallo stecker con B e viceversa. Facendo fluire corrente sul filo b del cavo A questa fluisce anche nel filo a del cavo B.

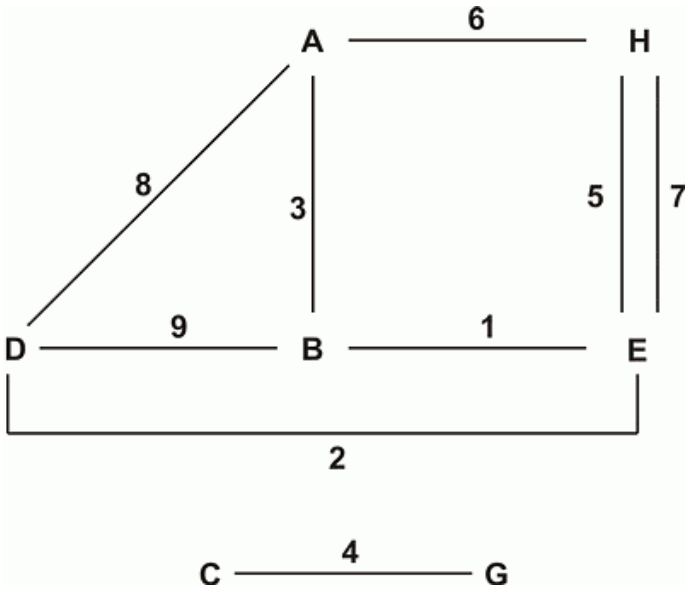
Bomba con Tavola Diagonale

Configurare la bomba

Per impostare la bomba con tavola diagonale abbiamo bisogno semplicemente di una coppia crib-cifrato, come abbiamo visto prima. Per rendere leggibili gli schemi utilizziamo un alfabeto di 8 lettere (A..H), e le coppie:

```
1 2 3 4 5 6 7 8 9
B E A C H H E A D
E D B G E A H D B
```

il menu corrispondente è:



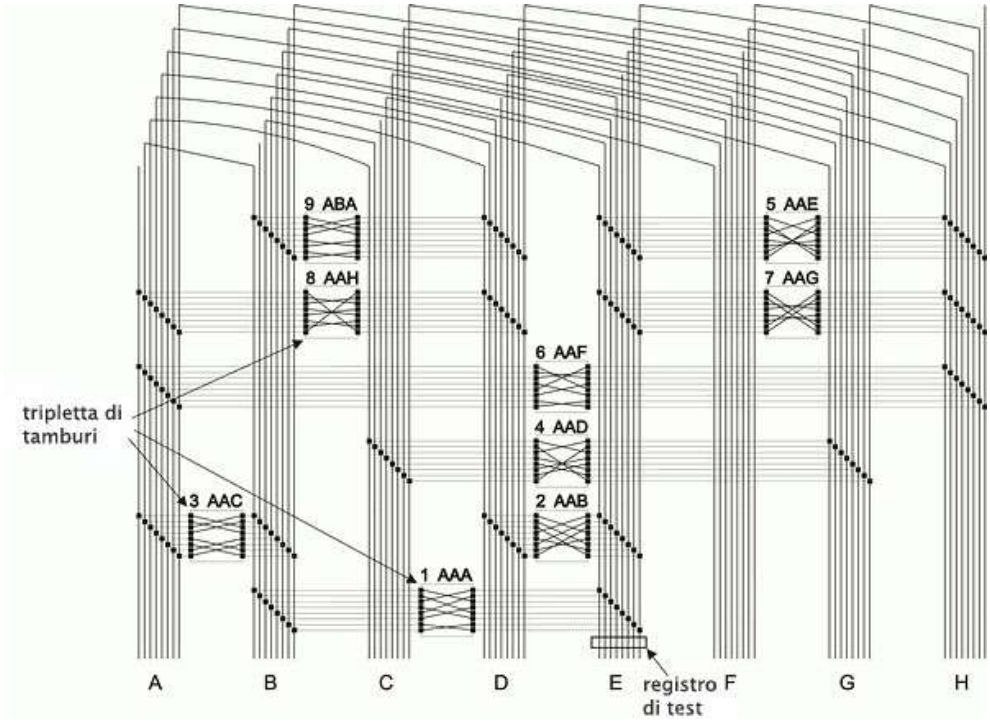
ora calcoliamo la lettera iniziale di ciascun tamburo.

TAMBURO	CAVI CONNESSI DAI TAMBURI	POSIZIONE DELLA COPPIA	LETTERA INIZIALE DEL TAMBURO
veloce	B – E	1	A
veloce	E – D	2	B
veloce	A – B	3	C
veloce	C – G	4	D
veloce	H – E	5	E
veloce	H – A	6	F
veloce	E – H	7	G
veloce	A – D	8	H
veloce	D – B	9	A
medio	D – B	9	B

Ogni riga si riferisce ad una tripletta di tamburi diversa, esclusa le ultime due che si riferiscono alla stessa tripletta (infatti hanno la stessa posizione della coppia). La prima

colonna (TAMBURO) indica il tamburo che deve essere posizionato come indicato dalla quarta colonna (LETTERA INIZIALE). La seconda (CAVI CONNESSI) indica quali cavi della tavola diagonale la tripletta deve collegare, i due cavi collegati sono indicati dalla coppia corrispondente all'indice indicato dalla terza colonna (POSIZIONE) nel crib-cifrato.

Ora abbiamo tutte le informazioni per configurare la bomba:



Sul cavo corrispondente alla lettera più frequente era posto un registro di test, in grado di contare il numero di fili in cui c'era corrente (fili vivi).

Come funzionava la bomba

Una volta configurata, la bomba era messa in funzione quindi si faceva fluire corrente su ciascun filo, se il registro di test contava più fili vivi allora la configurazione era da scartare. La disposizione dei rotori non andava bene perché se fluisce corrente nel filo b del cavo A (ovvero nel filo a del cavo B), vuol dire che A e B sono scambiate dallo stecker, e una lettera può essere scambiata solo ed esclusivamente con solamente un'altra, perciò se il registro contava più fili vivi, voleva dire che non si aveva uno scambio univoco, quindi una disposizione dei rotori non valida.

Gli Stop

Una configurazione era corretta se:

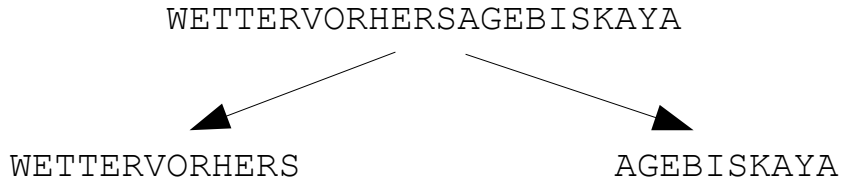
- il registro di test contava un solo filo vivo, configurazione corretta e ipotesi iniziale corretta
- il registro di test contava un solo filo morto, configurazione corretta e ipotesi iniziale errata

Il problema del secondo rotore

Alla base della bomba c'è la supposizione che il secondo e il terzo rotore siano statici ma questo effettivamente non è vero. Con un crib di 23 lettere come:

WETTERVORHERSAGEBISKAYA

abbiamo una probabilità di 23 / 26 che il secondo rotore, durante la digitazione del messaggio, giri. Se il secondo rotore cambia posizione tutte le ipotesi cadono e gli attacchi sono del tutto vani.
Per sopperire a questo inconveniente, si divide il crib in due, ad esempio:



così il crib è diviso in due testi da 13 e 10 lettere, riducendo il problema del secondo rotore ad uno solo dei due crib (anche se rimane con una probabilità di 23 / 26). Così si risolve questo inconveniente però si riduce, dividendo il crib, la complessità del menu rendendo meno efficiente la bomba stessa.