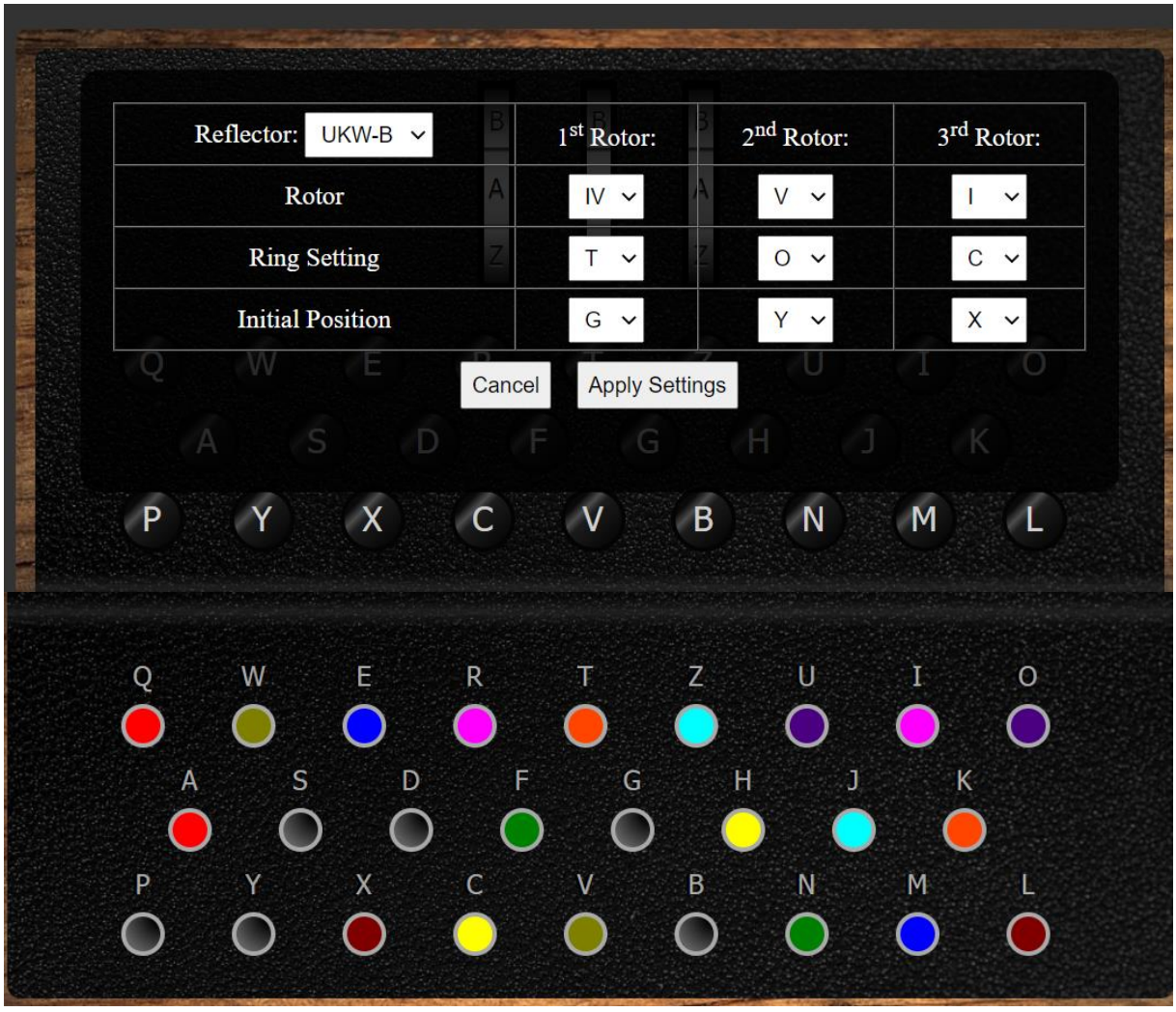
# Laborator 2 – Rezolvare

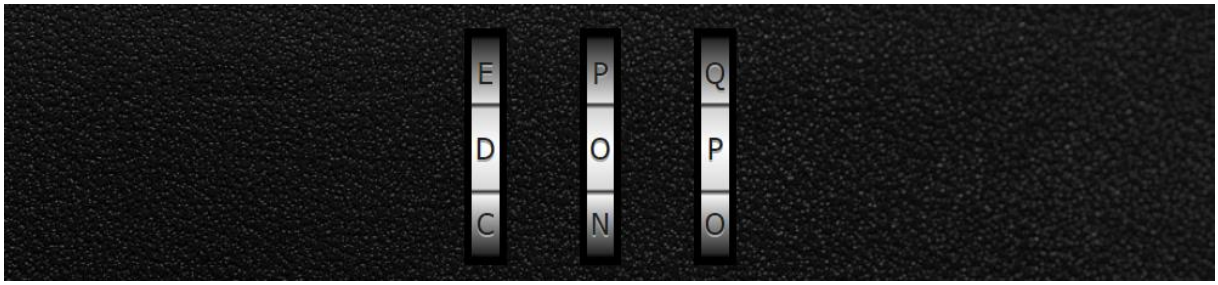
## II) Criptare

1. C = MECHANISATION OF SECRECY
    a. MECHANISATIONXOFXSECRECY (X pentru spațiile libere)
    b. Link Mașină Enigma Virtuală sau Aici

```
| 04 | B | IV  V  I  | 20 15 03 | G Y X | AQ CH EM FN IR JZ KT LX OU VW
```



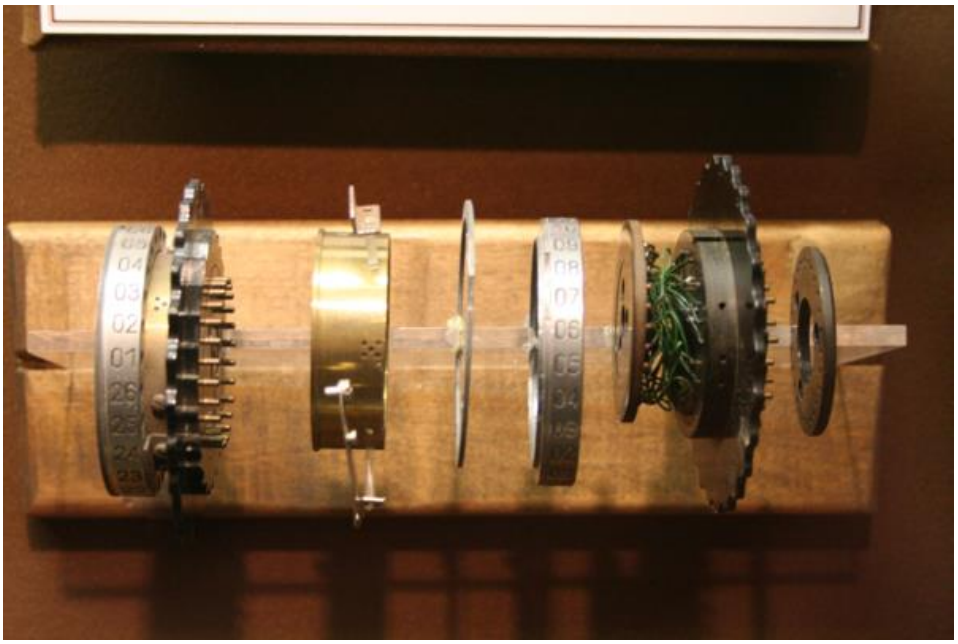

    c. DOPDOP → CYNLS W

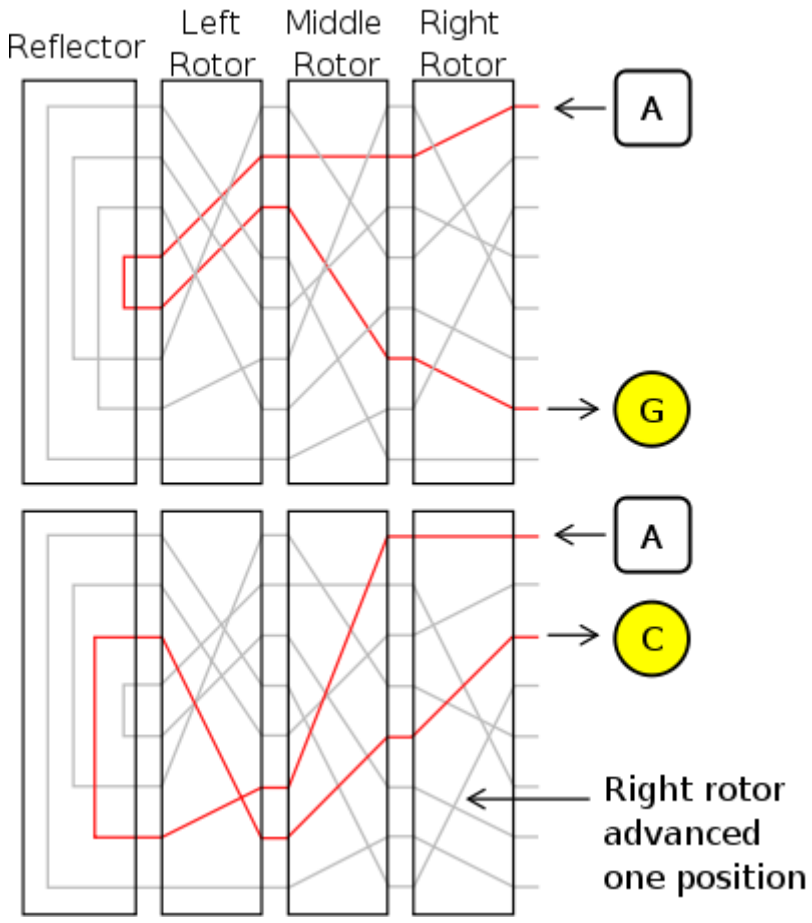


MECHANISATIONXOFXSECRECY → USUIE GZEVL UVDFR QEUBB XRDF

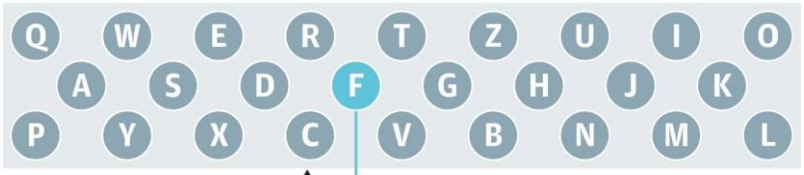
Mesaj Final: CYNLS WUSUI EGZEV LUVDF RQEUB BXRDF

2. Mod Funcționare Enigma:





## **Enigma** How the machine worked




**1** | Sender types each letter of the message into a **standard keyboard**

**2** | Signal passes through **plugboard** which switches letters around


**3** | Three physical **rotors**, internally wired like spaghetti, each change the output letter before a **reflector** sends the signal back through the whole system

**4** | To add to the code's complexity, the first rotor rotates one step **after each key press** (after 26 the second starts to move) so 'FF' might produce 'AQ'


**5** | The reflected signal makes a second pass through the **plugboard**

**6** | Finally, the signal **lights up a letter** on a light board


**7** | Sender copies the lit letters and sends encryption using morse code. The system relies on sender and receiver **setting up** in the same pattern

**8** | The receiver writes down apparent gibberish but, on keying in 'A', finds a letter F lights up and soon the encrypted message becomes clear

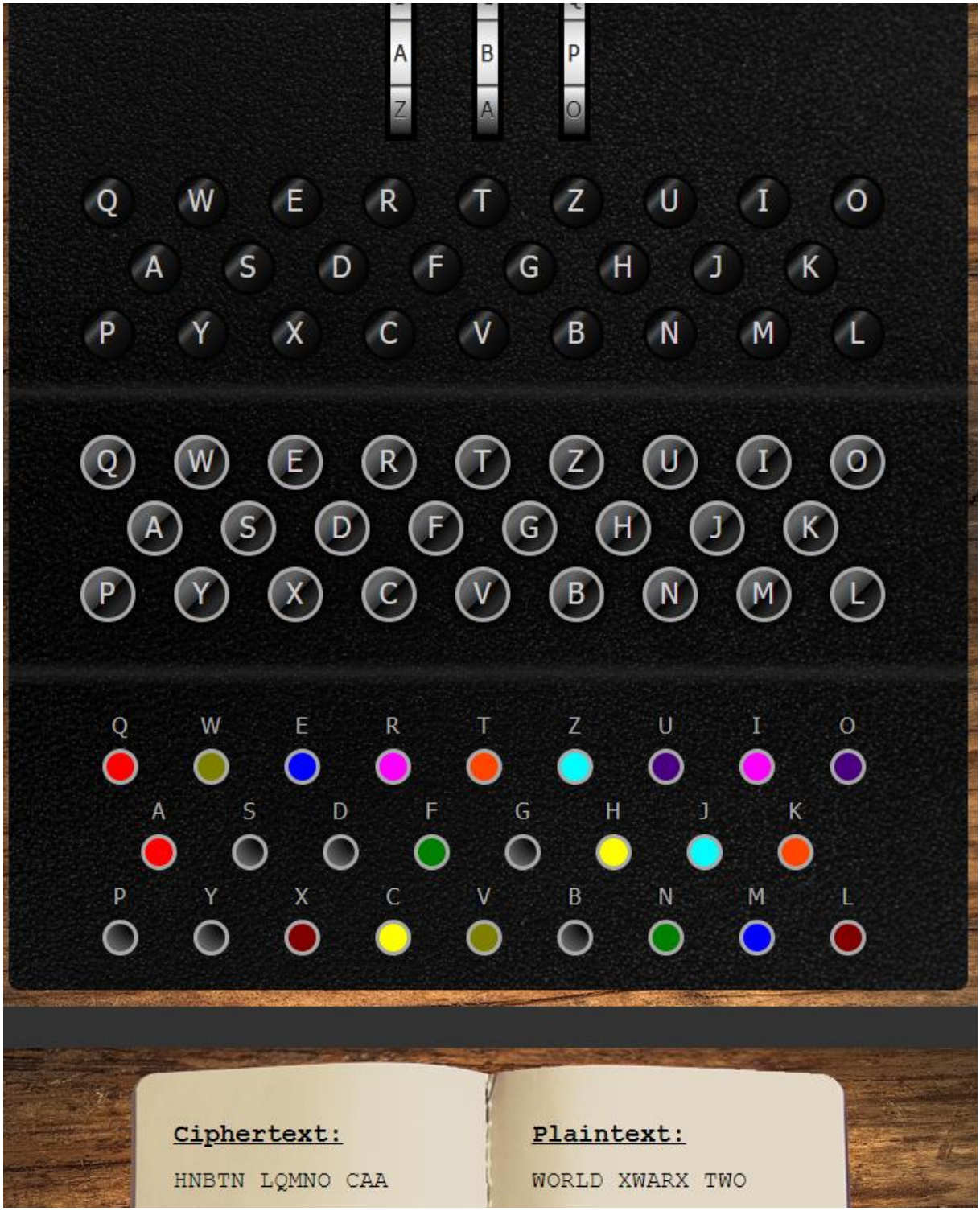
PAUL SCRUTON, GUARDIAN GRAPHIC

SOURCE: SIMON SINGH, LOUISE DADE

## III) Decriptare

M = RPVLU JHNBT NLQMN OCAA → WORLD XWARX TWO

K = RPVLU J → ABCAB C (Setăm ABC drept cheie de criptare și acum descifrăm mesajul)



# IV) Criptanaliza Poloneză (Marian Rejewski)

1. Slăbiciunea pe care a exploatat-o Rejewski face referire la faptul că germanii trimiteau codul de criptare împreună cu mesajul propriu-zis. De asemenea, alegeau un grup de 3 litere, pe care le încriptau de două ori, deci acest lucru ne poate oferi un indiciu asupra identității literelor criptate inițial (primele 6 litere din mesaj erau cifrul).

Pentru *Litera 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 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| V | * | M | N | T | G | P | I | Y | * | Z | A | S | Q | J | * | X | * | O | F | R | C | U | B | E | L |

Cicluri: (AVCMSOJ) → 7; (DNQXB) → 5; (ETFGP) → 5; (HIYETFGP) → 8; (KZLAVCMSOJ) → 10; (UR) → 2; (WUR) →3; (YETFGP) → 6.

Iau: (KZLAVCMSOJ) → 10; (HIYETFGP) → 8; (WUR) →3; (DNQXB) → 5.

Grupez și obțin caracteristica zilei (trebuie să am cicluri de lungime egală): (KZLAVCMSOJ WUR) → 13; (HIYETFGP DNQXB) → 13.

Pentru *Litera II*:

| 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 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| O | E | Z | B | R | * | C | P | * | Y | L | X | J | * | F | I | * | * | D | A | K | G | U | V | M | W |

Cicluri: (CZWUKLXVG) → 9; (HPI) → 3; (JYM) → 3; (N) → 1; (Q) → 1; (SDBER) → 5; (TAOF) → 4.

Grupez și obțin: (N) → 1; (Q) → 1; || (HPI) → 3; (JYM) → 3; || (CZWUKLXVG) → 9; (SDBER TAOF) → 9.

Pentru *Litera III*:

| 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 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| J | * | V | E | O | Y | N | * | D | M | W | U | * | S | H | L | * | * | A | F | Q | C | Z | K | X | * |

Cicluri: (B) → 1; (CV) → 2; (GNSAJM) → 6; (IDEOH) → 5; (PLUQ) → 4; (R) → 1; (TFYXKWZ) → 7.

Grupez și obțin: (BR) → 2; (CV) → 2; || (TFYXKWZ PLUQ) → 11; (GNSAJM IDEOH) → 11.

2. LOC → AFV (ne-am uitat în tabel) → LOCAFV (cheia de criptare)

3. Pt *Litera III*, caracteristica este 11, 11, 2, 2 și în tabel avem o singură linie care satisface aceaste valori și anume **BIX**. Dacă presupunerea noastră este corectă, știm că primul rotor se învârte pentru fiecare literă apăsată, deci, pentru a doua literă, ar trebui să obținem **BIW** și pentru prima literă **BIV**. Să verificăm; pentru *litera II* caracteristica este 9, 9, 3, 3, 1, 1 și în tabel avem o singură valoare care satisface condiția → **BIW**; iar pentru *litera I* caracteristica este 13, 13, dar am 4 poziții cu această caracteristică, deci numai **BIV** este corectă. Concluzionăm că poziția inițială a rotorilor este **BIV**.

4. Pentru a descoperi prizele, comparăm permutările din tabel, cu ce am obținut noi:

Noi: KZLAVCMSOJWUR HIYETFGPDNQXB

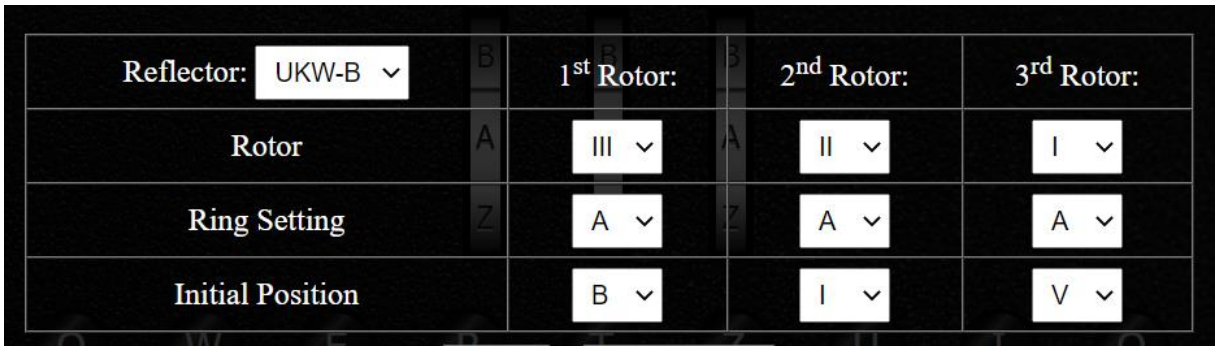
Tabelă: AVRMSTJWUCKZL BHIPEOFGYDNQX

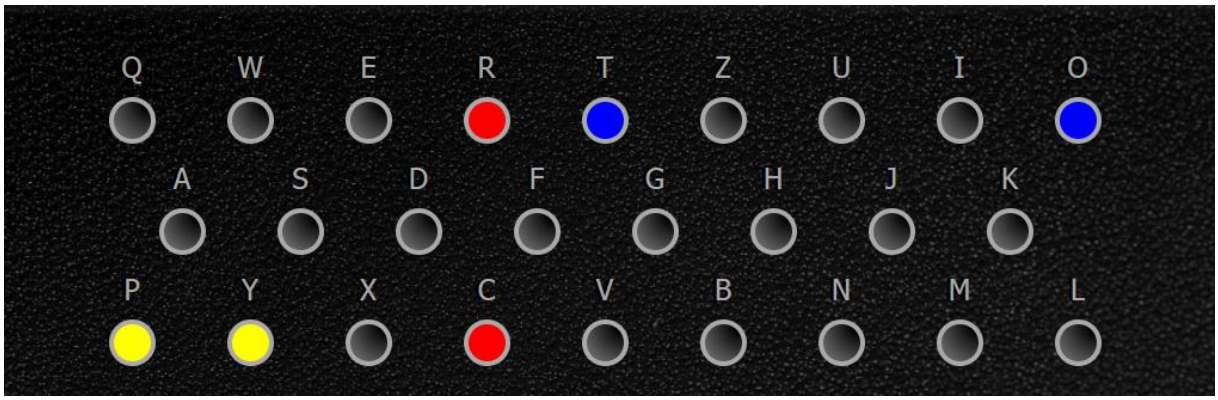
| A | V | C | M | S | O | J | W | U | R | K | Z | L | * | B | H | I | Y | E | T | F | G | P | D | N | Q | X |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| A | V | R | M | S | T | J | W | U | C | K | Z | L | * | B | H | I | P | E | O |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

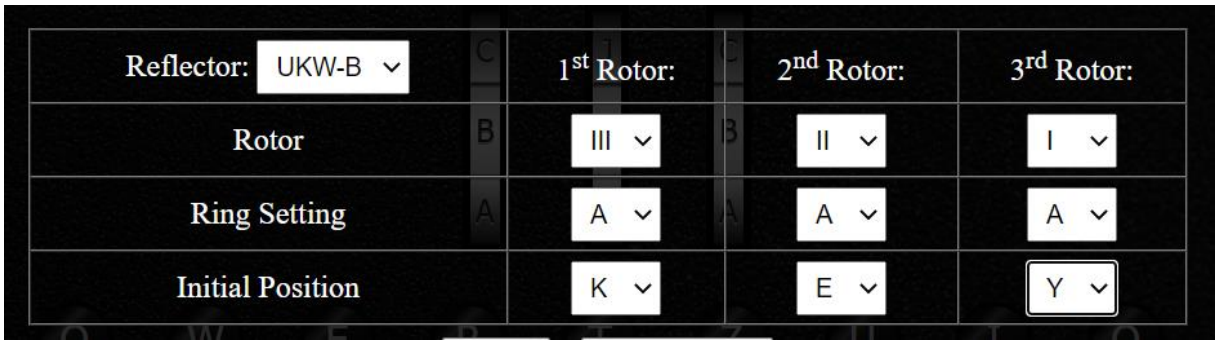
Prizele sunt simetrice. Deci, avem: **C – R; O – T; Y – P**.

5. Mesaj Criptat: BLGH XNST PVBX WMUZ P.

BLGHXN → KEYKEY





ST PVBX WMUZ P → NEXTX ATTAC K

Mesajul decriptat este: ***Next attack***.

# V) Criptanaliza Britanică (Alan Turing)

Alan Turing a remarcat o slăbiciune importantă a mașinii Enigma, iar acest lucru a ajutat la spargerea ei: să presupunem că vrem să criptăm litera *A*. Enigma nu va cripta niciodată litera *A* în ea însăși. (Mașina Type X, descendentul Enigmei, folosită de britanici, nu mai prezenta această slăbiciune, printre alte îmbunătățiri.)

Astfel, Alan Turing, împreună cu Gordon Welchman, au construit Bombe, mașina de spart cifruri Enigma, care reușea să spargă codurile în mai puțin de 20 de minute, folosind, la bază procesul de eliminare.

M = CETINFWUTYPED...

Avem următoarele cribs: WEATHERXREPORT, BATTLEXREPORT, ATTACKXREPORT

Deci, obținem următoarele comparații:

| | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Cipher text: | C | E | T | I | N | F | W | U | T | Y | P | E | D | Invalid Crib |
| Plain crib: | W | E | A | T | H | E | R | X | R | E | P | O | R | |

| | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Cipher text: | C | E | T | I | N | F | W | U | T | Y | P | E | D | Invalid Crib |
| Plain crib: | E | A | T | H | E | R | X | R | E | P | O | R | T | |

| | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Cipher text: | C | E | T | I | N | F | W | U | T | Y | P | E | D | Invalid Crib |
| Plain crib: | B | A | T | T | L | E | X | R | E | P | O | R | T | |

| | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Cipher text: | C | E | T | I | N | F | W | U | T | Y | P | E | D | Invalid Crib |
| Plain crib: | A | T | T | A | C | K | X | R | E | P | O | R | T | |

Concluzie: Folosindu-ne doar de aceste informații, nu putem determina o criptare corectă.

Suplimentar: Cu toate acestea, putem avea o criptare în acest fel:

| | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Cipher text: | C | E | T | I | N | F | W | U | T | Y | P | E | D | Valid Crib |
| Plain crib: | A | T | H | E | R | X | R | E | P | O | R | T | | |

Și am putea folosi un simulator Bombe pentru a găsi o posibilă spargere.