Mașina Enigma

Am ales acest subiect deoarece m-au fascinat întotdeauna mașinăriile legate de criptare și decriptare. Un alt motiv este importanța pe care a avut-o armatelor în timpul celui de-al Doilea Război Mondial.

Mașina Enigma[4]

Istoric

De-a lungul anilor au existat numeroase modele și variante ale mașinii Enigma, dar primele au fost cele comerciale ca după să fie folosite și de diferite ramuri ale armatei germane.

În anul 1918, inginerul Arthur Scherbius creează mașinăria Enigma și abordează marina germană și ministerul de externe. Ajunge să fie refuzat de ambele așa că decide să îl comercializeze. Începe producția mașinăriei în anul 1923 și de-a lungul timpului lansează patru modele (A,B,C,D), fiecare având un aspect inovativ, dar afacerea este neprofitabilă până în anul 1924 [3].

Marina germană începe să își caute un nou sistem de criptare întrucât au descoperit "că britanicii au citit mesajele codificate ale marinei germane pentru o mare parte din Primul Război Mondial" [1:38]. La final au decis ca mașinăria lui Scherbius să fie folosită și au început producția versiunii pentru forțele navale a mașinăriei Enigma.

Abia în anul 1932 spargerea a fost posibilă datorită criptografilor polonezi și, în anul 1939, Polonia a prezentat reconstrucția și descifrarea mașinăriei, astfel ajutând Aliații, inamicul Germaniei în Al Doilea Război Mondial [3].

În prezent, multe exemplare ale mașinii Enigma sunt expuse în muzee din jurul lumii și au fost creat diferite derivate, cum sunt Typex, M-325, GREEN (o clonă japoneză după Typex) etc.

Componenetele unei mașini Enigma

Componentele principale ale unei mașini Enigma sunt tastatura, tabla cu lămpi (*lampboard*), rotoarele(*rotors*) și reflectorul [2]. Pentru versiunea armatei germane și a marinei s-a mai adăugat și tabloul de prize (*plugboard*) pentru că oferă o dificultate extrem de mare în a decripta mesajul rezultat de către mașinărie.

- Tastatura și tabla cu lămpi – sunt calea de intrare și de ieșire. Tastatura este una standard a unei mașinării de scris și tabla cu lămpi este un set cu 26 de lumini amplasate deasupra tastaturii. Un exemplu de funcționalitate este introducem o literă de la tastatură (calea de intrare), se codifică și litera rezultată se va aprinde pe tabla (calea de ieșire).
- Rotoarele – sunt cele mai importante componente ale mașinăriei. Erau așezate una lângă cealaltă în mașină și ordinea și poziția lor inițială era schimbă periodic, astfel

făcând Enigma mai greu de rezolvat. Un rotor este un disc mic care înăuntru are 26 de conectoare, astfel pe o parte conectoare care sunt conectate aleatori cu alte conectoare din cealaltă parte așa că curentul trecea dintr-o parte și ieșea în cealaltă. Mecanismul de funcționare este așa: de fiecare dată când primul rotor ajunge la o anumită literă/poziție rezultă al doilea se rotește o poziție, de fiecare dată când al doilea rotor ajunge la o anumită literă/ poziție rezultă al treilea se rotește o poziție și așa mai departe până la ultimul rotor. Fiecare rotor are o poziție de *turnover* care este determinată de inelul său (adică banda din jurul circumferinței sale unde este imprimat alfabetul) care poate fi rotit și apoi blocat pe loc. Datorită acestui lucru în criptare putea varia poziția de *turnover*.

- Reflectorul – este un tambur staționar care are 26 de conectoare pe o parte, dar în loc să se trimită curentul pe cealaltă parte, acesta este scos înapoi prin aceeași parte datorită cablării conectoarelor cu celelalte prin aceeași parte. Atsfel, curentul urmează o cale înapoi prin mașină până la tabloul cu lămpi.
- Tabloul de prize – este o placă cu 26 de prize, fiecare reprezentând o literă, care erau conectate între ele prin cabluri scurte cu mufe. Era conectată la tastură și la tabla cu lămpi, astfel încât curentul (adică codul) traversa tabloul la începutul și sfârșitul criptării, așa permițând prin aceeași metodă și decriptarea.


Tablou de prize[4]


Tastatura și tabloul cu lămpi[4]


Reflector și rotoare[5]

Mecanismul de funcționare

Mașina Enigma a fost folosită pentru criptarea și decriptarea mesajului datorită modalității sale de funcționare întruncât le putea face pe ambele. Mecanismul de funcționare se bazează pe un circuit electric și pe anumite părți componente al mașinii care sunt rotoarele, tabloul de prize și mecanismul tastaturii.

Pentru început vom discuta funcționalitatea rotoarelor și legatură lor cu reflectorul. Așa cum am mai spus mai sus, un rotor are 26 de conectoare, astfel încât curentul intră pe o parte și iește pe altă parte, acest lucru realizându-se datorită cablurilor din interiorul rotorului care fac legătura dintre conectoarele de pe ambele părți. Curentul trece prin toate rotoarele și ajunge la reflector, unde cum am precizat mai sus, acesta are la fel ca și un rotor 26 de conectoare, dar în cazul acestuia, curentul iește pe partea unde a intrat datorită cablurilor. Așa că curentul trece din nou prin toate rotoare până când ajunge la tabloul de prize. Pe tot parcusul acestei părți, litera inițială se tot schimbă la trecerea printr-un conector, astfel având o nouă valoare de fiecare dată.

Tabloul de prize este componenta care a făcut mașina Enigma și mai dificilă de spart. Avem două cazuri pentru curentul care ajunge ajunge la tabloul de prize. Primul caz este când literă ajunge la tablou și nu este legată de nicio altă literă printr-un cablu cu mufe, așadar se va

returna aceeași literă. Al doilea caz este când litera este legată de altă literă, rezultând după acest proces o noua literă, adică cea cu care era legată litera inițială.

Mecanismul tastaturii este important deoarece chiar dacă pare o tastatură obișnuită din aceea vreme, de fapt, pe înăuntru era foarte complex. Tastatura are 26 de butoane și fiecare dintre acestea este alcătuită din 3 file de cupru care la un căpăt au câte un fir și la celălalt capăt este controlat cum merge curentul. Filul de curu din mijloc se mișcă în funcție de poziția butonului și acesta duce curentul la tabloul de prize. Când butonul nu este apăsat, filul de mijloc este împreună cu cel de sus, care acesta face legătura cu tabloul de lămpi. Când butonul este apăsat, filul de mijloc este legat cu cel de jos, care face legătura cu bateria.

Circuitul mașinăriei Enigma începe de la baterie, care transmite curentul la filul de cupru de jos al fiecărui buton de la tastatură. Când un buton este apăsat, filul din mijloc se leagă de cel de jos, astfel, curentul își continuă mișcarea pe ruta acelei litere. Curentul de la tastură ajunge la tabloul de prize, unde se verifică cele două cazuri menționate mai sus. După ce trece de tabloul de prize, curentul se duce mai departe în rotoare și reflector și se face mecanismul explicat mai sus. Pe urmă, revine la tabloul de prize și se verifică cele două cazuri, dar de această dată curentul se duce la tastatură la litera finală obținută, care este diferită de cea inițială. La această literă nouă, fileul mijloc este conectat cu cel de sus așa că curentul se duce la tabloul cu lămpi unde se va afișa litera rezultată. La final, curentul se duce de la tabloul cu lămpi la baterie, astfel, terminându-se tot circuitul mașinăriei.

Setările mașinei Enigma

Înainte să utilizăm mașina Enigma trebuie să îi punem setările bune, adică pentru criptare folosim niște anumite setările pe care trebuie să le folosim pe aceleași când decriptăm același mesaj. Setările constă în ordinea rotoarelor, setarea inelului de pe rotor (adică așezarea poziției unde se va face rotirea următoarei rotoare) , poziția de start al rotoarelor și legăturile din tabloul de prize.

Referințe

[1] Kahn, D. (2001). *Seizing the enigma: the race to break the German U-boat codes, 1939-1943*. Barnes & Noble Publishing.

[2] Faint, S. (2016). *The Enigma History and Mathematics* (Master's thesis, University of Waterloo).

[3] Wikipedia (5.02.2023). Mașina Enigma. Disponibil la URL-ul: https://ro.wikipedia.org/wiki/ (accesat la data 20.02.2023)

[4] Artmark (25.03.2021). 38. Celebra mașină de criptat Enigma, folosită de armata germană în timpul celui de-al Doilea Război Mondial, model M 2-3, 1938-1940, piesă de muzeu, extrem de rară. Disponibil la URL-ul: https://www.artmark.ro/ro (accesat la data 5.03.2023)

[5] Cipher machines and cryptology (24.08.2022). Technical Details of the Enigma Machine. Disponibil la URL-ul: https://www.ciphermachinesandcryptology.com (acces la data 5.03.2023)