**MINISTERUL EDUCAȚIEI ȘI TINERETULUI AL REPUBLICII MOLDOVA**

**UNIVERSITATEA DE STAT ,,ALECU RUSSO’’ DIN BĂLȚI**

**FACULTATEA ,,ȘTIINȚE REALE ECONOMICE ȘI ALE MEDIULUI’’**

**CATEDRA ,,INFORMATICĂ ȘI MATEMATICĂ’’**

REFERAT

La disciplina universitara ,,Criptografie’’

Tema : Maşina Enigma

.

Autor : studentul gr IS31FR Scripnic Andrei

## Enigma a fost cea mai complexa masina de criptat mesaje construita de germani în cel de-al doilea razboi mondial. Aceste mesaje erau trimise prin radio si destinate în general submarinelor „U-Boat” din Atlantic. Enigma a fost considerata sigura de catre germani deoarece chiar daca una dintre aceste masini ar fi cazut în mâinile aliatilor, cheia algoritmului de criptare era schimbată în fiecare zi dupa o regula stabilita în prealabil.

## Maşina Enigma a fost un produs patentat iar autorii au încercat ani la rând sa-l vânda marilor corporatii pentru o comunicare sigura cu partenerii lor externi.

## Ideea unor masini de criptat ce folosesc rotoare a aparut si a fost patentata în mai multe locuri în lume într-un interval de timp foarte scurt. Primii au fost doi ofiteri navali olandezi Theo van Hangel si R.P.C. Spengler în 1915. În statele unite, Edward Hugh Hebern a construit astfel de masini începând cu anul 1917 si în loc sa ajunga celebru a ajuns falit dupa ce a vândut doar câteva exemplare marinei SUA. Alte variante ale algoritmilor ce folosesc rotoare au fost patentati în Suedia si Regatul Unit.

## În perioada celui de-al doilea razboi mondial militarii germani au început sa foloseasca comunicatiile prin radio (folosind codul MORSE) pentru a putea comunica cu submarinele U-Boat si cu trupele aflate din ce în ce mai departe de cartierul general din Berlin. Stiind ca mesajele lor radio sunt interceptate si de aliati, au cautat un mod cât mai simplu si cât mai sigur de criptare a datelor trimise trupelor. Masinile de tip Enigma ce ofereau mai mult de 712 milioane de combinatii posibile au fost în cele din urma alese pentru criptarea si decriptarea datelor. Chiffriermaschinen Aktiengesellschaft, compania germana producatoare a masinii de criptat militare, a oferit si guvernului britanic aceasta masina în iunie 1924, la pretul de 190$ bucata. Britanicii nu au acceptat oferta pâna ce compania germana nu a patentat produsul la „British Patent Office”, oferind astfel si algoritmii de criptare/decriptare. ☺Cu toate acestea, criptanalistii britanici nu au reusit sa decripteze cu succes primele mesaje decât la începutul anilor 1940, dupa ce au primit informatii importante de la oamenii de stiinta polonezi. În forma modernă, cunoscută şi în zilele noastre,maşina Enigma a fost construită pentru întîia oară în 1918 de Arthur Scherbius în Berlin. Ideea lui a fost criptarea unui mesaj prin executarea unei substituţii după alta folosind conexiuni electrice.Britanicii nu au acceptat oferta pâna ce compania germana nu a patentat produsul la „British Patent Office”, oferind astfel si algoritmii de criptare/decriptare. Cu toate acestea, criptanalistii britanici nu au reusit sa decripteze cu succes primele mesaje decât la începutul anilor 1940, dupa ce au primit informatii importante de la oamenii de stiinta polonezi. O modalitate simplă de a implementa această idee, este aceea de a folosi o baterie ce va fi legată în paralel la toate cele 26 de taste ale maşinii de scris. Pentru a exemplifica, în figura de mai jos, la apăsarea tastei Q, se va aprinde un bec, corespunzător literei R din ultima linie:

## wiring2

## În realitate, pentru a simplifica din punct de vedere constructiv problema s-au folosit rotoare,asttfel încât să se simplifice problema multiplelor cablări necesare. Următorul pas a fost folosirea unui al treilea rotor ceea ce va duce la 26x26=676 alfabete de substutuţie.

## Un prim effect al acestei idei a fost creşterea numărului de alfabete de substituţie la 26 x 26 x 26 = 17576.

## Efectul cel mai important al acestei invenţii a fost însă faptul că maşina Enigma a devenit „reciprocă” în sensul că dacă vom cripta Q şi vom obţine A, la criptarea lui A în aceleaşi condiţii iniţiale vom obţine Q.

## Un al treilea efect foarte important al acestui reflector a fost că nici o literă nu se va cripta la ea înseşi niciodată.

## Din punct de vedere operaţional, algoritmul Enigma a fost un mare pas înainte al criptografiei deoarece nu trebuia să folosească două maşini diferite: una pentru criptare şi una pentru decriptare, ci doar una care trebuia să folosească aceleaşi condiţii iniţiale (setarea iniţială a rotoarelor dată de cheia de criptare). În cele din urmă acest avantaj economic şi operaţional avea să coste siguranţa mesajelor trimise de armata germană.

## Un alt impediment iniţial pentru analiştii britanici (pănă la capturarea primei maşini Enigma) a fost aşezarea neuzuală a literelor pe tastatura maşinii enigma:

## 

## Pentru a creşte numărul de substituţii folosite, maşina Enigma folosea un număr de 10 rotoare diferite în ordinea R1,R2,..R8, Rotor Alfa şi Rotor Beta din care vom prezenta doar primele 3:

## 

## De asemeni au fost folosite 4 tipuri de reflectoare diferite (din care prezentam doar primele două):

## 

## În ceea ce priveşte rotaţia în plan orizontal (în figură), cele trei rotoare prezentate îşi schimbau configuraţia la fiecare 26 de caractere criptate după regulile din tabelul următor (Obs: literele nu vor mai fi codificate la fel):

## 

## Pentru a cripta litera G, vom urma algoritmul

## 

## Dacă vom incerca paşii inverşi:

## 

Pentru a putea cripta eficient masina Enigma, armata germană a folosit următorul mod de a stabili cheia de criptare / decriptare:

Se va seta maşina Enigma (rotoare şi reflectoare folosite), funcţie de data calendaristică.

Se vaseta configuraţia îniţială a poziţiei acestora rotoarelor, funcţie de tabelul dată-poziţii

Se va da operatorului radio mesajul cifrat precum şi header-ul format din cheile criptate funcţie de data calendaristică

Pentru decriptare se vor urma aceeaşi paşi, fiind cunoscută cheia folosită (header-ul din mesajul primit prin radio) iar setările se vor face în aceeaşi ordine.

## Perechile de litere de la rotoare sunt fixe. Nu au fost aproape niciodată schimbate cu excepţia câtorva ocazii speciale. În timp ce numărul stărilor oferit de posibilităţile matematice era astronomic, doar o mică parte a acestora au fost utilizate din motive de cost şi logistică.

## Deşi existau 10 rotoare în setul standard, doar 3 (sau 4) au fost utilizate simultan.

## Rotoarele se roateau doar cu o poziţie odată. Al doilea se roatea doar după 26 de rotaţii ale primului, al doilea după 26 de rotaţii al celui de al doilea, etc. Drept rezultat, doar primul rotor se rotea frecvent, cel de-al doilea odată pe frază(propoziţie) iar cel de-al treilea aproape niciodată.

## Reflectorul nu se rotea niciodată (cu excepţia modelelor timpurii).

## O slăbiciune subtilă observată anterior este că o literă nu se cripta niciodată la ea însăşi.

## A fost o maşină scumpă atât din vedere constructiv cât şi în operare. Odată ce a fost de terminate modul de simulare pentru rotoare precum şi a trecerii curentului, problema cea mai importantă din punctul de vedere al criptanalistului a fost rezolvată.

## Exploring the Enigma by Claire Ellis

## “Messages often began with the same opening text - many began with the word *Spruchnummer* (Message Number), and many Air Force messages began with the phrase *An die Gruppe* (To the Group).

## Messages often enciphered routine information such as weather reports and phrases such as *Keinebesondere Ereignisse* (Nothing to report).

## Messages often ended with *Heil Hitler*!

## The Germans often transmitted the same message more than once, with each version enciphered differently. ”