UNIVERSITETI I PRISHTINËS “HASAN PRISHTINA”FAKULTETI I SHKENCAVE MATEMATIKO-NATYROREDEPARTAMENTI I MATEMATIKËSPROGRAMI: SHKENCA KOMPJUTERIKE

Lënda: Siguria e të dhënave

TEMA: Makina Enigma

**Punuar nga: Albina Grajqevci, Diellza Bajraktari, Dalina Elshani**

**Mars 2023**

Përmbajtja

[**1.** **Hyrje** 2](#_Toc130166847)

[**2.** **Konteksti historik** 2](#_Toc130166848)

[**3.** **Detajet teknike te makinës** 3](#_Toc130166849)

[**4.** **Mangësitë kriptografike** 4](#_Toc130166850)

[**5.** **Impakti në luftë** 4](#_Toc130166851)

[**6.** **Trashëgimia dhe rëndësia** 5](#_Toc130166852)

[**7.** **Pseuodokodi** 6](#_Toc130166853)

[**8.** **Shembull** 7](#_Toc130166854)

# **Hyrje**

Gjatë Luftës së Dytë Botërore, u zhvilluan disa makina për të ndihmuar në enkriptimin dhe dekriptimin e mesazheve. Shembuj të këtyre makinave përfshijnë makinën Enigma të përdorur nga gjermanët, makinën Typex të përdorur nga britanikët dhe makinën SIGABA të përdorur nga amerikanët.

Makina Enigma ishte një pajisje portative enkriptimi për të koduar mesazhet. Makina përdori një sërë rotorë dhe komponentë të tjerë për të përthyer shkronjat e një mesazhi, duke e bërë jashtëzakonisht të vështirë deshifrimin pa njohuri për cilësimet specifike të përdorura nga makina.

Kriptografët aleatë, duke përfshirë Alan Turing dhe ekipin e tij në Bletchley Park, punuan për të thyer kodin e përdorur nga makina Enigma. Ata përdorën një sërë teknikash, duke përfshirë analizën statistikore dhe zbritjen, për të thyer kodin dhe për të fituar akses në inteligjencën e vlefshme ushtarake.

# **Konteksti historik**

Makina Enigma u zhvillua nga gjermanët në fillim të shekullit të 20-të si një mjet për komunikim të sigurt. Ai përdori një seri cilësimesh të rotorëve dhe plugboard për të përzier mesazhet, duke i bërë praktikisht të pamundur deshifrimin e tyre pa cilësimet e duhura.

Gjatë Luftës së Dytë Botërore, makina Enigma u bë një mjet kritik për ushtrinë gjermane dhe u përdor gjerësisht për të kriptuar komunikimet e tyre. Makina u përdor nga të gjitha degët e ushtrisë gjermane, duke përfshirë Ushtrinë, Marinën dhe Forcat Ajrore, dhe konsiderohej si një nga pajisjet më të sigurta të enkriptimit të kohës së saj.

Megjithatë, aleatët ishin në gjendje të thyenin kodin dhe të fitonin akses në komunikimet gjermane, falë punës së kodeve në Parkun Bletchley në Angli. Kjo përpjekje për thyerjen e kodeve, e cila u drejtua nga Alan Turing dhe matematikanë dhe shkencëtarë të tjerë, ishte një faktor kritik në fitoren e Aleatëve në Luftën e Dytë Botërore.

Makina Enigma dhe përpjekja për thyerjen e kodeve që çoi në humbjen e saj patën një ndikim të rëndësishëm në zhvillimin e kriptografisë në vitet që pasuan. Ai u bë gjithashtu një simbol i fuqisë së thyerjes së kodeve dhe rolit që luajti kriptografia në formësimin e rezultatit të luftës. Sot, makina Enigma konsiderohet të jetë një objekt i rëndësishëm i Luftës së Dytë Botërore dhe është objekt i interesit dhe kërkimit të vazhdueshëm midis historianëve dhe kriptografëve.

# **Detajet teknike te makinës**

Makina Enigma ishte një pajisje komplekse elektromekanike e përdorur për të kriptuar dhe deshifruar mesazhet. Ai përbëhej nga disa komponentë kryesorë, duke përfshirë rotorët, një prizë dhe një llambë.

Rotorët ishin zemra e makinës dhe u përdorën për të përzier shkronjat e mesazhit. Makina Enigma kishte tre ose më shumë rotorë, të cilët mund të konfiguroheshin në pozicione të ndryshme për të krijuar modele të ndryshme kriptimi. Çdo rotor kishte 26 kontakte, një për secilën shkronjë të alfabetit, dhe shkronjat do të përziheshin ndërsa kalonin nëpër rotorë.

Plugboard ishte një tjetër komponent i rëndësishëm i makinës. Ai lejoi shkëmbimin e shkronjave para dhe pas kodimit të mesazhit, duke shtuar një shtresë shtesë kompleksiteti në procesin e kriptimit. Plugboard mund të konfigurohet në një sërë mënyrash, me shkronja të ndryshme që ndërrohen për të krijuar modele të ndryshme kriptimi.

Pllaka e llambës ishte komponenti përfundimtar i makinës Enigma dhe u përdor për të shfaqur mesazhin e koduar. Çdo shkronjë e mesazhit të koduar do të ndriçohej në tabelën e llambës ndërsa shtypej, duke lejuar operatorin të lexonte mesazhin e koduar.

Për të koduar një mesazh, operatori fillimisht do të zgjidhte një çelës, i cili do të përcaktonte konfigurimin e rotorëve dhe plugboard. Operatori më pas do të shkruante mesazhin në makinën Enigma, dhe makina do ta kodonte mesazhin duke gërvishtur shkronjat duke përdorur rotorët dhe plugboard. Mesazhi i koduar më pas do t'i transmetohej marrësit, i cili do të përdorte makinën e tij Enigma me të njëjtat cilësime kryesore për të deshifruar mesazhin.

# **Mangësitë kriptografike**

Pavarësisht kompleksitetit të saj, makina Enigma nuk ishte e paprekshme ndaj sulmeve kriptografike. Aleatët ishin në gjendje të thyenin kodin Enigma, falë një kombinimi faktorësh, duke përfshirë punën e kodeve britanike në Bletchley Park dhe shfrytëzimin e dobësive kriptografike në makinën Enigma.

Një nga dobësitë kryesore të makinës Enigma ishte se ajo kishte një numër të kufizuar të cilësimeve të mundshme të çelësave. Makina kishte 10^23 cilësime kyçe të mundshme, që duket si një numër astronomikisht i madh. Megjithatë, aleatët ishin në gjendje të shfrytëzonin dobësitë në mënyrën e përdorimit të makinës, si për shembull fakti që të njëjtat cilësime kryesore përdoreshin shpesh për mesazhe të shumta. Kjo i lejoi aleatët të aplikonin analizën e frekuencës për mesazhet e përgjuara dhe të përpunonin cilësimet kryesore të përdorura për ato mesazhe.

Puna e kodthyesve britanikë në Bletchley Park ishte kritike për suksesin e përpjekjeve të aleatëve për thyerjen e kodeve. Ata zhvilluan një makinë të quajtur Bombe, e cila u përdor për të automatizuar procesin e gjetjes së cilësimeve kryesore të përdorura nga makina Enigma. Bombe funksionoi duke aplikuar një sërë testesh logjike për mesazhet e përgjuara, duke ngushtuar gradualisht cilësimet e mundshme kryesore derisa të gjendej një ndeshje.

Puna e shkelësve të kodeve si Alan Turing ishte gjithashtu kritike për suksesin e përpjekjes për thyerjen e kodeve. Turing dha një sërë kontributesh të rëndësishme në përpjekjen për thyerjen e kodit, duke përfshirë zhvillimin e makinës Bombe dhe konceptin e "Testit Turing", i cili që atëherë është bërë një koncept i rëndësishëm në fushën e inteligjencës artificiale.

Në përmbledhje, dobësitë e makinës Enigma, të kombinuara me përpjekjet e kodeve britanike në Bletchley Park, i lejuan aleatët të thyejnë kodet gjermane dhe të fitojnë një avantazh të rëndësishëm në Luftën e Dytë Botërore. Makina Enigma mbetet një objekt i rëndësishëm i kësaj periudhe , si simbol i fuqisë së kriptografisë dhe rolit që luajti thyerja e kodeve në formësimin e rezultatit të luftës

# **Impakti në luftë**

Thyerja e kodit Enigma pati një ndikim të rëndësishëm në rezultatin e Luftës së Dytë Botërore. Duke përgjuar dhe deshifruar komunikimet gjermane, aleatët ishin në gjendje të fitonin inteligjencë të vlefshme për operacionet ushtarake gjermane, gjë që i lejoi ata të planifikonin operacionet e tyre në mënyrë më efektive.

Një nga fushat kryesore ku ndikoi thyerja e kodit Enigma ishte Beteja e Atlantikut. Kjo ishte një betejë kritike, pasi përfshinte U-boat gjermane që përpiqeshin të prishnin linjat e furnizimit midis Amerikës së Veriut dhe Evropës. U-boat gjermane ishin fillimisht shumë të suksesshme në këtë përpjekje, duke fundosur një numër të madh anijesh aleate dhe duke paraqitur një kërcënim serioz për përpjekjet e luftës aleate.

Megjithatë, thyerja e kodit Enigma i lejoi aleatët të fitonin inteligjencë të vlefshme në lidhje me lëvizjet dhe taktikat e U-boateve gjermane. Kjo i lejoi aleatët të kundërshtonin në mënyrë efektive kërcënimin gjerman të U-boat, duke përdorur taktika të tilla si konvoji dhe përdorimi i avionëve me rreze të gjatë për të patrulluar detet. Deri në fund të luftës, aleatët kishin fituar në mënyrë efektive Betejën e Atlantikut, falë pjesërisht të inteligjencës së fituar nga thyerja e kodit Enigma.

Përveç Betejës së Atlantikut, thyerja e kodit Enigma pati një ndikim të rëndësishëm edhe në operacione të tjera ushtarake. Për shembull, ai luajti një rol kyç në suksesin e pushtimit të Normandisë në Ditën D, pasi Aleatët ishin në gjendje të fitonin informacione rreth lëvizjeve dhe mbrojtjeve të trupave gjermane përmes komunikimeve të përgjuara.

Në përgjithësi, thyerja e kodit Enigma ishte një faktor kritik në fitoren e Aleatëve në Luftën e Dytë Botërore. Ai i lejoi aleatët të fitonin inteligjencë të vlefshme për operacionet ushtarake gjermane, gjë që i ndihmoi ata të planifikonin operacionet e tyre në mënyrë më efektive dhe të fitonin një avantazh të rëndësishëm në fushën e betejës.

# **Trashëgimia dhe rëndësia**

Makina Enigma ka lënë një trashëgimi të rëndësishme dhe ka pasur një ndikim të madh në rezultatin e Luftës së Dytë Botërore. Roli i saj në formësimin e rrjedhës së luftës, si dhe rëndësia e saj më e gjerë historike dhe kulturore, e ka bërë atë një simbol të qëndrueshëm të fuqia e kriptografisë dhe thyerjes së kodeve.

Për sa i përket ndikimit të tij në rezultatin e luftës, thyerja e kodit Enigma ishte një faktor kritik në fitoren e Aleatëve. Ai i lejoi aleatët të fitonin inteligjencë të vlefshme për operacionet ushtarake gjermane, gjë që i ndihmoi ata të planifikonin operacionet e tyre në mënyrë më efektive dhe të fitonin një avantazh të rëndësishëm në fushën e betejës.

Trashëgimia e makinës Enigma shtrihet edhe përtej vetë luftës, pasi ndikimi i saj në kriptografi dhe thyerjen e kodeve vazhdon të ndihet edhe sot e kësaj dite. Thyerja e kodit Enigma hapi rrugën për zhvillime të mëtejshme në kriptografi dhe thyerje të kodeve, duke përfshirë zhvillimin e metodave moderne të kriptimit të bazuara në kompjuter..

Poashtu ndikimi i kodit Enigma në kriptografinë moderne është i rëndësishëm, pasi shënoi një pikë kthese në zhvillimin e kriptografisë dhe teknikave të përdorura për të thyer kodet. Suksesi i përpjekjeve për thyerjen e kodit Enigma çoi në një zhvendosje të fokusit nga kriptografia klasike në kriptografinë moderne, e cila mbështetet në algoritme komplekse dhe teknika matematikore për të siguruar sigurinë e komunikimeve.

Një nga ndikimet më të rëndësishme të kodit Enigma në kriptografinë moderne është zhvillimi i kompjuterëve dhe përdorimi i fuqisë llogaritëse në thyerjen e kodeve. Përdorimi i makinës Bombe, e cila ishte një pajisje mekanike e përdorur për të automatizuar procesin e deshifrimit të mesazheve Enigma, hapi rrugën për zhvillimin e kompjuterëve elektronikë, të cilët kanë revolucionarizuar kriptografinë moderne. Sot, kompjuterët përdoren për të gjeneruar dhe thyer kode duke përdorur algoritme komplekse matematikore që do të ishte e pamundur të zbatoheshin manualisht.

Një tjetër ndikim i kodit Enigma në kriptografinë moderne është koncepti i sulmit "njeri në mes", i cili i referohet një sulmuesi që përgjon dhe ndryshon komunikimet midis dy palëve. Kodi Enigma ishte i prekshëm ndaj sulmeve të tilla sepse cilësimet e plugboard dhe reflektori ishin të fiksuara dhe operatori duhej të caktonte manualisht pozicionet e rotorit. Kjo dobësi çoi në zhvillimin e teknikave moderne të kriptimit që mbështeten në algoritme më të sofistikuara dhe çelësa të rastësishëm për të garantuar sigurinë e komunikimit.

Në përgjithësi, makina Enigma përfaqëson një simbol të fuqishëm të rolit që kriptografia dhe thyerja e kodeve mund të luajnë në formësimin e rrjedhës së historisë. Trashëgimia e saj ka pasur një ndikim të qëndrueshëm në fushën e kriptografisë dhe në kulturën popullore, dhe ajo mbetet një simbol i qëndrueshëm i fuqisë së zgjuarsisë njerëzore përballë fatkeqësive. Së fundmi, kodi Enigma ka pasur një ndikim të rëndësishëm kulturor, duke shërbyer si një simbol i fuqisë së kriptografisë dhe rëndësisë së thyerjes së kodit në luftën moderne. Thyerja e kodit Enigma ka qenë temë e shumë librave, filmave dhe shfaqjeve televizive dhe vazhdon të frymëzojë magjepsjen e publikut me botën e kriptografisë dhe thyerjes së kodeve.

# **Si bëhet enkriptimi i mesazhit në makinën Enigma?**

Në makinën Enigma, enkriptimi arrihet përmes një sërë zëvendësimesh dhe transpozimesh.

Së pari, mesazhi me tekst të thjeshtë shtypet në makinë dhe çdo shkronjë futet duke shtypur një tast në tastierë. Ndërsa shtypet çdo çelës, ai bën që rotorët të rrotullohen, gjë që ndryshon rrugët elektrike brenda makinës. Ky proces zëvendëson shkronjën hyrëse për një shkronjë të ndryshme sipas pozicioneve aktuale të rotorit.

Më pas, shkronja e zëvendësuar kalohet përmes plugboard, e cila më tej zëvendëson shkronjën bazuar në lidhjet e bëra midis çifteve të shkronjave në tabelë.

Pas kalimit nëpër plugboard, letra reflektohet jashtë reflektorit dhe dërgohet përsëri përmes plugboard dhe rotorëve në rend të kundërt. Kjo prodhon një zëvendësim tjetër të shkronjës.

Më në fund, shkronja e koduar shfaqet në tabelën e llambës, e cila tregon shkronjën e zëvendësuar bazuar në pozicionet aktuale të rotorit.

Ky proces përsëritet për secilën shkronjë në mesazh, me pozicionet e rotorit që ndryshojnë pasi çdo shkronjë të kodohet. Mesazhi i koduar që rezulton mund të deshifrohet vetëm nëse marrësi di saktësisht të njëjtat cilësime si dërguesi, duke përfshirë pozicionet e rotorit dhe lidhjet e plugboard.

# **Pseudokodi**

Hapi 1: Inicializoni cilësimet e makinës Enigma, duke përfshirë renditjen e rotorit, pozicionet e fillimit dhe lidhjet e plugboard.

Hapi 2. Funksioni i enkriptimit (tekst i thjeshtë):

a. Cakto tekstin e koduar në vargun bosh.

b. Për secilin karakter në tekstin e thjeshtë:

i. Kaloni karakterin përmes plugboard(nëse ka një lidhje për atë karakter).

ii. Rrotulloni rotorin e parë me një pozicion (përveç nëse ai ka arritur pozicionin e tij të rrotullimit).

iii. Kaloni karakterin përmes rotorëve në rendin e specifikuar.

iv. Kaloni karakterin përmes reflektorit.

v. Kaloni karakterin përsëri nëpër rotorë në rend të kundërt.

vi. Rrotulloni sërish rotorin e parë.

vii. Kaloni karakterin përmes plugboard(nëse ka një lidhje për atë karakter).

viii. Shtoni karakterin e koduar në tekstin e shifruar.

c. Ktheni tekstin e shifruar.

3. Funksioni i dekriptimit (teksti i shifruar):

a. Cakto tekstin e thjeshtë në vargun bosh.

b. Për çdo karakter në tekstin e shifruar:

i. Kaloni karakterin përmes plugboard(nëse ka një lidhje për atë karakter).

ii. Rrotulloni rotorin e parë me një pozicion (përveç nëse ai ka arritur pozicionin e tij të rrotullimit).

iii. Kaloni karakterin përmes rotorëve në rendin e specifikuar.

iv. Kaloni karakterin përmes reflektorit.

v. Kaloni karakterin përsëri nëpër rotorë në rend të kundërt.

vi. Rrotulloni sërish rotorin e parë.

vii. Kaloni karakterin përmes tavolinës (nëse ka një lidhje për atë karakter).

viii. Shtoni karakterin e deshifruar në tekstin e thjeshtë.

c. Ktheni tekstin e thjeshtë.

# **Shembull**

Le të themi se mesazhi me tekst të thjeshtë është: "ATTACK AT DAWN"

Operatori fillimisht do të vendoste çelësin për makinën Enigma, e cila do të përfshinte zgjedhjen e një kombinimi të veçantë të cilësimeve të rotorit, lidhjeve të plugboard dhe cilësimeve të reflektorit. Për qëllimet e këtij shembulli, le të themi se cilësimet kryesore janë:

Pozicionet e rotorit: 1-2-3

Lidhjet e pllakave: A-D, F-G, J-K, Q-S, T-Z

Reflektori: B

Operatori më pas do të shkruante mesazhin me tekst të thjeshtë në tastierën e makinës Enigma. Ndërsa shtypet çdo shkronjë, makina do ta kodonte letrën duke përdorur cilësimet aktuale të çelësit dhe do të shfaqte shkronjën përkatëse të tekstit të shifruar në llambë. Për shembull:

A bëhet G

T bëhet L

T bëhet M

A bëhet G

C bëhet Q

K bëhet B

hapësira mbetet hapësirë

A bëhet G

T bëhet L

hapësira mbetet hapësirë

D bëhet S

A bëhet G

W bëhet X

N bëhet D

Pra, mesazhi i koduar me tekst do të ishte: "GLMGGQB GLDX"

Operatori më pas do t'i transmetonte mesazhin e tekstit të shifruar marrësit të synuar, i cili do të përdorte makinën e tij Enigma me të njëjtat cilësime kryesore për të deshifruar mesazhin dhe për të zbuluar mesazhin origjinal të tekstit të thjeshtë.