Enigma

Cembauer, Josip

Sveučilište J.J. Strossmayera u Osijeku
Odjel za matematiku
Sveučilišni preddiplomski studij matematike

Josip Cembauer

Enigma

Završni rad

Osijek, 2017.

Sveučilište J. J. Strossmayera u Osijeku
Odjel za matematiku
Sveučilišni preddiplomski studij matematike

Josip Cembauer

Enigma

Završni rad

Mentor: prof. dr. sc. Ivan Matić

Osijek, 2017.

Sažetak Tema ovog završnog rada je njemački šifrirni uređaj Enigma. Opisana je ideja i razvoj iste, te zašto su kriptoanalitičari imali težak posao oko probijanja njene šifre. U nastavku se govori o poljskom i britanskom utjecaju na probijanju Enigme, te njenom utjecaju na tijek Drugog svjetskog rata.

Ključne riječi: kriptografija, kriptoanaliza, Enigma, Arthur Scherbius, Marian Rejewski, Alan Turing, Drugi svjetski rat

Abstract The theme of this final paper is the German encryption device Enigma. The idea and development of the same are described, and why the cryptoanalysts have had a tough job of breaking the code. The following is the Polish and British influence on the breaking of Enigma and its impact on the course of World War II.

Key words: cryptography, cryptanalysis, Enigma, Arthur Scherbius, Marian Rejewski, Alan Turing, World War II

Sadržaj

1 Uvod

Kroz povijest vođe država i naroda oslanjali su se na efikasnu komunikaciju kako bi uspješno vodili svoje države i vojsku, te su uvijek morali biti na oprezu da njihove poruke neće otići u krive ruke te tako saznati njihove planovi. Samim time rodila se želja za tajnošću, što je dovelo do razvoja kriptografije, a samim time na neprijateljskoj strani do razvoja kriptoanalize.

Kriptografija je znanost koja se bavi otkrivanjem metoda spremanja i slanja podataka u šifriranoj formi kako bi ju samo oni kojima je namijenjena mogli pročitati, odnosno obraditi. Kriptoanaliza predstavlja proučavanje metoda za otkrivanje šifriranih podataka bez posjedovanja tajnog ključa koji je potreban za pristup tim podacima.

Kriptografi su u prošlosti često gubili bitke nad kriptoanalitičarima, tako je bilo i u Prvom svjetskom ratu. Godine nakon rata donijele su da se kriptografi ostave do tada najkorištenijih „olovka-papir“ šifri i okrenu se, u to vrijeme, modernijem pristupu. mehanizaciji tajnosti. Takvi mehanički izumi doveli su do većeg broja tajnih ključeva, pa su samim time šifrirani podaci bili sigurniji. Također je dovelo do bržeg šifriranja, pa samim time i dešifriranja podataka.

Radeći u tom smjeru njemački izumitelj Arthur Scherbius i njegov prijatelj Richard Ritter 1918. osnivaju inovativnu inžinjersku tvrtku Scherbius und Ritter. Kako je Scherbius bio zadužen za istraživanje i razvoj, jedan od projekata mu je bio i da zamijeni do tad neadekvatne kriptografske sustave korištene tijekom Prvog svjetskog rata. Upravo taj projekt je donio razvoj Enigme, najpoznatijeg sustava u povijesti enkripcije.

Slika 1: Arthur Scherbius

2 Enigma - princip rada

Enigma je kriptografski električno-mehanički uređaj koji je izgledom ličio na pisaći stroj. Sastojao se od:

- Tipkovnice, koja služi za unos otvorenog teksta
- Enkripcijske jedinice (rotora), koja služi za enkripciju otvorenog teksta u šifrirani
- Zaslona, kojI služi za prikaz šifriranog teksta

Kroz sve mehaničke dijelove bile su provučene žice koje bi pritiskom na tipku zatvarale strujni krug. Tipkovnica se sastojala od 26 tipki na kojoj su slova engleske abecede. Zaslon se sastojao od 26 lampica na kojima su također bila ispisana slova engleske abecede. Kako su kroz enkripcijsku jedinicu odnosno rotore provedene žice, pritiskom na tipkovnicu slova otvorenog teksta na zaslonu bi zasvijetlila lampica slova šifriranog teksta. Operator na Enigmi bi najprije morao podesiti postavke enkripcijskog dijela u određeni položaj, no o tome malo kasnije. Nakon toga pritiskom na tipku prvog slova otvorenog teksta, enkripcijski dio šifrira slovo te se strujni krug zatvara i na zaslonu zasvjetli lampica slova koje je prvo slovo šifriranog teksta, te ga operator zapisuje.

Enkripcijska jedinica glavni je dio uređaja. Princip rada enkripcijske jedinice, pa tako i Enigme se temelji na Albertijevom šifrirnom disku kojeg je oko 1470. izumio Leone Battista Alberti. On je uzeo dva bakrena diska različitih veličina i na oba ispisao abecedu. Stavljanjem manjeg na veći i učvrstivši ih sa iglom koja je služila kao osovina, diskovi su se mogli okretati neovisno jedan od drugoga, pa su tako abecede mogle biti u različitim relativnim položajima. Veći disk predstavlja otvoreni tekst, a manji šifrirani tekst.

Na taj način Albertijevim diskom se može enkriptirati Cezarovom šifrom koja funkcionira na principu da se pomakom od npr. 3 mjesta unutarnjeg diska slovo A enkriptira u slovo D, slovo B u E i tako dalje. Pa bi tako koristeći Cezarovu šifru na Albertijevom šifrirnom disku otvoreni tekst „DOBRO“ bio šifriran u „GREUR“. Koristeći samo Cezarovu šifru na disku je relativno jednostavno za razbiti, pa je Alberti predlagao da se nakon svakog enkriptiranog slova promjeni položaj diskova.

Sljedećeg stoljeća Blaise de Vigenère iz te ideje stvorio je Vigenèreovu šifru koja je pomake radila prema tajnom ključu odnosno riječi. Uzmemo li da nam tajni ključ bude riječ „MIR“, a otvoreni tekst „DOBRO“. Albertijev disk namještamo prema tajnom ključu. Manji disk pomičemo u položaj da slovo „M“ bude uz slovo „A“, pa tako slovo „D“ enkriptiramo u slovo „Q“. Kako bi enkriptirali drugo slovo „O“, manji disk pomičemo u položaj da slovo „I“ bude uz slovo „A“ na većem disku, te na taj način „O“ postaje „X“. Nastavkom istog procesa dobivamo šifriranu poruku koja glasi „QXTEX“. Iako kompliciranija od Cezarove, Vigenèrovu šifru su u 19. stoljeću probili Kasiski i Babbage.

Unatoč tome, Scherbius je iskoristio gore navedene sustave te ih ugradio u kompleksniju cijelinu. Pa su tako diskovi bili osnova Enigme. U ovom tekstu zvat ćemo ih rotori.

Rotor je bio debeli disk isprepleten žicama na kojem je bilo ispisano 26 slova engleske abecede. Isprepletenost žica unutar rotora određuje na koji način će otvoreni tekst biti šifriran. Scherbiusova ideja je da se disk automatski zakrene za jednu dvadesetšestinu njegove rotacije svaki puta kada bi se slovo enkriptiralo pa se na taj način šifrirna abeceda mijenja nakon svake enkripcije. Sa takvom rotacijom rotor definira 26 (dvadeset i šest) šifrirnih abeceda pa zbog toga Enigmu nazivamo polialfabetski šifrirni uređaj.
Rotacija rotora je najbitnija značajka dizajna međutim upravo zbog toga uređaj ima jednu očiglednu slabost. Ukoliko bi isto slovo pritisnuli 26 puta rotor bi se vratio u početni položaj te bi se nastavkom tipkanja i ponavljanjem istog rasporeda šifrata vidjela frekvencija ponavljanja što bi dovelo do lakog probijanja. Kriptografi uglavnom izbjegavaju ponavljanje šifriranog teksta jer dolazi do regularnosti i strukture šifriranog teksta, što je simptom slabe šifre.
Iz tog razloga Scherbius je ugradio drugi rotor koji je spojio. U ovom slučaju prvi rotor bi se zakretao za jednu poziciju dok bi drugi mirovao sve dok prvi rotor ne napravi kompletnu rotaciju. Na taj način potrebno je 26 puta više pritisnuti istu tipku kako bi došlo do ponavljanja. U tom slučaju dva rotora bi izmjenjivala 26×26 odnosno 676 šifrirnih abeceda. Zbog dodatne kompleksnosti Enigma je sadržavala 3 rotora što bi predstavljalo $26 \times 26 \times 26$ odnosno 17576 različitih šifrirnih abeceda.

Scherbiusa je u Enigmu ugradio i reflektor. Reflektor je nalik na rotor, ali se ne rotira. Također, žice izlaze na istu stranu na koju ulaze. Pritiskom na tipku električni signal putuje kroz rotore te dolazi do reflektora koji signal vraća u ista 3 rotora, ali drugim putem. Naizgled bespotreban dodatak jer zbog svoje statičnosti ne povećava broj različitih šifrirnih abeceda. Međutim pravi smisao se vidi kada shvatimo na koji način uređaj enkriptira i dekriptira tekst.

Zamislimo kako je to bilo tijekom Drugog svjetskog rata. Operator A na Enigmi bi imao zadatak da pošalje poruku putem radioveze drugom operatoru B udaljenom više stotina kilometara. Operator A podešava početne položaje 3 rotora. Ta početna postavka definira kako će se otvoreni tekst šifrirati. Što bi drugim riječima značilo da je početna postavka uređaja zapravo tajni ključ ili ključ šifre. Operator A utipkava prvo slovo otvoreniog teksta, enkripcijom kroz rotore i zatvaranjem strujnog kruga, na zaslonu sa lampicama zasvijetli lampica enkriptiranog slova. Rotor se zakreće te operator nastavlja sa šifriranjem otvorenog teksta. Šifrirani tekst se radio vezom šalje operatoru B. Kako bi operator B mogao prevesti šifrirani tekst morao je imati tajni ključ kako bi rotore Enigme postavio u isti položaj.

Tajni ključevi su se mijenjali svakodnevno te su bili zapisani u knjigu šifara koju je čuvala osoba od povjerenja. Knjiga šifara bi se mijenjala svakih 28 dana, odnosno četiri tjedna. Operator bi dobio tajni ključ koji će koristiti taj dan te bi prema njemu podesio postavke Enigme. Operator B utipkava šifrirani tekst slovo po slovo te mu zasvijetle lampice slovo po slovo otvorenog teksta. To bi zapravo značilo da Operator A utipkava otvoreni tekst da ga enkriptira u šifrirani tekst, a operator B utipkava šifrirani tekst da ga dekriptira u otvoreni tekst. Lakoća dešifriranja je razlog zašto je ugrađen reflektor.

Vrlo je jasno da tajni ključ i knjiga šifara u kojoj su se nalazili tajni ključevi ne smije doći u neprijateljske ruke. Neprijatelj je lako mogao doći u posjed Enigme no bez knjige šifara dešifriranje poruke bilo bi teško. Bez tajnog ključa neprijateljski kriptoanalitičar morao bi provjeriti 17 576 mogućih početnih postavki. Kriptoanalitičar bi morao unijeti početnu postavku, upisati šifrirani tekst i provjeriti dali dobiveni tekst ima smisla. Ako nema morao bi promijeniti postavke i početi ispočetka. U slučaju da kriptoanalitičar uspije u jednoj minuti provjeriti jednu početnu postavku uređaja, i kada bi radio cijeli dan i noć bilo bi mu potrebno skoro dva tjedna da provjeri sve kombinacije. No ukoliko neprijatelj aktivira više ljudi na taj zadatak sve postavke mogu biti provjerene u dan pa čak i u nekoliko sati.

Iz tog razloga Scherbius je uveo dvije nove komponente u Enigmu. Prva je da se rotori mogu zamijenjivati. Npr. rotor na prvom mjestu zamijenio bi se sa onim u sredini. Raspoered rotora utječe na enkripciju pa se tako broj mogućih kombinacija povećava za 6 puta jer rotore možemo složiti u 6 različitih položaja (123, 132, 213, 231, 312, 321).

Druga komponenta je ploča priključaka koja operatoru omogućuje da ukopča kabel koji ima efekt da zamijeni slova sa nekim drugim slovom prije nego uđe u rotor. Npr. kabel može služiti da se zamijene slova A i B, pa će na taj način kada operator pritisne slovo A električni signal putovati putem koji je dodijeljen slovu B i obrnuto. Operator je imao na raspolaganju 6 kablova, što je značilo da 6 parova slova mogu biti zamijenjena, ostavljajući 14 slova nezamijenjenih. Položaji kablova također su dio tajnog ključa pa su morali biti uneseni u knjigu šifara. Ova komponenta uvelike je povećala razinu sigurnosti Enigme.

Koliko različitih početnih postavki (šifriranih abeceda) ima Enigma?

- Položaji rotora – 3 rotora koji imaju 26 položaja: $26 \times 26 \times 26 = 17\ 576$
- Redoslijed rotora – 3 rotora se mogu postaviti u 6 različitih redoslijeda
- Ploča priključaka – broj kombinacija na koji se mogu složiti 6 parova od 26 slova=100 391 791 500
- Ukupno: $17576 \times 6 \times 100391791500 = 10\ 586\ 916\ 764\ 424\ 000$

Kriptoanalitičaru koji može provjeriti jednu postavku u minuti trebalo bi starost svemira da provjeri sve moguće postavke.
Kako najveći broj tajnih ključeva donosi ploča priključaka, zapitali bi se zašto su uopće potrebni rotori. Naime, ukoliko bi se samo služili pločom priključaka, tada bi to bila monoalfabetska šifra koja zamijenjuje slova. Zamijene se ne bi mijenjale svakom novom enkripcijom, pa je time monoalfabetska šifra podložna frekvencijskoj kriptoanalizi. Rotori su donijeli mali broj ključeva ali njihove postavke se mijenjaju svakom novom enkripcijom pa je zbog toga Enigma bila otporna na frekvencijsku analizu. Kombiniranjem rotora i ploče priključaka Scherbius je dobio veliki broj mogućih ključeva koji su bili otporni na frekvencijsku kriptoanalizu.

Scherbius je vjerovao da je izumio uređaj koji je nepobjediv, te ga je 1925. počeo masovno proizvoditi. Enigmu su koristile banke, željeznice, pošte, a najviše vojska. Uistinu, Scherbius je napravio najbolji kriptografski sustav u svijetu toga vremena.Tijekom Drugog svjetskog rata činilo se da će Enigma imati ključnu ulogu u pobjedi Njemačke, ali ne. Enigma je odigrala ključnu ulogu nacističkog poraza i završetka Drugog svjetskog rata. Scherbius nije doživio Enigmin uspon i pad jer je 1929. poginuo u nesreći.

Slika 2: Enigma

3 Probijanje Enigme

Poslije Prvog svjetskog rata, britanski kriptoanaltičari nastavili su pratiti njemačku komunikaciju. Enigma je 1926. ušla u vojnu upotrebu u Njemačkoj i kada su britanski kriptoanalitičari presreli jednu šifriranu poruku zbunila ih je potpuno. Kako se broj Enigmi u upotrebi povećavao kriptoanalitičarima je bilo sve teže. Amerikanci i Francuzi su također pokušali odgonetnuti rad Enigme ali su jednako bili zbunjeni, te su ubrzo gubili nadu da će ju probiti. Njemačka je sada imala najsigurniju komunikaciju na svijetu. No, jedna nacija si nije mogla priuštiti odustajanje.

3.1 Poljski utjecaj

Nakon Prvog svjetskog rata, Poljska je bila neovisna država, ali zabrinuta za svojoj suverenitet. Istočno od njih bila je Rusija koja je željela proširiti komunizam, a zapadno Njemačka koja je željela vratiti teritorij koji su izgubili u ratu. Iz straha od dva moguća neprijatelja osnovali su šifrirni ured Biuro Szyfrow. Zadužen za dešifriranje njemačke komunikacije bio je kapetan Maksymilian Ciezki. Kako Poljaci nisu u posjedu imali Enigmu bilo mu je nemoguće dešifrirati njemačke vojne poruke.

Prvi korak prema probijanju Enigme napravio je razočarani njemac Hans-Thilo Schmidt. Schmidt je prihvatio karijeru u njemačkoj vojsci no po završetku rata nije više bio potreban u vojsci. Poniženje Schmidta uvelike je utjecalo uspjeh njegovog brata Rudolpha, koji se također borio u ratu ali koji je ostao u vojsci nakon istog. Rudolph je tijekom 20-ih godina 20. stoljeća postavljen za šefa osoblja Službe veza i bio je odgovoran osigurati sigurnu komunikaciju. Upravo je Rudolph odobrio korištenje Enigme u vojne svrhe. Hans-Thilo je pitao za pomoć, pa mu je Rudolph dogovorio posao u Berlinu u Enigminom zapovjednom centru. U skupom Berlinu, sam bez obitelji i ljubomoran na brata, te ogorčen prema naciji koja ga je odbacila, Hans-Thilo je odlučio prodati tajne informacije.

Krajem 1931. Schmidt se susreo sa francuskim tajnim agentom kojem je dopustio fotografiranje dva tajna dokumenta za tadašnjih 10 000 maraka (današnjih otprilike 30 000 eura). Tajni dokumenti su bili upute za uporabu šifrirnog uređaja Enigma. Prema tim uputama Saveznici su bili u mogućnosti stvoriti kopiju Enigme, no to im nije bilo dovoljno da dešifriraju poruke jer im je za to potreban i tajni ključ. Francuzi su smatrali da bez ključa ne mogu ništa postići te čak nisu napravili niti kopiju Enigme. Kako su poslije rata sa Poljacima imali sporazum o vojnoj suradnji, Francuzi su sa njima podijelili fotografije.

Poljaci su prihvatili beznadni zadatak probijanja Enigme uvjerivši se da mora postojati brži način da dođu do tajnog ključa. Dokumenti su uz informacije kako funkcioniraju rotori i ploča priključaka, sadržavali i informacije o procedurama i izgledu Knjige šifara. Procedura je da svi operatori početkom mjeseca dobiju Knjigu šifara za taj mjesec u kojoj je naznačeno za koji dan je koji ključ. Prema ključu za taj dan operatori zamjenjuju 6 parova slova preko ploče priključaka, postave redoslijed rotora i postave rotore u početne položaje. Nakon toga poruka se utipkava, šifrira te šalje primatelju-operatoru koji putem Enigme dešifrira.

Proces je relativno siguran. Ono što ga slabi je velika količina poruka poslana u istom danu. Upravo ono što kriptoanalitičari žele, dobiti što veću količinu materijala koji je korišten primjenom istog tajnog ključa kako bi mogli jednostavnije otkriti tajni ključ.
Iz tog razloga su Nijemci koristeći dnevni ključ slali novi ključ za svaku novu poruku. Novi ključ bi imao iste postavke ploče priključaka i redoslijed rotora, ali drugačije početne položaje rotora. Koristeći dnevni ključ poslali bi nasumične nove položaje rotora za sljedeću poruku. Npr. dnevna šifra je KOD, operator pošiljatelj odabire nasumični položaj rotora za sljedeću poruku GSJ, utipkava ju dvaput, pa se GSJGSJ šifrira u JBZLAI, operator primatelj ukucava JBZLAI, te dobije GSJGSJ. Sljedeću poruku koju primatelj dobije šifrirana je sa početnima postavkama rotora GSJ.
Da su Nijemci koristili samo dnevni ključ tada bi kriptoanalitičari skupili ogromnu količinu podataka vezanu uz taj ključ. Međutim, na ovaj način dnevni ključ se koristio samo za slanje ključeva za poruke. Uz to, svaki novi ključ za poruke se kreirao nasumično tako da se koristeći isti ključ može skupiti svega par stotina šifriranih slova.

Na prvu, sistem je izgledao nedodirljiv, ali Poljski kriptoanalitičari su bili neustrašivi. Biuro je organizirao tečaj kriptografije te pozvao dvadeset matematičara sa sveučilišta u Poznanu. Kako je Poznan bio pod vlašću Njemačke do 1918. matematičari su odlično znali njemački jezik. Od njih dvadeset, trojica su pokazala sposobnosti u rješavanju šifara te su zaposleni u Biuro-u. Najdarovitiji od njih bio je Marian Rejewski.

Njegova strategija je bila činjenica da je ponavljanje neprijatelj sigurnosti Enigme. Ponavljanjem dolazi do obrazaca, a kriptoanalitičari uspijevaju zbog obrazaca. Najočiglednije ponavljanje je poruka s novim ključem, no Njemci su zahtijevali ponavljanje kako bi se smanjila greška operatora ili radioveze. Rejewski je svakodnevno na raspolaganju imao novu hrpu poruka i sve počinju sa šest slova gdje se troslovna poruka ponavlja, te su napisane istim ključem tijekom jednog dana.

	1.	2.	3.	4.	5.	6.
1. poruka	G	B	T	N	R	A
2. poruka	L	S	O	S	C	I
3. poruka	R	U	Z	L	I	K
4. poruka	S	T	G	B	W	X

U svakoj poruci prvo i četvrto slovo su enkripcija istog slova i to prvog slova ključa za novu poruku. Pa je tako, drugo i peto slovo enkripcija istog slova, te treće i šesto slovo enkripcija istog slova. Razlog zašto je enkripcija istog slova različita leži u tome da se rotor pomakao za tri polja.Poznato je da su npr. iz prve poruke G i W enkripcija istog slova nakon 3 rotacije rotora, no ne zna se kojeg slova. Nepoznanica je početna postavka rotora. Poznato nam je da su G i W povezani, također znamo iz druge poruke da su L i P. Nastavimo li dalje imamo povezane R i L, te S i B . Rejewski je unosio u tablicu koja bi za naše poruke izgledala ovako:

1. slovo	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
4. slovo							N					S						L	B						

Ako bi Rejewski presreo dovoljno poruka u jednom danu kompletirao bi cijelu povezanu abecedu, koja bi izgledala ovako:

1. slovo	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
4. slovo	M	T	J	P	K	D	N	V	A	Y	H	S	I	Z	U	X	F	L	B	E	Q	R	G	O	W	C

Rejewski nije znao koji je ključ, ali je znao da je tablica povezanosti rezultat ključa. Da je ključ drugačiji tablica povezanosti izgledala bi potpuno drugačije. Pa se sljedeće pitanje samo nametnulo, pa se Rejewski pitao da li je moguće iz tablice otkriti koji je dnevni ključ. Zatim je počeo tražiti obrasce unutar tablice. Naposljetku je počeo tražiti slovni lanac. Npr. slovo A je povezano sa slovom M, slovo M iz gornjeg reda je povezano sa I, I sa R, R sa L, L sa A. S ostalim slovima je napravio njihove pripadajuće lance te naznačio koliko veza ima među njima.

A - M - I - A	3 veze
B - T - E - K - H - V - R - L - S - B	9 veza
C - J - Y - W - G - N - Z - C	7 veza
D - P - X - O - U - Q - F - D	7 veza

Do sad smo promotrili samo vezu između prvog i četvrtog slova u poruci. Rejewski je isto radio i za preostala povezana slova, drugo i peto, te treće i šesto slovo. Shvatio je da karakteristike ključa direktno ovise o postavkama rotora, a ne o ploči priključaka. Uzmimo gornji primjer zamijenimo li slova V i O te R i T lanci će izgledati ovako:

A - M - I - A	3 veze
B - R - E - K - H - O - T - L - S - B	9 veza
C - J - Y - W - G - N - Z - C	7 veza
D - P - X - V - U - Q - F - D	7 veza

Neka slova su se promijenila, ali broj veza u lancu je ostao isti. Iz tog slijedi zaključak Rejewskoga. Ukupan broj ključeva koji je sad potrebno provjeriti je umnožak broja rasporeda rotora (6) i broja pozicija rotora (17 576), što je 105 456. Puno manje od 10 586 916 764 424 000 svih mogućih ključeva.

Rejewski je zahvaljujući Schmidtu imao repliku Enigme te je njegov tim počeo provjeravati svih 105 456 postavki rotora, te zapisivanjem lanaca generiranu sa svakom postavkom. Cijela jedna godina je bila potrebna da dovrše knjigu sa svim zapisima, te je mogao krenuti u probijanje Enigme.

Svakodnevnom analizom enkriptiranih poruka koje su sadržavale nove ključeve shvatio je da ako promatra povezanost između prvog i četvrtog slova dobiva, za primjer, četiri lanca sa 3, 9, 7 i 7 veza. Analizirajući druga i peta slova rezultat je 4 lanca sa 2, 3, 9 i 12 veza. Te za treće i šesto slovo rezultat je 5 lanaca sa 5, 5, 5, 3 i 8 veza. Lanci su mu služili kao svojevrstan otisak prsta. Provjerio bi ih u knjizi sa svim obrađenim zapisima te je znao koji je dnevni ključ. Preostalo mu je da odgonetne ploču priključaka. Odlučio je da izvadi sve kablove iz ploče priključaka tako da ploča priključaka nema utjecaja na šifriranje. Ukucavanjem šifriranog teksta često je dobivao besmisleni poredak, jer su bile nepoznate postavke na ploči

priključaka. No povremeno dobio je približno poznate fraze: kao npr. „dorazimubelrin“, što bi trebalo biti „dolazim u Berlin“ ako se zamijene slova R i L = J. To bi značilo da se slova R i L spajaju kablom na ploči, dok se D, O, A, Z, I, M, U, B, E i N ne spajaju sa drugim slovima. Nastavkom analize došlo bi se do kompletne postavke ploče za priključke.
Na taj način Rejewski i njegov tim su do kraja dana saznali dnevni ključ te su mogli dešifrirati sve presretene poruke toga dana.

Probijanjem Enigme, njemačka komunikacija za Poljake je bila transparentna. Poljska nije bila u ratu sa Njemačkom, ali sada su mogli saznati koje su njihove namjere, te su se u slučaju napada mogli obraniti. Za uspjeh Rejewskog je bila potrebna velika intelektualna snaga i jaka volja. Rejewski je tijekom godina razvio mehanizirani sustav provjere koji bi automatski tražio odgovarajući ključ između 17576 mogućih. Kako ima 6 različitih redoslijeda rotora, značilo je da ih je moralo raditi 6 istovremeno. Rejewski je uređaj nazvao Bomba. Bomba je bila visoka oko jednog metra i za dva sata je mogla pronaći dnevni ključ. Tijekom 30-tih godina 20. stoljeća Rejewski i njegovi kolege su uložili mnogo truda kako bi dostigli svoj cilj, no možda nisu morali. Šef Biuro-a, bojnik Gwido Langer je preko Francuza i dalje dobivao informacije od Schmidta. Ukupno je dobio knjiga šifara sa pripadajućim dnevnim ključevima za 38 mjeseci. No, nije ih dao Rejewskom. Smatrao je da ga priprema za trenutak kada ključevi više neće biti dostupni.

U prosincu 1938. Njemački kriptografi su povećali sigurnost Enigme dodavši dva nova rotora, tako da su dobili 60 mogućih rasporeda rotora. To je značilo deset puta više „Bombi“, što je za Biuro bio preskup podvig. Sljedećih mjeseci Nijemci su povećali broj kablova koji se koriste na ploči priključaka, sa 6 na 10, dva nova dodatka povećala su broj mogućih ključeva na 159 000 000 000 000 000 000. Poljski kriptoanalitičari to nisu mogli pratiti. Rejewski je dokazao da Enigma nije neprobojna, ali bez sredstava potrebnih za otkrivanje dnevnog ključa dešifriranje nije moguće. Schmidt je prestao davati informacije poljskim saveznicima, Francuzima, te je za Langera uz nadolazeći rat i protupoljsku propagandu u Njemačkoj značilo da svoju tajnu moraju podijeliti sa saveznicima. Langer je 24. srpnja 1939. ugostio francuske i britanske kriptoanalitičare te im pokazao i podijelio rad Rejewskoga. Dva tjedna kasnije jedna od replika je poslana prema Londonu. Već 1. rujna Hitler je napao Poljsku i rat je započeo.

Slika 3: Marian Rejewski

3.2 Britanski utjecaj

Poljaci su dokazali da šifriranje Enigmom nije savršeno, te su pokazali Saveznicima koliko vrijede matematičari kao kriptoanalitičari. Britanski šifrirni ured „Room 40“ do početka Drugog svjetskog rata uglavnom je zapošljavao lingviste no sada su htjeli pojačati svoje snage sa matematičarima i znanstvenicima. Novi pripravnici su odlazili u netom osnovanu šifrirnu organizaciju „Government Code and Cypher School“ (skraćeno:GCCS) koja je polako preuzimala zadatke „Room 40“. Početkom rata GCCS su smjestili u Bletchley Park u Buckinghamshireu te je imala dvjestotinjak osoba u osoblju, a do kraja rata broj je narastao na oko 7 000.

Tijekom jeseni 1939. znanstvenici i matematičari u GCCS naučili su koristiti poljsku tehniku dešifriranja Enigminih poruka. Britanci su imali ono što je Poljacima nedostajalo, osoblje i sredstva, te su mogli podnijeti da se broj kombinacija enigminih ključeva povećao 10 puta. Nakon što su savladali Poljske tehnike, kriptoanalitičari iz Bletchleya počeli su koristiti svoje prečace u traženju ključa. Za primjer, oslanjali su se na činjenicu da su njemački operatori odabirali očite ključeve za nove poruke. Ključ koji bi trebali odabrati nasumično, njemački operatori bi često odabirali slova sa tipkovnice koja s u u nizu (npr. ASD ili JKL) ili bi često koristili isti ključ. Te predvidljive ključeve zvali su „ciliji“ i njih su prve provjeravali. Kako se Enigma tijekom rata razvijala, kriptoanalitičari su bili prisiljeni tražiti nove strategije u dešifriranju. Unatoč njemačkim izmjenama na Enigmi, Britanci su uspijevali u dešifriranju zbog dobre kombinacije osoblja među kojima su bili matematičari, znanstvenici, lingvisti, šahovski velemajstori i ljubitelji zagonetki. Između njih jednu osobu trebamo izdvojiti. Alan Turing pronašao je najveću Enigminu slabost i iskoristio je. Već početkom rata Turing je napustio svoje mjesto na sveučilištu Cambridge i pridružio se GCCS.

Nijemci su kod odabira novog ključa ponavljali svoj odabir (npr. pri odabiru KGH, operator bi šifrirao KGHKGH), Turing se pitao što će biti kada neprijatelj shvati da je upravo to jedna od slabosti njihovog šifriranja. Kada dođe do toga kriptoanalitičari iz Bletchley više neće moći koristiti Rejewskove tehnike, te se iz tog razloga Turing posvetio da pronađe alternativne načine probijanja Enigme.

Kako je vrijeme prolazilo, GCCS je u Bletchleyu izgradio ogromnu knjižnicu dekriptiranih poruka. Turing je proučavao stare dekriptirane poruke i uvidio da mnoge imaju strogu strukuru, te je vjerovao da može predvidjeti sadržaj šifriranih poruka ovisno o tome tko i kada ih je slao. Pa je tako za primjer, svako jutro poslije 6 sati njemačka vojska radiovezom slala vremensku prognozu koja je sadržavala riječ „wetter“ (vrijeme na njemačkom jeziku). Takvi vojni protokoli su vodili k tome da će poruke imati sličnu strukturu, pa je Turing bio siguran gdje se nalazi riječ wetter u šifriranom tekstu. Za primjer, prvih šest slova šifriranog teksta označavale su riječ wetter. Kada bi Turing povezao dio otvorenog teksta ša šifriranim, tu povezanost bi zvao „crib“ (engl. značenje za "kolijevka", u smislu "izvorište"). Dokazao je da cribovi ograničavaju postavke Enigme. Odnosno, došao je do toga da je preko cribova mogao otkriti ključ za poruke, a preko njega i dnevni ključ. No i dalje je bilo potrebno provjeriti veliki broj ključeva pa je tako dizajnirao svoj uređaj koji je to olakšavao, te ga po Rejewskovom izumu nazvao bombe. Do kraja 1941. godine petnaest bombi je bilo u funkciji te ako bi sve išlo kako treba u sat vremena bi otkrili ključ. Iako su bombe bile napredak u

dešifriranju, mnoge stvari su morale biti ispravne. Npr. kako bi bombe mogle raditi potrebno je zadati crib. Iskusniji kriptoanalitičari su otkrivali cribove ali nije bilo garancije da su ga točno odredili. Moguće je bilo i da ga točno odrede ali na krivom mjestu. Za prepoznavanje je li crib postavljen na dobro mjesto koristili su se zgodnom činjenicom. Enigma zbog svoje konstrukcije, točnije reflektora, nije bila u mogućnosti šifrirati slovo u isto. Dakle slovo A nikad nije moglo biti šifrirano u A, B u B i tako dalje.
Navedimo primjer kada je kriptoanalitičar siguran u otvoreni tekst, ali nije siguran odgovara li točnim slovima u šifratu.

Otvoreni tekst			W	E	T	T	E	R	N	U	L	L	S	E	C	H	S	
Šifrirani tekst	I	P	R	E	N	L	W	K	M	J	J	S	X	C	P	L	E	J	W

Konkretan primjer pokazuje poklapanje slova E u otvorenom i šifriranom tekstu, iz čega proizlazi da otvoreni tekst ne stoji na pravilnim pozicijama. Kako bi pronašli točne pozicije slova jednostavno se otvoreni tekst pomiče te provjerava da nijedan par na istim pozicijama nisu ista slova. Pa bi u ukoliko konkretan primjer pomaknemo ulijevo dobili poklapanje u slovu S. Ako ga pak pomaknemo u desno za jednu poziciju imamo sljedeće:

Otvoreni tekst				W	E	T	T	E	R	N	U	L	L	S	E	C	H	S
Šifrirani tekst	I	P	R	E	N	L	W	K	M	J	J	S	X	C	P	L	E	J	W

Sada ne postoji poklapanje te je ovaj crib spreman za obradu u bombama. Bombe bi nakon toga u sat vremena otkrile koji se ključ za tu poruku koristio, te bi nakon otkrivanja toga ključa došli do ključa koji je dodijeljen taj dan. I šifrirane poruke u tom danu su mogle biti dešifrirane. Čitav projekt probijanja Enigme bio je dio obavještajne operacije kodnog imena Ultra. Projekt Ultra je također dešifrirao talijanske i japanske poruke, te je Saveznicima uvelike pomogao u bitkama na sjeveru Afrike, čitavom Sredozemlju te i pri iskrcavanju na Siciliju 1943. Nekoliko mjeseci prije Dana D dešifriranje u Bletchley dalo je informacije gdje se njemačke trupe nalaze na francuskoj obali.

Bilo je bitno da Nijemci ne posumnjaju u Enigmine slabosti, pa tako Britanci često nisu otkrivali sve informacije koje su saznali iz Bletchleya. Jednom prilikom dešifriranjem Enigminih poruka saznali su lokaciju 9 njemačkih opskbnih brodova, ali su odlučili potopiti 7 od njih obavijestivši. Razarači su potopili njih sedam, te su dva odlučili poštedjeti. No, dva britanska razarača slučajno su presrela pošteđene brodove te su i njih potopili. Razarači nisu bili svjesni Enigme, niti politike tajenja mogućnosti dešifriranja Enigme. U Berlinu je to podiglo sumnju te su napravili istragu koja dovela do zaključka da se radilo o nesretnom slučaju ili o britanskom špijunu koji se infiltrirao u njemačku mornaricu. Probijanje Enigme smatrali su nemogućim i nezamislivim.

Britanci su i nakon rata nastavili čuvati tajnu probijanja Enigme. Kako su tijekom cijelog rata uspješno dešifrirali poruke neprijatelja željeli su i dalje održavati svoju obavještajnu operaciju. Pa su tako zarobivši nakon rata više tisuća Enigmi, podijelili ih među svojim bivšim kolonijama koje su smatrale da Enigmina šifra nema slabosti te su ih koristili u svojoj komunikaciji. Naravno, Britanci su redovito dešifrirali njihovu tajnu komunikaciju.

Naposljetku, tisuće ljudi koji su doprinijeli uspjehu kriptoanalize tijekom Drugog svjetskog rata nisu dobili priznanje za svoj doprinos. Većina kriptoanalitičara iz Bletchleya vratila se svome civilnom životu, čuvajući tajnu i ne otkrivajući ništa o svojoj velikoj ulozi u Savezničkoj pobjedi. Nakon 30 godina rada u tajnosti, kada se 70-ih godina godina prošlog stoljeća Enigma prestala koristiti je otkrivena i tajna o njenom probijanju, te su kriptoanalitičari napokon mogli dobiti priznanje koje zaslužuju.

Sam Alan Turing nije to doživio. Umjesto da je nakon rata slavljen kao heroj jer je pronašao slabost u njemačkom šifrirnom uređaju, bio je progonjen zbog svoje homoseksualnosti. Dok je prijavljivao provalu 1952. slučajno je otkrio svoju osobnu tajnu te je zbog toga optužen za veliku nepristojnost. Mediji su ga javno osramotili te je njegova seksualnost bila javna stvar. Britanci su mu oduzeli sigurnosne dozvole te je bio maknut sa istraživačkih projekata vezanih uz razvoj računala. Bio je prisiljen posjećivati psihijatra i primati hormonsku terapiju koja ga je odvela u depresiju. Nakon dvije godine agonije 7. lipnja 1954. godine otrovao se pojevši jabuku natopljenu cijanidom.

Alan Turing je postavio temeljne odredbe rada modernih računala. Smatra se ocem teoretske računalne znanosti i umjetne inteligencije. Radio je i u drugim znanstvenim poljima pa je tako jednom prilikom njegov kolega kriptoanalitičar Peter Hilton rekao: „Alan Turin je očito bio genij, ali bio je pristupačan prijateljski genij. Uvijek je bio spreman odvojit vrijeme kako bi objasnio svoje ideje. Ali nije bio uski specijalist, tako da su njegove svestrane misli bile u velikom rasponu područja egzaktnih znanosti.“

Slika 4: Alan Turing

Literatura

[1] A. Dujella, M. Maretić; Kriptografija; Element; Zagreb, 2007.

[2] I. Matić; Uvod u teoriju brojeva; Sveučilište Josipa Jurja Strossmayera u Osijeku - Odjel za matematiku; Osijek, 2015.

[3] S. Singh; The Code Book: how to make it, brake it, hack it, crack it; Delacorte Press; New york, 2002.