Kriptografija u Prvom i Drugom svjetskom ratu

Čavajda, Andrea

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

Andrea Čavajda

Kriptografija u Prvom i Drugom svjetskom ratu

Završni rad

Osijek, 2017.

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

Andrea Čavajda

Kriptografija u Prvom i Drugom svjetskom ratu

Završni rad

Voditelj: izv.prof.dr.sc. Ivan Matić

Osijek, 2017.

Sažetak

U ovome radu, obrazložiti ćemo ulogu kriptografije i kriptoanalize tijekom Prvog i Drugog Svjetskog rata. Najveći dio rada odnosi se na Zimmermanov telegram i njemački šifrirni stroj Enigmu.

Ključne riječi:

kriptografija, kriptoanaliza, Prvi svjetski rat, Drugi svjetski rat, Zimmermannov telegram, Enigma, Marian Rejewski, Alan Turing

Abstract

In this paper, we will explain the role cryptography and cryptanalysis played in World War I. and World War II. Most of the thesis refers to Zimmermann telegram and German chiper machine Enigma.

Key words:

cryptography, cryptoanalysis, World War I., World War II., Zimmermann telegram, Enigma, Marian Rejewski, Alan Turing

Sadržaj

1 Uvod

Kriptografija je znanstvena disciplina, usko povezana s matematikom, koja se bavi proučavanjem i pronalaženjem metoda za slanje informacija u obliku u kojemu ih samo onaj kome su namijenjene može pročitati. Sama riječ kriptografija je grčkog podrijetla i mogla bi se doslovno prevesti kao *tajnopis*.
Pretpostavimo da dvije osobe žele uspostaviti sigurnu komunikaciju. Poruka koju će pošiljatelj poslati naziva se *otvoreni tekst*. Pomoću *ključa* koji predstavlja pravilo po kojem se formira šifra, pošiljatelj poruku transformira u šifrirani tekst, odnosno *šifrat*. Otvoreni tekst i šifrat sastoje se od elemenata određenih, ne nužno jednakih, skupova simbola (alfabeta). Tako šifrirana poruka se zatim šalje primatelju, koji nakon dešifriranja dobije sadržaj otvorenog teksta.
Ljudi su od davnina imali potrebu komunicirati na siguran način, ali su istovremeno bili svjesni da njihove poruke često prolaze nepovjerljivim komunikacijskim kanalima. Kroz stoljeća, kriptografija se razvijala i koristila kao sredstvo u zaštiti informacija, naročito u vojne i diplomatske svrhe.
U povijesti kriptografije razlikujemo dva velika razdoblja. Današnje razdoblje nazivamo modernom kriptografijom, dok razdoblje do pojave interneta nazivamo klasičnom kriptografijom. Upravo je klasična kriptografija imala jednu od odlučujućih uloga u ishodima brojnih ratova sve do polovice prošlog stoljeća. Opasnost od razotkrivanja tajni i sudbonosnih planova potaknula je razvoj šifri i kodova. Povijest šifri temelji se na stoljetnoj borbi između tvoraca šifri i njihovih dešifranata. Stoga se razvoj kriptografije odvijao paralelno s razvojem *kriptoanalize*, znanosti koja se bavi dešifriranjem šifrata i kodova.
Prvi svjetski rat donio je niz uspjeha dešifrantima, ponajviše dešifriranje Zimmermanovog telegrama. Nakon Prvog svjetskog rata, kriptografi su ulagali velik napor u pronalaženje novih, sigurnih enkripcijskih sustava. Odlučili su papirnate šifre i olovke zamijeniti tehnologijom, konstruirajući naprave za šifriranje. Takve naprave činile su proces šifriranja i dešifriranja puno bržim i znatno sigurnijim (zbog velikog broja ključeva). Najpoznatiji kriptografski stroj svakako je bila Enigma. Do njene masovne uporabe došlo je neposredno prije i za vrijeme Drugog svjetskog rata u Njemačkoj. Zbog velikog broja različitih ključeva koje je stroj generirao, vjerovalo se da je nepobjediv, te je tako predstavljao najsigurniji kriptografski sustav na svijetu. Razbijanje Enigme uvelike je utjecalo na tijek i ishod Drugog svjetskog rata, te tako i na povijest općenito.

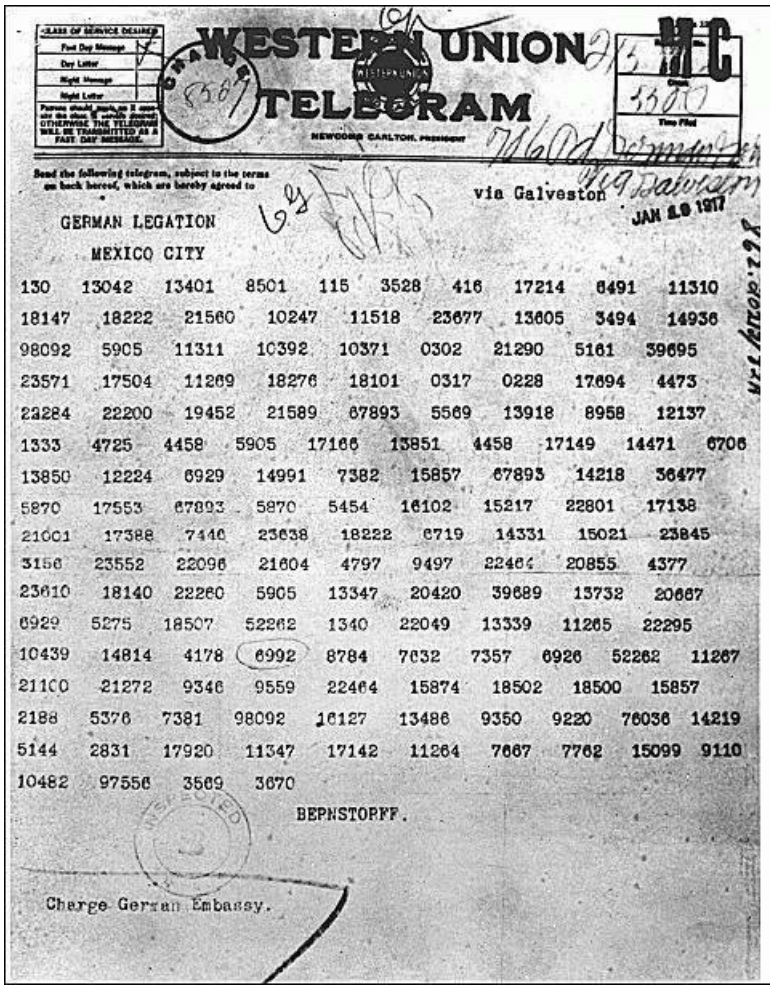
2 Prvi svjetski rat

Od 1914. godine do proljeća 1917. godine europske zemlje sudjelovale su u sukobu koji je postao poznat kao Prvi svjetski rat. Rat se odvijao na teritoriju Europe, a neutralne Sjedinjene Američke države zajedno s predsjednikom Thomasom Woodrowom Wilsonom nisu imale namjeru uplitati se u sukob. To je odgovaralo građanima Amerike, zbog čega je 1917. Wilson dobio drugi mandat pod sloganom *"On nas drži podalje od rata"*. Međutim, jedan izuzetno značajan događaj promijeniti će stav cijele zemlje prema ratu, a osobito prema Njemačkoj. To je objavljivanje onoga, što je postalo poznato kao Zimmermannov telegram, nazvanog prema autoru, njemačkom ministru vanjskih poslova Arthuru Zimmermannu.

2.1 Zimmermannov telegram

Arthur Zimmermann u telegramu predlaže Meksiku savezništvo u slučaju da Sjedinjene Američke Države uđu u rat. Predlaže Meksiku da ukoliko do toga dođe, uspostavi rat sa SAD-om kako bi povratio ranije izgubljeni teritorij, te time ograniči broj američkih vojnika na europskoj fronti. Zahvaljujući britanskim dešifrantima, taj plan je ubrzo razotkriven, a Amerika je proglasila rat. U neznanju, Nijemci su vjerovali kako je riječ o svojevrsnoj izdaji, te kako su kodovi kojima je telegram bio šrifriran ostali povjerljivi. No, pogriješili su, dešifriranje Zimmermannovog telegrama bilo je najveće kriptološko postignuće Prvog svjetkog rata.

Zimmermanov telegram kodiran je pomoću šifrata "0075", dvodijelnog koda od 10 000 riječi i fraza s brojevima od 0000 do 9999. Brojevi su nasumično odabirani, kako bi se izbjegle analize frekvencija, te dodatno individualno kodirani jednostavnom supstitucijom. Šifrat je siguran sve dok knjiga kodova ostane tajna. Stariji kod "13040", već je ranije bio dešifriran od strane britanskih dešifranata, no kod "0075" se smatrao pouzdanim. Međutim, Nijemci su podcijenili britanske dešifrante. Telegram su na putu za Washington presreli Britanci, a dešifrirali su ga u *"Sobi 40"*, uredu za šifriranje, u kojem je radila nekolicina sposobnih kriptoanalaitičara.



WESTERN UNION

TELEGRAM

NEWCOMB CARLTON, PRESIDENT

Send the following telegram, subject to the terms on back hereof, which are hereby agreed to

via Galveston

JAN 19 1917

GERMAN LEGATION

MEXICO CITY

130 13042 13401 8501 115 3528 416 17214 6491 11310
18147 18222 21560 10247 11518 23677 13605 3494 14936
98092 5905 11311 10392 10371 0302 21290 5161 39695
23571 17504 11269 18276 18101 0317 0228 17694 4473
23284 22200 19452 21589 67893 5569 13918 8958 12137
1333 4725 4458 5905 17166 13851 4458 17149 14471 6706
13850 12224 6929 14991 7382 15857 67893 14218 36477
5870 17553 67893 5870 5454 16102 15217 22801 17138
21001 17388 7446 23638 18222 6719 14331 15021 23845
3156 23552 22096 21604 4797 9497 22464 20855 4377
23610 18140 22260 5905 13347 20420 39689 13732 20667
6929 5275 18507 52262 1340 22049 13339 11265 22295
10439 14814 4178 6992 8784 7632 7357 6926 52262 11267
21100 21272 9346 9559 22464 15874 18502 18500 15857
2188 5376 7381 98092 16127 13486 9350 9220 76036 14219
5144 2831 17920 11347 17142 11264 7667 7762 15099 9110
10482 97556 3569 3670

BEPNSTORFF.

Charge German Embassy.

Slika 1: Zimmermanov telegram

Britanci su imali priliku dešifriranu poruku prenijeti SAD-u, no time bi SAD otkrio njihovo prisluškivanje kabela i presretanje poruka. Istodobno, Nijemci bi saznali da je njihov novi "pouzdani" kod "0075" razotkriven. Stoga su Britanci odlučili prenijeti SAD-u da je telegram dobiven podmićivanjem zaposlenika telegrafske tvrtke u Meksiku (telegram je poslan iz Njemačke ambasade u Washington, pa zatim u Meskiko). Štoviše, telegram koji je poslan u Meksiko bio je kodiran pomoću starog koda "13040", tako da u najgorem slučaju, Nijemci pomisle da je stari kod "13040" dešifriran. Tako je dešifriranje telegrama postignuto u Sobi 40, navevši SAD u rat, promijenilo tijek Prvog svjetskog rata, a time i povijesti.

3 Drugi svjetski rat

Nakon Prvog svjetskog rata velik napor se ulagao u pronalaženje novih, sigurnijih sustava za enkripciju. Kako bi poboljšali pouzdanost sustava, kriptografi se oslanjaju na tehnologiju, a svoju pozornost usredotočuju na mehanizaciju tajnosti. Konstruiraju prve naprave za šifriranje.

3.1 Albertijev disk

Iako primitivan, najraniji kriptografski stroj imao je veliku ulogu u konstrukciji složenijih naprava, a datira još iz 15. stoljeća. Bio je to šifrirajući disk, danas poznat kao *Albertijev disk*, a izumio ga je Leo Alberti. Disk se sastojao od dva bakrena kruga. Jedan je bio veći zvao se *statični*, a drugi je bio manji i nazivao se *pomični*. Promjer statičnog kruga bio je veći od pomičnog kruga. Prednju stranu diskova Alberti je podijelio u 24 jednaka dijela, koje je nazvao poljima. U polja na velikom krugu upisao je slova abecede u pravilnom poretku, s time da je izostavio slova H, K i Y jer je smatrao da nisu bila potrebna za razumijevanje poruka. Tako je iskoristio 20 polja (latinska abeceda nije sadržavala slova J, U i W). U preostala četiri polja upisao je brojeve od 1 do 4. Dvadeset i četiri polja malog kruga ispunio je malim slovima abecede, ali ne u pravilnom poretku nego nasumično. Kada su sva slova ispisana na oba kruga, manji se postavi na veći i kroz sredinu se umetne igla, koja služi kao os oko koje se manji krug može rotirati.

Slika 2: Albertijev disk

Sugovornici moraju imati identične diskove, a prije komuniciranja trebaju dogovoriti *indeksno slovo* u pomičnom krugu. Pošiljatelj poruke određuje poziciju unutarnjeg kruga, tj. s kojim će slovom velikog kruga upariti indeksno slovo. O toj odluci pošiljatelj obavještava primatelja na početku šifrata. Sada svako slovo pomičnog kruga ima odgovarajuće slovo u statičnom krugu. Veliki krug sadrži slova koja predstavljaju otvoreni tekst, a mali krug šifrat.
Revolucionarnost njegovog diska došla je do izražaja u naputku da se nakon tri, četiri riječi promijeni pozicija indeksnog slova. Prilikom promjene pozicije, pošiljatelj prije novog šifriranja u šifrat ubaci slovo koje sad predstavlja indeks na vanjskom krugu. Svaka nova postavka Albertijevog diska donosi novu abecedu za šifriranje (alfabet). Postoji onoliko različitih vrsta abeceda, koliko ima pozicija diska.

3.2 Enigma

Petsto godina nakon Albertijevog izuma šifrirajućeg diska, on dobiva električnu verziju. Ta kompleksnija verzija diska, dovest će do nove generacije šifrirnih naprava, teže odgonetivih nego ijednih dotada.
1918. godine njemački izumitelj Arthur Scherbius i njegov prijatelj Richard Ritter osnovali su strojarsku tvrtku Scherbius & Ritter. Glavna Scherbiusova ideja bila je zamijeniti kriptografski sustav, koji se koristio u Prvom svjetskom ratu, novim, sigurnijim sustavom enkripcije koji bi koristio tehnologiju dvadesetog stoljeća. Svoj izum Scherbius je nazvao *Enigma*. U Njemačkoj, Enigma je predstavljala glavno sredstvo za šifriranje i dešifriranje poruka. Tijekom godina pojavljivale su se različite verzije Enigme, a ovdje ćemo spomenuti standardni model.

3.2.1 Konstrukcija i princip rada Enigme

Standardni model Enigme sastojao se od sljedećih dijelova spojenih električnim vodovima:

- *tipkovnice*
- *premetačke jedinice*
- *reflektora*
- *prespojne ploče*
- *ploče sa žaruljicama*

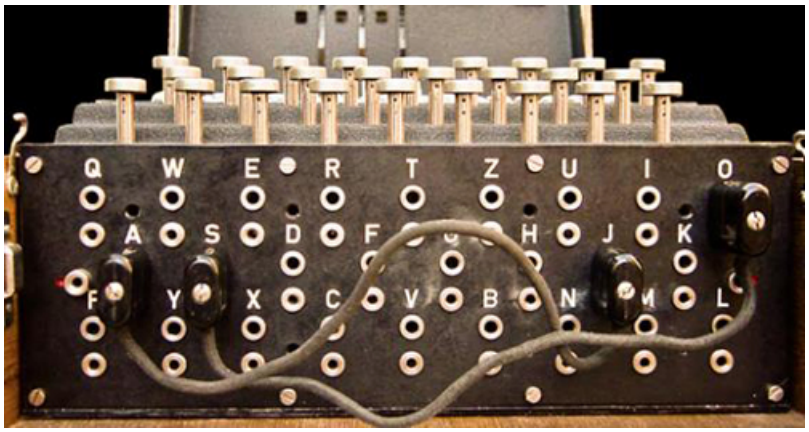
Slika 3: Standardni model Enigme

Premetačka jedinica koju čini *rotor* (premetalo ili scrambler) predstavlja najvažniji dio stroja. Rotor je debeli disk isprepleten žicama koje određuju kako će se slova otvorenog teksta enkriptirati. Prvotna ideja je bila da se disk rotora automatski zakrene za dvadesetšestinu poslije enkripcije svakog slova. Šifrirna se abeceda poslije svake enkripcije mijenja, a zahvaljujući toj rotaciji, rotor stvara dvadeset i šest šifrirnih abeceda. Dakle, stroj omogućava pisanje polialfabetskom šifrom. No, stroj u takvom obliku ima jednu veliku slabost. Naime, utipkamo li isto slovo dvadeset i šest puta, premetalo će se vratiti u početni položaj. Neprestanim upisivanjem istog slova stalno se ponavlja i obrazac enkripcije. Dodavanjem dodatnog rotora stroju, obrazac će se ponoviti tek nakon $26 \cdot 26$ puta, odnosno 676 puta. Drugi rotor će se pomaknuti za jedno mjesto tek nakon što je prvi rotor napravio puni krug. Enigma se sastojala od tri rotora i time je mogla zauzeti $26 \cdot 26 \cdot 26 = 17\,576$ položaja.

Slika 4: Tri spojena rotora

Kada bi protivnik mogao isprobati samo jednu kombinaciju u minuti, trebalo bi mu svega dva tjedna da pronađe ispravne postavke rotora. Sigurnost se mogla povećati dodavanjem novih rotora, no time bi se istodobno povećavale i veličina i težina samog uređaja. Umjesto toga, Scherbius je odlučio povećati sigurnost povećanjem broja mogućih početnih postavki na dva načina: izmjenjivim rotorima i prespojnom pločom. Budući da su rotori mehanički gotovo identični, a njihovi električni spojni putevi nužno različiti, njihovom jednostavnom zamjenom mijenja se i način šifriranja samog stroja. Broj mogućih permutacija triju rotora je 3!, tj. broj početnih postavki množi se faktorom 6.

Znatno veći doprinos sigurnosti šifre donosi prespojna ploča. Ona mijenja električne puteve između tipkovnice i prvog rotora, omogućujući inicijalnu zamjenu slova prije samog procesa šifriranja. Na primjer, moguće je zamijeniti slova “B” i “F” tako da se pritiskanjem tipke “B” odašilje slovo “F” i obratno. Operater je imao šest kablova. Dakle, šest parova slova moglo je zamijeniti mjesta, a ostalih četrnaest slova ostalo je na istom položaju.

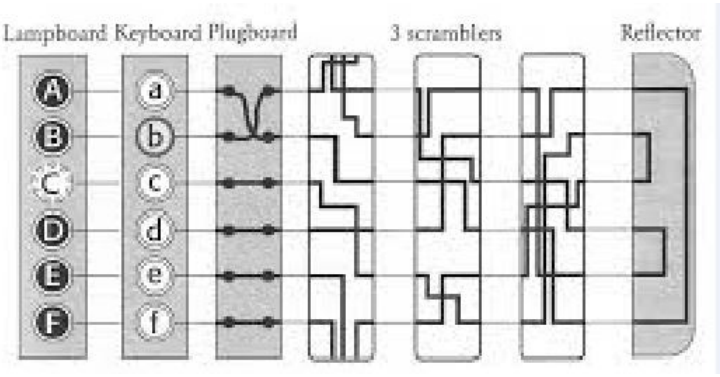


Slika 5: Prespojna ploča

Dakle, položaj rotora određuje 17 576 različitih ključeva, zatim tri rotora mogu se ispremetati na 6 različitih načina, te 6 parova slova od njih ukupno 26 mogu se prespojiti na prespojnoj ploči na ukupno 100 391 791 500 različitih načina. Množeći dobivene brojeve dobivamo ukupan broj ključeva:

$$17576 \cdot 6 \cdot 100391791500 = 10\ 000\ 000\ 000\ 000\ 000.$$

S obzirom da prespojna ploča najviše doprinosi broju ključeva, logično je pitati se zašto je stroj uopće sadržavao rotore. Naime, sama prespojna ploča, premetajući parove slova, proizvodila bi jednostavan šifrat, lako odgonetiv analizama frekvencije. Iako rotori sami po sebi imaju manji doprinos broju ključeva, s obzirom da se njihov položaj kontinuirano mijenja, nastali šifrat ne može se odgonetnuti takvim analizama. Kombinirajući rotore i prespojnu ploču, Scherbius je zaštitio svoj izum od dešifriranja analizama frekvencija, istovremeno stvarajući ogroman broj mogućih ključeva.
Osim, navedenih sastavnih jedinica, Enigma je sadržavala i reflektor - statičan mehanički disk sličan rotoru, s međusobno prespojenim električnim kontaktima samo na jednoj strani. Izlaz trećeg rotora povezan je na reflektor. Njegova je zadaća da električni signal šalje natrag kroz rotore, no drugim putem.
Kad operater pritisne tipku, električni signal putuje do ulaznog kontakta prvog rotora. S obzirom da interno ožičenje rotora predstavlja transformaciju slova, električni signal na izlazu kroz sva tri rotora predstavlja neko drugo slovo, a postupak se nastavlja kroz reflektor, ali drugim putem, te ponovno kroz sva tri rotora do odgovarajuće žaruljice.



Slika 6: Princip rada Enigme

Na prvi pogled, reflektor se čini kao besmislen dodatak. Zbog svoje statične prirode on ne pridodaje broju ključeva. No, prednost reflektora uočljiva je prilikom enkriptiranja i dekriptiranja poruke.

Recimo da želimo šifrirati neku poruku. Prije no što bismo započeli s unošenjem otvorenog teksta, potrebno je rotore okrenuti u unaprijed dogovoren položaj koji predstavlja ključ šifre. Šifre su bile zapisane u knjigama šifri dostupnim samo onima koji su sudjelovali u komunikaciji. Svaka četiri tjedna, distribuirala se nova knjiga s ključevima za naredna četiri tjedna. Knjiga je sadržava ključeve za svaki dan. Osoba zadužena za enkripciju bi prvo slovo upisala u stroj, zatim bi pogledala koje je slovo osvijetljeno na ploči sa žaruljicama, te bi zapisala tako enkriptirano slovo. Rotori se tada automatski zakreću i osoba nastavlja s enkripcijom. Enkriptirani tekst bi se zatim predao radiooperateru koji bi ga poslao primatelju. Primatelj također mora rotore postaviti na isti način, odnosno po istom ključu. On zatim upisuje šifrirani tekst, a na ploči sa žaruljicama dobiva otvoreni tekst. Upravo za to je zaslužan reflektor. Dokle god je stroj u istom položaju, on će dekriptirati šifrirano slovo i time će ono postati slovo otvorenog tekst.

3.3 Razbijanje Enigme

Nakon Prvog svjetskog rata, britanski kriptoanalitičari nastavili su s praćenjem njemačkih komunikacija. No, 1926. godine presretali su poruke koje nisu znali dešifrirati. Pojavila se Enigma.
Osim Engleske, velik interes u razbijanju Engime imala je i Poljska. Unatoč tome što je nakon Prvog svjetskog rata proglasila neovisnost, Poljska je bila na stalnom oprezu zbog prijetnji upućivanih od strane susjednih zemalja, Njemačke i Rusije. Tako je osnovan šifrirni ured Biuro Szyfrow. Zadužen za dešifriranje njemačkih poruka bio je kapetan Maksimilijan Ciezki, odan domoljub rođen u centru poljskog nacionalizma, Szamotuliyu. No, s obzirom da nije posjedovao Enigmu niti je znao kako stroj funkcionira, dešifriranje mu nije polazilo za rukom.
Prvi korak ka razbijanju Enigme napravo je Nijemac Hans-Thilo Schmidt. Njegov brat Rudolph bio je načelnik stožera Službe veza i osobno je odobrio primjenu Enigme u vojnoj službi. On je Hansa zaposlio u Enigminom komandnom centru u Berlinu. Frustriran što nije uspio služiti u njemačkoj vojsci kao brat, te siromaštvom, Hans je odlučio surađivati s francuskim tajnim agentom. Na njihovom sastanku, dopustio mu je da fotografira dokumente na kojima su bile upute za uporabu Enigme, zaradivši tako 10 000 tadašnjih maraka.
Iako su uspjeli stvoriti kopiju Enigme, Saveznici nisu uspjeli dešifrirati poruke bez ključeva. Francuzi su smatrali da je nemoguće pronaći ključeve te su odustali od rekonstuiranja stroja, a dobivene dokumente proslijedili su Poljacima, s kojima su ranije potpisali sporazum o vojnoj suradnji. Osim uputa u kojima je bilo objašnjeno u koji položaj postaviti rotore, kako postaviti spojeve na prespojnoj ploči, te redoslijed i orijentacija rotora, dokumenti su sadržavali i detaljan opis izgleda knjige kodova.

Slika 7: Knjiga ključeva korištena tjekom Drugog svjetskog rata "Sondermaschinen Schlussel" ("Special Machines Key")

Svaki mjesec operateri su dobivali knjigu s ključevima u kojoj su pisali ključevi za svaki dan. Obzirom da se jedan ključ koristio čitav dan, a velika količina poruka slana svakodnevno, postupak dešifriranja je bivao lakši. Zbog toga su Nijemci slali novi ključ u svakoj poslanoj poruci. Pri tome, promijenili bi samo orijentaciju rotora, dok bi ostale postavke ostale nepromijene. Novi ključ nije bio zapisan u knjizi ključeva, pa su ga pošiljatelji slali sljedećom procedurom:

- pošiljatelj bi prvo postavio stroj prema dogovorenom ključu iz knjige, npr. neka QNS predstavlja orijentaciju rotora
- zatim bi nasumično odabrao novu orijentaciju rotora npr. KDF, te enkriptirao KDF prema prvotno postavljenom položaju (ključ bi se dvaput utipkao kako bi primatelj mogao biti siguran da je točno dešifrirao) npr. pošiljatelj enkriptira ključ KDFKDF kao LKQUSP (primijetimo da šifrirajući dvaput KDF dobijemo prvo LKQ, pa USP, to je rezultat zakretanja rotora nakon svakog unešenog slova)
- pošiljatelj zatim postavi stroj po novom ključu KDF, te po njemu šifrira cijelu poruku
- primatelj prvotno postavi stroj po zadanom ključu za taj dan QNS
- prvih 6 slova dolazne poruke, LKQUSP dešifriraju se i otkriju novi ključ KDFKDF
- primatelj tada postavi stroj po novom ključu, te potom dešifrira cijelu poruku.

To je učinilo Enigmu znatno sigurnijom, te time otežalo proces dešifriranja. No, to nije sprječavalo Poljake u nakani da razbiju Enigmu. Biuro je organizirao kriptografski kurs na koji je pozvao dvadeset matematičara. Među njima najviše se istaknuo Marian Rejewski.

3.3.1 Marian Rejewski

Strategija Mariana Rejewskog temeljila se na ponavljanjima. Najočitije ponavljanje kod šifriranja Enigmom bio je novi ključ, šifriran dvaput na početku svake poruke. Ako bi operater odabrao ključ VHD, šifrirao bi ga dvaput, pa bi primjerice VHDVHD bilo šifrirano kao NZWQDS, te u tom obliku poslano na početku poruke. Nijemci su to ponavljanje zahtjevali radi sigurnosti i provjere, no nisu

razmišljali da bi upravo to moglo predstavljati veliku slabost. Primjerice, neka su četiri dobivene šifrirane poruke započinjale sljedećim ključevima:

1. poruka: L O K R G M
2. poruka: M V T X Z E
3. poruka: J K T M P E
4. poruka: D V Y P Z X

U svakoj poruci prvo i četvrto slovo su enkripcije istog slova, zatim drugo i peto, te treće i šesto. Slova su drugačije enkriptirana jer se između enkripcije pojedinog slova rotor svaki put zakrene. Primjerice u prvoj poruci se prvo slovo prvo enkriptiralo u J, a zatim u T. Rejewski je zaključio kako su slova J i T povezana početnom postavom Enigme, tj. dnevnim ključem za taj dan. Odnose između slova prikazivao je tablicom za svaku novo dobivenu poruku. Tako bi primjerice tablica za prijašnje navedene četiri poruke izgledala ovako:

$$\begin{array}{c} ABCDEFGHIJKLMNOPQRSTUVWXYZ \\ \quad P \qquad\qquad M \quad RX \end{array}$$

Kada bi uhvatili barem 26 poruke tijekom jednog cijelog dana, tablica bi se cijela mogla popuniti.

$$\begin{array}{c} ABCDEFGHIJKLMNOPQRSTUVWXYZ \\ FQHPLWOGBMVRXUYCZITNJEASDK \end{array}$$

Rejewski je na temelju tablica i povezanosti između pojedinih slova započeo s konstruiranjem lanaca. Npr. u tablici slovo A je povezano slovom F, a slovo F slovom W, koje je zatim povezano slovom A, gdje smo i započeli. Dobili smo jedan lanac. Isto bismo potom mogli napravili i s preostalim slovima abecede:

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

Osim veza između prvog i četvrtog slova, Rejewski je zapisivao i one između drugog i petog, te trećeg i šestog slova. Kako se ključ mijenjao svaki dan, tako su se mijenjali i lanci. No, broj veza u lancima ovisio je isključivo o rotorima. Prespojna ploča nije imala nikakav utjecaj na taj broj. Primjerice ako bi prespojnom pločom zamijenili slovo S za slovo G, lanci bi se promijenili na sljedeći način:

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

Dakle, iako smo na prespojnoj ploči zamijenili neke parove slova, broj veza ostao je isti. To znači da je Rejewski morao promatrati samo one ključeve koje su generirali rotori. Iako je taj broj i dalje bio velik (iznosio je 105 456), bio je znatno manji od početnih 10 000 000 000 000 000 koje su rotori generirali zajedno s prespojnom pločom. Rejewski je nastojao odrediti jednu od 105 456 mogućih konfiguracija rotora na temelju broja veza u nekom skupu lanaca.

Zahvaljujući Hans-Thilou Schmidtu, Rejewski je posjedovao repliku Enigme. On i njegov tim započeli su provjeravati svaku od 105 456 konfiguracija, te zapisivati dužinu lanaca koje svaka od njih generira. Za taj pothvat trebala im je cijela godina. Preostalo je još odrediti spojeve na prespojnoj ploči. Nakon što bi iz kataloga i pomoću lanaca utvrdio položaj rotora, izvadio bi sve kablove iz prespojne ploče. Time ploča gubi ulogu i nema više nikakav utjecaj u stroju. Kada bi unosili šifrirani tekst u stroj, ponekad bi dobivali neke jedva prepoznatljive fraze, npr. "*Syizeubenrli*", što bi vjerojatno predstavljalo "*Stiže u Berlin*". Time bi otkrili način kako spojiti kablove na prespojnoj ploči. Tako bi Rejewski dolazio do potpunog ključa za taj dan i prilike da dešifrira sve poruke uhvaćene tijekom tog dana.

Otkrićem Rejewskog, razbijena je Enigma. Poljska je imala pristup njemačkim komunikacijama nekoliko godina, sve dok Nijemci nisu promijenili način slanja poruka. Rejewski je mehanizirao verziju svog kataloga, što je omogućavalo automatsku pretragu svih konfiguracija rotora. Rotori su se mogli poredati na šest načina, pa je šest *Rejewskih strojeva*, predstavljajući svaki od poredaka, radilo usporedno. Ta jedinica nazvana je "*bomba*". Bila je visoka otprilike jedan metar, a dnevni ključ mogla je pronaći za otprilike dva sata.

Slika 8: Replika "bombe" Mariana Rejewskog

Tijekom tridesetih godina, Rejewski i njegov tim mjesecima su mukotrpno otkrivali ključeve, neznajući da ih načelnik Biuro-a, Gwido Langer redovito dobiva u šifrantskim knjigama proslijeđenim od ranije spomenutog Hans Schmidta. Hans Schmidt nastavio je redovito isporučivati tajne dokumente, a uz njih i knjige kodova. Iako je bio u mogućnosti uskratiti Rejewskog mukotrpnog posla, Langer je zadržavao knjige za sebe jer je smatrao da će doći do trenutka kada ih više neće imati na raspolaganju.
Njemačka je u prosincu 1938., uvevši dva dodatna rotora, povećala sigurnost Enigme. Od pet rotora na raspolaganju, tri su se stavljala u poredak. Tako je broj poredaka rotora sa šest povećan na šezdeset.
Sljedećeg mjeseca, broj kablova na prespojnoj ploči povećan je sa šest na deset, povećavajući broj mogućih ključeva na 159 000 000 000 000 000 000. Dešifriranje je time postalo nemoguće, a Langer je prestao dobivati knjige s ključevima. Kako svi poljski napori pri razbijanju Enigme nebi bili uzaludni, načelnik Langer dotadašnja saznanja odlučio je podijeliti sa Saveznicima.

Tijekom Hitlerovog Blitzkriega Enigma je predstavljala glavno sredstvo sigurne i efikasne komunikacije. Krajem srpnja 1939. godine u Biuro su stigli najbolji britanski i francuski kriptoanalitičari. Isto tako, dvije replike Enigme poslane su u London i Pariz. Dva tjedna nakon toga, točnije 1. rujna 1939. Hitler je napadom na Poljsku započeo Drugi svjetski rat.

3.3.2 Alan Turing

Iako, unatoč poljskim naporima, nije u potpunosti razbijena, Enigma dešifrantima više nije predstavljala potpuno nemoguć pothvat. Osim toga, zahvaljujući Poljacima, Saveznici su uočili važnost zapošljavanja matematičara na pozicije koje su dotad zauzimali lingvisti. U Velikoj Britaniji prethodno poznato sjedište "Soba 40" premješteno je u Buckinghamshire, točnije u Bletchley Park. Bletchley Park mogao je primiti puno više osoblja, što je bilo iznimno važno s obzirom na očekivani broj presretanih poruka početkom rata. Prvotno, Bletchley Park je zapošljavao samo dvije stotine ljudi. Taj broj se tijekom narednih pet godina povećao na čak sedam tisuća.

Slika 9: Bletchley Park

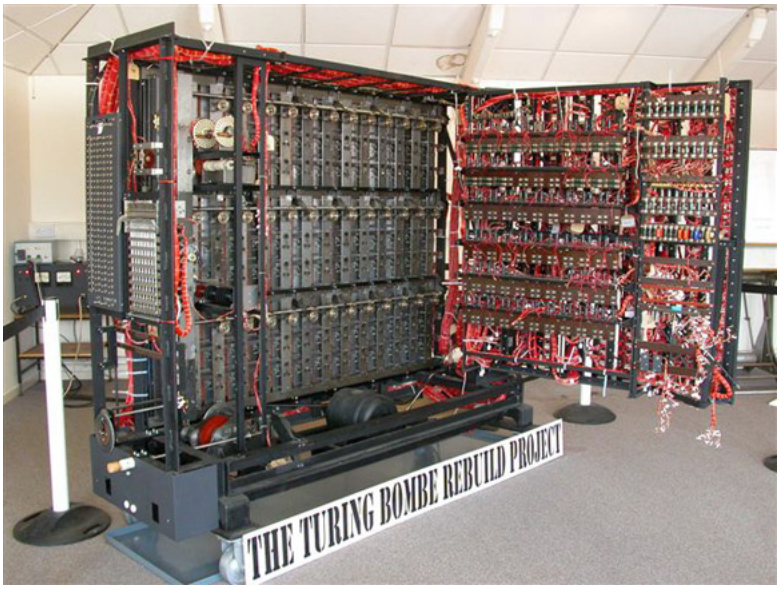
Tijekom jeseni 1939. godine, znanstvenici i matematičari u Bletchleyu svladali su zamršenosti Enigme i usavršili poljske tehnike dešifriranja. S obzirom na broj osoblja, u usporedbi s poljskim Biuro-om, Britanci su bili u stanju savladati sve veću kompliciranost Enigme, a time i sve veći broj naknadno dodanih rotora. Svakih 24 sata, dešifranti su prolazili istu rutinu. U ponoć, njemački bi operatori izmijenili dnevni ključ. To bi za dešifrante značilo, da sve što je postignuto tijekom tog dana, više nema nikakvu ulogu. Svakog dana dešifranti bi, u vremenu od nekoliko sati, uspjevali identificirati novi ključ. Tek tada, bili bi u stanju dešifrirati poruke. Te poruke su često bile od neizmjerne važnosti za tijek rata. Pravovremeno dešifriranje je, stoga, Saveznicima predstavljalo glavno oružje u ratu.

Kako je kompliciranost Enigme neprestano napredovala tijekom rata, tako su i kriptoanalitičari bili kontinuirano prisiljeni mijenjati strategije i usavršavati svoje konstrukcije za dešifriranje. Najistaknutiji među njima bio je matematičar Alan Turing. Upravo je on identificirao i razotkrio najveću slabost Enigme. Zahvaljujući njemu, Enigma je, iako uz dotad najteže moguće okolnosti, bila razbijena.

Slika 10: Alan Turing

Početkom rata, Turing je napustio svoju dužnost na sveučilištu Cambridge i pridružio se kriptoanalitičarima u Bletchley Parku. Fokusirao se na ono što bi se dogodilo kada bi njemačka vojska promijenila način razmijenjivanja dnevnog ključa. Dotadašnji uspjeh postignut u Bletchleyu oslanjao se na prijašnja dostignuća Rejewskog obzirom na šifriranje dnevnog ključa dvaput na početku svake poruke. Turingova dužnost bila je pronaći način razbijanja Enigme, ne oslanjajući se na šifriranje dnevnog ključa.
Proučavanjem dešifriranih poruka, Turing uočava kako većina njih ima strogo određenu strukturu. Smatrao je da na osnovu činjenice kada je i odakle je poruka poslana, može predvidjeti dijelove šifrirane poruke. Primjerice, promatrajući prijašnje poruke, lako je uočljivo da Nijemci svakog dana oko 6 sati ujutro šalju vremensku prognozu. Presretnuta poruka u 6:05 ujutro bi stoga, vrlo vjerojatno sadržavala riječ “wetter” (vrijeme).

Također, s obzirom na prijašnje poruke zaključio je da se ta riječ većinom nalazi na početku, tj. prvih šest slova šifriranog teksta većinom predstavljaju riječ "wetter". Kada dio običnog teksta možemo povezati s nekim dijelom šifriranog teksta, tu kombinaciju nazivamo "kućište" (engl. crib). Turing je pokazao da te kombinacije postavljaju određena ograničenja na početne postavke stroja. Dakle, one usmjeravaju na dnevni ključ, no i dalje je bilo potrebno provjeriti tisuće postavki rotora kako bi pronašli odgovarajuću. Turing je dizajnirao stroj nazvan "Bomba", čiji je zadatak bio upravo taj, pronaći odgovarajuću postavku rotora.



Slika 11: Replika stroja"The Bombe"Alana Turinga

Kako je sav posao u Bletchley Parku bio strogo povjerljiva tajna, nitko izvan njega nije bio svjestan Turingova izvanredna postignuća. Krajem 1941. godine petnaest Turingovih "bombi" bilo je u funkciji, a do kraja rata čak i nekoliko stotina njih. Za samo sat vremena stroj je bio u stanju pronaći odgovarajući ključ. No, nije se sve odvijalo sasvim jednostavno. Primjerice, za upravljanje bombom potrebna je kombinacija (kućište). Dešifranti bi kombinaciju proslijedili operaterima bombe, no ipak, ne sasvim sigurni u točnost predviđenog običnog teksta. Također, ako je kombinacija točna, ne znači da je pozicija teksta u odnosu na šifrat točno pretpostavljena. Jedan jednostavan trik, omogućavao je provjeru pozicije predviđenog teksta unutar šifrata.

Recimo da smo u sljedećoj kombinaciji sigurni da je predviđen tekst "wetternullsechs" točan, no nismo sigurni da li je on dobro pozicioniran s obzirom na šifrat.

$$w\ e\ t\ t\ e\ r\ n\ u\ l\ l\ s\ e\ c\ h\ s$$
$$I P R E N L W K M J J S X C P L E J W Q$$

Naime, jedna karakteristika Enigme onemogućuje nam da šifriramo slovo u isto to slovo. Dakle, Enigmom ne možemo šifrirati slovo A u slovo A, niti slovo B u slovo B, itd. To je posljedica reflektora. Prethodno navedena kombinacija, je stoga krivo pozicionirana. Slovo e u riječi "wetter" pridruženo je slovu E u ispod navedenom šifratu. Pomicanjem predviđenog teksta "wetternullsechs", sve dok nijedno slovo ne bude pridruženo samom sebi, dolazimo do ispravne pozicije predviđenog teksta obzirom na šifrat.

$$w\ e\ t\ t\ \ e\ \ r\ n\ u\ l\ \ l\ \ s\ e\ c\ h\ s$$
$$I P R E N L W K M J J S X C P L E J W Q$$

Dešifriranje njemačkog stroja Enigme bio je dio tajne obavještajne operacije poznate pod imenom "Ultra". Ultra je bila izvor izvještaja o stanju i lokaciji protivnika na čitavom Sredozemlju. Zahvaljujući tim informacijama, Saveznici su mogli uspješno isplanirati mnoge bitke i invazije.
Postignuća iz Bletchley Parka odigrala su ključnu u ulogu u Drugom svjetskom ratu, a vjeruje se kako su baš ona donijela pobjedu Saveznicima. Neosporivo je zasigurno da je, zahvaljujući kriptoanalitičarima iz Bletchley Parka, značajno skraćen rat. Poruke koje su savezničke snage uspjele presresti dovele su ih do velikih pobjeda. Ipak, vojska nije uvijek mogla iskoristiti sve primljene informacije. Kada bi savezničke snage bile uspješne na svakom koraku, te neprestano izbjegavale napade, njemačka bi vojska vjerojatno postala sumnjičava. Takvim potezima, Nijemci bi promijenili svoj kriptosustav, a Saveznici bi opet bili na početku. Saveznici su, stoga, iskorištavali samo dio informacija u svoju korist. Vjeruje se da je rat, zahvaljujući naporima savezničkih kriptografa, skraćen za čak dvije godine.

Tek početkom sedamdesetih godina, nakon što se Enigmina šifra prestala upotrebljavati, Britanci su otkrili da su ju razbili. Nažalost, Alan Turing nije doživio svoje priznanje. Prije rata, Turing se, objavljivanjem djela o osnovama rada računala, pokazao matematičkim genijem. Nakon rata, umjesto priznanja za svoj rad, 1952. godine optužen je zbog homoseksualnosti, koja je u Velikoj Britaniji do 1980. godine bila zabranjena. Isto tako, zabranjen mu je i rad na istraživanjima koja su se bavila razvojem računala. Bio je prisiljen na hormonsku terapiju, a počinio je samoubojstvo u 42. godini života.

Literatura

[1] John H. Lienhard, The Engines of Our Ingenuity, OUP USA, 2003.

[2] David P. Mowry, German Cipher Machines of World War 2, National Security Agency, 2014.

[3] Simon Singh, The Code Book, Delacorte Press, New York, 2001.

[4] https://www.awesomestories.com/asset/view/ENIGMA-CODE-BOOKS-at-STATION-X-The-Imitation-Game

[5] http://www.historyofinformation.com/expanded.php?id=3604

[6] http://www.cryptomuseum.com/