Kriptografija u Drugom svjetskom ratu

Mršić, Doris

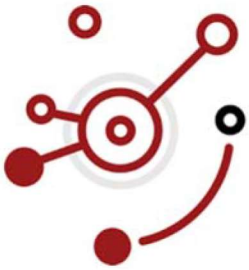
Master's thesis / Diplomski rad

2019

Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj: **Josip Juraj Strossmayer University of Osijek, Department of Physics / Sveučilište Josipa Jurja Strossmayera u Osijeku, Odjel za fiziku**

Permanent link / Trajna poveznica: https://urn.nsk.hr/urn:nbn:hr:160:777681

SVEUČILIŠTE JOSIPA JURJA STROSSMAYERA U OSIJEKU
ODJEL ZA FIZIKU



DORIS MRŠIĆ

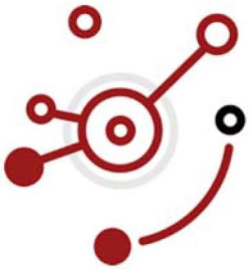
KRIPTOGRAFIJA U DRUGOM SVJETSKOM RATU

Diplomski rad

Osijek, 2019.

SVEUČILIŠTE JOSIPA JURJA STROSSMAYERA U OSIJEKU

ODJEL ZA FIZIKU



DORIS MRŠIĆ

KRIPTOGRAFIJA U DRUGOM SVJETSKOM RATU

Diplomski rad

predložen Odjelu za fiziku Josipa Jurja Strossmayera u Osijeku u postupku stjecanja zvanja magistra edukacije fizike i informatike

Osijek, 2019.

Ovaj diplomski rad je izrađen u Osijeku pod mentorstvom prof. dr. sc. Darka Dukića u sklopu Sveučilišnog diplomskog studija Fizike i informatike na Odjelu za fiziku Sveučilišta Josipa Jurja Strossmayera u Osijeku.

ZAHVALA

...mojoj obitelji, bližnjima i prijateljima na motivaciji i razumijevanju…

...profesoru na trudu i zalaganju…

Sveučilište Josipa Jurja Strossmayera u Osijeku
Odjel za fiziku

Diplomski rad

KRIPTOGRAFIJA U DRUGOM SVJETSKOM RATU

Doris Mršić

Sažetak

Predmet izučavanja ovog diplomskog rada je kriptografija za vrijeme Drugog svjetskog rata. Nakon uvoda je ukratko prikazan razvoj kriptografije u starom, srednjem i novom vijeku. Zatim su opisani kriptografski uređaji Enigma, SIGABA i Purple, koji su se koristili tijekom Drugog svjetskog rata, kao i kod plemena Navajo. Naposljetku je sažeto prezentiran razvoj kriptografije u suvremenom dobu. Cilj je rada bio upoznati se s ulogom i značajem ovog važnog područja, poglavito u Drugom svjetskom ratu, u kojem su kriptografija i kriptoanaliza u velikoj mjeri odredile njegov konačan ishod.

Ključne riječi: kriptografija, kriptografski uređaji, Enigma, SIGABA, Purple

(50 stranice, 19 slika, 16 tablica, 45 literaturna navoda)

Rad je pohranjen u knjižnici Odjela za fiziku

Mentor: prof. dr. sc. Darko Dukić
Ocjenjivači: izv. prof. dr. sc. Igor Lukačević, izv. prof. dr. sc. Branko Vuković
Rad prihvaćen: 10. prosinca 2019.

Josip Juraj Strossmayer University in Osijek
Department of Physics

Master Thesis

CRYPTOGRAPHY DURING THE SECOND WORLD WAR

Doris Mršić

Abstract

The case study of this thesis is cryptography during the World War II. After the introduction, there is a short overview of the evolution of cryptography through the old, middle and the new ages. That is followed by the description of the encryption machines Enigma, SIGABA and Purple, all of which were used during the World War II, also as the code of Navajo tribe. Lastly, there is concise presentation of how cryptography has been developed in the modern times. The aim of this thesis was to explore the role and significance of this important area, especially during the World War II, in which cryptography and cryptanalysis, to a large degree, decided its outcome.

Keywords: cryptography, encryption machines, Enigma, SIGABA, Purple

(50 pages, 19 figures, 16 table, 45 references)

Thesis deposited in Department of Physics library.

Supervisor: Darko Dukić, PhD, Full Professor
Reviewers: Igor Lukačević, PhD, Associate Professor, Branko Vuković, PhD, Associate Professor
Thesis accepted: December 10, 2019

SADRŽAJ

1. UVOD

„Može se otvoreno tvrditi da ljudska dosjetljivost ne može smisliti šifru koju ljudska genijalnost ne može riješiti.“

Edgar Allan Poe[1]

Potreba za sigurnom komunikacijom stara je gotovo koliko i ljudska civilizacija. Već su se s nastankom pisma pojavili prvi pokušaji skrivanja sadržaja poruke ili njezinog šifriranja. Kroz povijest se šifriranje poruka odvijalo na različite načine, od metoda pisanja šifri i korištenja jednostavnih uređaja za šifriranje, do izuma različitih složenijih strojeva i upotrebe računala. Kako su informacije postajale sve važnije, tako je kodiranje i šifriranje poruka imalo sve veću ulogu u svakodnevnom životu. Grana matematičke teorije, vjerojatnosti i statistike koja istražuje sve procese povezane s prijenosom i obradom informacija naziva se teorija informacija.[2] Informacija, kao značenje koje se pridaje podacima, ima od samih početaka civilizacije ključnu ulogu u svim ljudskim postignućima.[3] Korijeni teorije informacije sežu u vrijeme izuma telegrafa i telefona, kada se javila potreba za poboljšanjem elektromehaničke komunikacije. Začetnikom moderne teorije informacije smatra se Claude Elwood Shannon, koji je 1948. godine u članku "Matematička teorija komunikacije" postavio model komunikacije temeljen na matematičkom pristupu.[4]

Teorija informacija ima široku primjenu, a jedno je od njih i kriptografija. Kriptografija je znanstvena disciplina koja se bavi metodama šifriranja i kodiranja poruka, s ciljem ostvarivanja sigurne komunikacije između pošiljatelja i primatelja, odnosno onemogućavanja razumijevanja sadržaja poruke onima kojima nije namijenjena.[5] Nasuprot kriptografije, kriptoanaliza izučava metode dekodiranja i dešifriranja poruka. Najznačajniju su ulogu kriptografija i kriptoanaliza odigrale u velikim međunarodnim sukobima. Bežična radio komunikacija koja se koristila tijekom Drugog svjetskog rata bila je od iznimne važnosti zbog usmjeravanja vojnih snaga i provođenja taktike napada i obrane. Radio poruke su se mogle presresti te su se zato informacije morale

[1] Cimino, A. (2017). *The story of codebreaking.* London: Arcturus Publishing Limited., str. 6.
[2] Alonso, A., Molenberghs, G. (2008). Evaluating time to cancer recurrence as a surrogate marker for survival from an information theory perspective. *Statistical Methods in Medical Research*, 17(5), 497-504.
[3] Dnoenosova, G. A. (2012). Document properties. *Scientific and Technical Information Processing*, 39(4), 220-228.
[4] Pandžić, I. S., Bažant, A., Ilić, Ž., Vrdoljak, Z., Kos, M., Sinković, V. (2007). *Uvod u teoriju informacije i kodiranje*. Zagreb: Element d.o.o., str. 4-6.
[5] Vesić, N. O., Simjanović, D. J. (2014). Matrix-based algorithm for text-data hiding and information processing. *Vojnotehnički glasnik*, 62(1), 42-57.

prenositi u tajnim šiframa i kodovima. Sve velike sile koristile su složene uređaje za šifriranje i dešifriranje poruka. Njemački se zvao Enigma, američki SIGABA, a japanski Purple. Ovo su samo neki od uređaja koji su u ratu korišteni s ciljem osiguranja sigurne komunikaciju. Dakle, rat se nije vodio samo na bojištu, nego i na polju efikasnog i sigurnog prijenosa informacija. Upravo će umijeće probijanja neprijateljskih šifri u velikoj mjeri pridonijeti pobjedi Saveznika u najrazornijem svjetskom ratu.

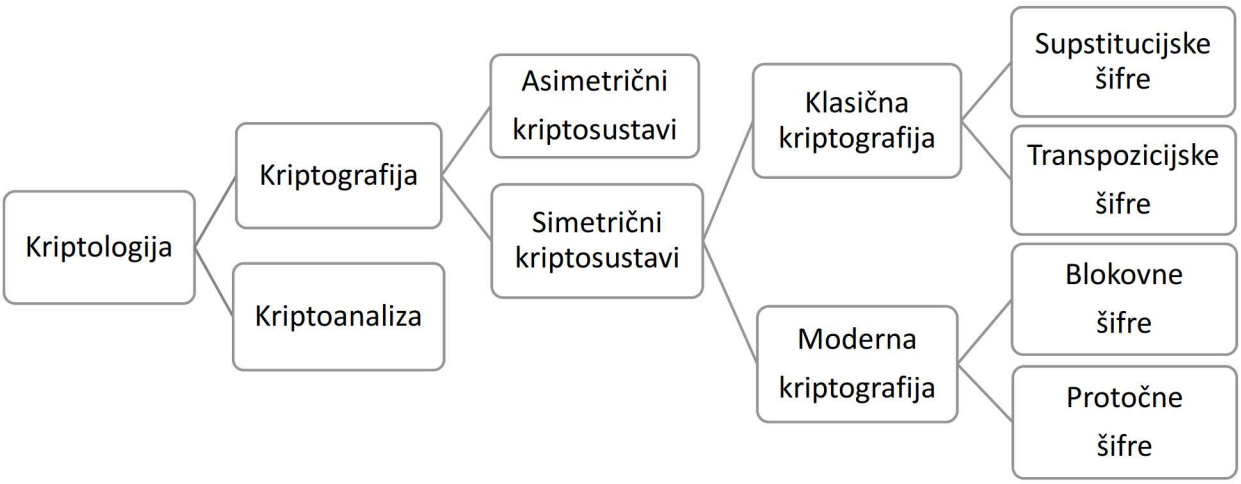
U ovom radu upoznat ćemo se s osnovama kriptografije i njezinim razvojem koji je podijeljen na razdoblje starog, srednjeg i novog vijeka, Drugog svjetskog rata te suvremenog doba. Detaljnije će biti prikazana uloga kriptografije i opisan princip rada strojeva za šifriranje poruka upotrebljavanih u Drugom svjetskom. Nekoliko riječi će biti posvećeno i kodu plemena Navajo, kao specifičnom obliku šifriranja kojeg su koristili Amerikanci. Također ćemo saznati nešto o suvremenoj kriptografiji i njezinoj širokoj upotrebi.

Što je kriptografija? Kada je nastala i kako se razvijala kroz povijest? Kakvu je ulogu kriptografija imala u Drugom svjetskom ratu? Koje je značenje kriptografije danas i zašto je bitna? Ovaj će rad nastojati pružiti odgovore na ova i druga pitanja vezana uz kriptografiju i kriptoanalizu.

2. OSNOVNI POJMOVI KRIPTOGRAFIJE

Kriptologija je grana znanosti koja se dijeli na kriptografiju i kriptoanalizu.[6] Kriptografija (grč. kryptó ~ skrivam, pokrivam + gráfo ~ pišem) je riječ grčkog podrijetla koju doslovno možemo prevesti kao tajnopis.[7] To je znanstvena disciplina kojoj je glavni zadatak preoblikovati poruku koja je svima razumljiva u sadržaj koji mogu shvatiti i otkriti samo oni kojima je poruka namijenjena. Za razliku od kriptografije, kriptoanaliza (grč. kryptó ~ skrivam, pokrivam + analýein ~ odrješavam) je znanstvena disciplina koja proučava tehnike i metode dekriptiranja poruke bez poznavanja ključa.[8]

Ovisno o odnosu ključeva razlikuju se simetrični i asimetrični kriptosustavi. Simetrični kriptosustavi su oni koji koriste samo jedan, tajni ključ za šifriranje i dešifriranje poruke. Sva kriptografija od vremena antike do druge polovine 20. stoljeća bila je temeljena na kriptografiji simetričnog ključa. Nasuprot tome, asimetrični kriptosustavi upotrebljavaju dva različita ključa. Naime, osim tajnog ključa za dešifriranje, koristi se i javni ključ za šifriranje poruke.[9]

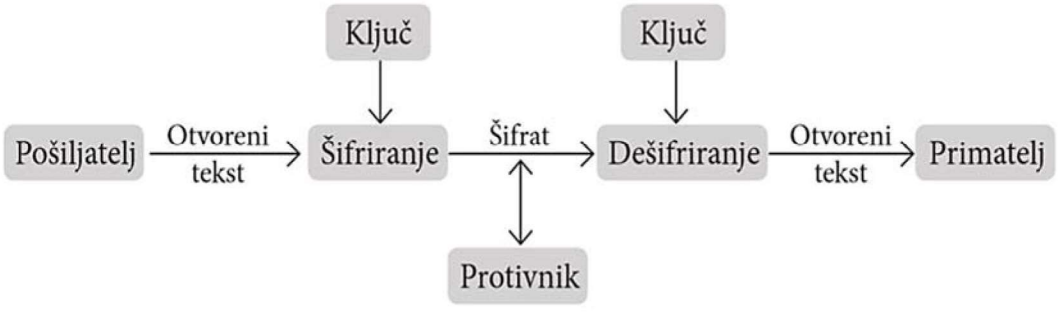


Slika 1. Podjela kriptologije[10]

[6] Zulkifli, M. Z. W. M. (2007). *Evolution of cryptography*. Dostupno na http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.698.2641&rep=rep1&type=pdf (pristupljeno 5.10.2019.)
[7] Klaić, B. (2001). Rječnik stranih riječi. Zagreb: Nakladni zavod Matice hrvatske., str. 761.
[8] Dujella, A., Maretić, M. (2007). *Kriptografija*. Zagreb: Element., str. 1.
[9] Paar, C., Pelzl, J. (2010). *Understanding cryptography: A textbook for students and practitioners*. Berlin: Springer., str. 3.
[10] Shashank (2019). *What is cryptography?*. Dostupno na https://www.edureka.co/blog/what-is-cryptography/ (pristupljeno 05.10.2019.)

Kako je i prikazano slikom 1, simetrična kriptografija se nadalje grana na klasičnu i modernu kriptografiju. Klasična kriptografija obuhvaća podjelu na supstitucijske i transpozicijske šifre, a moderna kriptografija na blokovne i protočne šifre.[11] Supstitucijske šifre su šifre u kojima se svaki element otvorenog teksta zamjenjuje s nekim drugim elementom, a transpozicijske one u kojima se elementi otvorenog teksta premještaju, odnosno permutiraju. S druge strane imamo blokovne šifre kod kojih se, kao što i sama riječ kaže, obrađuje jedan po jedan blok elementa otvorenog teksta koristeći jedan ključ, te protočne šifre kod kojih se elementi otvorenog teksta obrađuju jedan po jedan koristeći niz ključeva koji se generiraju.[12]

Nakon ove jednostavne podjele, možemo se osvrnuti na temeljne pojmove kriptografije koji su nužni za razumijevanje ovoga rada. Izvorna ili originalna poruka koja je čitljiva i jasna svima naziva se otvoreni tekst. Pošiljatelj nastoji sadržaj te poruke osigurati njezinim šifriranjem. To je postupak transformacije otvorenog teksta uz pomoć unaprijed dogovorenog ključa. Rezultat šifriranja je šifrirana poruka ili šifrat, koju pošiljatelj šalje primatelju. Uz pomoć postupka inverznog šifriranju, koji se naziva dešifriranje, primatelj dolazi do izvorne poruke. Onaj kome poruka nije namijenjena, ako je i presretne dok prolazi određenim komunikacijskim kanalom do primatelja, bez odgovarajućeg ključa ne može saznati njezin pravi sadržaj. Iz ovoga proizlazi da je ključ zapravo podatak na kojem je temeljen postupak šifriranja i dešifriranja, odnosno ključ se koristi za konfiguraciju kriptosustava. Kriptosustav je pojam koji obuhvaća sve moguće šifre, šifrate, ključeve i otvorene tekstove.[13]



Slika 2. Shema kriptografije[14]

[11] Paar, C., Pelzl, J. (2010). *Understanding cryptography: A textbook for students and practitioners*. Berlin: Springer, str. 3.
[12] Dujella, A., Maretić, M. (2007). *Kriptografija*. Zagreb: Element., str. 3.
[13] Igrec, A. (2016). Skrivene poruke. *Matka*, 24(96), 222-228.
[14] Igrec, A. (2016). Skrivene poruke. *Matka*, 24(96), 222-228.

Najčešće pogrešno korišteni pojmovi u kriptografiji su šifra i kod. Čak i stručnjaci povremeno koriste ove izraze kao sinonime. U prošlosti je ta razlika bila relativno nebitna, ali u suvremenim komunikacijama je važno napraviti distinkciju između ova dva pojma. I šifre i kodovi temelje se na supstituciji na razini slova, riječi ili fraze otvorenog teksta s nekim drugim objektom. Šifre su nerazumljivog sadržaja, a šifriranje i dešifriranje se obavlja u skladu s pravilom koje definira ključ. Suprotno tome, kod se šalje kao nešto razumljivo drugima, ali sadržaj nosi tajnu poruku. Za kodiranje i dekodiranje je isključivo potrebna knjiga s kodnim riječima i izrazima.[15]

Također je bitno naglasiti razliku između pojmova monoalfabetske i polialfabetske šifre. Monoalfabetske šifre su šifre u kojima svakom slovu otvorenog teksta odgovara jedinstveno slovo šifrata. Polialfabetske šifre za svako slovo otvorenog teksta imaju jedno od nekoliko mogućih slova alfabeta prema kojima se vrši sam postupak šifriranja.[16]

[15] Curley, R. (2013). *Cryptography: Cracking codes*. London: Britannica Educational Publishing., str. 2-3.
[16] Dujella, A., Maretić, M. (2007). *Kriptografija.* Zagreb: Element., str. 15.

3. KRATAK PRIKAZ RAZVOJA KRIPTOGRAFIJE DO DRUGOG SVJETSKOG RATA

3.1. STARI VIJEK

Najraniji primjeri kriptografije datiraju oko 2000. godine pr. Kr. u drevnom Egiptu. Tada su se slikovnim pismom hijeroglifima ukrašavale grobnice vladara kako bi se opisao njihov život i pridodala važnost njihovoj vladavini.[17] U zapisu dijela Biblije u 6. stoljeću pr. Kr. korištenjem jednostavne supstitucijske šifre zamjenjuju se znakovi hebrejskog alfabeta prvog sa zadnjim, drugog sa predzadnjim i tako redom. Ova metoda šifriranja je poznata pod nazivom *atabash*.[18] Elementi kriptografije su bili prisutni i u antičkoj Grčkoj i Rimu. Spartanci su u 5. stoljeću pr. Kr. koristili napravu za šifriranje zvanu *skital*. Ta naprava se sastojala od drvenog štapa oko kojeg bi se namotala pergamentna vrpca. Na vrpcu bi se okomito ispisala poruka, a njezinim odmotavanjem na njoj bi bio prikazan samo niz beznačajnih znakova. Primatelj bi pročitao poruku jedino upotrebom *skitala* jednakog promjera kao što je promjer skitala pošiljatelja. Kriptografskim rječnikom *skital* predstavlja uređaj za šifriranje i dešifriranje, a promjer *skitala* kriptografski ključ. Ovo je primjer transpozicijske metode šifriranja.[19]

Slika 3. Skital[20]

[17] Cimino, A. (2017). *The story of codebreaking.* London: Arcturus Publishing Limited., str. 12.
[18] Zulkifli, M. Z. W. M. (2007). *Evolution of cryptography*. Dostupno na http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.698.2641&rep=rep1&type=pdf (pristupljeno 05.10.2019.)
[19] Stamp, M., Low, R. M. (2007). *Applied cryptanalysis: Breaking ciphers in the real world.* Hoboken: John Wiley & Sons, Inc., str. 5.
[20] Cimino, A. (2017). *The story of codebreaking.* London: Arcturus Publishing Limited., str. 19.

Grčki povjesničar Polybius, koji je djelovao u 2. stoljeću pr. Kr., razvija svoju verziju monoalfabetske supstitucijske šifre koja će imati ogroman utjecaj slijedećih nekoliko tisućljeća. Njegova metoda je danas poznata pod nazivom *Polybiusov kvadrat*. On je slova alfabeta smjestio u tablicu dimenzija 5 x 5 gdje je na sjecištu svakog retka i stupca u tablici slovo bivalo zamijenjeno određenim parom brojeva.[21]

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I/J	K
3	L	M	N	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z

Tablica 1. Polybiusov kvadrat[22]

Gaj Julije Cezar, jedan on najvećih i najpoznatijih vladara Rima, razvija svoju, također monoalfabetsku supstitucijsku metodu šifriranja danas poznatiju pod nazivom *Cezarova šifra*. Metoda koristi rotaciju alfabeta na način da su se slova pošiljateljeve poruke zamjenjivala slovima koja su se nalazila tri mjesta dalje od njih u alfabetu. Danas se Cezarovom šifrom nazivaju i šifre istog oblika s različitim brojem pomaka.[23]

Otvoreni tekst:	A	L	E	A	I	A	C	T	A	E	S	T
Šifrat:	D	O	H	D	L	D	F	W	D	H	V	W

Tablica 2. Cezarova šifre za latinsku frazu *"Alea iacta est"*[24]

3.2. SREDNJI VIJEK

Stagnacijom pismenosti i učenosti u Europi tijekom srednjeg vijeka, kriptografija se pretvorila iz korisne tehnike za sigurnu komunikaciju u mračnu umjetnost koja graniči s magijom.

[21] Dooley, J. F. (2018). *History of cryptography and cryptanalysis: Codes, ciphers, and their algorithms*. Cham: Springer., str. 14-15.
[22] Dooley, J. F. (2018). *History of cryptography and cryptanalysis: Codes, ciphers, and their algorithms*. Cham: Springer., str. 14.
[23] Kahn, D. (1973). *The codebreakers.* New York: Macmillan Company., str. 73.
[24] Primjer riješen prema: Kahn, D. (1973). *The codebreakers.* New York: Macmillan Company., str. 73.

Najrelevantniji u ovom razdoblju za spomenuti je francuski redovnik i filozof Roger Bacon, prvi Europljanin koji tek u 13. stoljeću u svom djelu navodi i opisuje do tada poznate tehnike kriptografije.

Nasuprot Europi, kriptoanaliza u srednjem vijeku doživljava procvat u arapskom svijetu. Svestrani znanstvenik al–Kindi u svom djelu "Rukopis o dešifriranju kriptografskih poruka" opisao je metodu zvanu frekvencijska analiza. Metoda se zasniva na usporedbi učestalosti pojavljivanja slova alfabeta nekog jezika u šifriranom i otvorenom tekstu slične duljine. U Europi se metoda počela koristiti znatno kasnije, a prvi su je počeli upotrebljavati talijanski kriptografi.[25]

3.3. NOVI VIJEK

Razdoblje novog vijeka donosi povećan interes za upotrebu kodova i šifri, posebice u vojnim, diplomatskim i trgovačkim poslovima, ali i razvoj tehnologije pa tako i izum kriptografskih uređaja i strojeva. U ovom se razdoblju pojavljuju raznoliki izumi, od koji će u nastavku biti navedeni oni najvažniji i najistaknutiji. Sve do otkrića frekvencijske analize, stoljećima je upotreba jednostavne monoalfabetske supstitucijske šifre bila dovoljna za sigurnu komunikaciju. Svjesni njezine slabosti te opasnosti presretanja i lakog dešifriranja poruke, kriptografi su bili prisiljeni otkrivati nove metode.[26]

Leon Battista Alberti, jedna od utjecajnijih osoba renesanse, prvi predlaže upotrebu dvaju ili više šifriranih alfabeta i njihovo izmjenjivanje prilikom šifriranja. Prednost ovakvog načina je ta što se ista slova u otvorenom tekstu sada ne pojavljuju nužno kao ista slova u šifriranom tekstu. Ovo je bio začetak upotrebe polialfabetske supstitucijske šifre. Alberti je izumitelj i naprave za šifriranje, koja je u čast njemu nazvana *Albertijev disk*. Disk se sastojao od dviju ploča različitih polumjera položenih jedna na drugu i šiljka koji prolazi njihovim središtem. Svaka je ploča podijeljena na 24 jednaka dijela. Na gornjoj nepokretnoj ploči redom su ispisana slova latinskog alfabeta (bez slova j, u, w) i brojevi od 1 do 4, a na donjoj rotirajućoj ploči izmiješanim redoslijedom sva slova latinskog alfabeta te znak &. Gornja ploča je predstavljala otvoreni tekst, a donja šifrirani alfabet. Poruka se šifrirala tako što bi se dogovorno uzelo jedno slovo koje bi bilo indikator promijene.

[25] Dooley, J. F. (2018). *History of cryptography and cryptanalysis: Codes, ciphers, and their algorithms*. Cham: Springer., str. 15-17.
[26] Singh, S. (2001). *The code book.* New York: Delacorte Press., str. 51.

Ako zavrtimo donju ploču, njezinim zaustavljanjem dobivamo šifrirani alfabet. Ponovimo li postupak dobivamo drugi šifrirani alfabet i tako redom.[27] Isti uređaj s ponekim izmjenama tek pet stoljeća kasnije Amerikanci su upotrebljavali u Prvom svjetskom ratu.[28]

Slika 4. Albertijev disk[29]

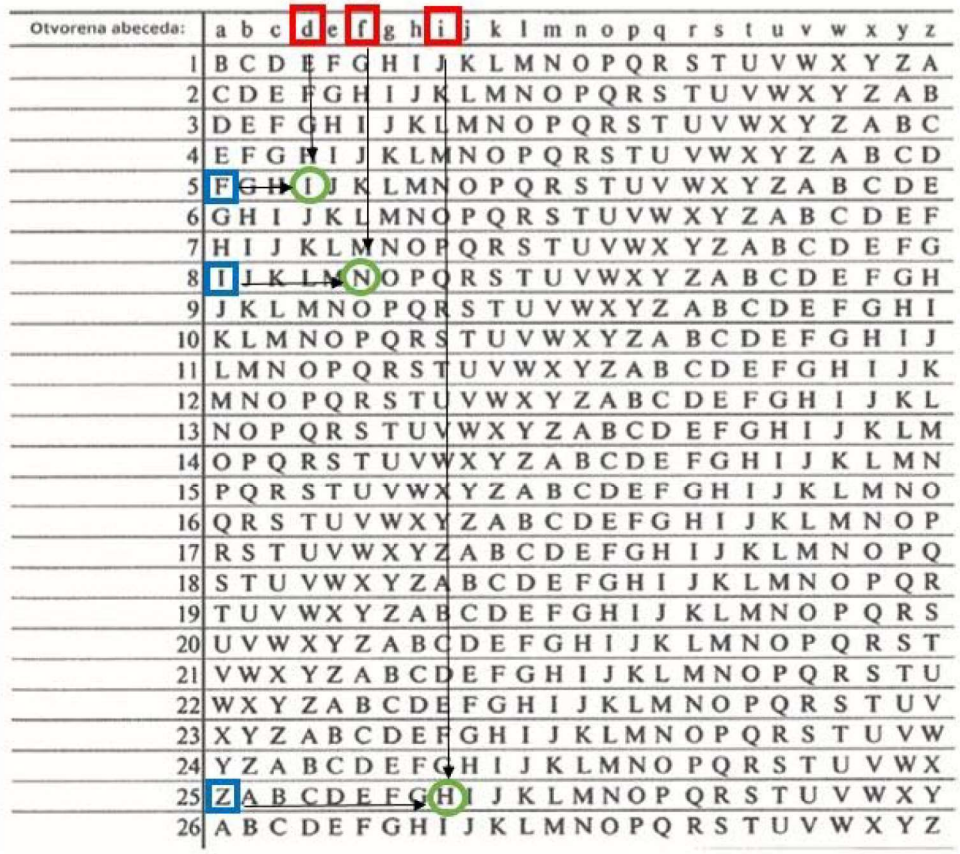
Johannes Trithemius u knjizi "Polygraphie", koja je objavljena 1518. godine, predlaže prvu polialfabetsku tablicu zvanu *tabula recta*, koja se sastojala od 26 šifriranih alfabeta. Svaki slijedeći alfabet je u odnosu na prethodni bio pomaknut za jedno slovo udesno. Poruku je ciklički šifrirao na način da je prvi šifrirani alfabet koristio za početno slovo, drugi šifrirani alfabet za drugo slovo i tako redom. Talijan Giovani Battista Belaso unaprijedio je tehniku šifriranja upotrebom stalnog ključa. Slovo ključne riječi koje je iznad slova otvorenog teksta određuje red u Trithemiusovoj tablici kojim šifriramo to slovo. Ovo bi bio primjer blokovne šifre.[30]

Blaise de Vigenère, najpoznatiji francuski kriptograf 16. stoljeće, u svojoj knjizi "Traicté des Chiffres", objavljenoj 1523. godine, opisao je sve što se do tada znalo o kriptografiji. Zaslužan je za razvoj metode šifriranja autoključem (otvoreni tekst generira ključ). Vigenère tu uvodi početni ključ isključivo za šifriranje prvog slova otvorenog teksta. Ostatak ključa predstavlja otvoreni tekst na način da drugo slovo otvorenog teksta koristi prvo slovo kao ključ za šifriranje i tako redom.

---

[27] Dooley, J. F. (2018). *History of cryptography and cryptanalysis: Codes, ciphers, and their algorithms*. Cham: Springer., str. 37-38.
[28] Curley, R. (2013). *Cryptography: Cracking codes*. London: Britannica Educational Publishing., str. 2-3.
[29] Cimino, A. (2017). *The story of codebreaking.* London: Arcturus Publishing Limited., str. 49.
[30] Dooley, J. F. (2018). *History of cryptography and cryptanalysis: Codes, ciphers, and their algorithms*. Cham: Springer., str. 38-39.

Ova metoda šifriranja pripada protočnim šiframa. Vigenèreovom šifrom naziva se i šifra s upotrebom stalnog ključa i takozvane *Vigenèreove tablice*, temeljene na prethodno opisanom postupku Battista Belasa. Vigenèreova šifra je jedan od najpopularnijih kriptosustava u povijesti, posebice korištena za vrijeme Američkog rata za neovisnost i tijekom Američkog građanskog rata.[31, 32]



POČETNI KLJUČ:	D					
OTVORENI TEKST:	F	I	Z	I	K	A
ŠIFRAT:	I	N	H	H	S	K

Tablica 3. Vigenerova tablica s riješenim primjerom[33]

Krajem 18. stoljeća Thomas Jefferson, kasniji američki predsjednik, osmislio je prijenosan uređaj, jednostavan za korištenje, nazvan *Jeffersonov kotač za šifriranje*. Uređaj se sastojao od 36 neovisnih, numeriranih, rotirajućih, drvenih diskova koji su se nalazili na metalnom kolcu koji je

[31] Dujella, A., Maretić, M. (2007). *Kriptografija.* Zagreb: Element., str. 16.
[32] Dooley, J. F. (2018). *History of cryptography and cryptanalysis: Codes, ciphers, and their algorithms*. Cham: Springer., str. 39-40.
[33] Dujella, A., Maretić, M. (2007). *Kriptografija.* Zagreb: Element., str. 15.

prolazio kroz njihova središta. Oko ruba svakog diska bio je uklesan mješoviti alfabet. Kako bi se šifrirala poruka potrebno je posložiti diskove određenim redoslijedom na kolac (ključ), a zatim ih rotirati dok se ne dobije niz od 36 slova otvorenog teksta u jednom od redova uređaja. Fiksiranjem diskova odabere se neki od preostalih redova i zapiše šifrat. Svoju primjenu uređaj je našao tek stotinjak godina kasnije, a na osnovu njegova principa rada patentirani su drugi mehanički uređaji.[34]

Slika 5. Rekonstrukcija Jeffersonovog kotača za šifriranje[35]

Izum telegrafa i radija te razbijanje "neprobojne" Vigenèreove šifre potaklo je razvoj složenijih kodova i šifri te dovelo do razvoja strojne kriptografije. Od brojnih metoda šifriranja otkrivenih u slijedećih stotinjak godina istaknut ćemo ADFGX šifru, koja je kombinacija transpozicije i supstitucije. To je jedna od najpoznatijih šifri korištena od strane Nijemaca tijekom Prvog svjetskog rata. U Morseovom kodu navedena slova imaju najmanje sličnosti te su, radi smanjenja grešaka u komunikaciji, ona i odabrana. Za šifriranje poruke koristi se izmijenjeni Polybiusov kvadrat dimenzija 5 x 5 unutar kojeg su upisana redom slova alfabeta nakon određene ključne riječi ili nasumično odabrana slova alfabeta bez ključne riječi.

Slova ADFGX se koriste kao zaglavlja stupca i retka kvadrata, kako je prikazano tablicom 4. Zatim se za svako slovo otvorenog teksta, očitavanjem iz tablice, odredi digraf. U tablici 5 navedena je kao primjer poruka "otkriveni smo spasite se" i pripadajući digrafi. Nakon toga se

[34] Dooley, J. F. (2018). *History of cryptography and cryptanalysis: Codes, ciphers, and their algorithms*. Cham: Springer., str. 60-61.
[35] Dooley, J. F. (2018). *History of cryptography and cryptanalysis: Codes, ciphers, and their algorithms*. Cham: Springer., str. 60.

digrafi ispisuju u drugu tablicu red po red, po jedno slovo po stupcu, uz unaprijed dogovorenu ključnu riječ, koja u primjeru glasi "sudbina". Naposljetku se tablica razvrsta abecednim redom po ključnoj riječi te se šifrirani tekst ispiše po stupcima.

	A	D	F	G	X
A	t	f	e	c	u
D	s	h	y	k	a
F	n	i	j	z	g
G	x	r	p	d	b
X	q	l	v / w	o	m

Tablica 4. ADFGX tablica s mješovitim alfabetom

o	t	k	r	i	v	e	n	i	s	m	o
XG	AA	DG	GD	FD	XF	AF	FA	FD	DA	XX	XG

s	p	a	s	i	t	e	s	e
DA	GF	DX	DA	FD	AA	AF	DA	AF

Tablica 5. Digraf otvorenog tekst

6	7	3	2	4	5	1
S	U	D	B	I	N	A
X	G	A	A	D	G	G
D	F	D	X	F	A	F
F	A	F	D	D	A	X
X	X	G	D	A	G	F
D	X	D	A	F	D	A
A	A	F	D	A	A	F

Tablica 6. Sortirani šifrirani tekst prema ključnoj riječi SUDBINA

Šifrat: GFXFA FAXDD ADADF GDFDF DAFAG AAGDA XDFXD AGFAX XA[36]

[36] Primjer riješen prema: Dooley, J. F. (2018). *History of cryptography and cryptanalysis: Codes, ciphers, and their algorithms*. Cham: Springer., str. 102-104.

Kako bi se omogućilo slanje brojeva, šifri je dodano slovo V te se naziva ADFGVX šifra. Sastoji se od matrice dimenzija 6 x 6 u kojoj su sada ispisana slova alfabeta te deset brojevnih znamenaka. Postupak šifriranja je isti. Kao i većinu šifri nastalih u tom razdoblju kriptoanalitičari su je uspjeli vrlo brzo dešifrirati.[37, 38]

Umjesto oslanjanja na šifre nastale upotrebom olovke i papira, kriptografi su se nakon otkrića rotora ubrzo usredotočili na mehanizaciju postupka šifriranja te se okrenuli tehnologijama koje su trebale osigurati značajno veću sigurnost. Unutar pet godina od završetka Prvog svjetskog rata četiri čovjeka u četiri različite zemlje neovisno jedan o drugome su razvili i patentirali uređaje s kojima se dobiva polialfabetski šifrat. Svi ti uređaji su bili elektromehanički i relativno mali, koristili su standardne tipkovnice i rotor, kao novi element, koji je automatski omogućavao strojevima promjenu alfabeta svaki put kad bi se unosila slova otvorenog teksta. Elektromehanički rotor je disk koji se obično proizvodi u dva dijela te koji s obje strane ima 26 električnih kontakata nasumično povezanih žicama. Električna struja koja prolazi kroz kontakt na jednoj strani rotora se tako pojavljuje na nekom od kontakta na drugoj strani rotora. Učinak rotora je stvoriti monoalfabetsku supstitucijsku šifru upotrebom mješovitog alfabeta. Što je veći broj rotora, to je postupak šifriranja složeniji, a proces dešifriranja poruke teži. Ubrzo nakon otkrića rotora uslijedili su izumi strojeva koji će obilježiti povijest kriptografije.[39]

[37] Newton, D. E. (1997). *Encyclopedia of cryptography.* Santa Barbara: Instructional Horizons., str. 6.
[38] Dooley, J. F. (2018). *History of cryptography and cryptanalysis: Codes, ciphers, and their algorithms*. Cham: Springer., str. 102-14.
[39] Dooley, J. F. (2018). *History of cryptography and cryptanalysis: Codes, ciphers, and their algorithms*. Cham: Springer., str. 138-139.

4. KRIPTOGRAFIJA I KRIPTOANALIZA U DRUGOM SVJETSKOM RATU

Drugi svjetski rat je razdoblje u ljudskoj povijesti koje je započelo 1. rujna 1939. napadom Nijemaca na Poljsku, a završilo 2. rujna 1945. kapitulacijom Japana. Kriptografiju je u tom razdoblju obilježila upotreba elektromehaničkih strojeva za šifriranje i dešifriranje poruka. Oni su u velikoj mjeri odredili ishod rata. Središnji dio rada upravo je posvećen opisu tri vjerojatno najpoznatija kriptografska stroja koja su se koristila tijekom Drugog svjetskog rata: Enigma, SIGABA i Purple. Naposljetku je prezentiran i kod plemena Navajo.

4.1. ENIGMA

Njemački inženjer elektrotehnike Arthur Scherbius je 1918. godine podnio zahtjev za patent, a 1920-ih je dizajnirao elektromehanički stroj za šifriranje i dešifriranje poruka, nalik na pisaći stroj, primarno namijenjen komercijalnoj upotrebi, pod nazivom Enigma. Uređaj je doživio više izmjena i poboljšanja. Sve njegove verzije sadržavale su rotore te su ih vezale određene zajedničke karakteristike. Najveću i najznačajniju upotrebu Enigma je imala kao glavni uređaj za prijenos informacija njemačke vojske tijekom Drugog svjetskog rata. Iako su Nijemci smatrali da je Enigma neprobojna, ipak su je uspjeli dešifrirati prvo poljski, a nakon njih i britanski kriptografi predvođeni Alanom Turingom te tako, prema statistikama, skratiti rat za nekoliko godina.[40]

4.1.1. Dijelovi i izgled

Enigma je elektromehanički uređaj izgledom i dimenzijama sličan pisaćem stroju. Smještena je u drvenu, prijenosnu kutiju sa čeličnim kućištem. Njezini glavni dijelovi su tipkovnica i ploča s žaruljama, baterija, statični rotor, brzi, središnji i spori rotor, reflektor i razvodna ploča.[41]

[40] Stamp, M., Low, R. M. (2007). *Applied cryptanalysis: Breaking ciphers in the real world.* Hoboken: John Wiley & Sons, Inc., str. 26.
[41] Oberzalek, M. (2000). *What is the Enigma cipher machine?* Dostupno na: http://www.mlb.co.jp/linux/science/genigma/enigma-referat/node3.html (pristupljeno 11.10.2019.)

Tipkovnica koja služi za unos otvorenog ili šifriranog teksta sadrži 26 tipki sa slovima latiničnog alfabeta, ali bez brojeva, interpunkcijskih i funkcijskih znakova. Pritiskom tipke kao izlazni rezultat zasvijetli jedna od 26 žarulja. Svaka žarulja predstavlja izlazno slovo. Raspored slova na tipkovnici i ploči s žaruljama je bio isti.[42]

Enigma nije imala mogućnost ispisa poruke. Stoga su za njezino slanje ili primanje bili potrebni operateri. Primjerice, prilikom slanja poruke jedan bi operater čitao otvoreni tekst, drugi bi unosio slova otvorenog teksta te izgovarao svako šifrirano slovo, dok bi treći operater zapisivao šifrirani tekst koji se tada prenosio Morseovim kodom.[43] Baterija je isključivo služila kao izvor strujnog kruga za osvjetljenje žarulja. Međutim, nije osiguravala snagu potrebnu za pokretanje rotora, jer su se oni pokretali mehanički.[44]

Ulazni rotor je nepomičan mehanički disk koji sadrži 26 električnih kontakata. On pruža povezanost između desnog rotirajućeg rotora te tipkovnice i ploče sa žaruljama. Ono što je iznenađujuće je činjenica da je povezanost s tipkovnicom bila u redoslijedu slova alfabeta, a ne slova na tipkovnici. Ovakav način nije pružao kriptografsku prednost te je samo zakompliciralo unutrašnje ožičenje sustava.[45]

Rotori, brzi, središnji i spori se biraju iz kutije u kojoj se nalazi 5 mehaničkih rotora, numerirani brojevima od 1 do 5. Kretanje rotora započinje pritiskom tipke na tipkovnici, a oni se rotiraju poput brojača kilometra. Opis mehanizma okretanja rotora će biti detaljnije objašnjen na narednim stranicama. Položaj kotača je vidljiv u prozorčićima te se ručno mogu postaviti u željeni početni položaj.[46] U unutrašnjosti rotora se nalazilo 26 isprepletenih, izoliranih žica od kojih je svaka bila spojena na 26 kontakata s obje strane rotora.[47] Postojalo je više verzija Enigme u ovisnosti o broju

---

[42] Klima, R. E., Sigmon, N. P. (2013). *Cryptology classical and modern with Maplets.* Boca Ration: CRC Press., str. 64.
[43] Dooley, J. F. (2018). *History of cryptography and cryptanalysis: Codes, ciphers, and their algorithms.* Cham: Springer., str. 152.
[44] Churchhouse, R. (2004). *Codes and ciphers: Julius Caesar, the Enigma and the internet.* Cambridge: Cambridge University Press., str. 112.
[45] Churchhouse, R. (2004). *Codes and ciphers: Julius Caesar, the Enigma and the internet.* Cambridge: Cambridge University Press., str. 113.
[46] Oberzalek, M. (2000). *What is the Enigma cipher machine?* Dostupno na: http://www.mlb.co.jp/linux/science/genigma/enigma-referat/node3.html (pristupljeno 11.10.2019.)
[47] Dooley, J. F. (2018). *History of cryptography and cryptanalysis: Codes, ciphers, and their algorithms*. Cham: Springer., str. 138-139.

rotora. Većina modela sadržavala je 3 rotora, dok su kasniji modeli sadržavali 4 rotora. Također verzije su se razlikovale i po broju rotora danih na odabir koji je varirao od 3 do 8 rotora.[48]

Reflektor je nepomičan mehanički disk sličan rotoru koji sadrži 26 kontakta samo s jedne, vanjske strane diska. Ti su kontakti povezani u parovima s 13 žica koje se nalaze unutar reflektora tako da struja koja ulazi u jednu od kontaktnih točaka izlazi u neku od drugih različitih izlaznih kontaktnih točaka. Glavna uloga je reflektirati električni signal i omogućiti povratak tog signala kroz rotore, ali različitim putem od prvotnog.[49]

Na prednjoj strani ispod tipkovnice stroja nalazi se razvodna ploča koju sadrži jedino vojna verzija Enigme. Ona se sastoji od 26 utora koje se mogu povezati pomoću 13 kratkih kabela. Razvodna ploča omogućavala je izmjenu parova slova na ulaznoj i izlaznoj razini Enigme.[50]

Slika 6. Enigma[51]

[48] Crypto Museum (2009). *Working principle of the Enigma.* Dostupno na: https://www.cryptomuseum.com/crypto/enigma/working.htm (pristupljeno 24.10.2019.)
[49] Dooley, J. F. (2018). *History of cryptography and cryptanalysis: Codes, ciphers, and their algorithms.* Cham: Springer., str. 142.
[50] Churchhouse, R. (2004). *Codes and ciphers: Julius Caesar, the Enigma and the internet.* Cambridge: Cambridge University Press., str. 121.
[51] Deutsches Museum (2019). *Enigma*. Dostupno na: https://www.deutsches-museum.de/sammlungen/meisterwerke/meisterwerke-ii/enigma/enigma-grossansicht2/ (pristupljeno 11.10.2019.)

4.1.2. Početne postavke

Unosom otvorenog teksta električna struja prolazi kroz elemente stroja te kao rezultat osvjetljena žarulja prikazuje slova šifriranog teksta. Svaki put kada bi se pritisnulo jedno slovo na tipkovnici, neki od 3 rotora bi promijenio svoj položaj, tako da kada bi se slijedeći puta unosilo to isto slovo ono bi bivalo drugačije šifrirano. Time je upotreba tradicionalnih metoda za dešifriranje poruka bila nemoguća. Prije same upotrebe uređaja korisnik je morao odabrati početne postavke koje su zapravo ključ za šifriranje i dešifriranje poruka. Različiti dijelovi stroja mogu se postaviti na različite načine. Nepoznavanjem početnih postavki stroja pokušaji dešifriranja su bili prilično komplicirani, a prema uvjerenju Nijemaca nemogući.

Već je spomenuto kako se 3 rotora Enigme biraju iz kutije u kojoj se nalazi ukupno 5 rotora, numeriranih brojevima od 1 do 5. Na koliko načina se mogu odabrati i postaviti 3 od mogućih 5 rotora koji su dani na odabir? Na prvi položaj može se postaviti bilo koji od mogućih 5 rotora, na drugi položaj bilo koji od preostala 4 rotora i naposlijetku bilo koji od preostala 3 rotora. Broj različitih permutacija na koji je to moguće napraviti iznosi:

$$R_1 = 5 \times 4 \times 3 = 60 \approx 2^{5.9}$$

Dakle, postoji 60 načina na koje se može postaviti 5 rotora u 3 utora u Enigmi. Sljedeće ja pitanje na koliko mogućih načina se može postaviti rotore u početni položaj? Kako alfabet ukupno sadrži 26 slova, tako je za svaki rotor postojalo 26 početnih položaja. Svaki od odabrana 3 rotora su se tako mogla postaviti u bilo kojem od 26 različitih početnih položaja.[52, 53] Primjenom principa multiplikacije dobiva se:

$$R_2 = 26 \times 26 \times 26 = 17\,576 \approx 2^{14.1}$$

Prema principu multiplikacije, ako se jedan događaj može dogoditi na m načina, a drugi se može neovisno o prvom dogoditi na n načina, tada se ova dva događaja mogu dogoditi na $m \times n$ načina.[54] Prema tome, postoji 17 576 mogućih različitih početnih položaja za 3 rotora Enigme.

---

[52] Ellis, C. (2005). Exploring the Enigma. *Plus magazine.* Dostupno na: https://plus.maths.org/content/exploring-enigma (pristupljeno 23.10.2019.)

[53] Klima, R. E., Sigmon, N. P. (2013). *Cryptology classical and modern with Maplets*. Boca Raton: CRC Press., str. 97-98.

[54] Weisstein, E. W. (2019). *Multiplication principle*. Dostupno na: http://mathworld.wolfram.com/MultiplicationPrinciple.html (pristupljeno 23.10.2019.)

Svaki puta kada bi se na tipkovnici pritisnulo slovo, desni, odnosno brzi rotor bi napravio pomak za jedno mjesto. Kada bi načinio puni krug, odnosno pomaknuo se za svih 26 mjesta, "gurnuo" bi središnji rotor koji bi se tada pomaknuo za jedno mjesto. Ako bi desni rotor napravio još jedan puni krug, ponovno bi se središnji rotor pomakao za jedno mjesto. Kada središnji rotor napravi puni krug, tada on "gurne" lijevi odnosno spori rotor i pomakne se za jedno mjesto. Trenutak kada desni rotor "gurne" središnji rotor prema naprijed te trenutak kada središnji rotor "gurne" lijevi rotor prema naprijed je moguće mijenjati. Ovo nazivamo položaj zakreta prstena rotora. Koliko je mogućih položaja prva dva rotora, u odnosu na treći rotor? Prvi rotor može se postaviti na bilo koji od 26 mogućih položaja, a tako i drugi rotor. Primjeni li se ponovo princip multiplikacije, dobiva se:

$$R_3 = 26 \times 26 = 676 \approx 2^{9.4}$$

Razvodna ploča sastojala se od 26 utora koji su se mogli povezati pomoću 13 kratkih kabela. Na koliko je načina moguće povezati parove slova pomoću kabela na razvodnoj ploči? Kako bi se dobio broj ovih kombinacija koristi se sljedeća formula:[55]

$$R_4 = \frac{N!}{(N-2m)! \times m! \times 2^m}$$

U navedenoj formuli *N* predstavlja ukupan broj utora, kojih je, kako je prethodno navedeno, bilo 26, a *m* broj kabela koje je moguće koristiti ($0 \leq m \leq 13$).[56]

Nijemci su kao dio ratnog standardnog operativnog postupka za vrijeme Drugog svjetskog rata koristili 10 kabela. Promotre li se rezultati izračuna prikazani u tablici 7, može se uočiti da najveći broj kombinacija postoji ako se koristi 11 kabela. Nakon toga broj opada. Iz navedenog proizlazi da bi dodavanjem još jednog kabela Nijemci imali maksimalan broj mogućih kombinacija na razvodnoj ploči.[57]

[55] Ellis, C. (2005). Exploring the Enigma. *Plus magazine.* Dostupno na: https://plus.maths.org/content/exploring-enigma (pristupljeno 23.10.2019.)
[56] Čavrak, H. (2004). Enigma. *Math.e: Hrvatski matematički elektronički časopis, 3.* Dostupno na: http://e.math.hr/old/enigma/index.html (pristupljeno 23.10.2019.)
[57] Short, K., Dagan A. (2013). An examination of the components and mathematics of the Enigma electromechanical rotor chipers. *Journal of Young Investigators*, 25(5), 33-40.

Broj kablova (m)	Broj kombinacija (R_4)
0	$1 = 2^0$
1	$325 \approx 2^{8.3}$
2	$44\,850 \approx 2^{15.5}$
3	$3\,453\,450 \approx 2^{21.7}$
4	$164\,038\,875 \approx 2^{27.3}$
5	$5\,019\,589\,575 \approx 2^{32.2}$
6	$100\,391\,791\,500 \approx 2^{36.5}$
7	$1\,305\,093\,289\,500 \approx 2^{40.2}$
8	$10\,767\,019\,638\,375 \approx 2^{43.3}$
9	$53\,835\,098\,191\,875 \approx 2^{45.6}$
10	$150\,738\,274\,937\,250 \approx 2^{47.1}$
11	$205\,552\,193\,096\,250 \approx 2^{47.5}$
12	$102\,776\,096\,548\,125 \approx 2^{46.5}$
13	$7\,905\,853\,580\,625 \approx 2^{42.8}$

Tablica 7. Prikaz svih kombinacija na razvodnoj ploči[58, 59]

U slučaju kada se koristi 10 kablova, primjenom prethodne formule dolazi se do ukupnog broja kombinacija razvodne ploče:

$$R_4 = \frac{N!}{(N-2m)! \times m! \times 2^m} = \frac{26!}{6! \times 10! \times 2^{10}} \approx 2^{47.1}$$

Uzme li se u obzir sve navedeno, ukupan je broj početnih postavki Enigme:[60, 61]

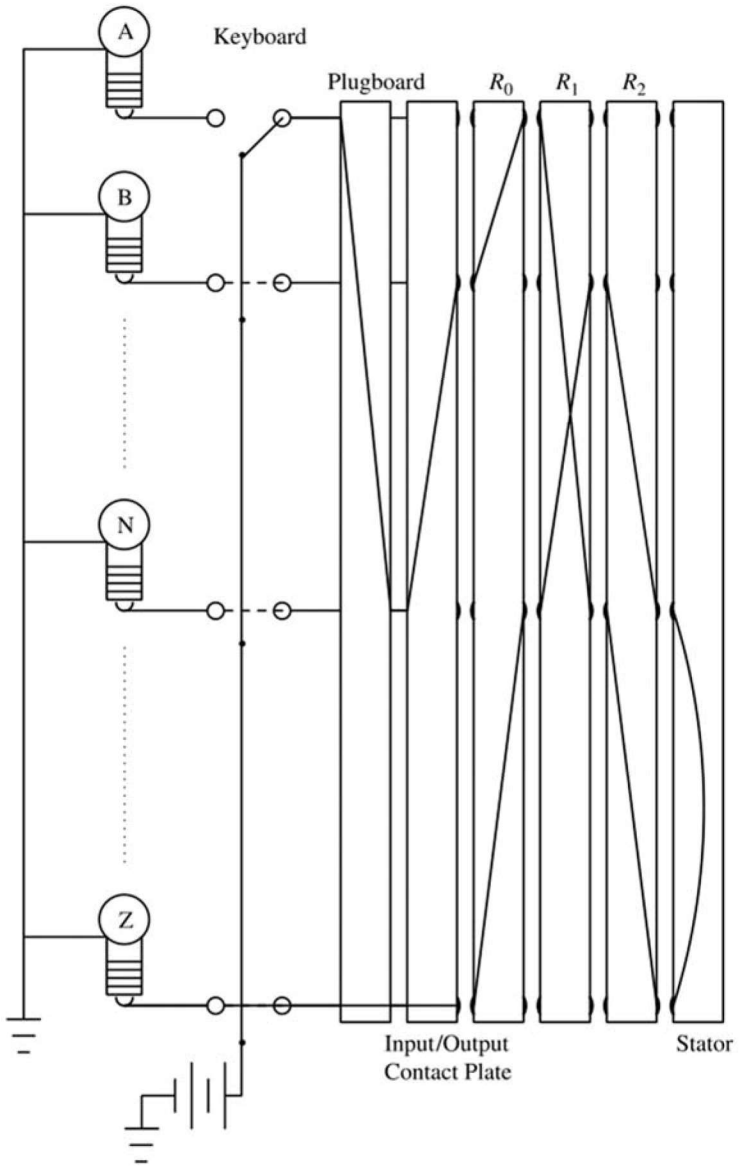
$$R_{ukupno} = R_1 \times R_2 \times R_3 \times R_4$$

$$R_{ukupno} = 2^{5.9} \times 2^{14.1} \times 2^{9.4} \times 2^{47.1} \approx 2^{77}$$

[58] Stamp, M., Low, R. M. (2007). *Applied cryptanalysis: Breaking ciphers in the real world.* Hoboken: John Wiley & Sons, Inc., str. 31.
[59] Čavrak, H. (2004). Enigma. *Math.e: Hrvatski matematički elektronički časopis, 3.* Dostupno na: http://e.math.hr/old/enigma/index.html (pristupljeno 23.10.2019.)
[60] Stamp, M., Low, R. M. (2007). *Applied cryptanalysis: Breaking ciphers in the real world.* Hoboken: John Wiley & Sons, Inc., str. 31.
[61] Čavrak, H. (2004). Enigma. *Math.e: Hrvatski matematički elektronički časopis, 3.* Dostupno na: http://e.math.hr/old/enigma/index.html (pristupljeno 23.10.2019.)

4.1.3. Princip rada – šifriranje i dešifriranje

Pritiskom slova A na tipkovnici, zatvara se strujni krug te se stvara električni signal. Signal prvo dolazi do razvodne ploče. Ako je slovo A na razvodnoj ploči povezano s nekim od preostalih slova alfabeta, tada dolazi do preusmjeravanja signala. Međutim, ako nema priključka na razvodnoj ploči, signal putuje do ulaznog kontakta statičkog rotora i dalje kao slovo A.



Slika 7. Shematski prikaz prolaza signala prilikom šifriranja poruke[62]

[62] Konheim, A. G. (2007). *Computer security and cryptography.* New Jersey: John Wiley & Sons, Inc., str. 126.

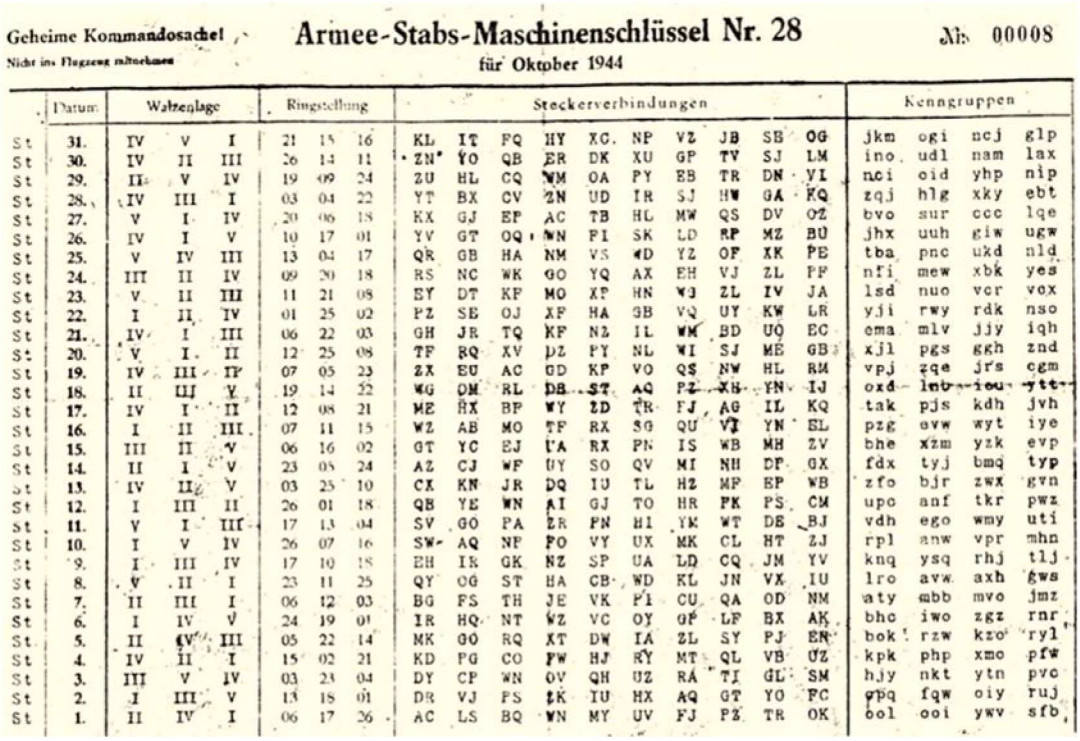
Prolaskom kroz statički rotor signal ostaje nepromijenjen i prolazi dalje kroz 3 rotora koja su na slici 7 označeni slovima R_0, R_1 i R_2. Rotor R_0 je takozvani brzi rotor, R_1 središnji rotor, a R_2 spori rotor. Unutarnje ožičenje tih rotora omogućuje permutaciju slova te tako električni signal na izlazu jednog rotora predstavlja neko drugo slovo na izlazu drugog rotora. Reflektor ulazni signal reflektira za povratni put kroz rotore. Prolaskom kroz rotore signal dolazi do izlaznog kontakta statičkog rotora, a nakon toga do razvodne ploče. Signal ostaje nepromijenjen ako ne postoji priključak na razvodnoj ploči. Ako priključak postoji, na razvodnoj ploči se signal ponovno preusmjerava.[63, 64] Na samom kraju signal dolazi do žarulje koja je povezana s baterijom. Osvjetljena žarulja kao rezultat daje šifrirano slovo. Korisnik bilježi šifrirano slovo, a zatim unosi svako slijedeće slovo otvorenog teksta koje se šifrira po istom principu.[65]

Dešifriranje poruke temelji se na inverznom postupku, pri kojem je prvo potrebno namjestiti uređaj na iste početne postavke kao prilikom šifriranja poruke. Nakon unosa slova šifriranog teksta, osvjetljena lampica kao rezultat prikazuje slova dešifriranog teksta. Nepoznavanjem početnih postavki stroja, proces dešifriranja poruka je krajnje kompliciran.

Kako bi maksimalno otežali posao Saveznicima u pokušajima probijanja Enigme, Nijemci su svakog mjeseca izrađivali nove tablice s popisom postavki stroja za svaki dan u tom mjesecu. Tablica je zapravo bila ključ za šifriranje i dešifriranje poruka pomoću Enigme. Sadržavala je položaje i odabir rotora, položaje prstena rotora, parove slova koji su se spajali na razvodnoj ploči i identifikacijsku grupu slova. Pomoću identifikacijske grupe slova provjeravale su se početne postavke uređaja.[66] Tablice su bile izuzetno strogo čuvane i ispisane rastopljivom tintom. Ako bi postojala mogućnost pronalaska liste od strane Saveznika, njemački vojnici bi je potopili u vodu i na taj način "isprali" sve informacije. Nijemci su mijenjali ključ svakoga dana kako bi smanjili broj poruka koje bi bile šifrirane na isti način. Također su smatrali kako snaga i neprobojnost Enigme leži u činjenici njezinog velikog broja mogućih kombinacija dnevnog ključa.[67]

---

[63] Konheim, A. G. (2007). *Computer security and cryptography.* New Jersey: John Wiley & Sons, Inc., str. 126.
[64] Stamp, M., Low, R. M. (2007). *Applied cryptanalysis: Breaking ciphers in the real world.* Hoboken: John Wiley & Sons, Inc., str. 26-29.
[65] Konheim, A. G. (2007). *Computer security and cryptography.* New Jersey: John Wiley & Sons, Inc., str. 126
[66] Rijmenants, D. (2004). *Enigma message procedures*. Dostupno na: http://users.telenet.be/d.rijmenants/en/enigmaproc.htm (pristupljeno 24.10.2019.)
[67] Ellis, C. (2005). Exploring the Enigma. *Plus magazine.* Dostupno na: https://plus.maths.org/content/exploring-enigma (pristupljeno 23.10.2019.)



Geheime Kommandosache! Nicht ins Flugzeug mitnehmen

Armee-Stabs-Maschinenschlüssel Nr. 28

für Oktober 1944

Nr. 00008

	Datum	Walzenlage			Ringstellung			Steckerverbindungen										Kenngruppen			
St	31.	IV	V	I	21	15	16	KL	IT	FQ	HY	XC	NP	VZ	JB	SB	OG	jkm	ogi	ncj	glp
St	30.	IV	II	III	26	14	11	ZN	YO	QB	ER	DK	XU	GP	TV	SJ	LM	ino	udl	nam	lax
St	29.	II	V	IV	19	09	24	ZU	HL	CQ	WM	OA	PY	EB	TR	DN	YI	nci	oid	yhp	nip
St	28.	IV	III	I	03	04	22	YT	BX	CV	ZN	UD	IR	SJ	HW	GA	KQ	zqj	hlg	xky	ebt
St	27.	V	I	IV	20	06	18	KX	GJ	EP	AC	TB	HL	MW	QS	DV	OZ	bvo	sur	ccc	lqe
St	26.	IV	I	V	10	17	01	YV	GT	OQ	WN	FI	SK	LD	RP	MZ	BU	jhx	uuh	giw	ugw
St	25.	V	IV	III	13	04	17	QR	GB	HA	NM	VS	KD	YZ	OF	XK	PE	tba	pnc	uxd	nld
St	24.	III	II	IV	09	20	18	RS	NC	WK	GO	YQ	AX	EH	VJ	ZL	PF	nfi	mew	xbk	yes
St	23.	V	II	III	11	21	08	SY	DT	KF	MO	XP	HN	WJ	ZL	IV	JA	lsd	nuo	vcr	vox
St	22.	I	II	IV	01	25	02	PZ	SE	OJ	XF	HA	GB	VQ	UY	KW	LR	yji	rwy	rdk	nso
St	21.	IV	I	III	06	22	03	GH	JR	TQ	KP	NZ	IL	WM	BD	UQ	EC	ema	mlv	jjy	iqh
St	20.	V	I	II	12	25	08	TF	BQ	XV	DZ	PY	NL	WI	SJ	ME	GB	xjl	pgs	gkh	znd
St	19.	IV	III	II	07	05	23	ZX	EU	AC	GD	KP	VO	QS	NW	HL	RM	vpj	zqe	jrs	cgm
St	18.	II	III	V	19	14	22	WG	OM	RL	DB	ST	AQ	PZ	XB	YN	IJ	oxd	lnb	iou	ytt
St	17.	IV	I	II	12	08	21	ME	RX	BP	WY	ZD	TR	FJ	AG	IL	KQ	tak	pjs	kdh	jvh
St	16.	I	II	III	07	11	15	WZ	AB	MO	TF	RX	SG	QU	VI	YN	EL	pzg	evw	wyt	iye
St	15.	III	II	V	06	16	02	GT	YC	EJ	UA	RX	PN	IS	WB	MH	ZV	bhe	xzm	yzk	evp
St	14.	II	I	V	23	05	24	AZ	CJ	WF	UY	SO	QV	MI	NH	DP	GX	fdx	tyj	bmq	typ
St	13.	IV	II	V	03	25	10	CX	KN	JR	DQ	IU	TL	HZ	MP	EP	WB	zfo	bjr	zwx	gvn
St	12.	I	III	II	26	01	18	QB	YE	WN	AI	GJ	TO	HR	PK	PS	CM	upo	anf	tkr	pwz
St	11.	V	I	III	17	13	04	SV	GO	PA	ZR	FN	HI	YK	WT	DB	BJ	vdh	ego	wmy	uti
St	10.	I	V	IV	26	07	16	SW	AQ	NF	PO	VY	UX	MK	CL	HT	ZJ	rpl	anw	vpr	mhn
St	9.	I	III	IV	17	10	18	EH	IK	GK	NZ	SP	UA	LD	CQ	JM	YV	knq	ysq	rhj	tlj
St	8.	V	II	I	23	11	25	QY	OG	ST	HA	CB	WD	KL	JN	VX	IU	lro	avw	axh	gws
St	7.	II	III	I	06	12	03	BG	FS	TH	JE	VK	PI	CU	QA	OD	NM	aty	mbb	mvo	jmz
St	6.	I	IV	V	24	19	01	IR	HQ	NT	WZ	VC	OY	GP	LF	BX	AK	bhc	iwo	zgz	rnr
St	5.	II	V	III	05	22	14	MK	GO	RQ	XT	DW	IA	ZL	SY	PJ	EN	bok	rzw	kzo	ryl
St	4.	IV	II	I	15	02	21	KD	PG	CO	FW	HJ	RY	MT	QL	VB	UZ	kpk	php	xmo	pfw
St	3.	III	V	IV	03	23	04	DY	CP	WN	OV	QH	UZ	RA	TJ	GL	SM	hjy	nkt	ytn	pvc
St	2.	I	III	V	13	18	01	DR	VJ	FS	EK	IU	HX	AQ	GT	YO	PC	qpq	fqw	oiy	ruj
St	1.	II	IV	I	06	17	26	AC	LS	BQ	WN	MY	UV	FJ	PZ	TR	OK	ool	ooi	ywv	sfb

Tablica 8. Prikaz dnevnog ključa Enigme[68]

4.1.4. Poljski i britanski napad na Enigmu

Poljaci su bili u neprestanom strahu od njemačke agresije. Stoga su 1932. godine, s ciljem "razbijanja" šifre novog uređaja, odlučili angažirati matematičare Mariana Rejewskog, Henryka Zygalskog i Jerzyja Rozyckog. Na raspolaganju su imali informacije o komercijalnoj Enigmi do kojih su došli nakon što je uređaj 1929. godine greškom poslan u Poljsku. Prije nego su uređaj vratili u Njemačku, Poljaci su ga vrlo pažljivo proučili. Nijemci za to nisu nikada saznali. No, komercijalna Enigma nije sadržavala razvodnu ploču pa nisu imali saznanja o unutarnjem ožičenju sustava rotora. S druge strane, francuski tajni agent je uspio doći do dvomjesečnih ključnih postavki Enigme, ali bez poznavanja rotora te informacije nisu bile iskoristive. U skladu s ugovorom o vojnoj suradnji, informacije do kojih su došli Francuzi su prenijeli britanskim i poljskim kolegama. Poljaci su bili u stanju vrlo brzo riješiti dio slagalice koji im je nedostajao, rekonstruirajući unutarnje ožičenje rotora Enigme. Osim što su uspjeli "razbiti" Enigmu izumili su i prvi elektromehanički uređaj za dešifriranje poruka poslanih pomoću tog stroja. Uređaj su nazvali *Bomba* jer je zvuk koji je stvarao pri radu podsjećao na udar bombe. Stroj se sastojao od 6 serijski

[68] Rijmenants, D. (2004). *Enigma message procedures*. Dostupno na: http://users.telenet.be/d.rijmenants/en/enigmaproc.htm (pristupljeno 24.10.2019.)

povezanih Enigmi, tako da svih 6 mogućih postavki rotora mogu biti testirane odjednom. Pomoću *Bombe*, Poljaci su mogli utvrditi postavke rotora Enigme i dešifrirati poruke Nijemaca u roku od samo dva sata. Ovo je bila strogo čuvana tajna, sve do nekoliko mjeseci prije napada Nijemaca na Poljsku. Tijekom 1939. godine Nijemci su dodali dva dodatna rotora Enigmi i time povećali broj mogućih kombinacija rotora sa 6 na 60 kombinacija. Ovo je poljsku *Bombu* učinilo neučinkovitom te Poljaci jednostavno odustaju od nastojanja da ponovo "razbiju" Enigmu. Neposredno prije početka rata Poljaci se za pomoć obraćaju Britancima i Francuzima te im prenose sve informacije vezane uz Enigmu. Nakon ovih saznanja, britanski kriptografi predvođeni Alanom Turingom dolaze do revolucionarnih ideja i uspjeha u dešifriranju Enigme. Bez informacija dobivenih od strane poljskih kriptoanalitičara, britanski napori u razbijanju Enigme bi bili uvelike otežani.[69]

Alan Turing je bio talentirani mladi matematičar koji je diplomirao na Sveučilištu Cambridge. Nakon što je Velika Britanija objavila rat Njemačkoj, Turing se prijavio na dužnost u Vladinom uredu za šifre i kodove sa sjedištem u Bletchley Parku. Idućih mjeseci njegov je tim ostvario veliki uspjeh u dešifriranju poruka njemačkih kopnenih i zračnih snaga. Uz pomoć svojih suradnika konstruirao je i prvi elektromehanički stroj, nazvan *Bomba*, s kojim će dešifriranje poruka postati bitno jednostavnije. Stroj je bio sličan i temeljio se na principima rada poljske *Bombe*.[70] No, njemačka mornarica koristila je veći broj rotora, što je onemogućavalo dešifriranje poruka. Turingov tim konačno je uspio riješiti i taj problem nakon što se Kraljevska mornarica s njemačke podmornice U-110 domogla opreme za šifriranje i dvomjesečne knjige šifri.[71]

Turing je pri pokušaju dešifriranja koristio dio otvorenog teksta za koji se pretpostavljalo da odgovara dijelu šifriranog teksta. Na temelju toga bi se napravio grafikon koji predstavlja različite odnose između slova šifriranog i otvorenog teksta. Konkretno, pronašlo bi se mjesto na kojem se fraza "wetterbericht" (vremensko izvješće) može uklopiti u šifrirani tekst.[72] Pomicanje fraze lijevo ili desno rezultiralo bi preklapanjem dvaju slova, a poznato je da se pojedino slovo ne može šifrirati samo u sebe, stoga se te mogućnosti odbacuju.[73]

---

[69] Simpson, R. (2016). *Cipher machines*. Dostupno na: https://ciphermachines.com/enigma (pristupljeno 24.10.2019.)
[70] Grime, J. (n.d.). *Maths from the talk: "Alan Turing and the Enigma machine"*. Dostupno na: http://www.singingbanana.com/enigmaproject/maths.pdf (pristupljeno 24.10.2019.)
[71] Čavrak, H. (2004). Enigma. *Math.e: Hrvatski matematički elektronički časopis, 3.* Dostupno na: http://e.math.hr/old/enigma/index.html (pristupljeno 23.10.2019.)
[72] Smart, N. P. (2016). *Cryptography made simple.* Cham: Springer., str. 150.
[73] Grime, J. (n.d.). *Maths from the talk: "Alan Turing and the Enigma machine"*. Dostupno na: http://www.singingbanana.com/enigmaproject/maths.pdf (pristupljeno 24.10.2019.)

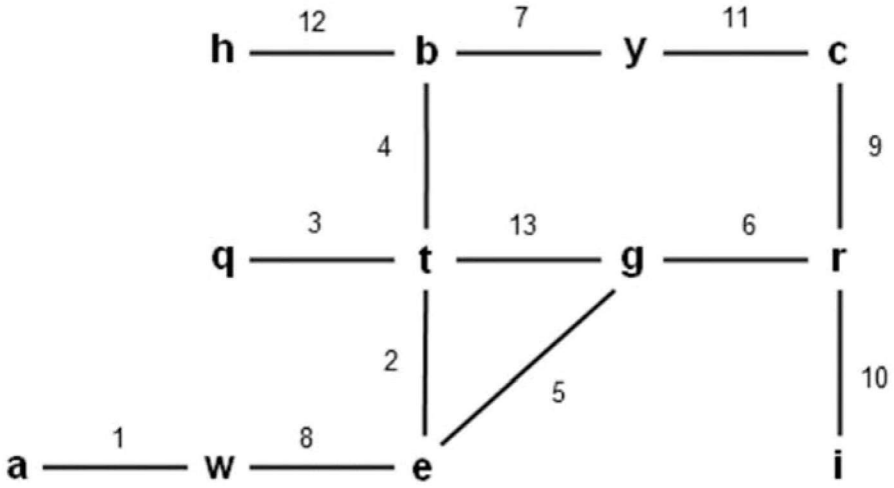
		1	2	3	4	5	6	7	8	9	10	11	12	13				
…	j	x	a	t	q	b	g	g	y	w	c	r	y	b	g	d	t	…
-	-	w	e	t	t	e	r	b	e	r	i	c	h	t	-	-	-	-

Tablica 9. Pretpostavka koja se odbacuje

			1	2	3	4	5	6	7	8	9	10	11	12	13			
…	j	x	a	t	q	b	g	g	y	w	c	r	y	b	g	d	t	…
-	-	-	w	e	t	t	e	r	b	e	r	i	c	h	t	-	-	-

Tablica 10. Pretpostavka koja se razmatra[74]

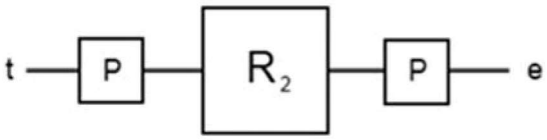
Zatim se nacrta dijagram koji opisuje odnose među parovima slova. Bilježe se slova i numerira položaj šifriranja jednog slova u drugo. Nastali dijagram se još naziva i "izbornik". On mnogo govori o konfiguraciji Enigme u smislu njezine temeljne permutacije. Na "izborniku" se temeljila ideja rada uređaja za dešifriranje poruka slanih pomoću Enigme.[75]



Slika 8. Izbornik[76]

[74] Primjer napisan prema: Grime, J (n.d.). *Maths from the talk: "Alan Turing and the Enigma machine"*. Dostupno na: http://www.singingbanana.com/enigmaproject/maths.pdf (pristupljeno 24.10.2019.)
[75] Smart, N. P. (2016). *Cryptography made simple.* Cham: Springer., str. 151.
[76] Grime, J. (n.d.). Maths from the talk: *"Alan Turing and the Enigma machine"*. Dostupno na: http://www.singingbanana.com/enigmaproject/maths.pdf (pristupljeno 24.10.2019.)

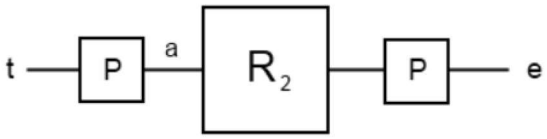
Neka se pretpostavi da odabrani dio šifriranog teksta odgovara našoj frazi. Opaža se kako na položaju broj 2, koji ujedno predstavlja položaj rotora, ulazno slovo "t" naposljetku postaje izlazno slovo "e". Skicirajmo reverzibilnu shemu rada Enigme kako bi si to lakše predočili. Slovo P predstavlja razvodnu ploču, a slovo R sustav rotora Enigme.[77]



Slika 9. Shematski prikaz rada Enigme[78]

Turing je shvatio kako je za dani položaj rotora moguće doći do određenih spoznaje o postavkama razvodne ploče.[79] Neka se pretpostavi da je slovo "t" na razvodnoj ploči spojeno sa slovom "a".

Pretpostavka: (t – a / a – t)



Slika 10. Shematski prikaz pretpostavke[80]

U nastavku će se koristiti tablica u kojoj su prikazani mogući izlazi 13 uzastopnih šifri Enigme bez uzimanja u obzir položaja na razvodnoj ploči. Ovo vrijedi jedino uz pretpostavku da se drugi i treći rotor neće pomaknuti.[81]

---

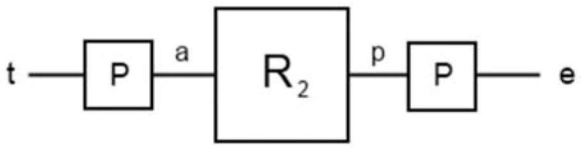
[77] Grime, J. (n.d.). *Maths from the talk: "Alan Turing and the Enigma Machine"*. Dostupno na: http://www.singingbanana.com/enigmaproject/maths.pdf (pristupljeno 24.10.2019.)
[78] Grime, J. (n.d.). *Maths from the talk: "Alan Turing and the Enigma Machine"*. Dostupno na: http://www.singingbanana.com/enigmaproject/maths.pdf (pristupljeno 24.10.2019.)
[79] Tang, L., Lee, N., Russo, S. (2018). *Breaking Enigma.* Dostupno na: https://courses.csail.mit.edu/6.857/2018/project/lyndat-nayoung-ssrusso-Enigma.pdf (pristupljeno 24.10.2019.)
[80] Grime, J. (n.d.). *Maths from the talk: "Alan Turing and the Enigma Machine"*. Dostupno na: http://www.singingbanana.com/enigmaproject/maths.pdf (pristupljeno 24.10.2019.)
[81] Grime, J. (n.d.). *Maths from the talk: "Alan Turing and the Enigma Machine"*. Dostupno na: http://www.singingbanana.com/enigmaproject/maths.pdf (pristupljeno 24.10.2019.)

input:	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
output 1:	j	f	q	x	h	b	s	e	k	a	i	y	z	t	v	u	c	w	g	n	p	o	r	d	l	m
output 2:	p	n	s	k	u	z	o	w	v	l	d	j	r	b	g	a	t	m	c	q	e	i	h	y	x	f
output 3:	k	d	p	b	i	q	t	m	e	o	a	n	h	l	j	c	f	t	g	r	x	z	y	u	w	v
output 4:	x	o	d	c	h	z	l	e	p	y	u	g	q	w	b	i	m	v	t	s	k	r	n	a	j	f
output 5:	o	f	y	e	d	b	z	x	l	w	q	i	n	m	a	s	k	v	p	u	t	r	j	h	c	g
output 6:	v	w	p	t	m	x	k	u	o	l	g	j	e	z	i	c	r	q	y	d	k	a	b	f	s	n
output 7:	d	r	t	a	g	u	e	m	z	k	j	x	i	v	y	w	s	b	q	c	f	n	p	l	o	i
output 8:	v	z	e	j	c	q	u	n	l	d	y	i	r	h	w	x	f	n	t	s	g	a	o	p	k	b
output 9:	h	x	i	z	g	p	e	a	c	y	o	v	s	t	k	f	w	u	m	n	r	l	q	b	j	d
output 10:	h	v	x	m	z	i	k	a	f	s	g	w	d	q	u	r	n	p	j	y	o	b	l	c	t	e
output 11:	o	w	m	p	y	l	t	z	k	x	i	g	c	u	a	d	r	q	v	f	n	s	b	j	e	h
output 12:	r	u	z	l	j	y	i	t	f	e	m	d	k	x	q	r	o	a	p	h	b	w	v	n	f	c
output 13:	t	l	s	p	o	h	x	f	q	k	j	b	w	r	e	d	i	n	c	a	y	z	m	g	u	v

Tablica 11. Prikaz trinaest uzastopnih šifri Enigme za svako slovo[82]

Očitavanjem iz tablice uočava se kako slovo "a" na drugoj poziciji postaje slovo "p". Budući da se zna da je naše izlazno slovo "e" može se zaključiti da je slovo "p" na razvodnoj ploči spojeno sa slovom "e".

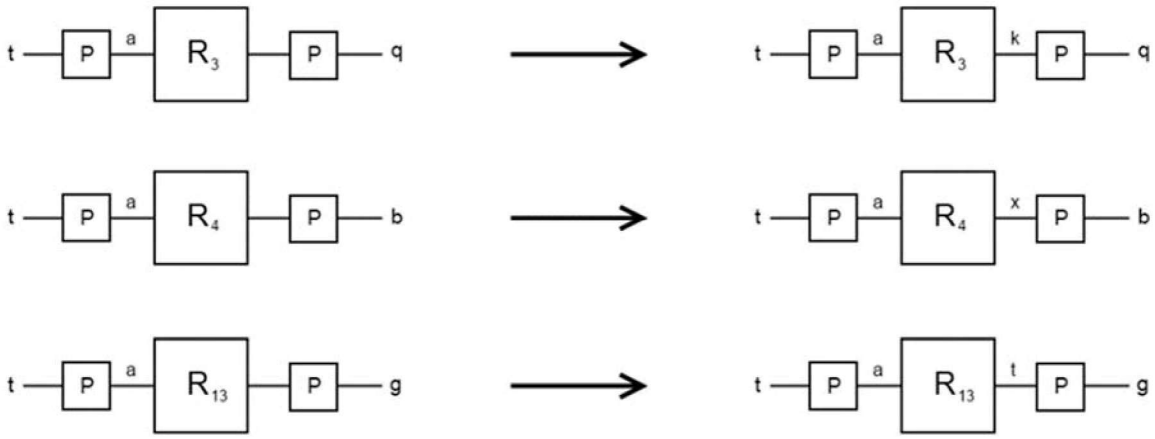
Zaključak br. 1: (p – e / e – p)



Slika 11. Shematski prikaz prvog zaključka[83]

Na isti način, razmatrajući što se događa na trećem, četvrtom i trinaestom položaju rotora, dolazi se do spoznaje za još tri postavke na razvodnoj ploči.

[82] Grime, J. (n.d.). *Maths from the talk: "Alan Turing and the Enigma machine"*. Dostupno na: http://www.singingbanana.com/enigmaproject/maths.pdf (pristupljeno 24.10.2019.)
[83] Grime, J. (n.d.). *Maths from the talk: "Alan Turing and the Enigma machine"*. Dostupno na: http://www.singingbanana.com/enigmaproject/maths.pdf (pristupljeno 24.10.2019.)



Slika 12. Shematski prikaz ostalih zaključaka[84]

Pretpostavka br. 1: (t – a / a – t)

Zaključak br. 2: (k – q / q – k)

Zaključak br. 3: (x – b / b – x)

Zaključak br. 4: (t – g / g – t)

Ako se razmotre rezultati uočava se kontradikcija jer parovi (t–a) i (t–g) ne mogu biti parovi na razvodnoj ploči. Stoga je početna pretpostavka netočna. Prema istom postupku može se pretpostaviti da je slovo "t" spojeno na razvodnoj ploči s nekim drugim slovom (npr. "b", "c", "d", "e", ...). No, ako se za slovo "t" ispišu svi mogući parovi slova i oni uvijek vode ka kontradikciji, tada je pretpostavka o položaju rotora pogrešna.

Da se prvotno pretpostavilo da je par slova (t–g) spojen na razvodnoj ploči, ponovljenim postupkom bi se došlo do zaključka da je onda i (t–a) jedan od parova slova na razvodnoj ploči, što je netočno. Iz tog se razloga mogu eliminirati i parovi slova (p–e), (k–q) i (x–b). Dakle, ako se jednom u postupku naiđe na kontradikciju, tada se mogu eliminirati i svi ostali parovi razvodne ploče koji su se temeljili na toj pretpostavci. Ova važna spoznaja do koje je došao Alan Turing iskorištena je pri konstrukciji *Bombe*.[85]

Bomba je radila kao istovremeni, serijski niz povezanih Enigmi, gdje su logičke upletenosti "jedne" Enigme mogle napajati "druge" Enigme koje su bile postavljene na različitim položajima.

---

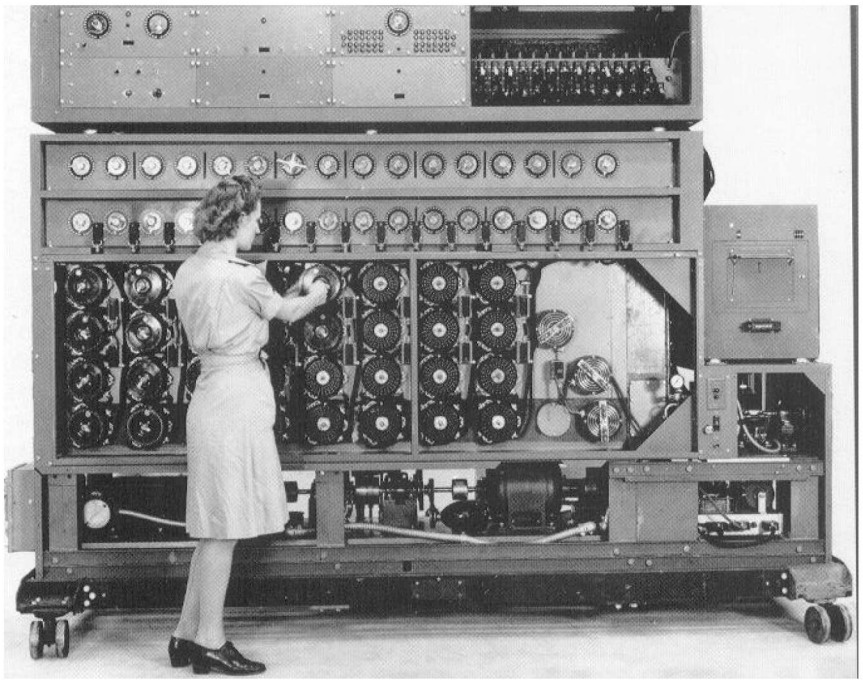
[84] Grime, J. (n.d.). *Maths from the talk: "Alan Turing and the Enigma machine"*. Dostupno na: http://www.singingbanana.com/enigmaproject/maths.pdf (pristupljeno 24.10.2019.)

[85] Grime, J. (n.d.). *Maths from the talk: "Alan Turing and the Enigma machine"*. Dostupno na: http://www.singingbanana.com/enigmaproject/maths.pdf (pristupljeno 24.10.2019.)

Njihovi ulazi i izlazi određivani su iz takozvanih "izbornika". Nakon početne postavke za razvodnu ploču moglo se dogoditi nešto od sljedećeg: [86]

- struja prolazi kroz sve utikače za zadano slovo, što znači da je položaj rotora netočan te treba pokušati s novim;
- struja prolazi kroz jedan utikač za dano slovo ili sve utikače osim jednog te se stroj zaustavlja;
- struja prolazi kroz druge utikače, što znači da je potrebna daljnja provjera;
- stroj se slučajno zaustavlja.

Kako bi umanjili probleme lažnih zaustavljanja i rezultate koji su zahtijevali daljnju provjeru kriptografi su koristili "izbornike" koji sadrže cikluse. Gordon Welchman kasnije *Bombi* dodaje "dijagonalnu ploču" koja je povećala brzinu i efikasnost samog stroja. Ona je svako slovo spajala sa svim ostalima i tako tvorila mrežu dijagonalnih linija. Bomba je tada mogla provjeriti svih 17 576 mogućih položaja rotora za manje od 20 minuta.[87]



Slika 13. Britanska *Bomba*[88]

[86] Grime, J. (n.d.). *Maths from the talk: "Alan Turing and the Enigma machine"*. Dostupno na: http://www.singingbanana.com/enigmaproject/maths.pdf (pristupljeno 24.10.2019.)
[87] Carter, F. (2010.) *The Turing Bombe*. Dostupno na: http://www.rutherfordjournal.org/article030108.html (pristupljeno 26.10.2019)
[88] Crypto Museum. (2012). *Bombe*. Dostupno na: https://www.cryptomuseum.com/crypto/bombe/ (pristupljeno 25.10.2019.)

4.2. SIGABA

SIGABA je elektromehanički uređaj za šifriranje i dešifriranje poruka kojeg su koristile Sjedinjene Američke Države za vrijeme Drugog svjetskog rata. Stroj je 1932. godine patentirao William F. Friedman i njegov asistent Frank. B. Rowlett, a kasnije su ga usavršili pripadnici američke ratne mornarice. Za vrijeme rata američka mornarica upotrebljava ga je pod nazivom CSP–888 ili ECM Mark II, a kopnena vojska kao Converter M–134–C ili SIGABA. Friedman je nastojao poboljšati sigurnost rotorskih strojeva pokušavajući izbjeći njihovo pravilno i zadano mijenjanje položaja. Zaključio je da će dešifriranje poruke biti puno teža ako se rotori okreću nasumično sa zasebnim ključem. Ideju je proveo ugradnjom papirne vrpce koja je određivala pomake rotora. Rowlett je kasnije predložio elektromehanički način generiranja ključa. Američka ratna mornarica čini značajna poboljšanja na originalnom dizajnu uređaja, neovisno o Friedmanu i Rowlettu. Jedno od tih poboljšanja je razvodnu ploču zamjenjivalo s pet indeksnih rotora koji primaju signale od upravljačkih rotora te se koriste za kontrolu nepravilnih okretanja rotora.[89]

4.2.1. Dijelovi i izgled

SIGABA je bio veći, masivniji i složeniji elektromehanički uređaj od Enigme. Iako nije bio praktičan kao Enigma, davao je bolje rezultate. Glavni dijelovi uređaja su tipkovnica, sustav rotora, printer i vijak s izbornikom. Tipkovnica je bila nalik tipkovnici pisaćeg stroja. Služila je za unos otvorenog ili šifriranog teksta te je sadržavala 26 tipki sa slovima latiničnog alfabeta, veliku tipku za razmak pri pisanju te brojeve od 0 do 9. U gornjem desnom kutu iznad tipkovnice se nalazio brojač znakova u poruci te tipka za njegovo ponovno pokretanje. Osoba koja je bila obučena za slanje šifriranih poruka pomoću ovog uređaja mogla je poslati čak 45 do 50 riječi u minuti.[90, 91]

SIGABA je rotorska mašina, ali za razliku od Enigme koristila je čak 15 rotora koji se mogu podijeliti u 3 skupine: 5 šifrirnih rotora, 5 kontrolnih rotora i 5 indeksnih rotora. Svaki od šifrirnih

---

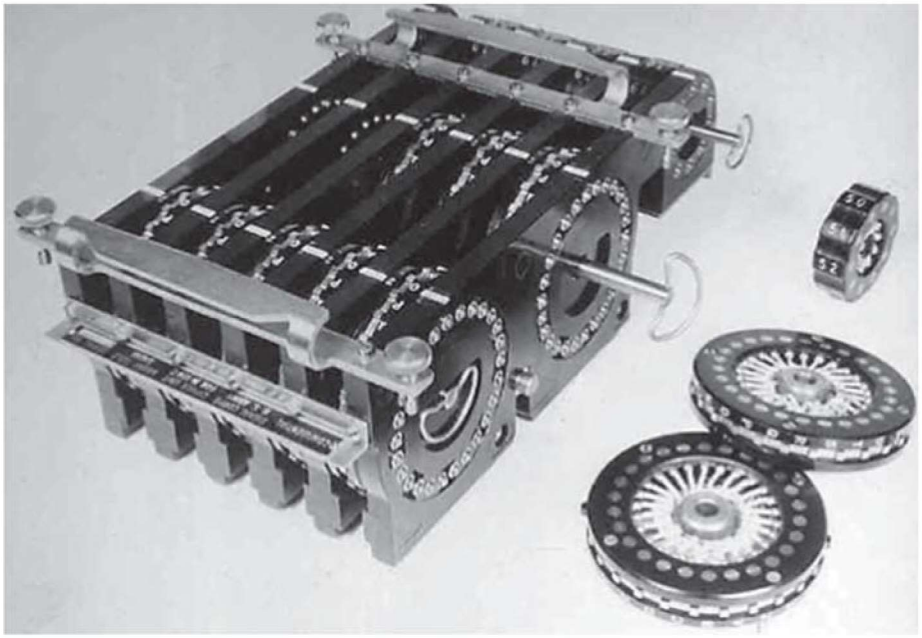
[89] Dooley, J. F. (2018). *History of cryptography and cryptanalysis: Codes, ciphers, and their algorithms.* Cham: Springer., str. 157-159.

[90] Crypto Museum (2019). *SIGABA.* Dostupno na: https://www.cryptomuseum.com/crypto/usa/sigaba/index.htm (pristupljeno 25.10.2019.)

[91] Sterling, C. H. (2008). *Military communications: From ancient times to the 21st century.* Santa Barbara: ABC-CLIO., str. 134

i kontrolnih rotora imaju po 26 električnih kontakata, a označeni su slovima alfabeta na vanjskoj strani rotora. Lijeve i desne strane tih rotora su identične pa je svejedno na koji način i na koje mjesto će se postaviti ovih 10 rotora u utore uređaja. Način umetanja rotora bio je dio ključa.[92] Svaki od pet šifrirnih rotora se rotira nasumično, odnosno nepravilnim redoslijedom u ovisnosti od kontrolnih i indeksnih rotora. Krajnji lijevi i krajnji desni kontrolni rotori su stacionarni, a 3 središnja (unutarnja) kontrolna rotora se rotiraju na isti način kao i rotori Enigme. Teći rotor se pomakne za svako uneseno slovo, četvrti rotor nakon punog kruga trećeg rotora, a drugi rotor nakon punog kruga četvrtog rotora.[93]

Svaki indeksni rotor ima po 10 kontakta, a označeni su nizom brojeva od 10 do 59, tako da indeksni rotor broj 1 sadrži brojeve od 10 do 19, rotor broj 2 brojeve od 20 do 29 i tako redom. Indeksni rotori su stacionarni i mogu se pomicati jedino ručno. Za razliku od Enigme, SIGABA ne sadrži reflektor niti razvodnu ploču. Funkciju razvodne ploče preuzimaju rotori.[94]



Slika 14. SIGABA – sustav rotora[95]

[92] Dooley, J. F. (2018). *History of cryptography and cryptanalysis: Codes, ciphers, and their algorithms.* Cham: Springer., str. 160.
[93] Mucklow, J. T. (2015). *The SIGABA / ECM II cipher machine:"A beautiful idea".* Fort George G. Meade: National Security Agency., str. 32.
[94] Dooley, J. F. (2018). *History of cryptography and cryptanalysis: Codes, ciphers, and their algorithms.* Cham: Springer., str. 160-161.
[95] Mucklow, J. T. (2015). *The SIGABA / ECM II cipher machine:"A beautiful idea".* Fort George G. Meade: National Security Agency., str. 18.

SIGABA je mogla ispisivati izlazni tekst izravno na gumiranu papirnu trakicu. Printer je koristio tintnu vrpcu koja je bila postavljena na prednjoj strani uređaja točno iznad tipkovnice. Papir koji ulazi u printer bio je namotan u kružnom prostoru na desnoj strani uređaja. Slova su se ispisivala na papirnu traku pomoću rotirajuće glave printera.[96]

Na gornjoj desnoj strani stroja nalazi se vijak s izbornikom koji određuje način rada stroja. Vijak može biti okrenut tako da stroj šifrira poruku, dešifrira poruku, piše samo otvoreni tekst, okrenut je u statusu isključenja stroja ili se nalazi u statusu ponovnog pokretanja.[97]

Slika 15. SIGABA[98]

4.2.2. Početne postavke

Odabirom rotora i njihovih početnih položaja određuje se duljina ključa. On ovisi o početnim postavkama kontrolnih, šifrirnih i indeksnih rotora. Neka se pretpostavi da imamo jedan set od 15

[96] Crypto Museum (2019). *SIGABA*. Dostupno na: https://www.cryptomuseum.com/crypto/usa/sigaba/index.htm pristupljeno (25.10.2019.)
[97] Mucklow, J. T. (2015). *The SIGABA / ECM II cipher machine:"A beautiful idea".* Fort George G. Meade: National Security Agency., str. 34.
[98] Mucklow, J. T. (2015). *The SIGABA / ECM II cipher machine:"A beautiful idea".* Fort George G. Meade: National Security Agency., str. 27.

rotora, koji sadrži 10 šifrirnih i kontrolnih rotora te 5 indeksnih rotora. Šifrirne i kontrolne rotore može se odabrati i postaviti na $R_1 = N! = 10!$ mogućih načina. Na prvi položaj može se postaviti bilo koji od mogućih 10 rotora, na drugi položaj bilo koji od preostalih 9 rotora, zatim bilo koji od preostalih 8 rotora i tako redom. Svaki od tih 10 rotora može se zatim postaviti na neko od 26 početnih položaja, što daje $R_2 = 26^{10}$ mogućih početnih položaja za 10 rotora. Nadalje, svaki od rotora može se postaviti u smjeru ili prema naprijed ili u obrnutom smjeru. To daje još dodatnih $R_3 = 2^{10}$ mogućih odabira položaja rotora. Iz navedenog slijedi da se šifrirne i kontrolne rotore može postaviti na:

$$R_{š+k} = R_1 \times R_2 \times R_3 = 10! \times 26^{10} \times 2^{10} = 2^{78.8} \text{ mogućih načina.}$$

Indeksne rotore može se odabrati i postaviti na $R_4 = N! = 5!$ mogućih načina. Svaki od tih 5 rotora zatim se može postaviti na neko od 10 početnih položaja što daje $R_5 = 10^5$ mogućih početnih rotora. Dakle, indeksne rotore može se postaviti na $R_i = R_4 \times R_5 = 5! \times 10^5 = 2^{23.5}$ mogućih načina. Prema tome, ukupan je broj postavki rotora:

$$R_{postavke\ rotora} = R_{š+k} \times R_i = 2^{78.8} \times 2^{23.5} = 2^{102.3}$$

Međutim, veličina ključa indeksnih rotora je ograničena činjenicom da su ti rotori stacionarni, te se za 10 ulaza dobiva samo 5 logičkih izlaza grupiranih u parove. Stoga, uključujući logičke izlaze indeksnih rotora, imamo:

$$R_{logički\ izlazi} = \frac{10!}{2^5} = 113400 = 2^{16.8} \text{ mogućih načina.}$$

Naposljetku se za ukupan broj kombinacija početnih postavki dobiva slijedeći iznos:[99, 100]

$$R_{ukupno} = 2^{78.8+16.8} = 2^{95.6}$$

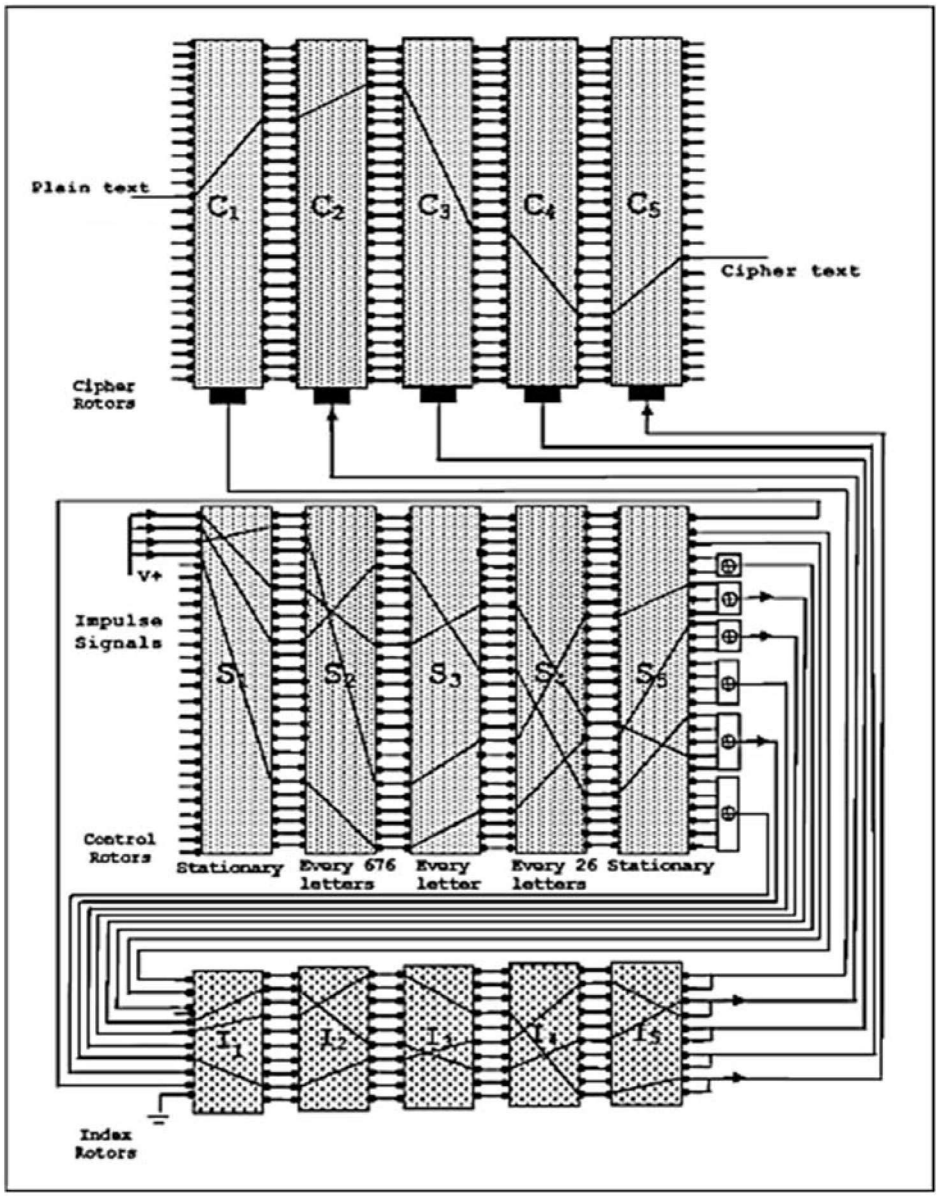
U usporedbi s Enigmom, SIGABA je imala veći broj kombinacija početnih postavka što se moglo i očekivati s obzirom na puno veći broj rotora.

[99] Stamp, M., Low, R. M. (2007). *Applied cryptanalysis: Breaking ciphers in the real world*. Hoboken: John Wiley & Sons, Inc., str. 57-59.

[100] Lasry, G. (2019). A practical meet-in-the-middle attack on SIGABA. U E. Antal, K. Schmeh, (ur.), *Proceedings of the 2nd International Conference on Historical Cryptology* (str. 41-49). Linköping: Linköping University Electronic Press.

4.2.3. Princip rada – šifriranje i dešifriranje

Tijekom postupka šifriranja otvoreni tekst se unosi pomoću tipkovnice. Kada se na tipkovnici pritisne slovo, poslani signal se dijeli na dva dijela. Prvi dio signala dolazi do lijeve strane šifrirnih rotora. Signal tada prolazi kroz svih pet rotora koji permutiraju slovo otvorenog teksta i proizvode šifrirano slovo.[101]



Slika 16. SIGABA – shematski prikaz unutarnjeg ožičenja[102]

[101] Mucklow, J. T. (2015). *The SIGABA / ECM II cipher machine:"A beautiful idea".* Fort George G. Meade: National Security Agency., str. 33.
[102] Mucklow, J. T. (2015). *The SIGABA / ECM II cipher machine:"A beautiful idea".* Fort George G. Meade: National Security Agency., str. 31.

Drugi dio signala dolazi do desne strane kontrolnih rotora. Taj signal uvijek aktivira četiri signala koji prolaze kroz pet kontrolnih rotora. Svaki signal se permutira prolaskom kroz rotore i zatim svaki dolazi na jedan od 26 izlaza. Ti izlazi (A do Z) su grupirani u 9 signala, a prikazuje ih tablica 12. Navedeni signali su ulazi u indeksne rotore, s time da je deseti ulaz uvijek isključen. Od tih 9 signala najviše 4 mogu biti aktivirana, a najmanje jedan. Na slici 16 uočava se kako su 3 ulaza u indeksne rotore aktivna. Indeksni rotori dalje permutiraju ulazne signale. Izlazi indeksnih rotora su grupirani u parove od 5 skupina. Svaki od tih 5 signala je spojen s jednim od 5 šifrirnih rotora. Ako je veza između indeksnih i šifrirnih rotora aktivna tada se šifrirni rotor okrene za jedan položaj.[103]

Ulazi u indeksne rotore	Logika (A do Z su izlazi iz kontrolnih rotora, ∨ je ILI)
Ulaz 1	B
Ulaz 2	C
Ulaz 3	D ∨ E
Ulaz 4	F ∨ G ∨ H
Ulaz 5	I ∨ J ∨ K
Ulaz 6	L ∨ M ∨ N ∨ O
Ulaz 7	P ∨ Q ∨ R ∨ S ∨ T
Ulaz 8	U ∨ V ∨ W ∨ X ∨ Y ∨ Z
Ulaz 9	A
Ulaz 10	Isključen

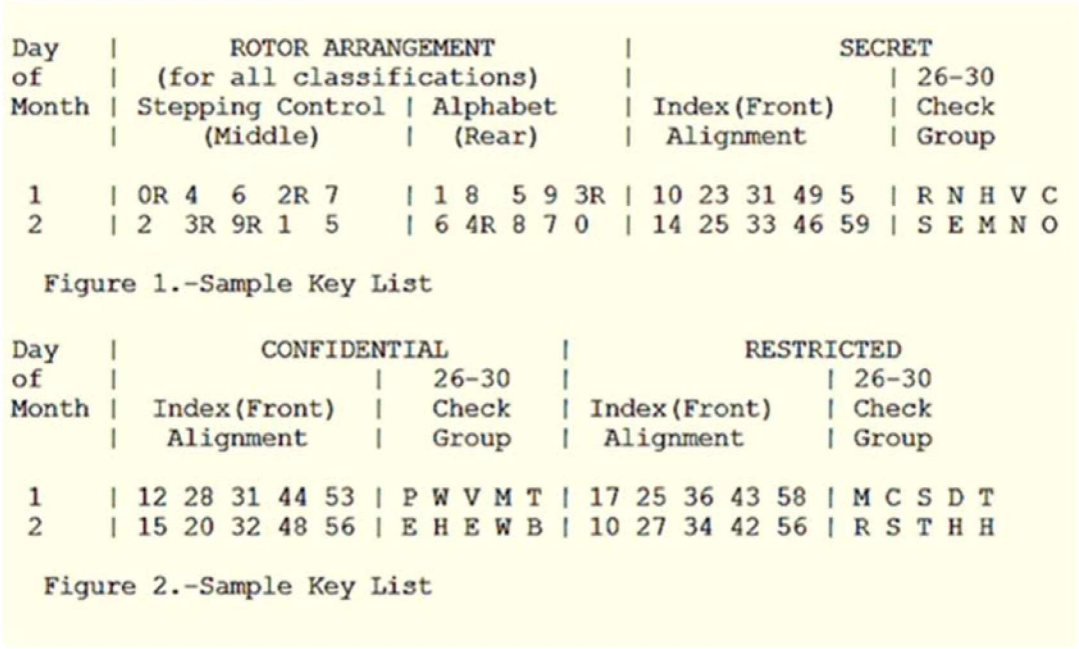
Tablica 12. Logika indeksnih rotora[104]

SIGABA je zanimljiva po tome što slovo "Z" i "razmak" tretira drugačije od ostalih slova. Nakon unosa, slovo "Z" se mijenja u slovo "X", a razmak se mijenja u slovo "Z" prije nego stignu do šifrirnih rotora.[105]

[103] Mucklow, J. T. (2015). *The SIGABA / ECM II cipher machine:"A beautiful idea".* Fort George G. Meade: National Security Agency., str. 31-33.
[104] Lasry, G. (2019). A practical meet-in-the-middle attack on SIGABA. U E. Antal, K. Schmeh, (ur.), *Proceedings of the 2nd International Conference on Historical Cryptology* (str. 41-49). Linköping: Linköping University Electronic Press.
[105] Stamp, M., Low, R. M. (2007). *Applied cryptanalysis: Breaking ciphers in the real world.* Hoboken: John Wiley & Sons, Inc., str. 56.

S istim početnim postavkama stroja dešifriranje se provodi prema istom principu kao i šifriranje, ali uz dvije promijene. Pritiskom tipke na tipkovnici prvi dio signala se šalje s desne na lijevu stranu šifrirnih rotora, umjesto s lijeve na desnu stranu, kao što je to bio slučaj kod šifriranja poruke. Druga promjena se odnosi na slovo "Z". Ako je izlazno slovo nakon šifrirnih rotora slovo "Z", ono se mijenja u razmak prije nego što se potpuno dešifrira. To znači da dešifrirani tekst nikada ne sadržava "Z". Svako slovo "Z" u originalnom tekst će se dešifrirati kao slovo "X".[106]

Kao i kod Enigme, svaki mjesec je izlazila nova tablica s popisom postavki stroja SIGABA za svaki dan u mjesecu. Tablica je sadržavala redoslijed i položaj šifrirnih i kontrolnih rotora, redoslijed indeksnih rotora te provjeru zadanih postavki. Slovo "R" označavalo je suprotnu orijentaciju rotora. Ako se pritiskom istog slova 30 puta, zadnjih 5 slova u tablici i isprintana slova poklapaju, onda je stroj bio dobro postavljen. Prva stavka je uvijek bila ista, a zadnje dvije su se razlikovale u ovisnosti o načinu na koji se poruka šalje. Poruka je mogla biti poslana tajno, povjerljivo ili strogo povjerljivo.[107]



Day of Month	ROTOR ARRANGEMENT (for all classifications) Stepping Control (Middle)	Alphabet (Rear)	SECRET Index(Front) Alignment	26-30 Check Group
1	0R 4 6 2R 7	1 8 5 9 3R	10 23 31 49 5	R N H V C
2	2 3R 9R 1 5	6 4R 8 7 0	14 25 33 46 59	S E M N O

Figure 1.-Sample Key List

Day of Month	CONFIDENTIAL Index(Front) Alignment	26-30 Check Group	RESTRICTED Index(Front) Alignment	26-30 Check Group
1	12 28 31 44 53	P W V M T	17 25 36 43 58	M C S D T
2	15 20 32 48 56	E H E W B	10 27 34 42 56	R S T H H

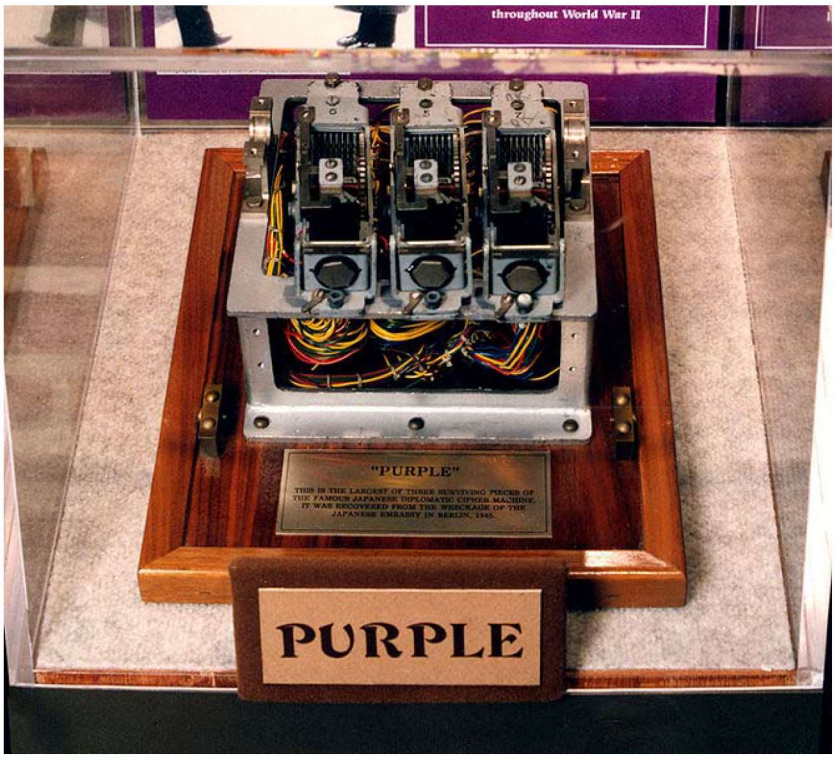
Figure 2.-Sample Key List

Tablica 13. SIGABA - dnevni ključ[108]

[106] Stamp, M., Low, R. M. (2007). *Applied cryptanalysis: Breaking ciphers in the real world.* Hoboken: John Wiley & Sons, Inc., str. 56.
[107] Pekelney, R. (2006). *Operating instructions for ASAM 1 (a.k.a. ECM Mark II).* Dostupo na: https://maritime.org/tech/ecminst.htm (pristupljeno 26.10.2019.)
[108] Pekelney, R. (2006). *Operating instructions for ASAM 1 (a.k.a. ECM Mark II).* Dostupo na: https://maritime.org/tech/ecminst.htm (pristupljeno 26.10.2019.)

4.3. PURPLE

Purple je kodno ime korišteno od strane američkih kriptografa za "Enkripcijski stroj tip B" kojeg su za vrijeme Drugog svjetskog rata upotrebljavali Japanci. Stroj su 1937. godine osmislili i dizajnirali Kazuo Tanabe, Masaji Yamamoto i Eikichi Suzuki po uzoru na njemačku Enigmu i prijašnju verziju ovoga stroja zvanu " Enkripcijski stroj tip A" ili jednostavno Red (engl. crvena). Za razliku od strojeva Enigma i SIGABA, Purple je bio elektromehanički uređaj koji je koristio prekidače umjesto rotore za šifriranje povjerljivih diplomatskih poruka te se razlikovao od navedenih uređaja po svojim specifikacijama i kompleksnosti. Saveznici su uspjeli "probiti" njegov sustav šifriranja poruka, iako ne postoje dokazi da su ikada zaplijenili uređaj. Upravo zbog toga se smatra kako dešifriranje poruka koje su šifrirane pomoću japanskog stroja Purple predstavlja najveći uspjeh kriptoanalitičara za vrijeme Drugog svjetskog rata.[109, 110]



Slika 6. Purple (ostaci uređaja iz japanskog veleposlanstva u Berlinu)[111]

[109] Verma, P. K., El Rifai, M., Chan, K.W.C. (2019). *Multi-photon quantum secure comunication.* Singapore: Springer., str. 6.
[110] De Leeuw, K., Bergstra, J. (2007). *The history of information security: A comprehensive handbook*. Amsterdam: Elsevier., str. 411.
[111] George C. Marshall Foundation. (2014). *Type 97 cypher machine*. Dostupno na: https://www.marshallfoundation.org/blog/marshall-purple-pearl-harbor/664px-type_97_cypher_machine/ (pristupljeno 26.10.2019.)

4.3.1. Dijelovi i izgled

Stroj se sastojao od tipkovnice, ulazne i izlazne razvodne ploče, 4 prekidača koji su zamjenjivali ulogu rotora u dosadašnjim strojevima te printera pomoću kojeg se ispisivala šifrirana poruka na papir. Prekidač je mehanički višeslojni uređaj korišten u tadašnjim telefonskim sustavima. Svaki sloj sadrži električne kontakte koji su raspoređeni u polukružnom luku. Kao odgovor na električni impuls, elektromagnet koji je priključen na prekidač pomiče prekidač na slijedeći položaj.[112, 113]

4.3.2. Početne postavke

Kod početnih postavki stroja bitno je odrediti koji od 3 prekidača L, M i R je takozvani brzi, središnji ili spori prekidač. Kako svaki od ta 3 prekidača može biti ili brzi ili središnji ili spori prekidač, slijedi da ih se možemo postaviti na 6 načina:

$$R_1 = N! = 3! = 3 \times 2 \times 1 = 6 \approx 2^{2.6}$$

Svaki od 4 prekidača može se postaviti na jedno od 25 početnih položaja. Stoga je broj kombinacija na koji se može postaviti prekidače S, L, M i R:

$$R_2 = 25 \times 25 \times 25 \times 25 = 25^4 \approx 2^{18.6}$$

Naposljetku se još mogu odabrati ulazne i izlazne permutacije razvodne ploče. Svaka razvodna ploča sadrži 26 slova alfabeta koje se mogu permutirati. Ukupan je broj takvih mogućnosti:

$$R_3 = N! \times N! = 26! \times 26! = (26!)^2 \approx 2^{176.8}$$

Kako su Japanci koristili istu razvodnu ploču za ulaz i izlaz, to reducira ukupan broj permutacija razvodne ploče na pola od navedenog iznosa. Iz navedenih izračuna slijedi da je ukupan broj mogućih postavki stroja:[114]

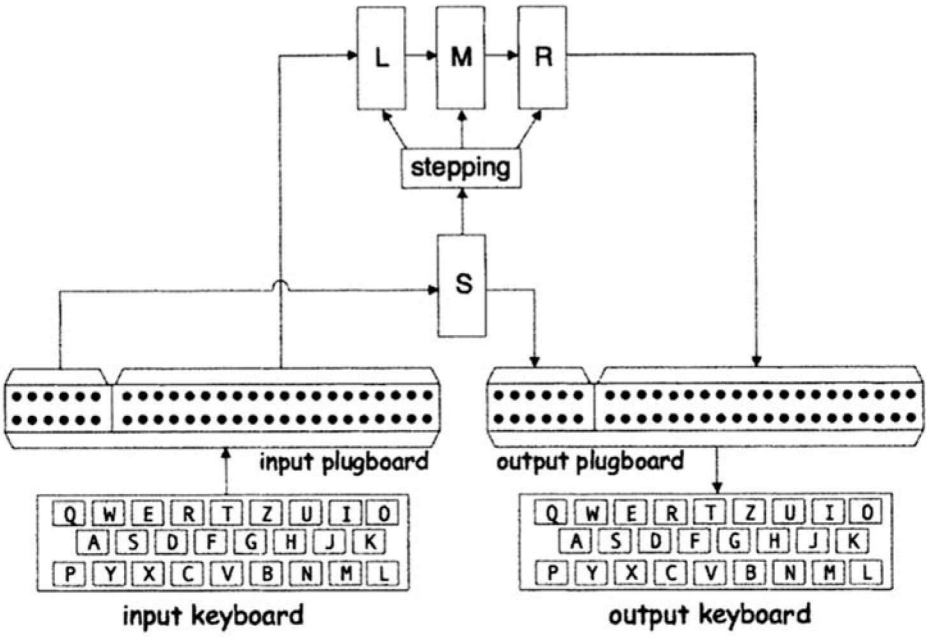
$$R_{ukupno} = R_1 + R_2 + R_3 = 2^{2.6} + 2^{18.6} + 2^{88.4} = 2^{109.6}$$

---

[112] Konheim, A. G. (2007). *Computer security and cryptography.* New Jersey: John Wiley & Sons, Inc., str. 211.
[113] Freeman, W., Sullivan, G., Weierud F. (2003). PURPLE revealed: Simulation and computer-aided cryptanalysis of Angooki Taipu B. *Cryptologia*, 27(1), 1-43.
[114] Stamp, M., Low, R. M. (2007). *Applied cryptanalysis: Breaking ciphers in the real world.* Hoboken: John Wiley & Sons, Inc., str. 44-45.

4.3.3. Princip rada – šifriranje i dešifriranje

Pritiskom slova na tipkovnici, signal prvo dolazi do ulazne razvodne ploče čiji je zadatak permutirati slova. Permutacija se odvija u dvije skupine. Prva skupina sadrži 6 slova alfabeta (AEIOUY), a druga skupina 20 suglasnika alfabeta (BCDFGHJKLMNPQRSTVWXZ). Ako je prolaskom kroz razvodnu ploču izlazno slovo rezultat permutacije prve skupine, ono tada prolazi kroz prekidač S do izlazne razvodne ploče pa sve do printera. Primjerice, ako je slovo "T" na tipkovnici spojeno na ulaznoj razvodnoj ploči sa slovom "O", ono će se šifrirati na izlazu iz razvodne ploče permutacijom prve skupine slova, i obratno. S druge strane, ako je prolaskom kroz razvodnu ploču izlazno slovo rezultat permutacije druge skupine, signal se dalje permutira prolaskom kroz 3 serijski spojena prekidača (L, M i R) pa sve do izlazne razvodne ploče. Permutacije na ulaznoj i izlaznoj razvodnoj ploči su uvijek bile iste. Ovo je bila jedna od mana ovog stroja. Razvodna ploča nije spajala parove slova alfabeta, kao kod Enigme koja ima samo jednu razvodnu ploču, nego je 26 slova alfabeta na tipkovnici spajala s nekim od 26 slova alfabeta kako bi se mogla izvršiti željena permutacija.[115]



Slika 18. Shematski prikaz postupka šifriranja[116]

[115] Stamp, M., Low, R. M. (2007). *Applied cryptanalysis: Breaking ciphers in the real world.* Hoboken: John Wiley & Sons, Inc., str. 40-41.

[116] Stamp, M., Low, R. M. (2007). *Applied cryptanalysis: Breaking ciphers in the real world.* Hoboken: John Wiley & Sons, Inc., str. 41.

Prekidač S određuje koji od 3 prekidača u drugoj skupini mijenja svoj položaj za jedno mjesto. Kod početnih postavki stroja bitno je odrediti koji od 3 prekidača je takozvani brzi, središnji i spori prekidač. Prekidač S iz prve grupe ima 25 mogućih položaja, kao i svaki od prekidača iz druge skupine. Prekidač S pomakne se za jedno mjesto svaki puta prilikom šifriranja slova, kao i brzi prekidač, osim u slijedeća dva slučaja. Ako je prekidač S na 24. položaju tada se središnji prekidač pomiče. Ako je prekidač S na 23. položaju, a središnji prekidač na 23. položaju tada se spori prekidač pomiče za jedno mjesto. Iz svega navedenog se može zaključiti kako se prekidač S i jedan od prekidača iz druge skupine pomiču istovremeno prilikom šifriranja pojedinog slova.[117, 118]

S	L	M	R
20	0	10	7
21	1	10	7
22	2	10	7
23	3	10	7
24	4	10	7
0	4	11	7
1	5	11	7
2	6	11	7
3	7	11	7

S	L	M	R
20	0	24	4
21	1	24	4
22	2	24	4
23	3	24	4
24	3	24	5
0	3	0	5
1	4	0	5
2	5	0	5
3	6	0	5

Tablica 14. Princip rada prekidača[119]

Kako bi dešifrirali poruku stroj treba imati iste početne postavke kao prilikom šifriranja poruke. Postupak je obrnut. Izlazna tipkovnica i razvodna ploča sada se koriste za unos slova, a ulazna razvodna ploča i tipkovnica za izlaz. Permutacije su iste u obje razvodne ploče pa se može primijeniti zamjena.[120]

---

[117] Stamp, M., Low, R. M. (2007). *Applied cryptanalysis: Breaking ciphers in the real world.* Hoboken: John Wiley & Sons, Inc., str. 43-44.

[118] Freeman, W., Sullivan, G., Weierud F. (2003). PURPLE revealed: Simulation and computer-aided cryptanalysis of Angooki Taipu B. *Cryptologia*, 27(1), 1-43.

[119] Stamp, M., Low, R. M. (2007). *Applied cryptanalysis: Breaking ciphers in the real world.* Hoboken: John Wiley & Sons, Inc., str. 44.

[120] Stamp, M., Low, R. M. (2007). *Applied cryptanalysis: Breaking ciphers in the real world.* Hoboken: John Wiley & Sons, Inc., str. 42.

4.3.4. Napad na Purple

Purple se nije koristio na bojnom polju, nego samo za slanje tajnih poruka na diplomatskoj razini, odnosno za razmjenu poruka između japanskog ministarstva vanjskih poslova i veleposlanstava. Budući da nisu znali kako stroj izgleda, njegovo "probijanje" predstavljalo je za Amerikance izuzetno težak izazov.

Američka vojska angažirala je Friedmana, čiji su posao nastavili Rowlett i suradnici, za pothvat dešifriranja japanskih poruka slanih pomoću uređaja Purple. Zaključili su da je najbolji način za to izrada preciznih replika uređaja. Prvo na što su se orijentirali bilo je prikupljanje informacija o samom stroju. Dio mehanizma mogli su pretpostaviti oslanjajući se na prethodnu verziju uređaja, zvanu Red, kojeg su uspjeli "probiti". Amerikancima je dešifiriranje olakšalo i to što je zamjena starijih s novijim verzijama uređaja bila postupna, zbog čega su Japanci istovremeno slali iste poruke korištenjem oba sustava.[121] S vremenom su Amerikanci otkrili i obrazac koji su Japanci koristili u svojim dnevnim ključevima. Svaki mjesec se dijelio na 3 skupine od po 10 dana u kojima se razaznavao uzorak korištenja početnih postavki stroja. Naime, ključ prvog dana prve skupine od 10 dana je bio povezan s preostalih 9 dana na način da se početni ključ permutirao. Isto je vrijedilo i za druge dvije skupine. Dakle, poznavanjem početnog ključa relativno lako se mogao odrediti ključ za ostale dane u toj skupini.[122]

Iako je Purple bio izrazito kompleksan stroj za šifriranje, u svojoj strukturi imao je slabih točaka koje su Amerikanci iskoristili za dešifriranje njegovih poruka. Jedna od mana je bila podjela permutacije slova alfabeta u dvije skupine, takozvane "šestice" i "dvadesetice", čime je ograničen ukupan broj konfiguracija stroja. Mana uređaja je također bio fiksni broj korištenih prekidača čime je sigurnost uređaja bila manja nego kod strojeva baziranih na rotorima. Sve navedeno dovelo je do učinkovitog "razbijanja" mehanizma šifriranja, čime je japanska tajna komunikacija razotkrivena. Amerikanci su proizveli više replika uređaja Purple. Operacija dešifriranja japanskih poruka koje su šifrirane pomoću uređaja Purple nazvana je kodnim imenom Magija.[123]

---

[121] Stamp, M., Low, R. M. (2007). *Applied cryptanalysis: Breaking ciphers in the real world.* Hoboken: John Wiley & Sons, Inc., str. 45.

[122] Dooley, J. F. (2018). *History of cryptography and cryptanalysis: Codes, ciphers, and their algorithms*. Cham: Springer., str. 150

[123] Hatch, D. A. (2000). ENIGMA and PURPLE: How the Allies broke German and Japanese codes during the war. U D. Joyner (ur.), *Coding theory and cryptography: From Enigma and Geheimschreiber to quantum theory* (pp. 53-61). Berlin: Springer.

4.4. NAVAJO KOD

Šifriranje poruka pomoću elektromehaničkih uređaja pružao je visoki stupanj zaštite informacija. Međutim, sam proces je zahtijevao vremena, određeni broj ljudi te opreznost operatera pri korištenju uređaja. Kako bi izbjegli navedene nedostatke, Amerikanci su se dosjetili koristiti jezik Navajo domorodaca kao kod. Njihov jezik je bio izrazito kompleksan, nepoznat ostalim nacijama svijeta te nije imao svoje pismo (temeljen je isključivo na govoru). Upravo ovakav način prenošenja informacija je Amerikancima osigurao veliku prednost tijekom Drugog svjetskog rata.

Slika 19. Navajo govornici pridruženi američkoj ratnoj mornarici[124]

Philip Johnston je bio veteran iz Prvog svjetskog rata i sin misionara koji je živio među Navajo narodom te je stoga bio jedan od rijetkih Amerikanaca koji je bio upoznat s njihovim jezikom i kulturom. Smatra se kako je ideju korištenja Navajo jezika, kao vojnog koda, dobio nakon čitanja jednog članka u novinama. Članak je govorio o tome kako je američka vojska upotrebljavala jezik Indijanaca za šifriranje poruka.[125] Ubrzo nakon toga regrutirao je četiri Navajo govornika kako bi demonstrirao grupi američkih mornaričkih časnika svoju ideju. Pokazao je kako se brzo i

[124] Silversmith, S. (2019). *Navajo code talkers created an unbreakable code. It helped win World War II*. Dostupno na: https://eu.azcentral.com/story/news/local/arizona/2018/07/11/navajo-code-talker-facts-unbreakable-code/460262002/ (pristupljeno 26.10.2019.)

[125] Klima, R. E., Sigmon, N. P. (2013). *Cryptology classical and modern with Maplets.* Boca Raton: CRC Press., str. 104.

besprijekorno poruka na engleskom jeziku mogla prevesti na Navajo jezik. Ta poruka bi se zatim brzo i efikasno prenosila putem radija između dva Navajo govornika i naposljetku ponovno prevela na engleski jezik. Fascinirana ovom idejom, 1942. godine američka ratna mornarica regrutirala je 29 Navajo govornika u okviru pilot projekta.[126] Svaki od njih je morao proći osnove obuke marinaca, tečno govoriti i Navajo i engleski jezik te završiti intenzivan tečaj prijenosa poruka putem radija. Nakon uspješno završene obuke, postajali su službeni govornici Navajo koda.[127]

Prije nego je Navajo kod primijenjen u ratu, bilo je potrebno riješiti neke njegove nedostatke. Naime, Navajo jezik nije imao riječi za specifične vojne izraze na engleskom jeziku. Oni su se zato mogli prevesti u nejasno definirane izraze Navajo jezika, ali je tada postojala vjerojatnost primateljevog krivog shvaćanja poslane poruke. Kako bi riješili ovaj problem obučavatelji Navajo govornika su odlučili takve izraze doslovno prevesti izrazima iz prirodnog okruženja, za što je postojao prijevod na Navajo jezik. Tako su ptice korištene za avione, ribe za brodove i sl. Primjerice sova (da-he-tih-hi) je bila borbeni avion, žaba (chal) tenk, a željezna riba (besh-lo) podmornica.[128]

English word	Literal translation	Navajo code word
ABANDON	RUN AWAY FROM	YE-TSAN
AMERICA	OUR MOTHER	NE-HE-MAH
ASSAULT	FIRST STRIKER	ALTSEH-E-JAH-HE
BATTALION	RED SOIL	TACHEENE
BRITAIN	BETWEEN WATERS	TOH-TA
CAPTAIN	TWO SILVER BARS	BESH-LEGAI-NAH-KIH
DIVE BOMBER	CHICKEN HAWK	GINI
GERMANY	IRON HAT	BESH-BE-CHA-HE
ORDER	ORDER	BE-EH-HO-ZINI
SAILORS	WHITE CAPS	CHA-LE-GAI
SUBMARINE	IRON FISH	BESH-LO
THE	BLUE JAY	CHA-GEE

Tablica 15. Navajo kod za određene riječi na engleskom jeziku[129]

[126] Klima, R. E., Sigmon, N. P. (2013). *Cryptology classical and modern with Maplets.* Boca Raton: CRC Press., str. 104.
[127] Silversmith, S. (2019). *Navajo code talkers created an unbreakable code. It helped win World War II*. Dostupno na: https://eu.azcentral.com/story/news/local/arizona/2018/07/11/navajo-code-talker-facts-unbreakable-code/460262002/ (pristupljeno 10.11.2019.)
[128] Singh, S. (2001). *The code book.* New York: Delacorte Press. str. 155-156.
[129] Klima, R. E., Sigmon, N. P. (2013). *Cryptology classical and modern with Maplets.* Boca Raton: CRC Press., str. 105.

Međutim, i dalje je postojao problem prijevoda manje predvidljivih riječi te imena nekih ljudi i mjesta. Kao rješenje osmišljen je šifrirani alfabet. Tako se primjerice riječ "Pacifik" rastavila na slijedeći niz: svinja, mrav, mačka, led, lisica, led, jarac što bi se zatim prevelo u Navajo kao: bi-sodih, wol-la-chee, moasi, tkin, ma-e, tkin, klizzie-yazzi. Sve riječi i alfabet su bili zabilježeni u jednu kodnu knjigu. Kako kodna knjiga ne bi završila u rukama neprijatelja, Navajo govornici su naučili cijelu knjigu napamet. To za njih nije predstavljalo težak posao, jer su se njihova kultura i jezik temeljili samo na usmenoj predaji, a time i na dobroj memoriji.

A	Ant	**Wol-la-chee**	**N**	Nut	**Nesh-chee**
B	Bear	**Shush**	**O**	Owl	**Ne-as-jah**
C	Cat	**Moasi**	**P**	Pig	**Bi-sodih**
D	Deer	**Be**	**Q**	Quiver	**Ca-yeilth**
E	Elk	**Dzeh**	**R**	Rabbit	**Gah**
F	Fox	**Ma-e**	**S**	Sheep	**Dibeh**
G	Goat	**Klizzie**	**T**	Turkey	**Than-zie**
H	Horse	**Lin**	**U**	Ute	**No-da-ih**
I	Ice	**Tkin**	**V**	Victor	**A-keh-di-glini**
J	Jackass	**Tkele-cho-gi**	**W**	Weasel	**Gloe-ih**
K	Kid	**Klizzie-yazzi**	**X**	Cross	**Al-an-as-dzoh**
L	Lamb	**Dibeh-yazzi**	**Y**	Yucca	**Tsah-as-zih**
M	Mouse	**Na-as-tso-si**	**Z**	Zinc	**Besh-do-gliz**

Tablica 16. Abeceda Navajo koda[130]

Prvi pokušaji primjene Navajo koda su izazvali veliku pomutnju među stalnim operaterima signala koji nisu bili obaviješteni o novom kodu. Panično su slali poruke širom Amerike misleći kako Japanci spremaju novi napad. No, ubrzo su Navajo govornici dokazali svoju vrijednost na bojnom polju.[131] Zahvaljujući njima, Amerikanci uspijevaju osvojiti područja na Pacifiku i ostvariti nadmoć nad Japanom. Smatra se da je do kraja rata više od 400 Navajo govornika bilo angažirano na prenošenju Navajo koda. Iako su odigrali ključnu ulogu, priznanje za njihov rad i trud dobili su tek 20-ak godina nakon završetka Drugog svjetskog rata. Vrlo je važno naglasiti kako se metodama kriptoanalize nikada nije uspio "probiti" Navajo kod. Upravo ova činjenica dokazuje koliko je ovaj kod bio snažan, kompliciran i siguran, iako se temeljio samo na jeziku jednog naroda.[132]

[130] Singh, S. (2001). *The code book.* New York: Delacorte Press. str. 157.
[131] Singh, S. (2001). *The code book.* New York: Delacorte Press. str. 155-158.
[132] Klima, R. E., Sigmon, N. P. (2013). *Cryptology classical and modern with Maplets.* Boca Raton: CRC Press., str. 107.

5. SUVREMENO DOBA

Kriptografija, kao disciplina na raskrižju računarstva, matematike i elektrotehnike, dugo se vremena koristila gotovo isključivo u vojne i diplomatske svrhe. Danas je kriptografija sveprisutna. Sigurnosni mehanizmi koji se oslanjaju na kriptografiju sastavni su dijelovi svakog modernog informacijskog sustava. Upotreba kreditnih kartica i telefona, pristupanje računalnim mrežama, instaliranje ažuriranja softvera i plaćanje vožnje u javnom prijevozu samo su neki od primjera primjene kriptografije.[133]

Dva su događaja u cijelosti promijenila kriptografiju. Prvi od njih je predstavljalo stvaranje javnog standarda za šifriranje, zvanog DES. DES (Date Encryption Standard) je algoritam simetrične blokovne šifre koji radi na podacima u 64–bitnim blokovima koristeći 56–bitni ključ. Problem ovog algoritma je duljina ključa. Čak su elektromehanički strojevi za šifriranje poruka, poput Enigme u Drugom svjetskom ratu, imali veću duljinu. Poruke su se lako mogle dešifrirati i time je sigurnost prenošenja informacija bila upitna.[134] DES je 2001. godine zamijenjen naprednim standardom za šifriranje, poznat pod nazivom AES. To je također algoritam simetrične blokovne šifre, ali koji koristi 128-bitni ulazni blok i daje korisniku 3 izbora veličine ključa, 128-bitni, 192-bitni i 256-bitni. Povećanjem duljine ključa se povećala i zaštita podataka korisnika.[135]

Simetričnu kriptografiju je karakterizirao problem korištenja ključa. Pošiljatelj i primatelj su morali posjedovati isti ključ kako bi se poruka mogla šifrirati i dešifrirati. Taj isti ključ se morao koristiti ispravnim redoslijedom. Ovaj problem prevladan je pojavom asimetrične kriptografije. Whitifield Diffie i Martin Hellman 1976. godine objavili su rad u kojem su iznijeli novu metodu distribucije kriptografskih ključeva. Asimetrična kriptografija, za razliku od simetrične, koristi različite ključeve za šifriranje i dešifriranje poruke. Javni ključ koji je svima dostupan koristi se za šifriranje poruke, a tajni ključ za dešifriranje poruka je dostupan samo korisniku. Ovo je bio značajan napredak u razvoju moderne kriptografije.[136]

---

[133] Paar, C., Pelzl, J. (2010). *Understanding cryptography: A textbook for students and practitioners.* Berlin: Springer., str. vii.
[134] Dooley, J. F. (2018). *History of cryptography and cryptanalysis: Codes, ciphers, and their algorithms*. Cham: Springer., str. 169.
[135] Paar, C., Pelzl, J. (2010). *Understanding cryptography: A textbook for students and practitioners.* Berlin: Springer., str. 88
[136] Dooley, J. F. (2018). *History of cryptography and cryptanalysis: Codes, ciphers, and their algorithms*. Cham: Springer., str. 185, 192.

Kao posljedica ideje asimetrične kriptografije, kriptografi su počeli tražiti metode kojima bi se upotreba javnog ključa mogla realizirati. Ronald Rivest, Adi Shamir i Leonard Adleman su 1977. godine predložili shemu čija će upotreba biti raširena sve do danas. RSA (Rivest – Shamir – Adleman) je asimetrična kriptografska shema koja se pretežno koristi za šifriranje malih količina podataka, uglavnom za prijenos ključeva te za digitalne potpise. RSA algoritam šifriranja podataka pak ne zamjenjuje AES, iz razloga što je RSA nekoliko puta sporiji od AES-a. Štoviše, često se upotrebljavaju zajedno.[137] Danas metode kriptografije prate tehnološki razvoj i temelj su sigurnog prijenosa informacija.

[137] Paar, C., Pelzl, J. (2010). *Understanding cryptography: A textbook for students and practitioners.* Berlin: Springer., str. 173-174.

6. ZAKLJUČAK

Informacija je oduvijek imala posebno mjesto u ljudskom društvu. Iz podataka i informacija nastaju sve ljudske spoznaje. U suvremenom dobu, ona je postala najvažniji resurs. Informacija je također glavni element komunikacije koja se kroz povijest odvijala na razne načine. Od pojave pisma pa sve do izuma pametnih aplikacija i uređaja komunikacija se nastoji temeljiti na točnom, brzom, sigurnom i efikasnom prijenosu informacija. S ciljem ostvarenja sigurne i tajne komunikacije razvila se disciplina koja se naziva kriptografija. Kriptografija se bavi raznim metodama i algoritmima šifriranja i kodiranja poruka kako bi njezin sadržaj bio poznat samo onima kojim je ta poruka namijenjena.[138]

U radu su navedeni brojni primjeri kriptografije, pri čemu je glavno mjesto zauzela njezina upotreba u Drugom svjetskom ratu. Upravo se na primjerima iz rada najjasnije uočava razlika između uspješnog i neuspješnog šifriranja. Američka SIGABA je u odnosu na njemačku Enigmu i japanski Purple imala prednost u duljini ključa te u kompleksnosti samog uređaja. Ne smije se zaboraviti ni dosjetljivost upotrebe zahtjevnog i relativno nepoznatog jezika američkih Indijanaca s ciljem šifriranja poruka. Razbijanjem njemačkih i japanskih sustava šifriranja Saveznici su nedvojbeno dobili značajnu prednost na bojnom polju. Kriptografi i kriptoanalitičari tako su dali veliki obol pobjedi Saveznika u Drugom svjetskom ratu.

S razvojem društva i tehnologije, kriptografija je prestala biti područje koje je prvenstveno interesantno vojsci i diplomaciji. Od sedamdesetih godina prošlog stoljeća kriptografija je snažno zakoračila u praktički sva područja ljudskog djelovanja. Danas je kriptografija dio digitalnog svijeta koji nas okružuje i dostupna je na dlanu svakom od nas. I stručnjacima je ponekad teško pratiti njezin nagli razvoj. S obzirom na opasnosti i rizike okruženja u kojem živimo, u kojem se mnoštvu informacija koje se odnose na nas može pristupiti u samo nekoliko klikova na računalu ili pametnom telefonu, i u kojem su mogućnosti zloupotrebe takvih informacija izuzetno velike, kriptografija će samo dodatno dobivati na važnosti. Već danas, a poglavito u vremenu koje dolazi, kriptografija se nameće kao glavni jamac sigurnosti komunikacije i zaštite privatnosti.

[138] Vesić, N. O., Simjanović, D. J. (2014). Matrix-based algorithm for text-data hiding and information processing. *Vojnotehnički glasnik*, 62(1), 42-57.

7. LITERATURA

1. Alonso, A., Molenberghs, G. (2008). Evaluating time to cancer recurrence as a surrogate marker for survival from an information theory perspective. *Statistical Methods in Medical Research*, 17(5), 497-504.
2. Carter, F. (2010.) *The Turing Bombe*. Dostupno na: http://www.rutherfordjournal.org/article030108.html (pristupljeno 26.10.2019)
3. Churchhouse, R. (2004). *Codes and ciphers: Julius Caesar, the Enigma and the internet.* Cambridge: Cambridge University Press.
4. Cimino, A. (2017). *The story of codebreaking.* London: Arcturus Publishing Limited.
5. Crypto Museum (2009). *Working principle of the Enigma.* Dostupno na: https://www.cryptomuseum.com/crypto/enigma/working.htm (pristupljeno 24.10.2019.)
6. Crypto Museum (2019). *SIGABA*. Dostupno na: https://www.cryptomuseum.com/crypto/usa/sigaba/index.htm pristupljeno (25.10.2019.)
7. Crypto Museum. (2012). *Bombe*. Dostupno na: https://www.cryptomuseum.com/crypto/bombe/ (pristupljeno 25.10.2019.)
8. Curley, R. (2013). *Cryptography: Cracking codes*. London: Britannica Educational Publishing.
9. Čavrak, H. (2004). Enigma. *Math.e: Hrvatski matematički elektronički časopis, 3.* Dostupno na: http://e.math.hr/old/enigma/index.html (pristupljeno 23.10.2019.)
10. De Leeuw, K., Bergstra, J. (2007). *The history of information security: A comprehensive handbook*. Amsterdam: Elsevier.
11. Deutsches Museum (2019). *Enigma*. Dostupno na: https://www.deutsches-museum.de/sammlungen/meisterwerke/meisterwerke-ii/enigma/enigma-grossansicht2/ (pristupljeno 11.10.2019.)
12. Dnoenosova, G. A. (2012). Document properties. *Scientific and Technical Information Processing*, 39(4), 220-228.
13. Dooley, J. F. (2018). *History of cryptography and cryptanalysis: Codes, ciphers, and their algorithms*. Cham: Springer.
14. Dujella, A., Maretić, M. (2007). *Kriptografija.* Zagreb: Element.
15. Ellis, C. (2005). Exploring the Enigma. *Plus magazine.* Dostupno na: https://plus.maths.org/content/exploring-enigma (pristupljeno 23.10.2019.)

16. Freeman, W., Sullivan, G., Weierud F. (2003). PURPLE revealed: Simulation and computer-aided cryptanalysis of Angooki Taipu B. *Cryptologia*, 27(1), 1-43.
17. George C. Marshall Foundation. (2014). *Type 97 cypher machine*. Dostupno na: https://www.marshallfoundation.org/blog/marshall-purple-pearl-harbor/664px-type_97_cypher_machine/ (pristupljeno 26.10.2019.)
18. Grime, J. (n.d.). *Maths from the talk: "Alan Turing and the Enigma machine"*. Dostupno na: http://www.singingbanana.com/enigmaproject/maths.pdf (pristupljeno 24.10.2019.)
19. Hatch, D. A. (2000). ENIGMA and PURPLE: How the Allies broke German and Japanese codes during the war. U D. Joyner (ur.), *Coding theory and cryptography: From Enigma and Geheimschreiber to quantum theory* (pp. 53-61). Berlin: Springer.
20. Igrec, A. (2016). Skrivene poruke. *Matka*, 24(96), 222-228.
21. Kahn, D. (1973). *The codebreakers.* New York: Macmillan Company.
22. Klaić, B. (2001). Rječnik stranih riječi. Zagreb: Nakladni zavod Matice hrvatske.
23. Klima, R. E., Sigmon, N. P. (2013). *Cryptology classical and modern with Maplets.* Boca Ration: CRC Press.
24. Konheim, A. G. (2007). *Computer security and cryptography.* New Jersey: John Wiley & Sons, Inc.
25. Lasry, G. (2019). A practical meet-in-the-middle attack on SIGABA. U E. Antal, K. Schmeh, (ur.), *Proceedings of the 2nd International Conference on Historical Cryptology* (str. 41-49). Linköping: Linköping University Electronic Press.
26. Mucklow, J. T. (2015). *The SIGABA / ECM II cipher machine:"A beautiful idea"*. Fort George G. Meade: National Security Agency.
27. Newton, D. E. (1997). *Encyclopedia of cryptography.* Santa Barbara: Instructional Horizons.
28. Oberzalek, M. (2000). *What is the Enigma cipher machine?* Dostupno na: http://www.mlb.co.jp/linux/science/genigma/enigma-referat/node3.html (pristupljeno 11.10.2019.)
29. Paar, C., Pelzl, J. (2010). *Understanding cryptography: A textbook for students and practitioners*. Berlin: Springer.
30. Pandžić, I. S., Bažant, A., Ilić, Ž., Vrdoljak, Z., Kos, M., Sinković, V. (2007). *Uvod u teoriju informacije i kodiranje*. Zagreb: Element d.o.o.
31. Pekelney, R. (2006). *Operating instructions for ASAM 1 (a.k.a. ECM Mark II).* Dostupo na: https://maritime.org/tech/ecminst.htm (pristupljeno 26.10.2019.)
32. Rijmenants, D. (2004). *Enigma message procedures*. Dostupno na: http://users.telenet.be/d.rijmenants/en/enigmaproc.htm (pristupljeno 24.10.2019.)

33. Shashank (2019). *What is cryptography?*. Dostupno na https://www.edureka.co/blog/what-is-cryptography/ (pristupljeno 05.10.2019.)
34. Short, K., Dagan A. (2013). An examination of the components and mathematics of the Enigma electromechanical rotor chipers. *Journal of Young Investigators*, 25(5), 33-40.
35. Silversmith, S. (2019). *Navajo code talkers created an unbreakable code. It helped win World War II*. Dostupno na: https://eu.azcentral.com/story/news/local/arizona/2018/07/11/navajo-code-talker-facts-unbreakable-code/460262002/ (pristupljeno 26.10.2019.)
36. Simpson, R. (2016). *Cipher machines*. Dostupno na: https://ciphermachines.com/enigma (pristupljeno 24.10.2019.)
37. Singh, S. (2001). *The code book.* New York: Delacorte Press.
38. Smart, N. P. (2016). *Cryptography made simple.* Cham: Springer.
39. Stamp, M., Low, R. M. (2007). *Applied cryptanalysis: Breaking ciphers in the real world.* Hoboken: John Wiley & Sons, Inc.
40. Sterling, C. H. (2008). *Military communications: From ancient times to the 21st century.* Santa Barbara: ABC-CLIO.
41. Tang, L., Lee, N., Russo, S. (2018). *Breaking Enigma.* Dostupno na: https://courses.csail.mit.edu/6.857/2018/project/lyndat-nayoung-ssrusso-Enigma.pdf (pristupljeno 24.10.2019.)
42. Verma, P. K., El Rifai, M., Chan, K.W.C. (2019). *Multi-photon quantum secure comunication.* Singapore: Springer.
43. Vesić, N. O., Simjanović, D. J. (2014). Matrix-based algorithm for text-data hiding and information processing. *Vojnotehnički glasnik*, 62(1), 42-57.
44. Weisstein, E. W. (2019). *Multiplication principle*. Dostupno na: http://mathworld.wolfram.com/MultiplicationPrinciple.html (pristupljeno 23.10.2019.)
45. Zulkifli, M. Z. W. M. (2007). *Evolution of cryptography*. Dostupno na http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.698.2641&rep=rep1&type=pdf (pristupljeno 5.10.2019.)

8. ŽIVOTOPIS

Doris Mršić rođena je 1. listopada 1993. godine u Osijeku. Pohađala je Osnovnu školu "Antunovac" u Antunovcu. Nakon završetka osnovne škole, 2008. godine upisuje I. gimnaziju u Osijeku. Maturirala je 2012. godine, a školovanje je nastavila na Sveučilišnom preddiplomskom studiju Fizike na Odjelu za fiziku Sveučilišta Josipa Jurja Strossmayera u Osijeku. Po završetku preddiplomskog studija, na istom Odjelu upisuje Sveučilišni diplomski studij Fizike i informatike. Dugi niz godina aktivno je trenirala odbojku. Po završetku studija planira usavršiti engleski jezik te naučiti njemački jezik.