Kriptologija u Drugom svjetskom ratu

Vlahović, Toma

SVEUČILIŠTE U ZAGREBU
FILOZOFSKI FAKULTET
ODSJEK ZA INFORMACIJSKE I KOMUNIKACIJSKE ZNANOSTI
Ak. god. 2020./ 2021.

Toma Vlahović

Kriptologija u Drugom svjetskom ratu

Završni rad

Mentori: dr. sc. Tomislava Lauc
dr. sc. Vjera Lopina

Zagreb, lipanj 2021.

Izjava o akademskoj čestitosti

Izjavljujem da je ovaj rad rezultat mog vlastitog rada koji se temelji na istraživanjima te objavljenoj i citiranoj literaturi. Izjavljujem da nijedan dio rada nije napisan na nedozvoljen način, odnosno da je prepisan iz necitiranog rada, te da nijedan dio rada ne krši bilo čija autorska prava. Također izjavljujem da nijedan dio rada nije korišten za bilo koji drugi rad u bilo kojoj drugoj visokoškolskoj, znanstvenoj ili obrazovnoj ustanovi.

potpis

_____

Toma Vlahović

Veliku zahvalu dugujem prof. dr. sc Vjeri Lopini koja me svojim stručnim savjetima i brzim ispravcima vodila kroz ovaj završni rad.

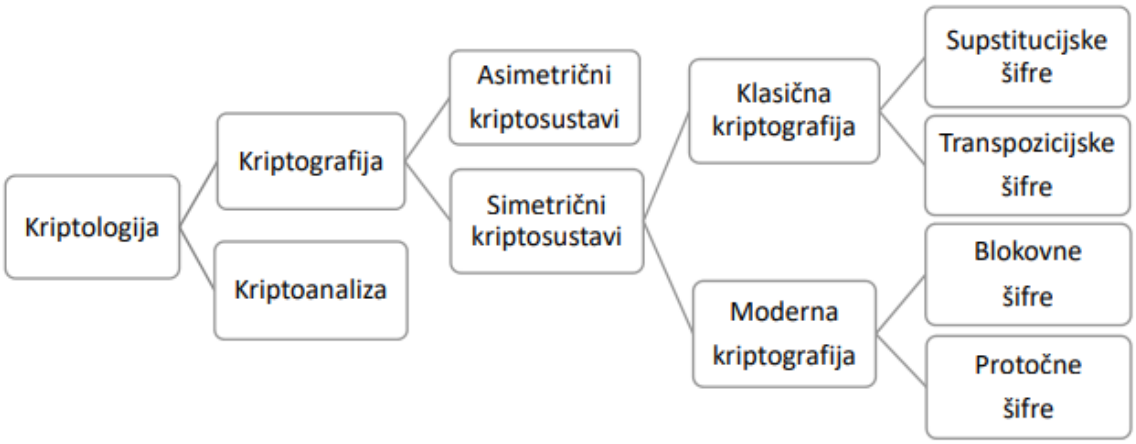
Sadržaj

1. Uvod

Teško bi bilo sa sigurnošću utvrditi kada je čovjek po prvi put počeo koristiti različite metode za skrivanje određenih poruka i prikrivanje nekog tipa komunikacije, naravno, šifriranjem i kodovima. To je jedan od onih fenomena za čije bi se razjašnjenje trebalo posegnuti za dokazima iz daleke prošlosti, a ni tada se ne bi moglo samouvjereno tvrditi da smo otkrili jasne korijene nečega što je danas tako poznato, a u određenim trenucima i situacijama i iznimno važno. Pitanje kriptologije, kripotografije i kriptoanalize čini izuzetno zanimljivo područje unutar znanosti i ljudske prakse, izvrstan je pokazatelj razvitka čovjekova razmišljanja i mentalnih sposobnosti općenito, a nadasve je vjeran svjedok određena vremena i potrebe za konkretnim djelovanjem u naizgled bezizlaznim situacijama. Takvo je razdoblje svakako bio Drugi svjetski rat, najveći i najstrašniji vojni sukob u ljudskoj povijesti čiji su aspekti i „otvorena“ poglavlja do danas predmet burnih rasprava i iscrpnih proučavanja. U ovom će se radu nastojati pružiti kratak prikaz jedne drukčije slike ratovanja, naličje rata gdje se drukčijim sredstvima pokušavalo nadmudriti i razotkriti neprijatelja, oduzeti mu prednost i učiniti bitnu prekretnicu u tijeku sukoba. Upravo su tu bile ključne kriptografske aktivnosti i stoga će se u nastavku, nakon kratkog povijesnog pregleda razvitka kriptologije, prikazati temeljna obilježja i način funkcioniranja danas već legendarnih strojeva poput *Enigme, Lorenza* ili *Purplea* te istaknuti njihovu važnost ne samo u konkretnom razdoblju i uvjetima u kojima su korišteni, nego i njihov cjelokupan značaj za napredak kriptologije i utvrđivanje njezina mjesta u informacijskoj znanosti.

2. Kriptologija – osnovni pojmovi i povijesni pregled

Kriptologija je znanost koja se bavi komunikacijom i pohranom podataka u sigurnom i tajnom obliku, te obuhvaća kriptoanalizu i kriptografiju. Što se tiče etimologije, kriptologija kao i mnoge druge riječi dolazi od grčkog *kryptos* (skriven) i *logos* (znanje). Prema Rošić (2018.) kriptologija je znanost koja se bavi proučavanjem i definiranjem metoda za zaštitu informacija (šifriranjem) i proučavanjem i pronalaženjem metoda za otkrivanje šifriranih poruka (dešifriranje). Kriptologija obuhvaća dvije znanstvene discipline: kriptografiju i kriptoanalizu. Rezultate kriptologije prvenstveno koriste oružane snage i diplomatska služba, a razvojem telekomunikacija i mnoge druge službe.



Slika 1. Podjela kriptologije (Izvor: Mršić, 2019.)

Kriptosustave prema ključu možemo podijeliti na simetrične i asimetrične. Simetrični kriptosustavi su oni koji koriste samo jedan tajni ključ za šifriranje i dešifriranje poruka, a asimetrični koriste dva različita ključa (tajni ključa za šifriranje i javni za dešifriranje). Sva je kriptografija, od antike pa sve do druge polovine 20. stoljeća, temeljena na kriptosustavima simetričnog ključa. Slika 1 prikazuje podjelu kriptologije na kojoj možemo vidjeti kako se simetrični kriptosustavi dijele na modernu i klasičnu kriptografiju. Klasična se dijeli na supstitucijske i transpozicijske šifre, a moderna na blokovne i protočne šifre. Kod supstitucijskih šifri se svaki element otvorenog teksta zamjenjuje drugim elementom, a kod transpozicijskih elementi otvorenog teksta se premještaju. Na drugoj strani se nalaze blokovne šifre kod kojih se jedan po jedan blok elementa otvorenog teksta obrađuje koristeći jedan ključ

i protčne šifre kod kojih se elementi otvorenog teksta obrađuju jedan po jedan koristeći niz ključeva koji se generiraju. (Mršić, 2019.)

Slika 2. Shematski prikaz kriptografije (Izvor: Mršić, 2019.)

„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.“ (Mršić,2019.)

Kriptoanaliza je znanstvena disciplina koja proučava metode otkrivanja značenja šifriranih informacija bez korištenja tajnih informacija za dešifriranje. Cilj je kriptoanalize pronalazak tajnog ključa i samo probijanje kriptirane poruke.

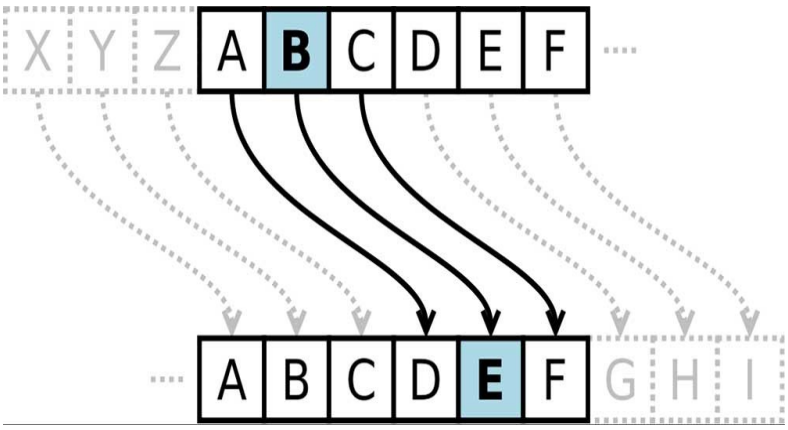
Kriptografija je također znanstvena disciplina koja se bavi metodama očuvanja tajnosti informacija te korištenjem kodova pazi da se informacijama mogu služiti samo oni kojima su one namijenjene. Drugim riječima, temeljni je cilj kriptografije omogućiti prijenos tajne informacije javnim kanalom. (Xifré Solana 7) Ovakvo pitanje komunikacije bilo je od velikog interesa još u antici, a još se uvijek smatra vitalnom, prije svega zbog sve veće informatizacije društva i činjenice da milijuni računala konstantno razmjenjuju informacije putem interneta,

svemoćne „svemreže“. (*Ibid.*) Stoga se može zaključiti da je primarni cilj kriptologije, odnosno kriptografije garancija tajnosti komunikacije između dviju strana (ljudi, organizacija...) i utvrđivanje autentičnosti informacije. (*Ibid.*)

Kao što je već istaknuto, kriptologija ima dugu povijest, usko vezanu uz samu pojavu i razvoj pisma. Mnogi su pismovni sustavi do danas nepoznanica, oni su šifre koje se još nisu uspjele razbiti. Dovoljno se sjetiti kretskog lineara A ili diska Faista, diska načinjena od spaljene gline koji sadrži 45 simbola čije je značenje još uvijek misterij, usprkos svim naporima koje su suvremeni informatički sustavi uložili u njegovo dešifriranje. (Gutiérrez 63) Kasnije su i stari Grci koristili različite metode enkripcije: neki su se temeljili na tome da se poruka skrije bez šifriranja, unutar druge poruke ili fizičkog objekta (steganografija), a neki su domišljato koristili robove pa su tako na njihovu tijelu, primjerice tjemenu, pisali poruke koje bi poslije skrila izrasla kosa.

Slika 3. DiskFaist (Izvor: sk.wikipedia.org)

Jedan od prvih i najpoznatijih načina šifriranja je Cezarova šifra. To je jednostavan oblik supstitucijske šifre kojoj je ključ zapravo broj pomaka, a on govori u koja slova prelaze slova poruke tj. primjerice slovo A kod pomaka 3 prelazi u D, B u E itd. Dakako, danas bi se ovakve metode šifriranja kao što je bila Cezarova činile smiješnima i djetinjastima te nipošto ne bi predstavljale izazov kriptoanalitičaru, ali treba ih prosuđivati imajući u vidu povijesni okvir u kojem su nastale. Činjenica je da je zahvaljujući tom šifriranju veliki Rimljanin pobijedio u mnogim bitkama, a i promijenio tijek ratova.



Slika 4. Cezarova šifra (Izvor: https://hr.izzi.digital/DOS/320/1095.html)

Veliki je zaokret i napredak u kriptologiji predstavljala analiza učestalosti. Sve je krenulo od nekolicine arapskih učenjaka i proučavanja svetih spisa, a metoda se može sažeti ovako: ako se svako slovo u nekom tekstu šifrira kao drugo slovo koje je uvijek isto (jednoabecedna šifra), šifrirano se slovo treba pojaviti s jednakom učestalošću u oba teksta, izvornom i šifriranom. Na taj je način moguće zaključiti koji šifrirani znakovi odgovaraju kojem slovu. (Gutiérrez 64) Ovo je otvorilo put višeabecednim supstitucijskim šiframa, a genijalna je primjena takvog sustava Albertijev disk u 15. stoljeću.

Slika 5. Albertijev disk (Izvor: http://www.mathos.unios.hr/~mdjumic/uploads/diplomski/ANT21.pdf)

Leon Battista Alberti je prvi predložio upotrebu dvaju ili više šifriranih alfabeta i njihovo izmjenjivanje prilikom šifriranja. Ovakav način je bio bolji u odnsou na prošle zbog toga što se ista slova u otvorenom tekstu ne moraju pojaviti kao ista slova u šifriranom tekstu. Alberti

je također i izumitelj naprave za šifriranje koja se zove Albertijev disk, a sastojao se od dviju ploča različitih polumjera koje su položene jedna na drugu te šiljka koji prolazi središtem tih ploča. Svaka je ploča podjljena na 24 jednaka dijela pri čemu su na gornjoj nepokretnoj ploči ispisana slova latinskog alfabeta, izuzev j, u, w, i brojevi od 1 do 4. Na donjoj rotirajućoj ploči su izmješana sva slova latinskog alfabeta i znak &. Poruka se šifrirala tako što bi se dogovorno uzelo jedno slovo koje bi bilo indikator promjene pri čemu je gornja ploča predstavljala otvoreni tekst, a donja šifrirani. (Mršić, 2019.)

Ono što naposljetku igra bitnu ulogu jest da su u 19. stoljeću kriptologija, kriptografija i kriptoanaliza ponovno otkrivene, a tijekom dva ključna događaja 20. stoljeća zadobile su vrijednost koju imaju danas. Riječ je o naravno, dva svjetska rata, a u nastavku rad će se baviti kriptologijom i njezinom ulogom u Drugom svjetskom ratu.

3. Njemačka kriptologija

3.1. Povijesni pregled

Tijekom prve dvije godine Prvog svjetskog rata, kodni sustavi koristili su se za zapovjedništvo i diplomatske komunikacije, baš kao i stoljećima, a šifrirani sustavi koristili su

se gotovo isključivo za taktičke komunikacije. Sustavima terenskih šifri kao što su diskovne šifre američkog Signalnog korpusa nedostajalo je sofisticiranosti i sigurnosti. Ipak, do kraja rata za komunikaciju na visokoj razini koristili su se neki komplicirani sustavi šifri, od kojih je najpoznatiji bio njemački ADFGVX.

Komunikacijske potrebe telegrafa i radija te sazrijevanje mehaničke i elektromehaničke tehnologije udružile su se 1920-ih kako bi donijele velik napredak u kripto strojevima razvojem strojeva s rotorskim šiframa. Iako je koncept rotora predviđen u starijim mehaničkim šifriranim diskovima, Amerikanac Edward H. Hebern je 1917. godine prepoznao da bi se povezivanjem monoalfabetske supstitucije u vezama iz kontakata s jedne strane električnog diska (rotora) na kontakte s druge strane, a zatim kaskadiranjem kolekcija takvih rotora, mogle realizirati polialfabetske zamjene gotovo proizvoljne složenosti. U radu, rotori u nizu pružaju električni put od kontakta do kontakta kroz sve rotore. U pravocrtnom sustavu rotora, zatvaranje ključnog kontakta na tipkovnici sličnoj pisaćoj mašini šalje struju na jedan od kontakata na krajnjem rotoru. Struja zatim prolazi kroz labirint međusobnih veza definiranih preostalim rotorima u nizu i njihovim relativnim rotacijskim položajima do točke na izlaznoj završnoj ploči, gdje je spojena na pisač ili indikator, čime se izbacuje šifrirani tekst.

Do 2003. godine Hebern je bio općenito priznat kao izumitelj rotorskoga stroja za šifriranje. Te godine znanstvenici su objavili istraživanje koje je pokazalo da su 1915. godine, dvije godine prije Hebernova rada, rotorski stroj dizajnirala i izradila dvojica nizozemskih mornaričkih časnika; R.P.C. Spengler i Theo van Hengel, te zatim drugi prototip koji je izgradio nizozemski inženjer strojarstva i bežični operater W.K. Maurits za mornaricu. Mornarica je međutim odbila nastaviti s projektom, a sudionici nisu odmah zatražili patent. Na kraju Prvog svjetskog rata Spengler i van Hengel pokušali su patentirati svoju ideju, ali mornarica se opirala deklasificiranju njihova rada. U međuvremenu, Hebern je 1917. podnio patentni zahtjev, koji se zadržao tijekom godina, i postupno su nizozemski izumitelji zaboravljeni.

Počevši od 1921. i nastavljajući kroz sljedeće desetljeće, Hebern je konstruirao niz stalno poboljšavajućih rotorskih strojeva koje je ocjenjivala američka vojska. Dvadesete godine prošlog stoljeća obilježene su nizom izazova izumitelja strojeva za šifriranje nacionalnih kriptoloških usluga i jedne službe za druge, što je rezultiralo stalnim poboljšanjem i kriptomašina i tehnika za analizu strojnih šifri. Gotovo u isto vrijeme kad je Hebern razvijao stroj za rotorsku šifru u Sjedinjenim Državama, europski inženjeri, posebno Arthur Scherbius iz Njemačke, neovisno su otkrili koncept rotora i dizajnirali strojeve koji su postali preteča

najboljih poznatih strojeva za šifriranje u povijesti, kao što je njemačka Enigma korištena u Drugom svjetskom ratu.

3.2. Enigma

Kada se govori o kriptologiji u Drugom svjetskom ratu vjerojatno je prvo što treba spomenuti njemačka *Enigma*. Riječ je o elektromehaničkom stroju za šifriranje koji je vanjskom konstrukcijom nalikovao na obični pisaći stroj, samo što je umjesto valjka koji pridržava papir imao ploču s 26 lampica, a na poklopcu iznad svake lampice bilo je otisnuto pojedino slovo abecede, od A do Z. (Derenčin 2015.)

Mowry (2014.) navodi kako je standardna vojna *Enigma* imala crne plastične rotore, odnosno cilindre s velikim pomičnim kotačem na jednom kraju i s abecedom ili brojevima na perimetru. Treba svakako reći da je izumitelj poznatog stroja njemački inženjer Arthur Scherbius koji je nakon iskustva s Zimmermanovim telegramom iz Prvog svjetskog rata radio na razvoju novih metoda za sigurnu vojnu i diplomatsku komunikaciju. Postojala su ukupno četiri tipa: Enigma A, B, C i D. Upravo su zadnja dva imala golem uspjeh, bila su manje mase i obujma, a sadržala su i četvrti rotor, tzv. reflektor, koji se nije micao za razliku od ostalih i svrha mu je bila omogućiti recipročnost procesa šifriranja. To znači da je pošiljatelj tajne poruke pisao slova u izvornom obliku, a njihove su se šifrirane varijante reflektirale na ploči. Primatelj je poruke, s druge strane, trebao samo napisati šifrirani tekst i u tom bi se slučaju izvorna slova reflektirala na ploči. (Gutiérrez, 70)

Čitav je proces bio izuzetno bitan, nerijetko i kompliciran. Derenčin detaljno opisuje postupak rada stroja i način na koji se koristio u njemačkim podmornicama:

„Nakon što je Enigma pripremljena, operater bi počeo proces šifriranja poruke: pritisnuo bi prvo slovo otvorene poruke na tipkovnici, iz baterije bi potekla struja prema dijelu s utičnicama, zatim prema rotorima, prošla bi kroz krajnje desni, srednji i krajnje lijevi rotor, došla do reflektora koji ju je vraćao nazad kroz krajnje lijevi, srednji i krajnje desni rotor, zatim bi struja ponovno došla do dijela s utičnicama, a naposljetku bi došla do jedne od lampica koja bi dolaskom struje zasvijetlila. Na poklopcu osvijetljene lampice nalazilo se otisnuto slovo. Operater bi, još uvijek pritišćući tipku na tipkovnici, pročitao i zapisao osvijetljeno slovo. Nakon toga bi pritisnuo drugo slovo otvorene poruke i tako sve do kraja otvorene poruke.

Vojne su Enigme imale samo slova, nije bilo tipki za brojke i interpunkciju. Mornarica je brojeve pisala kao NULA, JEDAN, DVA itd. X je bila točka, Y je bio zarez, UD je bio upitnik itd.“ (Derenčin, 2016.)

Citirani primjer opisuje rad tipa C, ali put je struje od baterije do lampice bio isti i kod tipa D, samo što je struja prolazila kroz još jedan rotor. Sve to pokazuje da je reflektor bio iznimno važan, ali treba ipak reći da su reflektori bili odgovorni i za najslabiju stranu *Enigme*, a to je da nijedno slovo nikad nije moglo biti šifrirano samim sobom: moglo se beskonačno pritiskati određeno slovo na tipkovnici, a da ne zasvijetli lampica na čijem je poklopcu bilo otisnuto to slovo. Upravo su tu pogrešku, točnije nedostatak, kasnije iskoristili Britanci pri dekriptiranju. (Rijmenants, 2014.)

Slika 6. Enigma (Izvor: http://pixelizam.com/wp-content/uploads/2013/11/Enigma-1.jpg)

Scherbiusova tvrtka je osim komercijalnih verzija razvila i neke sofisticiranije modele koji su se isključivo koristili u vojsci Trećeg Reicha. U njima se proširivao broj raspoloživih rotora, modificirao se reflektor da bi se mogao također promijeniti i smještati na različite položaje, a posebice je važno da se uvode novi tipovi poveznica između tipkovnice i prvog rotora koje su razmjenjivale jedno slovo za drugo po volji samog operatera te se na taj način uspjelo modificirati izvorno šifriranje na nepredvidljiv način. (Gutiérrez, 71)

3.2.1. Probijanje Enigme

Prema Callahan (2013.) Poljaci su bili prvi koji su se počeli baviti probijanjem Enigme. Tako su 1932. godine Marian Rejewski, Henryk Zygalski i Jerry Rożycki uspješno razbili prvu

varijantu Enigme. Njihov se uspjeh temeljio na čistoj matematičkoj analizi, potpomognutom informacijama njemačkog špijuna HansaThila Schmidta te komercijalne Enigme presretnute u poljskoj pošti. Upotrijebili su komercijalnu enigmu i prikupljene podatke kako bi je pretvorili u vojnu. Stvar je bila i u tome da su Nijemci koristili vrlo jednostavnu shemu upravljanja ključevima u kojoj je nasumično odabrani ključ poruke dva puta poslan u šifriranom obliku na početku svake poruke. Nijemci su 1936. promijenili način šifriranja mijenjajući broj kotačića odnosno prestaju koristiti 6 i koriste od 5 do 8. Rejewski je zbog toga razvio stroj za pomoć u izradi kataloga koji se zvao ciklometar. Taj katalog je sadržavao i duljinu i broj ciklusa za sve položaje kotačića i za svaki mogući redoslijed kotačića. Izrada je trajala godinu dana, ali je Poljacima omogućila ponovno probijanje Enigme. Zbog toga 1938. Nijemci u potpunosti mijenjaju postupak šifriranja ključeva što čini katalog beskorisnim. To je Poljake potaklo da osmisle novo rješenje, stroj nazvan Bomba, a ona se temelji na principu da se nasumični ključ poruke od 3 slova šalje dva puta na početku svake poruke i da svako malo, određeno slovo otvorenog teksta, daje isto šifrirano slovo tri mjesta dalje. Na temelju svih informacija dobivenih od Poljaka, Alan Turing je razvio stroj koji je mogao oporaviti ključne postavke čak i ako bi Nijemci odustali od dvostruke enkripcije ključa na početku svake poruke. Ovaj se stroj zvao Bombe, slično kao i poljski, ali je u usporedbi s poljskom bombom Turing koristio potpuno drugačiji pristup. Ubrzo je i Bombe poboljšan dodavanjem „dijagonalne ploče“ koju je izumio Gordon Welchman. Ovaj je Welchmanov izum uvelike smanjio broj koraka potrebnih za probijanje koda. Bombe sa Welchmanovom dijagonalnom pločom proizveden je 1940. u kolovozu i nazvan je „Agnus Dei“.

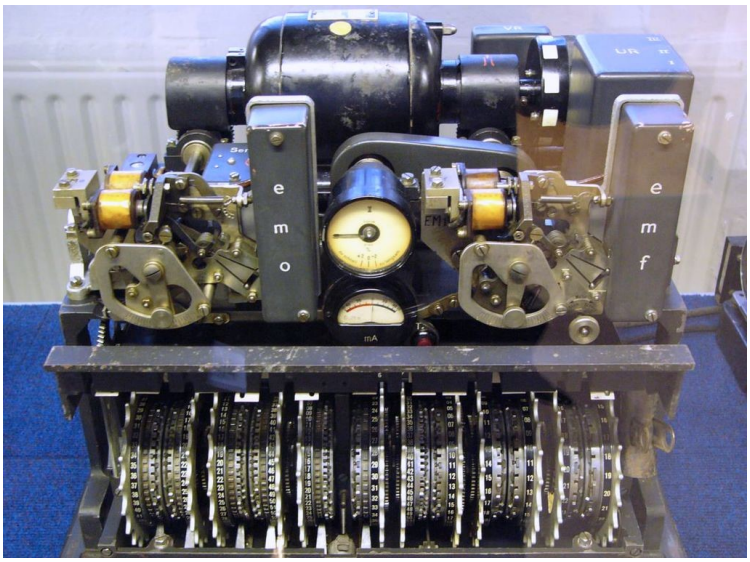
Tijekom rata napravljeno je 200 ovakvih strojeva kako bi se izbjegao rizik njihovog gubitka u slučaju bombaškog napada ili nečeg sličnog. Strojevi su bili raširenи između Bletchley Parka i njegovih takozvanih postaja u Wavendonu, Adstocku, Gayhurstu, Eastcoteu, i Stanmoreu gdje su njima upravljali najčešće RAF tehničari.

3.3. Lorenz SZ

Priča o Enigmi prilično je poznata s obzirom na to da je dobila relativno široku pokrivenost na televiziji i radiju, a bila je i tema filmova i knjiga. Nasuprot tome, javnost

uglavnom nije bila svjesna napada Bletchley Parka na Lorenza, pa čak ni postojanja samog Lorenza. U mnogim aspektima probijanje Lorenza dio je povijesti koji nedostaje i to je u velikoj mjeri zato što se Lorenz držao u tajnosti otprilike šezdeset godina nakon rata.

Vrhovno zapovjedništvo njemačke vojske zatražilo je od tvrtke Lorenz da za njih proizvede stroj za šifriranje teleprintera visoke sigurnosti koji bi im trebao omogućiti komunikaciju putem radija u potpunoj tajnosti. Tako je 1941. dizajniran šifrirni stroj zasnovan na aditivnoj metodi za šifiranje teleprinter poruka koju je osmislio američki inženjer Gilbert Vernam 1918. Teleprinteri se nisu temeljili na abecedi od 26 slova i Morseovom kodu o kojima je ovisila Enigma, već koriste Baudotov kod od 32 simbola. Baudotov kod zamjenjuje svako slovo s 5 električnih impulsa ili baudova, predstavljenih s „+“ (oznaka) ili 0 (razmak). Algoritam kojeg koristi ovaj stroj temelji se na XOR logici, a operacije se kod zakrivanja poruke provode na bitovima jasnopisa i ključa. (Pađen, 2018)



Slika 7. Lorens SZ (Izvor: https://en.wikipedia.org/wiki/Lorenz_cipher)

3.3.1. Njemačka pogreška

Kako se broj presretanja, koji se sada vrše u Knockholtu u Kentu, povećavao, u parku Bletchley formirana je sekcija na čelu s bojnikom Ralphom Testerom poznatim kao Testery. Brojne poruke su presretnute, ali nije učinjeno puno napretka u razbijanju šifre sve dok Nijemci

nisu napravili jednu strašnu pogrešku 30. kolovoza 1941. Njemački operater imao je dugu poruku od gotovo 4000 znakova koju je trebalo poslati iz jednog dijela Vrhovnog zapovjedništva njemačke vojske u drugi - vjerojatno iz Atene u Beč. Ispravno je postavio svoj Lorenzov stroj, a zatim je poslao pokazatelj od dvanaest slova, koristeći njemačka imena, operateru na prijemnom kraju. Ovaj je operater zatim namjestio svoj Lorenzov stroj i zatražio od operatora na kraju slanja da započne slati svoju poruku. Nakon što je na kraju slanja ručno uneseno gotovo 4.000 znakova, operator na prijemnom kraju poslao je putem radija ekvivalent na njemačkom jeziku "nije dobio to - pošalji ponovo". Sad su obojica vratili svoje Lorenzove strojeve u isti početni položaj. Apsolutno zabranjeno, ali oni su to učinili. Operator na kraju slanja tada je ponovo počeo ručno unositi poruku. Da je bio automat i da je koristio potpuno iste poteze tipkama kao i prvi put, svi presretači imali bi dvije identične kopije teksta šifre. Unesite isto - strojevi koji generiraju iste zamračujuće znakove - isti tekst šifre. No budući da je samo čovjek i da mu je teško i zamorno što to sve mora ponovno tipkati, operator pošiljatelj počeo je stvarati razlike u drugoj poruci u odnosu na prvu. Poruka je započela onim poznatim njemačkim izrazom SPRUCHNUMMER - "broj poruke". Prvi put je operater ukucao S P R U C H N U M M E R. Drugi put je ukucao S P R U C H N R, a zatim ostatak teksta poruke. NR znači isto što i NUMMER, pa kakva je razlika bila u tome? To je značilo da su se dva teksta odmah nakon N razlikovala. Ali strojevi su generirali isti zatamnjujući slijed, stoga su se šifrirani tekstovi od tog trenutka razlikovali. Presretači u Knockholtu shvatili su moguću važnost ove dvije poruke jer su dvanaest slovni pokazatelji bili jednaki. Poslani su nakon žurbe Johnu Tiltmanu u Bletchley Park. Tiltman je primijenio istu aditivnu tehniku na ovaj par kao i prethodne poruke. No, ovaj je put uspio postići puno više s razradom stvarnih tekstova poruka jer kada je na početku pokušao SPRUCHNUMMER, odmah je primijetio da je druga poruka gotovo identična prvoj. Stoga su kombinirane pogreške vraćanja strojeva u isti početni položaj i ponovnog unosa teksta uz samo male razlike omogućile Tiltmanu da u potpunosti obnovi oba teksta. Drugi je bio oko 500 znakova kraći od prvog jer je njemački operater štedio prste. Ova činjenica također je omogućila Tiltmanu da dodijeli ispravnu poruku izvornom tekstu šifre. Sada bi Tiltman mogao dodati, znak po znak, odgovarajuću šifru i tekstove poruka koji prvi put otkrivaju dugačak dio zamračujućeg niza znakova koji generira ovaj njemački stroj za šifriranje. Nije znao kako je stroj to uspio, ali znao je da je to ono što generira. (Sale, The Lorenz Cipher)

3.3.2. Važnost Lorenza u preokretu rata

Zahvaljujući pogrešci izumljen je Colossus, stroj za probijanje šifri Lorenza. Colossus je u potpunosti funkcionirao i probio Lorenzovu šifru za samo nekoliko sati, taman na vrijeme za Dan D. Koristeći Colossus, britanske i američke snage dešifrirale su poruke koje su Eisenhoweru i Montgomeryju, zapovjednicima savezničkih snaga, omogućile da dobiju bitne savjete o njemačkim vjerovanjima i postupcima. Te su poruke otkrile da je Hitlera uspješno prevarila fantomska vojska smještena u južnoj Engleskoj i fantomski konvoji koji su išli prema kanalu prema istoku. Te su fantomske vojske koristile tenkove na napuhavanje i manipulaciju medijima kako bi prevarile Hitlera. Hitler je vjerovao da će napadi doći iz Pas de Calaisa i zadržao je Panzer divizije u Belgiji. Ove su informacije britanskim i američkim trupama omogućile učinkovitiji odgovor. (Dinino, 2012.)

Lorenz šifra i Lorenz koje su koristili Nijemci izazvali su nevjerojatan tehnološki napredak prvog pravog elektroničkog digitalnog kalkulatora Colossus. Ovi nevjerojatni strojevi i šifre imali su presudnu ulogu u aktivnostima Drugog svjetskog rata, posebno utječući na ishod rata. Lorenz strojevi za implementaciju napredne kriptografije na strani šifriranja i Colossus za dekriptiranje bili su revolucionarna tehnologija. Te šifre i strojevi zauvijek su ostavili traga u povijesti i kriptografiji.

Lorenzovi strojevi za šifru građeni su u malom broju; danas ih je u muzejima preživjelo tek nekoliko. U Njemačkoj se primjeri mogu vidjeti u Heinz Nixdorf MuseumsForum, muzeju računala u Paderbornu i Deutsches Museumu, muzeju znanosti i tehnologije u Münchenu. Dva daljnja Lorenzova stroja također su izložena u parku Bletchley i u Nacionalnom muzeju računarstva u Ujedinjenom Kraljevstvu. Drugi je primjerak također izložen u Nacionalnom kriptološkom muzeju u Sjedinjenim Državama.

4. Japanska kriptologija

4.1. Početak japanske kriptologije

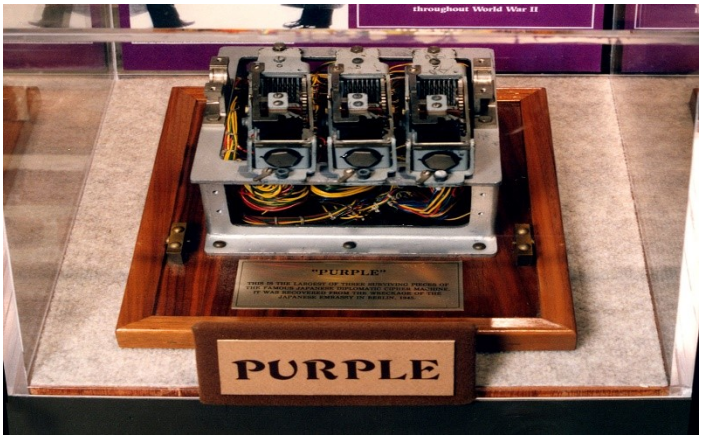
Nakon dobivanja povjerenja Hitlera i drugih njemačkih dužnosnika, japanski barun Hiroshi Oshima kupuje komercijalni stroj Enigmu od Nijemaca u nadi da će razviti novu verziju za Japance. Taj je napor rezultirao stvaranjem novog enigmatskog stroja, kod Amerikanaca kodnog naziva Red. Japanska mornarica koristila ga je otprilike od 1931. do 1936. godine, kada je kriptografsku metodu uređaja srušila američka obavještajna služba signala. Na nesreću SAD-a, informacija o dešifriranju Red-a nije bila dobro čuvana tajna i Japanci su postali sumnjičavi.

Ubrzo nakon toga, Japanci su počeli stvarati novi sustav za šifriranje svojih poruka. Japanci su 1937. godine stvorili 97-shiki O-bun In-ji-ki ili 97 abecednih pisaćih strojeva, nazvano po svom stvaranju u japanskoj 2597. godini. Ovaj je uređaj bio poznatiji pod američkim kodnim imenom Purple.

4.2. Purple

U Drugom je svjetskom ratu Japan dizajnirao stroj poznat pod kodnim nazivom *Purple* koji su mu dali američki kriptoanalitičari. Japanci su ga koristili da bi dešifrirali važne diplomatske i vojne poruke, a inače je zvan i Tipom B jer je bila riječ o nasljedniku japanskog stroja za dešifriranje poznatog pod imenom *Red (Tip A)*. (Lami *et al*.)

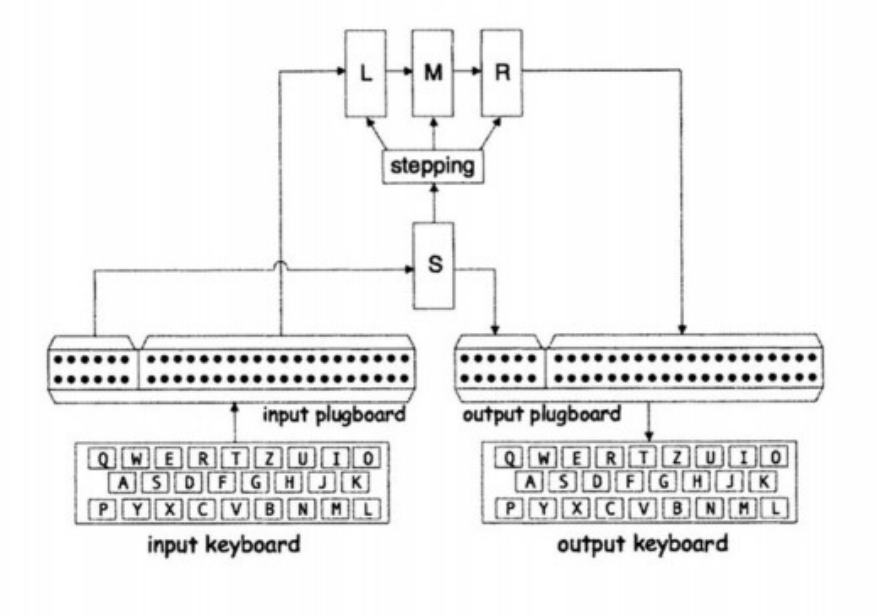
Radilo se o izrazito kompleksnom stroju. Slično Enigmi, koristio je polialfabetsko šifriranje, a sastojao se od ulazne i izlazne utične ploče i prekidača.



Slika 8. Purple (Izvor: https://www.wondersandmarvels.com/2013/02/secrets-abroad-a-history-of-the-japanese-purple-machine.html)

Japanski je stroj uveden u uporabu 1939, točnije u veljači te iste godine odaslane su prve poruke. Bitno je da se kod njega koristi tzv. koračni prekidač što je bio svojevrstan napredak u odnosu na *Red* jer je sigurnost koju je pružao ipak bila mnogo veća. Iako je, kao što je već istaknuto, sam stroj bio prilično kompleksan, najbitnije je reći da se sastojao od input dijela koji je bila tipkovnica i output dijela koji se odnosio na ispis poruka. Slova su unutar stroja bila podijeljena na šestice (samoglasnici) i dvadesetice (suglasnici), a prilikom povezivanja na ploči sama su se slova mogla povezati bez obzira na ovu podjelu, da bi se potom zakrivala u jednoj od tih grupa slova. (Pađen, 2018)

No, za razliku od Enigme koja je tekst predstavljala u obliku trepćućih lampica, Purple je upotrijebio drugu električnu pisaću mašinu koja bi na papir ukucala tekst šifre ili šifriranu poruku. Ovo je bio ogroman napredak od Enigma stroja, koji je zahtijevao dvoje ljudi za rad (jedan tipkanje i jedan za snimanje projekcija) jer je za rad Purplea trebala samo jedna osoba i to je uvelike smanjilo ljudske pogreške. Jedini nedostatak tome bio je u povećanoj veličini i težini Purplea, što ga je učinilo neprikladnim za upotrebu na borbenim mjestima.



Slika 9. Postupak šifriranja (Izvor: Mršić, 2019.)

Purple je šifrirao poruke pomoću svoja četiri rotora i razvodne ploče. Poput Enigme stroj ne bi imao samo nepoznatu metodu šifriranja, već i tajni ključ koji se svakodnevno mijenjao. To je značilo da bi, čak i ako bi ukrali stroj, bez ključa bio beskoristan. Uz to, kako se ključ mijenjao svaki dan, prekidači koda neće moći pronaći uzorke u porukama poslanim tijekom nekoliko dana. Dnevni ključ unosio bi se u uređaj rasporedom razvodne ploče i rotora. Razvodna ploča sadržavala je 25 veza, koje se mogu rasporediti u 6 parova veza, što daje više od 70 000 000 000 000 mogućih rasporeda koji će odrediti način šifriranja. I ne samo to, rotori bi se mogli rasporediti u različite početne položaje koji bi također varirali način šifriranja. Rotori stroja bili su koračni prekidači, koji bi se preuređivali kad bi se svako slovo unosilo i kodiralo abecedu koja se koristi za sljedeće slovo. Purple bi upotrijebio stotine tisuća abeceda šifre prije nego što bi ih ponovio, čime bi eliminirao očite uzorke u tekstu šifre. Zbog toga je Purple - baš kao i stroj Enigma - izuzetno težak za dešifriranje. Da bi se dešifrirala poruka, razvodna ploča i rotori trebali bi biti postavljeni ključem obrnutim od ključa koji se koristi za šifriranje. Tekst šifre tada bi se uključio u prvu pisaću mašinu i stroj bi otkucao otvoreni tekst.

Purple šifra korištena je za slanje tajnih poruka u inozemstvo, uglavnom diplomatima i vojnim dužnosnicima u Washingtonu, Berlinu i Londonu, gdje Japan nije želio da nenamjerni primatelji njuškaju okolo. Probijanje šifre bio je zastrašujući zadatak iz mnogih razloga, osim zbog složenosti samog koda. Dok pokušava razbiti kod, što više šifrira tekst razbijač koda, to je lakši njegov zadatak. Kako su se poruke slale u SAD i Englesku, vladama bi bilo lako

prihvatiti ih. Nažalost, budući da je stroj bio nov i još uvijek nije masovno proizveden, slale su se samo najtajnije vojne poruke, a razbijači koda imali su vrlo ograničenu količinu šifriranog teksta za rad. Međutim, budući da pošiljatelji kodova nisu imali iskustva s novim sustavom, neke su poruke poslane i u šifri Purple i u probijenoj šifri Red, što je omogućilo usporedbu tekstova. Uz to kako je vrijeme prolazilo Purple se kod koristio sve češće i SAD je imao mnoštvo šifriranog teksta za rad.

1939. godine američka vojska angažirala je stručnjaka za kriptografiju Williama Friedmana da radi na probijanju Purple šifre. Nakon osamnaest mjeseci rada Friedman je pretrpio mentalni slom i bio institucionaliziran. Srećom, uspio je postići određeni napredak prije toga, a koristeći se njegovim nepotpunim radom, drugi su članovi njegovog tima mogli kontinuirano napredovati. Iako američki kriptoanalitičari Purple nikada nisu vidjeli, stvoreno je osam funkcionalnih replika stroja. Na kraju je metoda šifriranja Purplea potpuno otkrivena. To međutim, nije značilo da bi se poruke mogle razbiti jer su dnevni ključevi koji su se koristili i dalje bili tajna za kriptoanalitičare. S vremenom je poručnik Francis A. Raven otkrio obrazac koji Japanci koriste u svojim dnevnim ključevima. Primijetio je da je svaki mjesec podijeljen u tri desetodnevna segmenta u kojima se razaznao obrazac. Posljednjim dodirima slagalice poručnika Ravena, Purple šifra je učinkovito probijena i izložene su japanske tajne.

Purple je bila jedna od najsloženijih i najrazvijenijih kriptografskih metoda svoga doba i premda je na kraju pukla, gotovo je dvije godine tijekom Drugog svjetskog rata čuvala strogo povjerljive japanske poruke od znatiželjnih očiju. Nakon velikog napora američke kriptoanalize, kod je slomljen i upotrijebljen protiv svojih proizvođača, za praćenje kretanja japanskih pomorskih snaga, kao i druge vojne komunikacije. Za razliku od Red šifre, SAD su to pokušali iskoristiti u potpunosti čuvajući ga dobro čuvanom tajnom Japanaca i njegovih saveznika kako bi se poruke nastavile slati u probijenom kodu. SAD je zaustavio i razbio mnoštvo japanskih tajnih poruka, čak i neke koje su sadržavale planove napada na Pearl Harbor koje su se mogle koristiti za pripremu. Međutim, kako povijest otkriva, nisu svi oni bili iskorišteni u punom potencijalu.

5. Američka kriptologija

5.1. Sigaba (ECM Mark II)

ECM Mark II (u mornarici također poznat pod nazivom CSP-888/889 ili SIGABA od strane vojske) američki je stroj za šifriranje. Korišten je na brodu USS Pampanito za šifriranje poruka iz običnog, ili onoga što kriptolog (osoba koja proučava tajne komunikacije) naziva otvorenim tekstom, u tajni jezik, koji se naziva šifrirani tekst, pod kontrolom ključa (šifriranje). Kriptografski sustav sastoji se od kombinacije stroja za šifriranje, operativnih postupaka i upravljanja ključevima. Ako je sustav dobro dizajniran i pravilno implementiran, tekst šifre može pretvoriti natrag u običan tekst (dešifrirati) samo netko sa sva tri elementa sustava.

Početkom rujna 1944. američka flotna jedinica Pacific na Havajima snimila je japansku šifriranu radio poruku koja potječe iz Singapura. Američke su snage analizirale mnoge japanske poruke, a da Japanci to nisu znali, i kao rezultat briljantnog i napornog rada mogle su reproducirati neprimjereno osmišljen i implementiran kriptografski sustav njihovog neprijatelja. To se naziva kriptoanalizom ili probijanjem sustava. Pacific je dešifrirao (i dekodirao) poruku koja je najavila put važnog japanskog konvoja od Singapura do Japana. Vrijeme i očekivani put konvoja iz poruke šifriran je na ECM-u na Havajima i poslan u Pampanito gdje je dešifriran na ECM-u. Iako Pampanitova posada nije znala kako je Pacific došao do njegovih podataka, uspjeli su ići izravno na put konvoja i s velikom učinkovitošću napasti. Pampanitov napad tajio je vrhunski američki kriptografski sustav koji se vrtio oko ECM Mark II.

Nije poznato da je kriptografski sustav zasnovan na ECM Mark II neprijatelj ikada razbio i bio je siguran tijekom Drugog svjetskog rata. Sustav je povukla američka mornarica 1959. godine jer je bio prespor da bi udovoljio zahtjevima modernih pomorskih komunikacija. Snage osovine (prvenstveno Njemačka) povremeno su probijale niže stupnjeve sustava koje su koristile savezničke snage. Početkom rata (osobito tijekom konvojne bitke za Atlantik i sjevernoafričku kampanju) probijanje savezničkih sustava pridonijelo je uspjehu Osovine. Suprotno tome, saveznici su uspjeli prekinuti komunikaciju Osovine tijekom većeg dijela rata opskrbljujući mnoge ciljeve koje je napao Pampanito. Presretnute poruke pružale su ne samo mjesto potencijalnih ciljeva, već često i uvid u razmišljanja neprijateljskih zapovjednika. Na Pacifiku su ove informacije bile ključne za uspjeh u bitkama na Midwayu i Koraljnom moru

1942. Međutim, obavještajni podaci, uključujući kriptoanalizu, može biti mač s dvije oštrice. Presretnuta poruka koja je usmjerila Pampanita da napadne konvoj tijekom rujna 1944. nije ukazivala na to da se na japanskim brodovima nalazilo 2000 australskih i britanskih ratnih zarobljenika. Cijela priča o ovom napadu i Pampanitovom spašavanju 73 ratna zarobljenika nalazi se u izvješću Trećeg ratnog ophodstva. Kombinacija sigurnih američkih kriptografskih sustava i ranjivih sustava Osovine izravno je pridonijela uspjehu savezničkih sila tijekom Drugog svjetskog rata, skrativši tako rat za nekoliko godina i spasivši nebrojene ljudske živote.

5.1.1. Kako funkcionira Sigaba

Sigaba ili ECM Mark II je zasnovan na principu elektromehaničkog rotora koji ima izgled glomazne pisaće mašine, slično Enigmi. Stroj se sastoji od 3 skupine po 5 rotora (šifrirni, kontrolni i indeksni), od kojih šifrirni i kontrolni imaju po 26 kontakata sa svake strane, a indeksni 10. Na prednjoj se strani stroja nalazi potpuna engleska tipkovnica, a ispisivanje koda se vrši najčešće na papirnatoj traci. Prva verzija ovog stroja napravljena je 1937. godine zahvaljujući snagama američke vojske i mornarice, a posebno direktoru SIS-a Williamu Friedmanu i njegovu suradniku Franku Rowlettu. Rich Pekelney upravljanje ovim strojem opisuje na sljedeći način:

„Operater pregledava tajni dnevni popis ključeva i različito poravnava kotačiće indeksnog rotora za tajne i povjerljive poruke, a poravnanje indeksnog rotora mijenja se samo kad se promjeni klasifikacija poruke koja se šifrira ili po završetku dana. Kontrolni i šifrirni rotori sastavljaju se jednom dnevno po tajnom dnevnom popisu ključeva, međutim njihovo poravnanje je mijenjano sa svakom porukom. Nakon sastavljanja i poravnanja svih rotora, koristi se kontrolna grupa za provjeru inicijalizacije i rada stroja prije samog šifriranja poruka. Za svaku poruku pregledava se tajni dnevni popis ključeva, a kontrolni rotori i šifre ravnaju se u početni položaj, ovisno o klasifikaciji poruke. Tada operator slučajno odabire grupu od bilo kojih pet slova, isključujući „Z“, koja će biti interni indikator poruke. Zatim se taj interni indikator šifrira, a vanjski indikator poruke ispisuje se na vrpcu i prenosi porukom. Nakon toga se kontrolni i šifrirni rotor poravnaju bez ispisa s unutarnjim indikatorom poruke. Sada se tijelo poruke može šifrirati i prenijeti vanjski indikatorom.“ (Pekenley, 2010)

Slika 10. SIGABA (Izvor: https://maritime.org/tech/ecm2.htm)

5.1.2. Enigma ili Sigaba

Strojevi Enigma i SIGABA imaju važne sličnosti i razlike. Obojica su "strojevi s rotorom", odnosno šifrirali su utipkane poruke slanjem električne struje kroz rotirajuće kotače. Nijedan od ta dva stroja nije računalo. Oni koriste električnu energiju samo za zamjenu slova u abecedi s pokretnim mehaničkim dijelovima koji su ožičeni na vrlo složen način.

Niti jedan stroj ne može slati ili primati poruke poput radija ili računala - oni mogu samo šifrirati ili dešifrirati uneseni tekst. Samo drugi stroj s potpuno istim postavkama može dekodirati poruku. I Enigma i SIGABA ovisile su o tajnom dnevnom "popisu ključeva" postavki stroja kako bi spriječile neprijateljske kriptoanalitičare od dekodiranja poruka.

Najvažnija razlika između strojeva je u njihovoj složenosti. Većina Enigmi koristila je tri rotora, a neke četiri; SIGABA je koristio 15. To je SIGABINO pismo učinilo mnogo složenijim, a kriptoanalitičari ga praktički nisu slomili. Enigma je također starija od SIGABE. Enigma je stvorena u Njemačkoj 1918. i u početku je bila komercijalni uređaj za zaštitu bankovnih transakcija. SIGABA je izumljena 20ak godina kasnije i bila je isključivo vojna oprema.

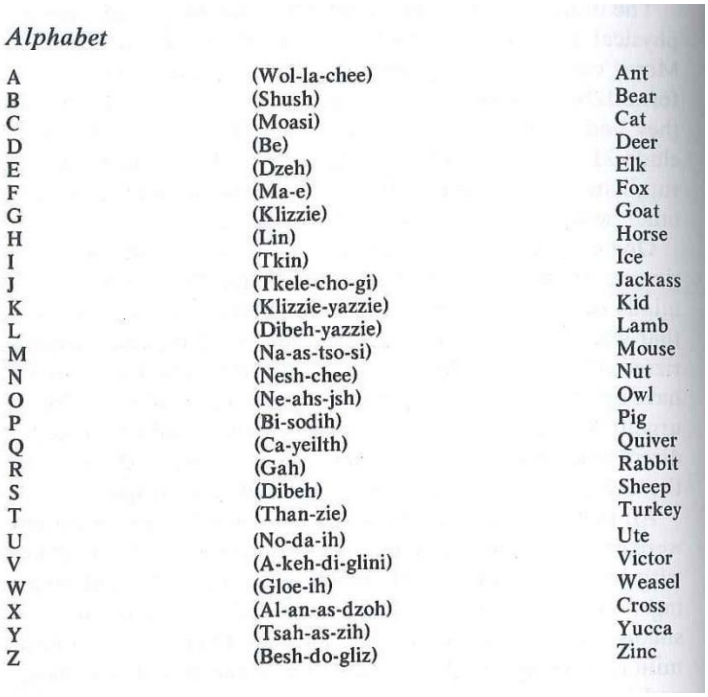
SIGABA je bila lakša za upotrebu od Enigme. Njemačkom stroju za rad su bile potrebne dvije osobe - jedna je upisala poruku, a druga prepisala nastala osvijetljena slova. SIGABA je, međutim, slova tiskala na papirnatu traku, dopuštajući jednoj osobi da njome upravlja. (*War of Secrets: Cryptology in WWII* , National museum of the United States air force)

5.2. Navajo code

Slika 11. Navajo Indijanci u američkoj vojsci (Izvor: https://edition.cnn.com/2014/06/04/us/gallery/navajo-code-talker/index.html)

Navajo kôd je zapravo jezik plemena Navajo koji se koristio u Drugom svjetskom ratu zbog svoje kompleksnosti. Ideju za upotrebu jezika Navajo Indijanaca kao koda dao je Phillip Johnston 1942. koji je odrastao kao sin misionara u samom plemenu. Ideju je dobio čitajući članak u novinama koji je govorio o tome kako je američka vojska koristila indijanske vojnike za davanje signala tijekom obuke. Njegovo iskustvo i odrastanje s jezikom i kulturom plemena Navajo naveli su ga da predloži jezik kao vojni kôd jer je sam jezik bio nepoznat ostalim plemenima i javnosti. Johnston je tako otišao u ured američke mornarice u Los Angelesu te je tamo bio upućen bojniku Jamesu E. Jonesu u kamp Elliot. Bojnik je bio sumnjičav i nije bio siguran u pouzdanost jezika, no nakon što mu je Johnston rekao nekoliko riječi Navajoa, bojnik mu je odobrio probno testiranje s drugim Navajo govornicima. Nakon što se probno testiranje pokazalo uspješnim, general Clayton Vogel izdao je pismo kojim je podržao regrutaciju Navajo ljudi za američke marince. Tako je odobreno početno zapošljavanje Navajo govornika koji su morali proći standardnu vojnu obuku, ali i ispuniti jezične zahtjeve engleskog jezika. Tako je osmišljen sustav abecede koji koristi Navajo riječi koje prevedene na engleski započinju svaka jednim od 26 slova engleske abecede.

Slika 12. Navajo Indijanac desifrira kod (Izvor: https://eu.azcentral.com/story/news/local/arizona/2018/07/11/navajo-code-talker-facts-unbreakable-code/460262002/)



Alphabet

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

Slika 13. Navajo kod (Izvor: https://arizonahistoricalsociety.org/2020/08/14/celebrating-navajo-code-talkers-day/)

Zbog mornaričkog ratovanja s Japanom na Tihom oceanu, u kojem su i Navajo govornici najviše sudjelovali, razvila se potreba za Navajo radio kodom. Navajo radio kod sadržavao je samo odabrane riječi Navajo jezika koje su primjenjivane na vojne fraze. U početku je kod

sadržavao 211 fraza koje su se tijekom Drugog svjetskog rata udvostručile. Navajo jezik nema vojnu terminologiju tako da je većina razvijenog koda bila nova.

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

Slika 14. Primjer Navajo koda koji se upotrebljavao u mornaričkom ratovanju (Izvor: Mršić, 2019.)

„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. 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. 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. 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.“ (Mršić, 2019:42-43)

6. Važnost kriptologije za pobjedu

Prema članku *War of Secrets: Cryptology in WWII* iz National museum of the United States air force, u Drugom svjetskom ratu bežična radio komunikacija bila je vrlo važna za usmjeravanje vojnih snaga raširenih po cijelom svijetu. No radio-poruke su se mogle presresti, pa su se tajni podaci - planovi i naredbe - morali prenositi u tajnim kodovima. Sve velike sile koristile su složene strojeve koji su pretvorili običan tekst u tajni kôd. Njemački stroj pod nazivom Enigma i američki uređaj poznat kao SIGABA izloženi su na izložbi u muzejskoj galeriji Air Power Gallery.

Saveznici su vrlo rano u ratu mogli čitati njemačke poruke zahvaljujući sjajnom radu poljskih i britanskih matematičara-kriptoanalitičara. Tridesetih godina prošlog stoljeća poljski kriptoanalitičari (stručnjaci za razbijanje kodova) kopirali su njemački stroj Enigma uz pomoć njemačkog izdajnika i riješili njegove obrasce kodiranja slova. Kasnije su to znanje podijelili s Francuskom i Britanijom. Obavještajni podaci iz dešifriranih poruka Enigme, kodnog naziva "ULTRA", bila je iznimno tajna i vrlo je malo ljudi znalo za njih. Iako Nijemci nikada nisu saznali da saveznici mogu riješiti njihove kodove, sumnjali su da je njihova sposobnost potapanja saveznička plovila dramatično oslabila 1942. To je dovelo do toga da je njemačka mornarica dodala dodatni rotor u svoje strojeve Enigma i podmornički "vučji čopori" ponovno su uzeli svoj danak u brodarstvu. Kriptoanalitičari su također iskorištavali japanske kodove. Do kraja 1940. američka vojska i mornarica mogle su čitati japanske diplomatske poruke između Tokija i veleposlanstava u Londonu, Washingtonu, Berlinu i Rimu. Američki stručnjaci nazvali su japanski kod PURPLE, a obavještajne podatke iz ovih poruka nazvali su MAGIC. Nažalost, PURPLE diplomatski kôd nije dao posebne vojne podatke, pa Amerikanci nisu imali

nikakvo prethodno znanje o napadu na Pearl Harbor 7. prosinca 1941. (*War of Secrets: Cryptology in WWII* , National museum of the United States air force)

Kako je rat trajao, savezнички analitičari kombinirali su MAGIC i ULTRA obavještajne podatke. Japanska komunikacija ironično je odigrala važnu ulogu u ratu u Europi, budući da je Tokyo od svojih diplomata želio informacije o njemačkom i talijanskom napretku. Presretanje ovih japanskih poruka dalo je savezničkim zapovjednicima vitalne informacije o nacističkoj proizvodnji oružja i njemačkim planovima za obranu Europe od invazije. Savezнички čelnici također su iz MAGIC-a znali da se Japan neće bezuvjetno predati ako nije prisiljen.

7. Utjecaj na modernu tehnologiju

Nakon što se kriptografski sustav razbije, kriptografi uče iz njegovih slabosti i pokušavaju stvoriti novi kriptosustav koji je ili naprednija verzija ili se stvara novi način šifriranja. Njemačka i Japan shvatili su da su njihovi strojevi za šifriranje, Enigma i Purple, ugroženi te da su im potrebni novi kriptosustavi za šifriranje njihovih poruka. Kriptosustavi koji su se razvili kao odgovor pomogli su daljnjem utjecaju na kriptosustave koji se danas koriste. Kriptografija kao znanost razvila se od Drugoga svjetskog rata. Kriptografiju više ne koriste samo vojske, već je sada uključena u svakodnevni život većine ljudi. Primjer je uloga kriptografije u očuvanju sigurnosti internetskog bankarstva. Podaci su šifrirani kao pokušaj odvraćanja treće strane od krađe milijuna. Kriptografija i dalje igra važnu ulogu u pitanjima nacionalne sigurnosti. Iako, zbog svoje tajne prirode, u kojoj mjeri vlada koristi kriptografiju ili točne šifre i kriptosustave koje koristi neće biti poznato sve dok se sustav ne razbije. Iako se Enigma više ne koristi za šifriranje poruka, nedavno se ponovno pojavila. Stroj je bio na aukciji u Londonu 29. listopada 2013. Proizveden je 1944. godine i koristila ga je njemačka vojska za šifriranje svojih poruka. Nema mnogo Enigmi koje su i danas netaknute. Njemačka vlada uništila je njihove kopije kako bi osigurala da strojevi nisu zarobljeni od strane neprijatelja. Također su šifrarnici i nacrti ožičenja spaljeni ili izgubljeni tijekom Drugog svjetskog rata i narednih godina. Stroj koji se prodaje na aukciji jedna je od rijetkih preostalih Enigma koje još uvijek sadrži sve svoje originalne dijelove. Prodao se za 91.839 dolara. (Callahan, 2013.)

8. Zaključak

Cilj ovog rada bio je prikazati utjecaj kriptologije u Drugom svjetskom ratu, njezinu ključnu ulogu koja je određivala tijek ratovanja u Njemačkoj, Japanu i Sjedinjenim američkim državama, kako se upotrebljavala, koji su uređaji i sustavi proizašli iz rata te naposljetku kako su se upotrebljavali i dešifrirali. Također je opisan njen utjecaj na moderne tehnologije današnjice.

U uvodnom dijelu dan je kratak pregled definicije i opisa kriptologije te njezino grananje i shematski prikaz, te povijesni pregled. Nakon sažetog pregleda njemačke, japanske i američke kriptografije, kao i povijesnog razvoja kriptologije i kriptografije možemo zaključiti da je riječ o područjima od iznimne važnosti za znanost, prije svega zbog izuzetne praktične vrijednosti.

U velikom sukobu kao što je bio Drugi svjetski rat šifriranje i dešifriranje strojnih poruka bilo je ključno za tijek zbivanja te je upravo u tom razdoblju oblikovan najveći interes za daljnji razvitak kriptologije. Strojevi poput *Enigme, Lorenza, Purplea, Sigabe*, usprkos svim svojim nedostacima, odigrali su bitnu ulogu u ratnoj djelatnosti saveznika i sila Osovine te se razbijanjem njihovih kodova i međusobnim „nadmetanjem“ omogućio napredak unutar područja kriptozaštite i kriptoanalize. Utjecaj je vidljiv u današnjim bankovnim sustavima te unutar nacionalne sigurnost i čuvanja informacija.

Literatura

1. Callahan, K. (2013.) *The Impact of the Allied Cryptographers on World War II: Cryptanalysis of the Japanese and German Cipher Machines*, Link: https://www.gcsu.edu/sites/files/page-assets/node-808/attachments/callahan.pdf [Pristupljeno: 1.9.2021.]
2. Crypto Museum (2019.) History of the Enigma, Link : https://www.cryptomuseum.com/crypto/enigma/hist.htm [Pristupljeno: 1.7.2021.]
3. Crypto Museum (2021.) Bombe, Link: https://www.cryptomuseum.com/crypto/bombe/index.html [Pristupljeno: 2.7.2021.]
4. Derenčin, R. (2016.) Enigma i njemačke podmornice u Drugom svjetskom ratu, stručni rad, Polemos 19, 1: 137-155 str.
5. Denino, E. (2012.) The Lorenz Cipher and the World's First (Secret) Computer, Cryptography The History and Mathematics of Codes and Code Breaking, Link: https://derekbruff.org/blogs/fywscrypto/historical-crypto/the-lorenz-cipher-and-the-worlds-first-secret-computer/ [Pristupljeno: 2.7.2021.]
6. Gutiérrez, Á. (2009.)„ Criptografía y criptoanálisis en las dos guerras mundiales". *Manual formativo de Acta* 52: 63 – 77.
7. Mršić, D. (2019) Kriptografija u Drugom svjetskom ratu, Sveučilište Josipa Jurja Strossmayera u Osijeku, diplomski rad. 58 str.
8. Mowry, D. P. (2014) German Cipher Mchines of World War II, Center for Cryptologic History National Security Agency
9. National museum of the United States air force (2015.) *War of Secrets: Cryptology in WWII* , Link: https://www.nationalmuseum.af.mil/Visit/Museum-Exhibits/Fact-Sheets/Display/Article/196193/war-of-secrets-cryptology-in-wwii/ [Pristupljeno: 1.9.2021.]
10. Navajo Code Talker (2000), Link: https://navajopeople.org/navajo-code-talker.htm
11. Pađen, L. (2018.) Kriptologija u teoriji i praksi u prvoj polovici dvadesetog stoljeća, Filozofski fakultet Sveučilišta u Zagrebu, diplomski rad
12. Pekelney, R. (2010.) Electronic Cipher Machine (ECM) Mark II, Maritime Park Association, Link: https://maritime.org/tech/ecm2.htm [Pristupljeno: 1.7.2021.]
13. Rošić, K. (2018.) *Transpozicijske šifre*, Sveučilište J.J. Strossmayera u Osijeku, diplomski rad, 44. str.

14. Sale, T. The Lorenz Cipher and how Bletchley Park broke it, Link: https://www.codesandciphers.org.uk/lorenz/fish.htm [Pristupljeno: 2.7.2021.]
15. Uglješa, K. (2015.) Kriptologija u Drugom svjetskom ratu, Filozofski fakultet Sveučilišta u Zagrebu, završni rad, 20 str.
16. Xifré Solana, P.(2009.) Antecedentes y perspectivas de estudio en historia de la criptografía, Universidad Carlos III de Madrid, završni rad, 273 str.

Kriptologija u Drugom svjetskom ratu

Sažetak

Tema je ovog rada kriptologija i kriptografija u Drugom svjetskom ratu i utjecaj kriptografskih procesa tj, šifriranja i dešifriranja na ishod rata. Posebna se pozornost usmjerava na strojeve poput *Enigme, Lorenza* i *Purplea*, njihove temeljne karakteristike i način funkcioniranja te na proces enkripcije i razbijanja strojne šifre, ali i američki enkripcijski sustav koji se temeljio na jeziku Navajo Indijanaca.

Ključne riječi: kriptologija, kriptografija, Drugi svjetski rat, *Enigma, Purple, Lorenz*, Navajo Indijanci

Cryptology in World War II

Summary

The main focus of this paper is cryptology and cryptography in World War II and the influence of cryptographic processes, ciphering and deciphering, on the outcome of the war. The central part is dedicated to the machines such as *Enigma, Lorenz, Purple*, to their main characteristics and to the description of their functioning and to the process of breaking its code. An American encoding system based on Navajo language is also described.

Key words: cryptology, cryptography, World War II, *Enigma, Lorenz, Purple,* Navajo Indians