FILOZOFSKI FAKULTET SVEUČILIŠTA U ZAGREBU

ODSJEK ZA INFORMACIJSKE I KOMUNIKACIJSKE ZNANOSTI

AK. GOD. 2014./2015.

Karmen Uglješa

Kriptologija u Drugom svjetskom ratu

Završni rad

Mentorica: dr. sc. Vjera Lopina

Zagreb, 2015.

Sadržaj

1. Uvod

Drugi svjetski rat najrašireniji je i najrazorniji rat u povijesti čovječanstva. Počeo je napadom Njemačke na Poljsku 1. rujna 1939. te se do 1945. vodio između savezničkih sila i sila Osovine. Najjače zemlje Saveznika činili su Ujedinjeno Kraljevstvo i Sjedinjene Američke Države (i kasnije SSSR), a sile Osovine činili su Njemačka, Italija i Japan. Svaka od tih zemalja imala je jaku vojsku i često su zahvaljujući tome bile uspješne u mnogim bitkama.

No, vojska često ovisi o informacijama o protivnicima, a za to su zadužene obavještajne i kontraobavještajne službe. Nijedna zemlja ne dopušta da osjetljive informacije budu nezaštićene, stoga su poruke do kojih te službe dolaze često enkriptirane. Zato obavještajne službe surađuju s kriptološkim službama koje pronalaze razne načine na koje će razbiti kriptografski sustav protivničkih zemalja, dok istovremeno smišljaju kako će svoj sustav poboljšati.

Drugi svjetski rat se pokazao kao događaj u kojem je kriptološka djelatnost bila od goleme važnosti i u nekim slučajevima čak presudna za tijek događaja, stoga je tema ovog rada prikaz kriptološke djelatnosti nekih velesila Drugog svjetskog rata. Opisat će se kako je kriptologija utjecala na uspjehe i neuspjehe pojedinih zemalja u ratu te navesti neki od najpoznatijih uređaja za šifriranje koje su koristile. Prvo poglavlje sadrži kratko objašnjenje osnovnih pojmova u kriptologiji te sažet prikaz njezinog razvoja do Drugog svjetskog rata, a sljedeća poglavlja opisuju djelovanje kriptoloških službi dviju europskih sila Osovine, Njemačke i Italije, te kriptološku djelatnost dvaju Saveznika, Ujedinjenog Kraljevstva i SAD-a.

2. Osnovni pojmovi u kriptologiji

Kriptologija je znanost koja proučava tajno komuniciranje te se može podijeliti na kriptografiju i kriptoanalizu. Kriptografija stvara i proučava sustave za kriptiranje pisanih poruka, a ti sustavi se dijele na šifre i kodove. Šifre (ili kritopisni sustavi) sastoje se od algoritma, tj. niza uputa po kojima se poruka šifrira ili dešifrira, te ključa, podatka koji se sastoji od znaka ili niza znakova koji je potreban da bi se poruka uspješno šifrirala pomoću algoritma; kad se koriste šifre, svako se slovo u poruci ili zamjenjuje znakom (supstitucijska šifra), ili premješta na drugo mjesto (transpozicijska šifra). S druge strane, kodovi su simboli ili riječi koji mogu zamijeniti cijelu riječ ili frazu u poruci. Kriptoanaliza je grana koja se bavi probijanjem sustava bez prethodnog poznavanja informacija koje su potrebne za dešifriranje ili dekodiranje poruke.

Do 20. stoljeća koristili su se različiti sustavi za šifriranje. Jedan od prvih poznatijih je Cezarova šifra – monoalfabetska supstitucijska šifra kojoj je ključ broj za koji se šifarski alfabet pomiče u stranu. Nešto složenija je Vigenèreova šifra koja je polialfabetska; njezin je ključ neka riječ čiji broj slova određuje koliko se šifarskih alfabeta koristi. Cezarovu šifru lako je bez ključa razbiti metodom frekvencijske analize (sastavljanjem popisa najučestalijih znakova u poruci i uspoređivanjem s najfrekventnijim slovima jezika na kojem je poruka pisana), a Vigenèreova šifra dugo se smatrala neprobojnom, dok je nisu razbili (neovisno jedan o drugom) engleski matematičar Charles Babbage i pruski časnik Friedrich Kasiski, po kojem je danas i nazvana ta metoda.

Ideje za strojeve za šifriranje su se počele češće pojavljivati tek u 20. stoljeću; dotad su se većinom koristile aparature koje bi samo ubrzavale šifriranje, bez povećavanja sigurnosti sustava; jedna takva aparatura su diskovi svestranog talijanskog humanista Leona Battiste Albertija. Sličnu ideju kotača s diskovima proveo je Thomas Jefferson, ali njegov kotač je povećavao sigurnost sustava jer su se diskovi mogli razmještati.

Slika 1: Shema Albertijevih diskova

Slika 2: Jeffersonov kotač

3. Kriptologija u međuratnom razdoblju

Kriptologija je doživjela veliki razvoj početkom 20. stoljeća, kad je američki inženjer Gilbert Vernam razvio ideju koja se temeljila na Baudotovom kodu, teleprinterskoj varijanti Morseovog koda – osim postojeće perforirane vrpce u koju se „štampala“ poruka, u teleprinter je dodao još jednu vrpcu na koju bi se „štampala“ slova ključa te bi telegraf na kraju otipkao šifrat koji je nastao kombinacijom impulsa slova otvorenog teksta i impulsa slova ključa, postupkom neprenosivog pribrajanja, odnosno XOR operacije. Ovim putem je kriptografija automatizirana. Kasnije je tom sustavu povećana sigurnost tako da je odlučeno

da ključ bude potpuno nasumičan i da se ne smije ponavljati; rezultat toga danas je poznat kao jednokratni sustav („one-time system“).

Još jedan važan izum za kriptografiju bio je stroj s rotorima pokretan električnom energijom. Osnovna ideja takvog stroja se sastojala u tome da svaki rotor sadrži slova alfabeta i da su slova spojena nasumično, tako da se određeno slovo na jednom rotoru spaja s drugim slovom na drugom rotoru, odnosno ne sa tim istim slovom. Takav sustav s više rotora je mnogo sigurniji od dotadašnjih jer ima više ključeva: ako ima tri rotora od kojih svaki sadrži 26 slova, broj mogućih ključeva je 26^3 ili 17 576, što znatno otežava razbijanje sustava. Ono što su rotori također omogućavali je to da, kad se jedno slovo šifrira više puta zaredom, svaki put će se šifrirati u drugo slovo. Stroj s rotorima izumljen je gotovo istodobno u čak četiri zemlje: prvi ga je 1919. izumio Amerikanac Edward Hebern. Drugi istaknuti izumitelj, Šveđanin Arvid Gerhard Damm, kasnije je postao poznat po tome što je „osnivač jedine firme za proizvodnju šifarskih strojeva koja je komercijalno uspjela“ (Kahn 1979), no, i sin njegovog suradnika, Boris Hagelin, kasnije je napravio strojeve za šifriranje koje su koristile francuska i američka vojska i talijanska ratna mornarica. Ipak, najpoznatiji među četvoricom izumitelja je Arthur Scherbius – njegov stroj, nazvan Enigma, koristila je njemačka vojska i njezino razbijanje imalo je golem utjecaj na tijek Drugog svjetskog rata.

I kriptoanaliza je napredovala u tom razdoblju kad je američki kriptograf William Frederick Friedman objavio niz radova o kriptoanalizi poznatih kao The Riverbank Publications, u kojima ju je usko povezao sa statistikom.

4. Njemačka kriptologija u Drugom svjetskom ratu

Njemačka diplomacija 20-ih godina 20. stoljeća koristila je numeričke kodove koja bi se pribrojio ključ postupkom neprenosivog pribrajanja, što je bilo slično Vernamovoj ideji dodatne vrpce s ključem. Tri njemačka kriptologa, Werner Kunze, Rudolf Schauffler i Erich Langlotz, tad su dobila zadatak da dodatno osiguraju taj način šifriranja te su zaključili da je jedini neprobojni sustav onaj koji ima nasumični i neponavljajući ključ. Za taj sustav koristili su bilježnice koje su sve bile različite, a sadržavale peteroznamenkaste grupe ključa. Svaki bi se ključ primijenio samo jednom i taj bi se list onda istrgnuo. Sustav se zato zvao „jednokratna bilježnica“, tj. „one-time pad“ i bio je najsigurniji sustav koji je neka diplomacija koristila u to vrijeme.

Njemačko Ministarstvo vanjskih poslova osnovalo je svoju dekriptersku službu 1919. Služba se neko vrijeme zvala Referada IZ (Z sekcija I odjeljenja Ministarstva vanjskih poslova) i sastojala se od dvije sekcije: dekripterske i kriptografaske. 1936. služba je preimenovana u Pers Z (Z sekcija Kadrovskog i općeg odjeljenja; „Z" nije imalo nikakvo značenje). Dekripterska sekcija je 1939. podijeljena na grupe: jedna se bavila šiframa i predvodio ju je ranije spomenuti kriptolog Werner Kunze, a druga kodovima i jedan od njezinih šefova je bio također spomenuti Rudolf Schauffler. Kriptografska sekcija kasnije je prešla pod izravnu nadležnost ministra vanjskih poslova Joachima von Ribbentropa. Obje grupe dekripterske sekcije morale su se seliti tijekom rata i tako razdvajati. Osim toga, posao im je otežavala zabrana upotrebe tinte, zaključavanje i detaljno spaljivanje papira te obavezno znanje stranih jezika (engleskog i francuskog, a često i trećeg) koje bi se svake četiri godine provjeravalo. Sav njihov rad motrio je doušnik kojeg su u službu ubacili nacisti. Sve poruke koje su dekriptirali slali su svom šefu Kurtu Selchowu koji ih je prosljeđivao državnom sekretaru Ministarstva, a kasnije i samom ministru Ribbentropu. 1945. dekriptere Pers Z-a uhvatio je jedan od američkih timova TICOM-a (Target Intelligence Committee) koji su oformljeni upravo da otkriju njemačke obavještajne i kriptološke službe i sačuvaju dokumente, tehnologiju i osoblje prije nego što ih otkriju i potencijalno unište Rusi[1]. Tijekom svog rada dekripteri Pers Z-a čitali su poruke čak 34 zemlje[2], a razbili su i jedan japanski diplomatski kod pomoću kojeg su imali saznanja o vojnim aktivnostima SSSR-a, što je uvelike pomoglo njemačkoj vojsci prije napada na tu zemlju.

Kad je Hermann Göring 1933. postavljen za ministra ratnog zrakoplovstva, osnovao je Geheime Staatspolizei (Državnu tajnu policiju), poznatiju kao Gestapo, i Forschungsamt (Istraživački ured), jedinicu za interceptiranje poruka. Forschungsamt je prisluškivao telefone, otvarao pisma, dekriptirao telegrame, ali i snimao i arhivirao telefonske razgovore Hitlera i Göringa. Šef Forschungsamta je bio Christoph von Hesse koji je imao čin u nacističkoj organizaciji Schutzstaffel (SS). Unutar SS-a postojao je SD – Sicherheitsdienst, odnosno Služba sigurnosti. SD je nadzirao njemačke građane, a kasnije je imao domaću i inozemnu sekciju, iako je inozemna sekcija najviše materijala dobivala od Forschungsamta. 1939. su djelatnosti koje su obavljali SD, Gestapo i Kripo (Kriminalistička policija) spojene u RSHA (Reichssicherheitshauptamt - Glavna uprava za sigurnost Reicha).

[1] *http://www.ticomarchive.com/home/origin-of-ticom*
[2] *Kahn, D. (1979). Šifranti protiv špijuna 2. Zagreb : Centar za informacije i publicitet. str. 27.*

Od njemačkih vojnih obavještajnih službа najstarija je Abwehr (Obrana) koji je bio pod nadležnošću OKW-a (Oberkommando der Wehrmacht, vrhovnog zapovjedništva njemačke vojske). Abwehr je imao 3 sekcije: jedna se bavila špijunažom, druga organiziranjem sabotaža, tj. specijalnih akcija, a treća kontrašpijunažom (nadziranjem stranih obavještajnih službi).

Sve službe većinom su samo prisluškivale i vrlo malo dekriptirale dok se Njemačka nije počela naoružavati 1934. Tad je OKW postavio interceptorsku i kriptološku službu WNV (Wehrmachtsnachrichtenverbindungen). Za njezinog šefa postavljen je Erich Fellgiebel koji je nekoliko godina kasnije smijenjen zbog sumnje da je umiješan u pokušaj atentata na Adolfa Hitlera (pokušaj je poznat kao Srpanjska urota). Jedna podslužba WNV-a bila je Amtsgruppe WNV koja je imala šifrarsku sekciju Chiffrierabteilung, često zvanu samo Chi. 1944. Chi je podijeljena na 8 grupa i jednu dodatnu koja je provjeravala sigurnost njemačke kriptografije. Chi je nadgledala jednu službu koja se bavila interceptorsko-dekripterskim aktivnostima i koja se zvala Heeresnachrichtenwesens (Komunikacijski sistem kopnene vojske); HNW je svoje dekriptate slao vojnoj obavještajnoj službi, a osim toga izrađivao je kriptografske sustave i distribuirala ih kopnenoj vojsci. Dekriptere Chiffrierabteilunga zadesila je ista sudbina kao i dekriptere Pers Z-a – 1945. uhvatio ih je jedan od timova TICOM-a.

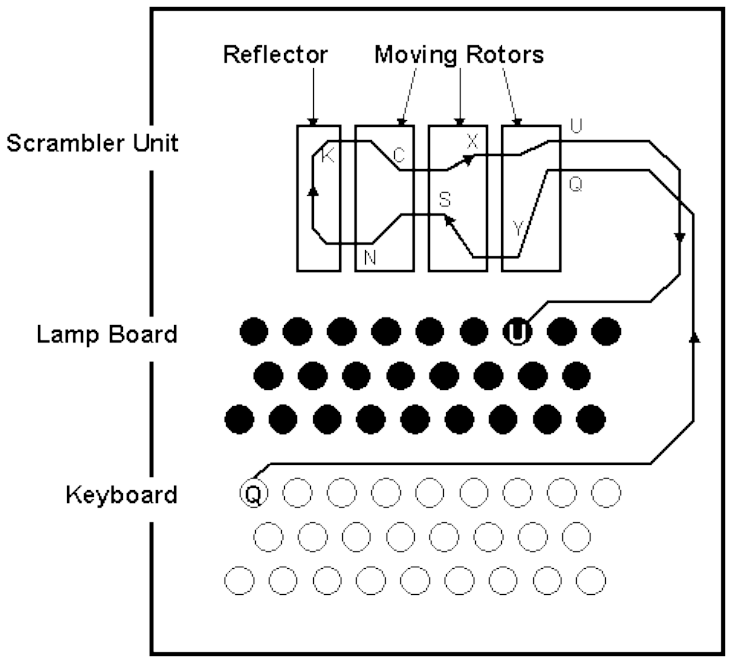
Kopnena vojska koristila je sustav dvostruke transpozicije ÜBCHI koji je koristila i u Prvom svjetskom ratu, no vojnici su često radije koristili numeričke kodove ili čak slali nešifrirane poruke. Kasnije su koristili bigramsku supstituciju i transpozicijski sustav rešetke. Više razine zapovjedništva koristile su Enigmu, o kojoj će se više reći kasnije.

Još jedna vojna kriptoanalitička služba pripadala je ratnoj mornarici i zvala se B-Dienst (skraćeno od Beobachtungsdienst, Služba osmatranja). Britanska dekripterska služba je u Prvom svjetskom ratu otkrila kodove njemačke ratne mornarice, što je uzrokovalo jačanje ove službe koja je „zauzvrat“ razbila kodove britanskog admiraliteta. Upravo zahvaljujući radu B-Diensta otkriveno je da Britanci hoće spriječiti prolaz njemačkih brodova u Norvešku radi preuzimanja pošiljka rude – Nijemci su zatim razvili strategiju kojom su izmamili britanske brodove na drugu stranu i nesmetano došli do Norveške.

4.1. Enigma

Enigma je vjerojatno najpoznatiji stroj za šifriranje, barem u Drugom svjetskom ratu. Kao što je već rečeno, konstruirao ju je Arthur Scherbius 1918. Sastojala se od tri dijela: tipkovnice, premetačke jedinice (rotorâ) i zaslona (žaruljica koje su prikazivale slova šifrata). Tri su rotora sa svake strane imala 26 kontakata, svaki za jedno slovo. Treći je rotor bio spojen na reflektor koji je imao kontakt samo s jedne strane i koji je bio statičan. Kad bi operater pritisnuo tipku za neko slovo, signal je išao do ulaznog kontakta prvog rotora pa kroz izlazni kontakt koji je bio spojen na neko drugo slovo na drugom rotoru, a tako je bilo i između drugog i trećeg rotora. Kad bi signal došao do reflektora, on bi ga poslao natrag na isti način. Svakim pritiskom na tipku prvi rotor bi se pomaknuo za jedan kontakt, a kad bi napravio puni krug, drugi rotor bi se pomaknuo za jedan kontakt; treći bi se rotor, dakle, pomaknuo za jedan kontakt kad bi drugi rotor napravio puni krug. Radi povećanja sigurnosti, njemačka je vojska napravila dvije stvari: dodali su razvodnu ploču s kablovima koja je omogućavala da određena slova prije ulaska signala u rotor zamijene mjesta, i omogućili su da se rotori vade i zamjenjuju mjesta. Tako je broj mogućih ključeva bio golem i smatralo se da je sustav neprobojan, no kasnije će se pokazati da su greške operatera (i jedan njemački špijun) bile ključne u razbijanju Enigme.

Slika 3: Enigma



Slika 4: Osnovni princip rada Enigme

5. Talijanska kriptologija u Drugom svjetskom ratu

Italija je za presretanje poruka i obavještenja koristila službe ratne mornarice i kopnene vojske. Služba ratne mornarice zvala se B sekcija Službe tajnih obavještenja (Servizio Informazioni Segreti, Sezione B) i zaslužna je za probijanje šifara koje je koristila britanska ratna mornarica. Služba kopnene vojske zvala se Vojna obavještajna služba (Servizio Informazioni Militari). Unutar nje postojala je Peta sekcija koja je dekriptirala vojne i diplomatske poruke; u tom joj je pomagala Šesta sekcija koja je bila prislušna stanica. Jedna podsekcija unutar Pete sekcije bavila se proizvodnjom šifara i kodova za vojsku koje su koristila viša zapovjedništva, a dijelom i mornarica, no ona je većinom koristila stroj za šifriranje koji je konstruirao ranije spomenuti Boris Hagelin.

Talijanska služba uspjela je razbiti sustav šifriranja koji je koristila Jugoslavija, što je pomoglo talijanskoj vojsci da se obrani od jugoslavenske na zanimljiv način: kad je jugoslavenska vojska 1941. krenula u napad na Italiju koja je tad bila zauzeta zauzimanjem Albanije i Grčke, SIM je jugoslavenskim sustavom šifrirao telegrame koje je zatim poslao jugoslavenskoj vojsci, a u kojima je pisalo da se ofenziva prekida i da se jedinice povuku.

Međutim, SIM svoj najveći uspjeh ne duguje kriptologiji, već krađi: SIM je imao posebnu Sekciju za dobavljanje (Sezione Prelevamento) koja je 1941. u Rimu ukrala kod Black (Crni kod) koji su koristili američki vojni izaslanici. Jedan od izaslanika nalazio se u Kairu i često je obavještavao Washington o položaju i stanju britanskih vojnih jedinica. Jedan primjerak koda Talijani su predali njemačkom Abwehru, tako da su poruke izaslanika u Egiptu omogućavale dobru pripremu njemačke vojske na sjeveru Afrike. Tamo se nalazio general Erwin Rommel (poznat kao Pustinjska lisica upravo zahvaljujući svojim dostignućima na tom području) kojem je probleme stvarala Malta, budući da su je Saveznici koristili kao bazu iz koje su napadali osovinske konvoje. U lipnju 1942. Britanci su prema Malti poslali dva velika konvoja sa suprotnih strana s namjerom da istodobno napadnu sile Osovine, no izaslanik u Kairu to je javio SAD-u, a prislušna OKW-a Rommelu. Tako su talijanska i njemačka vojska na vrijeme uspjele potisnuti konvoje te se pripremiti i obraniti i britanska operacija nije uspjela, a Rommel je još neko vrijeme nakon toga dobivao informacije od njemačkih prislušnih i dekripterskih stanica. No, mjesec dana kasnije Britanci su napali njemačku mobilnu radio-stanicu i otkrili da Njemačka i Italija čitaju njihove poruke (i usput otkrili slabosti svog sustava koje Nijemci iskorištavaju), tako da su nedugo nakon toga promijenili način kriptiranja. Kao posljedica toga, Rommel više nije dobivao informacije o položajima

savezničke vojske i iduća bitka, ona kod El Alameina, bila je presudna za prevlast Saveznika u Sjevernoj Africi. Ta tajna priprema britanskih snaga bila je dio goleme obavještajne operacije ULTRA koja je označavala sve informacije dobivene dešifriranjem njemačkih poruka, većinom poslanih Enigmom (više informacija o razbijanju Enigme nalazi se u sljedećem poglavlju).

6. Britanska kriptologija u Drugom svjetskom ratu

U Prvom svjetskom ratu Ujedinjeno Kraljevstvo imalo je kriptoanalitičku sekciju koja je bila poznata pod imenom Soba br. 40 i koja je bila pod nadležnošću britanske mornarice. Ta je grupa, između ostalog, presrela i dekriptirala Zimmermannov telegram, dokument u kojem Njemačka Meksiku predlaže vojni savez u slučaju da SAD krene u rat protiv nje; može se reći da je taj dokument bio uzrok ulaska SAD-a u rat. Nakon rata tu je službu preuzelo britansko Ministarstvo vanjskih poslova i ona se nastavila baviti čuvanjem šifara i kodova te njihovim razbijanjem, tada pod imenom Odjeljenje za komunikacije (Department of Communications). I Ministarstvo rata je imalo svoju vojnu obavještajnu službu, unutar koje je postojala sekcija MI1b. Te su se dvije kriptološke službe 1919. spojile u jednu koja je dobila ime Government Code and Cypher School (GC&CS; Vladina škola za kodiranje i šifriranje). 1939. je škola premještena na posjed Bletchley Park nedaleko od Londona odakle je u malim kolibama radila na razbijanju njemačke Enigme, po čemu je vjerojatno i najpoznatija.

Slika 5: Vila na posjedu Bletchley Park

6.1. Razbijanje Enigme

Prvi koji su imali potrebu za razbijanjem Enigme su bili Poljaci. U međuratnom razdoblju Poljska je bila okružena Njemačkom i SSSR-om, i obje su države imale planove o zauzimanju poljskog teritorija. Zato je poseban dio poljske obavještajne službe, Biuro Szyfrów (Ured za šifre), godinama presretao i dekriptirao njemačke poruke. Međutim, kad je njemačka vojska počela koristiti Enigmu, Poljaci su morali krenuti ispočetka. Tada je Enigma bila u slobodnoj prodaji pa su kupili nekoliko primjeraka, no nakon što su shvatili da su Nijemci adaptirali svoju verziju tako da su za svaku poruku koristili poseban ključ, ipak je bila potrebna kriptoanaliza. Za nju su bila zadužena tri matematičara: Marian Rejewski, Henryk Zygalski i Jerzy Rozycki, no nisu uspijevali razbiti sustav. U isto vrijeme njemački zaposlenik u šifarskoj službi Reichswehra (njemačke vojske) Hans-Thilo Schmidt, razočaran načinom na koji ga je tretirala Njemačka kojoj je služio u Prvom svjetskom ratu, imao je pristup uputama za uporabu Enigme i dokumentima s informacijama o ključevima te je prodavao te dokumente francuskoj vojnoj obavještajnoj službi, Deuxième Bureau. Francuska je u to doba vojno surađivala s Poljskom pa joj je prosljeđivala te dokumente, misleći da su beskorisni.

Međutim, ti su dokumenti bili od velike koristi Rejewskom koji je uspio razbiti kriptograme, a osim dokumenata pomogle su mu i pogreške njemačkih operatera – oni su jedno vrijeme prvo već spomenuti ključ poruke šifrirali dvaput zaredom (uzmimo za primjer ključ GLT: on bi se šifrirao dvaput zaredom pa je šifrat ključa GLTGLT glasio npr. RPQVAM). Tako su Rejewski i ostali kriptoanalitičari otkrili obrasce pomoću kojih su razbili šifru. Schmidtovi dokumenti pomogli su im i da konstruiraju kopiju Enigme (točnije, njih šest radi bržeg provjeravanja rješenja) koju su nazvali „bomby" (množina riječi „bomba"). No, 1938. su Nijemci dodali još dva rotora i još četiri kabla na razvodnoj ploči, čime su znatno povećali broj mogućih ključeva i otežali probijanje sustava. Kad su počele pripreme za napad na Poljsku, Poljaci su bili prisiljeni potražiti pomoć. Pozvali su britanske i francuske kriptoanalitičare i predali svakome po jednu repliku Enigme i nacrte „bomba". Britanski kriptoanalitičari odnijeli su ih u Bletchley Park gdje su proučili poljske nacrte i pokušaje probijanja. Zapazili su još jednu grešku njemačkih operatera – za ključ poruke često su koristili tri slova u slijedu umjesto nasumičnih ili su upotrebljavali isti ključ za više poruka. Tako su nekad uspijevali dešifrirati poruke (u međuvremenu su poljski kriptoanalitičari došli u Englesku, no nije im bilo dopušteno da se bave dešifriranjem Enigminih poruka[3]).

Najpoznatiji kriptoanalitičar Bletchley Parka je matematičar Alan Turing. On je „napao" sustav Enigme tako što je pročitao mnoštvo već dešifriranih poruka i utvrdio da mnoge imaju određenu strukturu pa je tako predvidio položaj neke riječi u šifratu. I Turing je dao napraviti svoju verziju „bombe"; do 1941. su ih imali petnaest, i svaka je mogla otkriti ključ za sat vremena (ako bi predviđeni položaj riječi bio točan).

Britanski kriptoanalitičari dešifrirali su mnoge poruke vezane uz njemačke vojne operacije, posebice one vezane za zračne napade, što je u nekoliko navrata omogućilo Britancima da se obrane; i to je bio dio već spomenute operacije ULTRA. Ta je operacija postala poznata javnosti tek 30 godina nakon završetka rata[4], a osim uspjeha u Sjevernoj Africi, podaci dobiveni u toj operaciji pomogli su i kod borbe za oslobođenje Francuske te u bitki za Atlantik.

[3] *Sebag-Montefiore, H. (2014). Enigma: bitka za šifru. Zagreb : Profil knjiga. str. 398.*
[4] *Kahn, D. (1979). Šifranti protiv špijuna 3. Zagreb : Centar za informacije i publicitet. str. 92.*

7. Američka kriptologija u Drugom svjetskom ratu

Od 1919. do 1929. SAD se, što se tiče kriptoanalize, oslanjao na Crni kabinet (The Black Chamber) koji je najpoznatiji po tome što je u Prvom svjetskom ratu razbio kodove japanske diplomacije. Crni kabinet je službeno raspušten 1929. pod izgovorom ministra vanjskih poslova Henryja Stimsona da „džentlmeni ne čitaju tuđa pisma“[5]. Kriptološka djelatnost tada je prebačena u Službu veze koja je zato osnovala Signal Intelligence Service. SIS je vodio William Friedman, a njihov zadatak bio je priprema šifara i kodova za kopnenu vojsku i presretanje i dekriptiranje neprijateljskih poruka.

Ratna mornarica imala je vlastitu dekriptersku službu, Sekciju za kodove i signale (Code and Signal Section) koja se službeno zvala OP-20-G. Unutar nje poručnik Laurence Safford osnovao je radio-prislušnu službu kojoj je zadatak bio interceptiranje i dekriptiranje poruka, većinom japanske mornarice. Imala je mnoštvo stanica na sjeveru Atlantskog oceana pomoću kojih je interceptirala njemačke poruke iz podmornica i, nakon ulaska SAD-a u rat, svojim informacijama pomogla pri potapanju mnogih podmornica; taj se sustav zvao HF/DF (high frequency direction-finding, odnosno visokofrekventno utvrđivanje smjera).

Iako je SAD zahvaljujući Crnom kabinetu bio uspješan u kriptoanalizi, njihovi su diplomati u Prvom svjetskom ratu i u međuratnom razdoblju koristili kodove koje je bilo lako ukrasti i razbiti – razbili su ih i njemački Pers Z i japanska Sekcija za ispitivanje kodova. Kodovi su bili toliko nesigurni za korištenje da je predsjednik Franklin D. Roosevelt radije koristio kodove američke ratne mornarice.

30-ih godina 20. stoljeća američka kopnena vojska (a kasnije i Ministarstvo vanjskih poslova) koristila je M-138-A, aparaturu baziranu na Jeffersonovom kotaču koja je umjesto diskova koristila trake. Pers Z je razbio i taj sustav, no u međuvremenu se vojska prebacila na SIGTOT, stroj koji je radio na Vernamovom principu, te ga dala na korištenje i američkoj diplomaciji.

Kao i Njemačka, i SAD je koristio stroj s rotorima. Bio je to model M-134-C koji je konstruirao Friedman, a ujedno je to bio i prvi stroj koji je nastao zajedničkim naporima SIS-a i OP-20-G-a koji dotad nisu surađivali. Kopnena vojska taj je uređaj zval SIGABA, a ratna mornarica ECM MARK II. Imao je čak petnaest rotora, a Friedman mu je dodatno povećao sigurnost sustava tako što je dodao telegrafsku vrpcu koja je pomoću impulsa kontrolirala

[5] *Kahn, D. (1979). Šifranti protiv špijuna 2. Zagrev : Centar za informacije i publicitet. str. 166.*

pokretanje rotora, tako da su se pokretali nasumično. Za razliku od Enigme, taj stroj neprijateljski kriptoanalitičari nikad nisu uspjeli razbiti, a njegovu neprobojnost potvrdila je i Signal Security Agency, posebna grupa unutar kopnene vojske koja se bavila testiranjem neprobojnosti američkih sustava za šifriranje.

Slika 6: SIGABA

7.1. Američki kriptolozi protiv japanskih kriptologa

Japanska mornarica koristila je kod JN-25 (to su mu ime dali američki kriptoanalitičari). Kod je bio numerički te je imao i aditivne grupe pomoću kojih bi se kodovi prešifrirali. Nakon napada na Pearl Harbor 7. prosinca 1941., rad OP-20-G-a i triju stanica na Pacifiku (Pearl Harbor, Singapur i Filipini) bio je usmjeren na razbijanje tog koda, budući da je Japan planirao napad na strateški važan otok Midway. Budući da je kod imao više izdanja (od kojih se najsigurnijim smatrao JN-25b) i zato što su se knjige s aditivnim grupama često mijenjale, američki kriptoanalitičari nikako nisu uspijevali razbiti cijeli sustav. Jedan od razloga tog neuspjeha bio je taj što su se američki državnici više zanimali za dekriptate koji su stizali iz japanskog stroja PURPLE.

Za slanje diplomatskih poruka Japanci su koristili stroj 97-shiki-obun In-ji-ki, odnosno „stroj za šifriranje 97“, kojem su Amerikanci dali jednostavnije ime – PURPLE. PURPLE je bila japanska verzija Enigme – imala je razvodnu ploču i rotore (njih četiri) i koristila je latinicu. Danas nijedan taj stroj nije sačuvan, no SIS, predvođen Friedmanom, uspio je prvo napraviti svoju repliku (svojevrsnu američku „bombu“), a zatim i razbiti sustav. Razbijanje šifre PURPLE-a spada u savezničku operaciju MAGIC koja je, slično kao i ULTRA, organizirana da interceptira i dešifrira protivničke kodove (u ovom slučaju japanske). Jedna od najvažnijih informacija dobivenih dešifriranjem poruka PURPLE-a su podaci o strategiji Japana u bitki kod Midwayja – jedna od poruka sadržavala je plan odvlačenja američkih brodova dalje od otoka da bi ih Japanci mogli uništiti i zauzeti otok. To je omogućilo Amerikancima da ostanu blizu otoka i obrane ga.

Još jedan vrijedan alat protiv Japanaca Amerikanci su pronašli u indijanskom plemenu Navajo. Američki inženjer Philip Johnston odrastao je u rezervatu tog plemena u Arizoni te je bio jedan od rijetkih ljudi van plemena koji su znali komplicirani Navajo jezik. Upravo ga je to potaknulo da smisli neprobojan kod za američku vojsku koja se borila protiv Japanaca – predložio je jednom potpukovniku da svaka jedinica na Pacifiku ima dva Indijanca kao radiooperatere koji bi prevodili poruke na svoj jezik i onda ih prenosili. Smatrao je da je to neprobojan sustav jer je jezik imao kompleksnu gramatiku, govorio se na vrlo malom području te nije bilo pisanih tragova. Jedini problem bilo je prevođenje imena i naziva modernih uređaja za koje Indijanci nisu imali izraze, no to je riješeno tako što su za nazive uređaja koristili svoje riječi ili neologizme (npr. podmornicu bi zvali „željezna riba“), a imena bi slovkali pomoću engleskih riječi koje bi onda preveli na Navajo. Tijekom jedne demonstracije poruka je prevedena na Navajo, prenesena i prevedena natrag na engleski za nekoliko sekundi, što je bilo mnogo brže od bilo kojih strojeva koje je dotad koristila vojska. „Navajska kodna pričala“ bila su važan dio ratovanja na pacifičkom bojištu jer je slano mnogo poruka, a svaka je bila bez pogreške. Ovaj jedinstveni način kodiranja otkriven je javnosti tek 1968.

8. Zaključak

Kriptologija se netom prije početka Drugog svjetskog rata ubrzano razvila na svim svojim područjima te u ratu prikazala svu svoju snagu, odnosno koliko može utjecati na sudbinu neke zemlje. Kao u svakom ratu, informacije do kojih dolaze obavještajne službe od velike su važnosti, no kad su te informacije enkriptirane, sve ovisi o kriptoanalitičarima. Drugi svjetski rat bi se po mnogočemu mogao nazvati kriptološkim ratom, odnosno borbom kriptografa i kriptoanalitičara. Po Davidu Kahnu (1979), razlika između kriptografije i kriptoanalize je sljedeća:

> „Kriptoanaliza može izmijeniti *status quo*; kriptografija ga može, u najboljem slučaju, sačuvati. Kriptoanaliza može gurnuti države u rat (…). Kriptoanaliza može mijenjati svijet; kriptografija to ne može."

Drugi svjetski rat to jasno ilustrira – najviše u slučaju Enigme, stroja koji je Saveznicima donio mnoge pobjede u bitkama, a za čije su probijanje zaslužni upravo kriptoanalitičari (uz malu pomoć jednog njemačkog špijuna).

9. Literatura

Callahan, K. (2013). *The Impact of the Allied Cryptographers on World War II: Cryptanalysis of the Japanese and German Cipher Machines*. <http://math.gcsu.edu/~ryan/13capstone/papers/callahan.pdf>. Pristupljeno 6. rujna 2015.

Freeman, W., Sullivan, G. & Weierud, F. (2003). *Purple Revealed: Simulation and Computer-Aided Cryptanalysis of Angooki Taipu B*. Cryptologia, 27(1), 1-43. <http://cryptocellar.web.cern.ch/cryptocellar/pubs/PurpleRevealed.pdf> Pristupljeno 6. rujna 2015.

Kahn, D. (1979). *Šifranti protiv špijuna 2, 3, 4*. Zagreb : Centar za informacije i publicitet.

Mucklow, T. J. (2015). *The SIGABA/ECM II Cipher Machine: „A Beautiful Idea"*. National Security Agency, Center for Cryptologic History. <https://www.nsa.gov/about/_files/cryptologic_heritage/center_crypt_history/publications/The_SIGABA_ECM_Cipher_Machine_A_Beautiful_Idea3.pdf> Pristupljeno 6. rujna 2015.

Sebag Montefiore, H. (2014). *Enigma: bitka za šifru*. Zagreb : Profil knjiga.

Singh, S. (2003). *Šifre: kratka povijest kriptografije*. Zagreb : Mozaik knjiga.

Christos military and intelligence corner. *Italian codebreakers of WWII*. <http://chris-intel-corner.blogspot.hr/2012/08/italian-codebreakers-of-wwii.html>. Pristupljeno 6. rujna 2015.

Crypto Museum. *SIGABA*. <http://cryptomuseum.com/crypto/usa/sigaba/index.htm>. Pristupljeno 6. rujna 2015.

Encyclopedia of Espionage, Intelligence, and Security. *Operation Magic*. <http://www.faqs.org/espionage/Nt-Pa/Operation-Magic.html>. Pristupljeno 6. rujna 2015.

National Security Agency. *Pearl Harbor Review - JN-25*. <http://www.nsa.gov/about/cryptologic_heritage/center_crypt_history/pearl_harbor_review/jn25.shtml> Pristupljeno 6. rujna 2015.

Navajo Code Talker. *Navajo Code Talkers History*. <http://navajopeople.org/navajo-code-talker.htm> Pristupljeno 6. rujna 2015.

Secret Intelligence Service. *GCHQ*. <http://www.sis.gov.uk/our-history/gchq.html>. Pristupljeno 6. rujna 2015.

TICOM Archive. *OKW/Chi (High Command)*. <http://www.ticomarchive.com/the-targets/okw-chi>. Pristupljeno 6. rujna 2015.

TICOM Archive. *Origin of TICOM*. <http://www.ticomarchive.com/home/origin-of-ticom>. Pristupljeno 6. rujna 2015.