UNIVERZA V LJUBLJANI

FAKULTETA ZA DRUŽBENE VEDE

JURE SOKLIČ

VLOGA KRIPTOGRAFIJE V ČASU II. SVETOVNE VOJNE

Diplomsko delo

LJUBLJANA, 2002

UNIVERZA V LJUBLJANI

FAKULTETA ZA DRUŽBENE VEDE

JURE SOKLIČ

MENTOR: doc.dr. DAMIJAN GUŠTIN

VLOGA KRIPTOGRAFIJE V ČASU II. SVETOVNE VOJNE

Diplomsko delo

LJUBLJANA, 2002

Kazalo

1. Uvod

1.1. Uvod

Proučevanje kriptografije druge svetovne vojne, tako kodiranja kot dekodiranja kod in njenih implikacij na potek vojne, je pomembno, saj je igralo zelo pomembno vlogo skozi vso vojno in končno tudi močno vplivala na njen izid. Izšlo je veliko del in bilo izdelanih veliko dokumentarnih oddaj o razbijanju nemške kode Enigme, bolj točno mornariške Enigme, medtem ko o drugih kodah, prav tako pomembnih, skoraj ni bilo govora. Mornariška Enigma je le ena od mnogih šifer, ki so bile v uporabi med drugo svetovno vojno, dejstvo pa je, da je bila ena najbolj zahtevnih za dešifriranje in verjetno tudi zato najbolj poznana. Odločil sem se predstaviti najpomembnejše šifre štirih največjih udeleženk spopada: Nemčije, Japonska, ZDA in Velike Britanije, vendar se ne bom bistveno posvetil načinom kodiranja le-teh, ker bi to moje delo naredilo statistično, matematično, temveč predvsem posledicam uspehov in neuspehov kriptografskih spopadov. Skušal bom pokazati vlogo teh v nekaterih najpomembnejših operacijah in bitkah, ki so pomenili strateške zasuke in tako pričajo o pomembnosti vloge kriptografije v vojskovanju.

Pri oblikovanju diplome in navajanju literature si pomagam z navodili za pisanje seminarske naloge in diplomskega dela, ki so bila izdana na katedri za mednarodne odnose FDV, avtorjev dr. Bojka Bučarja, doc. dr. Zlatka Šabiča in as. mag. Milana Brgleza.

1.2. Metodološki pristop

Metoda mojega dela bo zgodovinska analiza, s pomočjo katere bom analiziral primarne in sekundarne vire in poskušal pridobljene podatke ovrednotiti in iz njih pridobiti informacije, ki me zanimajo.

1.3. Hipoteze

Splošna hipoteza

Preprečitev dešifriranja z različnimi postopki, tako posrednimi kot neposrednimi, je ključnega pomena za zmago v boju, operaciji, vojni.

Izvedene hipoteze

Razkritje mornariške Enigme je bilo poglavitni razlog za zmago zaveznikov nad silami osi v Evropi.

Kompliciranost šifriranja ni nujni pogoj za preprečitev dešifriranja s strani nasprotnika

Operacija Magic s strani ZDA ima največ zaslug za zmago nad japonsko mornarico v bitki pri Midwayu.

1.4. Opredelitev temeljnih pojmov

Za razumevanje teksta v nadaljevanju se zdi pomembno, da najprej opredelim temeljne kriptološke pojme. Opredelil bom le najpomembnejše, tiste, ki se najpogosteje uporabljajo, ostale pa bom razložil med tekstom.

Kriptologija je beseda, ki izvira iz grških besed kriptos (skrito) in logos (veda), in označuje vedo o skrivnem komuniciranju. (Glossary) Deli se na kriptografijo in kriptoanalizo. Kljub temu je raba izrazov kriptologija in kriptografija pogosto sopomenska in slednji izraz tudi pogosteje uporabljan. Poimenovanje kriptologija se več uporablja pri označevanju in raziskovanju tehničnih (matematičnih) vidikov vede, medtem ko se pri opisovanju in raziskovanju širših implikacij teh postopkov bolj uporablja izraz kriptografija. Odločil sem se

za uporabo izraza **kriptografija**, v katerega zajemam tako kriptografski kot tudi kriptoanalitični del vede.

Odprti tekst (plaintext) je tekst sporočila, preden se mu doda tajnost. Ponavadi je pisan v maternem jeziku kriptografov.

Kriptografija je postopek, transformacije odprtega teksta v šifriran ali kodiran tekst. Obstajata dva načina, transpozicija ali premeščanje, pri katerem se zamenja vrstni red črk, in substitucija, kjer črke obdržijo svoje mesto, vendar so zamenjane z drugimi.

Zelo pomembno je razlikovanje med šifro in kodo. **Kode** so sestavljene iz veliko besed, fraz, črk in njihovih substitutov (npr. 3964 London, 1232 onemogočen itd.).
Pri **šifrah** pa je osnovna enota črka, včasih črkovni par, zelo redko pa večja skupina črk (diagram, biagram). Kode so torej sestavljene iz lingvističnih celot, medtem ko šifre razdelijo le-te na manjše dele. Pri kriptografiji lahko pride tudi do mešanja obeh načinov. Tak sistem pa imenujemo nomenklatorski.

Pri večini šifrirnih sistemov se uporablja **ključ (key)**, sistem o razporejanju črk v šifrirni abecedi, obrazec razporejanja pri transpoziciji, nastavitev začetnih črk pri strojih za šifriranje itd. Če se za ključ uporablja neka številka, beseda ali fraza, govorimo o ključni besedi, ključni frazi ali ključni številki. Tudi te so lahko podvržene substituciji ali transpoziciji.
Šifrirani ali kodirani odprti tekst lahko imenujemo z več sinonimi, šifrirani tekst, šifrat, kodirani tekst, **kriptogram**.

Dešifriranje ali dekodiranje pomeni obratno transformacijo, torej spreminjanje kriptogram v odprti tekst, pod pogojem, da oseba, ki to počne, pozna ključ. V tem smislu je to legitimen proces. Rezultat dela imenujemo dešifrat. Če pa kdo ključa ne pozna in vseeno to počne, potem govorimo o **kriptoanalizi** ali o razbijanju kod (code-breaking). Rezultat dela pa se imenuje dekriptat.

Tekste, ki jih pošiljamo nekodirane, imenujemo **en clair** poslani teksti ali tudi nekriptografirani teksti. (Kahn, 1979: 7-12)

2. Zgodovina kriptografije

Ko je Julij Cezar osvojil Galijo, je sporočil v Rim: EHOE JEOLME MH TEBGHOMHRE RE ZTL GHOH. Rimski vladar ni bil prvi, ki je svoje sporočilo napisal s tajno pisavo, je bil pa prvi, ki je le-to začel sistematično uporabljati. Že stari Hebrejci so začeli uporabljati metodo šifriranja, ki se imenuje temurah, kar dobesedno pomeni zamenjavo, in temelji na tem, da so 22 črk svoje abecede razdelili na dva dela ter ju v obrnjenem vrstnem redu zapisali drugega pod drugim. S tem so dobili šifrirno tabelo, s katero so po želji zamenjevali črke. Ta metoda je uporabljena na določenih delih tudi v Svetem pismu, kjer so večinoma to besedne igre, v vsaj enem primeru pa gre tudi za sporočilo, ko namreč prerok Jeremija kliče prekletstvo nad kralje sveta, še posebej nad kralja dežele Šešak. Na prvi pogled se zdi, da je to kralj neznane dežele, če pa uporabimo šifrirno tabelo, ugotovimo, da gre za kralja Babilona.
(Osredkar, 1999: 11)

V Enejevem vojaškem priročniku iz časa antike pa je opisan še boljši način šifriranja, ki se je ohranil v rabi skoraj do današnjih dni. Ta priporoča, da se v kaki knjigi ali drugem dolgem besedilu z iglo pod ustreznimi črkami naredijo komaj opazne luknjice, tako označene črke, brane po vrsti, pa tvorijo sporočilo. Nemški vohuni so z iglicami označevali črke še v prvi svetovni vojni, v drugi pa so jih označevali z nevidnim črnilom. Za nesumljivo osnovno besedilo pa so uporabljali časopis.

Med vsemi antičnimi vojskovodji je Julij Cezar menda najpogosteje pošiljal šifrirana sporočila. Imel je precej enostaven način šifriranja, vsako črko je zamenjal s črko, ki v abecedi leži tri mesta pred njo. Njegov nečak in prvi rimski cesar, Avgust, je uporabljal podoben sistem, vendar je vsako črko zamenjal s črko, ki leži za njo. Ahajec Polibij, grški zgodovinar, pa je izumil drug sistem, ki se je v različici ohranil vse do današnjih dni. S številkami je označil stolpce in vrstice, tako da je bila vsaka črka označena z dvema številkama. Prva pomeni stolpec, druga pa vrstico, v kateri je zaznamovana črka.

Prvi mehanski pripomoček za pošiljanje šifriranih sporočil, lesen valj, imenovan skital, so si približno 400 let p. n. š. izmislili Špartanci. Sporočilo so napisali na papirus, navit na leseno

palico. Ko so papirus odvili, so bile črke pomešane, ko pa je prejemnik sporočila papirus zopet navil na svojo palico, pa je postalo razumljivo. Druga kriptografska priprava pa se je imenovala astragal. To je bila 25-krat prevrtana palica, na kateri je vsaka luknja ustrezala eni črki. Zapisovanje je potekalo tako, da so skozi luknje, ki ustrezajo zaporednim črkam odprtega sporočila, vlekli tanko nit. Tako je nastal zapleten klobčič, sporočilo pa so prebrali tako, da so vlekli nit iz lukenj in sproti zapisovali črke.

Arabci so se prav tako ukvarjali s kriptografijo. Vse njihovo znanje s tega področja je leta 1412 v svoji enciklopediji Sub al aša sistematiziral egipčanski učenjak Al Kalkašandi. V poglavju z naslovom O skrivanju skrivnih sporočil v pismih najprej trezno ugotavlja, da bi sporočila poleg naslovnika utegnila zanimati še koga drugega, včasih s škodljivimi posledicami za pošiljatelja in prejemnika. Nato pojasni, da je za pošiljanje skrivnih sporočil najbolj primeren kakšen nepoznan jezik. Pove, da obstaja sedem načinov šifriranja, ki temeljijo na zamenjavi, premeščanju črk, uporabi sličic in številk namesto črk in podobno. Na koncu pa govori o postopkih dešifriranja tajnih sporočil.

Leta 1404 se je v Firencah rodil Leon Battista Alberti, ki je zaostanek na področju kriptografije Zahoda proti arabskemu svetu več kot izničil. Napisal je esej, v katerem opisuje razne sisteme šifriranja, zamenjavo, premeščanje … Opiše tudi novo napravo, ki si jo je izmislil, in sicer dvojno ploščo z vrtljivim srednjim delom. Na stoječem in vrtljivem delu plošče sta vgravirana obroča z abecedami, ki ju je mogoče zasukati drugega proti drugemu. Šifrer in prejemnik sporočila se pred izmenjavo le-tega dogovorita za ključno črko na vrtljivem obroču, ki jo nato nastavita na drugo črko na drugem obroču. Za dešifriranje bi sedaj zadostovalo le odčitati zaporedno črko in bi bil to običajen postopek zamenjave, vendar gre tu Albert še dlje. Po tem postopku se šifrira le nekaj besed, potem pa se vrtljivi obroč zopet zasuče, kar pa pomeni, da dobijo s tem črke zopet nov pomen in je sporočilo še težje dešifrirati. Takšen sistem imenujemo polialfabetski.

Šifriranje je postajalo vedno bolj in bolj komplicirano, kajti napredovala je tudi kriptoanaliza, tako so se morali kriptologi precej truditi, da nezaželjeni bralci niso razumeli njihovih sporočil.

Leta 1790 je Thomas Jefferson izumil šifrirno kolo, s katerim je mehanično kodiral in dekodiral sporočilo. To metodo so kasneje začeli množično uporabljati šele v drugi svetovni vojni. (Dupuis, 1999)

Konec obdobja polialfabetskega šifriranja je pomenila leta 1861 izdana knjiga o rešitvi polialfabetskega šifriranja, katere avtor je pruski vojaški poveljnik Friedrich W. Kasiski. V njej je pojasnil načine kriptoanalize tega načina šifriranja. S tem je ta način šifriranja postal preveč ranljiv, da bi bil lahko še množično uporaben za najvišje nivoje skrivne komunikacije.

Skozi stoletja je prihajalo do vse večjih skritih spopadov držav na tem področju, to področje pa je tudi vedno bolj pridobivalo na pomenu. Razmah pa se je zgodil šele v 20. stol. z razvojem modernih komunikacij in uvedbo množičnih armad. (Singh, 1999: 31-67)

3. Kriptografija med II. svetovno vojno

Po letu 1920 je razvoj mehanike in elektromehanike pripeljal do velikega napredka na področju kriptografije, razvitja kolesnega sistema šifriranja. Kolesni sistem se je uporabljal že prej, vendar je šele Američan Edward Hebern izpopolnil ta sistem s povezavo več koles, ki so se vrtela s pomočjo električnih impulzov. Od leta 1921 je Hebern sestavil serijo kolesnih šifrirnih naprav, ki jih je ocenila mornarica ZDA. Nedvomno je bilo to delo, ki je omogočilo vodilno vlogo ZDA na tem področju med drugo svetovno vojno. Skoraj istočasno sta v Evropi Nizozemec Hugo Koch in Nemec Arthur Scherbius ločeno razvila koncept koles in razvila predhodnico najbolj znane šifre druge svetovne vojne Enigme.

Do začetka druge svetovne vojne se je močno izpopolnil kolesni način šifriranja, tako da je močno zmanjšal možnost ponovitve zamenjane črke in s tem povečal varnost šifre. Prišlo je do navideznega onemogočenja kriptoanalize, za katerega pa se je kasneje pokazalo, da je bil le začasen. Sistem kod se je še vedno uporabljal, vendar le pri manj pomembnih komunikacijah in komunikacijah, kjer šifrirni stroji niso bili na voljo. Šifrirni stroji so bili podobni pisalnim strojem, vendar niso sami zapisovali šifriranega teksta, pač pa je moral operater iz njega odčitati zamenjano črko.

Vse velesile so razvile svoje sisteme strojnega šifriranja, ki so jih tudi veliko uporabljale med vojno. Nemčija je za namen strojnega šifriranja razvila Enigmo, Japonska Purple code, ZDA Sigabo in Velika Britanija TypeX. Sistem delovanja teh šifer je bil dokaj podoben, razlikovala se je predvsem uporaba. Enigmo je Nemčija uporabljala do najnižjih ravni poveljevanja, uporabljale pa so jo tudi železnice, velika trgovska podjetja, vladni uradi itd. Japonska je zaradi razbitja svojih kod v dvajsetih letih 20. stoletja razvila šifro Purple, ki je bila mešanica Hebernovega stroja in nemške Enigme, uporabljala pa sta jo predvsem vojna mornarica in zunanje ministrstvo. ZDA so razvile šifrirni stroj imenovan Sigaba, ki so ga uporabljali predvsem na najvišjih nivojih komunikacije, med visokimi vojaškimi poveljstvi in vladnimi uradi. Velika Britanija pa je svojo šifrirno napravo TypeX uporabljala le na najvišjih nivojih komuniciranja.

Vsaka država je imela veliko število kod in šifer, nekatere so bile bolj enostavne, druge spet bolj kompliciranе. Med njimi je vzpostavljena hierarhija, uporabljajo pa se glede na tajnost sporočila. Večje število kod se uporablja zaradi zmanjševanja števila sporočil, napisanih v eni kodi, kar pa bistveno oteži delo kriptoanalitikom. Strojno šifriranje je bilo šifriranje, ki se mu je med drugo svetovno vojno najbolj zaupalo, zato je bilo uporabljeno za najbolj tajno komunikacijo, vsa ostala komunikacija pa se je še vedno opravljala s pomočjo kod.

Z razvitjem strojne kriptografije pa so se razvile tudi izpopolnjene kriptoanalitične metode, celo kriptoanalitični stroji. Tako je med celotno drugo svetovno vojno potekala skrita vojna, vojna kriptografov in kriptoanalitikov, ki je imela velik vpliv na potek vojne.

Kriptografija in kriptoanaliza se je izvajala na posebej za to organiziranih državnih službah. Nekatere države so imele to delo centralizirano v eni službi, druge pa so organizirale več podobnih služb na različnih ministrstvih. Naloga kriptografskih služb je bila razviti uspešne kriptografske metode in s tem zagotoviti varnost lastnih sporočil, naloga kriptoanalitičnih služb pa s pomočjo kriptoanalize brati sovražnikova sporočila.

Poznavanje namenov drugih držav, pomemben del tega poznavanja je izviral iz dešifriranih sporočil, je za vsako državo pomenilo veliko prednost, zato so vse države v času pred drugo svetovno vojno in med njo temu področju namenjale vse večjo pozornost in sredstva. Informacije dobljene z dešifriranjem sporočil drugih držav so se nato koristno uporabljale

predvsem v vojski, pomembne pa so bile tudi za diplomacijo, obveščevalne službe in druge večje sisteme, ki so delovali v okviru države. (BBC MMII, 2001)

4. Japonske šifre in operacija Magic

4.1. Japonske šifre in kode

Najenostavnejša japonska koda je bila LA, ki je dobila ime po oznaki LA, ki je bila na začetku vsakega kodiranega sporočila. Sistem kodiranja je deloval tako, da so pisma napisana s znaki kata kana[1] (Duane, 1995) prevedli v latinico in da se je zaradi varčevanja s prostorom ponekod besede skrajševalo. Kodo LA je bilo zelo lahko razbiti, delno zato, ker se je uporabljal vse od leta 1925, deloma pa zaradi statističnih pravilnosti v konstrukciji. Tako so se vsi kata kana znaki, ki so se končevali na e, imeli kodne ekvivalente, ki so se začeli s črko A itd. Ta koda ni bila tako pomembna, ker so z njo kodirali le rutinske administrativne zadeve.

Kriptografsko stopničko višje je bil sistem, ki so mu Japonci dali ime Oite, Američani pa PA-K2. Bil je podoben kodi LA, vendar je bil obsežnejši, kodne skupine pa so bile razmetane. Sistem ni bil zahteven za ameriške kriptoanalitike, za razvozljanje sporočila pa so v povprečju porabili tri dni. S to kodo se niso šifrirala pomembna sporočila, razen v enem primeru, ko je japonski konzulat v Honoluluju, potem ko je uničil kode višjega ranga, poslal svoje zadnje sporočilo kodirano v tej kodi.

Največ so Japonci uporabljali serijo šifer imenovanih TSU, pri Američanih imenovanih z J., ki je pomenila prvo črko v oznaki šifre. Te šifre so imeli več znakov kot vse prejšnje, bile so bolj pomešane, transpozicija pa je bila izpopolnjena. Pri teh šifrah se je tudi bolj pogosto menjal sistem transpozicije. Tako se je sistem v pol leta zamenjal iz J17-K6 na J18-K8 in potem J19-K9. S tem sistemom so šifrirali vohunska poročila o premikih bojnih ladij, aktivnosti vojske, ki so jih rutinsko po svetu pošiljali japonski konzulati Tokiju.

[1]Abeceda za zapis japonskega jezika, močno podobna Morsejevi abecedi, vendar vsebuje dvakrat toliko kombinacij dolgo kratko.

Kriptoanalitiki so imeli največ težav s transpozicijo, v praksi pa je pomenilo, da so potrebovali po mesec dni, da so razbili šifro J18-K8. Za razbijanje vsakega razporeda, ki se je menjal vsak dan, pa je bila potrebna nova analiza. Hitrost razbijanja šifre je bila odvisna predvsem od količine prestreženih sporočil kodiranih z istim ključem, 10 do 15 odstotkov sporočil šifriranih s to šifro pa ni bilo nikoli dešifriranih.

Situacija pa se je povsem spremenila s šifro JN-25 ali PURPLE. Ta šifra je bila zelo zahtevna, vendar so kljub temu Američani uspevali razbiti 97 odstotkov ključev, večina depeš pa je bila dekriptirana v samo nekaj urah. Vse to je bila posledica določenih pravilnosti v šifriranju in pravilnosti pri menjanju ključev. PURPLE je bil sistem, ki je bil na začetku precej težji za rešitev od J19-K9. Razbijanje te šifre je bila ena najtežjih kriptoanalitičnih nalog druge svetovne vojne.

Službeno ime tega stroja za šifriranje je bilo 97-shiki O-bun In-ji-ki (prev. alfabetski pisalni stroj 97). Japonci so ji kasneje pravili samo stroj, japonska mornarica pa ji je dala oznako J. Ta je napravo kupila od Nemcev (ENIGMA), jo priredila za svoje potrebe, kasneje pa posodila zunanjem ministrstvu, ki jo je še dalje modificiralo. Če so hoteli sporočilo šifrirati s tem strojem, so morali najprej pogledati v debelo knjigo strojnih šifrirnih ključev YU GO, potem vtakniti žice v razvodnik po ključu, ki je veljal za tisti dan in pravilno namestiti štiri okrogle diske. Prvi stroj je tipkal odprti tekst, drugi pa je sprejemal impulze in tipkal šifrat. Dešifriranje je potekalo v obrnjenem vrstnem redu. Ta alfabetski pisalni stroj je pisal v latinici in ne z znaki kata kana.

Ko so Američani ugotovili, da ne morejo več brati japonske šifre, so najprej hoteli ugotoviti, za kakšno šifro gre. Dotedanji uspehi s šifro RED, predhodnico šifre PURPLE in nekaterimi drugimi šiframi so jim pomagali, da so se spoznali z načini naslavljanja v japonski diplomaciji, poznali so fraze v diplomatskem jeziku in stil pisanja. To jim je pomagalo pri kreiranju spiska najbolj verjetnih besed in izrazov. Pri kriptoanalizi jim je močno pomagala tudi nepazljivost japonskih kriptografov. Zgodilo se je, da je japonsko zunanje ministrstvo pošiljalo eno sporočilo več ambasadam. Kakšen nepazljiv kriptograf je pomotoma šifriral sporočilo za eno ambasado s sistemom PURPLE, drugo sporočilo pa s kakšno lažjo kodo, ki je bila Američanom že znana. Počasi so, glede na verjetnost, teorijo sklopov, kongruenco in druge kriptoanalitične postopke, izdelali približek stroja na papirju. Na podlagi tega je dal Signal intelligence service, služba, ki se je v ZDA ukvarjala s kriptoanalizo, izdelati kopijo

stroja, ki bi postopke, ki so jih kriptoanalitki delali ročno, naredil strojno. Kljub temu da originala niso videli, so naredili zelo podoben dvojnik tako v izgledu kot v kriptografskem smislu. Vse to se je zgodilo po 20 mesecih najintenzivnejše analize. Ko so uspeli ugotoviti še, da Japonci kreirajo ključe za devet dni naprej, in ugotoviti vzorec, po katerem to delajo, je bilo delo že precej enostavno, ker so morali priti le do ključa za prvi dan, ostale so nato brez težav predvideli. Kljub temu, da je bila strojna šifra J najbolj uporabljana šifra japoncev med drugo svetovno vojno, pa se je določen del najbolj tajnih sporočil kodiral z admiralsko kodo, ki je bila običajna koda zapisana v kodnih knjigah, vendar zelo redko uporabljana in zato dokaj težka za razbitje. (Kahn, 1979c: 37-52)

4.2. Operacija Magic

4.2.1. Predzgodovina operacije Magic

Predzgodovina razvoja kriptoanalitične opracije ZDA proti Japonski, imenovane MAGIC, sega v leto 1919, ko je Herbert Yardley prepričal zunanje in obrambno ministrstvo, da ustanovita sekcijo, ki se bo stalno ukvarjala s kreiranjem in razbijanjem kod, imenovano Črni kabinet (BLACK CHAMBER). Glavna naloga kabineta je bila razbijanje japonskih diplomatskih kod in šifer.

28. novembra 1921 je Črni kabinet dosegel prvi večji uspeh. Prestregli in razbili so sporočilo Tokija japonskemu ambasadorju v ZDA, kjer mu dajejo navodila, kako naj se obnaša in kakšno stališče naj zavzema na washingtonski pomorski konferenci o omejevanju oboroževanja. Ameriškemu državnemu sekretarju je bilo to v veliko pomoč in zlahka je dosegel boljši dogovor pri določitvi razmerja sil na Pacifiku. Kljub temu uspehu pa se je leta 1929 pokazalo, da je bil Črni kabinet povsem nekoristen in zato drag za vzdrževanje. Njegov predstojnik Herbert Yardley je večino svojega časa posvečal kreiranju komercialnih kod, nepremičninskemu posredovanju in svetovanju podjetjem o vprašanjih kriptografije. Ko se je vse to razkrilo, je državni sekretar Henry Stimson sekcijo razpustil, z znamenito izjavo:,, Gospodje ne berejo tujih pisem.`` Yardley je kasneje v knjigi objavil vse o razbitju japonske diplomatske šifre, obstajajo pa tudi namigovanja, da je informacije že prej prodal Japoncem. Posledica tega je bila, da so Japonci spremenili kodo in jo izpopolnili, s tem pa zopet naložili ameriškim kriptoanalitikom ogromno dela. (Aldrich, 2000: 123-135)

Leta 1921 je ustanovila vojaška mornarica vzporedno s Črnim kabinetom kriptografsko pisarno, imenovano ONI (Office of Naval Intelligence), katere predstojnik je bil Andrew Long. V tem času se zgodita dva ključna dogodka, ki imata pomembne implikacije za kasnejšo vojno v Pacifiku. Long močno poveča število častnikov, učencev japonskega jezika na ambasadi v Tokiju, poročnik Ellis Zacharias, strokovnjak za protiobveščevalno dejavnost, pa je vdrl na japonski konzulat v ZDA, kjer je naredil fotokopijo trenutne japonske mornariške kode imenovane Rdeča koda (RED CODE).

Po ukinitvi Črnega kabineta, je vojska ustanovila nov kriptografski oddelek, imenovan Signal intelligence service. Poveljnik je bil general Gibbs, njegov direktor tega oddelka pa William F. Friedman, visoko usposobljen kriptoanalitik še iz časa med prvo svetovno vojno, ki se mu pripisujejo zasluge za razbitje PURPLE CODE-a.

Leta 1924 prevzame poveljstvo nad sekcijo, ki se ukvarja z razbijanjem kod, poročnik Laurence Safford. Zbere se skupina kriptoanalitikov, kjer v v strogo zaščiteni sobi 2646 stare mornariške zgradbe začnejo razbijati Rdečo kodo, to jim kmalu tudi uspe in s tem omogočijo dostop do vseh pomembnih informacij o moči, premikih, namenih japonske mornarice.

Leta 1925 je bila na Guamu postavljena radioprisluškovalna baza, ki je bila namenjena prestrezanju japonskaih sporočil. Ta baza je sporočila pošiljala sekciji za razbijanje kod, ki brez tega ne bi mogla delovati, kajti pri kripto-analizi je ključnega pomena prestreči čim več sporočil, da se lahko potem uporabijo matematične in statistične metode. Baza na Guamu je bila pomembna zaradi lokacije, ki ji je omogočala prestrezanje ogromnih količin sporočil.
Leta 1925 je ameriška mornarica naredila nov pomemben korak na področju radijskega prisluškovanja. Josepha Rocheforta, poročnika bojne ladje, je umaknila s položaja obveščevalnega častnika na letalonosilki Indianapolis in mu dala nalogo reorganizirati in povečati učinkovitost radioprisluškovalne baze v Pearl Harbouru. Imel je tri ključne sposobnosti, poznavanje kriptoanalize, radijskega prisluškovanja in znanje japonskega jezika, zato je postal eden najpomembnejših kriptoanalitikov druge svetovne vojne. Glavna tarča Rochefortovega delovanja je bila admiralska koda, koda, v kateri so se šifrirale najbolj tajne depeše. Razbitje te kode od leta 1926 do 1940 je močno pripomoglo pri zbiranju informacij ZDA o japonski mornarici. Leta 1940 pa se je pojavila nova različica admiralske kode, štiričrkovna koda s transpozicijskim prešifriranjem, ki za določen čas zopet pusti ZDA v temi.

Po pomembnosti takoj za admiralsko kodo pa je bil kriptografski sistem glavne operativne flote, ki ga je Japonska tudi največ uporabljala in je bil narejen prav zaradi domnevne Yardleyeve izdaje. Sestavljala so ga petštevilčne kode, katerim so bili kot ključ dodane še druge številke, tako da je bil sistem še težji za razvozljanje. Službeni naziv te kode je bil JN-25b (Japanese Navy) ali tudi PURPLE CODE, kot so jo imenovali Američani. Prvo razbitje dela sporočila šifriranega s to kodo zaznamuje rojstvo operacije MAGIC (dešifriranje japonskih sporočil), ki je močno pripomogla, če že ne odločilno pripomogla k zmagi ZDA proti Japonski na Pacifiku. (Henson, 1995)

4.2.2. Japonski napad na Pearl Harbour

V začetku leta 1941 se je na japonski strani močno domnevalo, da se vojni ne bo mogoče izogniti. Glede na to je Isoroku Jamamoto, vrhovni poveljnik združene flote Cesarske vojne mornarice, izdelal načrt napada na Pearl Harbour[1], z razlago, da če ne bodo tam uničili Pacifiške flote, ne bodo imeli dobrih izgledov za zmago v vojni.

V tistem času je potekala ”vojna” med obveščevalnimi in protiobveščevalnimi službami obeh držav. Obe strani sta hoteli čim več zvedeti o namenih, premikih, pripravljenosti nasprotnih sil. Američani so najprej, ko je bilo to še možno, uporabljali metodo opazovanja japonskih ladij s svojih trgovskih ladij, vohunjenja na ambasadah itd. Japonci pa so prav tako pošiljali svoje vohune na konzulate, kjer so zbirali podatke o sovražnikovih enotah, te pa so tako ali drugače šifrirane pošiljali domov s pomočjo radiotelegrafije. Japonska je uporabljala veliko število kodov, včasih tudi privatni kod neke japonske banke.

Napad je Jamamoto načrtoval za dan 8. decembra.1941 (po tokijskem času), za poveljnika napada pa je postavil viceadmirala Čuičija Naguma. Nekaj dni kasneje je 32 ladij udarne eskadre skrivaj izplulo iz luk na Japonskem in se usmerilo proti severu na kraj sestanka, ki je bil pri kurilskem otoku Etoforju. V eskadri so je bilo šest velikih letalonosilk, dve bojni ladji, tri križarke, petnajst rušilcev in pomožne ladje. Ladje so za seboj pustile svoje radiotelegrafiste, ki so imeli nalogo še vedno pošiljati rutinske depeše.

[1] Pearl Harbour je glavno pristanišče ameriške vojne mornarice za Pacifik na Havajih, v katerem je bil zasidran največji del Pacifiške flote.

Ko se je zbirala eskadra za napad, pa je japonsko ministrstvo za zunanje zadeve, ki za napad ni vedelo, pač pa je vedelo, da je situacija zelo napeta in kritična, sprejelo sistem odprte kode, za primer, če se pojavi potreba po čim hitrejši komunikaciji (npr. grožnja prekinitve diplomatskih odnosov se je označevala z severni dež z vetrom itd.). Sporočilo o sprejetju te kode je prestregla ameriška baza na Bainbridge Islandu. Ko so sporočilo, šifrirano s kodo JN-19, dešifrirali, so ugotovili, da morajo začeti spremljati tudi japonski radio, v čigar oddajanju se tudi lahko skriva skrivno sporočilo.

Nekaj ur po tem je japonski ambasador v Washingtonu, admiral Kičisaburo Nomura, izročil Hullu japonski ultimat. V primeru, da bi ga ZDA sprejele, bi to pomenilo čisto spremeniti svojo zunanjo politiko v azijskem prostoru, kar pa zanjo ni bilo sprejemljivo.

Tokijo je ambasadorju poslal sporočilo, da je skrajni rok, za ureditev odnosov med državama 25. november, razen če podpis pogodbe zaradi objektivnih ni možen, takrat se lahko rok premakne do najkasneje 29. novembra 1941.

25. novembra 1941 je admiral Jamamoto izdal ukaz eskadri, pripravljeni za napad na Pearl Harbour, da naslednji dan izpluje. Eskadra je izplula 26. novembra ob 18.00 proti jugu, v vode praznega oceana, kjer ni bilo ladijskega prometa in je bila tako možnost, da bi jo opazili, majhna. Če pa bi se to slučajno zgodilo pred 6. decembrom, je bil ukaz, da se vrnejo, v primeru pa, da bi se to zgodilo 7. decembra je imel admiral Nagumo proste roke.
Američani so medtem sestavili svoj odgovor, v katerem so zahtevali, da se Japonska umakne s Kitajske, v zameno pa so ponudili ponovno vzpostavitev trgovine in odmrznitev japonskega imetja v ZDA. Še isti večer so službe ZDA posnele pogovor med ambasadorjem in Tokijem, v katerem je bil Roosvelt imenovan gospa Kimiko, japonsko-ameriški pogovori ženitna ponudba, vprašanje Kitajske San Francisco itd.

29. novembra je japonski ambasador v Berlinu, baron Ošima, sporočil Tokiju, da se bo Nemčija takoj vključila v vojno, če Japonska napove vojno ZDA. Odgovor Tokija je bil, da obstoji velika nevarnost, da se bo vojna začela, lahko tudi naslednji dan. Ti dve sporočili sta bili prevedeni 1. decembra, Roosveltu pa se je drugo zdelo tako pomembno, da je naročil kopijo za lastni arhiv.

Da je situacija napeta, je 1. decembra ugotovil tudi poveljnik prisluškovalne baze v Pearl Harbourju, Rochefort, ko je japonska flota prerazporedila 20.000 klicnih signalov svojih ladij, kar je naredila že po 30 dneh veljave prejšnjih. V poročilu dne 1. decembra 1941, kje se nahajajo velike letalonosilke, je ONI napisal, da so še vedno v domovinskih vodah. Da je prišlo do te napake, so bili krivi Japonci, ker so uspešno zmedli ameriške kriptoanalitike s pošiljanjem sporočil po sistemu dežnika.[1] Vsaka ladja je imela tudi več pozivnih signalov, pošiljale pa so se tudi lažne depeše.

2. decembra, po dveh dneh analiziranja novih pozivnih signalov, je Rochefortova enota napisala v poročilu, da nimajo nobenih novih informacij o lokaciji letalonosilk. Sumljivo pa se jim zdi, da po preverjenih 200 klicnih številkah ladij ni niti ene letalonosilke. To je lahko pomenilo le, da je komuniciranje med njimi zmanjšano na minimum.

Američani so dešifrirali tudi sporočilo, v katerem Tokijo daje navodila, kako se v primeru potrebe uniči kode. Nekaj dni prej pa so dešifrirali sporočilo, kako uničiti šifrirni stroj PURPLE. Ti sporočili so si Američani razlagali, kot še en preventivni ukrep zaradi bližajoče se ofenzive na britanske in nizozemske posesti v južni Aziji. Kljub vsem tem sumljivim sporočilom pa so ZDA slepo verjele v to, da se jim ne more nič zgoditi.

2. decembra je eskadra namenjena za napad na Pearl Harbour dobila sporočilo NIITAKA-YAMA NOBORE (povzpnite se na vrh Niitake[2]), kar je pomenilo, da je sprejeta odločitev o vključitvi v vojno. Ladje so se iz lastnih tankerjev oskrbele z gorivom in nadaljevale plovbo proti Havajem.

3. decembra je bilo prestreženo sporočilo, v katerem se daje ukaz ambasadam, da uničijo kode, razen enega primerka koda PA-K2 in kode za skrajševanje LA. Ko je minister za zunanje zadeve Welles prebral to sporočilo, je rekel, da so se sedaj možnosti za izognitev vojni zmanjšale na ena proti tisoč.

5. decembra je minister za zunanje zadeve Japonske Togo sprejel predstavnika generalštaba in mornarice ter z njuno pomočjo dodelal zadnjo japonsko noto ZDA. V tej noti se zavrača

[1] Vsa sporočila pošljejo vsem ladjam, nato pa one izbirajo katero je namenjeno njim.

[2] Niitako-Yama poznana tudi pod imenom Mount Morrison (3886 m) takrat najvišja gora na Japonskem

Hullova ponudba z dne 26. novembra, konča pa se z besedami, da želi japonska vlada le obvestiti ZDA, da nadaljevanje pogovorov zaradi stališča ameriške vlade ne bi imelo smisla. Haška konvencija iz leta 1907 prepoveduje napad brez predhodnje vojne napovedi, Togo jo je želel upoštevati, menil pa je, da ta nota zadostuje, saj je več kot očitno to že vojna napoved. Nota je bila odposlana 6. decembra. Noto, ki je imela 14 delov, so na japonski ambasadi prepozno dešifrirali in prepisali, tako, da je bil izročena že po napadu na Pearl Harbour, Američani pa so njeno vsebino zaradi uspešne kriptoanalize že poznali.

7. decembra 1941 ob 7.53, dve minuti preden je padla prva bomba na Pearl Harbour, je Fučida, poveljnik prvega vala letal zaklical: Tora, Tora, Tora (tiger, tiger, tiger), kar je bila kodna beseda za napad. Napad na Pearl Harbour se je začel, napad, ki je bil eno največjih presenečenj druge svetovne vojne, ki ga je Japoncem uspelo prikriti, čeprav so Američani s pomočjo operacije MAGIC že brali večino kodiranih sporočil. (Kahn 1979c: 58-120)

4.2.3. Bitka pri Midwayu

Japonsko carsko vrhovno poveljstvo je 5. maja 1942 izdalo 18. povelje vojaški mornarici. Po tem povelju naj bi vojaška mornarica v sodelovanju s kopensko vojsko napadla in zasedla strateške točke na zahodnih Aleutih in otok Midway.

V operaciji naj bi sodelovalo več kot 200 ladij, zato se je temu primerno povečal tudi radiopromet. Čeprav se je večina ladij že nahajala v Japonskem morju, pa je bilo treba veliko letalonosilk, bojnih, transportnih ladij in tankerjev obvestiti, naj se vrnejo in se zberejo v Hirošimskem zalivu. Iz Jamamotovega štaba, ki se je nahajal na največji bojni ladji na svetu Jamato, je bilo po radijski zvezi poslanih mnogo ukazov, ki so jih ZDA prestregle in jih v veliki večini, okoli 90%, dešifrirale. Japonska mornarica je naredila napako, kajti datum uvedbe nove kriptografske kode je znova že drugič odložila za en mesec. Razlogi za to so bili predvsem v oddaljenosti japonskih enot od Japonske in v dosedanjih uspehih njihove vojske, ki so po njihovem mnenju kazali na to, da njihova koda ni bila razbita.

Admiral Nimitz, poveljnik pacifiške flote ZDA, je po tem, ko je v njegov štab začelo prihajati veliko sporočil, zaslutil, da Japonska pripravlja novo veliko ofenzivo. Takoj je nazaj v Pearl Harbour poklical letalonosilke Hornet, Enterprise in Yorktown. V poročilu obveščevalne

službe Pacifiške flote je dobil opozorilo, da se predvideva, da bo sovražnik izvedel operacijo, katere cilj bo zavzetje Dutch Harbourja na Aleutih. Nimitz je to napoved sprejel, vendar je predvideval, da bo ta operacija, če bo izvedena, le diverzija. Zato je bilo še vedno odprto vprašanje, kje in kdaj bo izveden glavni napad. Po njegovem prepričanju, naj bi bil to Midway, po prepričanju admirala Kinga, načelnika generalštaba vojne mornarice, pa Oahu, največji otok v Havajskem otočju.

Jamamoto je vedel, da je doseganje tako strateškega kot taktičnega presenečenja neprecenljivo pomembno za sam izhod operacije, zato je predvidel ameriški protinapad na mestu, kjer bodo najbolje pripravljeni. Poleg tega je razpolagal z veliko kvantitativno prednostjo v vojaški tehniki. V njegovi operativni eskadri je bilo 11 bojnih ladij, 5 letalonosilk, 16 križark in 49 rušilcev. Nimitz pa je razpolagal s preostalimi ladjami Pacifiške flote, v kateri so bile 3 letalonosilke, 8 križark in 14 rušilcev. 20. maja je Jamamoto poslal svojim enotam operativno povelje, v katerem je bila točno določena taktika, ki se bo uporabila v operaciji. Operacija naj bi se začela 3. junija 1942 z diverzantskim napadom na Aleute. Ko bodo tako zmedli Nimitzove sile, se bo začelo bombardiranje Midwaya, z namenom razbiti njegov garnizon. Ko bo ameriška flota priplula iz smeri Pearl Harbourja, da bi Midway branila, jo bodo napadla letala s torpedi in potopila večino ladjevja. Z ostalimi bodo obračunale bojne ladje, križarke in rušilci. Tako bodo uničili še preostanek Pacifiške flote, močno načete že z napadom na Pearl Harbour.

Jamamotovo operativno povelje so prestregle prisluškovalne baze na Pacifiku. Dolžina kriptograma je takoj implicirala na njegovo pomembnost. Po približno enem tednu zahtevne kriptoanalitične operacije je bila večina kriptografa dešifrirana. Šifrirani so ostali le deli, v katerih so bile napisane lokacije, datumi in čas japonskih operacij. Ti so bili kodirani s polialfabetskim sistemom, ki nikoli ni bil razbit, saj se je pojavil le v treh primerih. Mesto in čas napada so zato poskušali izračunati z drugimi metodami, hitrostjo ladij, smerjo itd.

Vprašanje, kje bo izveden napad, je rešila Combat Intelligence Unit, ameriška vojaška obveščevalna služba. Japonci so geografske lokacije označevali s pomočjo kart s kodiranimi koordinatami. Ta sistem se je imenoval CHI-CHE. Ameriški kriptoanalitiki so že prej uspeli delno dekodirati tako karto in so odkrili koordinate Pearl Harbourja. Nekaj tednov pred dogodkom, o katerem sedaj govorimo, so bile prestrežene kodne koordinate z oznako AF v sporočilu dveh japonskih izvidniških letal, ki so preletela Midway. Kontekst je bil takšen, da

so ameriški kriptoanalitiki prišli do zaključka, da AF pomeni Midway. Tako so lahko z veliko mero verjetnosti predpostavljali, da je cilj napada Midway, ker so se te koordinate nahajale tudi v Jamamotovem ukazu. Za preveritev domneve so z Midwaya poslali en clair sporočilo o tem, da se je pokvarila črpalka za vodo. Čez dva dni so Američani dešifrirali sporočilo, v katerem so Japonci sporočili, da je AF ostal brez pitne vode. Sedaj je ostalo odprto le še vprašanje datuma. Obveščevalna služba je naredila mozaično strukturo zgrajeno iz različnih predpostavk, ocen, dejstev, verjetnosti in prognoz, s katero je po temeljiti analizi predvidevala, da bo verjetni napad na Midway dne 3. junija. Podatki so bili zanesljivi in verjetni, vendar še zdaleč niso bili to, kar bi bili, če bi kripto-analitikom uspelo dešifrirati sporočilo.

Admiral Nimitz je 27. maja 1942 izdal svoj operativni načrt 29-42, v katerem je med drugim povedal, da se pričakuje sovražnikov napad na Midway. Letalonosilkam je ukazal, naj izplujejo in se usmerijo proti cilju POINT LUCK, ki se je nahajal približno 350 morskih milj severovzhodno od Midwaya. Tako bi bila njihova pozicija, bočno na japonske sile, s tem pa močno zmanjšana verjetnost, da bi jih sovražnik odkril.

1. junija 1942 so Japonci končno uvedli novo kodo JN25-c, ki je za nekaj časa pustila kriptoanalitike ZDA v temi, vendar je bilo to za operacijo Midway brez pomena, ker so bili vsi operativni načrti izdelani in poslani že prej. Japonci so se držali postavljenega programa, tako da so najprej, dne 3. junija napadli Aleute, bombardirali Dutch Harbour in se nato umaknili. Nimitz je poslal v aleutske vode Severno pacifiško floto križark in rušilcev, da si zaščiti bok. Japonsko eskadro so opazila izvidniška letala iz Midwaya, medtem ko ameriških letalonosilk Japonci niso. Zato je japonski poveljnik Nagumo ukazal, da se letala, ki so bila prej pripravljena za obrambo, pripravijo za napad na kopenske cilje na Midwayu. Ravno v trenutku, ko so Japonci menjali bojni komplet bomb na letalih, ko se je v letala pretakalo gorivo, so se pojavila ameriška letala in krenila v napad, uspeh ameriških letal je bil tako bistveno večji. V boju, ki je trajal tri dni, so Američani potopili vse štiri letalonosilke, sami pa izgubili le eno. Jamamoto je potem, ko je videl, da je poražen, ukazal umik.
(Kahn, 1979c: 225-237)

4.2.4. Smrt admirala Jamamota

Poleti 1943 je v Rabaul prišel admiral Isoroku Jamamoto, da bi dobil boljši pregled nad situacijo v Solomonskem otočju, ki se je hitro slabšala. Odločil se je, da bo opravil enodnevni obhod baz na severnih otokih Solomonskega otočja. Za ta korak se je odločil zaradi dvigovanja morale in preverjanja svojih enot. Za Japonce je to pomenilo, da morajo o tem obvestiti vse baze, da se lahko dostojno pripravijo na sprejem vrhovnega poveljnika Združene flote. Sporočilo, ki je vsebovalo urnik potovanja, je pet dni prej poslal poveljnik 8. flote, kodirano s kodo JN-25, ki so jo Američani že dalj časa uspešno brali.
V sporočilu je pisalo, da bo odhod poveljnika ob 6. uri zjutraj iz Rabaula s srednjim jurišnim letalom, ki ga bo spremljalo 6 lovskih letal. Ob 8. uri bo prihod na Ballale, takoj odhod na Shortland s protipodmorniško ladjo, prihod na Shortland ob 8 uri 40 minut itd. V sporočilu je tudi pisalo, da se v slučaju slabega vremena obhod prestavi za en dan.

Američani so vedeli, da je Jamamoto točen, saj se vsakega sestanka drži na sekundo točno, zato je bil dekripat, ki so ga imeli v rokah, smrtna obsodba tega visokega poveljnika. Vprašanje je bilo le, če naj se obsodba tudi izvrši. Nimitz in njegov štab so sedaj tehtali argumente za in proti. Vprašanje je bilo, če se izvrši napad, ali ni nevarnosti, da na njegovo mesto pride nekdo drug, ki je bolj sposoben in njemu superioren, ali pa je Jamamoto nezamenljiv. Ameriška obveščevalna služba je dala oceno, da je Jamamoto dominantna osebnost japonske vojske, visoko energičen, inteligenten in sposoben poveljnik, zato bi vsaka oseba, ki bi ga zamenjala bila njemu inferiorna, poleg tega pa bi njegova smrt močno demoralizirala Japonce. Ljudje v ZDA so ga sovražili, saj je bil prav on tisti, ki se je domislil načrta napada na Pearl Harbour, zraven pa se še hvalil, da bo on diktiral mirovne pogoje v Beli hiši. Nevarnost atentata na Jamamota je bila tudi ta, da bi potem Japonci lahko ugotovili, da Američani berejo njihova sporočila. Zato so si Američani izmislili izgovor, da so jih o Jamamotovem letu obvestili domačini v okolici Rabaula. Admiral Nimitz je nato podpisal povelje za napad. Napad na Jamamota je bil izveden leta 1943 v največji tajnosti, prav zaradi razloga, da Japonci ne bi ugotovili, na kakšen način so prišli do podatkov o Jamamotovem obhodu.

Operacija, ki so jo nato izvedli Američani, je morala biti na sekundo točna, kajti 14 lovcev P-38, ni imelo dovolj goriva, da bi na Jamamota čakalo v zraku. Vse je šlo po načrtu. Točno, kot je bilo predvideno, so opazili eskadriljo letal. Eno letalo se je takoj usmerilo na Jamamotovo

letalo, ki se je hotelo izogniti tako, da je letelo čisto nad drevesi. Izmik se ni posrečil, kajti pilot P-38 Lanphair je poveljniško letalo sestrelil.

Japonski radio je objavil novico, da je admiral Jamamoto hrabro umrl v vojaškem letalu v bitki s sovražnikom. (Kahn, 1979c: 269-278)

4.2.5. Skrivanje obstoja operacije Magic

Obstoj operacije MAGIC je bil skrbno varovana skrivnost. Zanjo je vedelo relativno malo ljudi, dejanja, ki so sledila zaradi dešifriranja, pa so bila skrbno načrtovana in ne nujno posledica kompromitacije šifre. V dveh primerih pa je vseeno prišlo do nevarnosti javne potrditve obstoja operacije.

Prvi je bil po zmagi ZDA v bitki pri Midwayu, ko je Chicago Tribune objavil članek o tem, kako so ZDA točno vedele za načrt japonske mornarice in zato zmagale. Niti na enem mestu, niti posredno niso bili omenjeni japonski kodi in ameriška prisluškovalna služba, vendar se je mornarica bala, da bi Japonci vseeno lahko prišli do zaključka, da so vse to lahko vedeli samo z branjem njihovih sporočil. Ameriška vlada je ustanovila komisijo, ki naj bi ugotovila, če je bil z objavo članka kršen Zakon o vohunstvu, vendar do javne obravnave nikoli ni prišlo, prav zaradi možnega velikega odmeva v javnosti, ki bi lahko Japonce opozorila na dogodek. Da Japonci nikoli niso izvedeli za članek v časopisu, je verjetno posledica nesposobnosti njihove obveščevalne službe. (Aldrich, 2000: 145-150)

Druga situacija, v kateri bi lahko bila ogrožena tajnost operacije, pa se je zgodila leta 1944, ko se je republikanska stranka potegovala za zmago svojega kandidata Thomasa E. Dewneya na predsedniških volitvah. V svoji kampanji je ta skušal diskreditirati svojega nasprotnika s tem, da je razglašal, kako se je Pearl Harbour zgodil le zaradi malomarnosti demokratske administracije, posredno pa obtoževal Roosvelta, da je za napad vedel, vendar ni ukrepal, ker je želel, da se ZDA vključijo v vojno. To ni bilo res, vendar pa ni bilo nasprotnih dokazov, zato so nekateri temu verjeli. Poveljnik ameriške vojske general Marshall se je po tem odločil za samostojen korak in je brez vednosti predsednika poslal Dewneyu pismo, v katerem mu je potrdil obstoj operacije MAGIC, razložil dogodke pred napadom na Pearl Harbour in ga prosil, če o tej zadevi ne govori nikomur. Prosil ga je, da naj iz svoje kampanje odstrani

vsebino, ki bi lahko močno škodovala državi in lahko povzročila smrt tisočev ameriških vojakov na Pacifiku. Po dveh dneh premišljevanja in posvetovanja s svojimi svetovalci se je Dewney odločil, da razbijanja kod ne bo več omenjal. Na volitvah leta 1944 je bil močno poražen, vendar bi imel malo možnosti, četudi bi nadaljeval s svojo prejšnjo kampanjo. (Kahn, 1979c: 285-291)

5. Kriptoanaliza šifer in kod ZDA

5.1. Šifre in kode ZDA

ZDA so v času pred drugo svetovno vojno in tudi med njo, prav tako kot druge države uporabljale veliko število šifer in kod, ki so bili med seboj prav tako hierarhično strukturirane. Prav tako so različne kode uporabljale vojna mornarica, kopenska vojska, letalstvo, diplomacija, trgovska mornarica itd. (SIGTOT, BROWN, GREY, SIGABA…) Odločil sem se, da bom podrobneje obdelal le dva kriptografska sistema, ki sta najbolj pomembna, predvsem zaradi nezmožnosti sovražnika, da bi jih kriptoanaliziral in zaradi svoje posebnosti šifriranja in kodiranja, in sicer električno šifrirno napravo vojaške mornarice in kopenske vojske za kodiranje najbolj tajnih sporočil imenovano SIGABA ter sistem kodiranja s pomočjo Indijancev plemena Navajo, kot posebnost druge svetovne vojne.

5.1.1. ECM Mark II – SIGABA

SIGABA, električno šifrirno napravo, sta razvili pred drugo svetovno vojno vojaška mornarica in kopenska vojska ZDA. Ideja za napravo, ki bi uporabljala električno kontrolirane rotorje, je prišla s strani kriptografskega strokovnjaka W. F. Friedmana. To idejo je že uporabil v predhodnici SIGABA-e, M-134, ki je imela pet rotorjev, ki so kodirali tekst, obrati pa so bili kontrolirani s preluknjanim trakom. Papirnati trak je imel luknjice, ki so zavrtele rotor naprej. Frank Rowlet, inženir in konstruktor SIGABE, je pri svoji napravi

uporabil sistem koles, ki kontrolirajo kolesa pri obratih. To pa je dalo videz, da se črke pojavljajo naključno. SIGABA-o je sestavljalo 15 koles od katerih jih je bilo deset klasičnih velikih koles in pet malih. Vsa ta so bila razdeljena v tri skupine. Pet tako imenovanih šifrirnih koles je šifriralo črke, pri vsaki pa so se premaknili naprej. Njihovo premikanje naprej so kontrolirali električni impulzi, ki so določili za koliko mest naprej naj se premaknejo. Drugih pet koles se je imenovalo kontrolna kolesa, saj so usmerjala električni impulz do kodnih koles. Zadnjih pet t. i. indeksnih koles je bilo nastavljenih ročno, pošiljali pa so električne impulze kontrolnim kolesom. Nastavljeni so bili po ključu, ki je bil takrat v veljavi. Zadnjih pet koles je torej usmerjalo obrate vseh petnajstih koles, njihova kombinacija pa je določila črko, ki je zamenjala črko sporočila.

SIGABA je bila šifrirna naprava, močno podobna nemški Enigmi, vendar za razliko od nje nikoli ni bila kompromitirana. Razlog je večji del v nesposobnosti japonske kriptoanalize, del pa tudi v kompliciranosti šifriranja. Sistem je bil v uporabi vse do leta 1959.
(The ECM Mark II, http://home.ecn.ab.ca/~jsavard/crypto/ro0205.htm)

5.1.2. Kriptografija s pomočjo Indijancev plemena Navajo

Začetnik ideje kriptografije s pomočjo jezika Navajev je bil Philip Johnston, civilni inženir iz Los Angelesa. V časopisu je malo pred začetkom vojne prebral, da oklepna divizija, nameščena v Louisiani, uporablja jezike Indijancev za skrivno komunikacijo. Zelo dobro je poznal jezik Navajev, ker so bili njegovi starši misionarji pri tem plemenu. Ideja o uporabi indijanskega jezika ni bila nova, vendar pa je bila nova ideja o uporabi jezika Navajev. Vso to svojo zamisel je predstavil vojski.

Johnston je vedel, da bo ta jezik v ta namen dober, ker je zelo kompleksen in izoliran. Naglas in že samo barva glasu lahko spremeni besedi pomen. Jezik pa tudi nikoli ni bil pisan, zato je težko, da bi ga poznal nekdo, ki ni pripadnik plemena. Predlagal je, da koda ne bi bila le prevod v jezik Navajev, temveč koda izpeljana iz tega jezika.
Johnstonov predlog je bil sprejet, zato je vojska začela mobilizirati indijance plemena Navajo in jih učiti kriptografije. Najprej so se naučili 211 vojaških terminov in jim določili

ekvivalentno kodno besedo. Nič niso smeli zapisati, temveč so si vse zapomnili. Obstajala so štiri osnovna pravila:

- Kodne besede so morale biti v logični povezavi s terminom, ki so ga označevale.
- Kodne besede so morale biti nenavadno zgrajene.
- Kodne besede so morale biti kratke.
- Kodne besede so si morale biti različne, da bi se izognili zamenjavi.

Navaji so potem dodali še abecedno kodo, s katero so označevali imena, kraje in termine, za katere niso imeli ekvivalenta.
Leta 1942 je bilo vseh Navajev 50.000, 540 jih je služilo pri marincih. 375 do 420 jih je bilo usposobljenih šifrantov, ostali so služili drugje. Šifranti so odšli v enote marincev, ki so se bojevale na Pacifiku. Njihova naloga je bila, da so prenašali sporočila o taktiki in premiku enot, ukazih in drugih pomembnih zadevah na bojišču. Za komunikacijo so uporabljali radio in telefon. Prednost takega prenosa je bila, da je bil hiter, šifriranje in dešifriranje pa zaradi enostavnih metod hitro in natančno, kar pa je na bojišču ključnega pomena. Japonska kriptoanaliza je bila proti tem kodu nemočna.

Indijanci plemena Navajev so ostali pomembni za državo še po drugi svetovni vojni, saj je bila kriptografija, zgrajena na podlagi njihovega jezika, zaradi uspešnosti, potencial tudi za kasneje. Zato so vso zadevo držali v strogi tajnosti. ZDA so jim šele pred kratkim izrekle hvaležnost za dosežke med drugo svetovno vojno. (Molnar, 1997)

5.2. Japonska kriptoanaliza-oddelek Tokumu Han

Japonska cesarska vojaška mornarica se je s kripto-anlizo začela ukvarjati leta 1925. Takrat je bil v ta namen formiran skrivni oddelek, imenovan Tokumu Han. Zaposloval je šest ljudi, 4 matematike in 2 lingvista, nameščen pa je bil na ministrstvu za mornarico. Prvi uspeh tega oddelka je bila razrešena koda ameriškega State Departmenta, imenovana GRAY. Kodo so razbili s klasično tehniko uporabe statističnih in matematičnih metod. Reševali so tudi kitajske kriptograme v času japonske invazije na Mandžurijo. Vendar pa Tokumu Han ni uspelo razbiti ameriške dvodelne kode, npr. kode BROWN, State Departmenta, kode ameriške vojaške mornarice in kod, ki jih je Yardley, ameriški kriptograf, vnesel v kitajsko komunikacijo. To pa seveda ne pomeni, da ni bil razbita nobena od teh kod. Včasih je

Japoncem preboj uspel predvsem zaradi ugodnih okoliščin. Taka situacija je nastala 26. aprila 1936, ko jim je uspelo zapleniti večjo količino šifriranih diplomatskih poročil. Nekaj časa so lahko zato brali vsa ameriška sporočila, med njimi tudi sporočila vojaškega pomorskega atašeja. To pa je bilo kratko obdobje, kajti Američani so kmalu sisteme šifriranja zamenjali.

Japonci so se znašli tudi na druge nedekriptološke načine. Konec leta 1937 so vlomili v ameriški konzulat v Kobeju in fotografirali kodo Brown in šifrirno napravo M-138, ki so jo takrat Japonci prvič videli in si s tem pomagali pri kriptoanalizi.

V času japonskega napada na Pearl Harbour je Tokuma Han zaposloval 20 ljudi, ki so bili vsi častniki, po tem napadu pa se je zaradi močno povečanega radioprometa, povečalo tudi moštvo. Prvi kontingent rekrutov, šestdeset, so pripeljali iz raznih šol in fakultet za tuje jezike, ekonomskih fakultetet in trgovskih šol. Bili so prvi civilisti v tem kriptološkem oddelku.

Za razliko od ameriških kriptografskih organizacij, ki so uspele razbiti večino japonskih kodov in uspele brati večino sporočil, tudi tiste šifrirane z najboljšimi sistemi, pa Tokumu Hana ni uspelo izvleči nobenih pomembnejših informacij iz dekriptiranih sporočil. Sporočil srednjega in visokega nivoja niso niti poizkušali dekriptirati, saj so sistemi močno presegali njihove sposobnosti. Zato so se koncentrirali le na tri enostavne kripto-sisteme, ki so jih uporabljala le najnižja ameriška poveljstva, vendar so tudi tu dosegali omejene uspehe.
Njihove kriptoanalitične uspehe lahko pokažemo na kodu ameriških izvidniških letal, imenovanem AN-103. Ta kod je sestavljalo nekaj deset izrazov, menjali pa so se vsakih sedem do deset dni. Na srečo ZDA so Japonci za dekriptiranje sporočil potrebovali toliko časa, da so bila sporočila že brez prave uporabne vrednosti.

Relativno boljše uspehe so imeli s kodo BAMS, dvodelno prešifrirano kodo, ki so jo uporabljale zavezniške trgovske ladje. Dokler je bila ta koda v uporabi, so Japonci dekriptirali okoli 50% sporočil šifriranih s to kodo. Sistem je bil relativno zapleten, uspehe pa so dosegali, ker so od Nemcev kupili bazno knjigo kode BAMS, ki so jo ti zaplenili na neki trgovski ladji. Vendar pa so tudi v tem primeru velikokrat delovali prepočasi in informacije niso bile več uporabne.

Največ moči pa so pripadniki Tokumu-a Hana namenili šifrirnem sistemu CSP 642, sistemu šifre na traku, ki so jo uporabljala nižja ameriška poveljstva. Uporabljali so metodo verjetnih besed, jih nato zlagali skupaj in tako dobili najbolj verjeten odprti tekst kriptograma. Zraven so polagali trakove, tako da se je na koncu oboje izšlo, s tem pa so dobili ključ za tisti dan. Kljub temu da je na tej kodi delalo 40 in več ljudi, pa do konca vojne niso dosegli nobenega uspeha, ki bi imel pomembnejše implikacije na potek vojne.
Največ, kar so dosegli, je bilo dokaj verjetno predvidevanje cone, v kateri bo prišlo do napada. To so lahko storili na podlagi nedekriptiranih sporočil, ki so jih iz določene cone pošiljala letala in podmornice. Čas pa so določili s pragmatičnimi izkušnjami iz prejšnjih ameriških operacij ali pa s pomočjo komunikacijskih fenomenov, kot so povečano število izvidniških sporočil ali pa prepoved oddajanja. Tako so vedeli, da Američani pripravljajo invazijo na Filipine, vendar so lahko le na mesec natančno določili, kdaj bo do napada prišlo. Otoka, ki naj bi ga napadli, pa niso mogli določiti. V štirih letih vojne so pripadniki Tokuma Hana samo enkrat uspeli pravočasno obvestiti enote na Marshalovih otokih, naj se pripravi na napad.

Poleg Tokumu Hana, ki je bil mornariški kriptološki oddelek, pa je imela tudi vojaška obveščevalna služba kopenske vojske organiziran oddelek, ki se je ukvarjal s kriptoanalizo. Rezultati so bili prav tako slabi, uspelo pa jim je dekriptirati le del komunikacij med gverilci ozemelj zasedenih s strani Japonske. Najboljše rezultate so dosegali leta 1943, ker se je močno povečalo število sporočil, gverilci pa še niso začeli uporabljati novih sistemov kriptografije. Japonci so stare sisteme uspešno brali predvsem zato, ker jim je uspelo zapleniti primerke med boji. (Kahn, 1979c: 247-258)

6. Nemške šifre in operacija ULTRA

6.1. Nemške šifre

6.1.1. Enigma

Šifrirno napravo imenovano Enigma je leta 1919 patentiral berlinski inženir Arthur Scherbius. Bila je elektro-mehanska naprava, katere šifriranje je temeljilo na polialfabetski zamenjavi črk odprtega teksta. Po različnih modifikacijah ga je v uporabo leta 1926 uvedla nemška mornarica, 1928 kopenska vojska in 1935 letalstvo. Uporabljali so jo tudi vojaška obveščevalna služba Abwehr, varnostna služba Sicherheitsdienst, varnostna policija Sicherheitspolizei, železnice, velika trgovska podjetja in vladni uradi. (Code breaking in the World War II, 1999)

Od uvedbe Enigme v uporabo do konca druge svetovne vojne je bila Enigma večkrat modificirana, odvisno od službe, ki je Enigmo uporabljala.

Prva različica Enigme je bila namenjena samo šifriranju in dešifriranju sporočil. Če gledamo skozi oči operaterja, je bila sestavljena iz tipkovnice, ki je imela 26 črk v obliki normalnega nemškega pisalnega stroja, brez številk in drugih znakov. Za to tipkovnico je bila plošča, na kateri je bilo 26 okroglih lučk, na njih pa je bila enaka črkovna razporeditev kot na tipkovnici. Operater je po vnosu črke v Enigmo na njeno mesto prepisal črko, katere lučka je zagorela. Šifrirna enota se je nahajala za ploščo z lučkami, sestavljalo pa jo je pet koles, skrajni dve, ki sta bili stalni, in tri sredinska, ki so se lahko menjala. Stalno kolo na desni (Eintrittwalze) je bilo neposredno povezano s tipkovnico, imelo pa je 26 izhodov na levi strani. Levo nepremično kolo (Umkehrwalze), ki je imelo prav tako 26 izhodov, je bilo namenjeno, da črko, ki jo dobi, šifrira in jo pošlje nazaj po drugi poti. Tri centralna kolesa so se izbirala iz škatle, ki je vsebovala pet koles, njihov položaj pa je narekoval ključ, ki se je menjal vsak dan po mesečnem razporedu. Ta kolesa so imela vhode in izhode prav tako za 26 črk. Vsakič, ko je operater pritisnil tipko s črko, se je desno kolo zavrtelo za eno pozicijo. Ko se je zavrtelo za 26 pozicij, je zavrtelo še njemu levo kolo itd. S tem so dosegli, da se črke skoraj nikoli niso ponovile, skoraj pa zato, ker je obstajala matematična verjetnost ponovitve, vendar je bila

zanemarljivo majhna. Nikakor pa se črka ni mogla zamenjati z isto črko. Vojaške Enigme so za razliko od komercialnih imele še ploščo s 26 odprtinami, imenovano Steckerbrett (vtična plošča), kjer so med seboj povezali po dve in dve črki. Delovanje je torej potekalo tako, da je operater pritisnil črko, ki jo je vtična plošča zamenjala s črko, ki je bila povezana s to črko. Nato je ta črka potovala skozi vsa kolesa, se zamenjala, pri zadnjem reflektirala in potovala nazaj, nato pa prižgala lučko nad črko, ki jo je zamenjala v šifriranem tekstu. Operater je nato črko prepisal na papir in tako celo besedilo. Šifriran tekst je nato poslal po radiu, na drugi strani pa je operater ponovil postopek v obratni smeri in tako dobil en clair sporočilo.

Enigma kopenske vojske in letalstva je imela tri sredinska kolesa, ki jih je operater izbral izmed petih, mornariška Enigma pa je imela komplet osmih koles. Pri različici mornariške Enigme, imenovane tudi Kriegsmarine Enigma, ki so jo leta 1942 začele uporabljati podmornice, je bilo uvedeno še četrto sredinsko kolo, kar je naredilo to različico najbolj zahtevno za kriptoanalitike. (Stripp, 1998)

6.1.2. Nemška šifra Lorenz SZ40/42

Leta 1940 so prisluškovalne enote britanske policije prvič prestregle nov tip sporočila, signal, ki ni bil v Morsejevi abecedi. Nemška vojska je začela uporabljati nov tip pošiljanja sporočil, teleprintersko zvezo z mednarodno Baudotovo kodo[1], za šifriranje in dešifriranje sporočil pa je začela uporabljati novo šifro imenovano Lorenz SZ40/42.

Metodo, ki je bila uporabljena pri tej šifri, je izumil matematik Gilbert Vernam v ZDA že leta 1918, tako da so vsi poznali metodo spreminjanja črk v bitni zapis, vendar nobeden ni točno poznal oznak in spreminjanja teh pri nemški šifri Lorenz. Ta šifrirna naprava je vsebovala 12 koles, ki jih je operater nastavil po dnevni nastavitvi. Ta so nato določila dnevno bitno oznako za določeno črko, možnost, da bi se en zapis ponovil, pa je bila skoraj ničelna, vsaj po prepričanju Nemcev. Delno se je zapis ponovil na vsakih 41 istih črk in to je dalo britanskim kriptoanalitikom možnost, da z zapletenimi, dolgotrajnimi matematičnimi postopki to šifro kompromitirajo. Napravi so dali delavci Bletchley parka kodno ime Tunny, sporočilom šifriranim s to šifro pa Fish. (BBC MMII, 2001)

Šifra je bila razbita, vendar pa je bil postopek predolg in je naredil informacije neuporabne, zato so v Bletchley parku, organizaciji, o kateri bom podrobneje govoril kasneje, leta 1944 izdelali prvi računalnik na svetu, imenovan Colossus. Največ zaslug pri tem je imel matematik Max Newman. Izdelava tega računalnika je skrajšala kriptoanalizo šifre Lorenz iz nekaj tednov na nekaj ur. (Hamer, 1998)

6.2. Predzgodovina kriptoanalitične operacije ULTRA

Operacija ULTRA, ki je bila kriptoanalitična operacija Britancev proti nemški in italijanski šifri Enigmi, se je začela že z uspešnim kriptoanalitičnim delom Poljakov na tem področju.
Začetki operacije segajo v leto 1929, ko so Nemci po pomoti poslali komercialno Enigmo na Poljsko, nato pa preko svoje ambasade zahtevali, da se jim paket vrne. To so Poljaki tudi storili, vendar so prej skrbno preučili njegovo vsebino. (Petterson, 1997)
Leta 1932 so v svojem šifrirnem biroju, imenovanem Biuro Szyfrow, zaposlili mlade študente matematike, ki so nato odločilno pripomogli k uspešni kriptoanalizi nemške šifre Enigme. Ti so bili Marian Rejewski, Jeryz Rozycki in Henryk Zygalski. Njihovo delo je potekalo v največji tajnosti.

Drugi človek, ki je močno pripomogel k dešifriranju nemške šifre, je bil Hans Thilo-Schmidt. S pomočjo svojega brata, ki je bil podpolkovnik nemške vojske, se je zaposlil pri zvezah. Ena od njegovih nalog je bila uničevanje zapisov ključev Enigme, ki niso bili več veljavni. Ker je močno potreboval denar za svoje razvratno življenje, je navezal stik z Gustavom Bertrandom, obveščevalcem pri francoski obveščevalni službi, in jim šifre in druge informacije o Enigmi prodal. Francozi so skupaj z Angleži preučili informacije in ugotovili, da so neuporabne, ker so le delne. Nato so informacije in kode ponudili Poljakom, ki so se jim zdele koristne, zato so jim jih začeli Francozi redno pošiljati.

Poljaki so tako imeli sporočila z odprtim tekstom, sporočila s šifriranim tekstom in stare ključe. Potrebovali so nastavitve koles in njihove obrate. Rejewskemu je s pomočjo

[1] Baudotova koda pomeni, da je vsaka črka sestavljena iz petih bitov (npr. a je sestavljena iz luknjica/prostor/prostor/luknjica/prostor ali 1,0,0,1,0).

matematičnih operacij uspelo ugotoviti pozicijo koles, zato so lahko leta 1933 izdelali približek Enigme, ki je temeljil na modelu komercialne Enigme iz leta 1929.
Kljub temu da so sedaj imeli napravo, pa je bilo to šele pol poti do branja sporočil. Potrebovali so še ključe, ki so bili v veljavi za tisti dan, ko je bilo prestreženo sporočilo.
Da so ugotovili te, so potrebovali največkrat uporabljene besede v nemških sporočilih, da bi s poskušanjem vstavljanja teh v šifrirano sporočilo, prišli do ključa.[1] S pomočjo teh je Rejewski uspel v enem letu izdelati katalog ključev, s katerim so lahko kriptoanalitiki v 20 minutah dobili dnevno nastavitev. 1. novembra 1937 so Nemci spremenili nastavitev (Umkehrwalze), s tem pa zopet onemogočili kriptoanalizo Poljakov. Leta 1938 so spremenili še metodo šifriranja črk, kar je Poljakom še otežilo izdelavo novega kataloga. Zygalski je izdelal 10 katalogov možnih variant dnevnih nastavitev, vendar pa je preizkušanje teh vzelo Poljakom preveč časa. Zato so skonstruirali napravo imenovano Bomby, s katero so lahko strojno preizkušali možnosti, s tem pa močno skrajšali čas in trud. S ključi, ki so jih dobili od Francozov, in uporabo replike Enigme je bila Poljska sposobna dešifrirati večino nemških sporočil. Najbolj so jih zanimala sporočila med nemškimi enotami, ki so se urile v Sovjetski zvezi in Berlinom. Svojih ugotovitev niso posredovali Francozom, verjetno zato, da Nemci ne bi izvedeli, da je bila njihova šifra kompromitirana, kljub temu pa so njim Francozi skozi ves čas posredovali informacije, pridobljene od H.T. Schmidta.

Za posredovanje ugotovitev Francozom so se odločili šele, ko so iz sporočil razbrali, da bo njihova država napadena. Informacije o njihovih dosežkih so jim predali 25. julija 1939 na skrivnem srečanju v gozdu pri kraju Pyry. Zaradi želje po porazu nacistov, so informacije posredovali še močno presenečenim Britancem. Predali so jim Nemške šifre, repliko Enigme in Bomby.
1. septembra 1939, ko je Hitler napadel Poljsko, so poljski kriptoanalitiki pospravili material in zbežali v Francijo. Svoje delo so tam nadaljevali; ko pa so Nemci zasedli celotno Francijo, so prebegnili v Veliko Britanijo. Tam jim Britanci nikoli niso dovolili delati na šifrah, razloge pa gre iskati v britanski aroganci in strogi tajnosti njihove operacije ULTRA.
(Sebag-Montefiore, 2000: 15-46)

[1]Npr. velika večina nemških sporočil se je začela z anx, kjer je an pomenil k, x pa presledek.

6.3. Operacija ULTRA

6.3.1. Bletchley Park

Med prvo svetovno vojno je britanska kriptoanalitična služba delovala v okviru mornariške obveščevalne službe, imenovana ”Room 40”. Leta 1920 se je preselila pod okrilje zunanjega ministrstva. Tam so se vse do leta 1939 brezuspešno trudili, da bi razbili kodo Enigme, prve uspehe so dosegli šele potem, ko so jim Poljaki predali vsa dotedanja odkritja v zvezi s to zapleteno šifrirno napravo.

Avgusta 1939 so se fizično preselili v Bletchley Park (”BP”), posestvo, 64 km oddaljeno od Londona. Uradno ime tega posestva je bilo Postaja X (Station X). Poveljnik je bil mornariški častnik Alastair Denniston, uslužbenci pa so bili matematiki, lingvisti, šahovski strokovnjaki in profesorji. (Welchman, 1982: 185-195)

Za različne oddelke je bilo zgrajenih več barak, v baraki številka 6 (Hut Six) so se ukvarjali s kopensko in letalsko Enigmo, baraka številka 3 (Hut Three) pa jim je pomagala s tem, da je dešifrirana sporočila spreminjala v obveščevalna poročila. Baraka številka 8 (Hut Eight) se je ukvarjala z mornariško Enigmo, ob obveščevalni pomoči barake številka 4 (Hut Four).
Material za obdelavo pa je prihajal iz prisluškovalnih Postaj Y (Station Y), ki so bile nameščene vse okoli Velike Britanije in tudi nekaterih drugih državah, njihova glavna naloga pa je bila prestrezanje sovražnikovega radioprometa. (Bletchley Park History, Enigma)

6.3.2. Kriptoanaliza nemških šifer

Od leta 1939 do leta 1944 se je število uslužbencev na posestvu Bletchley Parka povečalo s 120 na približno 7000. Vsi ti ljudje, večinoma zbrani z različnih fakultet, so skupaj razvili uspešne dešifrirne naprave in metode, brez katerih bi bili nemočni pravočasno razdreti zapletene nemške strojne šifre. Kljub temu pa so šifre lahko dešifrirali le zaradi napak nemških operaterjev, s pomočjo katerih so lahko izdelali ključe. Vendar pa so bili postopki prepočasni, zato se je pokazala potreba po izdelavi kriptoanalitičnega stroja, ki bi strojno ugotavljal dnevno nastavitev Enigme.

Alan Turing in drugi matematiki iz Cambridgea so leta 1940 izdelali napravo The Bombe. Bila je naslednica poljske Bomby, vendar okoli petnajstkrat hitrejša. Za obdelavo šifre Lorenz pa je Max Newman leta 1944 razvil prvi računalnik na svetu, imenovan Colossus. Napravi sta temeljili na ugibanju verjetnega odprtega teksta. S šifriranim tekstom sta ga primerjali toliko časa, da se je tekst vsaj na enem delu ujemal, s tem pa so dobili ključ.

Brez teh dveh naprav bi bila kriptoanaliza nemogoča, kajti Nemci so uporabljali tako Enigmo kot Lorenz ne samo z eno šifro (več različic šifer Enigme in šifer Lorenza), temveč z množico šifer in ključev. Tako je Nemčija uporabljala naenkrat približno 50 različnih šifer Enigme, nekaj v vojski, nekaj v letalstvu, železnicah, nekaj v mornarici in nekaj v obveščevalnih službah. Kriptoanalitiki se niso soočali le z eno različico šifre Enigme, temveč z veliko množico šifer in ključev, veljavnih za tekoči dan. Podobno je bilo s šifro Lorenz, ki je bila prav tako uporabljena v 22 možnih izvedenkah. (Hinsley, 1994)

Kljub temu pa so potrebovali še Enigmo in njena kolesa. S pomočjo poljske replike Enigme so lahko s pomočjo ”bombe” uspešno brali kopensko in letalsko Enigmo, na težave pa so naleteli pri mornariški Enigmi, ki je imela komplet osmih koles. Te so uspeli dobiti 12. februarja 1940, ko je britanski minopolagalec z globinskimi bombami prisilil na površje nemško podmornico U-33. Do drugega koristnega materiala so prišli z zajetjem nekaj nemških meteoroloških ladij na severu. 9. maja 1941 pa je britanski rušilec Bulldog zajel nemško podmornico U-110, z njo pa celotno Enigmo, s kolesi in knjigo ključev. Ta zajetja so bila hitra in niso dopustila kapitanom, da bi šifre, knjige ključev in kodne knjige uničili, kot

so narekovala navodila. Vse te pridobitve so pripomogle k uspešni kriptoanalizi nemške mornariške šifre. (Welchman, 1982: 119-138)

Nemci so 1. februarja 1942 k svoji podmorniški Enigmi (Shark Enigma) dodali še eno sredinsko kolo, vendar jim kljub temu ni uspelo za dalj kot za šest mesecev zaustaviti uspešnega dela Bletchley parka.

Britanci so torej s pomočjo intelektualnega jedra Bletchley Parka, skozi vso vojno, bolj ali manj v celoti brali nemška sporočila. Za ugotovitev dnevnega ključa Enigme so potrebovali okoli 8 ur, za ugotovitev dnevnega ključa kode Lorenz (Fish) pa so potrebovali 5 do 7 dni. V obeh primerih je bil to čas, ki ni bistveno ogrozil uporabne vrednosti informacij. Tudi teden dni pri kodi Lorenz ni pomenilo predolgega časa, kajti z njo so bila šifrirana sporočila najvišjega vojaškega in političnega vrha in se torej povečini niso nanašala na dnevne odločitve.
(Sebag-Montefiore, 2000: 46-92)

6.3.3. Implikacije operacije Ultra na potek vojne

Operacija Ultra, uspešna kriptoanalitična operacija Britancev proti Nemčiji, delno pa tudi Japonski, je imela velike implikacije na sam potek vojne. S svojimi informacijami je močno pomagala vojaškim in političnim strategom pri načrtovanju operacij, izbiri taktik itd. Pred letom 1941 je Ultra močno pripomogla v bitki za Britanijo[1] in k preprečitvi nemške operacije Morski lev[2]. Kasneje je privedla do poraza italijanske flote pri Matapanu, nudila pomoč pri potopitvi bojne ladje Bismark in pomagala angleškim branilcem Krete. Na Kreti je Nemčija sicer dosegla uspeh, vendar z veliko večjimi izgubami. Najmočnejše implikacije pa so se čutile šele po letu 1941, ko so kriptoanalitiki Bletchley parka začeli dosegati največje uspehe. Z branjem Enigme Abwehra so vedeli za vsakega vohuna, ki je prišel ali bil v Britaniji. Lahko so ga aretirali ali pa mu posredovali lažne informacije, ki so jih želeli posredovati Nemčiji. Na ta način, s pošiljanjem lažnih informacij so tudi prikrivali obstoj Ultre. Najbolj

[1]Letalska bitka, v kateri je RAF zdržala in preživela v boju z nemško Luftwaffe
[2]Operacija za invazijo na Britansko otočje, ki jo je Hitler načrtoval, potem ko bi bila RAF poražena

koristen je bil ta način prikrivanja, ko so v primeru bitke za Atlantik razglašali svoje uspehe kot posledico novega radarja, s katerim naj bi odkrivali položaj podmornic, in tako speljali sum stran od pravega vzroka.

Največje zasluge pa je imela Ultra v bitki za Atlantik. S pomočjo njenih informacij je uspelo zaveznikom močno znižati število potopljenih tovornih ladij, s preusmerjanjem konvojev mimo volčjih krdel in potopitvijo velikega števila nemških podmornic. Tovorne ladje so vozile veliko nujno potrebnega vojaškega materiala tako Britaniji kot Sovjetski zvezi. Ultra je imela tudi neposredne in posredne zasluge za uspešno izkrcanje v Normandiji, saj so prav z njenimi informacijami uspeli uspešno prepeljati vojaški material in vojake iz ZDA. Če pomoči iz ZDA ne bi bilo, bi se operacija prestavila za nekaj časa, to pa bi dalo Nemcem možnost, da dokončajo svoj Atlantski zid in povečajo število tankov na atlantski obali. Operacija pod kodnim imenom Overlord bi bila tako precej težje izvedljiva.

Jeseni 1941 je Ultra pripomogla pri vzpostavitvi ravnotežja v severni Afriki, poleti 1941 pa je dala velik prispevek k preprečitvi vstopa nemških sil v Egipt. Do tega ni prišlo, zaradi pomanjkanja streliva, goriva in rezervnih delov nemške vojske, kajti Britanci so prav zaradi informacij Ultre lahko močno ovirali dobavo.

Ultra je s svojimi informacijami pomagala tudi pri odkrivanju izstrelišč raket V-1 in V-2 in odkritja raziskovalnega centra za te rakete v Peenemundeju.
(Hinsley, 1994)

6.3.3.1. Bitka za Britanijo

Nemčija ni začela bombardirati ciljev v Veliki Britaniji pred julijem 1940, to pa je dalo Britancem dovolj časa, da so zgradili svoj obrambni sistem. Vključeval je radarje za zgodnje opozarjanje, mrežo opazovalnic za letala, telefonsko mrežo, veliko dislociranih letališč, skladišča za gorivo in poveljniški center letalstva, v katerem so se zbirale vse informacije.
10. julij je dan, ki se uradno šteje za začetek bitke za Britanijo, ko so Nemci začeli z masovnim bombardiranjem mest v Britaniji. Ti napadi so bili priprava na operacijo Morski lev. Rajhmaršal Hermann Gőring, glavni poveljnik Luftwaffe, je imel na voljo 1700

bombnikov in 1100 lovskih letal, medtem ko so se Britanci na začetku lahko branili le s 600 lovskimi letali.

Ta kvantitativna razlika pa se je lahko kompenzirala le s koristnimi informacijami s strani Ultre. Do tega časa je bila že vzpostavljena varna teleprinterska linija med Bletchley Parkom in letalskim maršalom Hughom Dowdingom, glavnim poveljnikom britanskega lovskega letalstva. V povprečju je dnevno dobival 200 dešifriranih sporočil, ki so mu dajala informacije o načrtih Luftwaffe. S pomočjo teh je lahko najbolj racionalno uporabljal razpoložljive lastne sile. Ker je za Ultrine informacije vedel le on, so bili njegove na videz nelogične rešitve velikokrat kritizirane s strani podrejenih, končalo pa se je s tem, da so ga konec leta 1940 premestili, leta 1942 pa upokojili.
Najbolj kritičen dan v celotni bitki pa je bil 15. september 1940, ko so Nemci sprožili močno ofenzivo s 328 bombniki in 769 lovci z namenom, da zadajo zadnji udarec RAF. Britanci, obveščeni s strani Ultre, so bili sposobni z le 300 letali uničiti 187 nemških letal in preprečiti ofenzivo.

17. septembra 1940 je Bletchley Park dešifriral sporočilo, v katerem je Hitler dal ukaz o opustitvi operacije Morski lev, s tem pa se je tudi zaključila bitka za Britanijo.

V celotni bitki za Britanijo je nemško letalstvo vrglo na mesta, kot so London, Liverpool, Birminghamin, Coventry, 40.000 ton bomb. Izgube Britancev so bile 20.325 ranjenih in 14.280 mrtvih in 900 uničenih letal. Nemci so istočasno izgubili 2.700 letal, 600 jih je bilo poškodovanih.

V bitki za Britanijo je RAF dosegla uspeh, ko je v spopadu z veliko močnejšim sovražnikom uspela preživeti, del zaslug za to pa gre zagotovo Bletchley Parku in operaciji Ultra. (Dabrowa, Lobodzinski, 1996)

6.3.3.2. Bitka za Atlantik

Ob izbruhu vojne septembra 1939, je imel admiral Dönitz, poveljnik nemške vojne mornarice, 39 podmornic v neposredni bližini britanskih preskrbovalnih poti. Prvi dan sovražnosti je

nemška podmornica potopila potniško ladjo Athenia. Poveljnik nemške podmornice kapitan Franz-Julius Lemp jo je zamenjal za vojaško transportno ladjo. Hitler je v skrbeh, da bi to lahko vključilo ZDA v vojno, kajti na krovu je bilo tudi veliko potnikov iz ZDA, prepovedal neomejeno podmorniško bojevanje. Poleg tega pa je hotel mir podpisati tudi z Britanci. Po nekaj tednih, ko je ugotovil, da to ne bo možno, je dovolil napade na britanske ladje, tudi brez opozorila. Britanci so odgovorili z oboroževanjem transportnih ladij in streljanjem na podmornice ob prvem stiku. V tistem času Bletchley park še ni uspel razvozlati mornariške Enigme.

Prvih nekaj mesecev je bilo na morju redko več kot šest ali sedem podmornic hkrati, večinoma pa so operirale v severnem Atlantiku. Tako majhna flota je težko dosegala večje uspehe, vendar pa so potapljali ladje, ki so jih Britanci zaradi počasnosti izključili iz konvojev. Do konca leta 1939 so izmed 5756 ladij, potopili le štiri ladje, ki so plule v konvojih, a kar 102, ki so plule posamezno.

Leta 1940 so Nemci po zasedbi Francije postavili veliko število oporišč za podmornice vzdolž atlantske obale. To jim je močno skrajšalo pot do območja delovanja, s tem pa se je močno povečalo število podmornic, ki so bile operativne. Druga pridobitev za Nemčijo po zasedbi Francije pa so bila letališča, iz katerih je lahko vzletalo novo letalo Focke-Wulfe 200, izvidniško letalo in bombnik z velikim dosegom, ki je oskrboval podmornice z informacijami o tem, kje se nahajajo britanske ladje.

17. avgusta 1940 je Hitler razglasil totalno blokado Britanskega otočja. Naslednji meseci so bili zelo uspešni za Nemce, saj so potopili 2.373.070 ton britanskega ladjevja, s samo 21 podmornicami na morju istočasno in z izgubo 26 podmornic.

Jeseni 1940 je poveljstvo podmornic preselilo operativno območje v srednji Atlantik, kjer so podmornice lahko napadale malo branjene konvoje brez letalske zaščite. Septembra je bila izvršena prva akcija podmornic z uporabo taktike volčjih krdel. Dešifriranje mornariške Enigme je sedaj postalo še bolj pomembno, saj so morale podmornice, da so lahko formirale krdela, sporočiti svoj položaj v Dönitzev štab. Če bi zaveznikom uspelo prebrati ta sporočila, bi lahko konvoje speljali mimo krdel. Ljudem v Bletchley Parku je bilo jasno, da brez dodatnega zaplenjenega materiala o šifri, predvsem z ladij in podmornic, kriptoanaliza ne bo uspešna.

Marca 1941 pa je Britanska kraljeva mornarica pri Norveški zasegla nemško transportno ladjo Krebs, na njej pa dve Enigmi z dnevnimi nastavitvami. To je kriptoanalitkom v Bletchley Parku omogočilo delen preboj. Dodatni material so dobili, ko je HMS Bulldog spomladi leta 1941 prisilila posadko U-110 pod poveljstvom kapitana Franza Lempa, da podmornico zapusti. Na njej so dobili Enigmo in kodno knjigo. S pomočjo tega so uspeli prvič brati večino sporočil nemških podmornic, in tako usmerjati konvoje mimo volčjih krdel.

V mesecu juliju 1941 nemške podmornice tri tedne niso opazile nobenega konvoja. Julija in avgusta se je število potopljenih ladij (100.000 ton) zmanjšalo na najmanjše v celotnem letu. Celotna zasluga za to ne gre le informacijam operacije Ultra, temveč tudi uspešnemu letalskemu izvidovanju in preusmeritvi operacij podmornic s strani Nemcev v Sredozemlje in k Arktiki. Ker pa britanski kriptoanalitiki niso brali vseh sporočil, so Nemci vseeno prestregli kakšen konvoj (npr. Arktični konvoj PQ17) in mu prizadejali hude izgube.

1. februarja 1942 pa je nemška vojna mornarica svoji Enigmi dodala še četrto kolo, ki je za 26 krat povečalo število možnih kodnih kombinacij in s tem onemogočilo britansko kriptoanalizo.

Za nemške podmorničarje se je začelo polletno obdobje, ki so ga oni imenovali zlati zahod (gold west) zaradi zelo dobrih rezultatov. Maja 1942 se je število podmornic, ki so bile istočasno na dolžnosti, povečalo na 30. Podmornice so začeli oskrbovati s podmorniškimi tankerji. V tem obdobju so nemške podmornice potopili 2.250.000 ton ladjevja, nemške izgube pa so znašale le 8 podmornic.

Oktobra 1942 pa je britanski rušilec HMS Petard z globinskimi bombami prisilil na površje U-559. Iz potapljajoče podmornice je britanskim mornarjem uspelo dobiti najnovejše kodne knjige. S pomočjo tega materiala so v Bletchley parku znova uspeli razbiti podmorniško Enigmo. Sedaj so bili sposobni ves čas do konca vojne brati to najbolj zapleteno različico Enigme. Seveda pa je bilo treba sporočilo tudi prestreči in ga pravočasno dešifrirati, tako da lahko sklepamo o tem, da so brali večino sporočil. (Welchman,1982: 119-138)

Rezultati nemških podmornic so se vidno slabšali, vendar Nemci niso nikoli pomislili, da je bila njihova koda kompromitirana. Prepričani so bili, da za uspešno kriptoanalizo zaplenjen material ni dovolj. 12. novembra 1943 je Dönitz prenehal uporabljati taktiko volčjih krdel. Poveljniki podmornic so od tedaj delovali samostojno, vendar so bili proti dobro organiziranim zavezniškim konvojem dokaj nemočni. V obdobju od novembra 1942 do

novembra 1943 je bilo potopljenih le 107 zavezniških ladij (600.000 ton) ob izgubi 136 nemških podmornic.

Leta 1944 je bilo podmorniško delovanje osredotočeno na prihajajočo invazijo. Nemčija je takrat imela 162 operativnih podmornic, dnevno pa jih je bilo na morju 43. Vendar pa so jih zaradi informacij Ultre organizirano potapljali, največ v trenutku oskrbovanja iz podmorniških tankerjev. Uspehi nemških podmorničarjev so bili slabi, saj so v času pred invazijo potopili le 21 zavezniških ladij za ceno 19 podmornic. V letu 1945 so bili rezultatu še slabši, 63 potopljenih ladij za ceno 154 potopljenih podmornic.

V bitki za Atlantik bi morale nemške podmornice po njihovih ocenah potopiti 700.000 ton zavezniškega ladjevja na mesec. Če bi to številko dosegli, zavezniške ladjedelnice ne bi mogle več zagotavljati dovolj transportnih ladij za prevoz nujno potrebnega vojaškega materiala. Tej številki se niso približali niti v času, ko Bletchley Park ni bral Enigme, zato težko rečemo, da je bila bitka za Atlantik dobljena zaradi informacij operacije Ultra. Dejstvo pa je, da je ta operacija rešila mnogo življenj in ohranila mnogo prepotrebnega vojaškega materiala, s tem pa močno skrajšala drugo svetovno vojno v Evropi.
(Sebag-Montefiore, 2000: 154-271)

6.3.3.3. Severna Afrika

Obveščevalna dejavnost je imela dve vlogi pri operacijah v severni Afriki. Prva je bila pomoč pri samem bojevanju in doseganju zmage na bojišču, druga pa je bila pomoč pri oviranju konvojev z vojaško pomočjo, brez katere bi bila tako ena kot druga stran nemočna. (Welchman, 1982: 119-125)

Pri obveščevalni dejavnosti je imela največjo vlogo operacija Ultra (poleg izvidovanja, vohunjenja, zasliševanja ujetnikov itd.). Ultra je bila takrat sposobna dešifrirati letalsko Enigmo, ta pa je bila v operacijah v Sredozemlju in severni Afriki tudi največ uporabljana, saj je letalstvo sodelovalo skoraj pri vseh operacijah.

Med majem in oktobrom 1941 so britanske enote potopile 180.000 ton ladjevja sil osi, ki so vozile pomoč v severno Afriko. Vsega skupaj je bilo to le 16% vsega ladjevja, vendar je bilo dovolj, da je prekinilo Rommelovo iniciativo. Onemogočilo mu je, da bi zbral dovolj orožja, goriva in drugega materiala, da bi pravočasno izpeljal ofenzivo na Tobruk. Posledica tega je bila, da so Britanci lahko napadli prvi in izvedli operacijo Crusader, s katero so potisnili nemške sile nazaj. Po novem letu 1942 je nemški vojski uspelo omejiti izgube v konvojih. To jim je uspelo predvsem zaradi izboljšane taktike konvojev, premika dela letalstva iz Sovjetske zveze na Sicilijo ter premika dela podmornic iz Atlantika v Sredozemlje. Uspelo jim je tudi potopiti nekaj zavezniških bojnih ladij. Vse to je omogočilo Rommelu, da je 21. januarja 1942 izvedel ofenzivo, ki je bila kljub Ultri presenečenje. S to ofenzivo so Nemci pridobili nazaj ves teritorij, ki so ga izgubili med zavezniško ofenzivo pred mesecem dni.

Zavezniki so sedaj potapljali le še 9% oskrbovalnega ladjevja. Posledica je bila, da so Nemci maja 1942 lahko prvi izvedli ofenzivo, na katero pa zavezniki, čeprav so bili o njej obveščeni s strani Ultre, niso uspeli uspešno odgovoriti. Rommel je potisnil Britance iz Libije, zasedel Tobruk in nadaljeval ofenzivo v Egipt, potem pa je bil ustavljen julija 1942 pri El Alameinu.
Razlog je bil v tem, da se je število potopljenega ladjevja zopet dvignilo na 20% in je na tej stopnji ostalo pet ali šest mesecev. Grof Ciano, italijanski zunanji minister, je zapisal: ″Če se bo to nadaljevalo, sile osi kmalu ne bodo imele več ladij, s katerimi bi vozili pomoč Libiji.″ (Budiansky, 2000: 277). S tem pa bi se tudi vse operacije tam zaključile. Tako velike izgube nemškega in italijanskega ladjevja so velik del posledica uspešnega dekriptiranja s strani Bletchley parka. (Budiansky, 2000: 267-293)

24. oktobra 1942 je general Bernard Montgomery začel z drugo bitko pri El Alameinu. S pomočjo Ultre je vedel, da je Rommel porabil vse zaloge goriva in zato ne bo sposoben za protinapad.
Dva tedna po uspešni britanski ofenzivi so z veliko operacijo, imenovano Bakla (Torch), izkrcanjem v severni Afriki, začele tudi ZDA. Preden so 7. novembra 1942 začeli z ofenzivo, je poveljnik Dwight D. Eisenhower dobil informacije od Ultre, da Nemci o pripravah nanjo ne vedo nič.
Do novega leta so pregnali Britanci Nemce iz Egipta proti Tripolisu. ZDA so izvedle uspešne ofenzivne operacije v Maroku in Alžiriji. V vseh pogledih se je vojna v severni Afriki končevala. Razlog je bil predvsem v 90% upadu oskrbovanja nemških in italijanskih enot.
(Winterbotham, 1976: 77-96; Suite.com)

6.3.3.4. Operacija Overlord

Do februarja 1944 je Bletchley park sodeloval z zavezniškimi poveljniki, med njimi tudi z generalom Eisenhowerjem, Montgomeryjem in Pattonom. Posredoval jim je vse pomembnejše informacije, ki so bile dobljene s kriptoanalizo, s tem pa jim omogočil ustreznejše rešitve. Vse bolj nujno in pomembno pa je postalo sodelovanje, ko so se začele priprave za izkrcanje v zahodni Evropi. Invazija na Normandijo je bila ena najbolj pomembnih in nevarnih operacij druge svetovne vojne, kar je naredilo vsako informacijo, ki bi pripomogle k njeni varnosti, še bolj pomembno.

Marca 1943 so bili s pomočjo operacije Ultra razkriti Hitlerjevi načrti o novem orožju V-1. Načrtoval je izgradnjo izstrelitvenih baz na francoski obali. Prestregli so sporočilo, v katerem je ukazal postavitev glavne baze za kontrolo V-1 orožja v bližini Amiensa. To je bil še eden od razlogov, nikakor pa ne ključni razlog, da se mora invazija začeti čim hitreje. Maja 1944 je Ultra prestregla sporočilo, v katerem Berlinu sporočajo, da je 50 izstrelišč pripravljenih. Zavezniki so z operacijo začeli 6. junija, ofenziva z nemškimi raketami V-1 pa naj bi se začela 12. junija. Razlog, da se je operacija začela ravno takrat ni pričakujoč napad z V orožjem, kot je literaturi o operaciji Ultra prikazano, pač pa predvsem v vojaškostrateških in političnih odločitvah.

Med nemškimi pripravami na obrambo je prišlo do nesoglasja med nemškimi generali o tem, kam naj se prerazporedijo tanki. Rommel je zagovarjal, da morajo biti takoj za prvo linijo Atlantskega zidu, Guderian pa je hotel, da se jih premakne bolj v notranjost Francije. Hitler se je odločil, da pusti tankovske divizije v notranjosti kot pomožne sile ob morebitni invaziji. To je bila odločitev, za katero je Bletchley park vedel in ki je naredila invazijo veliko lažjo. (Ultra, 2000)

7. Britanske kode in nemška kriptoanaliza

7.1. Britanska šifra TypeX

Typex (ali Type X ali TypeX) je bila glavna britanska šifra in šifrirna naprava v času druge svetovne vojne. Bila je elektromehanska naprava, ki je temeljila na istih postopkih kot nemška Enigma.
Koncem leta 1920 je začela Britanija iskati nadomestilo za svoj knjižni kodni kriptografski sistem. Za ocenitev delovanja so za ta namen kupili dve Enigmi. Leta 1935 je vlada pooblastila podjetje Creed&Company, da izdela šifrirni stroj na osnovi Enigme. V tem podjetju so izdelali stroj, ki je bil v osnovi Enigma, dodani pa so mu bili dodatki imenovani Type X, kasneje pa se je zaradi tega celotna šifrirna naprava preimenovala v TypeX.
TypeX je imela pet koles; tri zamenljive, odbojno kolo in hitro kolo podobno kot Enigma. Vendar pa sta bila pri tej šifrirni napravi dodani še dve kolesi, desno od hitrega kolesa (Stators), delovali pa sta kot nadomestilo za (Plugboard) vtično ploščo.

Za razliko od Nemčije, ki je s pomočjo Enigme šifrirala večino sporočil, tudi sporočila na taktični ravni, pa je bila britanska šifrirna naprava namenjena zgolj za komunikacijo najvišjega britanskega poveljstva, visokega političnega vodstva in RAF. Občasno so to napravo uporabljali tudi drugi. Ostale veje vojske so še vedno večinoma uporabljale ročno kodiranje, nikoli pa se ni TypeX uporabila na taktičnem nivoju.

Leta 1943 sta ZDA in Britanija podpisali t. i. Holden Agreement, sporazum, da bosta skupaj razvili združeno šifrirno napravo (Combined cipher machine) za medsebojno komunikacijo. Ameriška šifrirna naprava SIGABA (M-134-C) je bila močno podobna TypeXu, kljub temu da Američani nikoli niso dovolili Britancem, da bi jo videli. Obe napravi so modificirali z nekaj dodatki in izdelali skupni, stalni kriptografski sistem na najvišjem nivoju, ki je služil predvsem za izmenjavo informacij najvišjega političnega in vojaškega vodstva obeh držav.

Domneva se, da ta sistem ni bil nikoli razbit s strani sil Osi, kljub temu da je poskusni britanski kriptoanalitični napad na šifro pokazal opazen napredek. Šifra je bila bolj zapletena

od Enigme zaradi modifikacij, s katerimi so jo Britanci izpopolnili, za razbitje pa otežena tudi zaradi majhnega števila sporočil, šifriranih s to napravo. (TypeX, Wikipedia, 2002)

7.2. Kriptoanalitične službe Nemčije in njihovi uspehi

V Nemčiji je bilo po prvi svetovni vojni, še posebej pa po prihodu nacistov na oblast, ustanovljenih več kriptografskih in kriptoanalitičnih služb. Razlog je bil predvsem v tem, da so vsi pomembnejši voditelji na svojem področju hoteli imeti lastno prisluškovalno in kriptoanalitično službo, ki bi jih oskrbovala z informacijami, s tem pa bi si utrdili položaj in povečali družbeno moč v še razvijajočem se nacističnem sistemu oblasti.

7.2.1. Kriptoanalitična služba nemškega ministrstva za zunanje zadeve

Ustanovljena je bila že na začetku leta 1919. Do tega je prišlo na predlog Kurta Selchowa, takrat 32-letnega bivšega kapetana prestrezne službe nemške vojske. Postavljen je bil za administrativnega direktorja, osebje, ki ga je zaposlil, pa so bili njegovi nekdanji kolegi iz prve svetovne vojne. V začetku je imela nova služba naziv Referat IZ (Z je pomenilo sekcijo, I pa oddelek). Referat IZ je imel dva oddelka, kriptoanalitičnega (Chiffrierwesen) in kriptografskega (Chiffrierbüro). Leta 1936 je bila izvedena velika reorganizacija ministrstva za zunanje zadeve. Referat IZ se je takrat preimenoval v Pers Z. Kasneje je zunanji minister Joachim von Ribbentrop to sekcijo postavil v svojo neposredno pristojnost, zato da bi se čim bolj zmanjšalo število ljudi, ki bi imeli vpogled v dekriptate.

Leta 1939 se je Pers Z razdelil v dve skupini. Ena je bila bolj matematična, ki se je ukvarjala s šiframi, medtem ko je bila druga bolj lingvistična, ki se je ukvarjala s kodami. Lingvistično skupino sta vodila Rudolf Schauffler in Adolf Paschke, matematično pa dr. Werner Kunze. Vsi trije so bili kriptografski veterani še iz prve svetovne vojne.

Ko je leta 1933 na oblast prišel Hitler, je imel Pers Z zaposlenih 30 ljudi, ob začetku druge svetovne vojne pa že 200. Vsi niso bili kriptoanalitični strokovnjaki, temveč tudi administrativni delavci in pomožno osebje. Na koncu se je število uslužbencev povečalo že na 300. (Labovič, 1987a: 169-174)

Tajnost v tej sekciji je bila velika. Kriptoanalitikom je bila prepovedana vsaka uporaba črnila, noben papir se ni smel vreči, nobena skupina ni smela vedeti, kaj počne druga skupina, poleg tega pa so nacisti imeli v sekciji svoje notranje obveščevalce.

Kriptoanalitiki Pers Z so do konca vojne uspeli delno ali v celoti brati nekatere šifre in kode 34 držav, med njimi šifre Velike Britanije, ZDA, Irske, Francije, Poljske, Jugoslavije, Italije, itd. (Kahn, 1979c: 7-26)

7.2.2. Kriptoanalitična služba nemškega ministrstva vojnega letalstva

Hermann Gőring, minister vojaškega letalstva, je takoj po prihodu na položaj leta 1933 na svojem ministrstvu organiziral prisluškovalno enoto, imenovano Forschungsamt. Imela je 8 uslužbencev. Prisluškovali so telefonskim pogovorom, odpirali pisma in kriptoanalizirali tekst. Prestrezali so tako domača kot tuja sporočila, ki so bila poslana v obliki pisma, telegrama ali telefonskega pogovora. Posebna naloga Forschungsamta je bila, da snema, stenografira in zapisuje vse pogovore med Hitlerjem in Gőringom. Osebje je tesno sodelovalo z Sicherheitsdienstom (SD), ki pa je bila zaščitna služba nacističnega režima in je praviloma delovala na domačih tleh. (Kahn, 1979c: 26-30)

7.2.3. Organizacija Reichssicherheitshauptamt (RSHA)

Leta 1939 so bile združene vse strankarske in policijske organizacije v eno upravo, ki se je imenovala RSHA (Reichsicherheitshauptamt) – glavni državni varnostni urad, pod vodstvom Heinricha Himmlerja. Razdeljena je bila na več poduradov. Gestapo (policija proti političnim deliktom) je tako postal Amt IV, Kripo (kriminalistična policija) Amt V, varnostna služba SD

je postala Amt III, obveščevalna služba (zadolžena za zbiranje tajnih podatkov tujih držav) pa Amt VI.

Prav v okviru slednjega se je v Nemčiji tudi opravljala kriptoanaliza. Na začetku obveščevalnih podatkov niso pridobivali s pomočji kriptoanalize, temveč so se posluževali drugih postopkov. Svoja prestrežena sporočila so brali s pomočjo ukradenih ali kako drugače dobljenih kodov. Tako so uspeli dobiti španski dvodelni kod, kode jugoslovanskega generalštaba, Turčije, Vatikana, Portugalske, Brazilije pa so uspeli kupiti od Yamato Ominata, šefa japonske obveščevalne službe. Za kriptoanalitično delo pa je Amt VI sodeloval s Forschungsamtom in vojaško kriptološko službo. Himmler s tem sodelovanjem ni bil zadovoljen in je prosil Gőeringa, da Forschungsamt pripoji Amtu VI, kar pa se ni zgodilo, zato so organizirali svoj kriptološki oddelek. Večji uspeh so dosegli, ko so dobili odprte tekste britanskega ambasadorja v Turčiji s pomočjo obveščevalne operacije Cicero[1]. (U svetu špijunaže I, 145-149). Ker so imeli šifrirane iste tekste, so lahko na tej podlagi razbili ključ tega koda. Nesreča za Nemce pa je bila ta, da je bil to kod za enkratno uporabo.

Kasneje so uspehe dosegali tudi v sodelovanju z madžarsko kriptoanalitično službo, ko so uspešno brali sporočila turške ambasade v Moskvi, iz katerih so dobili zelo natančne informacije o Stalinovih namenih. General Alfred Jodl, načelnik operativnega štaba Wehrmachta (OKW), je rekel, da so to najboljši obveščevalni podatki, kar jih dobiva nemška vojska.
Uspeli so brati tudi nekatera britanska in ameriška sporočila, vendar brez večjih posledic za sam potek vojne. (Kahn, 1979c: 30-37)

7.2.4. Kriptoanaliza nemške vojne mornarice

Poveljstvo nemške vojne mornarice, ki je bilo leta 1920 močno razočarano nad odkritjem, da so Britanci v Sobi 40 ves čas vojne brali njena sporočila, je ustanovilo svojo kriptološko organizacijo imenovano B-Dienst (Beobachtung-Dienst). Imela je relativno malo uslužbencev (na začetku 9, kasneje pa se je število povečalo), ki pa so dosegali največje nemške kriptoanalitične uspehe. Že pred začetkom druge svetovne vojne so razbili nekaj najbolj

[1] Cicero je bil Elyes Bazna, Albanec, ki je bil sobar pri britanskem ambasadorju v Turčiji in nemški agent.

tajnih šifer britanske admiralitete. Dejstvo, da so zaradi tega Nemci brali sporočila britanske vojne mornarice, je na začetku vojne omogočilo nemškim gusarskim ladjam, da so se vedno izmikale britanski Domačinski floti. Informacije so reševal nemške bojne ladje pred močnejšimi sovražnikovimi sestavi, omogočale so napade presenečenja na britanske vojne ladje in pripomogle k temu, da je bilo v prvem obdobju, leta 1940, potopljenih 6 britanskih podmornic.

Verjetno največji uspeh B-Diensta pa je bil v zvezi z invazijo na Norveško. Hitler je 1. marca 1940 odobril načrt napada na Norveško in določil dan za invazijo. Malo za tem je B-Dienst dešifriral nekaj sporočil britanske Kraljeve mornarice, iz katerih so Nemci zvedeli, da bodo Britanci najprej minirali dohode do Narvika, potem pa zasedli Narvik, luko na skrajnem severu Norveške. Britanija se je za to operacijo odločila, da bi preprečila nemške pošiljke rude preko Norveške. Informacije, ki jih je dobil B-Dienst, so pomagale nemškem vrhovnem poveljstvu, da določi načrt, ki bi omogočil preko morja prepeljati vojake v slabo zaščitenih transportnih ladjah, ne da bi jih prestregla močnejša britanska flota. To so storili tako, da so poslali svoje bojne ladje na sever, s tem pa preslepili Britance, da hočejo napasti ladje, ki plujejo proti Narviku. Britanci so takoj svoje ladje poslali na pomoč tej floti, nemške transportne ladje pa so sedaj, po predhodnem obvestilu B-Diensta, da ni nevarnosti, lahko brez težav prepeljale vojake in tehniko čez Skagerrak. V svojih memoarjih je Churchill po vojni priznal, da so v tem primeru Nemci popolnoma izigrali Britance.(Kahn,1979c: 49)
B-Dienst si je pri svojem kripto-analitičnem boju močno pomagal z uspehi nekaj nemških ladij, med njimi tudi ladje Atlantis. To je bila posebno grajena zelo hitra trgovska ladja z dobro maskirano težko oborožitvijo in le ena od mnogih takih, ki so plule po morjih in napadale zavezniške ladje. V eni svojih prvih akcij leta 1940 je izstrelila nekaj strelov na britansko ladjo City of Baghdad v Indijskem oceanu in jo zavzela skoraj nepoškodovano. Med zaplenjenimi dokumenti je bila tudi koda trgovske mornarice (Merchant ships code), dvodelna koda, ki se je imenovala BAMS (Broadcasting for Allied Merchant Ships). Zaplenili so tudi nekaj tablic za prešifriranje, vendar niso bile več aktualne.

B-Dienst je torej imel kodo britanskega trgovskega ladjevja, branje njihovih sporočil pa je močno povečalo uspehe nemških podmornic v Atlantiku. Tako je npr. B-Dienst bral leta 1941 vsa sporočila, ki jih je konvojem pošiljal poveljnik Zahodnih dohodov na Atlantiku (Commander in Chief of Western Approaches). Pošiljal jim je nove načrte poti, po katerih bi se izognili nevarnim področjem. Zahvaljujoč uspešni kriptoanalizi teh sporočil, je poveljstvo

nemške podmorniške flote lahko reševalo dilemo, kako razporediti podmornice, da bo njihova učinkovitost največja. V bitki za Atlantik, ki jo je Nemčija na koncu izgubila, so bili najbolj uspešni v prvih letih vojne. Izgube britanskega ladjevja so bile velike, kasneje pa je bila nemška kriptoanaliza vedno manj uspešna, zato se je tudi število potopljenih ladij naglo manjšalo. Ko pa je admiral Dönitz opustil taktiko volčjih krdel, pa je bila bitka za Atlantik praktično končana. (Kahn, 1979c: 37-59)

8. Sklepi in verifikacija hipotez

8.1. Sklepi

Nedvomno ima kriptografija za vsako državo velik pomen. Pomembna je za vse institucije v državi, med katerim prihaja do komunikacije preko različnih zvez, najbolj pa je pomembna za institucije, vključene v nacionalno varnostni sistem, predvsem za vojaško organizacijo. V vojaški organizaciji je še toliko bolj pomembna, ker imamo tu opravka z drago vojaško tehniko, ljudmi in resnimi implikacijami na razvoj in ohranitev nacije. Uspešna kriptoanaliza pripomore k optimalni izbiri strategije, operatike in delno celo taktike[1], da si zagotovimo najboljši rezultat, na drugi strani pa je za preprečitev uspešne kriptoanalize, deloma pomembna tudi dobra kriptografija. Delno zato, ker se je v zgodovini največkrat pokazalo, da za kompromitacijo šifre ni bila odgovorna šifra, pač pa malomarnost operaterjev, varnostnih služb itd. Skušal sem to pomembnost prikazati s primeri iz druge svetovne vojne, iz katerih se zelo lepo vidi pomembnost kriptografije in kriptoanalize. Za drugo svetovno vojno sem se odločil predvsem zato, ker je bila tako množična, v njej pa se je odvijala zelo pomembna kriptografska "vojna". Ta je velikokrat premalo omenjena, verjetno zaradi tajnosti svoje narave, vendar so se njene implikacije močno čutile tako v samem poteku dogodkov kot tudi v samem trajanju vojne.
Obdobje obravnavane tematike ne sega samo v obdobje druge svetovne vojne, temveč tudi v obdobje pred spopadom, ko so potekali diplomatski boji in so se izvajale priprave na vojno.

Pri preučevanju vojne v Pacifiku se je jasno pokazalo, kakšno premoč pomeni branje sovražnikovih sporočil. Pri tem mislim predvsem na uspešno kriptoanalizo ZDA, ki jim je pomagala narediti preobrat v drugi svetovni vojni na Pacifiku že leta 1942 v bitki pri Midwayu. Do preobrata bi gotovo prišlo zaradi premoči ZDA v človeških in materialnih potencialih, vendar še ne tako kmalu. Admiral Nimitz je pri Midwayu z veliko manjšimi silami uspel premagati Japonce, potopiti velik del njihovih letalonosilk in zaustaviti njihovo napredovanje. Med uspehe operacije Magic lahko štejemo tudi sestrelitev admirala Jamamota, poveljnika japonske združene mornarice, potopitev največje bojne ladje na svetu Jamato in še množico drugih manjših uspehov. Uspešna kripto-analiza ZDA je bila posledica uspešno

[1] Informacije pridobljene s pomočjo kriptoanalize za taktični nivo največkrat nimajo uporabne vrednosti predvsem zaradi prevelike zakasnitve.

organizirane kriptoanalitične službe, ki je imela korenine že v obdobju po prvi svetovni vojni, tudi ob množici napak, ki jih je storila japonska kriptografska služba in njihovi operaterji. Ena večjih napak je bila zanemarjanje rednih menjav šifer, kar je bila verjetno posledica velikih dimenzij pacifiškega vojskovališča in je bila fizično težje izvedljiva, ter posledica velikega samozaupanja v nezlomljivost japonskih šifer. Druge napake pa so storili operaterji zvez, ko so isto sporočilo kodirali enkrat z eno, drugič pa z drugo šifro in tako močno pomagali kriptoanalitikom ZDA. Japonci so bili tudi prepričani, da že sama narava njihovega jezika pomeni dokaj veliko varnost pred razbitjem šifer in kod, zato so manj pozornosti namenjali varnostnim ukrepom.

Na drugi strani pa lahko ocenim japonsko kriptoanalizo kot zelo slabo, kajti njeni uspehi so bili zelo omejeni in brez prave uporabne vrednosti ter niso imeli nobenih implikacij na strateškem nivoju. Po mojem mnenju je to posledica zelo uspešne kriptografije ZDA ter miselnosti Japoncev, da so strojne šifre neprebojne. Zaradi te miselnosti se v celotnem obravnavanem obdobju japonski kripto-analitiki nikoli niso ukvarjali z zahtevno strojno šifro Sigabo in so vso svojo pozornost namenjali lažjim kodam, s katerimi pa se niso kodirala pomembnejša sporočila.

Velika Britanija je imela zelo dobro organizirano kriptoanalitično službo, stacionirano na posestvu Bletchley park. Tam so vse od poraza Poljske dokaj uspešno brali nemško šifro Enigmo. Zelo veliko so jim pri tem pomagala spoznanja poljskih kriptoanalitikov ter njihova replika Enigme. Kopensko in letalsko Enigmo so brali skozi celo vojno, z manjšimi prekinitvami, največ težav pa jim je predstavljala mornariška Enigma, ki je bila za sam potek vojne tudi najpomembnejša. Kljub temu so jo uspeli razvozlati in zmagati v bitki za Atlantik. Uspešno so Britanci brali tudi najbolj tajno nemško šifro Lorenz in tako spremljali pogovore v samem nemškem vrhu. Vsi ti uspehi so imeli pomembne implikacije na potek vojne. Verjetno niso imeli implikacij na sam izid vojne, so jo pa po mojem mnenju skrajšali, kar a priori pomeni manj žrtev in manj uničenja.
Uspešna kriptoanaliza Britancev je po mojem mnenju posledica uspešnega dela Poljakov že pred drugo svetovno vojno, nato pa dobro organizirane kriptoanalitične službe in nekaterih matematičnih genijev, ki so delali v njej. Ti so predvsem na podlagi napak operaterjev pri pošiljanju in kapitanov, ki niso uspeli uničiti Enigme ob zajetju njihovih ladij, izdelali repliko Enigme, s pomočjo Bombe pa so določali dnevne nastavitve koles. Močno je Britancem pomagala tudi nemška vzvišenost in miselnost, da je njihova šifra neprebojna. Večkrat so

Britanci pomislili, da je bilo zajetje kakšne ladje preveč očitno in da bodo Nemci šifro spremenili, vendar se to na njihovo srečo ni zgodilo.

Nemška kriptoanalitična služba je dosegla dokaj slabe rezultate, predvsem zaradi slabe organiziranosti. Kriptoanaliza se ni vršila le v eni službi, pač pa v mnogih, ki med seboj niso rade sodelovale. Do sodelovanja ni prišlo predvsem zaradi individualnih interesov voditeljev institucij znotraj katerih so bile organizirane, saj je pomenilo imeti kontrolo nad kriptoanalizo imeti moč, kar pa je bilo v nacistični Nemčiji zelo pomembno. Najpomembnejše uspehe je dosegla majhna služba, ki jo je organiziral admiral Dönitz, poveljnik nemške mornarice, imenovana B-dienst. Z uspešnim branjem britanskih mornariških kod jim je uspelo določen čas v bitki za Atlantik povzročati Britancem dokaj velike izgube, ki bi pomenile, če bi se nadaljevale, izgubo bitke za Atlantik in s tem podaljšanje druge svetovne vojne. To je bil edini uspeh nemške kriptoanalize, ki bi lahko imel tudi resnejše implikacije na potek vojne, vsi drugi pa so bili precej omejeni.

8.2. Verifikacija hipotez

Prva izvedena hipoteza, ki sem jo postavil, je bila, da je razkritje mornariške Enigme poglavitni razlog za zmago zaveznikov nad silami osi v Evropi. Te hipoteze ne morem potrditi, ker razkritje dejansko ni bil poglaviten razlog za zmago, saj bi do nje vseeno prišlo, je pa res, da je močno skrajšalo samo vojno v Evropi. Razlog, da bi do zmage vseeno prišlo, je v veliki človeški in materialni premoči zaveznikov nad silami osi, razen če ne bi prišlo v silah osi do kakšnega revolucionarnega odkritja na področju znanosti.

Drugo izvedeno hipotezo o tem, da kompliciranost šifriranja ni nujni pogoj za preprečitev dešifriranja s strani sovražnika, potrjujem, predvsem zaradi tega, ker je bila šifra Enigma, ki je veljala za eno najtežjih, razbita dokaj kmalu, medtem ko tako preprosto šifriranje kot je bilo tisto s pomočjo materinega jezika Indijancev plemena Navajo, ni bilo nikoli razbito. Razlog ni samo v kompliciranosti šifriranja, temveč tudi v načinu uporabe, množičnosti uporabe in pazljivosti operaterjev, kar se je v zgodovini pokazalo kot precej bolj pomembno od same zahtevnosti šifriranja.

Tretjo izvedeno hipotezo o tem, da ima operacija Magic največ zaslug za zmago ZDA v bitki pri Midwayu, bi potrdil, kajti kvantitativna premoč Japoncev je bila tolikšna, da bi bila zmaga nemogoča, če ZDA ne bi poznale kraja in čas napada. Po mojem mnenju je imela veliko vlogo v tej bitki tudi sreča, da japonska izvidniška letala niso opazila letalonosilk ZDA, vendar gre vseeno največ zaslug prav operaciji Magic.

Z glavno hipotezo o tem, da je preprečitev uspešne kriptoanalize ključnega pomena za zmago v boju, operaciji, vojni se ne morem strinjati, saj je vseeno na prvem mestu vojaški potencial, šele na drugem informacije o sovražnikovih namenih. To se je zelo dobro pokazalo v nemškem desantu na Kreto, ko so Britanci s pomočjo Ultre izvedeli, da se bo to zgodilo in kdaj, vendar vseeno niso mogli tega Nemčiji preprečiti. Posledice poznavanja namenov so bile le večje nemške izgube. Informacije o namenih sovražnika so brez zadostne vojaške moči na pravem mestu dokaj neuporabne.

Zaključil bi z ugotovitvijo, da je imela kriptografska vojna znotraj druge svetovne vojne dokaj pomembne implikacije na sam potek vojne, predvsem na strani zaveznikov, saj je uspela s svojimi informacijami, posredno preko zmag v nekaterih pomembnih bitkah zmanjšati število žrtev in materialno škodo te vojne z njenim skrajšanjem, po mnenju Sira Herryja Hinsleya, zgodovinarja in kriptoanalitika Bletchley Parka med drugo svetovno vojno, za približno dve leti. (Hinsley, 1994)

9. VIRI

Knjige in članki:

- Aldrich Richard James (2000), Intelligence and war against Japan, Britain, America and the politics of Secret service, Cambridge university press.

- Budiansky Stephen (2000), The Battle of Wits, The complete story of code-breaking in world war II, Viking, London.

- Boyle David (2001), World War II: A photographic history, Metro books, London.

- Ireland Bernard (1998), Jane`s Naval history of World war II, HyperCollinsPublishers, London, New York.

- Irving David (1976), Tajno orožje, Borec, Ljubljana.

- Kahn David (1979), Šifranti protiv špijuna (The Codebreakers, The story of secret writing), knjiga prva, a, Centar za informacije i publicitet, Zagreb.

- Kahn David (1979), Šifranti protiv špijuna (The Codebreakers, The story of secret writing), knjiga treča, c, Centar za informacije i publicitet, Zagreb.

- Kahn David (1979), Šifranti protiv špijuna (The Codebreakers, The story of secret writing), knjiga četvrta, d, Centar za informacije i publicitet, Zagreb.

- Kahn David (1996), The Codebreakers: The story of secert writing, Scribner cop., New York.

- Labović Đurica (1987), U svetu špijunaže I, Četvrti Jul, novinsko-izdavačka radna organizacija, Beograd.

- Labović Đurica (1987), U svetu špijunaže II, Četvrti Jul, novinsko-izdavačka radna organizacija, Beograd.

- Osredkar Radko (1999), Skrivnost kosmate glave, Življenje in tehnika, str. 11-18, Februar, Ljubljana.

- Schellenberg Walter (1961), V labirintu vohunstva, Večer, Maribor.

- Singh Simon (1999), The Code Book: The science of secrecy from ancient Egypt to quantum cryptography, Fourth Estate, London.

- Singh Simon (2000), The code book: The secret history of Codes and Code-breaking cryptography, Fourth Estate, London.

- Sebag-Montefiore Hugh (2000), The Battle for the Code, Weidenfeld&Nicholson, London.

- Winterbotham F.W. (1976), ULTRA, Mladinska knjiga, Ljubljana.

- Welchman Gordon (1982), The Hut six story-Breaking the Enigma Codes, McGraw-Hill Book Company, United States of America.

Enciklopedije, navodila in leksikoni:

- Verbinc France (1991), Slovar tujk, deseta izdaja, Cankarjeva založba, Ljubljana.

- Bojko Bučar, Zlatko Šabič, Milan Brglez, (sodelovanje Monika Kalin-Golob) (2000), Navodila za pisanje seminarske naloge in diplomskega dela, Fakulteta za družbene vede, Ljubljana.

- Leksikon Cankarjeve založbe (1982), Cankarjeva založba, Ljubljana.

- Vojni Leksikon (1981), Vojno Izdavački Zavod, Beograd.

- Britannica CD. (1997), Version 1997, Encyclopedia Britannica, Inc.

- Vojna enciklopedija (1974), Vojnoizdavački zavod, Beograd.

- Cambridgeov podatkovnik (1995), Cambridge University Press, DZS, Ljubljana.

Internet viri:

- Stripp Alan (1998), How Enigma works, Nova online,
  www.pbs.org/wgbh/nova/decoding/enigma.html, 25. 5. 2002.

- Molnar Alexander (1997), Navajo Code-talkers, Navy&Marine corps WWII,
  Commemorative Commitee,
  http://www.history.navy.mil/faqs/faq61-2.htm, 25. 5. 2002.

- The ECM Mark II, SIGABA,
  http://home.ecn.ab.ca/~jsavard/crypto/ro0205.htm, 26.5. 2002.

- Henson Jennifer (1995), The making of magic,
  http://history.acusd.edu/gen/WW2Timeline/magic.html, 26. 5. 2002.

- Petterson Max (1997), Enigma,
  home.earthlink.net/~nbrassl/lenigma.htm, 27. 5. 2002.

- Hamer David (1998), The Lorenz cipher attachment,
  www.eclipse.net/~dhamer/lorenz.htm, 27. 5. 2002.

- Bletchley Park history, Enigma: Breaking the Unbreakable Code,
  www.bletchleypark.org.uk/history1.asp, 1. 6. 2002.

- Hinsley Harry (1994), Interwiev,
  www.cl.cam.ac.uk/research/security/historical/hinsley.html, 1. 6. 2002.

- Dabrowa A., Lobodzinski R. (1996), Breaking the Enigma Code: Polish contribution to
  victory,
  pan.net/history/enigma/enigma9.htm, 25. 5. 2002.

- Ultra, cghs.dade.k12.tl.us/normandy/deception/ultra_enigma.htm, 2. 6. 2002.

- TypeX, Wikipedia (2002),
  www.wikipedia.com/wiki/typex, 7. 6. 2002.

- Suite.com,
  www.suite101.com/article.cmt/british_history/7252, 3. 6. 2002.

- Whitlock Duane (1995), The silent war against Japanese Navy,
  www.ibiblio.org/pha/ultra/nwc-01.html, 26. 5. 2002.

- BBC MMII (2001), Electro-Mechanical Cipher Machines,
  www.bbc.co.uk/dna/h2g2/A583959, 9. 7. 2002.

- Dupuis Clement (1999), Short history of Cryprology,
  http://webhome.idirect.com/~jproc/crypto/crypto_hist.html, 24. 5. 2002.

- Code breaking in the World War II (1999),
  history.acusd.edu/gen/WW2Timeline/espionage.html, 2. 6. 2002.

- Glossary, (1999),
  http://www.nsa.gov/programs/kids/glossary.shtml,1. 6. 2002.