ENIGMA I NJEMAČKE PODMORNICE U DRUGOM SVJETSKOM RATU

Robert Derenčin *

UDK: 355.40(100)"1939/1945"
327.84(100)"1939/1945"
629.58(100)"1939/1945"
623.9(100)"1939/1945"
Stručni rad
Primljeno: 11. XII. 2015.
Prihvaćeno: 18. VIII. 2016.

SAŽETAK

Jedan od razloga pobjede saveznika u Drugom svjetskom ratu je odličan rad britanskih i američkih službi za dekriptiranje. Najpoznatiji uspjeh tih službi je dekriptiranje poruka šifriranih Enigmom, njemačkim strojem za šifriranje. Članak opisuje kako to nije bio jednostavan i lak posao i kako su ponekad tek sreća ili osobna hrabrost nekolicine pojedinaca pomogli saveznicima da dekriptiraju poruke njemačke mornarice šifrirane Enigmom.

Ključne riječi: Enigma, „bomba", dekriptiranje, njemačke podmornice, Bletchley Park.

UVOD

„Prava je parodija da me oni koji me trebaju čuti nisu čuli, a da su me čuli oni koji me ne trebaju čuti." Te je riječi 15. ožujka 1943. napisao u ratni dnevnik podmornice U-518 njen zapovjednik, poručnik bojnog broda Friedrich-Wilhelm Wissmann. Podmornica je operirala u vodama Brazila, a s obzirom na to da je tih dana bila blizu istočne obale Brazila, Wissmann je osobito oprezno koristio radiovezu. Međutim, zapovjedništvo podmorničke flote dvaput je zapovjedilo slanje izvješća o situaciji (14. i 15. ožujka) pa je Wissmann ipak morao poslati poruku. Poruka je s podmornice poslana u 1.15 sati po srednjoeuropskom vremenu. Zapovjedništvo nije potvrdilo primitak poruke pa je ista poruka poslana ponovno u 5.04 i u 5.23 sati, opet bez potvrde da ju je primilo zapovjedništvo. Prijemnik radarskih signala na podmornici je u 7.09 sati uočio neprijateljski radarski signal (na valnoj duljini 140 cm), te je podmornica u 7.10 sati morala zaroniti.[1]

* Robert Derenčin (robert.derencin1@pu.ht.hr) umirovljeni je pripadnik OSRH iz Pule.

1 U-518 2nd War Patrol.

Saveznici ne samo da su „čuli" njemačke podmornice, nego su ih u pravilu i vrlo dobro razumjeli. Britanci i Amerikanci čitali su poruke njemačke podmorničke flote šifrirane Enigmom a da to Nijemci još dugo nakon završetka Drugog svjetskog rata nisu znali.

Enigma je bila elektromehanički stroj za šifriranje, koji je izvana bio nalik pisaćem stroju, samo što je umjesto valjka koji pridržava papir imao ploču s 26 lampica, a na poklopcu iznad svake lampice bilo je otisnuto pojedino slovo abecede, od A do Z. Postojalo je više modela Enigme, koji su izrađeni za razne njemačke državne službe, a neki su modeli prodavani i inozemnim vladama.

Enigma I, konstruirana za potrebe njemačkih oružanih snaga, za razliku od dotadašnjih modela Enigme imala je fiksni reflektor koji se nije mogao ručno podešavati okretanjem oko svoje osi prije početka šifriranja. Na prednjoj strani uređaja nalazila ploča s 26 utičnica, a pokraj svake utičnice bilo je otisnuto jedno slovo abecede (A–Z). Mornarica je koristila model M, koji je pod određenim uvjetima bio kompatibilan s Enigmom I, tako da su se mogle slati šifrirane poruke između mornarice, kopnene vojske, ratnog zrakoplovstva i Vrhovnog zapovjedništva oružanih snaga. Prije i tijekom rata postojale su četiri verzije mornaričke Enigme: M1, M2, M3 i, na kraju, M4. Nije se toliko radilo o različitim verzijama Enigme, nego je prije svega riječ o različitim procedurama šifriranja. Njemačka je mornarica 1940. koristila Enigmu M3, a u veljači 1942. u uporabu je ušla Enigma M4 s dva nova rotora i dva nova reflektora.

Sve vojne Enigme bile su opremljene kompletom od pet rotora označenih rimskim brojevima od I do V. Svaki rotor imao je (naravno) drugačije unutarnje ožičenje. Istovremeno su u uređaj bila umetnuta samo tri rotora, čiji je izbor i međusobni redoslijed bio naznačen u ključu šifre koji je vrijedio 24 sata. Mornaričke su Enigme u svom kompletu imale, uz tih pet rotora, još tri rotora označena brojevima VI, VII i VIII.

Enigma I i Enigma M3 imale su iste reflektore (Umkehrwalze – UKW), tijekom rata to je bio reflektor UKW-B, a ponekad se umjesto njega koristio reflektor UKW-C. Enigma M4 imala je dva posebna reflektora (oznake UKW-b i UKW-c) koji su se koristili zajedno s posebnim rotorima (oznake beta i gama). Budući da su Enigma M3 i Enigma M4 bile zapravo isti uređaji, ta dva posebna reflektora i dva posebna rotora bili su tanji od standardnih reflektora i rotora kako bi stali u uređaj. Istovremeno su u Enigmu M4 bila postavljena tri „normalna" rotora (oznake I–VIII), a desno od njih bili su postavljeni „tanki" rotor i „tanki" reflektor (u pravilu UKW-b i rotor beta). Pod određenim uvjetima, kombinacija reflektora UKW-b i rotora beta bila je kompatibilna s Enigmom M3 koja je koristila reflektor UKW-B. Isto tako je pod određenim uvjetima kombinacija reflektora UKW-c i rotora gama bila kompatibilna s Enigmom M3 koja je koristila reflektor UKW-C.

Prije postupka šifriranja, Enigma je morala biti pripremljena za rad prema podacima koji su se nalazili u dokumentima koji su bili dostavljani uz Enigme. Dnevni ključ određivao je osnovne postavke za sve Enigme u jednoj mreži u pojedinom danu i određivao je koji će rotori (i kojim redoslijedom) biti postavljeni u uređaj, kao i međusobni položaj njihovih jezgri i prstena oko tih jezgri, te kojih će deset

pari slova biti kabelima spojeno na prednjoj ploči (s utičnicama) uređaja. Naravno, ako bi unutar 24 sata sve poruke unutar jedne mreže bile šifrirane istim ključem, to bi neprijateljskoj strani olakšalo dekriptiranje. Zbog toga je svaka poruka imala i svoj poseban ključ koji se zvao ključ poruke. Ključ poruke bio je početni položaj rotora na početku šifriranja, koji se postizao ručnim rotiranjem rotora oko njihovih osi sve dok se u prozorčiću iznad svakog rotora ne pojavi određeno slovo ili broj (na prstenima rotora mornaričkih Enigmi bilo je otisnuto 26 slova, od A do Z, a ostale vojne Enigme imale su otisnute brojeve od 01 do 26). Prijemnoj se strani moralo javiti prema kojem je ključu (dnevnom i ključu poruke) poruka šifrirana, i to se činilo na način da je svaka poruka uz šifriranu poruku sadržavala i indikator poruke.

Do 1940. njemačka je vojska koristila zaista nesiguran indikator poruke, što je Poljacima omogućilo da shvate način na koji Enigma funkcionira i da čitaju poruke šifrirane Enigmom. Njemačke oružane snage su 1940. poboljšale sigurnost indikatora poruke, a mornarica je koristila potpuno drugačiju i puno sigurniju proceduru (odabira ključa poruke, koji je bio slučajan niz tri, kasnije četiri slova, i sastavljanja indikatora poruke) od kopnene vojske i ratnog zrakoplovstva. Zanimljivo je da je tu proceduru mornarica koristila samo na nekim najvažnijim područjima operacija na Atlantiku i (kasnije) na Sredozemlju. Na Crnome moru, Balkanu i Dalekom istoku mornarica je koristila proceduru koju su oružane snage napustile još 1940. (Rijmenants 2014). Britanci su do kraja rata dekriptirali mnoštvo poruka njemačke mornarice u područjima gdje se ta zastarjela procedura koristila.[2]

Nakon što je Enigma pripremljena, operater bi počeo proces šifriranja poruke: pritisnuo bi prvo slovo otvorene poruke na tipkovnici, iz baterije bi potekla struja prema dijelu s utičnicama, zatim prema rotorima, prošla bi kroz krajnje desni, srednji i krajnje lijevi rotor, došla do reflektora koji ju je vraćao nazad kroz krajnje lijevi, srednji i krajnje desni rotor, zatim bi struja ponovno došla do dijela s utičnicama, a naposljetku bi došla do jedne od lampica koja bi dolaskom struje zasvijetlila. Na poklopcu osvijetljene lampice nalazilo se otisnuto slovo. Operater bi, još uvijek pritišćući tipku na tipkovnici, pročitao i zapisao osvijetljeno slovo. Nakon toga bi pritisnuo drugo slovo otvorene poruke i tako sve do kraja otvorene poruke. Vojne su Enigme imale samo slova, nije bilo tipki za brojke i interpunkciju. Mornarica je brojeve pisala kao NULA, JEDAN, DVA itd. X je bila točka, Y je bio zarez, UD je bio upitnik itd.

Navedeni primjer opisuje rad Enigme s tri rotora (M3). Put struje od baterije do lampice isti je i kod Enigme M4, samo što struja prolazi kroz još jedan rotor. Rotori (osim tankih rotora Enigme M4) su se tijekom šifriranja rotirali (za jedno mjesto naprijed) oko svojih osi, krajnje desni rotor svaki put kad je pojedina tipka pritisnuta, utječući tako na rotiranje ostalih rotora (čije je rotiranje bilo rjeđe).

Bez reflektora ne bi bilo moguće imati iste dokumente za šifriranje i dešifriranje poruka, nego bi trebali posebni dokumenti za šifriranje i posebni dokumenti za dešifriranje poruka. Međutim, reflektori su bili „zaslužni" za najslabiju stranu Enigme: nijedno slovo nije nikad moglo biti šifrirano samim sobom. Moglo se be-

[2] R. Erskine, Naval Enigma Ciphers.

skonačno pritiskati, npr., slovo A na tipkovnici, a da nikad ne zasvijetli lampica na čijem je poklopcu bilo otisnuto slovo A. Poslije su tu slabu točku iskoristili Britanci (Rijmenants 2014).

Šifrirane poruke s podmornica slane su u zapovjedništvo radiovezom na kratkom valu, radiotelegrafijom, u skupinama od po četiri slova (kopnena vojska i zrakoplovstvo slali su šifrirane poruke u skupinama od po pet slova).

KRATKE I METEOROLOŠKE KRATKE PORUKE NJEMAČKIH PODMORNICA

Ako su se prilikom korištenja radioveze Nijemci ičeg plašili, bili su to savezнички radiogoniometri, prijemnici sa specijalnim antenama koji su mogli odrediti iz kojeg smjera dolazi radio-signal. Ukrštanjem dva ili više smjerova istog primljenog signala mogla se više ili manje točno odrediti pozicija objekta koji je signal poslao. Postoji nekoliko načina da se barem donekle onemogući rad radiogoniometra, a jedan od njih je smanjenje dužine poruka. Naime, kratke poruke mogu se brzo poslati pa protivnički radiogoniometri imaju vrlo malo vremena da se podese na frekvenciju na kojoj se poruka šalje i da odrede iz kojeg smjera signal dolazi.

Zbog toga su Nijemci uveli kratke (*Kurzsignale*) i meteorološke kratke poruke (*Wetterkurzsignal*). Tijekom rata korišteno je više vrsta kratkih poruka. Do 1942. kratka poruka uobičajeno je sadržavala samo jednu skupinu od četiri slova, koja je imala određeno značenje. To su bili alfa signali. Na početku 1942. njemačka je mornarica počela koristiti beta signale za kratke poruke. Pomoću kratkih poruka njemačke su podmornice mogle izvijestiti zapovjedništvo o opaženom konvoju (pozicija, smjer plovidbe, brzina, pratnja, broj brodova), potrebama za nadopunom goriva i torpeda itd.

Za sastavljanje kratke poruke postojala je knjiga kodova (*Kurzsignalheft*) pomoću koje su cijele rečenice (na kraju) pretvarane u nekoliko skupina od po četiri slova. Knjiga kodova sadržavala je sve moguće izraze, pozicije, imena luka, država, tipova brodova itd. Obične poruke su se potpisivale (ili bile naslovljene) imenom zapovjednika podmornice, a kratke poruke potpisivane su u početku bigramom (dva slova), a poslije trigramom (skupinom od tri slova). Svaka je podmornica imala svoj trigram čiji se popis nalazio u posebnoj knjizi.

Nakon što je poruka kodirana, trebala je prije slanja također biti šifrirana. Šifriranje se vršilo uobičajenim načinom, dnevnim ključem, uz jednu razliku. Naime, kao i obične poruke, i kratke su poruke sadržavale indikator poruke kako bi operater na prijemnoj strani znao kojim je ključem poruke (početnim pozicijama rotora Enigme na početku šifriranja četveroslovnih skupina) poruka šifrirana. Indikator (bio je to trigram) se dobivao iz knjige indikatora kratkih poruka (*Kenngruppenheft*) koja je imala nekoliko dijelova. Prema pojedinoj mreži (šifri) i datumu, operater je u knjizi imao na raspolaganju nekoliko indikatora od kojih bi odabrao jedan. Kraj svakog se indikatora (*Kenngruppe*) nalazio i ključ poruke (*Spruchschlüssel*).

Njemačka je mornarica sve knjige vezane za kratke signale tiskala na ružičastom papiru posebnom crvenom tintom, koja je bila razgradljiva u vodi, da bi se onemogućila njihova fizička kompromitacija. Zamisao je bila da u slučaju potrebe posada jednostavno baci te dokumente u vodu. Čak je navedeno da se ti dokumenti moraju držati na mjestima do kojih će, u slučaju potonuća podmornice, doprijeti voda.

Na početku poruke slao se signal ßß (beta beta, kako bi se odmah znalo da je riječ o kratkoj poruci), slao se Morseovom abecedom kao spojena slova B i T, tj. -…-, zatim je dolazio nešifrirani indikator poruke (*Kenngruppe*), šifrirana poruka (obično se sastojala od tri ili četiri skupine od po četiri slova), potpis (šifrirani trigram) i, na kraju, ponovljeni nešifrirani indikator poruke. Iskusni je radiotelegrafist mogao ovakvu poruku poslati unutar 20 sekundi (Rijmenants 2014). Budući da su kratke poruke počinjale signalom ßß, saveznički su ih operateri u prislušnim postajama lako prepoznavali. Međutim, operateri na goniometrima morali su biti brzi kako bi u otprilike 20 sekundi napravili što je više moguće smjeranja podmornice koja je slala kratku poruku. Na početku rata radiooperateri na njemačkim podmornicama bili su odlično uvježbani. Naravno, kako je rat trajao obuka novih operatera bila je sve slabija (Horn 1974).

Slanje meteoroloških podataka s podmornica bilo je toliko važno da je zapovjedništvo moralo prihvatiti sve opasnosti koje su iz toga proizlazile. Kako bi se barem skratilo slanje meteoroloških poruka, podmornice su imale knjige meteoroloških kratkih kodova (*Wetterkurzschlüssel*). Svaka se meteorološka kratka poruka (*Wetterkurzsignal*) sastojala od 23 ili 24 slova, svako je slovo predstavljalo određenu vrijednost (podatak), kao što su tlak, temperatura, vlažnost, naoblaka, smjer i jačina vjetra, visina valova, vidljivost itd. Ukupno je trinaest tablica određivalo koje slovo (ili kombinacija slova) zamjenjuje određeni podatak.

Prije slanja ta su se slova morala šifrirati Enigmom namještenom prema dnevnom ključu (rotori, parovi slova povezani kablovima…). Indikator poruke, koji je operateru na prijemnoj strani pokazivao kojim je ključem poruke (početnim položajima rotora na početku šifriranja) kratka meteorološka poruka šifrirana, nalazio se u mjesečnim tablicama (*Spruchschlüsseltafel*) u kojima je pojedini ključ poruke bio predstavljen jednim slovom (Rijmenants 2014).

"BOMBA"

"Bomba" (engl. *Bombe*) je bio elektromehanički stroj koji je Britancima služio za otkrivanje dnevnih ključeva Enigme.

Ured za šifre (polj. *Biuro Szyfrów*) poljskog Glavnog stožera prvi je uspješno dekriptirao njemačke poruke šifrirane Enigmom. Najzaslužniji za taj uspjeh bili su Marian Rejewski, Jerzy Rózycki i Henryk Zygalski, izuzetno sposobni matematičari dekripteri. Rejewski je uspio, potpuno matematičkom metodom, odrediti ožičenja Enigminih rotora i reflektora. Poljaci su uspješno dekriptirali poruke njemačke kopnene vojske i ratnog zrakoplovstva prvenstveno koristeći slabu proceduru sastavljanja

indikatora poruke. Njemačka je mornarica 1. svibnja 1937. uvela sigurniju proceduru pa Poljaci više nisu mogli dekriptirati poruke mornarice.[3]

Poljski Ured za šifre konstruirao je više strojeva koji su pomagali u dekriptiranju njemačkih poruka. Izrađene su replike Enigme, a Rejewski je (vjerojatno u listopadu 1938.) za lakše (prije svega brže) otkrivanje dnevnih ključeva Enigme dizajnirao uređaj koji je nazvan kriptološka bomba (polj. *bomba kryptologiczna*). Poduzeće AVA (koje je izrađivalo opremu za Ured za šifre) izradilo je šest „bombi", a svaka „bomba" oponašala je rad šest Enigmi.[4] Kad je postalo jasno da je rat neizbježan i da se Poljska vjerojatno neće moći obraniti, poljski su dekripteri 25. srpnja 1939. na sastanku u šumi Kabaty, u blizini mjesta Pyry južno od Varšave, predali svoja saznanja i po jednu repliku Enigme svojim britanskim i francuskim kolegama.[5]

Od ljeta 1939. do ožujka 1946. u Bletchley Parku u Buckinghamshireu bilo je središte britanske službe za dekriptiranje (Government Code and Cypher School – GC&CS). Na vrhuncu aktivnosti u Bletchley Parku je radilo više od deset tisuća osoba.[6] Iako su Britanci od Poljaka dobili repliku Enigme, problem pronalaženja dnevnih ključeva Enigme je ostao. Poljska je metoda funkcionirala, ali je Britancima bilo jasno da Nijemci mogu promijeniti sistem indikatora poruka, što se 1. svibnja 1940. i dogodilo pa je poljska metoda postala neuporabljiva. Zbog toga su Britanci izradili svoju „bombu" odnosno elektromehanički stroj za pronalaženje dnevnih ključeva Enigme. Inače su britanska i poljska „bomba" radile na potpuno drugačijim principima (Ellsbury 2003).

Britansku „bombu" je osmislio Alan Turing, a poboljšao ju je Gordon Welchman. I Turing i Welchman bili su matematičari sa Sveučilišta u Cambridgeu. Turing je odlučio iskoristiti činjenicu da Enigma nikad nije šifrirala jedno slovo tim istim slovom. Ako bi se znao barem dio otvorene poruke (taj su dio nazivali *crib*), i ako bi se taj *crib* mogao locirati unutar šifrirane poruke, usporedbom *criba* i tog dijela poruke vidjelo bi se koje je slovo šifrirano kojim slovom. Na osnovi toga su „bombe" pronalazile dnevne ključeve Enigme (Ellsbury 2003).

Glavni dio „bombe" bili su rotori (cilindri), koji su unutar sebe imali ožičenja jednaka onima u Enigmi (uz neke preinake), i dijagonalna ploča (*diagonal board*) koju je osmislio i konstruirao Welchman. Radilo se o kabelima koji su spajali određene rotore i na taj se način „nadomještao" rad kabela koji su na Enigmi spajali deset parova slova. Prva „bomba", koja još nije imala dijagonalnu ploču, stigla je u Bletchley Park u ožujku 1940. Druga je „bomba" (s dijagonalnom pločom) stigla 8. kolovoza 1940. „Bombe" su se tijekom rata usavršavale i bilo ih je sve više. Do svibnja 1945. u Bletchley Parku bilo je 211 „bombi" koje je posluživalo skoro 2000 poslužitelja.[7]

Princip rada „bombe" bio je sljedeći. Prvo bi prislušne postaje (postaje „Y") presrele njemačke poruke te ih najbrže moguće poslale u Bletchley Park (postaja

[3] Biuro Szyfrów, Wikipedia.

[4] Bomba (cryptography), Wikipedia.

[5] Biuro Szyfrów, Wikipedia.

[6] WWII: Bletchley Park.

[7] Bombe, Wikipedia.

„X"). Ovdje bi ih preuzeli matematičari koji bi pokušali pogoditi gdje se unutar pojedine šifrirane poruke nalazi *crib*. Ako bi točno odredili gdje se *crib* nalazi (što je bilo rijetko), saznali bi koja su slova dijela otvorene poruke šifrirana kojim slovima šifrirane poruke, i kojim redoslijedom. Na osnovi toga bio bi izrađen izbornik (engl. *menu*) prema kojem bi operateri pripremili „bombu" za rad spojivši rotore (postavljene u seriju od tri rotora) s određenim kabelima dijagonalne ploče, te dovodeći rotore u odgovarajući početni položaj. Dijagonalna ploča imala je 26 kablova od kojih je svaki sadržavao 26 žica, ukupno je bilo 325 spojeva između njih. Zatim bi se rotori počeli okretati oko svojih osi, simulirajući rad Enigme. Ako je izbornik bio dobro napravljen, rotori bi se zaustavljali u položaju koji je mogao šifrirati *crib* u šifrirani dio poruke. Ako je izbornik bio loš, rotori su se zaustavljali kad bi došli na početne položaje.

Ako je sve bilo u redu, „bomba" bi pokazala koji su rotori (i kojim redoslijedom) umetnuti u Enigmu, kao i neke parove slova, neka slova koja su ostala slobodna, te početni položaj jezgri rotora prilikom šifriranja. Da bi se pronašao kompletan ključ za taj dan trebalo je izvršiti provjeru na uređaju sličnom Enigmi. Uređaj bi bio postavljen prema postavkama koje je pokazala „bomba". Zatim bi se otipkao tekst šifrirane poruke. Ako bi se „pojavio" (barem donekle) suvisli tekst na njemačkom, to je značilo da je ključ za taj dan pronađen i da „bombe" mogu biti uporabljene za pronalaženje nekog drugog ključa (u nekoj drugoj mreži). Ako se takav tekst ne bi pojavio, provjeravao bi se rezultat dobiven nekom drugom „bombom", sve dok ključ za taj dan ne bi bio pronađen (Ellsbury 2003).

Na taj način su manje-više uspješno dekriptirane poruke šifrirane Enigmom. Naravno da se puno toga moralo „posložiti", bilo je puno nagađanja koji *crib* i gdje se nalazi u poruci, trebalo je napraviti točan izbornik, „bombe" su trebale ispitati puno kombinacija u puno njemačkih mreža svih grana oružanih snaga i „bombi" nikad nije bilo dovoljno. Ipak, s vremenom je dekriptiranje poruka njemačke kopnene vojske i ratnog zrakoplovstva postalo relativno jednostavno. Za poruke mornarice to se ne može reći.

Britanci su imali sve rotore mornaričke Enigme. U kolovozu 1939. od Poljaka su dobili rotore I–V. Kod preživjelih članova posade potopljene podmornice U-33[8] pronašli su 12. veljače 1940. rotore VI i VII.[9] U kolovozu 1940. u njemačkoj podmornici potopljenoj u blizini britanske obale pronađen je rotor VIII (Johnson 2004). Ipak, Britanci u početku nisu mogli dekriptirati poruke njemačke mornarice jer one skoro da nisu u sebi sadržavale *cribove*, a bez *cribova* „bombe" su bile beskorisne.

[8] Podmornica U-33 morala je izroniti nakon napada dubinskim bombama, a rotori su podijeljeni članovima posade koji su ih trebali baciti u more. Međutim, rotori su ostali kod njih i Britanci su ih pronašli. Ne treba kriviti te podmorničare jer u stresnoj situaciji kad podmornica mora izroniti samo da bi ju posada napustila, da bi odmah zatim potonula i odnijela sa sobom njihove kolege (preživjelo je samo 17 članova posade, a 25 ih je potonulo s podmornicom) sigurno se ne misli na ono što je u džepovima odore. Britanci su to znali te su i inače svojim posadama zapovijedali da odmah nakon zarobljavanja pretraže zarobljenike ne bi li kod njih otkrili zanimljive bilješke i sl. U ovom slučaju otkrili su pravo blago!

[9] R. Erskine, Breaking Naval Enigma.

Trebalo je doći do *cribova* da bi se mogao izraditi izbornik, da bi se „bombe" pravilno podesile i da bi se otkrili dnevni ključevi Enigmi.

TRAŽE SE *CRIBOVI*!

Da bi se došlo do *cribova* trebalo je zaplijeniti dokumente veze njemačke mornarice, što znači da je moralo doći do fizičke kompromitacije. Međutim, Nijemci nisu smjeli saznati, čak ni posumnjati, da je došlo do fizičke kompromitacije. Uz to, trebalo je doći do dokumenata veze namijenjenih za dužu uporabu. S obzirom na uvjete pomorskog ratovanja, to je bila teška, skoro nemoguća zadaća.

Nakon što su pronašli kodnu knjigu kratkih signala[10] i knjige kratkih meteoroloških kodova (*Wetterkurzschlüssel*, izdanje iz 1940. godine)[11] (Rijmenants 2014), Britanci su poruke šifrirane ključem Dolphin uspješno dekriptirali od 1. kolovoza 1941. do 5. listopada 1941., kad su njemačke podmornice na Atlantiku počele koristiti novi ključ Triton, koji su Britanci nazvali Shark.[12] To je bila nova šifra za Enigmu M4.

Britanci su već u prosincu 1941. rekonstruirali ožičenje četvrtog (beta) rotora Enigme zahvaljujući pogrešci nekoliko operatera na njemačkim podmornicama. Naime, iako je šifra Triton stupila na snagu, sve podmornice još nisu dobile Enigmu M4. Podmornice koje su imale Enigmu M4 morale su je podesiti tako da odgovara Enigmi M3. To se postizalo kombinacijom tankog reflektora UKW-b i posebnim podešavanjem tankog (četvrtog) rotora beta (međusobni položaj jezgre i prstena rotora u položaju A, te je ručno trebalo zarotirati rotor kako bi se u prozorčiću kraj rotora vidjelo slovo A). Neki su operateri napravili grešku pa se u prozorčiću nije vidjelo slovo A, nego, npr., slovo Z. Tako šifriranu poruku, šifriranu zapravo Enigmom M4, poslali su u zapovjedništvo. Kad su uvidjeli pogrešku, istu su poruku poslali ispravno, šifriranu Enigmom M3. Imajući istu poruku šifriranu na dva načina i uvidjevši pogrešku Nijemaca, Britanci su rekonstruirali ožičenje tankog reflektora UKW-b i četvrtog beta rotora.

Međutim, kad su 1. veljače 1942. podmornice prešle na Enigmu M4 uz drugo izdanje knjige kratkih meteoroloških kodova (*Wetterkurzschlüssel*, izdanje iz 1941), Britanci su opet ostali bez *cribova*. Budući da su „bombe" bez *cribova* bile neuporabljive, od 1. veljače do sredine prosinca 1942. Britanci nisu mogli čitati poruke njemačke mornarice. Preokret se dogodio 30. listopada 1942. u blizini Port Saida. Tri člana posade britanskog razarača *Petard* uspjela su se ukrcati na njemačku podmornicu U-559 i domoći se dokumenata veze među kojima su bila nova izdanja knjiga kratkih i meteoroloških kratkih kodova.[13] Individualna hrabrost u ratnoj mornarici

[10] Kodnu knjigu kratkih signala pronašli su 9. svibnja 1941., južno od Islanda, na podmornici U-110.

[11] Knjige kratkih meteoroloških kodova pronašli su na meteorološkim brodovima *München* (7. svibnja 1941., jugoistočno od Islanda) i *Lauenburg* (28. lipnja 1941., Arktik).

[12] R. Erskine, Naval Enigma Ciphers.

[13] Dvojica od njih, poručnik bojnog broda (*Lieutenant*) Anthony Fasson i razvodnik (*Able Seaman*) Colin Grazier smrtno su stradali potonuvši zajedno s podmornicom U-559.

rijetko je kad bila toliko važna kao u slučaju te trojice britanskih pomoraca. Šifra Shark je razbijena zahvaljujući njihovoj hrabrosti. Nakon proučavanja tih knjiga, Britanci su shvatili da Nijemci prilikom šifriranja meteoroloških kratkih poruka koriste Enigmu M3, dok su M4 koristili za šifriranje ostalih poruka. Britanci su 13. prosinca 1942., prvi put nakon više od deset mjeseci, imali pozicije njemačkih podmornica na Atlantiku.

Nijemci su u ožujku 1943. počeli koristiti novo, treće izdanje knjige kratkih meteoroloških kodova pa su Britanci opet ostali bez *cribova*. Međutim, već nakon devet dana, pomoću knjige kratkih kodova s U-559 uspjeli su ponovno pronalaziti ključeve Enigme (Rijmenants 2014). Pomoglo im je to što su meteorološke kratke poruke šifrirane Enigmom M3, a tadašnje su „bombe" konstruirane za pronalaženje ključeva Enigme M3. Te su „bombe" mogle pronalaziti i ključeve Enigme M4, ali je taj postupak trajao puno duže – 18 dana umjesto oko 17 sati.

Britanci i Ratna mornarica SAD-a pokrenuli su razvoj „bombi" s četiri rotora, koje su se počele koristiti u lipnju (britanske) i kolovozu (američke) 1943. i otada su poruke šifrirane šifrom Triton u pravilu bile dekriptirane unutar 24 sata od presretanja.[14] Američke „bombe" bile su bolje i bilo ih je više pa je krajem 1943. rad na pronalaženju ključeva šifre Triton prepušten službi za dekriptiranje Ratne mornarice SAD-a (Op-20-G) u Washingtonu. Naravno, riječ je samo o uporabi „bombi", sve ostalo su Britanci i Amerikanci radili zajedno (pronalaženje *cribova*, izrada izbornika itd.). Treba uzeti u obzir da su britanske „bombe" korištene ne samo za pronalaženje mornaričkih ključeva, nego i za pronalaženje ključeva kopnene vojske i ratnog zrakoplovstva, pa su ih pojedini odjeli u Bletchley Parku morali međusobno dijeliti (Milner-Barry 1978). Posebno je to bilo osjetljivo na početku rata (u Britaniji) kad nije bilo dovoljno „bombi".

Toliko potrebne *cribove* Britanci nisu dobivali direktno, nego su morali rekonstruirati moguću poruku poslanu s podmornice. Na primjer, nakon što bi njemačka mornarička meteorološka služba prikupila izvješća s podmornica, slala bi opće meteorološko izvješće kodirano posebnim kodom, koji su Britanci uspjeli razbiti. Iz tih bi izvješća Britanci doznali rezultate meteoroloških mjerenja na određenim pozicijama na Atlantiku. Imajući knjigu kratkih meteoroloških kodova, Britanci su mogli sastaviti poruku u obliku kakav je bio prije šifriranja Enigmom. Ako su presreli izvješće s podmornice, i uspješno locirali podmornicu koja je izvješće poslala, mogli su usporedbom šifrirane poruke poslane s podmornice i poruke koju su sami sastavili izraditi izbornik za „bombe". „Bombe" bi pronašle dnevni ključ za Enigme s tri rotora pa su Britanci toga dana mogli čitati poruke šifrirane Enigmom u M3 modu. Naravno, malo kad je sve funkcioniralo savršeno.

Kod kratkih signala princip je bio sličan. Bletchley Park je primao podatke o poziciji, smjeru i brzini plovidbe itd. savezničkih konvoja. Ako bi uspjeli locirati podmornicu koja je poslala kratku poruku, znali bi o kojem konvoju ta podmornica podnosi izvješće. Nakon toga se pomoću knjige kratkih kodova, zarobljene na

Šesnaestogodišnji mornar Tommy Brown uspio se spasiti.

[14] R. Erskine, Breaking Naval Enigma.

U-559, pokušala sastaviti originalna poruka kakva je bila prije šifriranja Enigmom. Ta rekonstruirana poruka sastavljala se na način uobičajen na njemačkim podmornicama – „ugledan konvoj, pozicija, smjer, brzina". Na kraju bi matematičari pomoću tako dobivenih *cribova* sastavili izbornik prema kojem bi „bombe" bile podešene i, ako bi sve bilo savršeno, pomoću „bombi" bi se doznao dnevni ključ Enigme M3 (Sale). Puno je toga trebalo savršeno funkcionirati, svi kotačići u tom mehanizmu morali su odraditi svoj posao da bi dnevni ključ bio pronađen, a odmah nakon ponoći sve je trebalo ponoviti i nadati se najboljem. Ako bi samo jedan detalj bio pogrešan, npr. u slučaju da podmornica, koja je izvijestila o konvoju, nije dobro odredila svoju poziciju, sistem nije funkcionirao.

ODGOVORNOST ZA PROPUSTE U ZAŠTITI RADIOKOMUNIKACIJA

Vrhovno zapovjedništvo njemačkih oružanih snaga (Oberkommando der Wehrmacht – OKW) imalo je službu za dekriptiranje (Chiffrierabtellung – OKW/Chi) koja je (uz praćenje prometa stranih država) trebala brinuti i o sigurnosti kriptoloških sistema u oružanim snagama. Međutim, odgovornost (i ovlaštenja koja uz to moraju doći) nad cjelokupnim oružanim snagama bila je samo teorijska. Ratno zrakoplovstvo i ratna mornarica su do kraja rata zadržali samostalnost u razvoju svojih sistema i odlukama koji će njihovi sistemi i gdje biti uporabljeni.[15]

Nakon neuspjelog atentata na Hitlera 20. srpnja 1944. i reorganizacije oružanih snaga, OKW/Chi je trebao postati vrhovni autoritet za kriptologiju, ali to je došlo prekasno. Situacija u Njemačkoj postala je previše kaotična, nije se moglo ispitati sve sisteme pojedinih grana, a stalno bombardiranje tvornica onemogućilo je masovnu proizvodnju novih uređaja za šifriranje. OKW/Chi je razvijao nove, mnogo sigurnije sisteme kriptozaštite. Uvođenje novog modela rotora Enigme s promjenjivim (nepravilnim) okretom (*Lueckenfuellerwalze*) vjerojatno bi spriječilo dekriptiranje Enigminih poruka nakon 1942. Uređaj Schluesselgeraet 39 (SG-39), koji je razvijan od 1939., trebao je zamijeniti Enigmu, ali do kraja rata proizvedeno je tek nekoliko pokusnih primjeraka. Taj bi uređaj potpuno onemogućio dekriptiranje poruka. Američki su stručnjaci, proučavajući odmah nakon rata te i druge njemačke uređaje za kriptozaštitu, došli do novih spoznaja u razvoju uređaja za kriptozaštitu.[16]

OKW/Chi je znao da se poruke šifrirane vojnom Enigmom mogu dekriptirati i da je šifre moguće razbiti pomoću stereotipnog početka poruke, stereotipnih poruka ili pomoću većeg broja dugih poruka. Njihova službena procjena bila je da je Enigma sigurna ako se operateri pridržavaju pravila pri njenoj uporabi. Pravi je problem ležao u tome što nijedna poruka, koju je bilo koja grana oružanih snaga zaista poslala „na terenu", nikad nije bila dana njima na raspolaganje pa OKW/Chi nije mogao realno procijeniti sigurnost Enigme. Također, OKW/Chi nije bio zadužen za kontrolu provođenja pravila o uporabi Enigme na terenu.[17]

[15] European Axis Signal Intelligence in World War II (1946).

[16] European Axis Signal Intelligence in World War II (1946).

[17] European Axis Signal Intelligence in World War II (1946).

Već je spomenuto da je mornarica bila samostalna po pitanju svojih sistema zaštite informacija. Kad je početkom 1944. ratna mornarica postala zabrinuta za sigurnost Enigme, časnik iz odjela mornarice za dekriptiranje[18] (OKM/4 SKL/III) Hans-Joachim Frowein prebačen je u odjel zadužen za sigurnost mornaričkih komunikacija[19] (OKM/4 SKL/II) kako bi proučio sigurnost mornaričke Enigme. Frowein je pomoću *criba* (dijela otvorene poruke) od 25 slova uspio dekriptirati poruku šifriranu mornaričkom Enigmom. Treba spomenuti da je Frowein znao koji su rotori (i s kojim unutarnjim ožičenjima!) uporabljeni.[20] Kad se uzme u obzir da su Britanci trebali *crib* od najmanje (oko) 14 slova kako bi mogli podesiti svoje „bombe", onda Froweinov rezultat i nije bio tako loš (Erskine 2004). Frowein je predložio strojnu (IBM) metodu dekriptiranja Enigminih šifri pomoću *criba* od 25 slova. Možda je OKW/Chi smatrao da neprijatelj ne može doći do *cribova* potrebnih za Froweinovu metodu. U svakom slučaju, kad su im pokazani Froweinovi rezultati, OKW/Chi se nije previše zabrinuo.

U izvješću o mornaričkim šiframa (od 10. srpnja 1944.), koje je napisala (vjerojatno) mornarička služba za sigurnost komunikacija (OKM/4 SKL/II), navodi se kako je rješenje mornaričke Enigme zamislivo uz uporabu nekog posebnog stroja koji bi neprijatelj uporabio. Iako oni (OKM/4 SKL/II) mogu zamisliti takav stroj, nemaju nijedan raspoloživ ili u razmatranju jer se još nije pojavio problem koji bi opravdao poduzimanje tako teške konstrukcijske zadaće. Ipak, njemački kriptoanalitičari nisu bili intelektualno nimalo inferiorni svojim britanskim i američkim kolegama, što su Amerikanci u svom izvješću priznali. Nijemci su u potpunosti shvatili teorijske slabosti vojne Enigme, a zanimljivo je da su i dekriptirali poruke šifrirane Enigmom.

OKW/Chi je, npr., dekriptirao švicarske diplomatske poruke. Švicarci su izmjenjivali ožičenje rotora svaka tri mjeseca, ali izmjena na vezi Bern – Washington kasnila je za onom na vezi Bern – London. Presretanje istih poruka, poslanih iz Berna u Washington i London tijekom perioda izmjene ožičenja, omogućilo je Nijemcima da dođu do informacija o novim ožičenjima rotora. I NDH je koristila Enigmu, a Nijemci su redovito čitali vojne i diplomatske poruke NDH šifrirane Enigmom jer su dobili podatke o ožičenjima rotora od berlinske firme Konski i Krueger koja je rotore izradila, poredak rotora i položaj jezgre rotora prema prstenu rotora nisu se mijenjali, samo stotinu početnih položaja rotora (na početku šifriranja) koristilo se tijekom jednog mjeseca.[21] Naravno, te modele Enigme nisu koristile njemačke oružane snage. Švicarci su koristili Enigmu tipa „K", a NDH je koristila „komercijalni" tip Enigme. Nijemci su razmatrali opremanje NDH vojnim tipom Enigme, ali to se nije dogodilo jer su vjerovali da bi „korumpirani Hrvati" prodali ključeve britanskim agentima.[22]

[18] Oberkommando der Marine / 4 Seekriegsleitung III – OKM/4 SKL/III, služba mornarice za prikupljanje informacija iz dekriptiranih neprijateljskih poruka.

[19] Oberkommando der Marine / 4 Seekriegsleitung II – OKM/4 SKL/II

[20] European Axis Signal Intelligence in World War II (1946).

[21] European Axis Signal Intelligence in World War II (1946).

[22] European Axis Signal Intelligence in World War II (1946).

SIGURNOST ULTRE

Ultra, tj. rezultati svih mjera dobivenih praćenjem neprijateljskih komunikacija, bila je saveznicima neprocjenjivo važna. Međutim, taj izvor podataka mogao je „presušiti" u svakom trenutku ako bi (u ovom slučaju) Nijemci došli do čvrstih dokaza da se njihove poruke (stalno) čitaju. Zbog toga su saveznici poduzeli sve moguće mjere za zaštitu Ultre. Mit da je Churchill, kako bi zaštitio Ultru, zabranio opću evakuaciju Coventryja i na taj način žrtvovao stanovnike tog grada, nije točan (West 1988), ali su ostale mjere zaštite odlučno provođene. Ultra je bila zaštićena ne samo za vrijeme rata, nego i dugo poslije toga. Međutim, nijedna zaštita nije savršena, uvijek ima opasnih trenutaka, pa je tako bilo i u ovom slučaju.

Odmah nakon okupacije Poljske 1939., Nijemci su pretražili poljski Ured za šifre i pronašli dokaze, uključujući dekripte, da su Poljaci čitali poruke šifrirane Enigmom. Pronađene su i tri otvorene poruke za koje su Nijemci znali da su poslane s njemačke krstarice (koja se nalazila u španjolskim vodama) tijekom Španjolskog građanskog rata, ali nisu uspjeli otkriti jesu li do njih Poljaci došli dekriptiranjem ili su te poruke bile naprosto ukradene.[23] Ured za šifre uspio je uništiti najvažnije dokumente i (što je bilo još važnije) opremu za dekriptiranje, uključujući i „bombu", jer se Varšava predala tek 27. rujna 1939., a najvažniji djelatnici Ureda za šifre uspjeli su na vrijeme prijeći u Rumunjsku i zatim u Francusku, gdje su nastavili svoj rad u sklopu francuske službe za dekriptiranje.

Nakon pada Francuske 1940., francuski i poljski dekripteri prešli su u Vichy, koji nije bio okupiran. Svi su dokumenti ili uništeni ili premješteni u Vichy pa Nijemci opet nisu ništa pronašli (Meyer 1975). U studenom 1942., nakon ulaska Nijemaca u dotad neokupirani dio Francuske, poljski dekripteri podijelili su se u manje skupine kako bi se bolje prikrili i lakše pobjegli u Španjolsku (i nakon toga u Veliku Britaniju). Vodeći matematičari[24] Rejewski i Zygalski uz silne su teškoće to i uspjeli, te su se u Velikoj Britaniji pridružili tamošnjim poljskim oružanim snagama.

Drugu su skupinu sačinjavali pukovnik Gwido Langer (prijeratni šef Ureda za šifre), njegov zamjenik (i šef njemačkog odjela Ureda) bojnik Maksymilian Ciezki i civilni djelatnici Ureda – Antoni Palluth, Edward Fokczynski i Kazimierz Gaca. Njihov francuski vodič ih je izdao te su ih u noći 10. na 11. ožujka 1943. uhvatili Nijemci. Langer i Ciezki poslani su u logor za ratne zarobljenike, gdje su ispitivani o Enigmi, ali su zavarali Nijemce navodeći kako je Ured za šifre mogao čitati neke poruke šifrirane Enigmom sve dok Nijemci nisu uveli neke izmjene (nisu rekli koje).[25] Oni su kombinacijom istine i laži uvjerili Nijemce da se ne trebaju previše brinuti za sigurnost Enigme. Pomoglo im je i to što ih je Abwehr (njemačka vojno-obavještajna služba) ostavio zajedno prije ispitivanja pa su mogli uskladiti priče.[26] Civili Palluth,

[23] European Axis Signal Intelligence in World War II (1946).

[24] Treći matematičar, Rózycki, te još dva poljska dekriptera i francuski časnik koji ih je pratio stradali su u siječnju 1942. prilikom potonuća francuskog putničkog broda *Lamoricière* u blizini Baleara. Tom je prilikom poginulo ukupno 222 putnika.

[25] Gwido Langer, Wikipedia.

[26] European Axis Signal Intelligence in World War II (1946).

Fokczynski i Gaca poslani su u koncentracijski logor (kao robovska radna snaga), gdje su Palluth i Fokczynski preminuli.[27] Oni su bili su upoznati sa svim detaljima rada Ureda za šifre. Naposljetku, Palluth i Fokczynski su prije rata bili suvlasnici tvrtke AVA, koja je za Ured proizvela mnoge uređaje, među ostalima i replike Enigmi i poljsku „bombu". Znali su mnogo, ali nisu odali ništa, unatoč užasnim uvjetima u kojima su ih Nijemci držali.

Tijekom rata Nijemci su ispitivali djelatnike Ureda za šifre i tvrtke AVA koji su ostali u Poljskoj. Nitko od njih nije odao ono najvažnije, da je Ured prije rata osmislio (i tvrtka AVA proizvela) repliku Enigme i „bombu"[28] pa Nijemci nikad nisu saznali koje su to izmjene, poduzete krajem 1938. i početkom 1939., uspjele onemogućiti daljnje dekriptiranje Enigminih poruka. Na kraju su Nijemci zaključili da je duplo šifriranje ključa poruke omogućilo Poljacima dekriptiranje poruka kopnene vojske i ratnog zrakoplovstva, te su te dvije grane njemačkih oružanih snaga 1. svibnja 1940. prekinule praksu duplog šifriranja ključa poruke.

Nijemci su mogli prihvatiti činjenicu da su Poljaci napadali Enigmu matematički, ali nisu saznali ništa o tehničkoj strani dekriptiranja, o replikama Enigme i o „bombi". Nisu vjerovali da su Poljaci sposobni stvoriti specijalni stroj za dekriptiranje, ili da su sposobni koristiti ogroman broj računara (Meyer 1975). U svakom su slučaju svi ispitani Poljaci pokazali veliku hrabrost, a Langer i Ciezki i veliku prisebnost i domišljatost. Langer i Ciezki imali su kakvu-takvu zaštitu kao ratni zarobljenici. Uhićeni civili držani su u strašnim uvjetima u koncentracijskom logoru i ipak nisu rekli ništa!

Nijemci su znali da Britanci i Amerikanci koriste računare. Jedan savezнички vojnik, zarobljen u sjevernoj Africi, prilikom ispitivanja rekao je da Britanci i Amerikanci u velikom „parku" zajedno rade i koriste Hollerithovu opremu (mehaničke računare). Krajem 1943. jedan njemački časnik, koji je pobjegao iz zarobljeništva u sjevernoj Africi, rekao je da Amerikanci imaju veliku službu za dekriptiranje koja koristi Hollerithovu opremu (Meyer 1975). Međutim, nije postojao način na koji bi Nijemci mogli slijediti te tragove, a i ti računari nisu bili novost. I Nijemci su koristili IBM-ove elektromehaničke računare (tabulatore) koje je proizvela i održavala IBM-ova njemačka podružnica Dehomag.

IBM-ovi računari (poznati, po svojem izumitelju, i kao Hollerithovi strojevi) već su 1930-ih omogućavali obradu (za ono doba) golemih količina podataka, što su koristile i vlade SAD-a i Trećeg Reicha. To su bili elektromehanički strojevi koji su radili tako da su se podaci (koji su se željeli obraditi) upisivali na perforirane kartice (ili, u slučaju tvrtke Siemens, na perforirane papirne vrpce) koje su se ubacivale u stroj. Rupice na perforiranoj kartici omogućavale su električni kontakt koji bi aktivirao pojedini brojač te bi podatak bio „upisan".

Sve važnije njemačke službe za dekriptiranje (uključujući i mornaričku službu OKM/4 SKL/III) koristile su IBM-ove strojeve kao pomoć u dekriptiranju. Iako su ponekad ti strojevi bili „prerađeni" za neke posebne izračune, većina računara korištena je za klasične matematičke operacije i statistiku, što se moglo izvršiti i „ručno", ali su

[27] Biuro Szyfrów, Wikipedia.

[28] Biuro Szyfrów, Wikipedia.

računari bili brži. Amerikanci su odmah poslije rata otkrili da su Nijemci koristili IBM-ove strojeve „na skoro identičan način kao i dekripteri američke kopnene vojske"[29]. Zbog svega toga Nijemci se nisu previše zabrinuli kad su saznali da i protivničke službe za dekriptiranje koriste IBM-ove računare.

Možda najopasniji trenutak za sigurnost Ultre dogodio se u kolovozu 1943. kad je njemačka vojno-obavještajna služba Abwehr od svog agenta, koji je bio visokopozicioniran u američkom Ministarstvu mornarice (*US Navy Department*) u Washingtonu, primila izvješće da se operativne zapovijedi poslane njemačkim podmornicama čitaju. Abwehr je smatrao tog agenta svojim najvažnijim agentom u Washintonu (Meyer 1975), međutim, on je vjerojatno imao pristup „samo" obrađenim podacima i nije mogao znati način na koji saveznici čitaju zapovijedi podmornicama jer je samo nekoliko osoba znalo baš sve o Ultri ili, u ovom slučaju, o dekriptiranju Enigminih poruka. Ne treba zanemariti ni to da Nijemci nikad nisu uspjeli čitati šifrirane poruke koje su izmjenjivali Britanci i Amerikanci, a koje su se ticale Ultre, pa je tajna Ultre bila dobro zaštićena.[30]

Sa SSSR-om je situacija bila malo drugačija. Barem su dva sovjetska agenta tijekom rata odavala podatke Ultre Sovjetskom Savezu. Jedan od njih, John Cairncross, bio je pripadnik Tajne obavještajne službe (Secret Intelligence Service), poznate i kao MI6, otkud je poslan na rad u Bletchley Park. Drugi, Leo Long, radio je u MI 14, odjelu vojno-obavještajne službe zaduženom za analizu njemačkih vojnih planova. Leo Long je imao pristup analizama u kojima su korištene informacije dobivene od tajnih izvora, ali ne i samim tajnim izvorima. Sasvim je sigurno da ni Cairncross nije imao podatke o načinu dekriptiranja njemačkih poruka. U svakom slučaju, radilo se o podacima koji su dobiveni dekriptiranjem poruka njemačke kopnene vojske i ratnog zrakoplovstva, i to ne samo poruka šifriranih Enigmom, nego i ostalim njemačkim sistemima kriptozaštite (Andrew 2009).

ZAKLJUČAK

Iako su Britanci znali detalje o Enigmi, uključujući njene rotore, dekriptiranje poruka njemačke mornarice nikad nije bilo jednostavno. Dekriptiranje običnih poruka šifriranih općim (*Allgemein*) ključem bilo je relativno jednostavno. Međutim, dekriptiranje poruka šifriranih prvo časničkim (*Offizier*), a potom općim ključem znalo je potrajati i više od tjedan dana.[31] Poseban ključ (*Sonderschlüssellen*) za komunikaciju pojedinog zapovjednika podmornice s vrhovnim zapovjednikom ratne mornarice Karlom Dönitzom, uveden krajem 1944., tek je ponekad bio dekriptiran u Bletchley Parku. Neki ključevi, npr. Aegir (bivši Ausserheimisch, britanski naziv Pike) koji su koristili njemački gusarski brodovi, nije razbijen nikad (Erskine 1988).

[29] European Axis Signal Intelligence in World War II (1946).

[30] European Axis Signal Intelligence in World War II (1946).

[31] R. Erskine, Breaking Naval Enigma.

Njemačka istraživanja, kojima se provjeravala sigurnost vojne Enigme, nisu rezultirala nekom praktičnom metodom rješavanja (dekriptiranja) poruka. Međutim, u američkom izvješću iz 1946. vrlo se pošteno priznaje da je pitanje bi li Britanci i Amerikanci došli na pomisao da konstruiraju „bombu" a da prije toga Poljaci nisu razvili svoju „bombu".[32] Na početku rata općenito se smatralo da je Enigma neprobojna, čak su i u Bletchley Parku tvrdili da nije vrijedno truda pokušavati razbiti Enigmu (Andrew 2009).

Saveznici su pobijedili u bitci za Atlantik zbog više razloga. Prvo, američka brodogradilišta gradila su sve više brodova (ratnih i trgovačkih) koje Nijemci jednostavno nisu stigli potopiti. Drugo, s vremenom je pratnja savezničkih konvoja bila sve jača, posebno kad su u uporabu uvedeni mali (eskortni) nosači zrakoplova. Treće, savezнички radari i sonari odigrali su važnu ulogu na licu mjesta, kad je trebalo odrediti točnu lokaciju njemačkih podmornica. Već 1944. 3-centimetarski radar mogao je uočiti šnorkel njemačke podmornice, a savezнички zrakoplovi bacali su hidroakustične plutače koje su slale u zrakoplov šumove zaronjenih podmornica a da podmornice to uopće nisu znale (Kahan 2001). Sve to bilo je kobno za njemačke podmornice. Ali, na strateškoj razini, najučinkovitija sredstva u borbi protiv podmornica bili su radiogoniometrija i razbijanje šifriranih poruka. I, što je još važnije, ta su dva sredstva bila tijesno povezana. Nijemci ne bi uveli u rad kratke signale da se nisu bojali savezničkih radiogoniometara, a bez njemačkih kodnih knjiga saveznici ne bi došli do *cribova* u porukama.

Sigurno je „izvanredno opsežan radiopromet njemačkih podmornica" pomogao saveznicima (Kahn 1979: 121) jer je dekriptiranje lakše što je više uhvaćenih poruka. Međutim, pogrešno je smatrati da su zapovjednici njemačkih podmornica previše koristili radiovezu. Admiral Dönitz je iz svog zapovjedništva vodio sve operacije podmornica, posebno one na Atlantiku, i morao je znati situaciju „na terenu", a to je bilo moguće samo stalnim slanjem izvješća s podmornica, radiovezom. Dönitz bez radioveze nije mogao djelovati pa je sve opasnosti korištenja radioveza morao prihvatiti pokušavajući ih smanjiti koliko je to bilo moguće.

Njemačka je mornarica organizirala odličan sistem radiokomunikacija koji je tijekom rata razvijan i poboljšavan. Znajući da imaju odličan sistem veza, i vjerujući u neprobojnost Enigme, Nijemci su logično za svoje gubitke krivili savezničke radiogoniometre, sonare i radare (osobito radare na zrakoplovima) i u svezi toga su poduzimali određene (ponekad vrlo uspješne) mjere. Dovoljno je istaknuti samo jedan primjer kako bi se pokazalo da je slanje izvješća s podmornica bilo neophodno. U lipnju 1944. u Engleskom je kanalu vladalo nevrijeme, ali su savezнички meteorolozi znali da će doći do višesatnog prekida u oluji. Upravo zbog toga je savezničko zapovjedništvo odlučilo pokrenuti invaziju na kontinent, nešto što se Nijemcima (u tom periodu) činilo nemogućim (Kahn 1979). Da bi se došlo do tako preciznih podataka, potrebno je izvršiti što je više moguće meteoroloških mjerenja na što je moguće većem prostoru. Zato su bila važna meteorološka mjerenja u sjevernom

[32] European Axis Signal Intelligence in World War II (1946).

Atlantiku i Nijemcima nije preostalo ništa drugo osim da koriste podmornice za prikupljanje (i slanje) meteoroloških podataka.

U dnevniku admirala Dönitza 10. svibnja 1944. zapisano je da podmornice (kojima je to zapovjeđeno) neredovito šalju meteorološka izvješća. Uz loše uvjete za slanje poruka, spominje se i dojam da je neprijatelj pojačao napade na te podmornice. Međutim, budući da su meteorološka izvješća neophodna (procjena trenutka invazije, procjena vremena savezničkih zračnih napada), izvješćivanje se mora nastaviti. Kako bi izbjegle neprijatelja, podmornice moraju između dva izvješćivanja proslijediti velikom brzinom na drugu poziciju, a ako su u njihovoj okolini snažno prisutni saveznici, moraju nakon slanja izvješća ostati zaronjene nekoliko sati.[33]

Zapovjedništvo je stalno upozoravalo podmornice da pažljivo koriste radioveze. U zapovijedi od 26. prosinca 1943. podmornicama *Merkator* (transportne podmornice koje su plovile iz Europe u Penang, Malezija, i obrnuto) navedene su mjere koje su trebale smanjiti opasnost: trebalo je koristiti kratke signale koliko god je to bilo moguće, a zapovjednici podmornica trebali su razmisliti moraju li zaista poslati poruku i je li poruka napisana najkraće i najjasnije moguće.

Poruke je trebalo slati u suton i prije nego što podmornica značajnije promijeni smjer plovidbe, a imena mjesta označavana su kodiranim geografskim pozicijama. Podmornice su trebale slati poruke u suton iz dva razloga. Prvo, u suton i zoru stanje u ionosferi se mijenja pa goniometriranje nije najtočnije. Drugo, ako podmornica koja šalje poruku bude točno locirana, nakon zalaska sunca ima puno veću šansu da ostane nezamijećena. S tim u vezi je i detalj o značajnijoj promjeni smjera plovidbe. Imena mjesta se u porukama nisu smjela navoditi kako protivnik ne bi došao do *cribova*.

Kad je podmornica bila u plitkim vodama pod kontrolom neprijatelja, dokumenti veze (upute, kodne knjige) tiskani crvenom tintom trebali su biti postavljeni tako da u slučaju potonuća voda dopre do njih.[34] Zbog svega navedenog u najmanju je ruku pretjerano ili previše pojednostavljeno tvrditi da „njemačka podmornička flota bijaše najbrbljavija vojna organizacija u povijesti ratova" (Kahn 1979: 122) ili da je „Dönitz previše brbljao" (Kahn 1979: 128).

Enigma je bila odličan stroj za šifriranje, a procedura njemačke mornarice bila je sigurna koliko je to bilo moguće. Nijemci su pokušali smanjiti mogućnosti dekriptiranja, ali nisu znali koliko su saveznici bili odlučni da stvore sistem koji će moći svakodnevno dekriptirati poruke njemačke mornarice. Upravo je ta odlučnost, uz tek nekoliko njemačkih pogrešaka, pomogla saveznicima da pobijede u bitci za Atlantik, bez čega konačna pobjeda ne bi bila moguća.

[33] F.d.U./B.d.U.'S War Log, 1–15 May 1944.

[34] F.d.U./B.d.U.'S War Log, 1–15 December 1943.

LITERATURA

Andrew, Christopher. 2009. *The defence of the Realm: The Authorized History of MI5*. London: Penguin Books.

Bauer, Arthur O. 2004. HF/DF An Allied Weapon against German U-Boats 1939-1945. http://jproc.ca/rrp/hfdf1998.pdf (pristupljeno 9. prosinca 2015.).

Biuro Szyfrów. https://en.wikipedia.org/wiki/Biuro_Szyfrów (pristupljeno 9. prosinca 2015.).

Bomba (cryptography). http://en.wikipedia.org/wiki/Bomba_(cryptography) (pristupljeno 9. prosinca 2015.).

Bombe. http://en.wikipedia.org/wiki/Bombe (pristupljeno 9. prosinca 2015.).

Brown, Anthony Cave. 1977. *Velike obmane Drugog svjetskog rata*. Zagreb: Centar za informacije i publicitet.

Ellsbury, Graham. 2003. The Enigma and the Bombe. http://www.ellsbury.com/enigmabombe.htm (pristupljeno 9. prosinca 2015.).

Erskine, Ralph. Breaking Naval Enigma (Dolphin and Shark). http://cryptocellar.web.cern.ch/cryptocellar/bgac/HMTR-2066-2.pdf (pristupljeno 25. studenog 2014.).

Erskine, Ralph. 1988. Naval Enigma: An Astonishing Blunder. *Intelligence and National Security* 3(1): 162.

Erskine, Ralph. Naval Enigma Ciphers. http://uboat.net/technical/enigma_ciphers.htm (pristupljeno 9. prosinca 2015.).

Erskine, Ralph. 2004. Shore High-Frequency Direction-Finding in the Battle of the Atlantic: An Undervalued Intelligence Asset. *The Journal of Intelligence History* 4(2): 1–32. http://www.intelligence-history.org/jih/journal.html (pristupljeno 25. studenog 2014.).

European Axis Signal Intelligence in World War II. 1946. Army Security Agency, Washington, D. C. https://www.nsa.gov/public_info/declass/european_axis_sigint.shtml (pristupljeno 9. prosinca 2015.).

F.d.U./B.d.U.'S War Log, 1–15 December 1943. http://www.uboatarchive.net/BDUKTB30336.htm (pristupljeno 9. prosinca 2015.).

F.d.U./B.d.U.'S War Log, 1–15 May 1944. http://www.uboatarchive.net/BDU/BDUKTB30346.htm (pristupljeno 9. prosinca 2015.).

Gwido Langer. http://en.wikipedia.org/wiki/Gwido_Langer (pristupljeno 9. prosinca 2015.).

Horn, Joseph. 1974. Building an Intercept Station During World/War II. *Cryptologic Spectrum Articles*, 45. sv., br. 4. http://www.nsa.gov/public_info/_files/cryptologic_spectrum/buidling_intercept_stn.pdf (pristupljeno 9. prosinca 2015.).

Johnson, Thomas R. 2004. The Sting – Enabling Codebreaking in the Twentieth Century. *Cryptologic Quarterly Articles*, 23. sv., br. 1–2. http://www.nsa.gov/public_info/_files/cryptologic_quarterly/the_sting.pdf (pristupljeno 9. prosinca 2015.).

Kahan, W. 2001. How Blabber-Mouth U-Boats got Sunk in World War II. http://www.cs.berkeley.edu/~wkahan/BlaUboat.pdf (pristupljeno 9. prosinca 2015.).

Kahn, David. 1979. *Šifranti protiv špijuna*. Zagreb: Centar za informacije i publicitet.

Marian Rejewski. http://en.wikipedia.org/wiki/Marian_Rejewski (pristupljeno 9. prosinca 2015.).

Meyer, Joseph A. 1975. Der Fall WICHER: GermanKnowledge of Polish Success on ENIGMA. *NSA Technical Journal Articles*, XX sv. http://www.nsa.gov/public_info/_files/tech_journals/Der_Fall_Wicher.pdf (pristupljeno 9. prosinca 2015.).

Milner-Barry, Stuart. 1978. Conel Hugh O'Donel Alexander: A Personal Memoir. *Cryptologic Spectrum Articles*, 8. sv., br. 2. http://www.nsa.gov/public_info/_files/cryptologic_spectrum/cono_hugh.pdf (pristupljeno 9. prosinca 2015.).

Rijmenants, Dirk. 2014. Cipher Machines and Cryptology. http://users.telenet.be/d.rijmenants (pristupljeno 9. prosinca 2015.).

Sale, Tony. Explore the Breaking of German Naval Enigma. http://www.codesandciphers.org.uk/virtualbp/navenigma/navindex.htm (pristupljeno 9. prosinca 2015.).

U-518 2nd War Patrol. http://www.uboatarchive.net/KTB518-2.htm (pristupljeno 9. prosinca 2015.).

West, Nigel. 1988. *Nepouzdani svjedok*. Zagreb: Alfa.

WWII: Bletchley Park. http://www.gchq.gov.uk/history/Pages/WWII-Bletchley-Park.aspx (pristupljeno 9. prosinca 2015.).

ENIGMA AND GERMAN SUBMARINES IN WW2

Robert Drenčin

SUMMARY

One of the reasons of Allied victory in WW2 was excellent work of British and American decrypting services. The most known success of the services was decrypting of German messages ciphered by cipher machine Enigma. The article describes how decrypting of German naval messages encrypted with the Enigma cipher machine was not simple and easy and how sometimes just good luck or personal bravery of few individuals helped allied codebreakers in their work.

Keywords: Enigma, Bombe, codebreaking, German submarines, Blechley Park.