UNIVERZA V LJUBLJANI
FAKULTETA ZA DRUŽBENE VEDE

Tina Cehtl

Kriptoanaliza v času prve svetovne vojne

Diplomsko delo

Ljubljana, 2016

UNIVERZA V LJUBLJANI
FAKULTETA ZA DRUŽBENE VEDE

Tina Cehtl

Mentor: doc.dr. Damijan Guštin

Kriptoanaliza v času prve svetovne vojne

Diplomsko delo

Ljubljana, 2016

Kriptoanaliza v času prve svetovne vojne

Odkritje radijskih valov in posledična možnost brezžične komunikacije preko le-teh je pomenila velik napredek v komuniciranju. Tudi države, ki so se spopadle v prvi svetovni vojni, so to novo obliko komunikacije s pridom izkoristile in tako bistveno skrajšale čas za prenos sporočil med enotami. Slaba stran brezžične komunikacije je pomanjkanje zasebnosti. Vsak lahko ujame brezžični signal, tako prijatelj kot nasprotnik. Zaradi tega se je povečala potreba po učinkovitem kodiranju in šifriranju podatkov. Prav tako pa se je povečala pomembnost enot znotraj obveščevalnega sistema, ki so se ukvarjale z razbijanjem nasprotnikovih šifer in kod. Tako pridobljene informacije so v nekaterih primerih bistveno vplivale na potek prve svetovne vojne. V pomorskih bitkah so zagotavljale prevlado Kraljeve vojne mornarice, saj so Britanci že v začetku vojne zasegli pomembnejše nemške kodirne knjige. Uspeh kriptoanalitikov je pomembneje vplival tudi na vstop Združenih držav Amerike v vojno, saj se je po razkritju Zimmermanovega telegrama javno mnenje prevesilo v prid vojne. Na zahodni fronti so Nemci v zadnjem poskusu leta 1918 začeli spomladansko ofenzivo in dokler so njihovi načrti ostali prikriti, so želi velike uspehe, ko pa so francoski kriptoanalitiki zlomili njihove šifre, se je njihovo napredovanje ustavilo. Vse to kaže na pomembno vlogo, ki jo je kriptoanaliza igrala v poteku in razpletu prve svetovne vojne.

Ključne besede: brezžična komunikacija, prestrezanje sporočil, kode in šifre, kriptoanaliza.

Cryptanalysis during the First World War

The discovery of radio waves and consequently the possibility of wireless communication was a major step forward in terms of communication. Countries participating in the First World War, ebraced this new form of communication and significantly reduced the time for transmission of messages among units. The downside of wireless communication is the lack of privacy. Anyone can catch a wireless signal, a friend or the opponent. This has increased the need for effective encoding and encripherment of data. It also increased the importance of the units within the intelligence communities that dealt with cryptanalysis. Information obtained through cripanalysis in some cases significantly affect the course of the First World War. In the naval battles they ensured the supremacy of the Royal Navy, as the British already at the beginning of the war seized important German coding books. Successful codebreaking had a significant impact on the entry of the United States into the war, because after disclosure of Zimmerman telegram, the public opinion waged towards the war. On the Western Front the Germans in the last attempt to win the war, started the spring offensive and as long as their plans were obscured they had great success, but when the French cryptanalysts broke their code, their progress stopped. All this points to an important role that cryptanalysis played in the course of the First World War.

Keywords: wireless communications, interception of communications, codes and ciphers, cryptanalysis.

KAZALO

1 Uvod

Kriptoanaliza (znanost razbijanja šifer) je doživela svoj razcvet ravno v času prve svetovne vojne. Poznali so jo že mnogo stoletij prej, vendar so bila prestrežena sporočila nasprotnikov redka in posledično je kriptoanaliza predstavljala le droben delec v obveščevalni dejavnosti držav. Večino obveščevalnih podatkov so zbrali vohuni in tako pridobljene informacije so lahko kvečjemu vplivale na srategijo vodenja vojne, na taktično poveljevanje pa niso imele večjega vpliva. Začetek 20. stoletja je prinesel velik napredek na področju komuniciranja na daljavo. Telefon je sicer bil v uporabi že pol stoletja, vendar je ta komunikacija zahtevala žično povezavo, katere postavitev je bilo zamudno, včasih pa tudi nemogoče delo. Na prelomu stoletja je italijanski fizik Guglielmo Marconi naredil velik preskok in uveljavil radijsko povezavo, katere največja prednost je bila neposredna povezava med poljubnimi kraji brez žične povezave. Radijsko prestrezanje je pomenilo pridobivanje informacij v realnem času in če so bili vojaški poveljniki obveščeni o npr. premikanju nasprotnikovih enot ali njihovi oborožitvi, je to bistveno vplivalo na njihove taktične odločitve.

Ob izbruhu vojne je bila radijska oprema še zelo primitivna, s kratkim dosegom in pogostimi motnjami. Vojaški radio je bil velik in težek, zato ga je bilo težko premikati po bojišču, vendar se je v času vojne razvil v učinkovito napravo, ki jo je bilo mogoče pripeti na na sedlo konja. Vendar je preprostejši način komuniciranja prinesel tudi preprostejši način prisluškovanja, in bližajoča se vojna je povzročila drastično potrebo po zanesljivem kodiranju.

Uporaba kod v procesu komuniciranja preko telegrafa se ni pojavila kot potreba vojne. Telefonska podjetja so računala prenos sporočil po številu uporabljenih besed. Posledično so se pojavile kodirne knjige, ki so cele stavke ali fraze skrajšale na eno besedo. Takšne kodirne knjige so se uporabljale v komercialne namene in niso bile skrivne. Podjetja so kupovala kodirne knjige za svoja področja, npr. za zavarovalništvo, prodajo avtomobilov ipd. Tudi vojaška poveljstva so imela svoje kodirne knjige, vendar je bilo v tem primeru ohranjanje tajnosti le-teh ključnega pomena. Države so v ta namen rekrutirale kriptografe, strokovnjake, ki so bili zadolženi za pisanje šifer in kod, kot tudi kriptoanalitike z nalogo razbijanja nasprotnikovih šifer in kod.

Zadnji večji prodor na področju kriptoanalize sta v drugi polovici 19. stoletja naredila britanski genij Charles Babbage in upokojeni pruski častnik Friederich Wilhelm Kasiski, ki sta ločeno dešifrirala Vigenerjevo šifro, ki je veljala za nezlomljivo skoraj tri stoletja. Pred

izbruhom prve svetovne vojne je bila takrat najvarnejša šifra že razvozlana in na vrsti so bili kriptografi, da uvedejo nov način varnega komuniciranja.

Prva svetovna vojna je prinesla potrebo po organiziranih kriptografskih službah z osebjem, ki je bilo posebej v ta namen izobraženo na področju matematike, logike in jezikov. Novoustanovljeni organi so zaposlovali tako kriptoanalitike in prevajalce kot tudi tajne agente in protiobveščevalno osebje. Četudi nekatere države v vojno niso vstopile povsem pripravljene na tem področju, so kmalu ugotovile, da je varen prenos podatkov bistvenega pomena za uspeh v vojni in so kmalu okrepile (ali šele na novo ustanovile) svoje kriptografske službe.

2 Metodološko-hipotetični okvir

2.1 Predmet in cilj proučevanja

V diplomskem delu bom predstavila kriptografske službe svetovnih velesil med 1. svetovno vojno, kode in šifre, ki so jih države uporabljale, in načine s pomočjo katerih so se strokovnjaki spopadali z dekriptiranjem nasprotnikovih šifer.

V diplomskem delu bom analizirala nekatere večje dosežke dekripterjev v času 1. svetovne vojne in vpliv teh prebojev na potek in razplet vojne.

2.2 Hipoteze

Hipoteza 1:

Šifrirni postopki v vojni udeleženih držav so zaradi njihovega pomena in prepoznanih tveganj postajali bolj zapleteni in težje zlomljivi.

Hipoteza 2:

Uspešno dešifriranje prestreženih dokumentov je, v nekaterih primerih, bistveno vplivalo na potek prve svetovne vojne.

2.3 Metodologija

V diplomskem delu sem uporabila različne metode raziskovanja. Za razumevanje in oris teme sem uporabila *metodo interpretacije sekundarnih virov*. Za opis in razlago osnovnih

pojmov sem uporabila *deskriptivno metodo,* s pomočjo *metode zgodovinske analize* pa bom predstavila razvoj kriptologije. Pri predstavitvi in analizi značilnih primerov bom uporabila *metodo študije primerov*. V postopku potrjevanja hipotez sem uporabila *primerjalno analizo.*

2.4 Temeljni pojmi

Komunikacije lahko prikrijemo na dva osnova načina. S *stenografijo* prikrijemo obstoj samega sporočila npr. z nevidnim črnilom ali tako, da določene črke znotraj drugega besedila npr. časopisnega članka prestavljajo skrivno sporočilo. Na drugi strani pa *kriptografija* ne zanika obstoja takega sporočila, ampak ga naredi neberljivega z različnimi zamenjavami črk ali besed v besedilu (Kahn 1996, xv).

Kriptologija je znanost, ki se ukvarja z varnimi in običajno skritimi komunikacijami. Sestavljata jo kriptografija in kriptoanaliza. Prva se ukvarja z uporabo načel in tehnik s katerimi naredimo sporočilo neprepoznavno za vse razen za namenjenega prejemnika. Slednja pa je znanost in hkrati umetnost, ki se ukvarja z reševanjem kriptosistemov z namenom pridobiti takšne skrite informacije (Adler 1998, 768).

Vojna enciklopedija (Gaževič ur. 1985, 714) pojem kriptografija opredeli kot »znanost o zaščiti informacij pred nepooblaščenimi osebami s preprečevanjem branja ali potvarjanja informacij«, kriptoanalizo pa kot »odkrivanje informacij in šifriranih sporočil brez predhodnega poznavanja postopka, s katerim so bila šifrirana«.

Pri terminologiji s področja kriptologije moramo biti pozorni na nekatere na videz majhne, a vseeno pomembne razlike.

Pomembno je razlikovati med *kodo* in *šifro*. Kodiranje se nanaša na postopek, ko določeno besedo ali stavek zamenjamo z drugo besedo. Njegova alternativa je šifriranje, kjer ne zamenjamo celotnih besed, ampak vsako črko posebej. Prav tako je potrebno pojasniti razliko med pojmoma *dekodirati oz. dešifrirati* in *dekriptirati*. Dekodiranje (dešifriranje) pomeni spremeniti kodirano (šifrirano) sporočilo nazaj v prvotno sporočilo. To dejanje lahko izvede vsak, ki mu je na voljo ključ, s katerim je bilo besedilo kodirano (šifrirano). Ko nam ključ ni na voljo, govorimo o dekriptiranju. To je pojem, ki ga imamo v mislih, ko govorimo o prestrezanju nasprotnikovih sporočil in ugibanju njihove vsebine. Veda, ki raziskuje, kako odpreti besedilo brez poznavanja ključa, se imenuje kriptoanaliza (Singh 2008, 11–16).

Odprto besedilo je sporočilo, preden ga spremenimo v prikrito obliko, ki jo imenujemo *skrito besedilo*. Večina šifer uporablja *ključ,* ki nam pove, na kakšen način so

razporejene črke znotraj šifrirane abecede, vzorec premika črk v transpoziciji ali nastavitve šifrirne naprave (Kahn 1996, xv).

Prav tako moramo razlikovati ključ in *algoritem*. Algoritem je splošna šifrirna metoda, s katero je neko sporočilo šifrirano. Ključ pa nam razkrije, kako je v določenem sporočilu algoritem uporabljen. Pošiljatelj in prejemnik morata najprej izbrati algoritem, s katerim bosta šifrirala sporočilo in nato še ključ. Algoritem je torej postopek, ki se načeloma ne spreminja in je večinoma znan tudi nasprotniku, ključ pa je podvržen redni menjavi in od njegovega prikritja je odvisno prikritje besedila (Beutelspacher 1994, 5–6).

Osnovna kriptografska postopka pretvorbe odprtega besedila v skrito besedilo sta: *transpozicija* in *substitucija*. Pri uporabi transpozicije premešamo vrstni red črk v besedilu, vendar pa te ostanejo enake (npr. špartanska skitala, glej poglavje Razvoj kriptologije do prve svetovne vojne). Pri substituciji pa črke v odprtem besedilu zamenjamo z drugimi črkami, številkami ali simboli (npr. Cezarjev premik, glej poglavje Razvoj kriptologije do prve svetovne vojne). Če uporabimo transpozicijo, torej spremenimo vrstni red črk in jih ohranimo, pri substituciji pa spremenimo črke in ohranimo vrstni red. Lahko pa uporabimo kombinacijo obeh načinov. Metoda substitucije je veliko bolj varna in pogosteje uporabljena. Temelji na uporabi alfabetske šifre tj. seznama črk, številk ali simbolov, s katerimi pretvorimo odprto besedilo v skrito besedilo. Poznamo monoalfabetski in polialfabetski sistem. Pri prvem je v uporabi le ena abeceda, pri drugem pa dve ali več. Tako lahko npr. prvo črko odprtega besedila zamenjamo s črko iz prve alfabetske šifre, drugo z drugo, tretjo ponovno s prvo itd. Takšno šifro je bistveno težje dekriptirati (Kahn 1996, xv–xvii in Blake 2010, 82–99).

3 Razvoj kriptologije do prve svetovne vojne

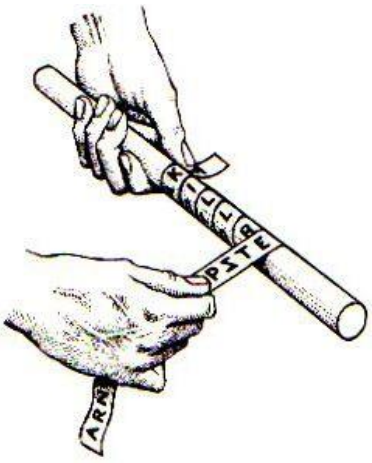
Kahn (1996, 84) ugotavlja, da se »takoj ko določena kultura doseže določeno stopnjo, najbrž merjeno glede na pismenost, kriptografija pojavi spontano.« Potreba po zasebnosti komunikacije med dvema ali več ljudmi privede do razvoja kriptografije, ne glede na časovni ali geografski okvir.

Zametke skrivnega pisanja tako najdemo že v času zgodnjih civilizacij. Egipčani so na stene svojih grobnic dali vklesati hieroglifske zapise z nekoliko drugačnimi simboli. Namen tega sicer ni bilo skrivno pisanje, saj je bilo včasih besedilo v svoji običajni obliki zapisano takoj zraven spremenjenega besedila. Kitajci niso razvili posebnih kriptografskih postopkov. To lahko pripišemo dejstvu, da so večino svojih sporočil prenašali tako, da si je sel zapomnil

sporočilo in ga osebno predal prejemniku. Pri zapisovanju sporočil so Kitajci uporabili steganografijo in sicer tako, da so sporočilo zapisali na zelo tanko svilo ali papir, ga zmečkali in namočili v vosek. Takšno voščeno kroglico je nato sel skril pri sebi ali jo pogoltnil. V sosednji Indiji so uporabljali več načinov skrivnega pisanja. Celo Kama-sutra navaja skrivno pisanje kot eno izmed 64 veščin, ki jih mora obvladati ženska. Vendar pa zgodnja dela npr. Mudra Raksasa kažejo, da kriptografija v Indiji ni bila v širši rabi. V okviru zgodnjih civilizacij je bila kriptografija najbolje razvita v Mezopotamiji. Najstarejše danes znano prikrito besedilo, napisano okoli leta 1500 pr.n.št., je majhen klinopis, ki vsebuje najstarejše navodilo za lakiranje lončevine. Pisec je uporabil najmanj znan izmed več možnih znakov za določen zlog. Besedila sicer ni bilo težko razvozlati, vendar je v okolju z izredno majhno pismenostjo dovolj dobro ohranilo svojo skrivnost (Kahn 1996, 71–76).

Prvi, ki so uporabili kriptografijo v vojaške namene, so bili Špartanci. Uporabljali so pripomoček imenovan skitala (glej Slika 3.1: Špartanska skitala). To je palica, okoli katere so ovili pergamentni trak in nanj napisali sporočilo. Trak so nato odvili in tako prikrili sporočilo, ki je bilo sestavljeno iz posameznih črk ali črkovnih skupin. Uporabili so torej transpozicijsko metodo, ključ pa je bil v tem primeru velikost palice, okoli katere je moral prejemnik naviti trak, da je lahko prebral sporočilo (Blake 2010, 75).

Slika 3.1: Špartanska skitala



Vir: Blatner (2011)

Grški pisec Polybius (ok. 200 pr. n. št. – ok. 118 pr. n.št.) je razvil metodo šifriranja, ki je kasneje, kljub temu, da ni nobenih dokazov o njeni uporabi v tem času, postala osnova za številne druge šifrirne sisteme. Črke abecede je razvrstil v kvadrat ter oštevilčil vrstice in stolpce (glej Slika 3.2: Polybiusov kvadrat). Predlagal je, naj se sporočila prenašajo s pomočjo

bakel, kar omogoča premagovanje dolgih razdalij v kratkem času. Število bakel v desni roki je predstavljalo mesto črke v stolpcu, število bakel v levi roki pa njeno mesto v vrstici. Če je nekdo želel prikazati črko e, je moral v desni roki držati pet bakel, v levi pa eno.

Slika 3.2: Polybiusov kvadrat

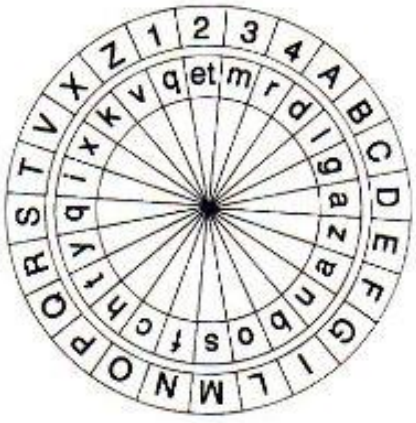
	1	2	3	4	5
1	a	b	c	d	e
2	f	g	h	ij	k
3	l	m	n	o	p
4	q	r	s	t	u
5	v	w	x	y	z

Polybiusov kvadrat je preprosta substitucijska metoda, kjer črke pretvorimo v določen par številk. Takšno šifro je mogoče dekriptirati s frekvenčno analizo (Kahn 1996, 83).

Prvi, ki je potrjeno uporabljal Polybiusov kvadrat, je bil Julij Cezar. Uporabljal je več tajnih pisav, med drugim je nadgradil Polybiusovo metodo v metodo, ki jo danes poznamo kot Cezarjevo šifro ali Cezarjev premik. Deluje tako, da pod abecedo odprtega besedila zapišemo abecedo skritega besedila, ki je zamaknjena za tri mesta. Gre za uporabo substitucije, ključ pa predstavlja število mest, za katerega je abeceda skritega besedila zamaknjena v primerjavi z abecedo odprtega besedila, torej tri (Singh 2003, 27).

Šifriranje daljših besedil na tak način je bilo zamudno delo in renesančni arhitekt in teoretik Leone Battista Alberti (1404–1472) je izumil napravo, ki je bistveno poenostavila postopek takšnega šifriranja. Šlo je za dva diska, pri čemer se notranji disk, na katerem je zapisana abeceda odprtega besedila, zavrti za določeno število mest (ključ) in tako razkrije abecedo skritega besedila (Beutelspacher 1994, 5–6).

Slika 3.3: Albertijev disk



Vir: Blatner (2011)

Po propadu rimskega imperija je Evropa stopila v srednji vek, stopnja pismenosti je drastično padla, znanost je bila potisnjena na stranski tir, kriptografija pa prepovedana. Cerkev je kriptografijo označila kot črno magijo, saj se je zdelo, da je pridobivanje informacij iz navidezno nesmiselnih znakov enako neverjetno kot pridobivanje le-teh iz načina premikanja planetov, črt na človeški dlani ali vzorca v čajni usedlini. Kriptografija se je zdela enaka vedeževanju in zato prepovedana. V tem obdobju se pojavlja redko in v večini primerov v lastno zabavo piscev in ne za prenašanje skrivnih sporočil. Med znane uporabnike skritega pisanja sodita angleški menih Roger Bacon in carinski delavec ter ljubiteljski astronom Geoffrey Chaucer (Kahn 1996, 89–92).

Ko je bila Evropa globoko v temačnem obdobju srednjega veka, se je razcvet kriptografije preselil v arabske dežele. Arabci so bili prvi, ki so vedo kriptologije razvili v celoti, torej ne le kriptografije, tj. pisanja skrivnih sporočil, ampak tudi kriptoanalizo, tj. razkrivanje skritih besedil brez poznavanja ključa.

Egiptovski učenjak al-Qalqashandi je leta 1412 dokončal 14 knjig obsegajočo enciklopedijo, ki vključuje vse pomembne veje znanosti in vsebuje poglavje o kriptologiji. V njej je naštetih sedem šifrirnih sistemov: (1) posamezna črka lahko nadomesti drugo, (2) kriptograf lahko napiše besedo v obratnem vrstnem redu, (3) v obratnem vrstnem redu lahko napiše vsako drugo črko, (4) črke lahko nadomestijo številke, (5) vsako črko lahko nadomestita dve črki, seštevek njunih numeričnih vrednosti pa predstavlja numerično vrednost izvirne črke, (6) kriptograf lahko vsako črko nadomesti z imenom osebe ali (7) črke nadomesti z imeni držav, dreves idr. Pri svojem delu se je al-Qalqashandi nanašal na zgodnejše avtorje, med drugim na »filozofa Arabcev« al Kindija, ki je živel v devetem

stoletju. Al- Kindi je tisti, ki je prvi opisal tehniko kriptoanalize, imenovano frekvenčna analiza, ki je naredila večstoletij nezlomljivo monoalfabestko šifro neuporabno (Kahn 1996, 95–96).

V Evropi se je kriptografija razširila šele v 15. stoletju. Najbolj razvita je bila na področju današnje Italije, ker so mestne državice tekmovale med seboj. Svoje predstavnike so pošiljale po vseh večjih dvorih in tako se je razcvetela diplomacija, ki je zahtevala veliko mero tajnosti. Dvori so ustanavljali svoje kriptografske službe, vsak poslanik pa je imel svojega tajnika za šifriranje (Singh 2003, 48).

Za razvojem kriptografije se je razvijala tudi kriptoanaliza. Kahn (1996, 108–114) ugotavlja, da se je kriptoanaliza v Evropi najverjetneje razvila samostojno in ni prišla iz arabskih dežel, kjer so frekvenčno analizo poznali že več stoletij. Najbolj napredni na tem področju so bili Benečani, ki so prvi imenovali ministra za šifriranje. To funkcijo je leta 1506 prevzel Giovanni Soro, najboljši kriptoanalitik svojega časa. Med druge znane kriptoanalitike tega obdobja sodijo Pirrho Musefili iz Firenc, Cicco Simonetta iz Milana ter Philiber Babou iz Francije in Antonio Elio iz Vatikana. Konec 16. stoletja je kriptoanalizo v Vatikanu prevzela družina Argenti, ki je nadgradila enostavno monoalfabetsko šifro, ki je bila takrat v splošni rabi in je bila ranljiva za frekvenčno analizo ter ji dodala uporabo ključne besede (Singh 2008, 77–78).

Drugi načini, kako otežiti kriptoanalizo so dodajanje mašil, tj. simbolov, ki ne pomenijo ničesar, več simbolov, ki predstavljajo isto črko odprtega besedila ali posebni znaki, ki so označevali, da gre za dvojno črko (npr. pogosti dvojni l v italijanščini). Med take izboljšave spada homofona substitucijska šifra, pri kateri lahko vsako črko zamenjamo z več različnimi simboli, število le-teh pa je odvisno od pogostosti črke, ki jo želimo šifrirati. Črko *e,* ki v se v slovenskem jeziku pojavlja v skoraj 11 % vseh simbolov, lahko nadomestimo z 11 različnimi simboli, ki se nato v besedilu pojavljajo v zgolj enem odstotku. Tako izničimo bistveno predpostavko frekvenčne analize, tj. da se določene črke v besedilu pojavljajo pogosteje kot druge (Singh 2008, 77–78).

Naslednji večji preskok v kriptografiji je uvedba polialfabetske šifre, pri kateri lahko vsako črko odprtega besedila šifriramo z drugo abecedo, kar pomeni, da lahko isto črko odprtega besedila v skritem besedilu nadomestimo z različnimi črkami. Ta sistem je prvi predstavil Leon Batista Alberti v prvi polovici 15. stoletja kot odgovor na frekvenčno analizo s katero je bilo mogoče rešiti monoalfabetske šifre. Izdelal je t.i. albertijev disk (Slika 3.3: Albertijev disk) in za vsake tri ali štiri besede premaknil krog, da je zamenjal šifrirno abecedo ter tako ustvaril poliafabetsko šifro (Singh 2008, 69–70).

Alberti svoje ideje ni razvil v dozorel šifrirni sistem, ampak so to naredili tisti, ki so sledili njegovemu delu. Nemški menih Johannes Trithemius (1462-1516) je uvedel t.i. tabulo recta, kvadrat, v katerem je zapisanih toliko šifrirnih abeced, kolikor je črk v abecedi in vsako je premaknil za eno mesto v levo (glej Slika 3.4: Tabula recta). Prednost te šifre je ta, da vsako črko šifriramo z drugo abecedo, medtem ko je Alberti šifro zamenjal po nekaj besedah in zato dopustil možnost ponavljanja določenih besed, kar bi izurjen kriptoanalitik lahko izkoristil za vdor v šifrirni sistem (Singh 2008, 84–85).

Slika 3.4: Tabula recta

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

Polialfabetska šifra se torej pojavi že v 15. stoletju, v splošno uporabo pa ni prišla vse do poznega 18. stoletja, saj se je zdela preveč zapletena. Tako je večina kriptografov še naprej uporabljala monoalfabetske šifre. Na drugi strani pa so države organizirale t.i. črne komore (black chambers), tajne službe, katerih edina naloga je bila dekriptiranje diplomatskih pisem. Že ob koncu 17. stoletja je črna komora na Dunaju delovala z izjemno natančnostjo. Pisma, ki

so prispela z jutranjo pošto, so previdno odprli, prepisali in jih najkasneje v treh urah predali nazaj na poštni urad, ki jih je dostavil pravim naslovnikom. Ker je bil Dunaj ne le pomembno diplomatsko središče, ampak tudi postojanka na tranzitni poti skozi Avstrijo, je dunajska črna komora vsak dan prestregla okoli sto pisem. S pridobljenim vedenjem pa ni zalagala le avstrijskega cesarja, ampak je informacije prodajala tudi tujim monarhom (Singh 2008, 84–85).

Sedaj so bili kriptografi prisiljeni uporabiti zamudnejšo, vendar bolj zanesljivo Vigenerjevo šifro, ki je vse do sredine 19. stoletja veljala za nerešljivo. Ta šifra sestoji iz klasičnega kvadrata s 25. abecedami in kratko ključno besedo, ki pa kljub nazivu *le Chiffre indechiffrable* v resnici ni nerešljiva, kar je leta 1854 dokazal britanski genij Charles Babbage.

Naslednji korak v razvoju kriptografije predstavlja playfairov šifra, ki jo je leta 1854 razvil Charles Wheatstone – in je bila v uporabi še v času prve svetovne vojne. Šifra je na videz preprosta monoalfabetska substitucijska šifra, ki pa namesto menjave črke za črko uporablja menjavo dvojice črk. V tem primeru je standardna rešitev za monoalfabetske šifre – frekvenčna analiza bistveno težja, saj preidemo iz 26 možnih rešitev na kar 600. Šifra je bila popularna ravno zato, ker je zagotavljala bistveno večjo varnost, obenem pa je ni bilo bistveno težje zapisati, kot je to veljalo za Vigenerjevo šifro (Crypto Corner 2016).

Za zapis playfairove šifre začnemo s kvadratom 5×5, ki je bil najpogosteje uporabljen (kvadrat je sicer lahko bil poljubne velikosti) ter v katerega najprej zapišemo ključno besedo, ostale prostore pa zapolnimo z manjkajočimi črkami po abecednem vrstnem redu.

Slika 3.5: Playfairova šifra

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

Sedaj črke odprtega besedila zapišemo v skupinah po dve: besedilo RABIMO MUNICIJO zgleda tako RA BI MO MU NI CI JO. Pri uporabi playfairove šifre se držimo štirih osnovnih pravil:

- če sta obe črki v paru isti, ali nam na koncu ostane samo ena črka, namesto druge črke uporabi X,

- če se črki para v odprtem besedilu pojavita v isti vrsti, ju nadomesti s črkami na njuni desni, le se črka pojavi na koncu vrstice, jo nadomesti s prvo črko naslednje vrstice,
- če se črki pojavita v istem stolpcu, ju zamenjaj s črkami, ki se pojavita pod njima, če je katera črka na dnu stolpca, nadaljuj v naslednjem stolpcu,
- če se črki ne pojavita v isti vrstici ali stolpcu, okoli njiju tvori pravokotnik in ju nadomesti s črkami, ki tvorita druga dva kota pravokotnika. Na prvo mesto vedno spada črka, ki se nahaja v isti vrstici kot prva črka odprtega besedila.

Po uporabi teh pravil dobimo sledeče besedilo: PC IQ NL NT PK BK NE (Crypto Corner 2016).

Kot že rečeno, Playfairova šifra ni nezlomljiva, vendar potrebujemo za frekvenčno analizo parov črk bistveno daljše besedilo, ali skupino besedil, zašifriranih z istim ključem.

4 Kriptografija v času prve svetovne vojne

Ob izbruhu vojne so bile najpogosteje uporabljane substitucijske šifre z uporabo ključne besede.

Britanci so uporabljali Playfairovo šifro, ki sicer ni nerešljiva, vendar so ključ, ki je potreben za uporabo šifre menjavali dovolj pogosto, da je Nemcem ni uspelo zlomiti (Kahn 1996, 312).

Francozi so uporabljali t.i. Tableau de Concordance s superšifrirnim postopkom. Tako se imenuje, ker je za šifriranje potreben več kot en korak. Najprej s pomočjo kodirne knjige črke odrtega besedila spremenimo v štiri številke, te pa nato še v črke. Gre torej za dvojno substitucijo. Francozi so kodirno knjigo med avgustom 1914 in januarjem 1915 spremenili kar trikrat. Kljub temu, da je bila francoska šifra enostavnejša od nemške, so Nemci dosegli le delni uspeh (Kahn 1996, 313).

Tako Britanci kot tudi Francozi so ves čas vojne uporabljali iste šifre, seveda s pogosto menjavo ključev oz. kodirnih knjig. Na drugi strani pa so Nemci v času vojne zamenjali celoten sistem šifriranja.

Na začetku vojne so uporabljali šifro ÜBCHI. To je bila dvojna transpozicijska šifra, s ključno besedo ali frazo, ki jo je bilo pred šifriranjem besedila potrebno pretvoriti v numerično zaporedje. Ključno frazo *Zmaga je naša* pretvorimo tako:

Z	M	A	G	A	J	E	N	A	Š	A
11	9	1	6	2	7	5	8	3	10	4

Črke v frazi razporedimo po abcedenem vrstnem redu in jim dodelimo zaporedno črko. V našem primeru imamo v ključni besedi 4 A-je in jim zato po vrsti dodelimo številke 1, 2, 3 in 4. Naslednja po abecedi je črka E, ki dobi številko 5 itd.

Nato odprto besedilo horizontalno zapišemo pod ključ in nato vertikalno preberemo črke po vrstnem redu, ki ga določa zaporedje številk v ključu ter jih prepišemo v novo tabelo.

Odprto besedilo

11	**9**	**1**	**6**	**2**	**7**	**5**	**8**	**3**	**10**	**4**
N	I	K	A	R	N	E	D	O	V	O
L	I	D	A	B	I	S	O	V	R	A
Ž	N	I	K	V	E	D	E	L	K	J
E	B	O	Š	U	D	A	R	I	L	S
I	C	E	R	B	O	T	A	M	Z	B
R	A	L	V	S	O	S	V	O	J	O
M	O	Č	I	N	S	E	T	I	U	S
P	E	L	U	P	R	E	T	I		

Prva transpozicija

11	**9**	**1**	**6**	**2**	**7**	**5**	**8**	**3**	**10**	**4**
K	D	I	O	E	L	Č	L	R	B	V
U	B	S	N	P	O	V	L	I	M	O
I	I	O	A	J	S	B	O	S	E	S
D	A	T	S	E	E	A	A	K	Š	R
V	I	U	N	I	E	D	O	O	S	R
D	O	E	R	A	V	T	T	I	I	N
B	C	A	O	E	V	R	K	L	Z	J
U	N	L	Ž	E	I	R	M	P		

Glede na to, da gre za dvojno transpozicijsko šifro, postopek ponovimo.

Druga transpozicija

11	**9**	**1**	**6**	**2**	**7**	**5**	**8**	**3**	**10**	**4**
I	S	O	T	U	E	A	L	E	P	J
E	I	A	E	E	R	I	S	K	O	I
L	P	V	O	S	R	R	N	J	Č	V
B	A	D	T	R	R	O	N	A	S	N
R	O	Ž	L	O	S	E	E	V	V	I
L	L	O	A	O	T	K	M	D	B	I
A	I	O	C	N	B	M	E	Š	S	I
Z	K	U	I	D	V	D	B	U		

Nato besedilo prepišemo v skupinah petih črk za lažje pošiljanje: ISOTU EALEP JEIAE ERISK OILPV OSRRN JČVBA DTRRO NASNR OŽLOS EEVVI LLOAO TKMDB IAIOC NBME ŠSIZK UIDVD BU.

Francoski kriptoanalitiki so kmalu našli rešitev za to šifro in so lahko, če jim je bilo na voljo dovolj sporočil zašifriranih z istim ključem, prebrali že v enem dnevu.

Nemci so zato v pripravah na zadnjo veliko ofenzivo spomladi 1918 dali v uporabo novo šifro, ki je uporabljala tako substitucijo kot transpozicijo – imenovano ADFGX šifra.

Prvi korak pri uporabi ADFGX šifre je naključna razporeditev črk v kvadrat, ki ga vodoravno in navpično označimo z črkami ADFGX.

Slika 4.1: ADFGX kvadrat

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

Tako za vsako črko dobimo dvočrkovne kombinacije, ki označujejo vsako črko odprtega besedila. (npr. a=FX, b=DX itd.) Razlog za uporabo teh petih črk je ta, da v Morsejevi abecedi zvenijo zelo različno, zato je možnost za napako telegrafista majhna.

Besedilo ZMAGA JE BLIZU, zveni tako: AD XD FX DA AX FG DX DD AX AD GF.

Nadalje uporabimo ključno besedo in črke skritega besedila zapišemo v vrstice pod njo. To je prvi, substitucijski korak šifre.

Slika 4.2: ADFGX kvadrat – substitucija

G	E	S	L	O
A	D	X	D	F
X	D	A	A	X
F	G	D	X	D
D	A	X	A	D
G	F			

Nato črke ključa razvrstimo po abecednem vrstnem redu in temu primerno preuredimo stolpce kvadrata, torej izvedemo transpozicijo.

Slika 4.3: ADFGX kvadrat – transpozicija

E	G	L	O	S
D	A	D	F	X
D	X	A	X	A
G	F	X	D	D
A	D	A	D	X
F	G			

Skrito besedilo nato zveni tako: DADFXDXAXAGFXDDADADXFG.
(Goebel, 2012)

5 Obveščevalna dejavnost v času prve svetovne vojne

Ob izbruhu vojne je bilo na voljo veliko različnih načinov komunikacije med vojaškimi enotami. Starejši sistemi, kot npr. prenašanje sporočil z golobi ali sli, so se uporabljali skupaj z novimi tehnologijami – telefonom in radijem. Na kopnem so za komunikacijo med enotami in s poveljstvom uporabljali telegrafske kable in brezžične radie. Prvi so bili ranljivi zaradi bombardiranja, drugi zaradi prisluškovanja. Vendar je bil zaradi hitrosti prenosa sporočil v primerjavi z uporabo slov, ta način komunikacije najpogosteje uporabljen. Na morju so častniki za zveze za komunikacije na krajših razdaljah uporabljali

zastave, za daljše razdalje pa so se morali obrniti na bolj ranljivi brezžični telegraf. V času prve svetovne vojne so se letala razvila iz osnovnih modelov v prave vojaške stroje – bombnike in lovce, skupaj z njimi pa tudi njihove oblike komunikacije. Na začetku vojne so se piloti med seboj sporazumevali tako, da so premikali krila in zakrilca, do konca vojne pa so bili vsi opremljeni z radijem in so lahko komunicirali med sabo in s telegrafskimi postajami na kopnem. Piloti so brezžične komunikacije uporabljali predvsem za to, da so artilerijskim enotam na tleh sporočali položaje nasprotnikovih enot, tako da so lahko natančneje obstreljevale nasprotnika, ko niso imeli direktnega pogleda na njega (Bruton 2016).

Radio je tako postal ključen element v strategiji prve svetovne vojne. Nemci so takoj osvojili nov način komunikacije in opremili vse vojaške štabe in konjeniške enote z brezžičnimi seti. Statična vojna na zahodni fronti jim je omogočila postavitev večjih brezžičnih postaj, na drugi strani pa jim je britanska morska blokada in posledično pomanjkanje bakra onemogočila izdelavo telefonskih kablov. Na drugi strani pa so Britanci le počasi sprejemali takšen način komuniciranja. Na začetku vojne so se bolj zanašali na telefonske kable ter zastave, luči in heliografe. V zadnjih dveh letih vojne so Britanci močneje investirali v brezžične telegrafe in od sredine leta 1917 so večinoma komunicirali na tak način (Tworek 2016).

Nobena izmed velesil, ki so vstopile v Veliko vojno, ni bila dobro pripravljena nanjo. O obveščevalni dejavnosti so še vedno razmišljali kot v času francosko-pruske vojne, kjer so bili glavni aduti obveščevalne dejavnosti vohuni, ne pa prestrezanje nasprotnikovih sporočil, ki jih je omogočil telegraf (Stout 2014, 35).

Količina tako prestreženih sporočil je povzdignila pomembnost kriptoanalize. Pred tem je bila količina prestreženih sporočil majhna, za uspešno kriptoanalizo pa je potrebna večja količina podatkov. Tako so vojaški poveljniki in politiki spoznali vrednost kriptoalitskih enot in jih ob izbruhu vojne močno razširili ali šele na novo ustanavljali (Kahn 1996, 299) .

Spremenil se je celoten koncept obveščevalne dejavnosti. Večino je sicer še vedno obsegalo fizično opazovanje sovražnikovih sil, predvsem ob frontni liniji v Belgiji, kjer so agenti budno spremljali železniški sistem, ki je bil glavni način transporta sovražnikovih sil. Povečala se je tudi količina pridobljenih podatkov s strani vohunov znotraj nasprotnikovega birokratskega ali vojaškega sistema. Novost prve svetovne vojne je bilo izvidništvo iz zraka. Že obstoječim izvidniškim balonom so se pridružila izvidniška letala. Do konca vojne so bila opremljena s kamerami in radiji (Stout 2014, 36).

Na fronti zbrane informacije so prinašale zgolj lokalne in začasne prednosti pred nasprotnikom, medtem ko so bile informacije o vojaških zmogljivostih in strateških načrtih

ključnega pomena, posledično so bili vohuni v nasprotnikovih vrstah zelo dragoceni. Zavezniki so svojo vohunsko mrežo dobro razvili v zasedenih območjih Belgije in Nizozemske, nikoli pa v sami Nemčiji. Na drugi strani so nemški vohuni na zahodni fronti delovali na tujih teritorijih in zato običajno samostojno, brez podpore večje vohunske združbe. Na vzhodni fronti pa so Nemci rekrutirali pripadnike etničnih manjšin na Poljskem in v baltskih državah, kjer so gojili sovraštvo do Rusije. V Veliki Britaniji so Nemci dosegli le malo vohunskega uspeha, z izjemo vohuna Julesa Crawforda Silberja, ki se je vtihotapil v službo za cenzuro znotraj Vojnega ministrstva (Debruyne 2016).

Največji korak v okviru obveščevalne dejavnosti je bil storjen v t.i. tehničnem zbiranju podatkov – prestrezanju nasprotnikovih radijskih sporočil zapisanih v Morsejevi abecedi. Radio je bil hitro po svojem izumu leta 1895 uporabljen kot instrument vojne, saj je prinesel veliko prednost: takojšnji in neprekinjen nadzor enega samega poveljnika nad celotno vojsko. S tem, ko je odstranil potrebo po žični povezavi, je radio pospešil komunikacijo med enotami ter jo vzpostavil tam, kjer do tedaj ni bila mogoča zaradi razdalje, terena, hitrega premikanja ali prisotnosti sovražnikovih enot. Sedaj je bila komunikacija mogoča tudi z mornariškimi ali zračnimi silami. Vendar je vse to prineslo tudi veliko pomanjkljivosti. Za prestreganje nasprotnikovih sporočil ni bil več potreben fizični dostop do telegrafske linije nekje za sovražnikovo linijo, ampak je bilo potrebno le nastaviti svoj radio na isto frekvenco kot je bila sovražnikova (Kahn 1996, 298).

Ob izbruhu vojne so imeli Britanci le eno postajo za prestrezanje brezžičnega prometa v Stocktonu. Kmalu po začetku vojne sta dva amaterska navdušenca nad brezžično telegrafijo poročala, da lahko na njunih brezžičnih setih prestrezata nemška sporočila in ponudila svoje usluge. Prav tako na lastno pobudo, je brezžični promet spremljalo in predajalo sporočila podjetje Marconi. Kmalu so se Britanci organizirali in začeli prestrezati brezžični promet tudi na drugih postajah, npr. na sedežu Kraljeve mornarice v Londonu in na ladjah Kraljeve mornarice (Gannon 2010, 75).

To verigo prestreznih postaj so imenovali Y postaje. Tako so imeli Britanci že nekaj tednov po začetku vojne dostop do vse nemške brezžične komunikacije. Podatki, pridobljeni iz Y postaj, so bili zelo dragoceni. Med drugim so pokazali, da je bila potopitev Lusitanie leta 1915, kljub uradnem zanikanju, odobrena s strani nemškega generalštaba (Wander 2016).

Tudi Nemci so imeli svoje prestrezne postaje. Prvi večji uspeh so dosegli že leta 1914, ko so s prestrezanjem ruskih sporočil dosegli odločilno zmago pri Tannenbergu in tako preprečiti rusko napredovanje proti zahodu. Ruska vojska je uporabljala brezžične telegrafe za koordinacijo svojega napada, svojih komunikacij pa niso zavarovali. Nemški prestrezni

postaji v Thornu in Königsbergu sta poskrbeli za to, da so bili Nemci o vseh premikih obveščeni istočasno kot same ruske enote. Ta primer je Nemcem pokazal, kako pomembne so lahko prestrežene informacije, zato so postavili več prestreznih postaj na vseh frontah (Lee 2016).

Na drugi strani so Francozi povzdignili prestrezanje na še višjo raven. Z mrežo visokih stavb, vključno z Eifflovim stolpom, so lahko zaznali oddajanje tudi manjših nemški postaj – tistih, ki jih je imela vsaka enota. Tako pa niso pridobivali zgolj sporočil, ki jih je bilo potrebno še kriptoanalizirati, ampak so s pomočjo triangulacije določali položaje teh postaj in tako odkrivali lokacije in premike posameznih bojnih enot. V ta namen so ustanovili poseben oddelek, 8e Regiment de Transmissions s sedežem pod Eifflovim stolpom (Wander 2016).

Že ob izbruhu vojne so imeli Francozi 8 prestreznih postaj, njihovo število pa je nato še naraslo. Država je bil razdeljena v tri cone okrog Pariza Lyona in Bordeauxa, vse postaje pa so bile povezane z Vojnim ministrstvom v Parizu. Francozi so tako sprejemali nemška sporočila istočasno kot nemške enote same. Francoski analitiki so beležili moč, s katero so nemške postaje oddajale in tako ocenili razdaljo. Ob veliki količini prestreženih podatkov so si ustvarili sliko o verjetnih lokacijah nemških enot, ki se je izkazala za precej točno. To je bila prva analiza radijskega prometa, ki pa so jo v času trajanja vojne Francozi še razširili. Nenadno povečanje radijskega prometa na določenem območju jih je opozorilo na približujoči napad, hkrati pa so podatki o pošiljatelju in prejemniku sporočila olajšali delo kriptoanalitikov, saj so lahko različne vojaške enote uporabljale različne kodirne knjige (Kahn 1996, 299–300).

Cilj vseh kriptoanalitski služb je bil enak, kljub temu pa so med državami obstajale velike razlike - tako v organizaciji kot v uspešnosti. V sledečih poglavjih bom predstavila obveščevalne službe posameznih držav oz. enote znotraj obveščevalne dejavnosti, ki so se ukvarjale s kriptoanalizo prestreženih podatkov.

5.1 Velika Britanija

Britanci so imeli enega izmed bolje organiziranih obveščevalnih sistemov. Kopenska vojska in mornarica sta imeli ločeni obveščevalni službi, ki pa sta medsebojno sodelovali. Obveščevalne podatke za kopensko vojsko je zagotavljala MI-1 (Military Intelligence, Section 1), obveščevalna služba znotraj Kraljeve vojne mornarice pa se je imenovala Obveščevalni oddelek Kraljeve vojne mornarice (Naval Intelligence Division, NID).

Britanska vojaška obveščevalna služba je bila ustanovljena leta 1909 v okviru Ministrstva za vojno in v letu 1916 po reorganiizaciji postala MI-1. Sestavljena je bila iz naslednjih pododdelkov:

- MI-1(a): distribucija poročil in obveščevalnih podatkov,
- MI-1(b): prestrezanje in kriptoanaliza,
- MI-1(c): tajna služba (Secret Service),
- MI-1(d): varnost komunikacij,
- MI-1(e): brezžična telegrafija,
- MI-1(f): osebje in finance ter
- MI-1(g): varnost in protiobveščevalna dejavnost

(Debruyne 2016).

Za nas zanimiv je pododdelek C, kjer so delovali kriptologi. Poveljstvo MI1b je bilo na sedežu Britanskih ekspedicijskih sil, posamezni kriptoanalitki pa so bili priključeni raznim delom vojske. Vse do konca leta 1915 je bila MI1b majhna enota, dokler je ni prevzel Malcom Vivian Hay in začel iskati mlade talente in tako do konca vojne povečal število zaposlenih iz 4 na 84. Na začetku vojne so Francozi Britancem posredovali ključe in tehniko, kako se lotiti nemških šifer in kmalu so britanski obveščevalci zalagali vojaško poveljstvo s koristnimi informacijami (Kahn 1996, 310).

Na drugi strani je imela tudi Kraljeva vojna mornarica svojo obveščevalno službo in znotraj nje kriptološki oddelek, znan pod imenom Soba 40. Legenda o Sobi 40 se je začela, ko je Admiral Oliver, direktor Obveščevalnega oddelka Kraljeve vojne mornarice (NID) predal zasežene nemške kodirne knjige Alfredu Ewingu, vodji izobraževanja Kraljeve vojne mornarice in ga namestil v Sobo 40 na sedežu Admiralitete v Londonu. Ewing, ki se je do takrat s šiframi in kodami ukvarjal zgolj ljubiteljsko, je rekrutiral druge talente, med njimi večino lingvistov in matematikov (Gannon 2010, 27).

Obe kriptografski službi sta delali skupaj. Oblikovali sta 4 delovne pare, enega strokovnjaka za kriptografijo in drugega za nemški jezik. Trije pari so pokrivali dan v 8 urnih izmenah, četrti par pa je prevzel izmeno ob prostih dneh. Svoje delo so koncentrirali na terenske šifre, ki so jih Nemci uporabljali na zahodni fronti. To se jim je obrestovalo že oktobra 1914, ko so zlomili nemško dvojno transpozicijsko šifro in odkrili pripadajoči ključ ter tako postavili trdno osnovo za nadaljnje delo (Gannon 2010, 35–36) .

5.2 Francija

Francozi so imeli največ izkušenj s svojim nasprotnikom, saj se je fracosko-pruska vojna končala le dobrih 40 let pred začetkom prve svetovne vojne in obdobje nezaupanja med državama se je ohranilo tudi v tem času. Francozi so bili tako glede poznavanja nasprotnika in zbiranja obveščevalnih podatkov o njem najbolj pripravljeni.

Francozi so vojaško obveščevalno službo (Deuxieme Bureau) ustanovili po francosko-pruski vojni leta 1871, vendar so jo leta 1899 razpustili. Leta 1907 so jo ponovno aktivirali v okviru Generalštaba. Znotraj nje je delovala Služba za šifriranje (Service du Chiffre) z okoli 15 zaposlenimi (Richelson 1997, 32).

Njena glavna naloga je bila razkrivanje nemških sporočil, običajno s postopki in ključi, ki so jim jih posredovali iz Urada za šifriranje v Parizu. Naprej se je Služba za šifriranje delila na posamezne kriptografske pisarne, ki so bile priključene raznim vojaškim poveljstvom in so sodelovale z obveščevalnimi oddelki teh vojaških poveljstev. Običajno so jih sestavljali eden do treh uslužbencev, ker pa so bili podrejeni enemu viru, so med seboj odlično sodelovali in se sproti obveščali o vsakem napredku (Kahn 1996, 305–306).

Francoski kriptografi so bili med vsemi najbolj napredni. Že pred izbruhom vojne so imeli 5 kriptoanalitičnih skupin, ko se je vojna začela pa so v okviru Ministrstva za vojno ustanovili Bureau du Chiffre – Urad za šifriranje. Služba je bila najprej skoncentrirana na skrbno zbiranje in analizo prestreženih sporočil: od kod so bila poslana in kam, ob kateri uri, kako pogosto. Iz zbranih informacij so nato sklepali, kako je sestavljena nemška armada. Kljub temu, da je imelo pred izbruhom vojne radijski set le nekaj nemških enot, so le-te proizvedle veliko brezžičnega prometa, kar je Francozom pomagalo pri analizi prometa. Urad za šifriranje je imel sedež na vojnem ministrstvu v Parizu in je zaposloval več deset ljudi, vendar jih je bilo le okoli 10 kriptoanalitikov (Goebel 2012).

Večji kriptografski preboj se je zgodil v začetku septembra 1914. Francozi so prestregli odprto besedilo »Kje je Circourt?«, ki se je nanašalo na prejšnje, zašifrirano sporočilo. Tako so francoski kriptoanalitiki v šifriranem besedilu začeli iskati besedo Circourt in po mnogih neuspelih poskusih so v začetku oktobra razvozlali celotno šifro. Ko so sredi oktobra Nemci menjali ključ, so Francozi potrebovali 4 dni, da so ga razvozlali, ob novi menjavi v začetku -novembra, le še tri dni, naslednjič pa samo še en dan. Zasluge za ta preboj gre pripisati temu, da so Francozi uspeli zaseči nekatere pomembne nemške dokumente, med drugim Navodila za uporabo šifer za nemško vojsko. Tako so izvedeli, da Nemci uporabljajo preprosto transpozicijsko metodo, kar pomeni, da se dejanske črke odprtega besedila skrivajo

nekje v šifriranem sporočilu. Tako so lahko ugibali besede, ki se zelo verjetno pojavijo v besedilu npr. Circourt, meteorološka terminologija ali ime enote, ki ji je sporočilo namenjeno (Ganon 2010, 34-36).

Francoski kriptoanalitiki so bili torej uspešni pri svojem delu že od začetka vojne, vendar so svojo največjo zvezdo odkrili marca 1915, ko je poveljnik 6. armade general Michel-Joseph Maunoury premestil poročnika Georgesa Painvina v Urad za šifriranje. Mlad poročnik, pred vojno profesor paleontologije na pariški univerzi, se je izkazal za genija in je že ob prostih popoldnevih na fronti uspešno kriptoanaliziral prestrežena nemška sporočila (Kahn 1996: 304–305).

5.3 Nemčija

Nemci so imeli zelo dobro organizirano obveščevalno skupnost, sestavljeno iz vohunov in informatorjev razporejenih po celi Evropi, Severni Afriki, bližnjem vzhodu in Združenih državah Amerike. Uspešno so se infiltrirali in prisluškovali mnogim tujim vladnim organizacijam.

Nemška vojaška obveščevalna služba (Nachrichtendienst) je bila ustanovljena med francosko-prusko vojno leta 1870/71, vendar je svojo dejavnost nadaljevala tudi po vojni, v času prve svetovne vojne pa je prerasla v velikansko obveščevalno službo. Vendar pa je bila njena naloga zgolj zbiranje informacij, njihovo nadaljnjo analizo pa so prevzeli različni oddelki znotraj generalštaba (Abteilungen), ki so bili specializirani za posamezne države (Foley 2005, 3-4).

Glavnino obveščevalnih podatkov je predelal Abteilung IIIb, ustanovljen leta 1889. Del službe se je ukvarjal z Francijo, drugi del z Rusijo, Veliko Britanijo pa so prepustili obveščevalni službi vojaške mornarice – Nachrichten Abteilung. Abteilung IIIb je vodil polkovnik Walter Nicolai in po njegovih podatkih je organizacija na svojem višku leta 1918 zaposlovala kar 1000 ljudi (Debruyne, 2016).

Nemčija je kljub temu, da je imela dobro organizirano obveščevalno dejavnost, v vojno vstopila brez kriptoanalitske službe. To je potrebno deloma pripisati temu, da so imeli Francozi na lastnem ozemlju na voljo telegrafske napeljave (vsaj tiste, ki jih niso uničili pred napredujočimi Nemci) in so zato zmanjšali brezžično komunikacijo na minimum. Nemci tako niso imeli čemu prisluškovati (Singh 2008, 139).

V nadaljevanju vojne so tudi Francozi začeli pogosteje uporabljati radijske prenose. Nemci so tako dobili svojo priložnost, zato so leta 1916 znotraj Generalštaba kopenske vojske

ustanovili Službo za prestrezanje (Abhorchdienst), ki je imela svoj sedež blizu Neumünstra. Tam so nemški kriptoanalitiki v roku enega dne razbijali francoske šifre (Kahn 1996, 313–314).

Nemška mornarica je imela svojo obveščevalno službo – Nachrichten-Abteilung. Spadala je pod admiralski štab v Berlinu. Služba je imela več pododdelkov: NI (zbiranje informacij v tujini), G (protiobveščevalni oddelek), NIV (sabotaža). Mornariška obveščevalna služba je bila manjša od obveščevalne službe kopenske vojske Abteilung IIIb, prav tako ni imela stalnih zaposlenih, saj je vsak oddelal le nekaj let in se nato vrnil na svoje redno delovno mesto, običajno znotraj mornarice. V času vojne so se menjali kar trije direktorji (Boghardt 2004, 15–16).

5.4 Avstro-Ogrska

Avstro-Ogrska obveščevalna dejavnost je bila v skladu s političnimi interesi države skoncentrirana na vzhod proti Rusiji in Balkanu. Glavni adut obveščevalne skupnosti pred vojno so bili vohuni znotraj tujih vlad, ob izbruhu vojne pa so primarni vir informacij postala prestrežena radijska sporočila.

Avstro-Ogrska je svojo Vojaško obveščevalno službo (Evidenzbureau) ustanovila leta 1850, kot prva med evropskimi velesilami. Najprej je spadala pod Zunanje ministrstvo, ob izbruhu prve svetovne vojne pa so jo premestili pod okrilje Generalštaba. Tudi ta obveščevalna služba je bila organizirana podobno kot v drugih evropskih velesilah, kjer so se ločeni oddelki ukvarjali s posameznimi državami. V primeru Avstro-Ogrske je bil največji oddelek namenjen Rusiji (Debruyne, 2015).

Vojaška obveščevalna služba je imela odličen Kriptoanalitski oddelek (Chiffregruppe), ki so ga ustanovili leta 1911 in ga je v času prve svetovne vojne vodil Maximilian Ronge. Že septembra 1914 je ta oddelek uspešno razbijal ruske kode, tako da so ob vstopu Italije v vojno dobro obvladali svoje delo in so jim italijanske kode povzročale le malo težav (Debruyne, 2015).

Že 13 dni po napovedi vojne, so Avstrijci zlomili italijansko šifro. Italijani so uporabljali t.i. cifrario rosso (rdečo šifro), katero so avstrijski vohuni kupili od Italijanov že pred vojno. Tako so imeli dober vpogled v delovanje šifre, zato jim tudi sprememba ključa ni povzročala prevelikih težav (Kahn 1996, 319).

Avstrijski kriptoanalitiki so bili zaslužni za velik del uspešnosti njihove obveščevalne službe. Zato se je leta 1917 organizacija razširila. Obveščevalna služba je sedaj imela dva

oddelka. Kriptoanalitski oddelek I (Chiffrenguppe I) je vodil stotnik de Carlo, kriptoanaltiski oddelek II (Chiffrenguppe II) pa stotnik Imme (Kahn 1996, 317–318).

Najboljši in najbolj odlikovan avstro-ogrski kriptoanalitik je bil Hermann Pokorny, ki je zlomil skoraj vse ruske šifre od septembra 1914 do marca 1916 in tako pomagal avstro-ogrskim silam odbiti mnoge večje napade ruske vojske (Adams 2009, 349).

5.5 Združene države Amerike

Do izbruha prve svetovne vojne se je obveščevalna dejavnost v Združenih državah zaradi proračunskih omejitev in reorganizacije vojske skrčila na minimum. Zunanje ministrstvo je v manjši meri začelo zbirati podatke o centralnih silah v letu 1916, vendar so ameriški obveščevalci dobili potreben denar in osebje šele po vstopu Amerike v vojno leta 1917. Tega leta so znotraj kopenske vojske ustanovili Vojaško obveščevalno sekcijo - Military Intelligence Section. Ob ustanovitvi je ta organizacija premogla vodjo, Ralpha Van Demana, 3 častnike in dva tajnika, do konca vojne pa je zaposlovala 282 častnikov in 948 civilistov. Po zgledu britanske obveščevalne službe je bila tudi ameriška organizirana v oddelke od MI-1 do MI-12 (Finley ur. 1995, 80).

V predvojnem obdobju in na začetku vojne so se v Ameriki s kriptologijo ukvarjali časniki Šole za zveze iz Leavenwortha v Kansasu. Med njimi je izstopal stotnik Parker Hitt, ki je uspešno kriptoanaliziral mehiške šifre in napisal priročnik za reševanje vojaških šifer, ki je razložil kriptoanalizo standardnih šifer, tako monoalfabetskih kot tudi polialfabetskih, transpozicije in substitucije ter podal praktične primere za reševanje. V priročniku je priporočal dodajanje kriptografskih oddelkov vojaškim enotam ter njihovo organizacijo. Ob izbruhu vojne so ta priročnik uporabljali za izobraževanje bodočih kriptografov (Kahn 1996, 321–324).

Vodja novoustanovljene 8. enote Vojaške obveščevalne sekcije MI-8 je bil Herbert Yardley. Svoje delo je začel že pred vojno in sicer tako, da je opozoril na napake diplomatske šifre, ki so jo v tem obdobju uporabljali Američani. Njegova prva naloga ob ustanovitvi MI-8 je bila izučiti večje število kriptoanalitikov, ki bi lahko obdelovali takšno količino podatkov, kot je prehajala skozi njihove roke. V ta namen so mu zavezniki Britanci in Francozi posredovali praktične primere nemških šifer ter način njihovega reševanja.

MI-8 je v kratkem času prerasel v veliko organizacijo, sestavljeno iz 5 oddelkov:

- sestava kod in šifer (Code and Cipher Compilation),
- zveze (Communications),

- stenografski oddelek (Shorthand),
- laboratorij za prikrite pisave (Secret-Ink Laboratory),
- reševanje kod in šifer (Code and Cipher Solution)

(Yardley 1998, 46–47).

Po prihodu Ameriških ekspedicijskih sil v Evropo, spomladi 1917, so bili kriptologi organizirani po naslednjem ključu: kriptografi - torej uporabniki kod in šifer, so spadali pod okrilje Korpusa za zveze, pripravljanje in izdajanje kod in šifer, pa je bilo zaupano obveščevalni službi – MI8, ki je bila zadolžena tudi za prestrezanje in kriptoanalizo sovražnikovih šifer. Tako je v praksi MI8 nadzorovala častnike za zveze. Obe skupini sta tesno sodelovali ves čas vojne, kar je bila velika prednost (Kahn 1996, 325–326).

Začetki ameriških kriptoanalitikov so bili počasni. Njihovo urjenje je zavzemalo predvsem šifre, medtem ko so Nemci, po tem ko so se vojne linije ustalile, prešli na kode. Tako so Američani zaprosili za pomoč Francoze, ki so jim predali navodila za reševanje nemških kod in najbrž tudi rešitve kod, ki so ji imeli do tedaj. S francosko pomočjo so tudi Američani lahko dekodirali nemška sporočila. Glavna prednost ameriške obveščevalne dejavnosti so bile njihove prestrezne postaje. Radijski oddelek Korpusa za zveze je do konca vojne postavil pet prestreznih postaj, ki so prestregle ogromno nemških kodiranih sporočil. Američani pa so za razliko od drugih zaveznikov, informacije delili. Tako so prestrežena sporočila redno posredovali Francozom in Angležem. Ko so Nemci pred veliko spomladansko ofenzivo uporabili novo kodo, so jo Američani posredovali Francozom (Kahn 1996, 334–336).

6 Vpliv kriptoanalize na potek vojne

6.1 Vojna na morju

Bistvo prve svetovne vojne na morju je predstavljal trud zaveznikov, da ustvarijo morsko blokado in tako onemogočijo centralnim silam izhod na odprto morje ter na drugi strani poskuse centralnih sil, da to blokado prebijejo.

Že na začetku vojne se je na področju prestrezanja dokumentov zaveznikom nasmehnila sreča. 11. avgusta 1914 so se pripadniki Kraljeve avstralske mornarice v civilu vkrcali na nemško trgovsko ladjo in zasegli kodirno knjigo HVB (Handelsschiffsverkehrbuch). Avstralci so jo cel mesec zadržali zase, preden so jo končno

posredovali Britancem. Konec avgusta se je nemška ladja Magdeburg v Baltskem morju ob gosti megli ločila od flote in nasedla na čeri, kjer so jo čez nekaj ur našle ruske ladje in jo potopile. Pri tem so zasegli tri izvode kodirne knjige nemške vojne mornarice SKM (Signalbuch der Kaiserlichen Marine) in enega izmed njih predali Britancem. Tretja kodirna knjiga VB (Verkerhrsbuch) je prišla v roke Britancem konec leta 1914. Uradna zgodba pravi, da je angleški vlačilec po naključju z dna morja ob danski obali potegnil svinčeno skrinjo, v kateri se je med drugim skrivala kodirna knjiga (Gannon 2010, 37–40).

Do konca leta 1914 so torej imeli Britanci v rokah vse tri kodirne knjige, ki jih je uporabljala nemška mornarica. Kodirne knjige so delovale na zelo preprostem principu. V njih je bil seznam besed v abecednem vrstnem redu in pripadajoča koda, sestavljena iz treh črk. Pomanjkljivost nemških kodirnih knjig je bila ta, da so bile tudi kode podane v abecednem vrstnem redu, kar pomeni, da če vemo da ATW pomeni vojska, in ATY vojaška skupina, lahko sklepamo, da bo tudi koda ATX pomenila neko besedno zvezo, ki se začne z »vojaški«. Naslednja velika pomanjkljivost vseh treh kodirnih knjig je bila ta, da je imela vsaka beseda oz. besedna zveza zgolj eno kodo, kar pomeni, da so lahko kriptoanalitiki uporabili frekvenčno analizo. Besede, za katere so sklepali, da se pojavljajo najpogosteje, npr. imena ladij in vojaških enot, imena krajev itd., so primerjali z najpogosteje uporabljenimi kodami in tako poiskali rešitev (Gannon 2010, 48–56).

Britanci so tako že po nekaj mesecih vojne brez težav brali sporočila nemške mornarice in zato noben njihov napad ne bi smel biti presenečenje. Kljub temu so večkrat naleteli na težave, saj pridobljeni podatki niso bili posredovani v celoti, včasih jih poveljniki niso pravilno razumeli ali pa v celoti ignorirali, saj niso zaupali kriptoanalitikom v Sobi 40.

Prvi takšen primer je bila bitka pri Coronelu ob obali Čila. Oddajanje radijskih signalov je obema stranema razkrilo prisotnost nasprotnika. Nemški poveljnik von Spee je dobil dodatno poročilo od nemške trgovske ladje in je točno vedel, koliko ladij se mu približuje, na drugi strani pa je sam ukazal oddajanje radijskih signalov z zgolj ene svoje ladje in tako prikril moč svoje enote. Britanski poveljnik Cradock je bil tako prepričan, da se nemška eskadrilja premika na sever proti Panamskemu prekopu. Da bi potrdil te informacije, je poslal eno izmed svojih ladij Glasgow proti Coronelu, z ostalimi pa je začel iskati tisto eno nemško ladjo, ki je oddajala signal. Med vračanjem iz Coronela je Glasgow opazila nemško eskadriljo in javila Cradocku, da so nemške sile bistveno močnejše, kot so pričakovali. Britanci so imeli možnost pobegniti in se izogniti spopadu z močnejšim nasprotnikom, vendar se je poveljnik Cradock odločil za boj. 1. novembra je prišlo do bitke in posledično prvega poraza Britanske kraljeve mornarice od leta 1812 (Keegan 2004, 124–126).

Naslednjič sta se mornarici srečali v začetku decembra 1914 v pristanišču Stanley na Falklandskih otokih. Von Spee je tja odplul z namenom napasti britansko postojanko in jim tako onemogočiti zalaganje z premogom. Podatki, ki jih je prejel, so kazali, da se v pristanišču nahaja zgolj ena britanska ladja, vendar se je do trenutka, ko je sam prispel do Falklandskih otokov, tam zasidral tudi preostanek britanske flote. Nemci so se skušali umakniti, vendar so jih Britanci zasledovali in potopili vse razen dveh nemških ladij (Keegan 2004, 140).

Nemci so poskušali meriti moči z močno britansko mornarico, vendar jim to, z izjemo bitke pri Coronelu, nikakor ni uspelo. Bistven razlog je ta, da Nemcem nikakor ni uspelo prikriti položaja svojih ladij. Stalen tok informacij, običajno v realnem času in učinkovito kroženje le-teh med Admiraliteto, lokalnimi poveljstvi in enotami na morju, so zagotovili britansko prevlado. Tudi poskusi zavajanja kot npr. radijska tišina ali oddajanje signala iz zgolj ene ladje, niso prinesli velikih rezultatov (Keegan 2004, 142).

Konec maja 1916 so v Sobi 40 prestregli načrt nemške flote, da bi zvabila britansko mornarico na odprto morje, kjer bi jo napadle nemške podmornice, kar bi omogočilo nemškim ladjam preboj skozi britansko blokado. Na podlagi te informacije je glavnina Kraljeve vojne mornarice zaplula Nemcem naproti. Poveljnik glavne nemške ladje viceadmiral Reinhard Scheer je kot poskus zavajanja nasprotnika ukazal, naj klicni znak njegove ladje DK javljajo iz pristanišča v Vilhelmshavenu. Ko je poveljnik britanske flote admiral Joe Jellicoe v Sobo 40 povprašal, kje se nahaja glavna ladja nemške flote, so mu, kljub temu, da je bila to znana taktika zavajanja, odgovorili, da se nahaja v pristanišču. Okrog dveh popoldne sta se floti srečali sredi Severnega morja, kar je presenetilo britanskega poveljnika in zamajalo njegovo zaupanje v lastno obveščevalno službo. Floti sta se spopadli v največji pomorski bitki prve svetovne vojne – bitki pri Jutlandu. Le-ta je razkrila velike obveščevalne pomanjkljivosti, predvsem slabo komunikacijo med tistimi, ki zagotavljajo obveščevalne podatke – analitiki v Sobi 40 in tistim, ki jim ti podatki koristijo – v primeru bitke pri Jutlandu admiral Jellicoe. V Sobi 40 so imeli podatke o lokaciji nemških ladij ter njihovi smeri, vendar teh podatkov niso posredovali naprej (Kahn 1996, 272–273).

Admiral Jellicoe je po tej obveščevalni katastrofi zahteval, da mu posredujejo surove dekriptirane podatke, iz katerih bi potem sam izvlekel svoje zaključke, vendar so ga v Sobi 40 zavrnili (Gannon 2010, 107) .

Kljub temu, da so Britanci utrpeli večje izgube, so bili Nemci tisti, ki so se naposled umaknili, saj jim kljub elementu presenečenja ni uspelo potolči britanske flote. Zdi se, da so po tem neuspehu obupali nad idejo premoči svoje Hochseeflotte, posledično so svoje upe položili na podmorniško bojevanje (Kahn 1996, 272–273).

Februarja 1915 je nemška vlada sporočila, da je začela neomejeno podmorniško bojevanje. V nevarnosti so bile tako britanske trgovske ladje kot tudi ladje narodov, ki so z Britanci trgovali. Sporočilo, prestreženo 7. februarja, je razkrilo vojaško območje okoli Anglije, Škotske in Irske, v katerem je nemškim podmornicam dovoljeno potapljati, končna odločitev o tem, katero ladjo potopiti, pa je bila prepuščena poveljnikom podmornic (Gannon 2010, 100).

Nemčija je poleti 1915 dala v uporabo več podmornic in posledično potopila več ladij: junija 114, julija 86, avgusta 107 in septembra 58. Med marcem in majem je nemška podmornica potopila povprečno 10 ladij, junija in avgusta pa že 35. V Sobi 40 so beležili njihove premike, vendar so bile tako pridobljene slabo izkoriščene, saj je po bitki pri Jutlandu veljalo splošno nezaupanje v podatke, ki so jih pridobili iz Sobe 40 (Gannon 2010, 103).

Nemške podmornice so uporabljale iste štiri-črkovne kode kot njihove ladje, z dodatno transpozicijo, kar pa britanskim kriptoanalitikom ni povzročalo nobenih težav in Nemci so kmalu spoznali, da njihove kode niso varne. Avgusta 1916 so v uporabo dali novo kodo, vendar se je Britancem ponovno nasmehnila sreča in manj kot mesec dni kasneje so iz sestreljenega cepelina zasegli novo kodirno knjigo (Kahn 1996, 274).

Nemci na morju torej niso imeli možnosti. Tradicionalna prevlada Kraljeve vojne mornarice, ki je segala že v 17. stoletje, je skupaj s kriptoanalitskimi dosežki britanske obveščevalne službe, je zagotovila zmago v skoraj vsaki bitki.

Strateško gledano je bila v pomorskem bojevanju v prvi svetovni vojni odločilna uporaba radia. Pred letom 1914 so ladje iskale svoje nasprotnike znotraj svojega vidnega polja, ki jih je omejevalo tudi v komuniciranju med seboj. Sedaj pa so lahko bile informacije prenesene na neomejene razdalje v minimalnem času. Mornarice so rabile nekaj časa, da so se prilagodile novonastalim možnostim, kljub temu pa je uporaba radija za vedno spremenila vojno na morju (Keegan 2004, 143).

6.2 Zimmermanov telegram in vstop ZDA v vojno

Kriptoanaliza diplomatske pošiljke med nemškim zunanjim ministrom Arthurjem Zimmermanom in nemškim veleposlanikom v Mehiki Heinrichom von Echardtom je bil najverjetneje najpomembnejši kriptoanalitski dosežek prve svetovne vojne.

Glavna razloga, ki ju je predsednik Woodrow Wilson navedel ob vstopu v vojno, sta bila nadaljevanje neomejenega podmorniškega bojevanja s strani Nemčije in morebitna vojna z Mehiko, ki jo je Nemčija predlagala v dokumentu, ki ga poznamo kot Zimmermanov

telegram. Maja 1916 sta Nemčija in Združene države Amerike sklenili dogovor, v katerem se je Nemčija obvezala, da ne bo napadala potniških ladij in da bo ob napadu na trgovske ladje posadki dala priložnost, da se izkrca na varno. Januarja 1917 pa je poveljstvo Nemške mornarice prepričalo cesarja, da lahko ob nadaljevanju neomejenega podmorniškega bojevanja Veliko Britanijo prisili k vdaji v petih mesecih in vojna se je nadaljevala. Februarja in marca so nemške podmornice potopile več ameriških ladij, vendar predsednik Wilson kljub temu med senatorji ni dobil zadostne podpore za vstop v vojno. Marca 1917 pa je ameriški tisk razkril telegram, ki je prevesil javno mnenje in posledično pripeljal do vstopa Združenih držav Amerike v vojno (https://history.state.gov 2016).

Telegram je bil 16. januarja 1917 poslan nemškemu veleposlaniku v Washingtonu Johannu Heinrichu Bernstorffu. Prvi del telegrama je bil namenjen njemu, saj ga je obveščal o nadaljevanju neomejenega podmorniškega bojevanja, ki ga je Nemčija zaradi diplomatskih pritiskov Združenih držav prekinila. Drugi del telegrama je moral Bernstroff posredovati nemškemu veleposlaniku v Mehiki Von Eckhartdu. Ta del je vseboval navodila veleposlaniku, naj v primeru vojne z ZDA predlaga mehiškemu predsedniku zavezništvo med državama. Mehika bi v zameno za vstop v vojno in pridobitev Japonske na nemško stran pridobila nazaj svoja izgubljena ozemlja Novo Mehiko, Arizono in Teksas (Gannon 2010, 195–196).

Nemci so v tem času za svoja diplomatska sporočila uporabljali dve kodirni knjigi: 13040 in 7500. Slednjo so dostavili svojemu veleposlaniku v ZDA novembra 2016, torej je bila v času pošiljanja Zimmermanovega telegrama relativno nova. Celoten telegram so iz nemškega zunanjega ministrstva v Washington poslali z uporabo kodirne knjige 7500, del, ki je bil namenjen v Mehiko pa je moral Bernstroff zakodirati s pomočjo kodirne knjige 13040, saj von Ekhardt še ni imel nove kodirne knjige 7500 (Gannon 2010, 196–197).

Vsa čezoceanska sporočila, ki so potovala preko podmorskih kablov, so zaradi njihove razporeditve morala preko Londona. Tako so imeli Britanci kopijo Zimmermanovega telegrama preden je le-ta prispel do Bernstroffa. Njihovi kriptoanalitiki v Sobi 40 so se tako z njim začeli ukvarjati že 17. januarja zgodaj zjutraj in ga kmalu delno kriptoanalizirali, vendar ne dovolj, da bi informacije posredovali Američanom. Jasno pa je bilo, da je potrebno del telegrama posredovati naprej v Mehiko. Zato so pridobili tudi to kopijo, ki pa je bila zakodirana s starejšo kodo 13040, s katero so se v Sobi 40 ukvarjali že dlje časa in so uganili že približno polovico kodirnih besed (Kahn 1996, 287–288).

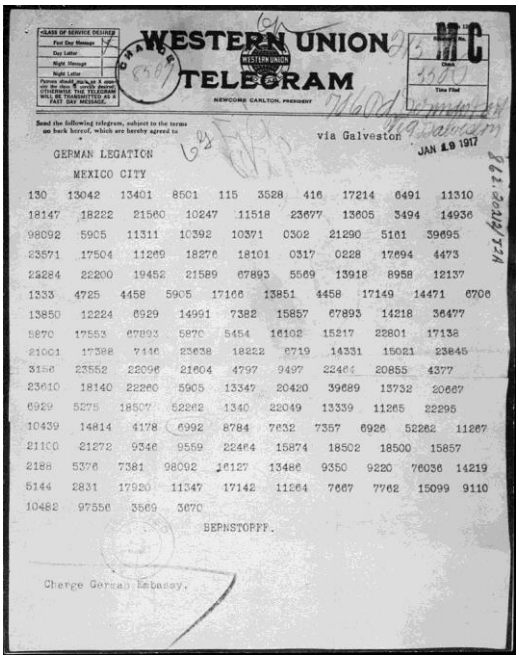
Britanci so takoj ugotovili, da imajo v rokah propagandni material velikih vojških razsežnosti. Razkritje telegrama bi zagotovo potegnilo Združene države Amerike v vojno, kar

je bil močan razlog za njegovo razkritje. Po drugi strani pa bi Britanci z razkritjem telegrama razkrili tudi njihovo največjo skrivnost – sposobnost kriptoanalize nemških sporočil. Najti so morali način, kako posredovati telegram Američanom, ne da bi pri tem razkrili sposobnosti svoje kriptoanalitske službe. Lahko bi trdili, da je bilo odprto besedilo telegrama ukradeno, vendar bi lahko Nemci kljub temu posumili na prevaro, zamenjali svoje kode in britanski kriptoanalitiki bi morali začeti znova. Dober razlog proti razkritju je bil tudi ta, da so bili odnosi med Združenimi državami Amerike in Nemčijo že tako slabi zaradi podmorniškega bojevanja in morda razkritje telegrama niti ne bi bilo potrebno. Tako je Velika Britanija čakala z razkritjem telegrama, med tem pa so se kriptoanalitiki lotili razkrivanja še preostalih besed telegrama (Kahn 1996, 287–288).

Sedaj so lahko prebrali celotno sporočilo, ki se je glasilo:

> *Telegram iz Zunanjega ministrstva z dne 16. januar št. 1. Strogo tajno, dešifrirajte sami. 1. februarja nameravamo začeti neomejeno podmorniško bojevanje. Kljub temu se bomo trudili preprečiti vstop Združenih držav Amerike v vojno. V primeru, da to ne uspe, želimo Mehiki ponuditi zavezništvo z naslednjimi pogoji: skupaj gremo v vojno, skupaj sklenemo mir. Izdatna finančna in druga pomoč, da si Mehika povrne izgubljena ozemlja Teksas, Novo Mehiko in Arizono. Predsednika obvestite o tem v skrajni tajnosti takoj ko bo izbruh vojne z ZDA neizbežen. Predlagajte tudi pridružitev Japonske naši strani in posredovanje Mehike med Japonsko in nami. Opomnite predsednika, da bomo lahko z neusmiljenim podmorniškim bojevanjem v nekaj mesecih prisilili Veliko Britanijo k podpisu miru. Potrdite sprejem. Zimmerman* (Gannon 2010, 206).

Slika 6.1: Zimmermanov telegram



WESTERN UNION TELEGRAM

NEWCOMB CARLTON, PRESIDENT

Send the following telegram, subject to the terms on back hereof, which are hereby agreed to

via Galveston

JAN 19 1917

GERMAN LEGATION
MEXICO CITY

130 13042 13401 8501 115 3528 416 17214 6491 11310
18147 18222 21560 10247 11518 23677 13605 3494 14936
98092 5905 11311 10392 10371 0302 21290 5161 39695
23571 17504 11269 18276 18101 0317 0228 17694 4473
25284 22200 19452 21589 67893 5569 13918 8958 12137
1333 4725 4458 5905 17166 13851 4458 17149 14471 6706
13850 12224 6929 14991 7382 15857 67893 14218 36477
5870 17553 67893 5870 5454 16102 15217 22801 17138
21001 17388 7116 23638 18222 6719 14331 15021 23845
3156 23552 22096 21604 4797 9497 22464 20855 4377
23610 18140 22260 5905 13347 20420 39689 13732 20667
6929 5275 18507 52262 1340 22049 13339 11265 22295
10439 14814 4178 6992 8784 7632 7357 6926 52262 11267
21100 21272 9346 9559 22464 15874 18502 18500 15857
2188 5376 7381 98092 16127 13486 9350 9220 76036 14219
5144 2831 17920 11347 17142 11264 7667 7762 15099 9110
10482 97556 3569 3670

BEPNSTOPFF.

Charge German Embassy.

Vir: Neiberg (2016)

Vojna na zahodni fronti je divjala še naprej, cela generacija mladih fantov je izgubila svoje življenje, ameriškega vstopa v vojno ni bilo na vidiku, Britanci pa so še vedno sedeli na pomembni informaciji, ki bi lahko vse to spremenila. 22. februarja so se končno zganili. Vodja Sobe 40 Hall je z dovoljenjem Zunanjega ministrstva posredoval Zimmermanov telegram Edwardu Bellu, sekretarju na ameriškem veleposlaništvu, ki sprva sam ni hotel verjeti povedanemu, saj se mu je zdelo nemogoče, da bi bili Nemci tako nespametni, da bi ponujali dele ameriškega ozemlja tretji državi (Kahn 1996, 291).

Odločili so se, da bodo telegram uradno predali sekretarju Bellu, ta pa bo poskušal prikriti njegov vir. Skupaj z Zimmermanovim je v Ameriko je poslal naslednji telegram:

> *Zgodaj v vojni je Britanska vlada pridobila kopijo nemških kod, ki so bile uporabljene v zgornjem sporočilu. Pridobili so kopijo Bernstorffovega telegrama namenjenega v Mehiko in ga dešifrirali. To pojasni, kako so dešifrirali telegram in zakaj so potrebovali mesec dni za njegovo posredovanje. Gre za njihovo ljubosumno varovano skrivnost, ki jo sedaj razkrivajo zaradi pomembnosti vsebine telegrama in zaradi prijateljskih nagnjenj, ki jih gojijo do Združenih držav Amerike. Britanska vlada iskreno prosi, da prikrijete vir teh informacij in kako so Britanci prišli do njih, nimajo pa nobenih zadržkov glede posredovanja vsebine telegrama ameriški javnosti* (Kahn 1996, 292–293).

Ko so o telegramu obvestili predsednika Wilsona, je poslal svoje kriptoanalitike v Sobo 40, da preverijo avtentičnost telegrama. Zimmermanov telegram so ameriški časopisi objavili 1. marca in po pričakovanjih je sprožil val ogorčenja. Potencialno zavezništvo Nemčije, Mehike in Japonske je bilo za Američane prava nočna mora in časopisni komentatorji so telegram enačili z napovedjo vojne. Kljub temu nekateri niso verjeli, da je telegram pristen in vnela se je napeta javna debata, vendar je njegov kabinet, ki ga je predsednik Wilson zbral 20. marca, enoglasno podprl vojno. 2. aprila jo je podprl Kongres, dva dni kasneje pa še Senat (Neiberg, 2016).

O tem, kako so Američani pridobili Zimmermanov telegram, je krožilo veliko zgodb. Po eni bi naj ameriški vojaki pridobili telegram, ko ga je nemški vohun skušal pretihotapiti preko meje z Mehiko. Druga zgodba je navajala, da so ga našli med Bernstorffovimi stvarmi, ki so jih preiskali na meji, ko je le-ta potoval v Mehiko. Medtem pa je britanski tisk napadal nesposobnost lastne vlade, da pridobi tako pomemben dokument in hvalil nadvlado ameriških obveščevalcev nad lastnimi. Tudi Nemci so se spraševali, kako so Američani pridobili tako pomemben in po njihovem mnenju dobro zavarovan dokument. Notranja preiskava je pokazala, da je bil telegram pridobljen iz nemškega veleposlaništva v Mehiki – zanka, ki jo je tako dobro nastavil Hall (Kahn 1996, 294).

Sedaj so bile sveže ameriške čete pripravljene, da okrepijo jarke zahodne fronte in pomagajo izčrpanim zaveznikom. Kriptoanalitski uspeh Sobe 40 je obrnil tehnico, pripeljal Združene države Amerike v vojno in omogočil zmago zaveznikov. Za kratek trenutek v zgodovini so krptoanalitiki držali v rokah usodo sveta, saj niti prej niti nikoli po tem, kriptoanaliza ni prinesla tako odločilnega preobrata v vojni (Kahn 1996, 297).

6.3 Nemška spomladanska ofenziva 1918

Pozimi 1917/18 je Nemčija pripravljala novo ofenzivo na zahodni fronti. Podmorniško bojevanje, ki bi naj prisililo Veliko Britanijo k podpisu miru, ni uspelo. Poleg tega so v vojno vstopile Združene države Amerike in potrebno je bilo narediti velik preboj, saj bi jih v nasprotnem primeru sveže ameriške čete popolnoma izčrpale. Na drugi strani je umik Rusije iz vojne sprostil nemške čete na vzhodu in so lahko okrepile zahodno fronto.

5. marca 1918 so Nemci dali v uporabo novo šifro, kar je bilo že samo po sebi znak, da se pripravlja nekaj velikega. Nova šifra se je imenovala ADFGVX in je vsebovala substitucijo in transpozicijo ter ključ, ki se je menjaval dnevno.

Glavni francoski kriptolog Georges Painvin se je s šifro ukvarjal od 5. marca, ko je šifra prešla v uporabo, vendar brez uspeha. Glede na uporabo zgolj petih črk, mu je bilo jasno, da gre za kvadrat, najverjetneje z uporabo substitucije in transpozicije, vendar se je ključ menjaval dnevno in prestreženih sporočil v enem dnevu preden se je menjal ključ, je bilo malo. Splošne rešitve ADFGX niso nikoli odkrili. Je pa Painvin razvozlal posamezne ključe za dneve, ko je bil radijski promet bolj gost (Kahn 1996, 344).

Slika 6.2: Spomladanska ofenziva

Legenda: (1) Operacija Michael (21.3. – 5.4.), (2) Operacija Goergette (9.4. – 29.4.), (3) Operacija Blücher-Yourk (27.5. – 6.6.), (4) Operacija Gneisenau (9.6. – 13.6.), (5) Operacija Friedensturm (15.7. – 19.7.)

Vir: Le Maner (2016).

Velika ofenziva se je začela 21. marca 1918 z operacijo Michael. Nemci so napadli z 74 divizijami, 6600 topovi, 3500 možnarji in 326 lovskimi letali. Na drugi strani so jih Britanci pričakali zs15 divizijami, 1650 topovi, 119 tanki in 357 letali. Nemci so napadli

jugozahodno od kraja St. Quentin, najprej s peturnim artilerijskim obstreljevanjem, nato s pehotnim napadom. Cilj napada je bil prebiti frontno linijo in presekati angleške oskrbovalne poti, kar je Nemcem tudi uspelo. Angleži so se brezglavo umikali in v enem tednu izgubili kar 65 km ozemlja. Kljub temu, da so zavezniki vedeli, da se pripravlja napad – tudi po uvedbi nove šifre in pogostejšem radijskem prometu, se nanj niso mogli pripraviti, saj je bila lokacija napada neznanka. 17. marca, le nekaj dni pred napadom, so njihova izvidniška letala sicer zaznala premike nemških sil v smeri St. Quentina, vendar jim to ni dalo na voljo dovolj časa za okrepitev tega dela linije (Le Maner, 2016).

Hitro nemško napredovanje je povečalo radijski promet in Francozi so se lotili dela. Painvin je začel s frekvenčno analizo, ki je potrdila, da so Nemci dnevno menjavali ključ. Rešitev šifre bo torej zahtevala veliko količino sporočil iz istega dne. 1. aprila se je Francozom posrečilo – z 18 prestreženimi sporočili so dobili dovolj materiala za začetek kriptoanalize. Vendar je bila nemška šifra zelo težko zlomljiva in Painvin je sporočila iz 1. aprila razvozlal komaj 29. aprila, do takrat pa so bila že popolnoma nekoristna (Kahn 1996, 341).

Druga faza ofenzive – operacija Georgette se je začela 9. aprila. Tokrat so se Nemci osredotočili na flandrijsko regijo na severu Francije s ciljem, da potisnejo Angleže do obale in jih tako stisnejo v kot. Po štiri in pol urnem artilerijskem obstreljevanju, je 14 nemških divizij napadlo 16 kilometrov dolgo linijo. Vendar so bili zavezniki (Britanci in dva oddelka Portugalske vojske) tokrat bolje pripravljeni in Nemci so v slabih treh tednih trajanja napadov pridobili »zgolj« 12 kilometrov. V tem času se je Painvin še vedno mučil s ADFGX šifro. Zavezniki so se morali še naprej zanašati zgolj na zračne posnetke izvidniških letal, kar jim ni zagotavljalo dovolj časa za priprave pred naslednjim nemškim napadom (Kahn 1996, 344 in Thomas, 2016).

V tretji fazi ofenzive so se Nemci osredotočili na greben Chemin des Dames, v smeri reke Marne. Preboj na tem področju bi jih zelo približal Parizu. Napad se je začel 27. maja in že prvi dan so Nemci pridobili 15 kilometrov ozemlja. Po začetnem šoku so se zavezniki (tokrat Francozi, podkrepljeni z Britanskimi enotami) reorganizirali in po številnih protinapadih zaustavili Nemce na Marni. Kljub temu so bili od Pariza oddaljeni le še 90 kilometrov (Firstworldwar.com 2016).

Sedaj je bilo ključno vprašanje, kje bo Ludendorff udaril naslednjič. Tanka zavezniška linija ne bi prenesla močnega udarca in če bi tudi v naslednji fazi ofenzive Ludendorff ohranil element presenečenja, bi lahko prebil obrambno linijo, zavzel Pariz in morebiti končal vojno. Edini način, kako bi zavezniki to lahko preprečili, bi bil koncentracija svojih sil na točki

napada. Pritisk na zavezniške kriptoanalitike se je povečal. Na drugi strani pa tudi Nemci niso bili brez težav. Taktika, ki so jo do sedaj tako uspešno uporabljali, je zahtevala močno bombardiranje in nato bliskovit pehotni napad. Hitro napredovanje nemških enot pa je prineslo določene logistične težave. Da bi prikrili svoje načrte, so velike količine artilerijske municije, ki so jo potrebovali, transportirali zgolj ponoči, kar je pomenilo, da je logistika zaostajala in s tem upočasnila tudi napredovanje nemške pehote (Kahn 1996, 346).

Konec maja je bil George Painvin že toliko seznanjen z delovanjem šifre, da je sporočila, če je le imel na voljo dovolj primerkov iz istega dne, rešil že v enem dnevu. Tako pridobljene informacije so bile ažurne in posledično tudi koristne. 3. junija so Francozi prestregli sporočilo in ga v nekaj urah tudi prebrali. Šlo je za poziv k hitrejšemu pošiljanju municije, kar samo po sebi ni bistvenega pomena. Vendar je sporočilo vsebovalo tudi naslovnika – poveljstvo 18. armade v Remaugiesu in ker je bila tja namenjena municija, je to pomenilo, da je znana lokacija naslednjega napada. Zračno izvidništvo je potrdilo transport municije in sedaj so zavezniki vedeli, kje morajo utrditi svojo obrambno linijo (Kahn 1966, 344–346).

Namen četrte faze (operacija Gneisenau) je bilo povezati ozemlja, pridobljena med prvo in tretjo operacijo in tako okrepiti celotno linijo. Napad se je začel 9. junija, vendar so bili zavezniki tokrat nanj pripravljeni. Francoska vojska, okrepljena s svežimi ameriškimi enotami, je napad odbila in 11. junija začela protinapad, ki je Nemce potisnil nazaj na začetne položaje. Prvič v veliki ofenzivi so se nemške čete umaknile preden so dosegle svoj cilj (Rickard, 2007).

Tudi lokacija zadnje faze napadov je bila zaveznikom znana. Bitka na Marni je sicer v prvih dneh Nemcem prinesla nekaj uspeha, saj so prečkali reko Marno, vendar jih je že 18. julija združen napad francoskih, britanskih, ameriških in italijanskih sil potisnil nazaj čez reko. Tudi Nemci so do sedaj dojeli, da spomladanska ofenziva ne bo prinesla željenih rezultatov in so tako odpovedali šesto fazo, ki bi naj dokončala začeto drugo fazo v Flandriji (www.greatwar.co.uk 2016).

7 Sklep in verifikacija hipotez

7.1 Sklep

Komunikacija med vojaškimi enotami je temelj uspešnega bojevanja. Prav prva svetovna vojna je postavila na preizkus največji napredek na področju komuniciranja – brezžično komunikacijo. Ta je omogočila hiter prenos podatkov, predvsem na daljših razdaljah, po drugi strani pa je odprla vrata novi veji znotraj obveščevalne dejavnosti tj. kriptoanalizi.

Kriptologija sama ni novost, ki bi jo prineslo novo stoletje, vendar je sama količina podatkov, ki je prehajala preko radijskih valov, brez dvoma okrepila njeno vlogo v vojni. Pred vojno je bila kriptologija sekundarnega pomena, v času prve svetovne vojne pa je postala primarni vir zbiranja informacij o nasprotniku. Na eni strani so se države in njihove vojske trudile prikrivati svoja sporočila z raznimi oblikami šifriranja in kodiranja, na drugi strani pa so oblikovale posebne enote vojske in mornarice, ki so se ukvarjale samo z razbijanjem nasprotnikovih šifer in kod.

V tem obdobju se je spremenila kriptografija sama. Do takrat je kriptoanalitik sedel sam v sobi s sporočilom, ki ga je želel razvozlati, uporaba šifer in kod v prvi svetovni vojni pa je za rešitev zahtevala vsaj dve sporočili enake dolžine in preden se je to zgodilo, jih je bilo potrebno prestreči veliko. Analitiki so se poleg tega zanašali tudi na druge podatke, ki so jih pridobili s prestrezanjem radijskega prometa, npr. na analizo lokacije prometa. Informacija o tem, od kod in iz katere enote je bilo sporočilo poslano, jim je velikokrat olajšalo kriptoanalizo, če ne pa vsaj podalo informacije o približni lokaciji enote, ki je sporočilo oddajala.

V obdobju prve svetovne vojne so države uporabljale različne šifre in kode. Kode so se uporabljale predvsem v mornarici, kjer je bila distribucija kodirnih knjig razmeroma lahka in varnost le-teh večja. Ko so prispele na ladjo, so bile knjige razmeroma varne. Hranili so jih v posebnih s svincem obdanih skrinjah in jih v primeru nevarnosti zajetja vrgli čez krov. Kodirne knjige so predstavljale večjo varnost, saj je bilo za razkritje nasprotnikovih sporočil potrebno imeti tudi njihovo kodirno knjigo ali vsaj del nje. Vendar je bilo mogoče kodirno knjigo zaseči in tako v trenutku pridobiti vpogled v nasprotnikova sporočila, kar je zaveznikom v teku vojne tudi večkrat uspelo.

Nobena šifra ni nerešljiva, če le imamo na voljo dovolj materiala in časa za kriptoanalizo. Države so to težavo reševale s pogostimi menjavami ključev, redko pa z

menjavo algoritma – torej šifre same. Britanci so ves čas vojne uporabljali playfairovo šifro, tudi Francozi in Američani so ostali zvesti svojim šifram. Nemci so bili edini, ki so v času vojne zamenjali celoten sistem šifriranja.

Na področju kriptoanalize so največje uspehe dosegali Britanci in Francozi. Prvim se je večkrat nasmehnila sreča, saj so zasegli več nemških kodirnih knjig, drugi pa so bili na to obliko vojnega delovanja najbolje pripravljeni, saj so ob izbruhu vojne imeli najbolje razvito kriptoanalitsko službo. Druge države so bile na tem področju v zaostanku, kot da se ne bi zavedale, kako pomembno je ohraniti tajne komunikacije in koliko prednosti lahko prinese poznavanje nasprotnikovih načrtov.

7.2 Verifikacija hipotez

Hipotezo, da *so šifrirni postopki v vojni udeleženih držav zaradi njihovega pomena in prepoznanih tveganj, postajali bolj zapleteni in težje zlomljivi,* lahko le delno potrdimo. Nemci so ugotovili, da je bila njihova prvotna šifra zlomljena in so jo zato nadomestili z novo, trdnejšo šifro, ki je zaveznikom sprva res povzročala velike težave. Druge države so se na morebitno kriptoanalizo njihovi šifer odzvale z menjavo ključa ali distribucijo novih kodirnih knjig.

Trditev, da je kriptografija oz. kriptoanaliza – del kriptografije, ki obsega branje skritih besedil brez poznavanja algoritma in ključa in je zaveznikom prinesla zmago v vojni, je nekoliko pretirana, vendar je uspešna kriptoanaliza vojno zagotovo skrajšala.

Drugo hipotezo, ki pravi, da *je uspešno dešifriranje prestreženih dokumentov v nekaterih primerih bistveno vplivalo na potek prve svetovne vojne*, lahko potrdimo.

Prvi primer vloge, ki jo je kriptoanaliza igrala v vojni, je bojevanje na morju. Zavezniki – predvsem Britanci so s pomočjo prestreženih podatkov uspešno blokirali nemško mornarico in tako onemogočili oskrbovanje po morju, kar je državo oslabilo in doprineslo k hitrejšemu porazu.

Tudi na kopnem so imeli zavezniški kriptoanalitiki – tokrat predvsem Francozi, prednost pred Nemci. Ko so ti leta 1918 začeli z veliko spomladansko ofenzivo, so bile prve bitke velik uspeh predvsem zaradi elementa presenečenja, ki ga je omogočila nova šifra, katere zavezniki niso pravočasno razbili. Ko jim je to po nekaj mesecih končno uspelo, so s tem izničili element presenečenja in pravočasno okrepili tiste dele linije, za katere so vedeli, da bo napadena. Ne moremo sicer trditi, da je bila kriptoanaliza nemške šifre edini razlog za preobrat, saj so imeli Nemci tudi druge težave. Zaradi hitrega napredovanja so pešale

oskrbovalne linije, vojaki so bili lačni, primanjkovalo jim je municije. Prav tako so jih v Franciji pričakale sveže in dobro opremljene ameriške čete, ki bi jih skupaj z izkušenimi Francozi in Britanci zagotovo premagale. Tako bi bila trditev, da je bila kriptoanaliza ključnega pomena za zmago, ponovno pretirana, je pa zagotovo prinesla veliko prednost in posledično hitrejšo zmago.

Primer, kjer je kriptoanaliza zagotovo prinesla velik preobrat, je razkritje Zimmermanovega telegrama. Zavezniki so prestregli sporočilo nemškega zunanjega ministra Arthurja Zimmermana, namenjeno nemškemu veleposlaniku v Mehiki, s ponudbo izdatne pomoči, če država vstopi v vojno na strani Centralnih sil. Po razkritju telegrama ameriški javnosti, se tudi glavni zagovornik nevtralnosti ameriški predsednik Woodrow Wilson, ni mogel izogniti pozivom k vojni. Združene države Amerike so tako vstopile v vojno, kar je prevesilo tehnico v prid antantnim zaveznikom.

Kriptoanaliza je igrala pomembno vlogo znotraj obveščevalnih sistemov držav udeleženk v prvi svetovni vojni. Predvsem antantne sile so po zaslugi informacij pridobljenih s kriptoanalizo, dosegle pomembne zmage tako na taktični kot na strateški ravni.

8 Literatura

- Adams, Jefferson. 2009. *Historical dictionary of German intelligence and counterintelligence.* Lanham: Scarecrow Press.
- Adler, Mortimer Y. (gl. ur.). 1975. *Encyclopedia Britannica Volume 1*. Chicago: W Benton.
- Beutelspacher, Albrecht. 1994. *Cryptology.* Washington: The Mathematical association of America.
- Blake, Barry J. 2010. *Secret language*. New York, Oxford Univerity Press Inc.
- Blatner, Adam. 2011. *Playing With Writing (Part 1).* Dostopno prek: http://www.blatner.com/adam/scriptology/6-Summaryetc/play.html (16.3.2014).
- Boghardt, Thomas. 2004. *Spies of the Kaiser: German covert operations in Great Britain during the first world war era.* New York: Palgrae Macmillan.
- Bruton, Elizabeth. 2016. *Communication Technology*. Dostopno prek: http://encyclopedia.1914-1918-online.net/article/communication_technology (7.8.2016).
- *Crypto Corner: Playfair cipher.* Dostopno prek: http://crypto.interactive-maths.com/playfair-cipher.html (9.7.2016).
- Debruyne, Emmauel. 2016. *Espionage.* Dostopno prek: http://encyclopedia.1914-1918-online.net/pdf/1914-1918-Online-espionage-2014-10-08.pdf (15.1.2014).
- Finley, James P., ur. 1995. *U.S. Army Military Intelligence History: A Sourcebook.* Fort Huachuca, Arizona: U.S. Army Intelligence Center & Fort Huachua. Dostopno prek: http://huachuca.army.mil/files/History_MIReader.pdf
- *First World War.* 2016. Dostopno prek: http://www.firstworldwar.com/battles/aisne3.htm (7.7.2016).
- Foley, Robert T. 2005. Easy Target or Invincible Enemy? German Intelligence Assessments of France Before the Great War. *Journal of intelligence history* Vol.5 (2): 1-24.
- Gannon, Paul. 2010. *Inside Room 40.* Surrey: Ian Allan Publishing.
- Gažević, Nikola (gl. ur.). 1985. *Vojna eciklopedija.* Beograd: Vojnoizdavački zavod.
- Gilbert, James L. 2012. *World war I and the Origins of U.S. Military Intelligence.* Dostopno prek: https://books.google.si

https://books.google.si/books?id=RsS_QiBFlyAC&pg=PA224&lpg=PA224&dq=code+and+cipher+compilation+communications+shorthand&source=bl&ots=MbgEPXvTq4&sig=upCgHcjnJF0gHleB2f1tyweWCfo&hl=sl&sa=X&ved=0ahUKEwiz8aiMgtzNAhUMaxQKHX7hAe8Q6AEIJDAC#v=onepage&q=code%20and%20cipher%20compilation%20communications%20shorthand&f=false (5.7.2016).

- Goebel, Greg. 2012. *Codes and codebreakers in world war 1*. Dostopno prek: http://www.vectorsite.net/ttcode_04.html (12.1.2014).
- Kahn, David. 1996. *The Codebreakers: The story of secret writing*. New York: Scribner.
- Keegan, John. 2004. *Intelligence in war.* Toronto: Vintage Canada.
- Kodrič, Sašo. 2013. *Orodja za razbijanje substitucijske šifre, diplomsko delo.* Ljubljana: Fakulteta za računalništvo in informatiko. Dostopno prek: http://eprints.fri.uni-lj.si/1976/1/Kodri%C4%8D_S-1.pdf (15.3.2014).
- Le Maner, Yves. 2016. *Kaiserschlacht: The German spring offensive*. Dostopno preko: http://www.remembrancetrails-northernfrance.com/history/battles/kaiserschlacht-the-german-spring-offensive-of-1918.html (7.7.2016).
- Lee, Bartholomew. 2016. *Radio intelligence developments during world war one and between the wars.* Dostopno prek: http://antiqueradios.com/chrs/journal/intelligence.html (7.8.2016)
- Neiberg, S. Michael. 2016. *The Zimmerman Telegram and American Entry into World War I*. Dostopno prek: https://www.gilderlehrman.org/history-by-era/world-war-i/essays/zimmermann-telegram-and-american-entry-world-war-i (30.5.2016).
- *Office of the Historian. U.S. Entry into World War 1, 1917*. 2016. Dostopno prek: https://history.state.gov/milestones/1914-1920/wwi (8.8.2016).
- Richelson, Jeffrey T. 1997. *A Century of Spies: Intelligence in the Twentieth Century*. Oxford: Oxford University Press.
- Rickard, J. 2007. *Battle of Noyon-Montdidier, 9-13 June 1918.* Dostopno prek: http://www.historyofwar.org/articles/battles_noyon_montdidier.html (7.7.2016).
- Singh, Simon. 2008. *Knjiga šifer: Umetnost šifriranja od starega Egipta do kvantne kriptografije*. Tržič: Učila international.
- Smith, Derek J. 2010a. *Codes an ciphers in history, Part 1 – To 1852*. Dostopno prek: http://www.smithsrisca.co.uk/crypto-ancient.html (12.1.2014).

- Smith, Derek J. 2010b. *Codes an ciphers in history, Part 2 – 1853-1917.* Dostopno prek: http://www.smithsrisca.co.uk/crypto-middle.html (12.1.2014).
- Stergaršek, Eva. 2006. *Kriptoanaliza.* Seminar podiplomskega študija. Dostopno prek: http://www.lkn.fe.uni-lj.si/Seminarji/e_stergarsek.pdf (12.1.2014).
- Stout, Mark. 2014. Intelligence in World War 1 1914-1918. *Intelligencer: Journal of U.S. Intelligence Studies* (spring/summer 2014): 35–38.
- The Great War 1914-1918. 2016. *1918 German Offensives to break the deadlock.* Dostopno prek: http://www.greatwar.co.uk/battles/#germanspringoffensives (7.7.2016)
- Thomas, Ronan. 2016. *Endgame in Flanders, 1918.* Dostopno prek: http://www.militaryhistoryonline.com/wwi/articles/endgameinflanders.aspx (7.7.2016).
- Tworek, Heidi J.S.. 2016. *Wireless Telegraphy.* Dostopno prek: http://encyclopedia.1914-1918-online.net/article/wireless_telegraphy (7.8.2016).
- Wander, Tim. 2016. *The Marconi company; Wireless Goes to War 1914-1918.* Dostopno prek: http://marconiheritage.org/ww1intro-3.html (5.8.2016)
- Yardley, Herbert O..1981. *American Black Chamber.* Brooklyn, New York: Press of Braunwoth &co. inc..