Kriptologija u Prvom svjetskom ratu

Vuković, Filip

SVEUČILIŠTE U ZAGREBU
FILOZOFSKI FAKULTET
ODSJEK ZA INFORMACIJSKE I KOMUNIKACIJSKE ZNANOSTI
Ak. god. 2021./2022.

Filip Vuković

Kriptologija u Prvom svjetskom ratu

Završni rad

Mentor: dr. sc. Vjera Lopina

Zagreb,lipanj 2022.

Izjava o akademskoj čestitosti

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

potpis

_____

Filip Vuković

Zahvaljujem dr. sc. Vjeri Lopini na mentoriranju tijekom pisanja ovog završnog rada.

Sadržaj

1. Uvod

Naziv kriptologija dolazi od grčkih riječi *kryptos*, što znači skriven te *logos* što znači riječ. Otkako ljudi međusobno komuniciraju putem poruka, postoje želja i potreba za što efikasnijom metodom zakrivanja spomenutih poruka. Samim time, razvoj kriptologije kao znanosti moguće je pratiti još od antičkih civilizacija pa sve do danas. Najveći napredak u kompleksnosti i efikasnosti metoda zakrivanja i raskrivanja poruka možemo primijetiti u prvim desetljećima 20. stoljeća. Primarni razlog ovomu je Prvi svjetski rat. Uz sve zlo koje sa sobom nosi, rat također tjera čovjeka na ekspresni, prije svega tehnološki, napredak kako ne bi zaostao za svojim suparnicima. Kao najveći do tada zabilježen sukob, upravo je Prvi svjetski rat odigrao ulogu te prekretnice unutar područja kriptologije. Većina je sudionika u ovaj rat ušla s, prema ubrzo postavljenim standardima, poprilično jednostavnim metodama zakrivanja poruka, od kojih su neke bile stare više stotina godina. Međutim, ubrzo je shvaćena jednaka vrijednost tzv. "rata u sjeni" kao i onog na bojištu, stoga tijekom rata dolazi do osnivanja brojnih kriptoloških organizacija čija je ključna ulogu za ishod rata ostala neupitna. Također su pred kraj i nakon samog rata kriptološki strojevi postajali sve češća pojava te će se daljnji razvoj ove znanosti na temelju njih nastaviti sve do danas. Stoga ovaj rad nastoji na što precizniji način prikazati stanje same kriptologije za vrijeme Prvog svjetskog rata te njen daljnji razvoj tijekom i nakon njega.

2. Njemačka kriptologija i istočno bojište

2.1 Situacija na istočnom bojištu

Važnost kriptologije i kvalitetnih kodova na bojištu dokazale su Njemačka i Austro-Ugarska još u samom početku rata. Na istočnom je bojištu ruska vojska međusobno komunicirala putem tada još relativno nove tehnologije radija te bez upotrebe ikakve metode šifriranja. Ovo je Nijemcima i Austrijancima omogućilo da bez ikakvih problema presretnu ruske poruke te otkriju njihov sadržaj, što dovodi do okruživanja ruske vojske te njihovog katastrofalnog poraza u bitci kod Tannenberga 1914. Rusi nakon ovoga počinju šifrirati poruke, ali uz jednako malo uspjeha. Naime, radi slabe organizacije istovremeno su koristili nove verzije jednostavnih kodova i starije verzije koje su Nijemci i Austrijanci odavno uspješno dešifrirali. Poruke je tako bilo moguće otkriti uspoređivanjem onih zakrivenih novijom verzijom koda s već dešifriranom starom verzijom[1]. Od 3 velesile na istočnom bojištu, s gledišta kriptologije je daleko najbolje pripremljena bila upravo Austro-Ugarska. Imajući na umu ključnost informacija koje uspješno dešifriranje neprijateljskih poruka može donijeti Austro-Ugarska je u rat ušla s već oformljenim kriptoanalitičkim stožerom na čelu s generalom Maximilianom Rongeom.

"Do 1914, kriptologija je bila zapostavljen izvor informacija. Prvi svjetski rat je pokazao njenu vrijednost. Prije rata samo su tri velesile imale kriptoanalitičke agencije. Nakon rata su ih imale sve." (Kahn, 1980.[2])

Prije samog početka rata austrijski stožer je imao pripremljen popis šifri i kodova koje bi Rusi mogli upotrijebiti tijekom rata, što im je omogućilo da veliku većinu ruskih šifriranih poruka razotkriju isti dan kada su i došli do njih. Primjer ovoga je telegram ruskog generala Aleksandra Novikova koji je austrijski kriptoanalitičar Hermann Pokorny uspio dešifrirati nakon samo 6 sati. Ova i brojne slične situacije su dozvolile Nijemcima i Austrijancima praćenje kretanja ruske vojske na svakodnevnoj bazi[3]. Shvativši svoju pogrešku, Rusi odlučuju uzeti svoje neprijatelje za primjer te razvijaju znatno kompleksniju metodu zakrivanja na temelju Vigenèreove šifre koju su Austrijanci koristili još od samog početka.

[1] Marshall, A. (2004.) Russian Military Intelligence, 1905–1917: The Untold Story behind Tsarist Russia in the First World War, War in History 11(4), 403-408 str.
[2] Kahn, D. (1980.) Codebreaking in World Wars 1 and 2: The major successes and failures, their causes and their effects, Cambridge university press, 621 str.
[3] Gylden, Y. (1935.) The contribution of the cryptographic bureaus in the World War, War department Washington, 56-63 str.

2.2 Vigenèreova šifra

Vigenèreova šifra nosi naziv po francuskom kriptologu Blaiseu de Vigenèreu, iako se smatra da je nije osmislio on već Giovan Battista Bellaso. Riječ je o jednom od najpoznatijih kriptosustava u povijesti koji potječe još iz 16. stoljeća te je također doživio masovnu primjenu tijekom Prvog svjetskog rata na istočnom bojištu gdje su ga između ostalog koristile ruska i austro-ugarska vojska.

KEY \ -- PLAINTEXT --	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
A	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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

Slika1. Tablica Vigenèreove šifre (izvor: https://www.researchgate.net/figure/Vigenere-Cipher-table_fig3_318260132)

Ovaj kriptosustav je sve do pojave modernijih tehnologija i načina zakrivanja poruka smatran neprobojnim te je među Francuzima koji su se suprotstavljali austro-ugarskoj vojsci dobio

naziv *"le chiffre indéchiffrable"*, što u doslovnom prijevodu s francuskog znači neprobojna šifra iako je sama šifra bila probijena nekoliko puta prije samog rata[4]. U svom najjednostavnijem obliku, Vigenèreova šifra funkcionira tako što se ranije određeni ključ ponavlja kolikogod je puta potrebno kako bi se poruka zakrila. Samim time ovakvu vrstu zakrivanja najlakše je razotkriti ukoliko je kriptologu ključ već poznat ili on pak nekako uspije doći do njega. Ključ se zatim uspoređuje sa zakrivenom porukom putem tablice (slika 1). Šifriranje putem ovog kriptosustava radi se prema sljedećoj formuli:

$$P = C = K = (\mathbf{Z}_{26})^m. \text{ Za ključ } K = (k_1, k_2, \dots, k_m)$$

$$e_K(x_1, x_2, \dots, x_m) = (x_1 +_{26} k_1, x_2 +_{26} k_2, \dots, x_m +_{26} k_m)$$
$$d_K(y_1, y_2, \dots, y_m) = (y_1 -_{26} k_1, y_2 -_{26} k_2, \dots, y_m -_{26} k_m)$$

"Dakle, slova otvorenog teksta pomičemo za k_1, k_2, ... ili k_m mjesta, u ovisnosti o tome na kojem se mjestu u otvorenom tekstu nalaze (preciznije, pomak ovisi o ostatku koji dobijemo kada poziciju slova podijelimo s duljinom ključa m). Kod ove su šifre osnovni elementi otvorenog teksta i šifrata "blokovi" od po m slova. No, šifriranje se zapravo provodi "slovo po slovo", pa ovdje nije nužno nadopuniti zadnji blok ako broj slova u otvorenom tekstu nije djeljiv s m." (Math PMF[5])

ključ	B	R	O	J	K	R	I	P	T	O	L	O
otvoreni tekst	K	R	I	P	T	O	L	O	G	I	J	A
šifrat	L	I	W	Y	D	F	T	D	Z	W	U	O

Slika 2. Primjer poruke zakrivene Vigenèreovom šifrom (izvor: https://web.math.pmf.unizg.hr/~duje/kript/vigener.html)

Njemački časnik i kriptoanalitičar Friedrich W. Kasiski razvio je tehniku rješavanja poruka zakrivenih Vigenèreovom šifrom koja se temelji na tome da identični parovi slova unutar poruke i ključa uvijek daju iste zakrivene simbole. Na primjer, ako se u zakrivenoj poruci više

[4] Knežević, M. (2015.) Vigenereova i Playfairova šifra, Svečilište J. J. Strossmayera u Osijeku, Završni rad, 8-9 str.
[5] Math PMF, Vigenereova šifra URL: https://web.math.pmf.unizg.hr/~duje/kript/vigener.html [Pristupljeno 28.7.2022.]

puta pojavi ista kombinacija triju slova tada se može pretpostaviti da ključ ima 3 ili 9 slova[6]. Upravo radi ove metode, većina kompleksnijih varijacija Vigenèreove šifre koriste ključ koji se ne ponavlja, ovo se može postići ili odabirom iznimno velikog i kompleksnog ključa ili pak skraćivanjem poruke što je više moguće bez da ona gubi svoje značenje.

2.3 Njemačka hijerarhija kodova

Za vrijeme rata njemačka vojska je razvila sistem korištenja kodova prema zonama opasnosti. Imajući na umu potencijalno iznimno kaotično stanje na prvoj crti bojišta, područje od prva 3 kilometra bilo je proglašeno opasnom zonom te unutar nje nikakva direktna komunikacija bez korištenja kriptosustava nije bila dozvoljena. Unutar ove zone koristio se tzv. kod tri broja. Nadalje, za međusobnu komunikaciju između divizija izvan opasne zone koristio se kod 3 slova. Za posebne situacije također su rjeđe upotrebljavani avijacijski kod i meteorološki kod, čija je uloga bila komunikacija tijekom velikih zračnih operacija. Dok se komunikacija između stožera odvijala isključivo u ADFGVX kodu, popularno prozvanom "*Geheimschrift der Funker"*, u prijevodu tajni spisi radiooperatera. Na samom vrhu hijerarhije nalazio se kod ratnog stožera, ovaj kod je bio korišten iznimno rijetko, isključivo za međusobnu komunikaciju članova njemačke vojske na najvišim položajima te nikad putem radija. Samim time o ovom kodu se ne zna gotovo ništa jer niti jedna poruka pisana njime nikad nije presretnuta[7].

2.3.1 Kod tri broja i tri slova

Namijenjeni za brzu i jednostavnu upotrebu u najtežim uvjetima kodovi tri broja su funkcionirali na sličnom principu kao današnji ABC kodovi. Točnije svaka skupina od tri slova ili broja predstavlja jedan znak ili ponekad pojam. Kako bi pokušali razotkriti poruke koje skriva ovaj kod američka vojska je razvila tehnika bilježenja i indeksiranja primijećenih troslovnih nizova prema sljedećim parametrima:

- učestalost pojavljivanja niza
- vrsta poruke u kojoj se niz najčešće pojavljuje
- položaj niza unutar same poruke

[6] Simmons, G. J, Vigenere cipher, Encyclopedia Britannica URL: https://www.britannica.com/topic/Vigenere-cipher [Pristupljeno: 28.7.2022.]
[7] Friedman, W. F.(1935.) Field codes used by the German army during the World War, War department office of the chief signal officer Washington, 5 str.

- mogućnost da je značenje samog niza ili određenog drugog niza unutar poruke već otkriveno
- sličnost niza određenoj riječi koju on potencijalno predstavlja (npr. niz CHI je predstavljao riječ *Chiffer*, odnosno šifra)

Nakon nekog vremena Amerikanci otkrivaju da Nijemci koriste tzv. KRU kod, u kojem svaki niz počinje jednim od spomenutih slova (K,R ili U) dok naredna dva slova nisu određena. Ova verzija koda nudi zakrivatelju mogućnost od 2028 različitih nizova triju slova. Dok je kasnije razvijen znatno napredniji KRUSA kod koji umjesto tri nudi pet mogućnosti za prvo slovo u nizu što broj mogućih troslovnih nizova diže na čak 4205. Svaka poruka zakrivena ovom metodom sastojala se od šest glavnih skupina nizova, a one su: brojevi, riječi i fraze, skupine za slovkanje, pomoćni signali, interpunkcija i slijepe grupe[8].

2.3.2 ADFGVX

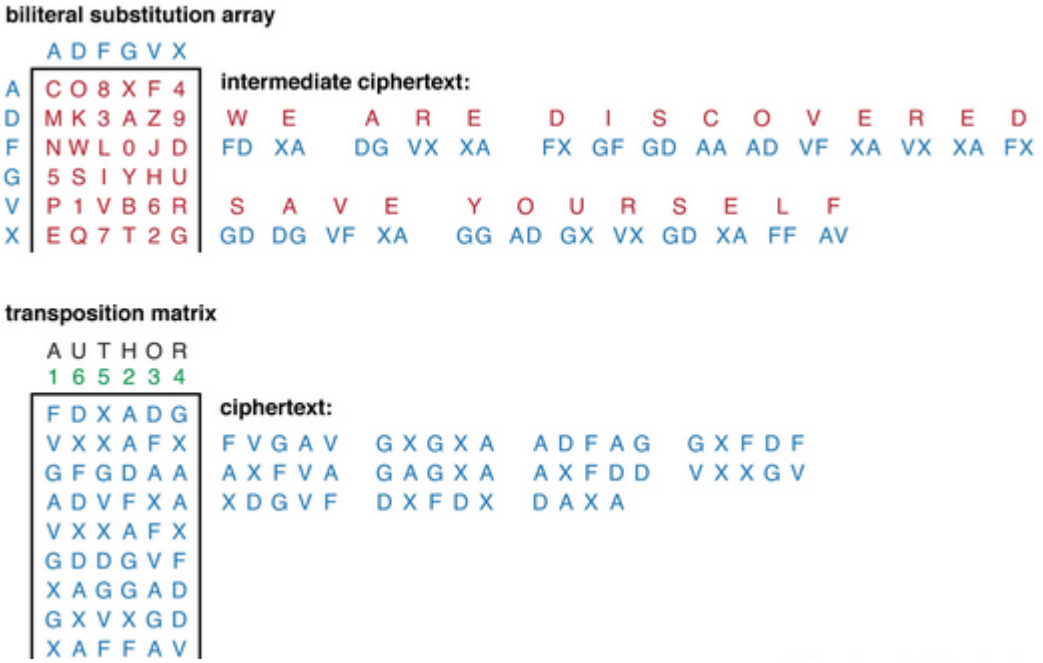
Osmišljen za sigurnu komunikaciju između njemačkih stožera na zapadnoj, a kasnije i istočnom bojištu, ADFGVX bio je jedan od najnaprednijih kriptosustava Prvog svjetskog rata. Riječ je o kombinaciji supstitucijskog i transpozicijskog sustava na temelju izmijenjene verzije Polybiusovog kvadrata koja koristi slova umjesto brojeva. 1918. njemački časnik Fritz Nebel osmišlja ADFGX sustav nazvan po slovima koja označuju stupce i redove Polybiusovog kvadrata (slika 3) pri enkripciji i dekripciji. Ubrzo Nebel unaprjeđuje sustav dodajući mu slovo V te s njim još po jedan stupac i red u kvadrat[9].

	A	D	F	G	V	X
A	1	4	7	R	E	G
D	I	M	N	T	A	B
F	C	D	F	H	J	K
G	L	O	P	Q	S	U
V	V	W	X	Y	Z	0
X	2	3	5	6	8	9

Slika 3. Polybiusov kvadrat u ADFGVX sustavu s ključem (izvor: https://crypto.interactive-maths.com/adfgvx-cipher.html)

[8] Friedman, W. F.(1935.) Field codes used by the German army during the World War, War department office of the chief signal officer Washington, 21-37 str.
[9] Rošić, K. (2018.) Transpozicijske šifre, Sveučilište J. J: Strossmayera u Osijeku, Diplomski rad, 25-26 str.

Prvi korak enkripcije putem ADFGVX sistema jest zamjena slova pomoću Polybiusovog kvadrata tijekom čega svako slovo mijenjaju dva slova iz skupine A,D,F,G,V i X koja mu odgovaraju prema položaju reda i stupca u kojem se originalno slovo nalazi. Ovdje ulogu igra prvi ključ koji dolazi na početak, dok svi ostali znakovi idu istim redoslijedom iza ključa, naravno bez znakova koji se već nalaze u samom ključu. Kako bi enkripcija bila još jača dolazi do novog zakrivanja, ovog puta putem transpozicije. Ovdje se pojavljuje drugi ključ iz kojeg je potrebno ukloniti sve ponavljajuće znakove te ranije zakrivenu poruku napisati ispod njega u koliko god je redova potrebno s time da svaki znak mora biti ispod jednog od znakova ključa (slika 4). Zatim je stupce potrebno složiti abecednim redoslijedom te ih ispisati vodoravno[10].



Slika 4. Primjer enkripcije pomoću ADFGVX sustava (izvor: https://www.britannica.com/topic/ADFGVX-cipher)

[10] Kulp, J., Poulter, W. (n.d.) The ADFGVX cipher, Lakehead University

2.4 Enigma

Iako je znatno veću slavu stekla dvadesetak godina kasnije, *Enigma* je nastala ubrzo nakon završetka Prvog svjetskog rata 1918. godine te je jedan od najboljih primjera tehnološkog napretka u polju kriptologije koji je pokrenuo Prvi svjetski rat. Riječ je o stroju za šifriranje poruka koji je svojedobno smatran najsigurnijim načinom zakrivanja poruka.

"Kada bi tekst bio napisan na tipkovnici, struja prolazi kroz razne elemente stroja i pali svijetlo šifriranog slova na ploči s lampicama. Što je *Enigmu* činilo posebnom je činjenica da svaki put kad bi pritisnuli slovo pokretni dijelovi stroja bi zamijenili položaje tako da sljedeći put kada isto slovo bude pritisnuto bilo bi zakriveno kao nešto drugačije. Ovo znači da nije bilo moguće pomoću tradicionalnih metoda probiti šifru." (Ellis, 2005[11])

Prva postaja signala unutar *Enigme* bila je priključna ploča koja bi zatim signal slala do rotora. *Enigma* je funkcionirala na principu reflektora koji šalje električne impulse natrag preko rotora, iz smjera odakle je impuls i došao te na taj način šifrira i dešifrira poruke. *Enigma* je imala tri rotora lijevi-brzi, srednji i desni-spori. Signal bi tako prvo prošao kroz brzi rotor koji bi se okrenuo i pokrenuo okretanje srednjeg rotora nakon što kroz njega prođe signal, dok bi srednji zatim, nakon svog okreta pokrenuo spori rotor. Radi ovog je sistema *Enigma* često bila uspoređivana sa satom, a rotori s kazaljkama[12].

"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 kariku *Enigme*: nijedno slovo nije nikad moglo biti šifrirano samim sobom. Moglo se beskonačno pritiskati npr. slovo A na tipkovnici, a da nikad ne zasvijetli lampica na čijem je poklopcu bilo otisnuto slovo A." (Derenčin, 2016.[13])

Enigma je također bila posebna po tome što je bila sam svoj ključ pri dešifriranju. Naime, kada bi primatelj dobio poruku trebao bi ju samo upisati u svoju *Enigmu* te ukoliko je ona postavljena na isti način kao kod pošiljatelja, stroj bi sam dešifrirao poruku.

[11] Ellis, C. (2005.) Exploring the Enigma, University of Cambridge, 2 str.
[12] Crypto museum, How did an Enigma machine work URL: https://www.cryptomuseum.com/crypto/enigma/working.htm [Pristupljeno 28.7.2022.]
[13] Derenčin, R. (2016.) Enigma i njemačke podmornice u Drugom svjetskom ratu, Polemos 19

3. Francuska kriptologija i zapadno bojište

3.1. Situacija na zapadnom bojištu

Zapadno bojište je tijekom Prvog svjetskog rata već u samim počecima pokazalo da se sprema najkrvaviji sukob u dotadašnjoj povijesti. Borbe na zapadnom bojištu započinju njemačkim provodom Schlieffenovog plana, ofenzive preko neutralne Belgije te pokušaja okruživanja francuske vojske. Nijemci bez većih poteškoća provode ovaj plan te dolazi do otvorenog sukoba s Francuzima[14]. Zapadno bojište je također ostalo zapamćeno po svakodnevnom rovovskom i kemijskom ratovanju. Što se tiče kriptologije na ovom bojištu Francuzi su se pokazali ravnopravnima, ako ne i superiornima Nijemcima. S obzirom na to da su u rat ušli s već osnovanim kriptološkim uredima, Francuzi su do kraja rata uspješno dešifrirali više od sto milijuna njemačkih riječi zakrivenih raznim šiframa. Ovo je bilo velikom većinom moguće zbog upotrebe telegrama i radija s kojim vojnici još nisu bili u potpunosti upoznati[15].

"Brzina napredovanja, poteškoće povezane s upotrebom telegrafskih linija u zauzetom području, zajedno s manjkom pripreme, navedeni su kao glavni razlog za neuspjeh. Očito je, između ostalog, da je neuspjeh sustava za komunikaciju doveo do neposrednih katastrofalnih nesporazuma njemačke komande što se tiče relativnih položaja Prve i Druge njemačke vojske točno prije odlučujuće faze bitke na Marni. Radi raspada žičane komunikacije, veliko breme je stavljeno na njemačke radio postaje, što dovodi do rasprave o kriptografiji. Ako se komunicira putem radija, nužno je bilo pretpostaviti da postoji opasnost od presretanja poruka od strane neprijatelja, posljedično tome, morao je biti korišten siguran sustav kodova i šifri." (Gylden, 1935.[16])

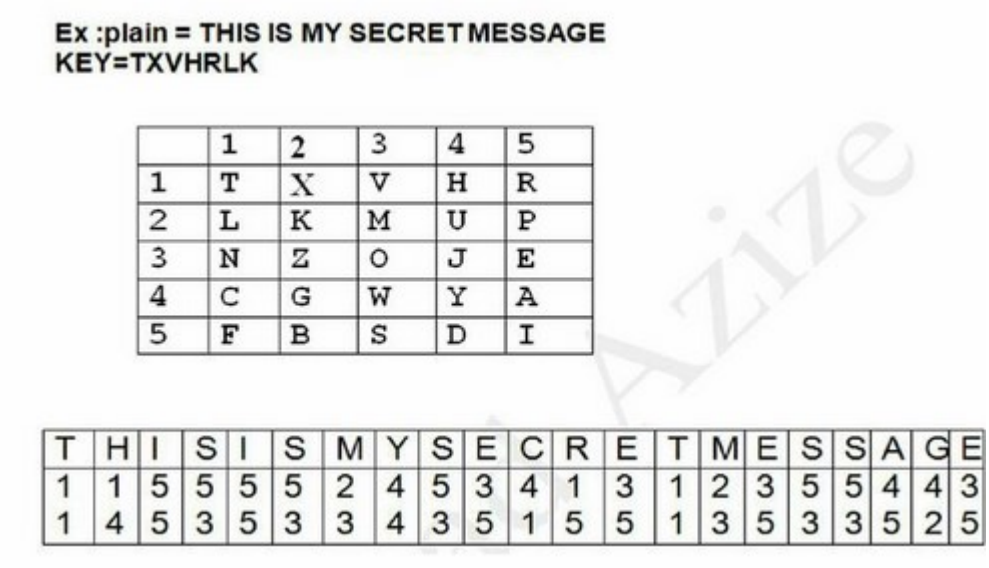
[14] Hamilton, R. F, hrwig, H. H. (2005.) The origins of World War 1, War in history 12(1), 159 str.
[15] Kahn, D. (1980.) Codebreaking in World Wars 1 and 2: The major successes and failures, their causes and their effects, Cambridge university press, 620 str
[16] Gylden, Y. (1935.) The contribution of the cryptographic bureaus in the World War, War department Washington, 28 str.

3.2 Kriptosustavi Felixa Delastella

Rođen 1850. godine, Felix Delastelle bio je jedan od najvećih kriptologa 19. stoljeća. Delastelle je posvetio gotovo svoj čitav život kriptologiji te tako postao jedini diplomirani francuski kriptolog koji nije služio u vojsci, umjesto u vojne svrhe odlučio je svoje znanje iskoristiti pišući knjigu. Smatrajući da su sve dotadašnje knjige tek zagrebale površinu ove teme, Delastelle piše jednu od najvažnijih knjiga u povijesti kriptologije pod nazivom *Traite elementarie de cryptographie* u kojoj razrađuje brojne kriptosustave od kojih su najpoznatiji bifidski i trifidski sustav[17].

3.2.1 Bifidska i trifidska šifra

Delastelleov prvi i vjerojatno najvažniji izum je bifidski sustav (slika 5) koji, iako nikada nije korišten u vojne svrhe, služi kao baza za često vojno upotrebljavan trifidski sustav. Temelji se na Polybiusovom kvadratu u koji se umeće ključ[18].

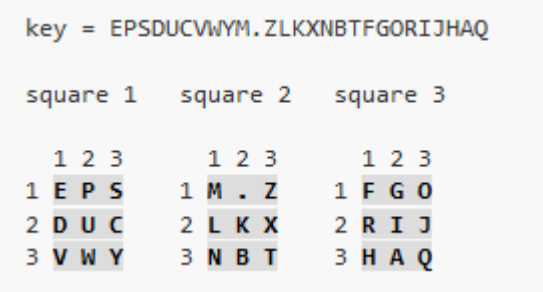


Slika 5. Primjer poruke zakrivene bifidskim sustavom (izvor: https://www.wattpad.com/933816164-codes-and-ciphers-bifid-cipher)

[17] Kahn, D. (1996.) The codebreakers: The comprehensive history of secret communication from ancient times to the internet, Simon & Schuster

[18] Machiavelo, A., Reis, R. (2006.)Automated cyphertext-only cryptanalysis of the bifid cipher, Faculdade de ciencias da universidade do Porto, 2 str

Pri zakrivanju poruke koristi se metoda supstitucije. Svako slovo mijenjaju dvije brojčane komponente koje označavaju njegov položaj unutar Polybiusovog kvadrata, točnije njegov red i stupac. Zatim dolazi do procesa transpozicije pri kojem se ovi parovi rastavljaju te tvore nove parove čiju je novu vrijednost moguće opet izvući iz Polybiusovog kvadrata[19].



Slika 6. Primjer trifidskih tablica s ključem (izvor: http://practicalcryptography.com/ciphers/trifid-cipher/)

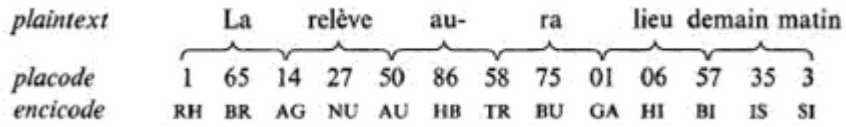
S druge strane, trifidska šifra je nešto naprednija i kompleksnija verzija temeljena na bifidskoj. Osnovni princip je to da se ranije određeni ključ upisuje u tablicu na početku dok preostala slova, ako ih ima, neizmijenjenim redoslijedom popunjavaju ostatak tablice. Razlika je u tome što trifidski sustav koristi tri tablice umjesto samo jedne (slika 6). Ovakav sistem ovu vrstu šifriranja čini relativno nepraktičnom za engleski pa čak i Delastelleov materinji francuski jezik, s obzirom na to da engleski i francuski imaju 26 slova dok tablice imaju 27 mjesta. Ovaj problem se obično rješava dodavanjem znaka točke ili plusa na preostalo prazno mjesto[20].

3.3 Tableau de concordance

Metode zakrivanja i raskrivanja poruka mijenjale su se i napredovale iz dana u dan tijekom rata, ovo je možda najviše vidljivo na primjeru francuske vojske i njihove tablice usklađenosti, odnosno *Tableau de concordance*. Prva verzija se pojavila na samom početku rata, 1914. godine. Dok je najpoznatija verzija 65 koja se pojavljuje 1915. godine. Zakrivanje pomoću ove verzije bilo je toliko kompleksno i napredno za ono vrijeme da su upute za ovaj kod sadržavale poruku "Iznimno, ako nemate vremena za potpunu enkripciju, šaljite poruku bez enkripcije." Zakrivanje bi funkcioniralo na temelju metode opkoračivanja tako što bi

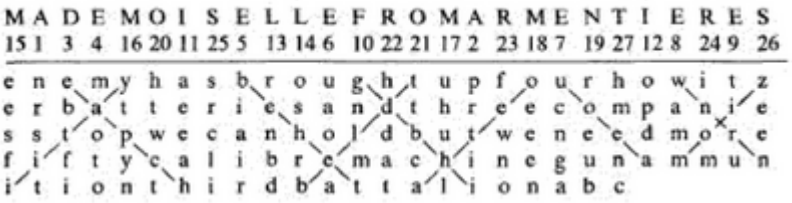
[19] Rošić, K. (2018.) Transpozicijske šifre, Sveučilište J. J: Strossmayera u Osijeku, Diplomski rad, 29 str.
[20] Delastelle, F. (1902.) Traite elementarie de cryptographie, Gauthier-Villars, 101-103 str.

poruka prvo bila prebačena u brojeve. Prva i posljednja znamenka u nizu bile bi zakrivene odvojeno dok bi znamenke između njih bile odvojene u parove te bi dobiveni brojevi tada bili opet prebačeni u slova (slika 7).



Slika 7. Primjer enkripcije putem Tableau de concordancea (Kahn, 1996.)

Upravo radi ove kompleksnosti, zakrivanje određenih poruka bilo je dozvoljeno alternativnom varijantom koja se koristila tablicom i ključem (slika 8). Ova varijanta je funkcionirala tako što bi se tekst upisivao vodoravno ispod iznimno dugog ključa, nakon čega bi se tekst iščitavao po nekoliko dijagonala koje određuje ključ. Nijemci su prvu poruku pisanu ovim kodom uspješno dešifrirali tek 1918[21].



Slika 8. Primjer poruke zakrivene alternativnom metodom Tableau de concordance (Kahn, 1996.)

3.4 Francuske kriptološke organizacije

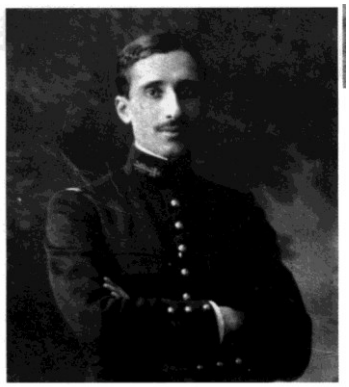
Francuska je u rat ušla kao jedna od spremnijih država, barem s gledišta kriptologije. Naime, kriptološki i kriptoanalitički uredi su u francuskoj primjenjivani u vojne svrhe još od doba Napoleona, kada je u njegovim osvajanjima od velike koristi bio čuveni *Cabinet noir* čija je primarna uloga bila presretanje i potencijalno dešifriranje pisama, čime će se nastaviti baviti i za vrijeme Prvog svjetskog rata[22]. Samim time, svi kriptografski zadaci bi se uvijek obavljali isključivo pod nadzorom vlade. U Francuskoj je čak postojala i specijalna policija zadužena

[21] Kahn, D. (1996.) The codebreakers: The comprehensive history of secret communication from ancient times to the internet, Simon & Schuster
[22] Andrew, C. (1968.) Theophile Delcasse and the makking of the Entente Cordiale: A reapraisal of the French foreign policy 1898-1905, 69 str.

isključivo za kriptoanalizu poznata pod nazivom *Surete generale*, u prijevodu Opća sigurnost. Početkom dvadesetog stoljeća, Francuzi osnivaju Vojnu kriptografsku komisiju, odnosno *Comission de cryptographie militarie*. Ova komisija se sastojala od vojnih lica koja su do tada pokazala izniman talent za kriptologiju te je odigrala ključnu ulogu tijekom Prvog svjetskog rata kada im je, uz kriptoanalizu neprijateljskih poruka, uloga bila osmišljanje šifri i kriptosustava za potencijalnu primjenu tijekom rata. Nedugo kasnije, komisija uz potporu Ministarstva rata stvara kompleksnu mrežu posebnih radio stanica čija je uloga bila prisluškivanje i presretanje neprijateljskih komunikacija. Redovno su provođena ispitivanja i vojne vježbe nad vojnicima u ovim postajama te nad samim članovima komisije kako bi se osigurala maksimalna efikasnosti obavljanja kriptografskih i kriptoanalitičkih zadataka tijekom rata[23].

3.5. Georges Painvin i probijanje ADFGVX koda

Rođen 1886. u Parizu, Georges Painvin (slika 9) tijekom svog ranog života nije pokazivao gotovo nikakvo zanimanje za tada još poprilično nepoznatu znanost kriptologije. 1905. godine Painvin, kako je bila tradicija njegove obitelji, upisuje Vojnu akademiju u Palaiseau te postaje vojni inženjer. Tijekom vojne službe u Prvom svjetskom ratu Painvin po prvi put dolazi u dodir s kriptologijom te ubrzo traži od narednika da se sve presretnute poruke njemačke vojske daju upravo njemu na kriptoanalizu. Nakon što je njegovo dešifriranje njemačkih poruka presudilo u okršajima neposredno nakon bitke na Marni, Painvin dobiva poziv za ulazak u *Cabinet noir* gdje će se zadržati do kraja rata[24].



Slika 9 Georges Painvin (izvor: https://www.annales.org/archives/x/painvinimages.html)

[23] Gylden, Y. (1935.) The contribution of the cryptographic bureaus in the World War, War department Washington, 9-14 str.
[24] Annales, Georges Jain Painvin URL: https://www.annales.org/archives/x/painvin.html [Pristupljeno 29.7.2022.]

3.5.1 Probijanje koda

Tijekom svoje službe u Cabinet noiru, Painvin je uspješno razotkrio brojne poruke te čak uspio u potpunosti otkriti princip njemačkog KRU kriptosustava. Međutim, njegov najveći podvig doći će 1918. godine pred sam kraj rata kad Painvin uspješno dešifrira ADFGX i ADFGVX kriptosustave.

"Francuzi su presreli 18 ADFGX poruka sa sveukupno 512 skupina od po pet slova. Dvije su poslane u tri dijela i Painvin je 4. travnja primijetio da su početci dvaju poruka imali identične dijelove teksta poredane istim redoslijedom. Ova neuobičajenost je najvjerojatnije mogla proizaći iz toga da oba kriptograma imaju identične početke transponirane prema istom ključu, identični dijelovi teksta bi tada predstavljali identične vrhove transpozicijske tablice. Odvajanje kriptograma tako da svaki identičan dio počinje novim segmentom dovelo bi do stupaca tablice, po redoslijedu transkripcije. Painvin je rastavio kriptograme tako da svaki identični dio započinje novi odjeljak. Ovi odjeljci su sastavljali stupce tablice po redu njihove transkripcije. Painvin je tada primijetio da su neki stupci dugi u oba kriptograma, neki kratki u oba, a neki dugi u jednom dok su kratki u drugom. Dugi stupci su najvjerojatnije stajali na lijevoj strani transpozicijske tablice. Ti brojevi su tada morali biti prvi u ključu za transponiranje. Painvin je tada napravio prvu aproksimaciju tog ključa. Vođen ovim razmišljanjem, posložio je ključne brojeve u zone unutar ključa. Zatim je stupce stavio jedne pored drugih i brojao dobivene parove slova. Većina kombinacija je bila neuspješna te nije pokazivala nikakva distinktivna obilježja. Ali neke su davale naznake monoalfabetske prirode. Ove kombinacije su predstavljale dva stupca koja su stajala jedan pored drugog u originalnoj tablici te su sadržavali digrafske zamjene s tablice. Na ovaj način Painvin je postepeno sagradio čitav transpozicijski ključ. Kada mu je to uspjelo, trebao je samo riješiti monoalfabetsku tablicu zamjene kako bi došao do izvornog teksta. Nakon 48 sati nevjerojatnog rada, Painvin je probio prve poruke najteže šifre koju je svijet do tada vidio." (Kahn, 1967.[25])

3.5.2 Radiogram pobjede

Nedugo nakon Painvinovog probijanja do tada najkompleksnijeg kriptosustava, Nijemci taj sustav čine još kompleksnijim te stvaraju ADFGVX kod. 1. lipnja jedna od francuskih radio stanica nailazi na poruku zakrivenu novim sustavom.

[25] Kahn, D. (1967.) The codebreakers: The story of secret writing, The Macmillan company, 157 str.

Poruka glasi:

FGAXA XAXFF FAFVA AVDFA GAXFX FAFAG DXGGX AGXFD XGAGX GAXGX AGXVF VXXAG XDDAX GGAAF DGGAF FXGGX XDFAX GXAXV AGXGG DFAGG GXVAX VFXGV FFGGA XDGAX FDVGG A

Painvin ubrzo shvaća da je razlika u tome što su dimenzije Polybiusovog kvadrata povećane s pet redova i stupaca na šest te da ovaj sustav koristi jedno slovo više dok se u tablici također nalaze brojevi od 0 do 9. Nakon 26 sati rada Painvin je sljedeći dan uspio probiti i ovaj kriptosustav te doći do poruke nakon čega se ruši od umora[26]. Tekst ove poruke glasi: "*Munitionierung beschleunigen Punkt Soweit nicht eingesehen auch bei Tag*" ("Ubrzajte opskrbu municijom. Ukoliko neprimijećeno i tijekom dana"). Izviđači iz zraka su potvrdili prijevoz municije tijekom dana za koju su Francuzi točno pretpostavili da je namijenjena za artiljerijsku baražu prije napada. U ponoć 9. lipnja počinje predviđen artiljerijski napad na koji su Francuzi sada bili spremni. 11. lipnja kreće francuski protunapad koji u potpunosti zaustavlja njemački prodor[27].

[26] Annales, Le radiogramme de la victorie URL: https://www.annales.org/archives/x/radiogramme.html [Pristupljeno 29.7.2022.]
[27] Kahn, D. (1967.) The codebreakers: The story of secret writing, The Macmillan company, 160-162 str.

4. Britanska kriptologija

4.1 Playfairova šifra

Rođen 1802. u malom predgrađu Barnwoodu, Sir Charles Wheatstone bio je jedan od najvećih engleskih umova 19. stoljeća. Pripisuju mu se brojni revolucionarni izumi kao što su stereoskop, engleska koncertina te najranija verzija električnog telegrafa. Upravo Wheatstoneov izum telegrafa dovesti će do njegovog najvećeg doprinosa kriptologiji nakon udruživanja s prijateljem barunom Lyonom Playfairom. 1854. godine, tražeći način za sigurnu komunikaciju putem telegrafa Wheatstone i Playfair osmišljaju tzv. Playfairovu šifru. Riječ je o prvom digrafskom kriptosustavu u povijesti, odnosno sustavu koji šifrira slova u parovima tako da rezultat ovisi o oba slova, što je bila iznimno napredna ideja za ono vrijeme. Ovaj sustav je prvi put upotrebljen u vojne svrhe tijekom Drugog burskog rata, dok je za vrijeme Prvog svjetskog rata bio službeni kriptosustav britanske vojske[28]. Playfairova šifra funkcionira na principu 5x5 matrice (slika 10) koja se konstruira unošenjem ključne riječi na početak te ispisivanjem preostalih slova abecede unutar matrice nakon ključne riječi.

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

Slika 10. Matrica Playfairove šifre s ključnom riječi Monarchy (izvor: https://sodocumentation.net/cryptography/topic/8869/playfair-cipher)

[28] Kahn, D. (1967.) The codebreakers: The story of secret writing, The Macmillan company, 113-118 str.

Šifriranje putem Playfairova sustava funkcionira tako što se nezakriveni tekst prvo dijeli na blokove od po dva slova, s time da se dva ista slova ne smiju nalaziti u istom bloku te da broj slova mora biti paran, što se postiže potencijalnim umetanjem slova x. Zatim se gleda položaj parova slova unutar ranije određene matrice te ako su slova unutar istog reda tada svako slovo mijenja ono njemu s desne strane, ako su unutra istog stupca slovo mijenja ono ispod njega te ako slova ne dijele niti red niti stupac slaže se pravokutnik koristeći njihove položaje kao vrhove te slova mijenjanju ona slova koja se nalaze u druga dva kuta pravokutnika. Dok je raskrivanje poruke samo pitanje obrnutog postupka [29].

"Wheatstone i Playfair objasnili su šifru podsekretaru Ministarstva vanjskih poslova, bez sumnje upućujući na glavnu prednost, da dva para koja dijele slovo ne moraju pokazivati ni najmanju sličnost nakon šifriranja... Nadalje, kada se šifriranje svlada, proces napreduje s nevjerojatnom lakoćom i brzinom. Kada je podsekretar napomenuo da je sistem prekompliciran, Wheatstone je ponudio pokazati da bi ga tri od četiri dječaka iz obližnje osnovne škole mogla naučiti u 15 minuta. Podsekretar nije bio zadovoljan. "To je možda i moguće," rekao je, "ali nikada ne biste mogli naučiti atašee." Playfair je ostao entuzijastičan i odgovorio da je to bolji prikaz diplomata nego same šifre." (Kahn, 1967.[30])

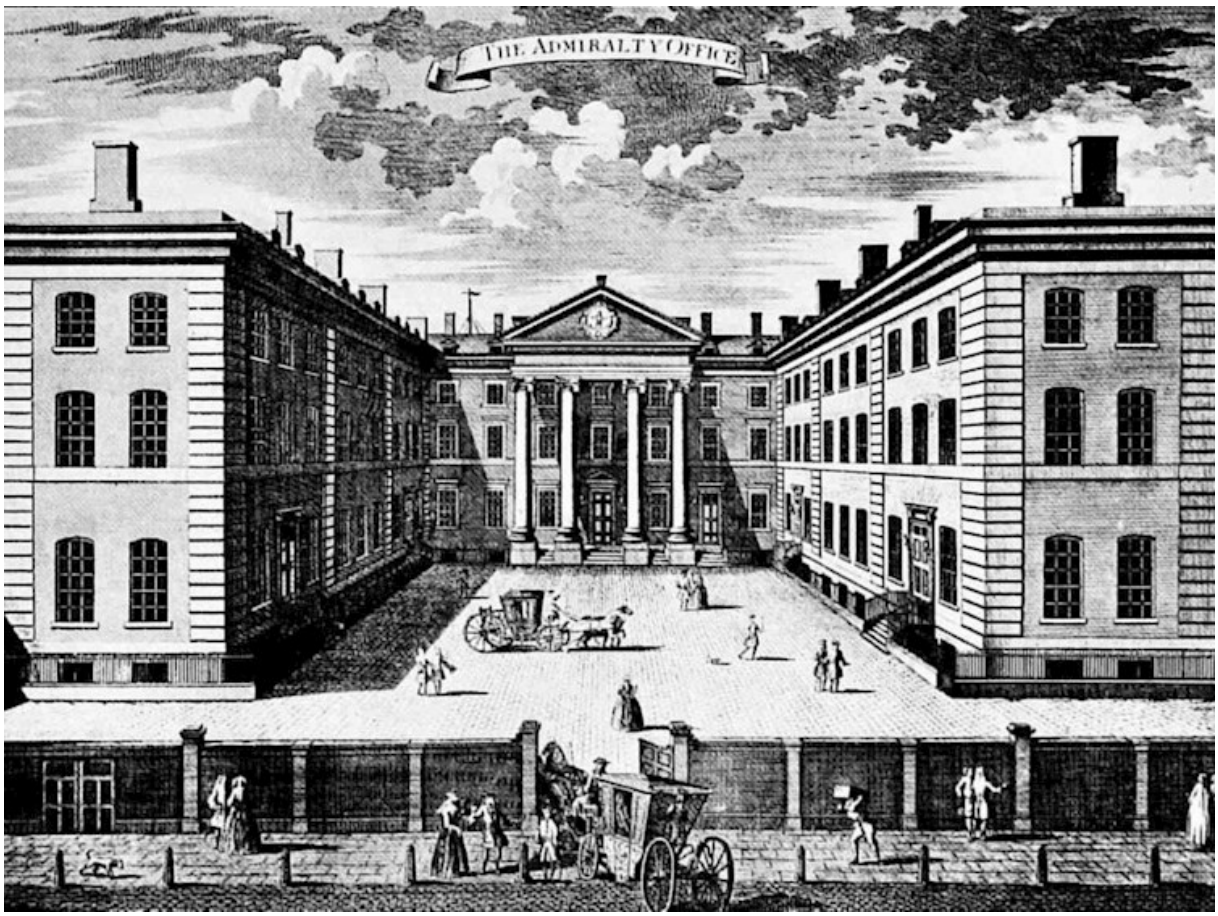
4.2 Britanske kriptološke organizacije

Iznimno malo je poznato o britanskim kriptoanalitičarskim podvizima prije početka Prvog svjetskog rata. Najveći razlog tome jest činjenica da vojna kriptoanalitičarska organizacija nije niti postojala, nadalje, britanska literatura o samoj znanosti kriptologije u to doba bili je blago rečeno minimalna. Vjeruje se da su Scotland Yard i Ministarstvo vanjskih poslova po potrebi tražili pomoć francuskih stručnjaka na području kriptologije. Međutim, tek na početku samog rata Britanci, opet po uzoru na Francuze, osnivaju svoje prve kriptoanalitičke organizacije[31]. Tako kao dio Britanske vojne obavještajne službe, tada MI1, nastaje odjel MI1b zadužen isključivo za presretanje poruka i njihovu kriptoanalizu. Dok kao dio Britanske ratne mornarice nastaje *Room* 40, odnosno Soba 40. Upravo će ova organizacija odigrati ključnu ulogu za sam ishod Prvog svjetskog rata.

[29] Knežević, M. (2015.) Vigenereova i Playfairova šifra, Svečilište J. J. Strossmayera u Osijeku, Završni rad, 18-20 str.
[30] Kahn, D. (1967.) The codebreakers: The story of secret writing, The Macmillan company, 117 str.
[31] Gylden, Y. (1935.) The contribution of the cryptographic bureaus in the World War, War department Washington, 19-20 str.

4.2.1 Room 40

Nazvan po sobi na prvom katu zgrade Britanske ratne mornarice (slika 11) u kojoj su obavljali svoju dužnost, *Room* 40 je bio kriptološki tim sastavljen od najvještijih kriptoanalitičara koje je britanska vojska tada imala za ponuditi. Osnovana pod vodstvom Sir Jamesa Alfreda Ewinga, *Room* 40 nastaje kao dio velikog projekta modernizacije britanske mornarice početkom Prvog svjetskog rata[32].



Slika 11. Zgrada Britanske ratne mornarice za vrijeme Prvog svjetskog rata (izvor: https://www.thehistorypress.co.uk/articles/the-forgotten-codebreakers-of-the-first-world-war/)

Tijekom čitavog rata *Room* 40 ekipa je operirala u potpunoj tajnosti te je samo postojanje ove kriptoanalitičke skupine bila tajna. Navodno je i sama soba bila na nedostupnom položaju, što je dovodilo do toga da ju novi članovi jedva uspijevaju pronaći. S obzirom na to da sami kriptoanalitičari nisu imali pristup svim informacijama koje ratna mornarica posjeduje,

[32] The history press, The forgotten codebreakers of The First World War URL: https://www.thehistorypress.co.uk/articles/the-forgotten-codebreakers-of-the-first-world-war/ [Pristupljeno 30.7.2022.]

admiral Herbert Hope dobio je ulogu pregledavanja dešifriranih poruka i uspoređivanja dobivenih informacija s onima koje mornarica već posjeduje. Stoga su rezultati rada *Room* 40 ekipe bili dostupni samo direktoru obavještajne službe Henryu Oliveru te samom Hopeu[33]. Potrebno je napomenuti da su, radi britanskog zapostavljanja kriptoanalize, svi članovi *Room* 40 ekipe bili iznimno neiskusni, nekima su čak ovo bila prva iskustva s kriptologijom. Tek mjesec dana nakon osnivanja, neiskusnu *Room* 40 ekipu je zatekla nevjerojatna sreća. Njemački bojni kruzer *Magdeburg* se, zahvaljujući lošim vremenskim uvjetima, nasukao na grebenu u Baltičkom moru. *Magdeburg* ubrzo zauzima posada obližnjeg ruskog torpednog čamca te u kapetanovoj kabini nalaze njemačku knjigu šifri, pod nazivom *Signalbuch der Kaiserlichen Marine* (SKM), koju ubrzo prosljeđuju Britancima. Međutim, britanski kriptoanalitičari su bili toliko neiskusni da čak ni s ovom knjigom nisu imali znatno veće uspjehe s dešifriranjem njemačkih poruka[34].

"Ali čak ni ovaj neočekivani prihod sreće, najsretniji u čitavoj povijesti kriptologije, nije omogućio Ewingovoj ekipi čitanje poruka njemačke mornarice, jer se četveroslovne kodne riječi iz knjige nisu pojavljivale u porukama. Napokon, Charles J. E. Rotter otkrio je da je kod dodatno zakriven monoalfabetskom supstitucijom. Rješavanje ovakvog zakrivanja nije velik problem ako u svom posjedu imate knjigu šifri. Kao i u nezakrivenom tekstu, određene kodne riječi se pojavljuju češće od ostalih i u sličnom okruženju, slova u jednoj kodnoj riječi pojavljuju se u ostalima drugačijim poretkom te same kodne riječi posjeduju određena strukturalna obilježja, u slučaju njemačke pomorske šifre, suglasnici su se mijenjali samoglasnicima unutar četveroslovnih kodnih riječi. Kada su ova obilježja poznata, kriptoanalitičar ih može prepoznati gotovo jednako dobro kao i u standardnom jeziku te ih iskoristiti za rješavanje zakritka." (Kahn, 1967.[35])

Otprilike tri tjedna nakon ove spoznaje, Ewingov *Room* 40 tim je konačno počeo dešifrirati njemačke poruke. Od ovog je trenutka njihova efikasnost samo nastavila rasti, s obzirom na to da je izgubljena knjiga šifri bila suviše velika i opširna da bi ju njemačka vojska odmah zamijenila. Dva mjeseca kasnije, krajem 1914. godine, Britanci se uspijevaju domoći još dvije knjige šifri. Prve kada njemački brod *Hobart*, ne znajući da je rat uopće počeo, biva zauzet u blizini Australije. U posjedu *Hobartova* kapetana, Britanci nalaze *Handelsverkehrsbuch* (HVB) knjigu šifri, namijenjenu za komunikaciju njemačke flote s trgovačkim brodovima. Do

[33] Beesly, P. (1983.) Room 40: British naval intelligence 1914-1918, Hamish Hamilton, 15-20 str.
[34] Johnson, T. R. (2008.) The sting – Enabling codebreaking in the twentieth century, Cryptologic quarterly, 45 str.
[35] Kahn, D. (1967.) The codebreakers: The story of secret writing, The Macmillan company, 129-130 str.

druge knjige Britanci dolaze nakon potapanja razarača SMS S119, međutim u bitci na rijeci Yser sama britanska flota u čijem je posjedu knjiga još uvijek bila je također bila potopljena. Tako *Verkehrsbuch* (VB), knjiga šifri namijenjena za časnike njemačke mornarice, dolazi u posjed *Room* 40 kriptoanalitičara tek mjesec dana kasnije kada ju je lokalni ribar slučajno pronašao. Ovaj događaj je, prema epizodi iz Biblije, dobio naziv "čudesni ulov riba". Tri spomenute knjige neće biti zamijenjene naredne dvije godine, što je britanskim kriptoanalitičarima neizmjerno išlo na ruku[36]. Tijekom ovog perioda Sir James Alfred Ewing odlazi u mirovinu te ga mijenja William R. Hall, poznat pod nadimkom *Blinker*. Upravo pod njegovim vodstvom *Room* 40 tim će doći do svog najvećeg uspjeha, dešifriranja Zimmermannovog telegrama.

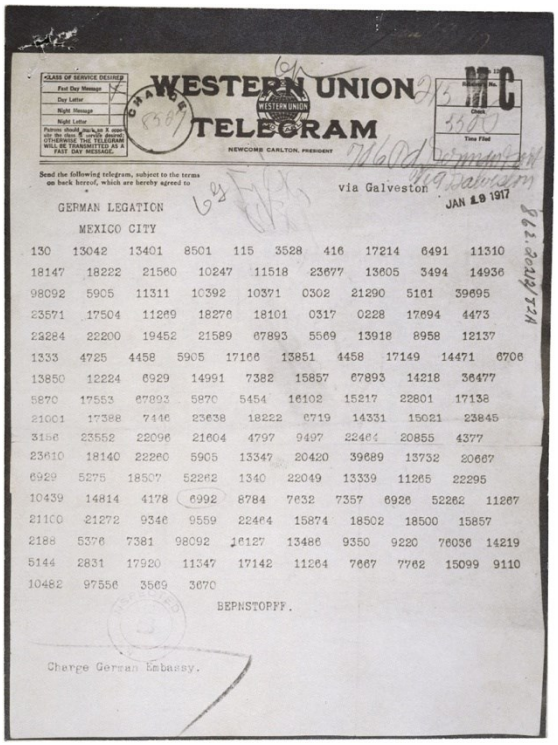
4.2.2 Zimmermannov telegram

1917. godine rat je postao iznimno usporen, prije svega radi nemogućnosti obje strane da dođu do ključne pobjede kojom bi tijek rata okrenuli u svoju korist. Nijemci su vjerovali da bi do ovoga moglo doći kada bi zaustavili opskrbu Britanaca i Francuza američkim oružjem, dok bi aktivan ulazak SAD-a u rat za Nijemce bio katastrofalan. Stoga njemački državni tajnik vanjskih poslova Arthur Zimmermann šalje telegram Johannu Heinrichu von Bernstorffu, njemačkom ambasadoru u SAD-u. Sadržaj telegrama je sljedeći:

"Prvog veljače planiramo započeti s neograničenim podmorničkim ratovanjem. Nastojati ćemo bez obzira na ovo zadržati Sjedinjene Američke Države neutralnima. U slučaju da ovo ne uspije, dajemo Meksiku prijedlog savezništva na sljedećim osnovama: ratujemo zajedno, zajedno smo u miru, velikodušnu financijsku potporu i razumijevanje s naše strane da će Meksiko zauzeti Teksas, Novi Meksiko, i Arizonu. Detalje dogovora ostavljamo vama. Informirat ćete predsjednika o gore navedenom na što tajniji način čim izbijanje rata sa Sjedinjenim Američkim Državama bude jasno i dodati prijedlog da bi trebao, po vlastitoj inicijativi, pozvati Japan na neposredno priključivanje i istovremeno posredovati između Japana i nas. Molimo vas dajte predsjedniku do znanja da bešćutna upotreba naših podmornica sada nudi mogućnost prisiljavanja Engleske na primirje unutar nekoliko mjeseci.[37]"

[36] Beesly, P. (1983.) Room 40: British naval intelligence 1914-1918, Hamish Hamilton, 3-28 str.
[37] Friedman, W. F. (1938.) The Zimmermann telegram of January 16, 1917, and it's cryptographic background, War department office of the chief signal officer Washington, 1 str.

Telegram je poslan 16. siječnja s očitim ciljem zaustavljanja američkog utjecaja na rat u kojem nisu aktivno sudjelovali. Ova ponuda će na kraju doći do Meksikanaca koji su tada bili usred građanskog rata te napad na SAD nikako nije bio unutar njihovih mogućnosti. Međutim, prije dolaska do svog cilja telegram će završiti u rukama Britanske obavještajne službe. 17. siječnja dva člana *Room* 40 tima, William Montgomery i Nigel de Grey dolaze do Williama Halla s djelomično dešifriranom porukom koju su smatrali iznimno bitnom. Poruka je bila šifrirana u 0075 kodu koji su Nijemci počeli koristiti 1916. Međutim, bio je baziran na ranijim verzijama sličnog koda koje su Britanci, imajući u posjedu tri njemačke knjige šifri, sada znali[38]. Nakon dešifriranja čitavog telegrama Britanci ga prosljeđuju američkom predsjedniku Thomasu Woodrow Wilsonu. Amerikanci šalju telegram u meksičku ambasadu te ga nedugo nakon toga i javno objavljuju (slika 12). Reakcija američkog naroda je bila burna te je ubrzo sam Zimmermann bio prisiljen potvrditi autentičnost telegrama. U strahu od neograničenog podmorničkog ratovanja koje je telegram najavio, Amerikanci počinju naoružavati svoje trgovačke brodove koji plove za Europu, a 6. travnja 1917. godine SAD objavljuje rat Njemačkoj[39].



WESTERN UNION TELEGRAM

NEWCOME CARLTON, PRESIDENT

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
23284 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 7446 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.

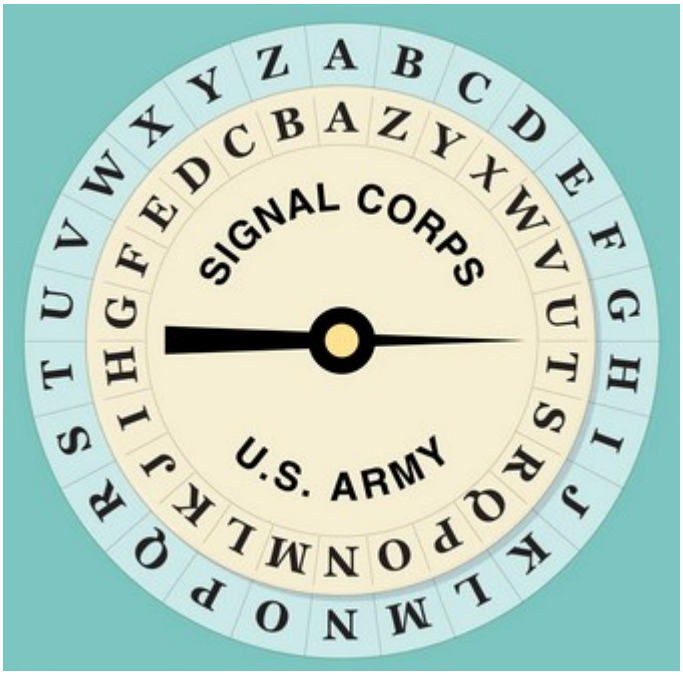
Slika 12. Šifrirana verzija Zimmermannovog telegrama poslana u Meksiko (izvor: https://www.theworldwar.org/learn/about-wwi/zimmermann-telegram)

[38] Kahn, D. (1967.) The codebreakers: The story of secret writing, The Macmillan company, 132-135 str.
[39] Meyer, M. C. (1966.) The Mexican-German conspiracy of 1915, The America 23(1), 76-89 str.

5. Američka kriptologija

5.1 Američke vojne šifre

Američka je vojska u rat ušla iznimno nepripremljena s kriptološkog gledišta. S obzirom na to da u rat ulaze tek 1917. godine, Amerikanci su lekciju o ključnoj ulozi kriptologije na bojištu naučili znatno kasnije od ostalih zaraćenih zemalja. Pri svom dolasku u Francusku, Amerikanci su koristili improvizirane kodove koje bi smišljali sami vojnici na bojištu te vojni disk za šifriranje (slika 13) za kojeg se pretpostavlja da je prvi put upotrebljen u 16. stoljeću.



Slika 13. Prikaz američkog vojnog diska za šifriranje (izvor: https://www.britannica.com/topic/cipher-disk)

Shvativši svoj zaostatak, Amerikanci preuzimaju Playfairovu šifru od Britanaca. U prosincu 1917. godine Amerikanci osnivaju tzv. Odjel za kompilaciju kodova te počinju osmišljati vlastite vojne šifre i kriptosustave. Prvi osmišljeni sustavi su očekivano bili iznimno jednostavni te samim time nisu donijeli veće uspjehe. Međutim, kako će rat dalje napredovati tako će se nastaviti razvijati i američka kriptologija.[40]

[40] Friedman, W. F. (1942.) American army field codes in the american expeditionary forces during The First World War, War department Washington, 1-14 str.

5.1.1 River i Lake kodovi

1918. godine američka vojska uvodi seriju *River* i *Lake* kodova. Riječ je o dvodjelnim kodovima od kojih je prvi bio Potomac kod, nakon čega se serija nastavila ažurirati s ponekad više od tri nova koda mjesečno. Potomac kod se sastojao od preko 1800 šifriranih riječi te je dolazio s knjižicom uputa od 47 stranica. Cilj uvođenja ovog koda bilo je minimaliziranje i pojednostavljivanja posla oko zakrivanja i raskrivanja poruka vojnika na prvoj crti, dok je sigurnost bila zagarantirana redovnim ažuriranjem koda, kako bi se osigurao što manji broj presretnutih poruka u jednom kodu. Ovaj plan se pokazao iznimno dobro promišljenim kada je jedna od knjižica uputstava za Potomac došla u ruke Nijemaca te su u roku dva dana dva nova koda postala aktivna i zamijenila Potomac. Prilikom smišljanja novih kodova i pisanja njihovih knjižica uputstava američki kripto stručnjaci su radili na principu sedam ranije određenih stavaka koje je bilo potrebno maksimizirati kako bi se stvorio što efikasniji kod, spomenute stavke su:

- vidljivost tiska, radi potencijalne slabe osvijetljenosti na bojištu
- jednostavnost operacije, na ovaj način su nastojali smanjiti broj mogućih pogrešaka pri kodiranju
- veličina kodne knjižice, kako bi s njom bilo što lakše rukovati
- vokabular, morao je biti dovoljno širok za svu potrebnu komunikaciju, ali ne suviše i nepotrebno opširan
- kvaliteta papira, kvaliteta je morala biti dovoljno dobra da bi papir izdržao predviđeni kratki životni vijek knjižice, ali također dovoljno loša radi brzog uništavanja knjižice u svrhu sprječavanja njenog dolaska u neprijateljske ruke
- dovoljan broj varijacija izraza, kako ne bi došlo do nepotrebnih repeticija i korištenja čestih izraza prilikom kodiranja
- određeni naglašeni segmenti, kako bi vojnici lakše zapamtili kodne riječi i određene korake pri zakrivanju

Nakon Potomaca slijedile su Suwanee, Wabash, Mohawk, Allegheny, Hudson, Colorado, Champalin, Huron, Osage, Seneca, Niagara, Michigan te je posljednja bila Rio Grande šifra. Na koricama svake knjižice bi velikim crvenim slovima, radi lakšeg pamćenja, bila ispisana kodna riječ “DAM“, šifra koja se šalje ukoliko je knjižica izgubljena. Dok je svaka verzija

koda također imala svoju skraćenicu (npr. POT, HUD ili COL) u slučaju da su istovremeno u upotrebi dva ili više koda[41].

5.1.2 Code talkeri

"21. kolovoza 1918, britanska vojska je počela napadati njemačke položaje uzduž dionice od 10 milja na zapadnom bojištu u sjeverozapadnoj Francuskoj. Ovaj napad je bio dio druge bitke na Sommi. Zajedno s britanskim trupama na tom području bile su i 119. i 120. SAD-ova pješačka pukovnija, koje su obje sadržavale velik broj vojnika iz Cherokee plemena iz Sjeverne Karoline. Tijekom rujna i listopada, dok je ofenziva napredovala i trajale su pripreme za prodor kroz njemačke obrambene položaje na Hindenburgovoj liniji, zapovjednici na ovom području su otkrili da njemački vojnici prisluškuju njihovo komuniciranje putem telefona. Nijemci bi tada koristili te poruke kako bi otkrili Savezničke položaje i napali ih. U tom trenutku su Cherokeeji stupili na scenu. Časnici su pretpostavili da Nijemci neće moći razumjeti jezik Cherokeeja, stoga su uputili vojnike Cherokeeje da šalju poruke telefonom na svom jeziku." (NC department of natural and cultural resources, 2016.[42])

Ovo je bio prvi zabilježeni primjer upotrebe jedne od najkreativnijih i najefikasnijih kriptoloških metoda u povijesti, jezika indijanskih *code talkera*. Nedugo kasnije počela je intenzivna upotreba jezika Choctaw vojnika (slika 14) za zakrivanje poruka.

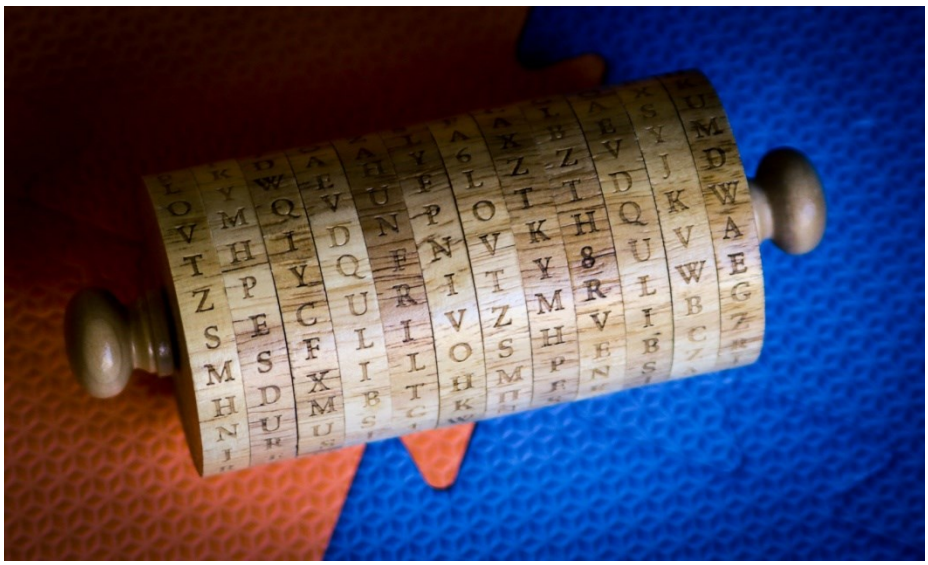
Slika 14. Code talkeri iz plemena Choctaw (izvor: https://www.worldwar1centennial.org/index.php/american-indians-in-ww1-code-talkers.html)

[41] Friedman, W. F. (1942.) American army field codes in the american expeditionary forces during The First World War, War department Washington, 17-19 str.
[42] NC department of natural and cultural resources, Cherokee codetalkers and Allied success in World War 1 URL: https://www.ncdcr.gov/blog/2016/08/21/cherokee-code-talkers-and-allied-success-wwi [Pristupljeno 31.7.2022.]

Korištenje Choctaw jezika za zakrivanje poruka navodno je započelo nakon što je američki časnik načuo dva Choctaw vojnika kako razgovaraju i došao do zaključka da je nemoguće dokučiti o čemu govore. Donesena je odluka da svaki bataljon mora imati barem jednog vojnika iz Choctaw plemena radi međusobne komunikacije. Međutim, u indijanskim jezicima nisu postojale riječi za brojne osnovne vojne pojmove. Ovaj problem je riješen tako što bi *code talkeri* koristili izraze kao što su "velika puška" za artiljeriju, "mala puška koja brzo puca" za mitraljez, "kamen" za granatu itd. Nakon uspješno provedene akcije povlačenja iskomunicirane isključivo na Choctaw jeziku, počela je upotreba jezika brojnih drugih indijanskih plemena za komunikaciju. Jedan od zarobljenih njemačkih vojnika otkrio je kako njihovi kriptoanalitičari nisu bili niti blizu uspjehu pri dešifriranju poruka na indijanskim jezicima[43].

5.2 Jeffersonov disk

Jeffersonov disk (slika 15) jedan je od kriptoloških sustava na kojem će američka vojska bazirati svoje nove kriptosustave kroz čitavu prvu polovicu 20. stoljeća pa čak i u vrijeme pojave kripto strojeva. Riječ je o načinu zakrivanja poruka koji je osmislio Thomas Jefferson između 1790. i 1800. godine, dok ga je kasnije unaprijedio Etienne Bazeries, jedan od članova francuskog *Cabinet noira*.



Slika 15. Jeffersonov disk (izvor: https://uvasrg.github.io/category/disk-processing.html)

[43] The United States World War 1 centennial commission, Native American code talkers during World War 1 URL: https://www.worldwar1centennial.org/index.php/american-indians-in-ww1-code-talkers.html [Pristupljeno 31.7.2022.]

Jeffersonov originalni dizajn je imao 36 kotačića na samom disku, broj mogućih kombinacija na ovakvom disku imao bi 42 znamenke. Zakrivanje funkcionira tako što se originalni tekst upisuje u sam disk okretanjem kotačića te se zatim odabire jedan od ostalih redova na disku kao zakriveni tekst. Položaj reda na kojem se nalazi zakriveni tekst u ovom slučaju igra ulogu ključa te je on naravno poznat pošiljatelju. Bilo bi poželjno kada bi bio poznat i primatelju, međutim Jeffersonov disk je jedan od rijetkih kriptosustava u kojem ovo nije nužno, s obzirom na to da primatelj nakon upisivanja zakritka može samo pregledati sve strane diska dok ne pronađe poruku. Jefferson ovaj koncept nikada nije predložio američkoj vojsci te će Amerikanci za njega saznati tek krajem Prvog svjetskog rata, prilikom pregleda Jeffersonovih spisa u Kongresovoj knjižnici. Ubrzo nakon ovoga, Amerikanci počinju konstruirati nešto modernije kriptosustave na temelju Jeffersonovog[44]. Jedan od ovakvih izuma je M-94 šifra. 1919. godine, nakon završetka Prvog svjetskog rata major Joseph Mauborgne šalje prvih 25 slova 25 različitih zakrivenih poruka u dva američka kriptološka ureda. Ove poruke, čak i nakon nekoliko savjeta od samog majora Mauborgnea, nitko nije uspio riješiti. Ovakav ishod naveo je Mauborgnea da nastavi s razvojem svog izuma kojem je dao naziv M-94. Ovaj kriptosustav će ostati u službi američke vojske punih 10 godina, sve do izuma nove M-138-A verzije čija će upotreba trajati sve do 1942. godine[45].

5.3 Američka crna komora

5. srpnja 1918. godine, Herbert Osborn Yardley, jedan od najuspješnijih američkih kriptologa za vrijeme Prvog svjetskog rata, postaje voditelj krila za kriptologiju i kriptoanalizu američke obavještajne organizacije M.I.8. Od svog osnivanja pa do kraja rata, ova organizacija napreduje iznimno velikom brzinom. Tijekom vremena provedenog u Europi, Yardley je pomno promatrao rad britanskih i francuskih kriptoloških organizacija, s ciljem održavanja daljnjeg razvoja kriptologije u SAD-u. Međutim, nakon završetka rata dolazi do masovnog raspuštanja vojnog osoblja unutar američke vojske, što dovodi do gotovo potpunog raspada kriptološkog krila M.I.8. Vidjevši ovo, Yardley nastoji nagovoriti direktora M.I.8 na osnivanje trajne kriptološke i kriptoanalitičke organizacije, pritom navodeći kako su američki kriptolozi tijekom rata uspješno dešifrirali više od 11000 neprijateljskih poruka. 17. svibnja 1919. godine Yardleyev je prijedlog odobren te dva dana kasnije nastaje kriptološki ured pod

[44] Kahn, D. (1967.) The codebreakers: The story of secret writing, The Macmillan company, 111-113 str.
[45] Friedman, W. F. (1965.) Six lectures on cryptology, National cryptologic school, 145-149 str.

nazivom *American black chamber*, odnosno Američka crna komora[46]. Prvi zadatak Crne komore bilo je probijanje šifri koje koristi vojska Japana, s kojim su tenzije iz dana u dan rasle. Yardley i njegov tim kriptoanalitičara je s ovim zadatkom imao znatno više poteškoća nego su predvidjeli. Međutim, uspijevaju otkriti da Japanci poruke zakrivaju tako što svoje pismo *katakana* prepisuju na latinicu te ih zatim kodiraju tzv. *Ja* kodom. Tijekom 1921. godine, Crna komora uspješno dešifrira telegram koji je japanski ambasador slao u Tokio te u njemu govorio o nadolazećoj konferenciji za globalno razoružavanje. Yardley je ovaj telegram kasnije prozvao najvažnijim telegramom koji je ikada dešifrirao. Daljnji zadatak Crne komore bio je praćenje svih komunikacija vezanih za spomenutu konferenciju te su tijekom narednih mjeseci uspješno dešifrirali više od 5000 poruka, što je brojne članove kriptoanalitičkog tima kao i samog Yardleya dovelo do ruba ludila. Iz godine u godinu, financiranje Crne komore se smanjivalo, dok je 1924. otpušteno više od pola kriptološkog tima. Yardley tvrdi da je državna potpora tijekom ovog perioda bila toliko mala da je često bio prisiljen na ilegalan način dolaziti do poruka za kriptoanalizu. Bez obzira na to, Yardley tvrdi da je Crna komora u ovom periodu dešifrirala više od 45000 poruka te otkrila kriptosustave 19 različitih država. 31. listopada 1929. godine, nakon stupanja Herberta Hoovera na mjesto predsjednika, dolazi do zatvaranja Crne komore. Američka vlada organizira novi kriptoanalitički ured tek tri godine kasnije. 1931. godine, Yardley objavljuje knjigu *The American black chamber* u kojoj detaljno opisuje stanje američke kriptologije te rad samog kriptološkog tima Crne komore. Ovakvo otkrivanje državnih tajni do tada je bila neviđena pojava te je izazvalo burnu reakciju unutar M.I.8. Knjiga je doživjela izniman uspjeh te ju se i danas često opisuje kao jednu od najvažnijih knjiga u povijesti kriptologije[47].

[46] NSA, The many lives of Herbert O. Yardley URL: https://www.nsa.gov/portals/75/documents/news-features/declassified-documents/cryptologic-spectrum/many_lives.pdf [Pristupljeno 1.8.2022.]
[47] Kahn, D. (1967.) The codebreakers: The story of secret writing, The Macmillan company, 169-180 str.

6. Zaključak

Cilj ovog rad bio je prikazati stanje kriptologije prije početka, za vrijeme te nakon Prvog svjetskog rata. Nakon kratkog uvoda, rad se bavi njemačkim, francuskim, britanskim i američkim kriptosustava, kriptološkim organizacijama te ključnim osobama i događajima s gledišta kriptologije. Prvi svjetski rat je velesilama svijeta prikazao na vrlo jasan način neupitnu važnost kriptologije u ratnom okruženju, natjerao ih na stvaranje i daljnji razvoj vlastitih kriptosustava te na školovanje vlastitih kriptoanalitičara. Niti jedan drugi događaj u povijesti nije imao ovakav utjecaj na jednu znanstvenu disciplinu i na njen položaj u kulturi. Brojni sudionici Prvog svjetskog rata u njega su ušli u potpunosti nepripremljeni, zanemarujući kriptologiju kao znanost te bez načina zakrivanja vlastitih i raskrivanja neprijateljskih poruka. U razdoblju od 1914. godine pa nadalje sve će se ovo promijeniti. Pojavili su se brojni novi kriptosustavi, neki s iznimnim uspjehom, a neki s nešto manjim. Dodatno su razvijene i modernizirane brojne stare kriptološke metode kao što su Playfairova šifra ili Jeffersonov disk. Zimmermanov telegram, Radiogram pobjede i slični događaji obilježili su sam rat i utjecali na daljnji tok čovjekove povijesti, dok su organizacije kao što su *Room* 40 ili *American black chamber* stvorile put za daljnji razvoj kriptologije kako u vojne tako i u brojne druge svrhe.

7. Literatura

1. Andrew, C. (1968.) Theophile Delcasse and the makking of the Entente Cordiale: A reapraisal of the French foreign policy 1898-1905
2. Annales, Georges Jain Painvin URL: https://www.annales.org/archives/x/painvin.html [Pristupljeno 29.7.2022.]
3. Annales, Le radiogramme de la victorie URL: https://www.annales.org/archives/x/radiogramme.html [Pristupljeno 29.7.2022.]
4. Beesly, P. (1983.) Room 40: British naval intelligence 1914-1918, Hamish Hamilton
5. Crypto museum, How did an Enigma machine work URL: https://www.cryptomuseum.com/crypto/enigma/working.htm [Pristupljeno 28.7.2022.]
6. Delastelle, F. (1902.) Traite elementarie de cryptographie, Pariz, Gauthier-Villars
7. Derenčin, R. (2016.) Enigma i njemačke podmornice u Drugom svjetskom ratu, Polemos 19
8. Ellis, C. (2005.) Exploring the Enigma, University of Cambridge
9. Friedman, W. F. (1942.) American army field codes in the american expeditionary forces during The First World War, War department Washington
10. Friedman, W. F. (1935.) Field codes used by the German army during the World War, War department office of the chief signal officer
11. Friedman, W. F. (1965.) Six lectures on cryptology, National cryptologic school
12. Friedman, W. F. (1938.) The Zimmermann telegram of January 16, 1917, and it's cryptographic background, War department office of the chief signal officer Washington
13. Gannon, P, The forgotten codebreakers of The First World War, The history press URL: https://www.thehistorypress.co.uk/articles/the-forgotten-codebreakers-of-the-first-world-war/ [Pristupljeno 30.7.2022.]
14. Gylden, Y. (1935.) The contribution of the cryptographic bureaus in the World War, War department Washington
15. Hamilton, R. F, Herwig, H. H. (2005.) The origins of World War 1, War in history 12(1)

16. Johnson, T. R. (2008.) The sting – Enabling codebreaking in the twentieth century, Cryptologic quarterly
17. Kahn, D. (1980.) Codebreaking in World Wars 1 and 2: The major successes and failures, their causes and their effects, Cambridge university press
18. Kahn, D. (1996.) The codebreakers: The comprehensive history of secret communication from ancient times to the internet, Simon & Schuster
19. Kahn, D. (1967.) The codebreakers: The story of secret writing, The Macmillan company
20. Knežević, M. (2015.) Vigenèreova i Playfairova šifra, Svečilište J. J. Strossmayera u Osijeku, Završni rad
21. Kulp, J., Poulter, W. (n.d.) The ADFGVX cipher, Lakehead University
22. Machiavelo, A., Reis, R. (2006.) Automated cyphertext-only cryptanalysis of the bifid cipher, Faculdade de ciencias da universidade do Porto
23. Marshall, A. (2004.) Russian Military Intelligence, 1905–1917: The Untold Story behind Tsarist Russia in the First World War, War in History 11(4)
24. Math PMF, Vigenèreova šifra URL: https://web.math.pmf.unizg.hr/~duje/kript/vigener.html [Pristupljeno 28.7.2022.]
25. Meyer, M. C. (1966.) The Mexican-German conspiracy of 1915, The America 23(1)
26. NC department of natural and cultural resources, Cherokee codetalkers and Allied success in World War 1 URL: https://www.ncdcr.gov/blog/2016/08/21/cherokee-code-talkers-and-allied-success-wwi [Pristupljeno 31.7.2022.]
27. NSA, The many lives of Herbert O. Yardley URL: https://www.nsa.gov/portals/75/documents/news-features/declassified-documents/cryptologic-spectrum/many_lives.pdf [Pristupljeno 1.8.2022.]
28. 27. Rošić, K. (2018.) Transpozicijske šifre, Sveučilište J. J: Strossmayera u Osijeku, Diplomski rad
29. Simmons, G. J, Vigenère cipher, Encyclopedia Britannica URL: https://www.britannica.com/topic/Vigenere-cipher [Pristupljeno: 28.7.2022.]
30. The United States World War 1 centennial commission, Native American code talkers during World War 1 URL: https://www.worldwar1centennial.org/index.php/american-indians-in-ww1-code-talkers.html [Pristupljeno 31.7.2022.]

Kriptologija u Prvom svjetskom ratu

Sažetak

Tijekom Prvog svjetskog rata korištene su brojne tada već poznate metode zakrivanja i raskrivanja poruka, dok je također osmišljen velik broj novih metoda. Stoga ovaj rad prikazuje stanje kriptologije i kriptografije te njihov razvoj za vrijeme Prvog svjetskog rata. Glavna tema je stvaranje, upotreba te dešifriranje kodova koje su koristili sudionici rata kao što je ruska verzija Vigenèreove šifre ili francuski *Tableau de concordance*. Rad se također dotiče određenih udruga i događaja koji su utjecali na ishod rata te na daljnji razvoj same kriptologije, ovo uključuje osnivanje Američke crne komore, dešifriranje Zimmermannovog telegrama kao i prvu upotrebu jezika indijanskih plemena u kriptologiji.

Ključne riječi: kriptologija, kriptoanaliza, šifra, Prvi svjetski rat, Zimmermannov telegram, Room 40, Američka crna komora

World War 1 cryptology

Summary

During World War 1, a great number of different methods of concealing and revealing the contents of a message were used, while many new ones were also created during this time. This paper aims to show the current stage and development of cryptology and cryptography during World War 1. The main topic is the creation of, use and deciphering of codes used by the war's participants such as the Russian version of the Vigenère cypher or the French *Tableau de concordance*. The paper will also touch on the topics of certain organizations and events which influenced the outcome of the war as well as the further development of cryptology, this includes the establishment of the American black chamber, deciphering of the Zimmermann telegram as well as the first use of Native American tribe languages in cryptology.

Key words: cryptology, cryptoanalysis, cipher, World War 1, Zimmermann telegram, Room 40, American black chamber