M-209

Keresteš, Jurica

SVEUČILIŠTE U ZAGREBU
PRIRODOSLOVNO–MATEMATIČKI FAKULTET
MATEMATIČKI ODSJEK

Jurica Keresteš

M-209

Diplomski rad

Voditelj rada:
Izv. prof. dr. sc. Zrinka Franušić

Zagreb, rujan, 2018.

Ovaj diplomski rad obranjen je dana _____ pred ispitnim povjerenstvom u sastavu:

1. _____, predsjednik
2. _____, član
3. _____, član

Povjerenstvo je rad ocijenilo ocjenom _____.

Potpisi članova povjerenstva:

1. _____
2. _____
3. _____

Diplomski rad napravljen je u sklopu aktivnosti Projekta KK.01.1.1.01.0004 - Znanstveni centar izvrsnosti za kvantne i kompleksne sustave te reprezentacije Liejevih algebri.

Sadržaj

Uvod

Tradicionalna kriptografija je vještina tajnog pisanja kako i kaže doslovni prijevod grčkih riječi *kryptós* (tajno, skriveno) i *graphein* (pisanje). Ona se bavi metodama za transformaciju poruka u nerazumljiv oblik, odnosno *šifriranjem*. Očito, učinjena transformacija mora biti reverzibilna tako da ju pojedinac kome je poruka namijenjena može pročitati, odnosno *dešifrirati*. Suvremena kriptografija je spoj različitih znanstvenih disciplima, u prvom redu matematike, računalstva, elektrotehnike, komunikologije i fizike. Njeni su glavni zadatci kreiranje i analiza različitih protokola i algoritama koji služe za sigurnu komunikaciju i zaštitu podataka.

Neki elementi kriptografije bili su prisutni već kod starih Grka. U 5. stoljeću prije Krista Spartanci su upotrebljavali napravu za šifriranje zvanu skital- drveni štap oko kojeg se namotavala vrpca od pergamenta te se na nju okomito pisala poruka. Samo osoba koja je imala štap iste debljine mogla je pročitati poruku. Kroz stoljeća, kriptografija se razvijala te se koristila kao sredstvo za zaštitu informacija, naročito u vojne i diplomatske svrhe. Nakon Prvog svjetskog rata, papirnate šifre i olovke zamijenile su naprave za šifriranje. Takve naprave činile su proces šifriranja i dešifriranja puno bržim i znatno sigurnijim. Najpoznatija takva naprava bila je Enigma. Do njene masovne uporabe došlo je za vrijeme Drugog svjetskog rata u Njemačkoj. S druge strane, Amerikanci su u to vrijeme koristili napravu M - 209 napravu koju je u Ameriku donio Boris Hagelin te koja je bio prenosiva i znatno manja od Enigme.

Prvo poglavlje diplomskog rada posvećeno je životopisu Borisa Hagelina i njegovim važnijim izumima. Boris Hagelin bio je švedski izumitelj u povijesti poznat kao jedan od najuspješnijih proizvođača kripto naprava. Do kraja Drugog svjetskog rata u Americi bilo napravljeno preko 140000 naprava M -209 te je time Boris Hagelin postao prvi milijunaš koji je zaradu ostvario prodajom kriptomašina.

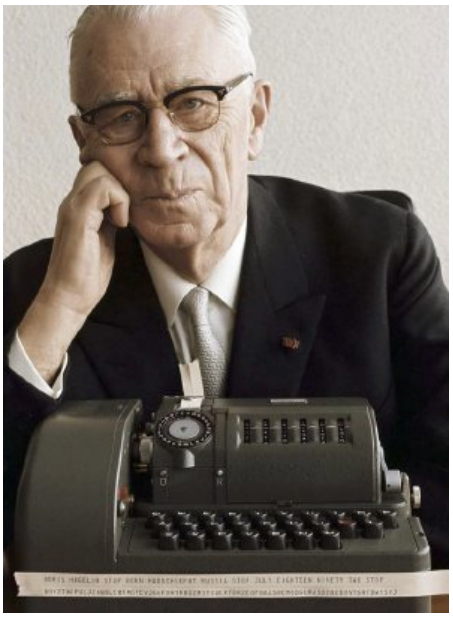
Drugo poglavlje posvećeno je simetričnim kriptosustavima - Cezarovoj i Vigenèreovoj šifri radi lakšeg razumijevanja procesa šifriranja budući da naprava M -209 za šifriranje koristi varijaciju Beaufort šifre koja je vrsta Vigenèreove šifre.

U trećem poglavlju navode se karakteristike i glavni dijelovi naprave M- 209, opće postavke naprave te se opisuje proces šifriranja i dešifriranja na konkretnim primjerima. Proces šifiranja i dešifiranja opisan je s matematičkog i mehaničkog aspekta. Kraj trećeg poglavlja posvećen je kriptoanalizi i kratkim opisima metoda napada pomoću šifrata na M- 209.

Poglavlje 1

Životopis i izumi Borisa Hagelina

Boris Caesar Wilhelm Hagelin rođen je 2. srpnja 1892. godine u Adschikentu, malom mjestu u Rusiji. Pohađao je rusku školu, no 1904. godine otac ga upisuje u švedsku školu. Diplomirao je strojarstvo 1914. godine na Royal Technical University u Stockholmu.



Slika 1.1: Boris Hagelin

Njegov otac Karl Wilhelm Hagelin bio je menadžer Nobel kompanije u Baku pa je Boris upravo tamo dobio i svoj prvi posao: nadgledanje konstrukcije električne centrale na jednom naftnom polju kompanije Nobel u Baku. Nakon Ruske revolucije 1920. godine Nobel kompanija ulazi u partnerstvo sa Standard Oil Company te je Boris poslan u SAD gdje je radio u njihovom odjelu tijekom 1921. Krajem te godine vladar Bolsheviks u Rusiji zaplijenio je sva privatna poduzeća uključujući i Nobel. Boris je mogao ostati u Standard Oil, ali u Americi se nije osjećao kao kod kuće te se seli u Švedsku.

Za Borisa više nije bilo budućnosti u naftnoj industriji, no i dalje je ostao u čvrstoj vezi s Emanuelom Nobelom koji mu je ponudio poziciju nadglednika male kompanije koju je počeo financirati 1921. – A. B. Cryptograph. Ta kompanija bila je osnovana 1915. godine s ciljem izrade naprava za kriptiranje koje je izumio švedski inženjer A. G. Damm. Tijekom 1921. u tvrtku nijedan ulagač nije htio uložiti, no Damm je ipak uspio zainteresirati Emanuela Nobela u njihove mogućnosti. Nobel se je savjetovao s Karlom Hagelinom te su zaključili da bi bilo dobro imati naprave za kriptiranje i kompaniju za nadolazeća vremena pa su obojica uložila u kompaniju.

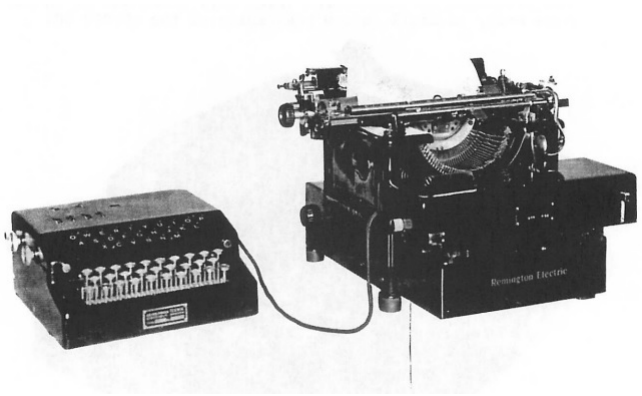
1925. godine Hagelin je dao svoj prvi veliki doprinos tvrtci A. B. Cryptograph i to se ispostavilo ključnim za budućnost kompanije. Saznao je da je švedski glavni stožer dobilo za pregled poznatu njemačku napravu za kriptiranje - *Enigmu*. Otišao do njih i objasnio im da njihova tvrtka već 10 godina ima iskustva iz područja naprava za kriptiranje te da im oni mogu ponuditi nešto bolje od Enigme. Oni su zahtijevali da naprave budu jednake veličine kao Enigma i da operativno funkcioniraju na podjednak način. Boris je imao samo šest mjeseci za napraviti takvu napravu, a imao je samo Dammove koncepte koji nisu potpuno zadovoljavali potrebe. Iako u to vrijeme Boris nije imao nikakvog iskustva u izradi naprava za kriptiranje, vjerovao je da će uspjeti zbog svog iskustva u prepravljanju i poboljšavanju postojećih naprava. Vjerovao je da će moći napraviti komplementarnu kompaktnu napravu Dammovog dizajna sa pojednostavljenim rotorima.

Boris je uspio načiniti prototip u dozvoljenim dimenzijama i predviđenom vremenu, no model je bio pomalo primitivan, ali svejedno dovoljno dobar za evaluaciju. Naprava je imala tipkovnicu, 2 rotora koja su bila kontrolirana parom rotora tzv. *pin-wheela* s drugačijim podjelama na svojoj periferiji i s ekranom od 25 elektrolampica koje su služile za prikaz izlaznih slova za šifriranje ili dešifriranje. Model je bio analiziran od strane matematičara te ga je glavni stožer odobrio za uporabu umjesto Enigme.

Prototip je imao 4 rotora s duljinama 17, 19, 21 i 23 koje su omogućavale *ključ* duljine 1 500 000. Koristeći različite kombinacije postavka iglica bilo je $2^{17} \cdot 2^{19} \cdot 2^{21} \cdot 2^{23} = 2^{80}$ ili približno 10^{24} različitih mogućnosti za odabir ključa, što uistinu velik broj. Prototip naprave koji je dobio nazvan je B-21.

Slika 1.2: B-21

Zadnji model koji je napravio u izgledu je bio jako sličan Enigmi. Korišteno je napajanje od 110 ili 220 volta za pokretanje rotora. Za prikaz lampica korištena je baterija. Radi lakšeg upravljanja naprava u centralnim uredima s ekstenzivnim operacijama, bila je spojena na Remington električnu tipkaču napravu umjesto prikaza lampicama.



Slika 1.3: Remington tipkača naprava

1927. godine A. G. Damm je preminuo i nakon njegove smrti njegovi nasljednici nisu više željeli ulagati u A. B. Cryptograph. Boris je tada radio bez plaće jer je tvrtka poslovala s vrlo malom dobiti. Usprkos limitiranim mogućnostima uspio je

obaviti nekoliko poslovnih putovanja van države i privući kupce za napravu B-21. Presudni uspjeh postigao je kod francuske vojske. No, vojsci su bile ključne dvije stvari koje naprava u tom trenu nije imala; naprava je morala moći isprintati tekst i morala je biti prijenosna. To je zahtijevalo ugradnju elektromehaničkog pogona. Boris je taj problem uspio riješiti u kratkom roku zamijenivši lampice sa specijalnim „rotornim ispisnim mehanizmom“, kojeg je sam dizajnirao. Naprava je nazvana B-211 i izrađivala se u Francuskoj. Prije zahuktavanja Drugog svjetskog rata izrađeno je i prodano oko 500 takvih naprava, a nakon početka prodano je još dodatnih 100.

Slika 1.4: B-211

Vrlo brzo nakon početka suradnje s francuskom agencijom za sigurnost *Deuxieme Bureau* tražili su od Borisa da izumi kompaktnu „džepnu“ napravu za kriptiranje koja ispisuje. Sličan je zahtjev Boris dobio i nekoliko godina prije od dvojice Šveđana. Tu napravu je tada uspio dizajnirati, no nisu mu platili pa je zadržao prava na taj dizajn. Taj dizajn pomogao je u izgradnji nove naprave za kriptiranje te su veliki dijelovi ugrađeni u novu napravu, posebice "kalkulatorni" mehanizam kojeg su neki kriptolozi smatrali revolucionarnom idejom. Kod prvih naprava za kriptiranje duljine (cyclic wheel lengths) bile su 17, 19, 21, 23 i 25, što je rezultiralo periodom duljine 3 900 225 operacija, duljina koju do onda ni jedna mehanička naprava za kriptiranje nije postigla. Štoviše, pošto je teoretski mogao sve iglice postaviti u 10^{29} različitih kombinacija, broj mogućih varijacija je bio toliko visok da su ove naprave dovoljno dobre za mnoge potrebe svakodnevice. Napravama koje je napravio dao je ime C s dodatnim slovom i zadnja dva broja godine koji su označavali model. Kasnije je Boris napravio mnoge promjene na napravama za kriptiranje u skladu s razvojem kriptoanalize koje su bile moguće radi suradnje s švedskim kriptoanalitičararem Y. Gyldenom. Glavno unaprjeđenje na napravama sastojalo se od povećanja broja rotora s 5 na 6. Kad se

takva naprava počela proizvoditi u većim količinama, dodane su gornje i donje zaštite tako da je naprava mogla biti zavezana za jedno koljeno operatera pa se mogla koristiti na terenu. Taj model je bio CX-52 (1952. godina).

Slika 1.5: CX-52

Da bi promovirao naprave iz serije C, Boris je putovao Europom, a 1937. godine dva puta je bio u Americi gdje su izrazili želju za strujno upravljanom napravom koja ima tipkovnicu. U ljeto 1939. predstavio je u Washingtonu prototip takve naprave nazvan BC. Nažalost, konstrukcija je trebala poboljšanja pa se je vratio u Švedsku točno u jesen kad je započeo Drugi svjetski rat. Početkom ožujka 1940. Boris je još jednom otputovao u SAD na svoju inicijativu bez ikakvih upita iz Washingtona. Krenuo je zadnjim brodom iz Europe (Italije) s napravom za kriptiranje u prtljazi netom prije no što su Talijani krenuli u rat. Taj put je bio presudan i Boris će postići najveću prodaju C naprava ikad.

Kad je izbio rat Hagelin je uspio prebaciti svoj prihod iz Francuske u Švedsku. Suma je bila dovoljna da bi opskrbio i pokrenuo svoju radionicu. To je bila prva radionica nakon A. B. Cryptograph. Bila je osnovana 1940. i nazvana A. B. Ingeniorsfirman Cryptoteknik.

Prodaja u Americi počela je probnom narudžbom od 50 naprava koje su zračno dostavljene u Ameriku. Nakon detaljnog testiranja, naprava C je prihvaćena. Redizajnirana je i izrađivala se u Americi pod imenom M-209. Proizvodila ju je tvrtka za izradu pisaćih mašina *L. C. Smith-Corona*, dnevno čak do 500 komada.

Tijekom rata Boris je ostao u Americi. Imao je mali dućan u kući za servisiranje BC naprava koje su Amerikanci koristili tijekom rata. 1944. godine Boris se vraća u Švedsku. Do tada je već bilo napravljeno više od 50 000 naprava za kriptiranje. Do

kraja rata u Americi je bilo napravljeno preko 140 000 takvih naprava.

Tijekom Borisova četverogodišnjeg izbivanja, radionica u Stockholmu je bila zauzeta narudžbama mnogih stranih država. Jedna dostava išla je čak i do Japana, iako je jako mali broj tih naprava zaista i završio u Japanu.

Njemačke vlasti prije rata nisu pokazivale interes za C naprave za kriptiranje, no pred kraj rata počele su izrađivati kopije BC naprave za svoju osobnu upotrebu. Do kada se Treći Reich urušio, uspjeli su napravili samo 700-tinjak naprava. Poslijeratne verzije C naprave bile su rađene s licencama. Tada je napravljeno preko 10 000 naprava. Francuska je također u to vrijeme dobila prava za proizvodnju C naprava.

C naprave izrađivane su za uporabu na bojištu, no radi svoje jednostavnosti i nosivosti također su se pokazale korisne za komunikaciju između diplomata pa je bilo potrebno napraviti neka poboljšanja, no novi dizajni nisu radili velike promjene u originalnoj strukturi. Boris je najprije dobio ideju da promjeni naprave tako da rotacije rotora budu iregularne. Takve naprave za kriptiranje dobile su ime CX-52, no kasnije, kad su napravljeni izmjenjivi rotori, bili su korišteni novi brojevi za model. No, dvije skupine poslodavaca tražile su različite pristupe. Jedna grupa je željela što veću duljinu ključa, dok je druga željela čim iregularnija micanja rotora. Da bi zadovoljili kupce razvili su i hibridni sustav koji je koristio jedan statički rotor, dok su ostali bili pomični.

Različita poboljšanja na C napravi za kriptiranje dovela su do povećanja veličine. Boris je tada želio napraviti džepnu napravu u pravom smislu te riječi. Uspio je predstaviti model koji, radi svoje malene dimenzije, nije mogao ispisati tekst, ali se s njega lako moglo očitati slovo po slovo. Naprava za kriptiranje je bila potpuno drugačija od C naprava, ali je bila potpuno kompatibilna s modernim verzijama C naprava.

Slika 1.6: Džepna naprava za šifriranje

1948. godine Boris se smjestio u Švicarskoj gdje je kraće vrijeme radio sa švicarskim izumiteljom dr. Edgarom Gretenerom na razvoju naprava za automatsko šifriranje i dešifriranje telegrafskih poruka. Njihova suradnja nije trajala dugo te se Boris odlučio napraviti vlastitu napravu za kriptiranje s novijom opremom. Kasnije osniva malu neovisnu podružnicu Crypto AG. Posao je brzo rastao te je 1966. godine otvorena nova tvornica i administracijska zgrada u Zugu. Tvornica je izrađivala mehaničke naprave za kriptiranje, osmišljene i izrađene u Švedskoj, orginalne „Hagelin Cryptos“. Prvi proizvod Crypto AG bile su telegraf naprave za kriptiranje. Naslijedile su ih elektronički kripto sustavi koji su postali dominanti posljednjih godina. Stare mehaničke naprave su se i dalje proizvodile, no u jako malim količinama. Brand „Hagelin Cryptos“ je bio pripisan svim napravama kasnije napravljenim, sve do Borisova umirovljena 1970 godine. Boris Hagelin napravio je još mnogo naprava za kriptiranje koje nažalost nikad nisu napravljene ili nisu imale veliki značaj.

Boris Caesar Wilhelm Hagelin umro je 7.9.1983. godine u 91. godini života u Zugu u Švicarskoj.

Poglavlje 2

Simetrični kriptosustavi

2.1 Osnovni pojmovi

Svaki *kriptosustav* mora imati definiranih sljedećih pet komponenti:

1. $\mathcal{P}$ - konačan skup svih mogućih osnovnih elementa *otvorenog teksta*,
2. $\mathcal{C}$ - konačan skup svih mogućih osnovnih elementa *šifrata*,
3. $\mathcal{K}$ - konačan skup svih mogućih *ključeva*,
4. $e_K : \mathcal{P} \to \mathcal{C}$ - *funkcija šifriranja*, $K \in \mathcal{K}$,
5. $d_K : \mathcal{C} \to \mathcal{C}$ - *funkcija dešifriranja*, $K \in \mathcal{K}$,

pri čemu vrijedi da je $d_K(e_K(x)) = x$ za svaki otvoreni tekst $x \in \mathcal{P}$.

Najednostavniji primjer klasičnog kriptosustava je tzv. *Cezarova šifra*. Skupovi $\mathcal{P}$ i $\mathcal{C}$ su jednaki i sastoje se od slova engleskog alfabeta

$$\mathcal{P} = \mathcal{C} = \{A, B, C, \ldots, X, Y, Z\}.$$

Funkcija šifriranja se sastoji u tome da svako slovo zamijeni slovom koje se nalazi npr. tri mjesta (ili neki dugi fiksan broj mjesta) dalje, pri čemu nakon zadnjeg slova Z se abecededa opet ciklički ponavlja. Dakle,

$$A \mapsto D,\ B \mapsto E,\ \ldots,\ Y \mapsto B,\ Z \mapsto C.$$

Ovdje se radi o *supstitucijskoj šifri* jer se svaki element otvorenog teksta (slovo) zamijenio s nekim drugim elementom (slovom). Postoje i *transpozicijske šifre* u kojima se elementi otvorenog teksta permutiraju.

Otoreni tekst

`AVE CEZAR`

se pomoću Cezarove šifre kriptira u

`DYHFHCDU`,

pri čemu se razmaci pri šifriranju zanemaruju. Dešifriranje je jednostavno, samo pomaknemo svako slovo tri mjesta unazad. Uočimo, da u ovom slučaju poznajući ključ za šifriranje ("pomak" slova unaprijed), odmah znamo i ključ za dešifriranje. Takvi sustavi u kojima ključ za dešifriranje možemo lako odgonenuti pomoću ključa za šifriranje zovu se *simetrični* ili *konvencionalni* kriptosustava. Posebno su praktični oni kojima je algoritam za šifriranje identičan algoritmu za dešifriranje. Naravno, sva sigurnost ovih kriptosustava leži u tajnosti ključa pa se iz tog razloga ti sustavi ponekad zovu *kriptosustavi s tajnim ključem*. Da ih se ne bi moglo lako razbiti *grubom silom*, skup ključeva simetričnih kriptosustava je najčešće ogroman. Za razliku od toga, danas popularni *kriptosustavi s javnim ključem* zasnivaju se se na tome što se deširirati može samo pomoću osobnog, tajnog ključa koji posjeduje samo osoba kojoj je poruka namijenjena.

Razbiti Cezarovu šifru nije posebno teško grubom silom jer se skup ključeva vrlo mali i sastoji se od 25 mogućih pomaka. No, može se koristiti i tzv. *frekvencijska analiza* slova koja se bazira na ideji da najfrekventnija slova šifrata odgovaraju najfrekventnijim slovima jezika. Naravno, što je dulji šifrat veća je vjerojatnost za takvo što. Nadalje, vrlo su korisni i podatci o najčešćim bigramima (parovima slova) i trigramima (nizovima od tri slova) u jeziku.

Matematički model Cezarove šifre dobivamo tako što svako slovo zamijenimo brojem:

$$A \mapsto 0,\ B \mapsto 1, \ldots, Y \mapsto 24,\ Z \mapsto 25.$$

Tada su

$$\mathcal{P} = \mathcal{C} = \mathcal{K} = \{0, 1, 2, \ldots, 25\} = \mathbb{Z}_{26}.$$

Skup $\mathbb{Z}_{26}$ uz operaciju zbrajanja modulo 26 čini Abelovu grupu pa je funkcija šifriranja dana s

$$e_K(x) = x +_{26} K,$$

za $x \in \mathcal{P}$, $K \in \mathcal{K}$. Budući je $(\mathbb{Z}_{26}, +_{26})$ grupa, postoji suprotan element K' od K, odnosno takav da je $K +_{26} K' = 0$ pa je funkcija dešifriranja dana s

$$d_K(y) = y +_{26} K',$$

za $x \in \mathcal{C}$. Vrijedi

$$d_K(e_K(x)) = e_K(x) +_{26} K' = (x +_{26} K) +_{26} K' = x +_{26} (K +_{26} K') = x.$$

Umjesto operacije $+_{26}$ ubičajeno je funkcije šifriranja i dešifriranja zapisivati sljedeći način:

$$e_K(x) = x + K \mod 26,\ d_K(x) = d - K \mod 26,$$

gdje operacija mod 26 daje ostatak pri dijeljenju s 26.

2.2 Vigenèrova šifra

Vigenèreova šifra je metoda šifriranja abecednog teksta korištenjem serije Cezarovih šifri s različitim pomacima. Korištena je tijekom američke revolucije, krajem 18. stoljeća. Godine 1917. u uglednom časopisu *Scientific American* objavljeno je da je ovu šifru "nemoguće razbiti". Razlog tome bio je to što je Vigenèreova šifra na raspolaganju imala znatno više ključeva nego Cezarova, njih 26^m gdje je m duljina ključa. Pa napad grubom silom ono vrijeme nije dolazio u obzir.

	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
X	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	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	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

Slika 2.1: Vigenèreov kvadrat

Vigenèreova šifra otkrivana je više puta, a metodu je prvi opisao Giovan Battista Bellaso. Međutim, u 19. stoljeću ta je shema pogrešno pripisana Blaiseu de Vigenèreu, tako da je sad poznata kao *Vigenèreova šifra*.

Za šifriranje teksta koristi se tablica alfabeta, tzv. *Vigenereov kvadrat* (Slika 2.1). Kvadrat se sastoji od alfabeta napisanog 26 puta u novom redu, a svaki red pomaknut je ulijevo za jedno mjesto u odnosu na prethodni, odgovarajući svim mogućim kombinacijama Cezarove šifre. U pojedinoj točki procesa šifriranja, šifra koristi "drugi" alfabet iz jednog od redova. Koji će se red koristiti ovisi o ponavljajućem ključu.

Na primjer, neka je otvoreni tekst koji treba šifrirati:

`AUTOMOBIL`

Osoba koja šalje poruku bira ključ i ponavlja ga onoliko puta koliko je potrebno da odgovara dužini otvorenog teksta, npr, ključ STOL:

`STOLSTOLS`

Prvo slovo otvorenog teksta A se šifrira koristeći alfabet iz reda S, koje je prvo slovo ključa. To se radi tako što se traži slovo na presjeku retka S i stupca A Vigenèreove tablice, odnosno traženo slovo je S. Za sljedeće slovo otvorenog teksta se koristi sljedeće slovo ključa, slovo u presjeku reda T i stupca U je traženo slovo N. Po tom principu nastavlja se do zadnjeg slova otvorenog teksta i dobiva se šifrat:

`SNHZFHPTD`

Matematički model Vigenèreove šifre dobivamo tako što svako slovo zamijenimo brojem:

$$A \mapsto 0,\ B \mapsto 1,\ \ldots,\ Y \mapsto 24,\ Z \mapsto 25.$$

Tada za m fiksan prirodan broj definiramo

$$\mathcal{P} = \mathcal{C} = \mathcal{K} = \{0, 1, 2, \ldots, 25\}^m = \mathbb{Z}_{26}^m.$$

Skup $\mathbb{Z}_{26}^m$ uz operaciju zbrajanja modulo 26 čini Abelovu grupu. Funkcija šifriranja dana je s

$$e_K(x_1, x_2, \ldots, x_m) = (x_1 +_{26} k_1, x_2 +_{26} k_2, \ldots, x_m +_{26} k_m),$$

za $(x_1, x_2, \ldots, x_m) \in \mathcal{P}$, $(k_1, k_2, \ldots, k_m) \in \mathcal{K}$. Budući je $(\mathbb{Z}_{26}^m, +_{26})$ grupa, postoji suprotan element od $K = (k_1, k_2, \ldots, k_m)$ kojeg označimo s $K' = (k_1', k_2', \ldots, k_m')$. Stoga je funkcija dešifriranja dana s

$$d_K(y_1, y_2, \ldots, y_m) = (y_1 +_{26} k_1', y_2 +_{26} k_2', \ldots, y_m +_{26} k_m'),$$

za $(y_1, y_2, \ldots, y_m) \in \mathcal{C}$. Kraće, za $X \in \mathcal{P}, K \in \mathcal{K}, Y \in \mathcal{C}$ pišemo

$$Y_i = e_K(X_i) = (X_i + K_i) \mod 26,\ X_i = d_K(Y_i) = (Y_i - K_i) \mod 26,$$

pri čemu se operacije izvršavaju po komponentama m-torki.

Vigenèrova šifra može se shvatiti i kao blokovna šifra koja otvoreni tekst šifrira u blokovima duljine m odnosno duljine ključa. U tom se slučaju se, ako duljina otvorenog teksta nije višekratnik od m, otvoreni tekst nadopuni potrebnim brojem slova (npr. X). Ukoliko se koristi Vigenèrov kvadrat takvo što nije potrebno.

Osnovna slabost Vigenèreove šifre je u duljini njezina ključa. Ako kriptoanalitičar otkrije duljinu ključa, onda se šifrat smatra serijom Cezarovih šifri. Testovi Kasiskog i Friedmana pomažu u određivanju dužine ključa.

Primjenu Kasiskog testa opisujemo u sljedećem primjeru.

Primjer 2.2.1. Pretpostavimo da je otvoreni tekst

```
UZ NOVI DAN DOLAZI NOVA SNAGA I NOVE IDEJE
```

Neka je zadani ključ

```
AB CDEA BCD EABCDE ABCD EABCD E ABCD EABCD
```

Uz zadani otovreni tekst i ključ dobivamo šifrat

```
UA PRZI ECQ HOMCCM NPXD WNBID M NPXH MDFLH
```

Rastojanje između ponovljenog NPX je 10. Stoga, pretpostavljajući da ponovljeni segmenti predstavljaju ponovljene segmente otvorenog teksta, nagovještava da ključ ima duljinu od 10, 5, 2 ili 1 znaka. Ako je ključ duljine 1 radi se o Cezarovoj šifri. Također, u praksi se vjerojatno nikad neće koristiti ni ključ duljine 2. Dakle, duljina ključa je u ovom slučaju 10 ili 5 znaka.

Kada se otkrije duljina ključa, onda se za svako m-to slovo šifrata može primjeniti metoda frekvencije, kao za Cezarovu šifru, koja će otkriti ključ.

Test Kasiskog koristi činjenicu da će pojedine česte riječi vjerojatno biti šifrirane istim slovima ključa, pa će se u šifratu pojaviti ponovljene grupe slova. Na primjer, dio otvorenog teksta `NOV` se jednom širira kao `PRZ` a drugi put kao `NPX`.

Kod dužih poruka je test točniji, jer obično sadrži više ponovljenih segmenata. Prikazani šifrat ima nekoliko ponovljenih segmenata te omogućuje kriptoanalitičaru da lakše otkrije duljinu ključa.

Poglavlje 3

M-209

3.1 Općenito o napravi M-209

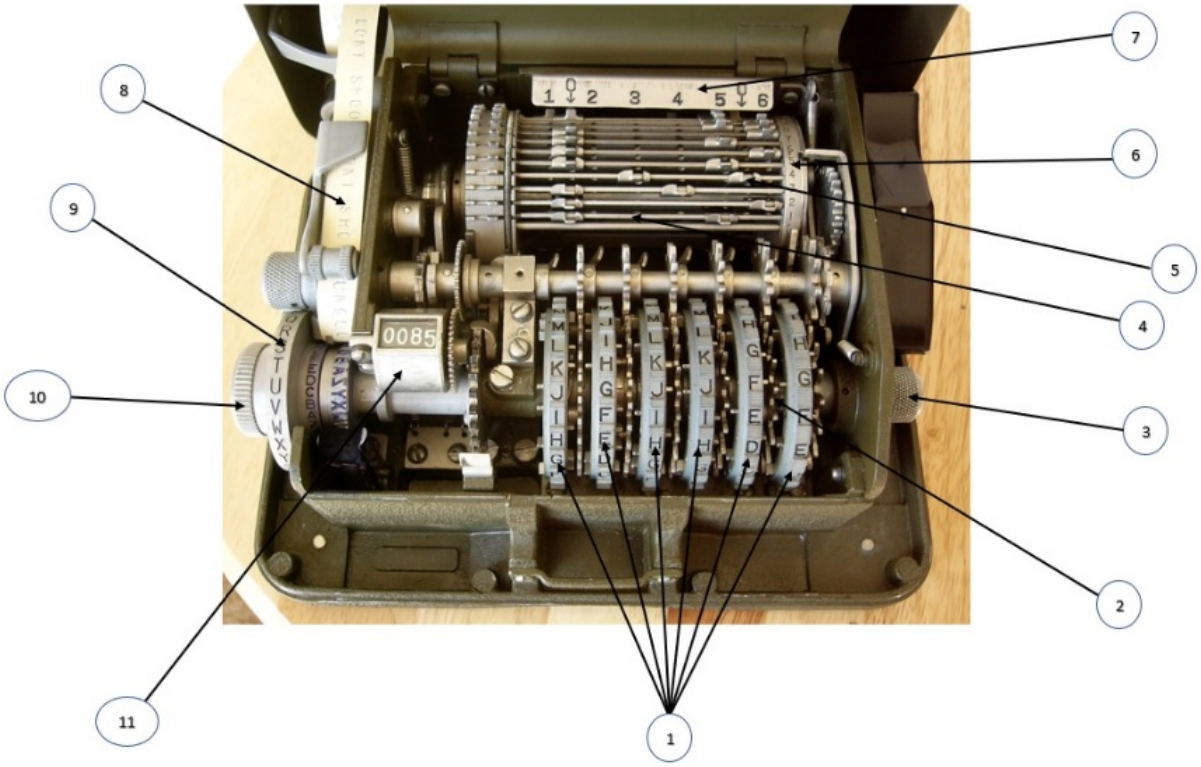
M-209, poznat kao i CSP-1500, je prijenosna i kompaktna mehanička naprava za šifriranje nastala od ranijeg modela C-38 kojega je dizajnirao Boris Hagelin 1938. godine. M-209 ne zahtijeva nikakav izvor energije. M-209 dimenzija je $83 \times 140 \times 178$ mm i težine oko 3 kg uključujući i njegovu kutiju. Njegova mala veličina i mala težina te činjenica da radi bez struje glavni su razlozi zašto je bila toliko upotrebljavana na bojišnici. Naprava je otporna na trešnju, prašinu, pijesak, tropske vlage te velike hladnoće. Također, naprava može i šifrirati i dešifrirati što je velika prednost u odnosu na druge naprave za kriptiranje.

Slika 3.1: M-209

Najvažniji dijelovi naprave su kavez, rotori i vodilice koje povezuju kavez i rotore. Kavez se sastoji od 27 horizontalnih šipki između 2 diska koje stvaraju rotirajući cilindar. Svaka šipka ima dvije pokretne spojne ušice koje se mogu namjestiti u 8 različitih pozicija: 2 neutralne i 6 pozicija koje uzajamno djeluju s rotorima. U ovisnosti o spojnim ušicama i rotorima te njihovim postavkama, pojedinačne šipke mogu klizati u lijevo i pridodati složenosti naprave. Broj šipki u svojoj lijevoj poziciji jednak je pomaku između otvorenog teksta i šifrata.

Svaki od šest rotora kontrolira jednu vodilicu te ima drugačija slova na svom naplatku i iglicu ispod tih slova. Broj slova s lijeva na desno je 26, 25, 23, 21, 19 i 17. Budući da su ti brojevi relativno prosti, tj. njihov najveći zajednički djelitelj je 1, rotori će se „poravnati“ nakon $26 \cdot 25 \cdot 23 \cdot 21 \cdot 19 \cdot 17 = 101\,405\,850$ šifriranih znakova. To se naziva *period*. Svako slovo na naplatku ima pomičnu iglicu. Postavljanjem iglice desno znači da je pozicija slova omogućena, dok postavljanje lijevo znači da je pozicija slova onemogućena. Omogućena pozicija slova postavit će vodilicu u operativno stanje. Rotori imaju sljedeća slova:

1. ABCDEFGHIJKLMNOPQRSTUVWXYZ
2. ABCDEFGHIJKLMNOPQRSTUVXYZ
3. ABCDEFGHIJKLMNOPQRSTUVX
4. ABCDEFGHIJKLMNOPQRSTU
5. ABCDEFGHIJKLMNOPQRS
6. ABCDEFGHIJKLMNOPQ



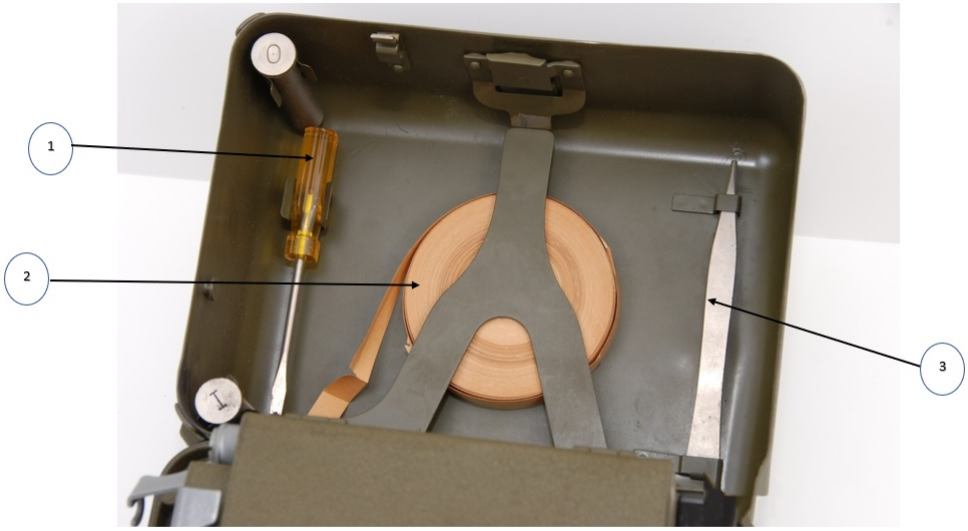
Slika 3.2: Dijelovi M-209

Dijelovi M-209:

1. Rotori
2. Iglice
3. Kotačić za resetiranje
4. Šipke
5. Ušice
6. Indikator šipki

7. Indikator ušica
8. Traka za ispis
9. Indikator slova
10. Kotačić za namještanje slova
11. Brojač

Pri vrhu poklopca nalazi se dodatni pribor. Na sredini naprave je dodatna traka za pisanje, a s lijeve strane je odvijač kojim se otvara naprava kada se namještaju postavke. S druge strane je pinceta za namještanje papira i nekih unutarnjih postavki.



Slika 3.3: Dodatni pribor

Dodatni pribor M-209:

1. Odvijač
2. Dodatna traka
3. Pinceta za namještanje papira i unutarnjih postavki

3.2 Postavke naprave M-209

Za komunikaciju pomoću M-209, odnosno za ispravno šifriranje i dešifrirati poruka, pošiljatelj i primatelj moraju imati iste postavke na svojim napravama. Da bi mogao postaviti svoju napravu, svaki operater mora imati svoju listu uputa, tj. tablicu kao Slici 2.4.

NR	LUGS	1	2	3	4	5	6
01	3-6	A	A	A	-	-	A
02	0-6	B	-	B	-	B	B
03	1-6	-	-	-	C	-	-
04	1-5	D	D	-	-	D	D
05	4-5	-	E	-	E	E	-
06	0-4	-	-	-	F	F	-
07	0-4	-	G	G	-	-	-
08	0-4	H	-	H	H	H	H
09	0-4	I	-	-	I	I	-
10	2-0	-	J	J	-	-	-
11	2-0	K	K	-	-	-	K
12	2-0	-	L	L	-	-	-
13	2-0	M	-	M	M	M	-
14	2-0	N	-	N	N	N	N
15	2-0	-	O	-	-	-	O
16	2-0	-	-	-	P	P	-
17	2-0	-	-	-	-	-	Q
18	2-0	-	R	R	-	-	
19	2-0	S	S	S	S	S	
20	2-5	T	-	T	T		
21	2-5	-	U	U	U		
22	0-5	V	-	-			
23	0-5	W	X	X			
24	0-5	-	-				
25	0-5	-	-				
26	0-5	-					
27	0-5						

BAR	1	2	3	4	5	6
01	-	-	X	-	-	X
02	-	-	-	-	-	X
03	X	-	-	-	-	X
04	X	-	-	-	X	-
05	-	-	-	X	X	-
06	-	-	-	X	-	-
07	-	-	-	X	-	-
08	-	-	-	X	-	-
09	-	-	-	X	-	-
10	-	X	-	-	-	-
11	-	X	-	-	-	-
12	-	X	-	-	-	-
13	-	X	-	-	-	-
14	-	X	-	-	-	-
15	-	X	-	-	-	-
16	-	X	-	-	-	-
17	-	X	-	-	-	-
18	-	X	-	-	-	-
19	-	X	-	-	-	-
20	-	X	-	-	X	-
21	-	X	-	-	X	-
22	-	-	-	-	X	-
23	-	-	-	-	X	-
24	-	-	-	-	X	-
25	-	-	-	-	X	-
26	-	-	-	-	X	-
27	-	-	-	-	X	-

TNJUW AUQTK CZKNU TOTBC WARMI O

KEY LIST INDICATOR: XA

Slika 3.4: Lista uputstva

Lista uputa sastoji se od postavki ušica za bubanj, rotora, 27 slovne provjere za potvrdu postavki te indikatora kojim bi u šifratu identificirali vanjski ključ s ostalim

primateljima. Prije upotrebe naprave, operater treba postaviti dvije ušice na svaku od 27 horizontalnih šipki u kavezu i omogućiti ili onemogućiti pomoćnu iglicu ispod svakog slova kod svakog rotora. Slovo označava aktivnu iglicu koja se postavlja s desne strane naprave, a razmak označava neaktivnu iglicu koja se postavlja s lijeve strane. Ove postavke nazivaju se *unutarnji ključ*. Kad su unutarnje postavke postavljene, operater postavlja startnu poziciju na rotorima. To se još naziva i *vanjski ključ* i on se mijenja kod svake nove poruke. Ovaj ključ umeće se u prije dogovoreno mjesto u šifratu tako da bi primatelj koji dešifrira poruku mogao postaviti svoje rotore na odgovarajuće mjesto. Budući da taj proces zahtijeva puno vremena, postavke su se rijetko mijenjale - najčešće samo jednom dnevno.

Kad su sve postavke postavljene, rabi se provjera od 27 slova. Naprava se postavlja u način rada šifriranja i svi se rotori postavljaju na slovo A. Zatim se šifrira svih 27 slova A, jedno za drugim. Rezultat se mora podudarati s 27 slova koja su na podnožju tablice.

Tijekom 40-ih i 50-ih godina 20. stoljeća bilo je nekoliko verzija uputstava za američku vojsku. Ona su se uglavnom sastojala od naputaka kako napraviti dobar ključ te primjera loših kombinacija ključa. Poznato je najmanje 6 verzija uputstva koje su objavljenje od strane američke vojske te su navedene na slici 2.5.

Year	**Details**
1942	TM 11-380 Technical Manual Converter M-209, 33 pages, April 27, 1942 [26]
1943	TM 11-380B Technical Manual Converter M-209, 42 pages, September 20, 1943 [27]
1944	TM 11-380 Technical Manual Converter M-209, M-209A, M-209B, 78 pages, March 17, 1944 [28]
1947	TM 11-380 Technical Manual Converter M-209, M-209A, M-209B, 170 pages, May 1947 [29][1]
1951	Update dated April 10, 1951. We could not find the document.
1953	Mentioned in correspondence from Crypto-Aids Division to C/SEC, April 8, 1953 [4]

Slika 3.5: Verzija uputstva

Uputstva su naglašavala da barem 40% iglica mora biti aktivno, no ne više od 60%. Također, na svakom rotoru ne smije biti više od 6 uzastopnih iglica u aktivnom ili neaktivnom stanju. Verzija iz 1947. godine je uključivala uputstva da se poruke dulje od 500 slova moraju razbiti na manje poruke, da se početne pozicije rotora moraju razlikovati za svaku poruku itd.

3.3 Proces šifriranja i dešifriranja

Mehaničko šifriranje

Jednom kad su postavke obavljene može se početi šifrirati poruka. Najprije, potrebno je resetirati brojač na simulatoru s razmakom i postaviti način rada na šifriranje. Zatim je potrebno postaviti 6 slučajnih slova na svih 6 rotora. To se zove indikator vanjske poruke. Tih šest slova zapisuju se radi kasnije upotrebe. Radi sigurnosnih razloga bitno je da se taj indikator rabi samo jednom s tim postavaka tijekom jednog dana. Svaki indikator vanjske poruke mora biti unikatan. Na primjer, rabi se `DUFLJB` kao indikator vanjske poruke te se bira slučajno slovo, recimo slovo `K`. Zatim se 12 puta šifrira slovo `K`. Rezultat je 12 slučajnih šifriranih slova nakon čega operator sačuva taj ispis te vrati brojač na nulu prije prve prave uporabe. Tih 12 slova koristi se za postavljanje tajnog indikatora unutarnje poruke. Počinje se s prvim slovom i postavlja se krajnje lijevi kotačić u tu poziciju. Nastavlja se s rotorima od lijeva prema desnom. Nakon što su svi rotori postavljeni, može se šifrirati poruka s tim indikatorom unutarnjeg ključa. U ovom slučaju, indikator unutarnje poruke napravljen od 12 slova je `PEQGBJ`.

Kad je otvoreni tekst postavljen na dugme s pokazateljem diska s lijeve strane naprave, operator pokreće ručicu za napajanje s desne strane, a kavez napravi kompletnu rotaciju kroz svih 27 šipka. Ako ruka vodilica dođe u kontakt sa spojnom ušicom koja je na šipci, šipka klizne lijevo. Sve šipke koje su na kraju s lijeve strane tvore postavku zupčanika pa slova mogu biti kriptirana. Pomak slova jednak je broju šipki u lijevoj poziciji. Nakon jedne rotacije sve šipke se pomoću zupčanika vraćaju u prvobitnu poziciju, a svi kotačići se pomaknu naprijed za jedno slovo, a vodilice zaključaju kavez da spriječi sljedeću enkripciju sve dok se indikator diska ne postavi na sljedeće slovo. To znači da, ako operator šifrira ili dešifrira dva jednaka slova zaredom, mora okrenuti disk naprijed i natrag. Vješt operator može šifrirati odnosno dešifrirati 15 do 30 slova po minuti.

Šifrat korišten u M-209 je varijacija Beaufort šifre, što znači da u procesu šifriranja koristi jednak algoritam i za kriptiranje i dekriptiranje.

$$\text{Šifriranje: } y_i = (z_i - x_i) \mod 26$$
$$\text{Dešifriranje } x_i = (z_i - y_i) \mod 26$$

Tijekom šifriranja, razmaci između slova zamjenjuju se sa slovom `Z`. Kad primalac dešifrira poruku, svako slovo `Z` zamjeni se razmakom, a odvojena slova zamjene se sa svojom fonetskom riječju, `C` za Charile, `E` za Easy, itd. Brojevi se pišu kao 1 kao ONE, 2 kao TWO, itd. Na primjer, poruka

```
OPERATION ZEBRA STARTS AT SUNSET
```

nakon šifriranja glasila bi

```
KBMUN ODDDC YWLVM RBVUS QYRHT XNZUI HX.
```

Jednom kad je poruka šifrirana u potpunosti, šifrat se ispisuje u grupama od 5 slova na papirnu vrpcu. Ako zadnjih 5 slova nije do kraja ispisano, dopisuje se slova X. U tom slučaju, navedeni šifrat ispisao bi se kao:

```
KBMUN ODDDC YWLVM RBVUS QYRHT XNZUI HXXXX.
```

Da bi se poruka završila, potrebno je dodati 3 indikatora. Oni se dodaju i na početku i na kraju poruke. Prvi indikator zove se *sistemski indikator* i on govori primatelju da je poruka šifrirana pomoću naprave M-209. To je početno kriptirano slovo, tj. u ovom slučaju KK.

Drugi indikator je slučajno odabrani vanjski indikator poruke (ne tajni unutarnji indikator). On se stavlja nakon sistemskog indikatora.

Treći indikator je indikator ključne liste. On govori primatelju koja lista uputa je bila korištena za šifriranje poruke. Taj indikator se zapisuje nakon vanjskog indikatora. Šifrat, uključujući i indikatore, glasi:
`KK DUFLJB XA KBMUN ODDDC YWLVM RBVUS QYRHT XNZUI HXXXX KK DUFLJB XA`
Grupirajući poruku po 5 slova, poruka glasi
`KKDUF LJBXA KBMUN ODDDC YWLVM RBVUS QYRHT XNZUI HXXXX KKDUF LJBXA`
Za kraj, potrebno je uništiti papirić koji sadrži 12 početnih slova i okrenuti rotore u nove pozicije kako bi se razbio indikator unutarnje poruke.

Mehaničko dešifriranje

Da bi dešifrirao poruku, primatelj mora postaviti napravu u način rada šifriranje (ne dešifriranje), a zatim sastavlja 6 rotora onako kako je zadano vanjskim indikatorom koji je dan u poruci. 12 puta šifrira slovo K koje je pronašao na početku i na kraju teksta i na taj način vraća onih 12 slova od kojih je sastavljen unutarnji indikator.

Zatim resetira brojač i postavlja rotore onako kako pokazuje unutarnji indikator. Tek tada stavlja način rada naprave u dešifriranje i dešifrira poruku. Kod dešifriranja, dešifrirana slova Z postaju razmaci. Kod riječi gdje očito fali slovo Z, ono se dopiše, npr. kod riječi ZEBRA u rečenici `OPERATION EBRA STARTS AT SUNSET`. Rečenica ispravno glasi `OPERATION ZEBRA STARTS AT SUNSET`.

3.4 Matematički model šifriranja

Objasnit ćemo šifriranje naprave M-209 korištenjem jednostavne matrične algebre. Najprije prikažimo kako matematički opisujemo ključ.

Neka je matrica $M \in M_{6,27}(\mathbb{Z})$ čiji su elementi 0 ili 1. Dakle, M matrica dimenzija 6×27. Dodatna je pretpostavka da niti jedan stupac od M nema više od dvije jedinice. Primjer jedne takve matrice je sljedeći:

$$\begin{bmatrix}
0&0&0&0&1&0&0&0&0&0&0&0&1&0&1&0&1&0&0&0&0&0&0&0&0&0&0\\
0&1&0&0&0&1&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&1&0&1&1&0&0\\
0&0&0&0&0&0&1&0&0&0&1&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0\\
0&0&1&1&0&0&0&1&0&1&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&1&0\\
0&0&0&0&0&0&0&0&1&0&0&1&0&0&0&1&1&1&1&0&1&1&1&0&0&0&0\\
0&1&0&0&0&0&0&0&0&0&1&0&0&1&0&0&0&0&0&1&0&0&0&1&0&0&1
\end{bmatrix}$$

Nadalje, neka je vektor $v \in \mathbb{Z}^6$ čiji su elementi također 0 ili 1. Ako v shvatimo kako jednoretčanu matricu, tj. $v \in M_{1,6}(\mathbb{Z})$, onda je moguć umnožak matrice v i M i $vM \in M_{1,27}(\mathbb{Z})$. Matricu vM možemo shvatiti i kao 27-dimenzionalni vektor s komponentama iz $\{0,1,2\}$, $vM \in \mathbb{Z}^{26}$.

Na primjer, za

$$v = (0,1,0,0,0,1),$$

je

$$vM = (0,2,0,0,0,1,0,0,0,0,1,1,0,1,0,0,0,0,0,1,0,1,0,2,1,0,1).$$

Broj pozitivnih komponenti od vM naziva se *broj bodova* od v. U našem primjeru broj bodova od v je 10. Općenito, broj bodova od v je neki broj između 0 i 27.

Step figura konstruira se tako da se složi 6 nizova brojeva iz $\{0,1\}$, jedan na drugi, a nizovi imaju duljine redom 17, 19, 21, 23, 25 i 26. Primjer jedne step figure je sljedeći:

1 1 1 0 0 1 1 0 0 0 1 0 1 0 1 1 0
0 0 0 1 1 1 0 0 1 0 0 0 1 0 0 0 1 0 0
1 0 1 0 0 0 1 0 1 0 0 1 0 0 0 0 1 0 0 1 0
0 1 1 0 0 0 1 0 1 0 0 1 0 0 1 0 1 0 0 0 1 0 1
0 0 0 0 1 0 0 1 0 0 1 0 0 1 1 0 0 0 1 0 1 0 0 1 0
0 1 1 0 0 1 0 0 0 1 0 1 0 0 1 0 1 0 1 0 0 1 0 1 0 0

Za razliku od matrica, step figura ograničenja vezanih za broj jedinica. Step figura generira beskonačan niz 6-dimenzionalnih vektora koje dobivamo iz njezinih stupaca,

s time da, kad se neki redak završi, on kreće iz početka. Na primjer, prva dva vektora u navedenom primjeru su (1,0,1,0,0,0) i (1,0,0,1,0,1), dok su 18., 19. i 20. vektor (1,0,0,0,0,0), (1,0,0,0,1,1) i (1,0,1,0,0,0).

Rotori u mašini odgovaraju step figuri, a kavez matrici M, odnosno matrica i step figura predstavljaju ključ za šifiranje pomoću M-209.

Nakon opisa matrice i step figure, može se krenuti na šifriranje. Neka je x_i numerička vrijednost i-tog slova u otvorenom tekstu, te h_i broj bodova i-tog vektora generiranog step figurom. Tada je šifrat y_i jednak

$$y_i = h_i - x_i - 1 \mod 26$$

odnosno,

$$x_i = h_i - y_i - 1 \mod 26$$

što znači da je ključ za šifiranje i dešifiranje isti. Također je važno primijetiti da su duljine redaka step figure u parovima relativno prosti brojevi što znači da je period niza generiranog step figurom jednak $17 \cdot 19 \cdot 21 \cdot 23 \cdot 25 \cdot 26 \approx 10^8$ iako u nekim specifičnim situacijama period može biti kraći. Na primjer, ako u step figuri nema nula, tada je (1,1,1,1,1,1) jedini generirani vektor pa je period jednak 1. Također, preporuča se izbjegavati ključeve u kojima je malo jedinica ili malo nula u matrici M, odnosno malo jedinica u step figuri.

Primjer 3.4.1. Neka je dan otvoren tekst

`UVIJEK JE DOBRO VRIJEME DA BI SE CINILO DOBRO`

te matrica M i step figura kao gore navedeno. Navedeni otvoreni tekst ima duljinu 37, a numerički ekvivalenti slova su redom
20, 21, 8, 9, 4, 10, 9, 4, 3, 14, 1, 17, 14, 21, 17, 8, 9, 4, 12, 4, 3, 0, 1, 8, 18, 4, 2, 8, 13, 8, 11, 14, 3, 14, 1, 17, 14.
Brojevi bodova vektora generiranih step figurom su redom
7, 15, 17, 6, 13, 14, 13, 9, 15, 6, 12, 13, 10, 9, 23, 4, 17, 4, 18, 7, 15, 8, 16, 21, 12, 6, 0, 13, 6, 24, 0, 16, 19, 0, 10, 16, 10.
Sada primjenom formule $y_i = h_i - x_i - 1 \mod 26$, $i = 1, \ldots, 37$, dobiva se šifrat

`MTIWI DDELR KVVNF VHZFC LHOMT BXESP QBPLI YV`

Bitno je primijetiti da se u otvorenom tekstu dva puta javlja niz slova `DOBRO`, no ona su se šifrirala jednom kao `LRKVV`, a drugi put kao `PLIYV`.

3.5 Kriptoanaliza

Sigurnost naprave za kriptiranje M-209 bila je dobra, no šifrat se mogao dešifrirati ručno od strane protivnika nakon što su saznali unutarnje postavke naprave. To se činilo pomoću kappa testa koji rabi indekse slučajnosti. Tehniku je napravio William F. Friedman tijekom 1920. Tijekom uporabe, M-209 je mogao doći u situacije gdje su rotori bili u bliskim pozicijama pa su naprave stvarale podudarajuće tekstove. Kappa test je koristio te podudarajuće tekstove te pomagao osobi koja dešifrira da sazna postavke rotora i kaveza.

Nijemci su uspjeli doći do većeg broja M-209 naprava te su dobro upoznali njezin način rada. Do 1943. godine naučili su da određene postavke daju određene uzorke pomoću kojih se lakše mogu otkriti postavke rotora i šipka u kavezu te time dešifrirati poruke duljine oko 150 slova. Ako je osoba koja dešifrira imala sreće, 35 slova je moglo biti dovoljno, no dešifriranje je svejedno bilo veoma dugotrajno. Zbog velikog broja mogućnosti postavki naprava je bila korištena ne samo za vrijeme Drugog svjetskog rata, već i za vrijeme Korejskog rata, no budući da je bilo poznato da je poruku moguće dešifrirati, na poruke se moralo reagirati unutar vremena za koje bi se poruka mogla dešifrirati.

Oko 1970. godine, kriptoanalizu naprave M-209 napravilu su Dennis Ritchie - kreator programskog jezika C, Robert Morris - jedan od osnivača UNIX operacijskog sistema i šef znanstvenika NSA tijekom ranih 90-tih te Jim Reed - matematičar kojemu je kriptografija bila hobi. Rezultat njihovog rada bio je računalni program koji je u relativno kratkom vremenu mogao dešifrirati polovinu tekstova duljine 2000 slova i gotovo sve tekstove duljine veće od 2500 slova.

Njihov rad je bio napisan i spreman za objavu u časopisu Cryptologia magazine, ali nakon dogovora s NSA, njihov rad nikad nije bio objavljen. Iako NSA u to vrijeme više nije imala interesa za M-209, još uvijek su u upotrebi bile mnoge naprave za kriptiranje koje su koristile slična načela pa je njihov rad mogao naštetiti vladi koja je koristila te naprave.

Uz rad od strane Reedsa, Ritcihiea i Morrisa koji nikad nije objavljen, nekoliko publicikacija opisale su različite metode napada samo pomoću šifrata na M-209. Prema deklasificiranim izvješćima TICOM I-175 i DF-120, njemački kriptolozi za vrijeme Drugog svjetskog rata uspjeli su izračunati postavke mašine iz šifrata u specijalnim slučajevima, poput poruke „in-depth“. Ti specijalni slučajevi uključivali su poruke poslane s jednakim postavkama kao prijašnje, poruke koje su bile poslane više puta ili poruke kod kojih su se postavke rotora malo razlikovale. Također, razvili su

statističku metodu određivanja jesu li poruke bile „in-depth“ u potpunosti ili samo djelomično te je su li korišteni dodatni mehanički ili električki uređaju kod slanja. Uz to, razvijali su više generički napad uz primjenu statističkih napada. Prema izvješću TICOM I-45, uspjeli su samo razbiti poruke s više od 5000 slova.

U svojoj knjizi iz 1977. godine, Barker opisuje napad na šifrat baziran na statističkoj analizi ferkvencije distribucije obrazaca koja se primjenjuje na svaku iglicu određenog rotora. Na primjer, rotor broj 6 ima 17 iglica. Taj rotor napravi potpunu rotaciju nakon 17 slova. Prema Barkerovoj metodi, kriptograf koji to pokušava dešifrirati sakuplja frekvencije slova za svaki od 17 iglica na rotoru broj 6. Za iglicu 1 on sakuplja statistiku za šifrirana slova na pozicijama 1, 18, 35, itd.. Za iglicu 2 sakuplja podatke na pozicijama 2, 19, 36, itd. Jednaki princip primjenjuje se i za ostale iglice na zadanom rotoru. Za poruku duljine od 2500 slova može se prikupiti frekvencija slova za uzorak od $N = \frac{2500}{17} = 147$ slova za svaku iglicu rotora 6. Ostali rotori se također rotiraju, no s različitim ciklusima te se statistike za frekvenciju njihovih slova prikupljaju u skladu s tim. Nadalje, za svaki mogući par iglica p_a i p_b u određenom rotoru, provodi se Chi test na F_a i F_b, koja su distribucije frekvencije slova za iglice p_a i p_b po formuli:

$$\sum_{l=A}^{Z} \frac{F_a[l] \cdot F_b[l]}{N_a \cdot N_b},$$

gdje su N_a i N_b su ukupni broj uzoraka za iglicu p_a, tj. p_b. Rezultat na Chi test ukazuje koliko su bliske distribucije frekvencije slova za iglice p_a i p_b. Za svaki dani rotor frekvencije slova za iglice u aktivnom stanju očekuje se da se razlikuje od frekvencije slova za iglice koje su u neaktivnom stanju jer samo iglice u aktivnom stanju uzrokuju pomak, dok iglice u neaktivnom stanju ne. Chi test također se rabi da bi se odredile iglice određenog rotora u dvije posebne klase. Jedna se klasa sastoji od iglica koje su vjerojatno u neaktivnom stanju, a druga klasa od iglica u aktivnom stanju. Barker opisuje načine identificiranja tih klasa i rješavanja nesigurnih slučajeva. Proces se ponavlja za sve ostale rotore uračunavajući rezultate dobivene na prijašnjim rotorima sve dok se postavke iglica na svim rotorima ne otkriju. Na kraju dobiva natrag postavke mašine. Barker demonstrira tu tehniku na teoretskom uređaju sa 4 rotora i ne prikazuje nikakve kvantitativne analize o učinku metode. U njihovoj knjizi iz 1982. godine, Barker i Piper prezentiraju sličnu metodu. Predlažu drugačiju metodu podijele iglica u klase i načina rješavanja nesigurnih slučajeva te demonstriraju tu metodu na napravi M-209 sa porukom od 3000 slova. Otvoreni tekst ove poruke ima neuobičajeno veliki broj razmaka (slova Z). Barker i Piper tvrde da njihova metoda generalno radi i sa šifratima od 2500 slova te nerijetko i sa 2000 slova, no ne pružaju nikakve detaljne kvantitivne analize. Zanimljivo, ti brojevi su slični brojevima iz

Ritchiejeve procjene iako je Ritchie tvrdio da Reeds-Ritchie-Morris metoda je bila drugačija od Barkerove metode. Budući da je metoda razvijena od strane Barker-Piper slična Barkerovoj metodi, taj se komentar vjerojatno odnosi i na tu metodu. Kasnije je Rivest prezentirao teoretsku analizu pokazujući da je potrebno 8000 slova za kriptoanalizu pomoću Barker Chi metode. No, zaključio je da je u praksi 2000 do 4000 slova često dovoljno. Ostale metode napada na šifrat su Sullivanova metoda koja koristi podijeli pa vladaj pristup, four-stage Hillclimbing metoda, itd.

Jedan od načina dešifriranja moguć je ukoliko kriptoanalitičar posjeduje dva ili više šifrata dobivenih šifriranjem različitih otvorenih tekstova jednakim ključevima za šifriranje, ili ključevima koji su "bliski", tako da se ključne riječi dobivene pomoću njih podudaraju na nekim segmentima. U tom slučaju može se primijeniti tzv. Kerckhoffsova metoda superpozicije. Pomoću nje može se odrediti odgovarajući segment ključne riječi, a potom, koristeći razne tehnike u ovisnosti o kojem je stroju riječ, to se može iskoristiti za rekonstrukciju čitavog ključa. Ukratko, Kerckhoffsova metoda glasi:

Pretpostavimo da su otvoreni tekst $x_1x_2\ldots x_n$ i šifrat $y_1y_2\ldots y_n$ povezani relacijama

$$y_i = x_i + k_i \mod 26 \text{ ili } y_i = k_i - x_i \mod 26.$$

Tada se iz dva šifrata dobivena istim ključem može eliminirati ključ:

$$y_i - y_i' = x_i - x_i' \mod 26 \text{ ili } y_i - y_i' = x_i' - x_i \mod 26.$$

Sada se svaka hipoteza o otvorenom tekstu $x_1x_2\ldots x_n$ može testirati na otvorenom tekstu $x_1'x_2'\ldots x_n'$, te tako hipotezu prihvatiti ili odbaciti. Jasno, metoda je još efikasnija ukoliko postoji više od dva šifrata dobivena istim ključem.

Primjenu Kerckhoffsove metode opisujemo u sljedećem primjeru.

Primjer 3.5.1. Pretpostavimo da su šifrati

```
C R U D L H G C A S
X V X D U X K U I A
```

dobiveni istim ključem po pravilu $y_i = x_i + k_i \mod 26$.

Kod dešifriranja, dobro je koristiti saznanja o vjerojatnim početcima poruka te podatcima o najčešćim prvim slovima u riječima. U hrvatskom jeziku to su slova S, P, N, D, I.

Pretpostavimo da otvoreni tekst počinje sa `SA`. Tada iz

$$X - C + S = 23 - 2 + 18 \equiv 13 \pmod{26} = N,$$

te

$$V - R + A = 4 = E$$

proizlazi da drugi otvoreni tekst počinje s NE. Nadalje, dobro je pogledati u rječnik koji su najčešći nastavci riječi koje započinju sa SA, odnosno NE. U ovom slučaju to su za SA slova M, V, N, a za NE slova P, O, D. Pretpostavka da je $x_3 = \mathrm{M}$, V ili N daje da je $x'_3 = \mathrm{P}$, Y ili Q što sugerira da prvi tekst počinje sa SAM, a drugi sa NEP. Četvrto slovo bi trebalo biti jednako u oba otvorena teksta i tu se kao najvjerojatnija nameću slova O i A, s time da je O ipak vjerojatnije. Dakle, početci riječi bili bi: SAMO i NEPO. U rječniku se kao vjerojatni nastavci prve riječi nalaze slova B, H, K, O, P, S, T, U, koji za x'_5 daju redom K, Q, T, X, Y, B, C, D, dok su vjerojatni nastavci za drugu riječ B, D, K, M, P, R, S, V. Kao najvjerojatnije nameću se dvije mogućnosti:

```
S A M O U        S A M O S
N E P O D        N E P O B
```

U prvom slučaju, vjerojatni nastavci prve riječi su B, P, V, što za x'_6 daje R, F, L, dok su nastavci druge riječi su M, N, O pa se ta mogućnost može barem privremeno odbaciti. U drugom slučaju, vjerojatni nastavak prve riječi je T, a druge I ili J. Budući da $x_6 = \mathrm{T}$ povlači $x'_6 = \mathrm{J}$, čini se vrlo vjerojatnom kombinacija

```
S A M O S T
N E P O B J
```

Sada je već jasno da je druga riječ NEPOBJEDIV, što za prvu riječ daje SAMOSTALAN.

Bibliografija

[1] Andrej Dujela, Marcel Maretić : Kriptografija, Element 2007. (srpanj, 2018.)

[2] *Boris Hagelin*, dostupno na `https://en.wikipedia.org/wiki/Boris_Hagelin`, (lipanj, 2018.)

[3] *Ciphertext-Only Cryptanalysis of Hagelin M-209*, dostupno na `https://pdfs.semanticscholar.org/c435/6f47fa9a2749b059d0fbf40d4cfea10df802.pdf`, (srpanj, 2018.)

[4] *Crypto Museum*, dostupno na https://en.wikipedia.org/wiki/Cryptography (rujan, 2018.)

[5] *Crypto Museum*, dostupno na `http://cryptomuseum.com/index.htm`, (lipanj, 2018.)

[6] *Hagelin Ciphers*, dostupno na `http://ciphermachines.com/hagelin`, (lipanj, 2018.)

[7] *History of the Hagelin Cipher Machines*, dostupno na `http://users.telenet.be/d.rijmenants/en/hagelin.htm`, (lipanj 2018.)

[8] *Operating Instructions for CSP-1500 (a.k.a. M-209)*, dostupno na `https://maritime.org/tech/csp1500inst.htm`, (lipanj, 2018.)

[9] Robert Churchhouse: Codes and Ciphers, Cambridge, 2004.

[10] *The Hagelin M-209 Cipher Machine*, dostupno na `https://www.slideshare.net/JohnAndrBjrkhaug/bjorkhaug2013m209`, (lipanj, 2018.)

[11] *The Story of HAGELIN-CRYPTOS*, dostupno na `http://www.cryptomuseum.com/crypto/hagelin/files/hagelin_story_en.pdf`, (lipanj, 2018.)

[12] *U.S. M-209 Simulator 3.0*, dostupno na `http://users.telenet.be/d.rijmenants/en/m209sim.htm`, (lipanj, 2018.)

[13] *Vigenereova sifra*, dostupno na https://hr.wikipedia.org/wiki/Vigen%C3%A8reova_%C5%A1ifra, (srpanj, 2018.)

Sažetak

Tijekom povijesti uvijek je postojala potreba za tajnom komunikacijom. Razvoj radio tehnologije i potreba za sigurnijim šiframa potaknula je mnoge izumitelje na razvoj naprava za šifriranje. Tako je Boris Hagelin u 20. stoljeću izumio napravu za šifriranje C-38 koja je u američkoj vojsci dobila naziv M-209. Hagelinova naprava M-209 bila je naprava za šifriranje, ispred svog vremena. Uz to, naprava M-209 bila je relativno malena, mogla je izvoditi operacije šifriranja i dešifriranja poruka te je bila potpuno mehanička i nije zahtijevala nikakav izvor energije. No, jedan od nedostataka naprave bile su unutarnje postavke koje je trebalo postavljati svaki put kod upotrebe što je bio izazov za vojnike na bojnim poljima.

U ovom diplomskom radu opisana je naprava M- 209 te su navedeni njezini glavni dijelovi i karakteristike. Također, opisan je postupak šifriranja koji se temelji na Beaufortovoj s matematičkog i mehaničkog gledišta.

Summary

Throughout history, there was always a need for secret communication. The growth of radio technology and the lookout for more secure encryption have inspired many inventors to develop encryption devices. So, in the 20th century, Boris Hagelin invented an encryption device called C-38 which was adopted by US Army under the name of M-209. Hagelin's M-209 was far in front of its time; it could perform encryption and decryption operations, it was relatively small, compact, portable and completely mechanical that needs no electricity or any other power source to operate. One of the disadvantages was that internal settings should be placed each time before use, which was quite a challenge for soldiers in battlefields.

In this graduate thesis, the M-209 device is described with its main parts and characteristics. Also, the encryption process, based on Beaufort's cipher, is elaborated from both a mechanical and mathematical perspective.

Životopis

Rođen sam 10.5.1991. u Čakovcu. Pohađao sam I. osnovnu školu Čakovec koju sam završio 2006. godine. Zatim sam upisao Ekonomsku i trgovačku školu u Čakovcu smjer ekonomist gdje sam maturirao 2010. godine. Iste godine upisao sam Preddiplomski sveučilišni studij matematike smjer: nastavnički na Prirodoslovno-matematičkom fakultetu u Zagrebu koji sam završio 2014. godine. Iste godine upisao sam Diplomski sveučilišni studij matematike i informatike smjer: nastavnički također na Prirodoslovno-matematičkom fakultetu u Zagrebu čijom ću diplomom steći zvanje magistra edukacije matematike i informatike.