Uvod u kriptografiju

Burazin, Ines

Master's thesis / Diplomski rad

2015

Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj: **Josip Juraj Strossmayer University of Osijek, Department of Mathematics / Sveučilište Josipa Jurja Strossmayera u Osijeku, Odjel za matematiku**

Permanent link / Trajna poveznica: https://urn.nsk.hr/urn:nbn:hr:126:878654

Sveučilište J.J. Strossmayera u Osijeku
Odjel za matematiku
Sveučilišni nastavnički studij matematike i informatike

Ines Burazin

Uvod u kriptografiju

Diplomski rad

Osijek, 2015.

Sveučilište J. J. Strossmayera u Osijeku
Odjel za matematiku
Sveučilišni nastavnički studij matematike i informatike

Ines Burazin

Uvod u kriptografiju

Diplomski rad

Voditelj: izv.prof.dr.sc. Ivan Matić

Osijek, 2015.

Sadržaj

1 Uvod

Kriptografija je znanstvena disciplina koja se bavi proučavanjem metoda za slanje poruka u takvom obliku da ih samo onaj kome su namijenjene može pročitati. Kako danas živimo u vremenu u kojemu su informacije dostupne, vrlo je važna njihova zaštita ukoliko ne želimo da dođu u krive ruke. Komunikacija je oduvijek bila bitan stoga se rano razvila svijest o razvoju šifri i kodova koje može pročitati samo ona osoba kojoj su namijenjene. Danas je komunikacija dostupna putem Interneta te je povezala sve korisnike u globalnu mrežu te je slanje elektroničke pošte je postalo dio naše svakodnevice. Informacije su dostupne svima, komunikacija je brža, a isto tako se mijenja i način poslovanja tvrtki. Svakodnevno se putem Interneta razmjenjuju velike količine podataka te je potrebna njihova zaštita i tu na scenu nastupa kriptografija. Kroz godine su se razvijale šifre koje su bile suočene s pokušajima napada. Danas, kada privatnost nije zaštićena i tehnologija se svakim danom sve brže razvija teško je pronaći najbolji mehanizam za zaštitu i čuvanje podataka . Svakodnevno pojavljuje se veći broj stručnjaka specijaliziranih za kriptografiju, isto tako se pojavljuje i sve veći broj zlouporabe privatnih podataka te se kriptografija nalazi u jednom nezavidnom položaju suočena s mnogobrojnim teškoćama svakodnevnog suvremenog života.

2 Modularna aritmetika, grupe, konačna polja

2.1 Modularna aritmetika

Većina ovog rada će se baviti primjenama modularne aritmetike s obzirom da je ključna za razumijevanje moderne kriptografije, a posebno za kriptosustave s javnim ključem. Stoga, u ovom poglavlju uvodimo temeljne koncepte i tehnike koje će nam biti potrebne.
Ideja modularne aritmetike je zapravo vrlo jednostavna i identična je satnoj aritmetici koju učite u školi. Na primjer, pretvaranje 24-satni sustav u 12-satni sustav je jednostavno. Vrijednost u 24-satnom sustavu se smanjuje za 12. Na primjer, 13:00 sati u 24-satnom sustavu je 1 sat u 12-satnom s obzirom da je 13 modul 12 jednako 1.
Formalnije, određujemo pozitivan cijeli broj N. Za dva cijela broja a i b pišemo $a = b \pmod N$ ako N dijeli $b - a$, a mi kažemo da su a i b kongruentni modulo N.
Iz praktičnih razloga definiramo $\mathbb{Z}/N\mathbb{Z} = 0, \ldots, N-1$.
što je potpun sustav ostataka modulo N. Skup $\mathbb{Z}/N\mathbb{Z}$ ima dvije osnovne operacije, zbrajanje i množenje koji su definirani u očitom obliku. Na primjer,

$$(11 + 13) \pmod{16} \equiv 24 \pmod{16} = 8$$
$$24 = 1 \cdot 16 + 8$$

i

$$(11 \cdot 13) \pmod{16} \equiv 143 \pmod{16} = 15$$
$$143 = 8 \cdot 16 + 15.$$

2.2 Grupe i prstenovi

Zbrajanje i množenje modulo N ima sljedeća svojstva:

1. Zatvorenost obzirom na zbrajanje; za sve $a, b \in \mathbb{Z}/N\mathbb{Z} : a + b \in \mathbb{Z}/N\mathbb{Z}$.
2. Zbrajanje je asocijativno; za sve $a, b, c \in \mathbb{Z}/N\mathbb{Z} : (a + b) + c = a + (b + c)$.
3. 0 je neutralni element zbrajanja; za svaki $a \in \mathbb{Z}/N\mathbb{Z} : a + 0 = 0 + a = a$.
4. Inverz zbrajanja uvijek postoji: za svaki $a \in \mathbb{Z}/N\mathbb{Z} : a + (N - a) = (N - a) + a = 0$.
5. Zbrajanje je komutativno; za sve $q, b \in \mathbb{Z}/N\mathbb{Z} : a + b = b + a$.
6. Zatvorenost obzirom na množenje; za sve $a, b \in \mathbb{Z}/N\mathbb{Z} : a \cdot b \in \mathbb{Z}/N\mathbb{Z}$.
7. Množenje je asocijativno; za sve $a, b, c \in \mathbb{Z}/N\mathbb{Z} : (a \cdot b) \cdot c = a \cdot (b \cdot c)$.
8. Množenje s 1 daje uvijek taj broj; za svaki $a \in \mathbb{Z}/N\mathbb{Z} : a \cdot 1 = 1 + a = a$.
9. Distributivnost množenja prema zbrajanju; za sve $a, b, c \in \mathbb{Z}/N\mathbb{Z} : (a+b) \cdot c = a \cdot c + b \cdot c$.
10. Množenje je komutativno; za sve $a, b \in \mathbb{Z}/N\mathbb{Z} : a \cdot b = b \cdot a$.

Mnogi od skupova sadrže ova svojstva tako da im dajemo posebna imena.

Definicija 2.1. *Uredeni par $(G, *)$, gdje je G skup s binarnom operacijom $*$ na G, nazivamo grupa ako su ispunjeni sljedeći uvjeti:*

1. *Za sve $a, b \in G$ vrijedi $a * b \in G$; (zatvorenost)*
2. *Za sve $a, b, c \in G$ vijedi $a * (b * c) = (a * b) * c$; (asocijativnost)*
3. *Postoji jedinični element e, tj. postoji element za kojeg vrijedi da je za sve $a \in G, e*a = a * e = a$;*
4. *Za svaki $a \in G$ postoji inverzni element a^{-1}, tj. element za kojeg vrijedi da je $a*a^{-1} = a^{-1} * a = e$;*

Grupa koja je komutativna se često naziva Abelova ako za sve $a, b \in G$ vrijedi $a * b = b * a$.

Gotovo sve grupe u kriptografiji su Abelove s obzirom da je komutativost svojstvo ono koje ga čini zanimljivo kriptografiji. Dakle, svaki skup sa svojstvima 1,2,3 i 4 se zove grupa, dok su skupovi sa svojstvima 1,2,3,4 i 5 Abelove grupe.
Standardni primjeri koje susrećemo u srednjoj školi su:

- Cijeli brojevi, prirodni ili imaginarni brojevi u zbrajanju. Identitet je 0, a suprotno od x je $-x$, jer $x + (-x) = 0$;
- Skup racionalnih, realnih ili kompleksnih brojeva bez nule obzirom na množenje Ovdje je identitet 1, a suprotno od x je x^{-1}, jer je $x \cdot x^{-1} = 1$.

Grupa se zove multiplikativna ako namjeravamo pisati operaciju te grupe na isti način kao i operaciju za množenje

$$f = g \cdot h \quad \text{i} \quad g^5 = g \cdot g \cdot g \cdot g \cdot g.$$

Rabimo zapis $(G, \cdot)$ u ovom slučaju ako postoji kakva nejasnoća vezana uz operaciju koju koristimo na G.
Grupa se zove aditivna ako namjeravamo pisati operaciju te grupe na isti način kao i operaciju zbrajanja.

$$f = g + h \quad \text{i} \quad 5 \cdot g = g + g + g + g + g.$$

U ovom slučaju rabimo zapis $(G, +)$. Abelova grupa G se naziva cikličkom ako postoji poseban element $a \in G$ zvan generator tako da vrijedi $G = \{a^k | k \in \mathbb{Z}\}$. Tada kažemo da je G ciklička grupa generirana elementom a. Na primjer, cijeli brojevi u zbrajanju, svaki se pozitivan cijeli broj može dobiti ponovljenim zbrajanjem broja 1. Na taj način 7 se može izraziti kao $7 = 1 + 1 + 1 + 1 + 1 + 1 + 1$.
Svaki negativni cijeli broj se može dobiti od pozitivnog cijelog broja koristeći obrnuti znak od zbrajanja, $x \to -x$. Dakle 1 je generator cijelih brojeva obzirom na zbrajanje. Ako je g generator cikličke grupe G, često pišemo $G = \langle g \rangle$.
Kao i grupe, definiramo prstenove.

Definicija 2.2. *Prsten je skup sa dvije operacije uglavnom označene sa $+$ i $*$ za zbrajanje i množenje što zadovoljava svojstva navedena od 1 do 9. Prsten možemo označiti i kao uređenu trojku $(R, +, *)$.*

Ako je slučaj da je množenje komutativno onda kažemo da je i prsten komutativan.
Ovo se može činiti kompliciranim, ali se zapravo radi o skupovima koje rabimo cijelo vrijeme, na primjer, beskonačni komutativni prsteni cijelih brojeva, realnih ili imaginarnih brojeva. Zapravo, u kriptografiji su stvari jednostavne jer samo trebamo uzeti u obzir konačne prstene kao komutativni prsten cijelih brojeva modulo N, $\mathbb{Z}/N\mathbb{Z}$.

2.3 Multiplikativan inverz modulo N

Upravo smo vidjeli da kada želimo riješiti jednadžbe oblika $ax \equiv b \pmod{N}$ najvažnije je ispitati kada cijeli broj a modulo N ima multiplikativnu inverz, odnosno, postoji li broj c kao $a \cdot c \equiv c \cdot a \equiv \pmod{N}$.
Takva vrijednost c se često piše kao a^{-1} i očito je rješenje jednadžbi $ax \equiv 1 \pmod{N}$.
Dakle, inverz od a postoji samo onda kada su a i N relativno prosti, odnosno kada je najveći zajednički djelitelj $(a, N) = 1$. Posebno je zanimljivo kada je N prost p.
Jer tada za sve nenul vrijednosti od $a \in \mathbb{Z}/N\mathbb{Z}$ uvijek dobijemo jedinstveno rješenje jednadžbe $ax \equiv 1 \pmod{p}$. Dakle, ako je p prost broj onda svaki nenul element u $\mathbb{Z}/N\mathbb{Z}$ ima multiplikativnu inverz.
Prsten kao $\mathbb{Z}/N\mathbb{Z}$ sa ovim svojstvom se zove polje.

Definicija 2.3. *Polje je skup s dvije operacije $(G, +, \cdot)$ na način da:*

- *$(G, +)$ je Abelova grupa s neutralnim elementom označenim s 0,*
- *$(G \setminus \{0\}, \cdot)$ je Abelova grupa,*
- *$(G, +, \cdot)$ zadovoljava distributivnost.*

Dakle, polje je komutativni prsten za koji svaki nenul element ima multiplikativni ineverz.
Definiramo sve skupove svih invertibilnih elemenata u $\mathbb{Z}/N\mathbb{Z}$ sa

$$(\mathbb{Z}/N\mathbb{Z})^* = \{x \in \mathbb{Z}/N\mathbb{Z} : (x, N) = 1\}.$$

* u A^* za bilo koji prsten A se odnosi na najveći podskup A koji formira grupu obzirom na množenje.
Dakle, skup $(\mathbb{Z}/N\mathbb{Z})^*$ je grupa obzirom na množenje. U posebnom slučaju kada je N prost p imamo

$$(\mathbb{Z}/p\mathbb{Z})^* = \{1, \ldots, p-1\}$$

jer je svaki nenul element iz skupova $\mathbb{Z}/p\mathbb{Z}$ relativno prost sa p. Za proizvoljno polje $\mathbb{F}$, skup $\mathbb{F}^*$ je jednak skupu $\mathbb{F} \setminus \{0\}$. Kako bi olakšali zapis za ovaj važan slučaj, definiramo
$\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z} = \{0, \ldots, p-1\}$,
$\mathbb{F}_p^* = \mathbb{Z}/p\mathbb{Z} = \{1, \ldots, p-1\}$.
Skup $\mathbb{F}_p$ je konačno polje karakteristike p. U nastavku ćemo diskutirati o općenitijima konačnim poljima.
Završit ćemo ovaj dio sa najvažnijim teoremom teorije konačnih grupa.

Teorem 2.4 (Posljedica Lagrangovog teorema)**.** *Ako $(G, \cdot)$ je grupa reda n tada za sve $a \in G$ vrijedi da je $a^n = 1$.*

Teorem 2.5 (Mali Fermatov teorem)**.** *Pretpostavka je da je p prost i $a \in \mathbb{Z}$ tada vrijedi da je $a^p \equiv a \pmod{p}$.*

2.4 Najveći zajednički djelitelj

U prethodnom dijelu smo rekli da ako želimo riješiti, $a \cdot x \equiv b \pmod{N}$ u cijelim brojevima ili $a\alpha \equiv b \pmod{f}$ za polinominalne modulo a prosti, trebali smo izračunati najveći zajednički djelitelj. To je bilo osobito važno u određivanju $a \in \mathbb{Z}/N\mathbb{Z}$ ili $a \in \mathbb{F}_p[X/f]$ im multiplikativni inverz. Što znači, najveći zajednički djelitelj $(a, N) = 1$ ili najveći zajednički

djelitelj $(a, f) = 1$.
Nismo objasnili kako se taj najveći zajednički djelitelj izračunava, niti smo objasnili kako se suprotna operacija izračunava kada znamo da postoji. Sada ćemo se posvetiti tom propustu time što ćemo objasniti jedan od najstarijih algoritama poznatog čovjeku, naravno, radi se o Euklidovom algoritmu.
Kada bismo bili u mogućnosti faktorizirati a i N na proste brojeve ili a i f u ireducibile polinome, onda bi izračun najvećeg zajedničkog djelitelja bio izrazito lak. Npr. ako

$$a = 230895588646864 = 2^4 \cdot 157 \cdot 4513^3$$

$$b = 33107658350407876 = 2^2 \cdot 157 \cdot 2269^3 \cdot 4513$$

onda kroz faktorizaciju lako izračunati najveći zajednički djelitelj kao

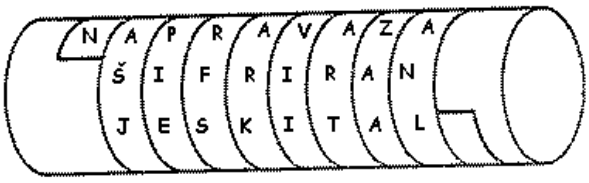
$$(a, b) = 2^2 \cdot 157 \cdot 2269^3 \cdot 4513.$$

Međutim, faktorizacija je preduga operacija za cijele brojeve, ali izračun najvećeg zajedničkog djelitelja je lako, a to ćemo i pokazati. Iako, faktorizacija polinoma prostog stupnja modulo a je jako jednostavna, čini se da gotovo svi algoritmi koji služe za faktorizaciju polinoma zahtijevaju algoritamski postupak kako bi izračunali najveći zajednički djelitelj. Stoga, u obje situacije moramo biti sposobni izračunati najveći zajednički djelitelj bez pribjegavanja faktorizaciji.

3 Klasične šifre

3.1 Uvod

Kriptografija je znanstvena disciplina koja se bavi proučavanjem metoda za slanje poruka u takvom obliku da ih samo onaj kome su namijenjene može pročitati. Sama riječ kriptografija je grčkog podrijetla i mogla bi se doslovno prevesti kao *tajnopis*.
Neki elementi kriptografije bili su prisutni već kod starih Grka. Naime, Spartanci su u 5. stoljeću prije Krista upotrebljavali napravu za šifriranje zvanu *skital*. To je bio drveni štap oko kojeg se namotavala vrpca od pergamenta, pa se na nju okomito pisala poruka. Nakon upisivanja poruke, vrpca bi se odmotala, a na njoj bi ostali izmiješani znakovi koje je mogao pročitati samo onaj tko je imao štap jednake debljine. Algoritam šifriranja, ili šifra, je



Slika 3.1: Naprava za šifriranje skital

sredstvo pretvaranja otvorenog teksta u šifrat pod kontrolom tajnog ključa. Ovaj proces se naziva enkripcija ili šifriranja. Pišemo

$$c = e_k(m),$$

gdje je

- m otvoreni tekst,
- e je funkcija šifre,
- k je tajni ključ,
- c je šifrat.

Obrnuti proces se naziva dekriptiranje ili dešifriranje i pišemo

$$m = e_k(c).$$

Uzmite u obzir da su algoritmi šifriranja i dešifriranja e, d javni, tajnost m dana c u potpunosti ovisi o tajnosti k.

Gornji postupak zahtijeva da svaka stranka treba pristup tajnom ključu. Treba biti poznat objema stranama, ali se treba držati u tajnosti. Algoritmi šifriranja koji imaju ovo svojstvo nazivaju se simetrični kriptosustavi ili kriptosustavi s tajnim ključem. Postoji oblik kriptografije koji koristi dvije različite vrste ključa, jedan je javno dostupan i služi za šifriranje, dok je drugi privatni i koristi za dešifriranje. Ove potonji vrste kriptosustava nazivaju se asimetrični kriptosustavi ili kriptosustavi s javnim ključem, na koje ćemo se vratiti u sljedećem poglavlju.

Obično su u kriptografiji strane koje komuniciraju označene sa A i B. Međutim, često koristimo korisnicima prilagođenija imena poput Alice i Bob. No ne bi trebali pretpostaviti

da su stranke nužno ljudi, mogli bismo opisivati komunikaciju koja se odvija između dva autonomna stroja. Prisluškivač, loša djevojka, protivnik ili napadač obično dobivaju ime Eva.

Definicija 3.1. *Kriptosustav je uređena petorka* $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ *za koju vrijedi:*

1. $\mathcal{P}$ *je konačan skup svih mogućih osnovnih elementa otvorenog teksta;*
2. $\mathcal{C}$ *je konačan skup svih mogućih osnovnih elemenata šifrata;*
3. $\mathcal{K}$ *je prostor ključeva, tj. konačan skup svih mogućih ključeva;*
4. *Za svaki* $K \in \mathcal{K}$ *postoji funkcija šifriranja* $e_K \in \varepsilon$ *i odgovarajuća funkcija dešifriranja* $dK \in \mathcal{D}$. *Pritom su* $eK : \mathcal{P} \to \mathcal{C}$ *i* $dK : \mathcal{C} \to \mathcal{P}$ *funkcije sa svojstvom da je* $d_K(e_K(x)) = x$ *za svaki otvoreni tekst* $x \in \mathcal{P}$.

U ovom poglavlju ćemo predstaviti neke povijesne šifre koje su korištene u predračunalno doba za šifriranje podataka. Pokazat ćemo da je ove šifre lako probiti čim shvatimo statistiku temeljnog jezika, u našem slučaju engleskog.

Slovo	Postotak	Slovo	Postotak
A	8.2	N	6.7
B	1.5	O	7.5
C	2.8	P	1.9
D	4.2	Q	0.1
E	12.7	R	6.0
F	2.2	S	6.3
G	2.0	T	9.0
H	6.1	U	2.8
I	7.0	V	1.0
J	0.1	W	2.4
K	0.8	X	0.1
L	4.0	Y	2.0
M	2.4	Z	0.1

Tablica 3.1: Frekvencija slova u engleskoj abecedi

Slika 3.2: Učestalost engleskih slova

Raspodjela učestalosti engleskih slova dana je u Tablici 3.1 i grafički prikazana na Slici 3.2.Kao što se može vidjeti najčešće slova su E i T. Često pomaže da znate statistiku drugog reda o osnovnom jeziku, kao koji su najčešći nizovi dva ili tri slova, pod nazivom

bigrami i trigrami. Najčešći bigrami u engleskom dani su u Tablici 3.2, s pripadajućim približnim postocima. Najčešće trigrami su, prema opadajućem redoslijedu,

$$THE,\ ING,\ AND,\ HER,\ ERE,\ ENT,\ THA,\ NTH,\ WAS,\ ETH,\ FOR.$$

Naoružani ovim informacijama o engleskom sada smo u mogućnosti ispitati i probiti niz povijesnih šifri.

Bigram	Postotak	Bigram	Postotak
TH	3.15	HE	2.51
AN	1.72	IN	1.69
ER	1.54	RE	1.48
ES	1.45	ON	1.45
EA	1.31	TI	1.28
AT	1.24	ST	1.21
EN	1.20	ND	1.18

Tablica 3.2: Frekvencija engleskih bigrama

3.2 Šifra pomaka

Prvo predstavljamo jednu od prvih šifri, naziva šifra pomaka. Šifriranje se provodi zamjenom svakog slova sa slovom koje je udaljeno određeni broj mjesta u abecedi. Tako na primjer, ako je ključ bio tri, onda će A u otvorenom tekstu biti zamijenjeno šifriranim D, slovo B će biti zamijenjeno s E i tako dalje. Riječ $HELLO$ u otvorenom tekstu bit će kodirana kao šifrirani tekst $KHOOR$. Kada se ta šifra koristi s ključem tri, to se često naziva Cezarova šifra, iako je u mnogim knjigama ime Cezarova šifra ponekad dano šifri pomaka s bilo kojim ključem. To nije sasvim točno, jer postoje dokazi da se Julije Cezar koristio šifrom s ključem tri.

Postoji više matematičko objašnjenje šifre pomaka koje će nam koristiti u nastavku rada. Prvo moramo identificirati svako slovo abecede s brojem. Uobičajeno je da se slovo A identificira s brojem 0, slovom B s brojem 1, slovo C s brojem 2 i tako dalje dok ne slovo Z s brojem 25. Nakon što smo pretvoriti našu poruku iz otvorenog teksta u niz brojeva, šifrirani tekst dobiva se tako to se svakom broju pridruži tajni ključ k modulo 26, gdje je ključ je broj u rasponu od 0 do 25. Na taj način možemo tumačiti supstitucijske šifre kao protočnu šifru, s nizovnim ključem danim ponavljajućim nizom

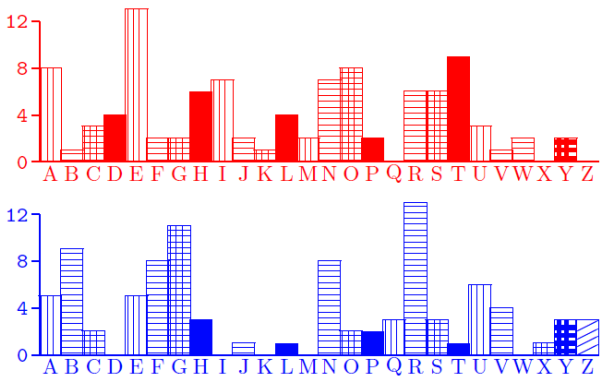
$$k, k, k, \ldots$$

Ovaj nizovni ključ nije veoma nasumičan, što rezultira lakim probijanjem šifre pomaka. Naivan način razbijanja šifre pomaka je jednostavno isprobavanje svakog od mogućih ključeva dok se ne pronađe pravi. Postoji samo 26 mogućih ključeva tako da je vrijeme za ovo pretraživanje ključeva veoma malo, pogotovo ako je lako prepoznati otvoreni tekst kad je dešifriran.

Pokazat ćemo kako probiti šifru pomaka pomoću statistike korištenog jezika. Iako to nije strogo potrebno za razbijanje ove šifre, kasnije ćemo vidjeti primjenu šifre koja se pak sastoji od niza šifri pomaka i onda će sljedeće statističke tehnike biti korisne. Koristeći statističku tehniku na šifri pomaka također je poučno u pogledu kako se statistika temeljnog otvorenog

teksta može pojaviti u rezultirajućem šifriranom tekstu. Uzmi sljedeći primjer šifriranog teksta, koji, budući da je javno poznat zapisujemo u plavoj boji. GB OR, BE ABG GB OR: GUNG VF GUR DHRFGVBA: JURGURE 'GVF ABOYRE VA GUR ZVAQ GB FHSSRE GUR FYVATF NAQ NEEBJF BS BHGENTRBHF SBEGHAR, BE GB GNXR NEZF NTNVAFG N FRN BS GEBHOYRF, NAQ OL BCCBFVAT RAQ GURZ? GB QVR: GB FYRRC; AB ZBER; NAQ OL N FYRRC GB FNL JR RAQ GUR URNEG-NPUR NAQ GUR GUBHFNAQ ANGHENY FUBPXF GUNG SYRFU VF URVE GB, 'GVF N PBAFHZZNGVBA QRIBHGYL GB OR JVFU'Q. GB QVR, GB FYRRC; GB FYRRC: CREPUNAPR GB QERNZ: NL, GURER'F GUR EHO; SBE VA GUNG FYRRC BS QRNGU JUNG QERNZF ZNL PBZR JURA JR UNIR FUHSSYRQ BSS GUVF ZBEGNY PBVY, ZHFG TVIR HF CNHFR: GURER'F GUR ERFCRPG GUNG ZNXRF PNYNZVGL BS FB YBAT YVSR.

Jedna od tehnika za razbijanje prethodnog uzorka šifriranog teksta je da se primijeti da šifrirani tekst i dalje zadržava podatke o duljinama riječi originalnog otvorenog teksta. Na primjer šifrirano slovo N pojavljuje se kao riječ s jednim slovom. Pošto su jedine riječi u engleskom s jednim slovom A (član) i I (ja) možemo zaključiti da je ključ ili 13, jer je N trinaesto slovo od A u abecedi, ili je ključ jednak 5 jer je N pet slova udaljeno od I u abecedi. Dakle, pouka je da se ovdje uvijek uklone razmaci između riječi iz originalnog otvorenog teksta prije šifriranje pomoću šifre pomaka. No, čak i ako zanemarimo ove informacije o riječima još uvijek možemo probiti ovu šifru analizom učestalosti. Računamo učestalost slova u šifriranom tekstu i uspoređujemo ih s učestalosti koje su dobivene iz engleskog jezika koje smo vidjeli na Slici 3.2.
Na Slici 3.3 predstavljamo dva stupčasta dijagrama jedan iznad drugog tako da možete vidjeti da jedan dijagram izgleda gotovo kao pomak drugog dijagrama. Statistike dobivene iz uzorka šifriranog teksta prikazana je plavo, dok su statistike dobivene od jezika originalnog otvorenog teksta prikazane crveno. Naglasimo da ne računamo crvene statistike od stvarnog otvorenog teksta, jer to još ne znamo, mi samo koristimo znanja o temeljnom jeziku.



Slika 3.3: Usporedba učestalosti otvorenog teksta i šifriranog teksta za primjer šifre pomaka

Usporedbom dva stupčasta dijagrama na Slici 3.3 možemo vidjeti koliko mislimo da je plavi dijagram pomaknut u odnosu na crveni dijagram. Ispitivanjem gdje mislimo da je pomaknuto slovo E otvorenog teksta, možemo pogađati da je pomaknuto za jedan od sljedećih brojeva

$$2,\ 9,\ 13\ \textit{ili}\ 23.$$

Zatim pokušavajući zaključiti koliko je slovo A otvorenog teksta pomaknuto možemo naga-

đati da je pomaknuta za jedan od sljedećih brojeva

1, 6, 13 *ili* 17.

Jedina vrijednost pomaka koji je dosljedan čini se da je vrijednost 13, a možemo zaključiti da je to najvjerojatnije vrijednost ključa. Sada pomoću ključa možemo otključati šifrirani tekst. To otkriva da je originalni otvoreni tekst sljedeći:

To be, or not to be: that is the question:
Whether 'tis nobler in the mind to suffer
The slings and arrows of outrageous fortune,
Or to take arms against a sea of troubles,
And by opposing end them? To die: to sleep;
No more; and by a sleep to say we end
The heart-ache and the thousand natural shocks
That flesh is heir to, 'tis a consummation
Devoutly to be wish'd. To die, to sleep;
To sleep: perchance to dream: ay, there's the rub;
For in that sleep of death what dreams may come
When we have shuffled off this mortal coil,
Must give us pause: there's the respect That
makes calamity of so long life.

"Biti ili ne biti"- to je pitanje.
Je l' dičnije za ljudski um sve praćke
I strjelice silovite sudbine
Podnositi il zgrabit oružje,
Oduprijet se i moru jada kraj
Učinit? Umrijet- usnut, ništa više!
I usnuvši dokončat srca bol
I prirodnih još tisuć' potresa.
Da živo ga poželiš! Umrijeti
- I usnut- usnut- pa i snivat možda!
Da- to je smetnja sva. Jer snovi, što
U smrtnom tome snu nas mogu snaći
Zemaljske ako muke stresemo,
Da to je što nam ruku ustavlja
I to je razlog što je nevolja
Dugovječna.

WONOJTL UOKSTAIWUW YVJ GONOLVCIAD TAG WZCCVJXIAD OAXJOCJOAOZJITL WXZGOAXW TAG WXTYY, TAG TIUW XV CLTQ T WIDAIYIKTAX JVLO IA XSO GONOLVCUOAX VY SIDS-XOKSAVLVDQ IAGZWXJQ IA XSO JODIVA.
XSO GOCTJXUOAX STW T LTJDO CJVDJTUUO VY JOWOTJKS WZCCVJXOG MQ IAGZWXJQ, XSO OZJVCOTA ZAIVA, TAG ZE DVNOJAUOAX JOWOTJKS OWXTMLIW-SUOAXW TAG CZMLIK KVJCVJTXIVAW. T EOQ OLOUOAX VY XSIW IW XSO WXJ-VAD LIAEW XSTX XSO GOCTJXUOAX STW HIXS XSO KVUCZXOJ, KVUUZA-IKTXIVAW, UIKJVOLOKXJVAIKW TAG UOGIT IAGZWXJIOW IA XSO MJIWXVL JODIVA . XSO TKT-GOUIK JOWOTJKS CJVDJTUUO IW VJDTAIWOG IAXV WO-NOA DJVZCW, LTADZTDOW TAG TJKSIXOKXZJO, GIDIXTL UOGIT, UVMILO TAG HOTJTMLO KVUCZXIAD, UTK-SIAO LOTJAIAD, RZTAXZU KVUCZXIAD, WQWXOU NOJIYIKTXIVA, TAG KJQCXVD-JTCSQ TAG IAYVJUTXIVA WOKZJIXQ.

Možemo izračunati sljedeće učestalosti za pojedina slova u gornjem šifriranom tekstu: Osim

Slovo	Učestalost	Slovo	Učestalost	Slovo	Učestalost
A	8.6995	B	0.0000	C	3.0493
D	3.1390	E	0.2690	F	0.0000
G	3.6771	H	0.6278	I	7.8923
J	7.0852	K	4.6636	L	3.5874
M	0.8968	N	1.0762	O	11.479
P	0.1793	Q	1.3452	R	0.0896
S	3.5874	T	8.0717	U	4.1255
V	7.2645	W	6.6367	X	8.0717
Y	1.6143	Z	2.7802		

Tablica 3.3: Frekvencija slova u gornjem šifratu

toga smo utvrdili da su najčešći bigrami u ovom šifriranom tekstu

$$TA, AX, IA, VA, WX, XS, AG, OA, JO, JV,$$

dok su najčešći trigrami

$$OAX, TAG, IVA, XSO, KVU, TXI, UOA, AXS.$$

Pošto se slovo O šifriranog teksta pojavljuje najčešće, točnije 11,479 puta, možemo pogoditi da slovo O šifriranog teksta odgovara slovu E otvorenog teksta. Sada pogledajte što to znači za dva uobičajena trigrama koja nalazimo u šifriranom tekstu.

- Trigram OAX u šifriranom tekstu odgovara E^{**}.
- Trigram XSO u šifriranom tekstu odgovara $^{**}E$.

Ispitujemo slične uobičajene trigrame na engleskom jeziku, koji počinju ili završavaju sa slovom E. Pronašli smo tri uobičajena ENT, ETH i THE. Budući da dva trigrama koja želimo spariti imaju jedan koji počinje s istim slovom s kojim drugi završava, možemo zaključiti da je vrlo vjerojatno da imamo sljedeće podudaranje

- $X = T$,
- $S = H$,
- $A = N$.

Čak i nakon ove male analize nalazimo da je mnogo lakše shvatiti što bi originalni otvoreni tekst trebalo biti. Ako se usredotočimo na prve dvije rečenice šifriranog teksta koju pokušavamo dešifrirati i promijenimo slova za koja smatramo da smo našli ispravna preslikavanja, onda dobivamo:

THE MJIWTVLJEDIVN HTW VNE VY EZJVCE'W LTJDEWT KVNKENTJTTIV NW VY HIDH TEKHNVLVDQ INGZWTJQ. KVUCZTEJW, KVUUZNIKTTIVNW TNG UIKJVELEKTJVNIKW TJE HELL JECJEWENTEG, TLVNDWIGE GIDITTL UEGIT, KVUCZTEJ DTUEW TNG ELEKTJVNIK KVUUEJKE.

Prisjetimo se da je to bilo nakon četiri zamjene

$$O = E, X = T, S = H, A = N.$$

Sada varamo i koristimo činjenicu da smo ustanovili duljine riječi u šifriranom tekstu. Vidimo da pošto se slovo T pojavljuje kao pojedinačno slovo šifriranog teksta da moramo imati

$$T = I \quad ili \quad T = A.$$

Slovo T šifriranog teksta pojavljuje se s vjerojatnosti od 8,0717, što je najveća vjerojatnost koja je ostala, pa je stoga mnogo vjerojatnije da imamo

$$T = A.$$

Već smo razmotrili najpopularniji trigram u šifriranom tekstu pa stoga usmjeravanjem pažnje na sljedeći najpopularniji trigram možemo vidjeti da je jednak TAG što pretpostavljamo da odgovara otvorenom tekstu AN^*. Stoga je veoma vjerojatno da je $G = D$, pošto je AND popularan trigram u engleskom jeziku.
Naš djelomično dešifrirani tekst sada je jednak

THE MJIWTVLJEDIVN HAW VNE VY EZJVCE'W LAJDEWT KVNKENTJATIV NW VY HIDH TEKHNVLVDQ INDZWTJQ. KVUCZTEJW, KVUUZNIKATIVNW AND UIKJVELEKTJVNIKW AJE HELL JECJEWENTED, ALVNDWIDE DIDITAL UEDIA, KVUCZTEJ DAUEW AND ELEKTJVNIK KVUUEJKE.

To bilo nakon šeste zamjene

$$O = E,\ X = T,\ S = H,\ A = N,\ T = A,\ G = D.$$

Sada promatramo riječi s dva slova koje se pojavljuju u šifriranom tekstu:

- IX Ovo odgovara otvorenom tekstu $^*T$. Stoga slovo I u šifriranom tekstu mora biti ili slovo A ili I otvorenog teksta, pošto su jedine dvije riječi engleskog jezika koje završavaju na T AT i IT. Već smo otkrili čemu odgovara slovo A otvorenog teksta, stoga moramo imati $I = I$.
- XV Ovo odgovara otvorenom tekstu $^*T$. Stoga, moramo imati $V = O$.
- VY Ovo odgovara otvorenom tekstu O^*. Stoga, slovo Y šifriranog teksta mora odgovarati ili F, N ili R. Već znamo slovo šifriranog teksta koje odgovara N. U šifriranom tekstu vjerojatnost pojave Y je 1,6, no u engleskom očekujemo F da se pojavi s vjerojatnosti 2,2 i R s vjerojatnosti 6,0. Stoga, vjerojatnije je da će biti $Y = F$.
- IW Ovo odgovara otvorenom tekstu I^*. Stoga, slovo W otvorenog teksta mora biti ili F, N, S ili T. Već imamo F, N, T, pa je stoga $W = S$.

Svi ovi zaključci pretvaraju šifrirani tekst u sljedeće

THE MJISTOLJEDION HAS ONE OF EZJOCE'S LAJDEST KONKENTJATIO NS OF HIDH TEKHNOLODQ INDZSTJQ. KOUCZTEJS, KOUUZNIKATIONS AND UIKJOELEKTJONIKW AJE HELL JECJESENTED, ALONDSIDE DIDITAL UEDIA, KOUCZTEJ DAUES AND ELEKTJONIK KOUUEJKE.

To bilo nakon deset zamjena

$$O = E,\ X = T,\ S = H,\ A = N,\ T = A,\ G = D,\ I = I,\ V = O,\ Y = F,\ W = S.$$

Sa utvrđenih pola slova šifriranog teksta već je veoma lako shvatiti originalni otvoreni tekst, koji je preuzet s web stranice Odjela za računalne znanosti Sveučilišta u Bristolu. Ostavljamo čitatelju da utvrdi konačne zamjene i dobije cijeli otvoreni tekst.

3.3 Vigenèreova šifra

Problem s šiframa pomaka i šiframa zamjene bio je da je svako slovo otvorenog teksta uvijek bilo šifrirano istim slovom šifriranog teksta. Stoga su se statistike originalnog jezika mogle koristiti za razbijanje šifre. Na primjer, bilo je jednostavno utvrditi koje slovo šifriranog teksta odgovara slovu E otvorenog teksta E. Od 1800. godine nadalje, dizajneri šifri pokušavali su probiti vezu između otvorenog teksta i šifriranog teksta.
Šifra zamjene koju smo koristili gore bila je mono-alfabetska šifra zamjene, tako da je korištena samo jedna abecedna zamjena za šifriranje čitave abecede. Jedan način za rješavanje našeg problema jest uzeti niz zamjenskih abeceda i zatim šifrirati svako slovo s drugom abecedom. Takav sustav naziva se polialfabetska šifra zamjene. Na prmjer možemo uzeti:

abecedu u otvorenom tekstu ABCDEFGHIJKLMNOPQRSTUVWXYZ,

abecedu u šifriranom tekstu TMKGOYDSIPELUAVCRJWXZNHBQF, te abecedu u šifriranom tekstu DCBAHGFEMLKJIZYXWVUTSRQPON. Tada slova otvorenog teksta na neparnom mjestu šifriramo pomoću abecede prvog šifriranog teksta, dok slova otvorenog teksta na pranim mjestima šifriramo pomoću druge abecede. Na primjer, riječ HELLO u otvorenom tekstu, koristeći gornje abecede, šifrira se u SHLJV. Zapazimo da se dva pojavljanja slova L u otvorenom tekstu šifriraju s dva različita slova šifriranog teksta. Stoga smo otežali korištenje statistike temeljnog jezika. Ako sada provedemo naivnu analizu učestalosti više nećemo dobiti zajedničko slovo šifriranog teksta koje odgovara slovu E otvorenog teksta. U osnovi šifriramo poruku po dva slova od jednom, pa stoga imamo blok šifru s duljinom bloka od dva slova engleskog jezika. U stvarnom životu mogli bi koristiti pet umjesto svega dvije abecede i rezultirajući ključ postaje odista veoma velik. S pet abeceda ukupni ključ ima

$$(26!)^5 \approx 2^{441},$$

no korisnik mora samo mora zapamtiti ključ koji je niz od

$$26 \cdot 5 = 130$$

slova. Međutim, kako bi otežali život napadaču, broj abeceda koje se koriste također bi trebao biti skriven od njegovog pogleda i od dijela ključa. No za prosječnog korisnika u ranim 1800ima to je bio isuviše nezgrapan sustav, pošto je ključ bio pretežak za pamćenje. Unatoč njegovim nedostacima, najpoznatija šifra tijekom 19. stoljeća temeljila se upravo na tom principu. Vigenèreova šifra izumljena je 1533 od strane Giovan Batista Belaso-a, te je bi varijacija na gornju temu, no ključ je bilo lako zapamtiti. Kada se gleda na jedan način Vigenèreova šifra je polialfabetska blok šifra, no kada se gleda na drugi način, to je šifra niza koja je prirodna generalizacija šifre pomaka.
Opis Vigenèreove šifre kao blok šifre uzima opis gornje polialfabetske šifre no ograničava moguće abecede otvorenog teksta na jednu od 26 mogućih cikličkih pomaka standardne abecede. Pretpostavimo da se koristi pet abeceda, to umanjuje prostor ključeva na

$$26^5 \approx 2^{23}$$

i veličina ključa koji je potrebno zapamtiti kao niz od pet brojeva je između 0 i 25.
Međutim, opis Vigenèreove šifre kao šifre niza je mnogo prirodniji. Baš poput šifre pomaka, Vigenèreova šifra ponovo identificira slova s brojevima $0, \ldots, 25$. Tajni ključ je kratak niz slova (npr. riječ) koji se ponavlja i formira nizovni ključ.

Šifriranje uključuje dodavanje slova otvorenog teksta slovu ključa. Stoga, ako je ključ *SESAME*, šifriranje je sljedeće,

THISISATESTMESSAGE

SESAMESESAMESESAME

LLASUWSXWSFQWWKASI.

Ponovo možemo primijetiti da će A biti šifrirano na drugo slovo ovisno o tome gdje se pojavljuje u poruci.

No Vigenereovu šifru je i dalje lako probiti koristeći temeljne statistike engleskog jezika. Jednom kad ustanovimo duljinu ključne riječi, razbijanje šifriranog teksta isto je kao i razbijanje šifre pomaka više puta.

Kao primjer, pretpostavimo da imamo sljedeći šifrirani tekst

UTPDHUG NYH USVKCG MVCE FXL KQIB. WX RKU GI TZN, RLS BBHZLXMSNP KDKS; CEB IH HKEW IBA, YYM SBR PFR SBS, JV UPL O UVADGR HRRWXF. JV ZTVOOV YH ZCQU Y UKWGEB, PL UQFB P FOUKCG, TBF RQ VHCF R KPG, OU KFT ZCQU MAW QKKW ZGSY, FP PGM QKFTK UQFB DER EZRN, MCYE, MG UCTFSVA, WP KFT ZCQU MAW KQIJS. LCOV NTHDNV JPNUJVB IH GGV RWX ONKCGTHKFL XG VKD, ZJM VG CCIMVGD JPNUJ, RLS EWVKJT ASGUCS MVGD; DDK VG NYH PWUV CCHIIYRD DBQN RWTH PFRWBBI VTTK VCGNTGSF FL IAWU XJDUS, HFP VHCF, RR LAWEY QDFS RVMEES FZB CHH JRTT MVGZP UBZN FD ATIIYRTK WP KFT HIVJCI; TBF BLDPWPX RWTH ULAW TG VYCHX KQLJS US DCGCW OPPUPR, VG KFDNUJK GI JIKKC PL KGCJ IAOV KFTR GJFSAW KTZLZES WG RWXWT VWTL WP XPXGG, CJ FPOS VYC BTZCUW XG ZGJQ PMHTRAIBJG WMGFG. JZQ DPB JVYGM ZCLEWXR: CEB IAOV NYH JIKKC TGCWXF UHF JZK.

WX VCU LD YITKFTK WPKCGVCWIQT PWVY QEBFKKQ, QNH NZTTW IRFL IAS VFRPE ODJRXGSPTC EKWPTGEES, GMCG TTVVPLTFFJ; YCW WV NYH TZYRWH LOKU MU AWO, KFPM VG BLTP VQN RD DSGG AWKWUKKPL KGCJ, XY OPP KPG ONZTT ICUJCHLSF KFT DBQNJTWUG. DYN MVCK ZT MFWCW HTWF FD JL, OPU YAE CH LQ! PGR UF, YH MWPP RXF CDJCGOSF, XMS UZGJQ JL, SXVPN HBG!

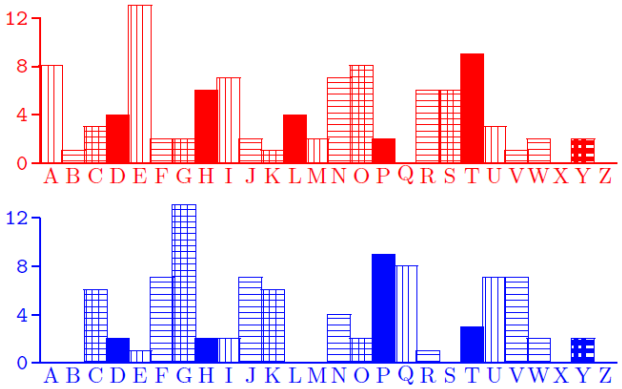
Postoji način pronalaženja duljine ključne riječi, koji se ponavlja kako bi se formirao nizovni ključ, koji nazivamo Kasinskijev test. Prvo moramo potražiti ponavljajuće nizove znakova. Prisjetimo se da engleski jezik ima veliko ponavljanje određenih bigrama ili trigrama i tijekom dovoljno dugog teksta postoji vjerojatnost da će se svako malo podudarati s ista dva ili tri slova u ključu. Pregledavajući udaljenost između ponovljenih nizova možemo pogoditi duljinu ključne riječi. Svaka od ovih udaljenosti trebala bi biti višekratnik ključne riječi, stoga bi uzimanje najvećeg zajedničkog nazivnika svih udaljenosti između ponovljenih nizova trebalo dati dobru aproksimaciju duljine ključne riječi.

Ispitajmo gornji šifrirani tekst i potražimo bigram WX. Razmaci između nekih ponavljanja ovog bigrama su 9, 21, 66 i 30, od kojih su se neki možda pojavili slučajno, dok neki možda otkrivaju informaciju o duljini ključne riječi. Sada uzimamo relevantne najveće zajedničke djelitelje kako bi pronašli,

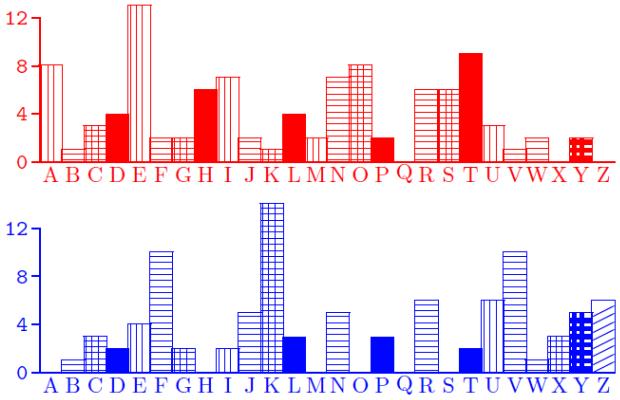
$$(30, 66) = 6, \ (3, 9) = (9, 66) = (9, 30) = (21, 66) = 3.$$

Malo je vjerojatno da ćemo imati ključnu riječ duljine tri pa stoga zaključujemo da su se razmaci od 9 i 21 pojavili slučajno. Stoga, možemo pogoditi da ključna riječ ima duljinu 6. Sada uzimamo svako šesto slovo i tražimo statistiku baš kao što smo to činili za šifru pomaka kako bi zaključili prvo slovo ključne riječi. Sada možemo vidjeti prednost korištenja histograma kako bi šifru pomaka razbili ranije. Ako koristimo naivnu metodu i pokušamo svaki od 26 ključeva možda i dalje nećemo moći detektirati koji ključ je točan, pošto svako šesto slovo engleske rečenice ne daje englesku rečenicu. U ovom slučaju je učinkovitije koristiti našu raniju metodu koja se temelji na histogramu.

Relevantni stupčasti dijagrami za svako šesto slovo počevši s prvim slovom dani su na Slici 3.4.Tražimo moguće lokacije tri vrha koja odgovaraju slovima A, E i T u otvorenom tekstu. Možemo zamijetiti da se čini da se ovaj niz pomiče za dvije pozicije na plavom grafu u usporedbi s crvenim grafom. Stoga možemo zaključiti da je prvo slovo ključne riječi C, pošto C odgovara pomaku za dva.



Slika 3.4: Usporedba učestalosti otvorenog teksta i šifriranog teksta za svako šesto slovo primjera Vigenereove šifre, počevši s prvim slovom



Slika 3.5: Usporedba učestalosti otvorenog teksta i šifriranog teksta za svako šesto slovo Vigenereovog primjera, počevši s drugim slovom

Obavljamo sličan korak za svako šesto slovo, počevši s drugim. Rezultirajući stupčasti dijagram dan je na Slici 3.5.Koristeći istu tehniku možemo ustanoviti da se čini da se plavi graf pomakao za 17 mjesta što odgovara drugom slovu ključne riječi jednakom R.

Nastavljajući na sličan način za preostala četiri slova ključne riječi možemo ustanoviti da je ključna riječ

$$CRYPTO.$$

Originalni osnovni tekst je tada sljedeći:

Scrooge was better than his word. He did it all, and infinitely more; and to Tiny Tim, who did not die, he was a second father. He became as good a friend, as good a master, and as good a man, as the good old city knew, or any other good old city, town, or borough, in the good old world. Some people laughed to see the alteration in him, but he let them laugh, and little heeded them; for he was wise enough to know that nothing ever happened on this globe, for good, at which some people did not have their fill of laughter in the outset; and knowing that such as these would be blind anyway, he thought it quite as well that they should wrinkle up their eyes in grins, as have the malady in less attractive forms. His own heart laughed: and that was quite enough for him. He had no further intercourse with Spirits, but lived upon the Total Abstinence Principle, ever afterwards; and it was always said of him,

that he knew how to keep Christmas well, if any man alive possessed the knowledge. May that be truly said of us, and all of us! And so, as Tiny Tim observed, God bless Us, Every One!

Gornji tekst je preuzet iz Božićne prče Charlesa Dickensa.

3.4 Permutacijska šifra

Definicija 3.2. *Neka je S skup od n elemenata i $r \in \mathbb{N}$. Tada je r-permutacija skupa S uređena r-torka $(x_1, x_2, \ldots, x_r)$ od koje su sve komponente $x_1, x_2, \ldots, x_r$ međusobno različiti elementi od S. Oznaka $P(n, r)$.*

Definicija 3.3. *Skup svih bijekcija $\{1, 2, \ldots n\}$ na $\{1, 2, \ldots, n\}$ označavamo s $(B(\{1, 2, \ldots, n\}), \circ)$ i zovemo grupom permutacija reda n. Operacija $\circ$ je komponiranje (permutacije su funkcije). Vrijedi $|S_n| = n!$. Napomenimo da ćemo permutaciju σ zapisivati na sljedeći način:*

$$\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix}$$

Ideja u pozadini supstitucijske šifre čini dio dizajna modernih simetričnih sustava. Druga komponenta koja se koristi u modernim simetričnim šiframa temelji se na permutacijama.

Permutacijske šifre su prisutne već čitav niz stoljeća. Ovdje ćemo opisati najjednostavniju, koju je posebice jednostavno probiti. Prvo utvrdimo grupu permutacija S_n i permutaciju

$$\sigma \in S_n$$

Vrijednost σ bit će tajni ključ. Kao primjer uzmimo

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 1 & 3 & 5 \end{pmatrix} = (1243) \in S_n.$$

Sad uzmimo neki otvoreni tekst recimo

"Once upon a time there was a little girl called snow white."

Razbijamo tekst u blokove od po 5 slova

onceu ponat imeth erewa salit tlegi rlcal ledsn owwhi te.

Prvo dopunjavamo poruku s nekim nasumičnim slovima kako bi bi mogli imati po pet slova u svakom bloku.

onceu ponat imeth erewa salit tlegi rlcal ledsn owwhi teahb.

Zatim uzimamo svaki blok od pet slova i zamjenjujemo slova u skladu s tajnom permutacijom σ. S našim primjerom dobivamo

coenu npaot eitmh eewra lsiat etgli crall dlsdn wohwi atheb.

Zatim uklanjamo prazna mjesta kako bi sakrili vrijednost n, te dobivamo šifrirani tekst.

coenunpaoteitmheewralsiatetglicralldlsdnwohwiatheb.

Međutim, razbijanje permutacijske šifre je jednostavno pomoću odabranog napada otvorenim tekstom, ako pretpostavimo da je grupa korištenih permutacija (npr. vrijednost od n) razumno mala. Kako bi napali ovu šifru pokrećemo odabrani napad otvorenim tekstom i tražimo od jedne od strana da šifriraju poruku

abcdefghijklmnopqrstuvwxyz,

kako bi dobili šifrirani tekst

cadbehfigjmknlorpsqtwuxvyz.

Zatim možemo zaključiti da permutacija izgleda poput

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & \cdots \\ 2 & 4 & 1 & 3 & 5 & 7 & 9 & 6 & 8 & 10 & 12 & 14 & 11 & 13 & 15 & \cdots \end{pmatrix}$$

Vidimo da se niz ponavlja (modulo 5) nakon svakih pet koraka pa je vrijednost od n vjerojatno jednaka pet. Ključ možemo povratiti ako jednostavno uzmemo prvih pet stupaca gornje permutacije.

3.5 Supstitucijske šifre

Znameniti rimski vojskovođa i državnik Gaj Julije Cezar u komunikaciji sa svojim prijateljima koristio se šifrom u kojoj su se slova otvorenog teksta zamjenjivala slovima što su se nalazila tri mjesta dalje od njih u alfabetu ($A \mapsto D$, $B \mapsto E$, itd.). Pretpostavljamo da se alfabet ciklički nastavlja, tj. da nakon zadnjeg slova Z, ponovo dolaze A, B, C. Ako bi smo upotrijebili današnji engleski alfabet od 26 slova, onda bi poznata Cezarova izreka

VENI VIDI VICI

bila šifrirana ovako:

YHQL YLGL YLFL.

Cezarovu šifru možemo pregledno zapisati na sljedeći način:

otvoreni tekst: 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

šifrat: 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

Koristit ćemo se engleskim alfabetom od 26 slova. Ukoliko ćemo raditi s otvorenim tekstom na hrvatskom jeziku, onda ćemo Č i Ć zamijeniti s C, a Đ, Dž, Lj, Nj, Š, Ž redom s DJ, DZ, LJ, NJ, S, Z. Danas se Cezarovom šifrom nazivaju i šifre istog oblika s pomakom različitim od 3. Da bismo Cezarovu šifru precizno definirali uvesti ćemo prirodnu korespodenciju između slova alfabeta ($A - Z$) i cijelih brojeva ($0 - 25$). Skup $0, 1, 2, \ldots, 25$ označavat ćemo sa $\mathbb{Z}_{26}$ i pretpostavljat ćemo da su na njemu definirane operacije zbrajanja, oduzimanja i množenja na isti način kao u skupu cijelih brojeva, ali tako da se rezultat (ukoliko nije iz skupa $0, 1, 2, \ldots, 25$) na kraju zamijeni s njegovih ostatkom pri dijeljenju s 26. Koristit ćemo oznake $a +_{26} b$ ili $(a + b) \pmod 2)6$, te analogno za oduzimanje i množenje. Skup $\mathbb{Z}_{26}$, uz operacije $+_{26}$ i $\cdot_{26}$ čini prsten. Potpuno analogno se definira skup $\mathbb{Z}_m$ i operacije na njemu za proizvoljan prirodan broj m.
Dakle, Cezarovu šifru možemo definirati na sljedeći način:

Definicija 3.4. *Neka je* $\mathcal{P} = \mathcal{C} = \mathcal{K} = \mathbb{Z}_{26}$. *Za* $0 \leq K \leq 25$ *definiramo*

$$e_K(x) = x + K \pmod{26}, \quad d_K(y) = y - K \pmod{26}.$$

Šifra je definirana nad $\mathbb{Z}_{26}$ budući da koristimo 26 slova, pa imamo sljedeću korespondenciju, koja za svako slovo alfabeta daje njegov "numerički ekvivalent":

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

$$0123456789101112131415161718192021222324 25$$

U Cezarovoj šifri su osnovni elementi otvorenog teksta slova, a ključ K određuje za koliko mjesta udesno ćemo pomicati slova pri šifriranju. Očito je $d_K(e_K(x)) = x$. Za $K = 3$ dobiva se originalna Cezarova šifra. Postoje naznake da je Cezarov nećak, prvi rimski car August, koristio najjednostavniju verziju ove šifre, pomičući slova samo za jedno mjesto u alfabetu, tj. uzimajući da je $K = 1$.

Primjer 3.5. *Dekriptirati šifru CQDQRVWW.*

Rješenje. C Q D Q R V W,
B P C P Q U V,
A O B O P T U,
ZNANOST.

K=3, rješenje je ZNANOST.

Kako bismo dobili sigurnije šifre, mogli bismo promatrati funkciju za šifriranje koja uključeviše o jednog parametra.
Najjednostavnija takva funkcija je afina funkcija $e(x) = ax + b$. No, tu se pojavljuje jedan novi problem jer takva funkcija na skupu $\mathbb{Z}_{26}$ ne mora imati inverz (ne mora biti injekcija). Zato parametar a ne može biti proizvoljan, već mora biti relativno prost s modulom 26. *Afina šifra* definira se na sljedeći način:

Definicija 3.6. *Neka je* $\mathcal{P} = \mathcal{C} = \mathbb{Z}_{26}$, *te neka je* $K = \{(a, b) \in \mathbb{Z}_{26} \times \mathbb{Z}_{26} : (a, 26) = 1\}$. *Za* $K = (a, b) \in \mathcal{K}$ *definiramo*

$$e_K(x) = ax + b \pmod{26}, d_K(y) = a^{-1}(y - b) \pmod{26}.$$

Ova šifra se zove afinom zato što su funkcije šifriranja afine.
Ovdje a^{-1} označava multiplikativni inverz broja a u prstenu $\mathbb{Z}_{26}$. Budući da broj 26 nije prost, nemaju svi elementi iz $\mathbb{Z}_{26}$ multiplikativni inverz, već ih imaju upravo brojevi koji su relativno prosti s 26, tj. za koje vrijedi da je najveći zajednički djelitelje od a i 26 jednak 1. Prikažimo te brojeve zajedno s njihovim inverzima:

a	1	3	5	7	9	11	15	17	19	21	23	25
a	1	9	21	15	3	19	7	23	11	5	17	25

Pr5imjer 3.7. *Neka je* $K = (5, 2)$. *Šifrirati otvoreni tekst Osijek.*

Rješenje. Koristeći ranije navedenu tablicu, slova otvorenog teksta poistovjećujemo s njihovim numeričkim ekvivalentima. Imamo:

$$5 \cdot 14 + 2 \equiv 20 \pmod{26},$$

$$5 \cdot 18 + 2 \equiv 14 \pmod{26},$$
$$5 \cdot 8 + 2 \equiv 16 \pmod{26},$$
$$5 \cdot 9 + 2 \equiv 21 \pmod{26},$$
$$5 \cdot 4 + 2 \equiv 22 \pmod{26},$$
$$5 \cdot 10 + 2 \equiv 2 \pmod{26},$$

pa je šifrat UOQVWC.

Osnovna metoda je analiza frekvencije slova. Broji se pojavljivanje svakog slova u šifratu, te se distribucija slova u šifratu uspoređuje s poznatim podatcima o distribuciji slova u jeziku na kojem pretpostavljamo da je napisan otvoreni tekst. Vrlo je vjerojatno da najfrekventnija slova šifrata odgovaraju najfrekventnijim slovima jezika. Ta vjerojatnost je to veća što je dulji šifrat. Također, korisni mogu biti i podatci o najčešćim *bigramima* i *trigramima* u jeziku. Kod nizova od četiri ili više slova, frekvencije već uvelike ovise o sadržaju teksta, i najfrekventniji nizovi obično dolaze od jedne riječi koja se često ponavlja u tesktu (npr. osobnog imena).
Začetci analize frekvencija se mogu naći u 14. stoljeću u djelu arapskog autora Ibn ad-Duraihima. Njegova zapažanja su objavljena u odjeljku posvećenom kriptologiji u velikoj enciklopediji u četrnaest svezaka čiji je autor Qalqashandi. Odjeljak ima naslov "O skrivanju tajnih poruka u pismima". Nedavno pronađeni rukopisi sugeriraju međutim da su arapski lingvisti tu metodu poznavali možda i pet stoljeća ranije. Čini se da su u europskoj kriptografiji metodu analize frekvencija u kriptoanalizi prvi počeli koristiti talijanski kriptografi u 15. stoljeću. Naime, poznato je da su svoje poruke šifrirali na način da su najfrekventnija slova zamjenjivali s više različitih simbola, pa na osnovu toga možemo zaključiti da im je bilo poznato kako analiza frekvencija slova može dovesti do razbijanja supstitucijske šifre. Za razliku od znanstvenika ad-Duraihima, oni svoja saznanja nisu javno objavljivali, već su ih nastojali što bolje unovčiti. Naime, mnoge su tadašnje talijanske kneževine imale ljude plaćene za razbijanje šifriranih poruka (jedan od najpoznatijih je venecijanski "tajnik za šifre" Giovanni Soro), i taj se posao često prenosio unutar obitelji.
Usprkos velikom prostoru ključeva, supstitucijska šifra vrlo laka za kriptoanalizu. To je bilo poznato već početkom 15. stoljeća, kada je u Italiji počela uporaba homofona, tj. šifriranje najfrekventnijih slova s više različitih simbola. Tu se ne zamjenjuje slovo za slovo, već npr. slovo za dvoznamenkasti broj, tako da je moguće šifrirati najfrekventnija slova na nekoliko različitih načina, dok će ona niskofrekventna i dalje imati samo jednu zamjenu. To svakako povećava sigurnost šifre, ali i dalje analiza frekvencija bigrama i trigrama može dovesti do rješenja. Također se može iskoristiti djelomično ponavljanje.

3.6 Playfairova šifra

Polialfabetska šifra gdje su osnovni elementi otvorenog teksta blokovi slova. Ovu bigramsku šifru (jer se šifriraju parovi slova) je izumio britanski znanstvenik Charles Wheatstone 1854. godine, a ime je dobila po njegovom prijatelju barunu Playfairu od St. Andrewsa koji ju je popularizirao.
Algoritam za šfriranje se bazira na 5×5 matrici slova koju konstruiramo koristeći ključnu riječ. Unosimo redom i bez ponaljanja prvo sva slova ključne riječi, a zatim preostala slova abecede. Na primjer, ako je ključna riječ PLAYFAIR, onda matrica izgleda ovako:

$$\begin{matrix} P & L & A & Y & F \end{matrix}$$

$$IJ \quad R \quad B \quad C \quad D$$

$$E \quad G \quad H \quad K \quad M$$

$$N \quad O \quad Q \quad S \quad T$$

$$U \quad V \quad W \quad X \quad Z$$

Budući da imamo 25 slova, dogovor je da se slova I i J poistovjete. U slučaju da je otvoreni tekst na hrvatskom jeziku, mi ćemo poistovjećivati V i W da bismo izbjegli moguće nesporazume kod dešifriranja.
Šifriranje se sada vrši na sljedeći način. Najprije podijelimo otvoreni tekst na blokove od po dva slova. Pritom pazimo da se niti jedan blok ne sastoji od dva jednaka slova, te da je duljina teksta parna. I jedno i drugo postižemo umetanjem npr. slova X ukoliko je to potrebno.
Kod šifriranja bloka od dva slova, mogu nastupiti tri slučaja, ovisno o položaju slova u matrici:

1. Slova se nalaze u istom retku. Tada ih zamijenimo sa slovima koja se nalaze za jedno mjesto udesno (ciklički, tj. iza najdesnijeg slova dolazi najljevije slovo iz istog retka). Npr. $EH\ GK$, $ST\ TN$, $FP\ PL$.

2. Slova se nalaze u istom stupcu. Tada ih zamijenimo sa slovima koja se nalaze za jedno mjesto ispod (ciklički, tj. iza najdonjeg slova dolazi najgornje slovo iz istog stupca). Npr. $OV\ VL$, $KY\ SC$, $PI\ IE$.

3. U protivnom, pogledamo pravokutnik koji određuju ta dva slova, te ih zamijenimo s preostala dva vrha tog pravokutnika. Redoslijed je određen tako da najprije dođe ono slovo koje se nalazi u istom retku kao prvo slovo u polaznom bloku. Npr.$OC\ SR$, $RK\ CG$, $PD\ FI$.

Primjer 3.8. *Neka je ključna riječ PLAYFAIR, a otvoreni tekst KRIPTOGRAFIJA.*

Rješenje. Kako smo slova I i J poistovijetii, a trebali bi se nalaziti u jednom blo zajedno, dodat ćemo slovo X između. Sada je niz priprdajućih bigrama $KR\ IP\ TO\ GR\ AF\ IX\ JA$. Sada šifrirajmo otvoreni tekst:

$$KRIPTOGRAFIxJA \longmapsto GCEINQOGYPCUBP.$$

Playfairova šifra ima nekoliko značajnih prednosti pred supstitucijskom šifrom. Budući da je šifra bigramska, gube se u šifratu jednoslovne riječi (npr. a) koje dosta utječu na frekvencije. Bigramsko šifriranje smanjuje na polovicu broj elemenata dostupnih analizi frekvencije. S druge strane, broj bigrama je puno veći od broja individualnih slova (26 slova - 676 bigrama), dok su frekvencije najfrekventnijih bigrama puno ujednačenije od frekvencija najfrekventnijih slova.
Iz ovih razloga, Playfairova šifra je dugo vremena smatrana sigurnom. Tako je bila standardna šifra u britanskoj vojsci za vrijeme 1. svjetskog rata, a čak je korištena (za šifriranje poruka manje važnosti) i u američkoj vojsci u 2. svjetskom ratu.
Ipak, kod dugih tekstova ova šifra postaje nesigurna jer se može iskoristiti analiza frekvencija bigrama. Poznato je da i kod ove šifre dio strukture jezika ostaje sačuvan.

3.7 Hillova šifra

Lester Hill je 1929. godine izumio kriptosustav kod kojeg se m uzastopnih slova otvorenog teksta zamjenjuje s m slova u šifratu. Radi se o poligramskoj šifri. Ukoliko broj slova u originalnom otvorenom tekstu nije djeljiv s m, poruku trebamo nadopuniti da bismo je mogli podijeliti u blokove od po m slova. Kriptosustav je definiran na sljedeći način:

Definicija 3.9. *Neka je m fiksan prirodan broj. Neka je $\mathcal{P} = \mathcal{C} = \mathbb{Z}_{26}^m$, te*

$$\mathcal{K} = m \times m \text{ invertibilne matrice nad } \mathbb{Z}_{26}.$$

Za $K \in \mathcal{K}$ definiramo

$$e_K(x) = xK,$$
$$d_K(y) = yK^{-1},$$

gdje su sve operacije u prstenu $\mathbb{Z}_{26}$.

Hill je preporučio uporabu invertibilnih matrica. To teoretski smanjuje sigurnost, jer je prostor ključeva manji, ali olakšava postupak šifriranja i dešifriranja. Napomenimo da je matrica invertibilna u $\mathbb{Z}_{26}$ ako i samo ako joj determinanta ima inverz u $\mathbb{Z}_{26}$, tj. ako je $(\det A, 26) = 1$.

Primjer 3.10. *Neka je*

$$K = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{pmatrix}$$

te neka je otvoreni tekst PJESMA.

Njegov numerički ekvivalent je $(15, 9, 4, 18, 12, 0)$. Računamo:

$$\begin{pmatrix} 15 & 9 & 4 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{pmatrix} = \begin{pmatrix} 79 & 107 & 135 \end{pmatrix} \pmod{26} = \begin{pmatrix} 1 & 3 & 5 \end{pmatrix} = BDF$$

$$\begin{pmatrix} 18 & 12 & 0 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{pmatrix} = \begin{pmatrix} 66 & 96 & 126 \end{pmatrix} \pmod{26} = \begin{pmatrix} 14 & 18 & 22 \end{pmatrix} = OSW$$

Dakle šifrat je BDFOSW.
HOvu šifru je vrlo lako probiti pomoću napada "poznati otvoreni tekst", a pogotovo pomoću napada "odabrani otvoreni tekst". To je i razlog zašto ovaj sustav gotovo uopće nije bio u praktičnoj uporabi.

4 Simetrične šifre

4.1 Uvod u simetrične šifre

Simetrična šifra funkcionira pomoću sljedeće dvije transformacije

$$c = e_k(m),$$

$$m = d_k(c)$$

gdje je

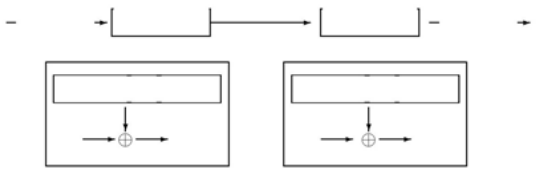
- m otvoreni tekst,
- e je funkcija šifriranja,
- d je funkcija dešifriranja,
- k je tajni ključ,
- c je šifrat.

Treba napomenuti da je poželjno da su i funkcija šifriranja i dešifriranja javno poznate i da tajnost poruke, s obzirom na šifrirani tekst, u potpunosti ovisi o tajnosti tajnog ključa, k. Iako je ovaj dobro utvrđeni princip, pod nazivom Kerckhoffsov princip, poznat od sredine 19. stoljeća, mnoge tvrtke ga još uvijek ignoriraju. Postoje slučajevi tvrtki koje implementiraju vlastite tajne sheme šifriranja koje se pokažu nesigurnima čim netko oda pojedinosti algoritama. Najbolje sheme bit će one koje su mnogi ljudi proučavali jako dugo, a za koje je utvrđeno da ostaju sigurne. Shemu koja predstavlja poslovnu tajnu ne može proučavati nitko izvan tvrtke.
Gornja postava naziva se sustav simetričnog ključa jer obje stranke trebaju pristup tajnom ključu. Ponekad se kriptografija simetričnog ključa provodi pomoću dva ključa, jednim za šifriranje i jednim za dešifriranje. Međutim, ako je to slučaj pretpostavimo da je s obzirom na ključ za šifriranje lako izračunati ključ za dešifriranje (i obrnuto).
Broj mogućih ključeva mora biti vrlo velik. To je zato što u izradi šifre pretpostavljamo najgori slučaj i dajemo napadaču prednost

- punog poznavanja algoritma šifriranja/dešifriranja,
- niz parova otvorenih/šifriranih tekstova povezanih s ciljanim ključem k.

Ako je broj mogućih ključeva mali tada napadač može probiti sustav pomoću iscrpnog pretraživanja. Napadač šifrira jedan od danih otvorenih tekstova svim mogućim ključevima i određuje koji ključ daje dotični šifrirani tekst. Dakle, prostor ključeva mora biti dovoljno velik da se izbjegne takav napad. Obično se pretpostavlja da će računanje s 2^{80} koraka biti nemoguće čitav niz godina, stoga bi ključna veličina prostora trebala bi biti barem 80 bitova kako bi se izbjeglo iscrpno pretraživanje.
Dizajner šifre mora igrati dvije uloge, onu nekoga tko pokušava provaliti šifru, kao i onoga koji kreira šifru. Trenutno, iako postoji mnogo teorija iza dizajna šifri, mi se još uvijek pouzdamo u simetrične šifre za koje se samo smatra da su jake, a ne one za koje znamo razlog zašto su jake. Sve to znači da ih najbolji pokušaji najiskusnijih kriptoanalitičara ne mogu probiti. To treba usporediti s šiframa s javnim ključem, tamo gdje sada postoji teorija

koja nam omogućuje da utvrdimo koliko je jaka dotična šifra (s obzirom na neke eksplicitne računalne pretpostavke).
Slika 4.1 opisuje jednostavan model za šifriranje bitova, koji je, iako jednostavan, sasvim primjeren za praktične implementacije. Ideja ovog modela je primijeniti reverzibilnu operaciju na otvoreni tekst



Slika 4.1: Jednostavan model za šifriranje bitova

kako bi se dobio šifrirani tekst, točnije, kombiniranjem otvorenog teksta s "nasumičnim nizom". Primatelj može stvoriti izvorni otvoreni tekst primjenom inverzne operacije, u ovom slučaju kombiniranjem šifriranog teksta s istim nasumičnim nizom.
Ovo je posebice učinkovito pošto možemo koristiti najjednostavniju operaciju dostupnu na računali, točnije isključivo-ILI ili XOR, kako ćemo, jednostavnosti radi, nadalje u radu ovu operaciju i nazivati $\oplus$. Ako je ključ različit za svaku poruku i ključ je dug koliko i poruka, onda se može dokazati da je takav sustav posve siguran, točnije imamo metodu šifriranja „One Time Pad“ ili OTP tj. XOR. Međutim, one-time pad nije praktičan u mnogim situacijama, npr. ukoliko

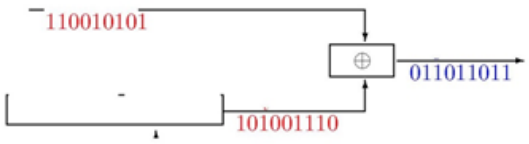
- želimo koristiti kratki ključ za šifriranje duge poruke,
- želimo ponovno koristiti ključeve.

Moderni simetrične šifre omogućuju oba ova svojstva, ali ovo je na štetu gubitka našeg svojstva savršene tajnosti. Razlog za to je što korištenje one-time pad-a proizvodi velike probleme distribucije ključeva. Vidjet ćemo da čak i višekratna upotreba kratkih ključeva proizvodi loše (ali ne tako loše) probleme distribucije ključa.
Postoji nekoliko načina za napad bulk šifri, od kojih neke navodimo u nastavku. Našu ćemo raspravu podijeliti na pasivne i aktivne napade; pasivni napad je općenito lakše provesti nego aktivni.

- Pasivni napadi: Ovdje je protivniku dopušteno samo vidjeti šifrirane poruke. Tada pokušava probiti kriptosustav bilo pronalaženjem ključa ili određivanjem neke tajne za koju stranke koje komuniciraju nisu htjele da procuri. Jedan čest oblik pasivnog napada je analiza prometa, tehnika posuđene iz vojske u Prvom svjetskom ratu, gdje je nagli porast radio prometa u određenom trenutku na zapadnoj fronti signalizirao neposrednu ofenzivu.
- Aktivni napadi: Ovdje je protivniku dopušteno umetanje, brisanje ili ponovno pregledavanje poruka između dvije strane koje komuniciraju. Opći uvjet je da neotkriven napad ubacivanja treba zahtijevati razbijanje šifre, dok šifra treba omogućiti otkrivanje i oporavak od brisanja ili ponovljenih napada.

Bulk simetrične šifre uglavnom dolaze u dvije varijante: slijedne šifre koje odjednom djeluju na jednoj točki podataka (bit / slovo) i blok šifre koje odjednom djeluju na blokovima podataka (npr. 64 bita).

4.2 Osnove slijednih šifri



Slika 4.2: Objašnjenje slijedne šifre

Slika 4.2 daje jednostavno objašnjenje slijedne šifre. Primijetimo kako je to vrlo slično našem prethodnom jednostavnom modelu. Međutim, slučajni bitovni tok se sada proizvodi iz kratkog tajnog ključa pomoću javnog algoritma, nazvanog generator nizovnog ključa. Stoga imamo $c_i = m_i \oplus k_i$ gdje su

- $m_0, m_1, \ldots$ bitovi otvorenog teksta,
- $k_0, k_1, \ldots$ bitovi nizovnog ključa,
- $c_0, c_1, \ldots$ bitovi šifriranog teksta.

To znači

$$m_i = c_i \oplus k_i$$

tj. dešifriranje je ista operacija kao i šifriranje.
Slijedne šifre kao ova gore opisana su jednostavne i brze za implementaciju. Omogućavaju veoma brzo šifriranje velike količine podataka, pa su stoga primjerene za audio i video signale u stvarnom vremenu. Također, nema propagiranja greške, te ako jedan bit šifriranog teksta postane raskomadan tijekom prijenosa (zbog napadača ili slabog radio signala) samo će taj jedan dešifrirani otvoreni tekst biti pod utjecajem.
Slijedne šifre imaju sljedeći problem; isti ključ se koristi dva puta daje isti nizovi ključ, koji može otkriti odnose između poruka. Na primjer pretpostavimo da su m_1 i m_2 šifrirani istim ključem k, onda protivnik može utvrditi XOR dva otvorena teksta ne znajući koji su otvoreni tekstovi

$$c_1 \oplus c_2 = (m_1 \oplus k) \oplus (m_2 \oplus k) = m_1 \oplus m_2.$$

Poznato i za kriptografiju važnost svojstva operacije XOR je da za proizvoljne bitove a i b vrijedi $(a \oplus b) \oplus b = a$, čime invertiranje postaje jednostavno ukoliko je poznat drugi korišteni bit, koji tako preuzima ulogu tajnog ključa.
Stoga, postoji potreba da se učestalo mijenjaju ključevi. To rezultira teškim tehnikama upravljanja ključem i distribucije. Obično se kriptografija s javnim ključem koristi za utvrđivanje ključeva, a tada se stvarni podatak brzo šifrira pomoću ili slijedne ili blok šifre. Gornji generator nizovnog ključa treba stvoriti nizovni ključ s nizom svojstava da bi slijedna šifra bila sigurna. Nizovni ključ bi trebao

- Imati dug period. Budući da je ključ k_i proizveden putem determinističkog procesa iz ranije dijela ključa, tu će postojati broj N takav da

$$k_i = k_{i+N}$$

za sve vrijednosti i. Ovaj broj N naziva se period niza, a treba bi biti velik da bi se nizovni ključ smatrao sigurnim.

- Imati pseudo-slučajna svojstva. Generator treba proizvesti slijed koji se čini slučajnim, drugim riječima trebao bi proći niz statističkih testova slučajnih brojeva.
- Imati veliku linearnu složenost.

Međutim, ovi uvjeti nisu dovoljni. Općenito, utvrđivanje više sekvencije od dijela trebalo bi biti u potpunosti neizvedivo. Idealno, čak i ako netko zna prvih milijardu bitova sekvencije nizovnog ključa, vjerojatnost točnog pogađanja sljedećeg bita ne bi smjela biti veća od jedne polovine.

4.3 Lorenzova šifra

Lorenzova šifra bila je njemačka šifra iz Drugog svjetskog rata koja je korištena za strateške informacije, za razliku od taktičkih podataka i podataka s bojišta koji su šifrirani pomoću stroja Enigma. Lorenzov stroj je slijedna šifra koja je radila na nizovima bitova. Međutim nije proizvodio samo jedan niz bitova, proizvodio je pet. Razlog je bio kodiranje poruka teleprintera korištenih u to vrijeme, točnije Baudotovog koda.

4.3.1 Baudotov kod

Kako bi shvatili Lorenzovu šifru prvo moramo shvatiti Baudotov kod. Svo smo upoznati s ASCII šifriranjem za standardna slova na tipkovnici, to koristi sedam bitova za podatke, plus jedan bit za detekciju grešaka. Prije ASCII, 1870., Baudot je izumio šifriranje koje je koristilo pet bitova podataka. Ono je dodatno razvijano sve dok 30-ih godina 20. stoljeća nije postalo standardni način komuniciranja preko teleprintera. Podaci su šifrirani preko vrpce, koja se sastojala od niza od pet redova rupa/praznina.
Ticker-vrpca je ostatak poruka koje su prenošene u Baudotovom kodu. Za one koji mogu sjetiti ranih dial-up modema, oni će se sjetiti da su brzine mjerene u Baudima ili znakova u sekundi, u spomen Baudotovog je izuma.
Pet bitova ne dopušta šifriranje svih znakova koje želimo, dakle Baudotova šifra koristi dva moguća "stanja" koja se nazivaju pomak slova i pomak brojki. Pomicanje između dviju stanja kontrolirano je kontrolnim znakovima, niz drugih kontrolnih znakova je rezerviran za stvari kao što su prazno mjesto (SP), povrat valjka (CR), dostava vrpce (LF) ili znaka koji bi zazvonio zvono teleprintera ($BELL$) (ta šifra još uvijek postoji u ASCII-u). Tablica za Baudotov kod u 1930. godini predstavljena je u Tablici 4.1.
Stoga kako bi odaslali poruku.
Please, Please Help! (Molim, molim pomoć) trebali bi odaslati šifru koju dajemo heksadecimalno,

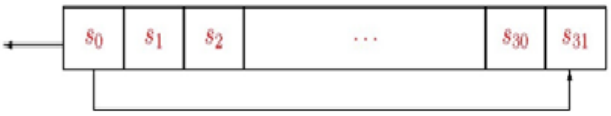
$$16, 12, 01, 03, 05, 01, 1B, 0C, 1F, 04, 16, 12, 01, 03, 05, 01, 04, 14, 01, 12, 16, 1B, 0D.$$

Bitovi u kodu	Pomak slova	Pomak brojki
0000	NULL	NULL
10000	E	3
01000	LF	LF
11000	A	−
00100	SP	SP
10100	S	′
01100	I	8
11100	U	7
00010	CR	CR
10010	D	ENQ
01010	R	4
11010	J	BELL
00110	N	,
10110	F	!
01110	C	:
11110	K	(
00001	T	5
10001	Z	+
01001	L	)
11001	W	2
00101	H	£
10101	Y	6
01101	P	0
11101	Q	1
00011	O	9
10011	B	?
01011	G	&
11011	Brojke	Brojke
00111	M	.
10111	X	/
01111	V	=
11111	Slova	Slova

Tablica 4.1: Baudotov kod

4.3.2 Lorenzova operacija

Lorenzova šifra je šifrirala podatke u obliku Baudotovog koda izradom niza od pet slučajnih bitova koji je bio isključivo ili (u nastavku ćemo koristiti XOR s oznakom $\oplus$), niz od pet slučajnih bitova dobivenih primjenom operacije XOR na bitove koji predstavljaju Baudotov kod. Stvarni Lorenzova šifra koristila je niza kotača, svaki kotač ima brojne igle. Prisutnost, ili odsutnost, igle signalizira postoji li signal jedan ili nula. Kako se kotač okreće, položaj igle mijenja se u odnosu na ulazni signal. U suvremenom govora svaki kotač odgovara pomačnom spremniku.
Na svaki otkucaj sata spremnik se pomiče ulijevo za jedan bit, alternativno se kotač okreće oko 1/32 okreta i najviša igla se uzima kao izlaz kotača.
To je prikazano na Slici 4.3.
Problem postoji s Lorenzovom šifrom, točnije, kako relativno jednostavan rad kotača/spremnika

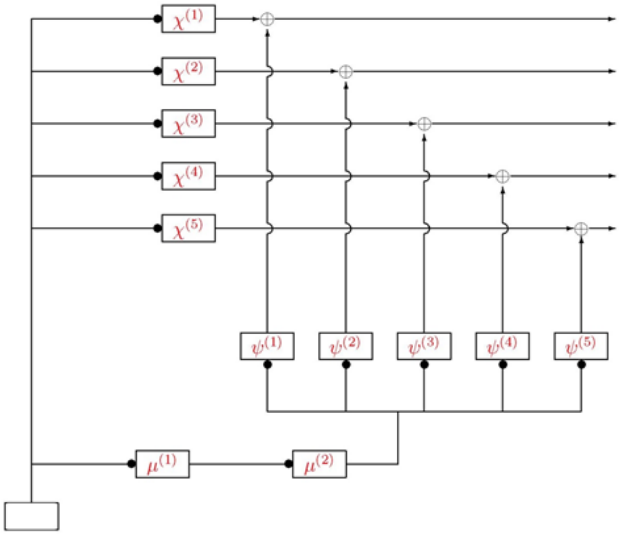


Slika 4.3: Spremnik pomaka od 32 bita

pomaka kombinirati da se dobije šifra koju je teško slomiti. Lorenzova šifra koristi dvanaest spremnika za kreiranje pet nizova nasumičnih bitova. Dvanaest spremnika je podijeljeno u tri podniza.
Kako Lorenzova šifra vremenski označava razne spremnike, zato koristimo varijablu t za označavanje globalnog sata, to će biti označeno za svaki znak Baudotovog koda koji je kodiran. Također koristimo varijablu t_ψ za označavanje koliko učestalo su ψ spremnici vremenski označeni, te kako varijabla t_μ koja označava koliko često je drugi spremnik μ vremenski označen. Za pokretanje šifre postavljamo $t = t_\psi = t_\mu = 0$, no tada te varijable napreduju u skladu sa sljedećim: U danom trenutku obavljamo sljedeće operacije:

1. Neka $\mathcal{K}$ označava vektor $\left(\chi_t^{(i)} \oplus \psi_{t_\psi}^{(i)}\right)_{i=1}^{5}$.
2. Ako je $\mu_{t+1}^{(1)} = 1$ postavljamo $t_\mu = t_\mu + 1$.
3. Ako je $\mu_{t_\psi}^{(2)} = 1$ postavljamo $t_\psi = t_\psi + 1$.
4. Izlaz $\mathcal{K}$.

Ovo je grafički opisano na Slici 4.4. Na ovoj slici označavamo vremenski signal kao liniju s kružnicom na kraju, izlazne žice su označene strelicom.



Slika 4.4: Grafički opis

Sami izlaz ψ i μ motora na svakom vremenskom koraku naziva se prošireni-ψ i prošireni-μ niz.

Nakon prvog koraka korištenja operacije XOR element po element dobivamo prvi vektor ključa

$$\mathcal{K}_0 = \chi_0 \oplus \psi_0 = \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \\ 1 \end{pmatrix} \oplus \begin{pmatrix} 1 \\ 1 \\ 1 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \\ 1 \end{pmatrix}.$$

U vrijeme $t = 1$ sada imamo drugi vektor ključa

$$\mathcal{K}_1 = \chi_1 \oplus \psi_0 = \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \\ 1 \end{pmatrix} \oplus \begin{pmatrix} 0 \\ 1 \\ 0 \\ 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}.$$

Ovaj pustupak se zatim ponavlja, tako da dobijemo sljedeći niz za prvih 60 izlaznih vrijednosti nizovnog ključa χ_t,

```
010010000101001011101100011011011101100011111110000000010001
000100011101110011111010111110011000011011000111111101110111
001010010110011011101110100001000100111100110010101101010000
101000101101110010011011001011000111010001111000111110101011
100011001000010001001000000101000000101000111000010011010011
```

Ovo se dobiva XOR operacijom izlaza spremnika χ koji je definiran sa:

```
111110001010110001111000101110100010001111111100010101100011
110000110101110110101101100100011000011010111010110110110010
100010011110011000111011101010001001111001100011101111010010
111100011010001000111010011111000110100010001110100111110001
110111100000010100011101101111000000101000111011011110000001
```

prema vrijednostima izlaza niza ψ_t' u vrijeme t,

```
10110000111111101001010011010111111111111000001101010110101
11010010100000010101011101101000000000000111110010101100010 1
10100000100000001101010101010000000000000000001101101011101 0
01010011011111101010000101010000000000000111111101101010011 0
01010010100000010101010110101000000000000000001100110101001 0
```

Kako bi olakšali razumijevanje također predstavljamo izlaz $\mu_t^{\prime(2)}$ koji je

```
11110111100000111111111111111100000000000100001011111111111 1
```

Prisjetite se, jedan u ovom nizu znači da su spremnici ψ vremenski označeni dok nula znači da nisu vremenski označeni.
Kako je rat napredovao Nijemci su počeli mijenjati sva unutarnja stanja spremnika svaki dan.
Zatim, uzimajući u obzir ove „dnevne“ vrijednosti za sadržaj spremnika, postavka po poruci daje se sa startnom pozicijom svakog spremnika. Stoga je ukupni broj ključeva poruke, obzirom na dnevni ključ, dan s 2^{64}. Slabost Lorenzove šifre je što se korišteni ključ lako može otkriti ukoliko se njime više puta šifrira ista duža poruka. Tako se i dogodilo u kolovozu 1941., kada je iz dva puta poslana poruka od gotovo 4000 znakova od strane Britanaca rekonstruiran način rada Lorenzove šifre.

4.3.3 Razbijanje kotača

Nakon utvrđivanja strukture Lorenzove šifre ostaje problem kako ju probiti. Metoda napada je podijeljena u dva stadija. U prvom stadiju je bilo potrebno probiti kotače, ovo je bio proces koji se trebao obaviti jednom za svaku konfiguraciju kotača. Tada je proizveden jednostavniji postupak koji je dao pozicije kotača za svaku poruku.
Sada objašnjavamo kako je obavljeno razbijanje kotača. Prva zadaća je s razumnom sigurnosti dobiti vrijednost niza za različite posebne vrijednosti i i j, obično $i = 1$ i $j = 2$. Postojali su različiti načini obavljanja ovoga, a poniže predstavljamo jako pojednostavljene tehnike koje su koristili kriptoanalitičari u Bletchleyu. Naš cilj je jednostavno pokazati razbijanje čak i 60 godina stare slijedne šifre zahtijeva određenu zamršenu manipulaciju procjenama vjerojatnosti, te da čak i mala odstupanja od nasumičnosti u izlaznom nizu mogu uzrokovati katastrofično zatajenje sigurnosti.
Zbog naravi njemačkih vojnih i Baudotovih metoda šifriranja, ovo je očigledno posebice bilo izraženo kad bi razmotrili prvi i drugi niz bitova, tj. $i = 1$ i $j = 2$.
U osnovi postoje dvije situacije za razbijanje kotača, prvi (složeniji) slučaj je kada ne znamo originalni otvoreni tekst poruke, tj. napadač ima isključivo pristup šifriranom tekstu. Drugi slučaj je kada napadač može pogoditi s razumnom sigurnosti vrijednost originalnog otvorenog teksta i tako može dobiti rezultirajući nizovni ključ.
Niz od 1271 bitova sada zapisujemo u polje od 41×31 bita, zapisivanjem prvih 31 bitova u prvi red, drugih 31 bitova u drugi red i tako dalje. Prazno mjesto se stavlja u matricu ako ne možemo utvrditi vrijednost s razumnom sigurnošću te bi mogli dobiti matricu koja izgleda poput sljedećeg;

```
10-1-010-0----01----1--10-0----
-1--0-011-1001-0----01101011--1
010-010-11-0--101--10--0--1--0-
-01---1-0---1-01000-1---0-001-0
--1-10--0--110-100001-0--10-110
----1--00001-00--00010010----10
011-0101-110-1-011-101101----01
01---1----100--01---01-01--0-01
-011--1-000-1--10-00-0---1001-0
1011-01--0---001---01-01--0----
---0--0-1-1--11----1----1-11---
----0---1--0---0-----11--0--00-
10--101--0----0-0-0--0--010----
-100---1-110-----11-01-0---1---
0100----1-1----01-1--1111--11--
0-0001-1-1-0011011-1---01011-0-
```

Sada je cilj napadača da napuni ovu matricu, proces poznat u Bletchleyu kao "rectangling", uzimajući u obzir da bi neke od unesenih nula i jedinica same mogle biti netočne. Razumna metoda je da se uzmu svi redovi koji počinju s nula i da se zatim izbroji broj nula i jedinica u drugoj komponenti tih redova. Ustanovit ćemo da postoji sedam jedinica i da nema nula, a ako isto učinimo za redove koji počinju s jedinicom ustanovit ćemo da postoje četiri nule i da nema jedinica. Stoga možemo zaključiti da bi dva tipa redova u tablici trebala početi s 10 i 01. Stoga zatim ispunjavamo drugu komponentu u bilo kojem redu koji ima postavljen prvi element. Nastavljamo na ovaj način, prvo gledajući redove i zatim stupce, sve dok cijela tablica ne bude ispunjena.
Gornja tablica je pronađena koristeći nekoliko tisuća znakova poznatog nizovnog ključa, što pomoću gore opisane metode omogućava jednostavnu rekonstrukciju cijele tablice. Prema dokumentima iz Bletcheya, kriptografi u Bletcheyu bi u biti koristili nekoliko stotina znakova nizovnog ključa u napadu s poznatim nizovnim ključem, a nekoliko tisuća u napadu s nepoznatim nizovnim ključem.
Jednom kad završimo možemo uzeti prvi redak i prvi stupac kao početne vrijednosti nizova. Zatim možemo ponoviti ovu analizu za različite spremnike dok ne utvrdimo moguće vrijednosti unutarnjeg stanja spremnika.
Međutim, kako je vrijeme prolazilo, dio koji je uključivao utvrđivanje gornjih nizova iz postupka „rectangling-a“ naposljetku je obavljalo računalo Colossus.
Računalo Colossus originalno je nije stvoreno za razbijanje kotača, tj. za utvrđivanje dugoročnog ključa Lorenzove šifre. Colossus je originalno napravljen za utvrđivanje postavki po poruci, te stoga da pomaže probiti pojedinačne šifrirane tekstove. Iako se prethodna metoda za razbijanje kotača mogla koristiti za napadanje šifriranog teksta, kako bi bila učinkovita potreban je veliki šifrirani tekst i mnogo sreće. Međutim, jednom kad su kotači razbijeni, tj. znamo bitove u različitim registrima, razbijanje sljedećeg šifriranog teksta postaje jednostavnije.
Ponovo koristimo trik de-χ-anja niza γ šifriranog teksta, a zatim primjenjujemo Δ metodu za rezultirajući niz β. Pretpostavljamo da znamo interna stanja svih spremnika, no ne i njihove početne pozicije. Neka s_i označava nepoznate vrijednosti pet početnih pozicija χ

kotača i s_φ (odnosno s_μ) globalno nepoznatu početnu poziciju niza φ (odnosno μ) kotača.

Definicija 4.1. *Za niz $a = (a_i)$ definiramo njegov delta niz Δa pomoću $\Delta a = (a_i \oplus a_{i+1})$.*

Tada vrijedi:

$$\beta_t = \gamma_t \oplus \chi_{t+s_\mu} = \varphi_t \oplus \psi'_{t+s_\varphi},$$

i zatim

$$(\Delta\beta)_t = (\Delta\varphi)_{t+s_\varphi} \oplus \left(\mu'^{(2)}_{t+s_\mu} \cdot (\Delta\psi)_{t_\psi}\right).$$

Zatim uzimamo rezultirajuće pet bitne nizove i xoramo ih zajedno kao i prije kako bi dobili

$$(\alpha^{(i,j)})_t = (\Delta\beta^{(i)})_t \oplus (\Delta\beta^{(j)})_t$$

$$= (\Delta\varphi^{(i)})_{t+s_\varphi} \oplus (\Delta\varphi^{(j)})_{t+s_\varphi} \oplus \mu'^{(2)}_{t+t_\mu} \left((\Delta\psi^{(i)})_{t_\psi} \oplus (\Delta\psi^{(j)})_{t_\psi}\right).$$

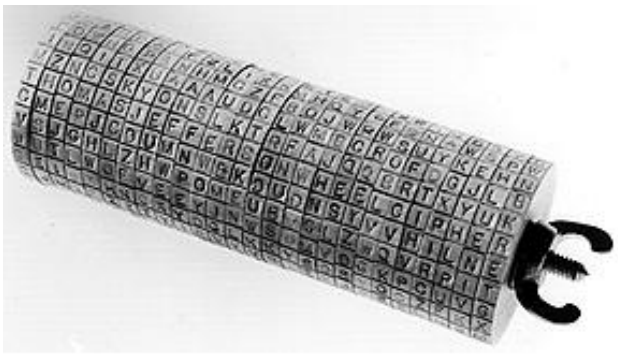
Usredotočimo se na $i = 1$ i $j = 2$. Pretpostavljajući da znamo vrijednosti za spremnike, sve što trebamo učiniti je utvrditi njihove startne pozicije s_1, s_2. Jednostavno trebamo proći svih $1271 = 41 \cdot 31$ mogućih startnih pozicija za prvi i drugi χ spremnik. Za svaku od ovih startnih pozicija računamo povezani niz $(\alpha^{(1,2)})_t$ i brojimo broj vrijednosti koje su nula. Točna vrijednost za startne pozicije odgovarat će posebno visokoj vrijednosti za broj nula. Ovo je jednostavan statistički test koji nam omogućava da utvrdimo startne pozicije prvog i drugog χ spremnika. Ponavljanje ovoga za ostale dijelove spremnika, ili korištenjem sličnih statističkih tehnika, možemo dobiti startnu poziciju svih χ registara. Ove statističke tehnike su ono za što je računalo Colossus dizajnirano.
Jednom kad bi se pozicije spremnika χ utvrdile, startne pozicije ψ i μ utvrđivale bi se manualno. Tehnike za ovu su veoma slične ranijim tehnikama koje su potrebne za razbijanje kotača, međutim, još jednom se pojavljuju različita pojednostavljenja pošto se pretpostavlja da znamo stanje svakog registra, no ne i njegovu startnu poziciju.
Računalo Colossus originalno nije stvoreno za razbijanje kotača, tj. za utvrđivanje dugoročnog ključa Lorenzove šifre. Colossus je originalno napravljen za utvrđivanje postavki po poruci, te stoga da pomaže probiti pojedinačne šifrirane tekstove. Iako se prethodna metoda za razbijanje kotača mogla koristiti za napadanje šifriranog teksta, kako bi bila učinkovita potreban je veliki šifrirani tekst i mnogo sreće. Međutim, jednom kad su kotači razbijeni, tj. znamo bitove u različitim registrima, razbijanje sljedećeg šifriranog teksta postaje jednostavnije. To su bila djelomično programabilna digitalna elektronička računala, a osnovna im je građevna jedinica bila elektronska cijev. Unos podataka je bio preko bušene papirne vrpce. Glavni je arhitekt Colossusa bio Tommy Flowers koji je radio u britanskoj pošti pri službi razvoja. Postojanje ovih računala je bilo tajno sve do 70-ih godina 20. stoljeća.

5 Naprave za šifriranje

Kriptosustavi koje smo do sada promatrali mogu se načiniti kompliciranijima, a time i sigurnijima, uporabom naprava za šifriranje. Takve naprave čine procese šifriranja i dešifriranja puno bržim, a također omogućavaju uporabu velikih prostora ključeva.

5.1 Jeffersonov kotač za šifriranje.

Najstariju takvu praktičnu napravu, Jeffersonov kotač za šifriranje, izumio je američki državnik Thomas Jefferson krajem 18. stoljeća. Naprava je bila toliko ispred svog vremena, da ju je američka vojska počela koristiti tek 1922. godine.
Jeffersonov kotač se sastoji od drvenog cilindra s rupom u sredini kroz koju je provučena željezna os. Cilindar je presječen na 26 manjih cilindara (diskova) jednakih širina. Ovi diskovi se mogu neovisno jedan od drugoga okretati oko zajedničke osi. Na vanjštini svakog diska nalazi se 26 jednakih kvadratića. Tih 26 kvadratića se na proizvoljan način popunjava s 26 slova engleskog alfabeta, koji se razlikuju od diska do diska.



Slika 5.1: Jeffersonov kotač

Pošiljalac i primalac imaju dva identična kotača. Da bi šifrirao otvoreni tekst, pošiljalac podijeli tekst na blokove od po 26 slova. Blok se šifrira tako da se rotiranjem diskova u jednom od 26 redaka dobije otvoreni tekst. Tada za šifrat možemo izabrati bilo koji od preostalih 25 redaka. Npr. koristeći kotač sa slike, otvoreni tekst

$$THOMASJEFFERSONWHEELCHIPER$$

bi se mogao šifrirati kao

$$VSJGHLZHWPOMEUBVSLZWQVRPIT.$$

Primalac dešifrira šifrat tako da rotiranjem diskova u jednom retku dobije šifrat. Sada među preostalih 25 redaka potraži onaj koji sadrži neki smisleni tekst i taj redak predstavlja otvoreni tekst.
Osnovna ideja Jeffersonovog kotača jest kreiranje polialfabetskog kriptosustava korištenjem diskova koji se rotiraju više ili manje neovisno.

5.2 Električni stroj za kodiranje.

Izumio ga je Amerikanac Edward Hugh Hebern izumio je 1915. godine.

Slika 5.2: Električni stroj za kodiranje

To je bio električni uređaj kojim su se dva električna pisača stoja spajala pomoću 26 žica, ali s razbacanim rasporedom, pa kad bi se udarila tipka na pisaćem stroju za otvoreni tekst, drugi bi stroj automatski otipkao šifarski ekvivalent tog slova. Dvije godine kasnije, u uređaj je ugradio 5 tzv. "rotora". Rotori su na svakoj strani imali po 26 električnih kontakata. Svaki kontakt na jednoj strani nasumce je spojen žicom s nekim kontaktom na drugoj strani. To zapravo predstavlja jednu monoalfabetsku supstituciju. No, rotiranjem rotora i to tako da najprije prvi napravi cijeli krug, pa se zatim drugi pomakne za jedno mjesto, itd., dobivamo polialfabetsku supstituciju s periodom $26^5 \approx 10^7$.

5.3 Enigma

Njemački pronalazač Artur Scherbius je 1918. godine izumio rotorsku napravu koju je nazvao Enigma. Razlikovala se od drugih rotorskih naprava po tome što su pomacima rotora upravljali zupčanici, pa se moglo postići da ti pomaci imaju nepravilan slijed.

Do masovne uporabe Enigme došlo je neposredno prije i za vrijeme Drugog svjetskog rata. Razbijanje njezine šifre (kombinacijom kriptoanalize i klasične špijunaže) imalo je važnu ulogu za tijek i ishod drugog svjetskog rata. Postojale su različite (vojne i komercijalne) inačice Enigme. Posebno je bila poznata japanska inačica Enigme, koju su Amerikanci nazivali Purple. Enigma je bila elektromehanička naprava koja se sastojala od tipkovnice s 26 tipki poput pisaćeg stroja, zaslona s 26 žaruljica za prikaz šifriranog izlaza, tri mehanička rotora (šifrarnika) i električne prespojne ploče. Pritiskom na tipku kroz mrežu kontakata rotora i prespojne ploče zatvorio bi se strujni krug i upalila bi se odgovarajuća žaruljica koja označava šifrirano slovo. Mehanički rotori sastojali su se od diskova s 26 kontakata. Svaki kontakt na jednoj strani diska bio je povezan s nekim drugim kontaktom na suprotnoj strani. Većina modela Enigme sastojala se od tri rotora koji su smješteni u ležište tako da se kontakti susjednih stranica međusobno dodiruju, tj. "izlaz" jednog rotora predstavljao je "ulaz" drugog. Izlaz trećeg (zadnjeg) rotora bio je povezan na reflektor - statičan mehanički

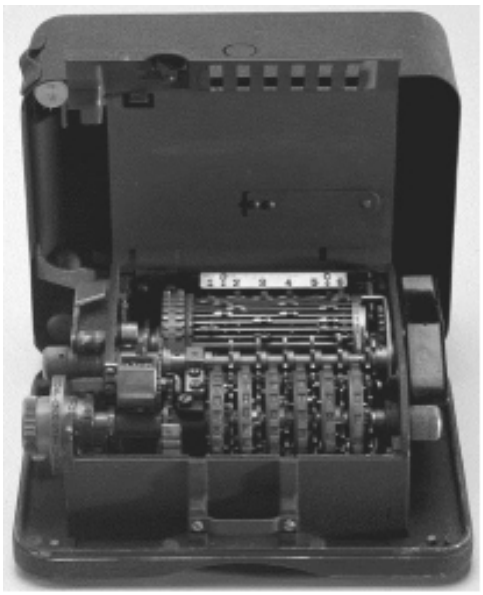
Slika 5.3: Enigma

disk sličan rotoru, s međusobno prespojenim električnim kontaktima samo na jednoj strani. Njegova je zadaća bila da električni signal šalje natrag kroz rotore, no drugim putem.
Tri ožičena rotora s 26 kontakata daju $26^3 = 17576$ mogućih kombinacija. To nije dovoljno velik broj da bi dao zadovoljavajuću sigurnost. Scherbius je povećao sigurnost Enigme povećavajući broj mogućih početnih postavki na dva različita načina: izmjenjivim rotorima i prespojnom pločom. Budući da su rotori mehanički gotovo identični, a njihovi električni spojni putevi različiti, njihovom međusobnom zamjenom mijenja se i način šifriranja samog stroja. Broj mogućih permutacija triju rotora je 6. Znatno veći doprinos sigurnosti donosi razvodna ploča, koja korisniku omogućuje da doda kablove, koji imaju efekt zamjene nekih slova prije ulaska u prvi rotor.
Dvije grupe matematičara-kriptoanalitičara uspjele su pronaći način za dekriptiranje Enigme. Bile su to poljska grupa, koju je predvodio Marian Rejewski, te britanska grupa, koju je predvodio Alan Turing.
Prvi napredak u kriptoanalizi Enigme ostvaren je 1931. godine akcijom francuske obavještajne službe, koja je stupila u vezu s bratom načelnika sektora veze njemačke vojske, Hansom-Thilom Schmidtom, koji je uz naknadu od 10 000 tadašnjih njemačkih maraka Francuzima dostavio upute za uporabu Enigme. Budući da su Francuzi i Poljaci po završetku Prvog svjetskog rata potpisali ugovor o vojnoj suradnji, ti su dokumenti dostavljeni poljskom uredu za kriptografiju Biuro Szyfrów. Dokumenti su opisivali i proceduru mjesečne distribucije knjiga s ključevima koje sadrže postavke uređaja potrebne za šifriranje ili dešifriranje poruke. Svaki mjesec, operateri Enigme bi dobili novu knjigu s ključevima koja je specificirala koji ključ se rabi koji dan. Svaki dan vrijedila je druga šifra, no, budući da su se dnevno šifrirale ogromne količine poruka, bilo je potrebno nekako postići da se sve te poruke ne šifriraju doslovno istim ključem, jer bi to znatno smanjilo sigurnost. Stoga su Nijemci uveli distribuciju "ključa za poruku" pomoću dnevnog ključa. Ključ za poruku je imao iste postavke na prespojnoj ploči i isti raspored rotora kao dnevni ključ, ali različitu orijentaciju rotora. Budući da ta orijentacija rotora nije bila u knjizi s ključevima, trebalo ju je sigurno poslati zajedno s porukom. To se radilo na sljedeći način. Pošiljalac bi postavljao svoj stroj

prema dogovorenom dnevnom ključu, koji ima orijentaciju šifrarnika npr. CXL. Zatim bi nasumično odabirao novu orijentaciju rotora za ključ za poruke, npr. YAQ i šifrirao YAQ pomoću dnevnog ključa (i to dvaput, da bi primatelj bio siguran da je primio dobar ključ za poruke). Na primjer, pošiljalac je mogao YAQYAQ šifrirati kao MIVWJE. Primijetimo da su dva niza slova YAQ šifrirana različito (prvi kao MIV, a drugi kao WJE) jer se rotori Enigme rotiraju nakon šifriranja svakog slova. Pošiljalac tada mijenja orijentaciju rotora u YAQ i šifrira ostatak poruke prema ovom ključu za poruke. Kod primatelja je stroj na početku bio postavljen prema dnevnoj orijentaciji CXL. Nakon što se unese prvih 6 slova dobivenog šifrata, MIVWJE, dobiva se YAQYAQ. Primatelj sada zna da treba podesiti orijentaciju šifrarnika na YAQ, koji je ključ za poruke, i onda dešifrirati preostali šifrat da bi dobio originalnu poruku.
Poljski su kriptoanalitičari predvođeni Rejewskim iskoristili ovo ponavljanje za kriptoanalitički napad. Znajući da prvo i četvrto slovo u šifratu odgovaraju istom slovu ključa za poruke, oni su istraživali veze među tim slovima unutar svih poruka dobivenih pomoću istog dnevnog ključa. Imajući na raspolaganju velik broj poruka, mogli su za svako slovo alfabeta naći s njim na ovaj način povezano slovo. Tako bi dobili jednu permutaciju alfabeta $A, B, \ldots, Z$. Važno svojstvo permutacija je da se one mogu rastaviti na produkt ciklusa. Rejewski je uočio da broj elemenata u ciklusima ovisi isključivo o rotorima, a ne o prespojnoj ploči. Ukupan broj postavki rotora je 105456, što je velik broj, ali ne i ogroman. Zahvaljući Schmidtovoj špijunaži, Poljaci su bili u stanju napraviti repliku Enigmenakon čegaa je dešifrirati dosta lako. Trebalo je još odrediti veze na prespojnoj ploči. Ako se krene u dešifriranje s prespojnom pločom bez ikakvih veza, dobit će se uglavnom nerazumljiv tekst. No, vjerojatno će se naići i na djelove teksta koji su "skoro čitljivi". I tako se otkrivaju slova koja su povezana kablovima na prespojnoj ploči. Na ovaj su način Poljaci nekoliko godina uspijevali redovito dešifrirati njemačke poruke, sve dok 1939. godine Nijemci nisu značajno povećali broj mogućih ključeva, uvođenjem većeg broja rotora.
Neposredno prije početka Drugog svjetskog rata, sva je dokumetacija rada Rejewskog poslana Britancima. Oni su u to vrijeme bili oformili veliku grupu kriptoanalitičara različitih profila u Bletchley Parku. Kako je ova grupa bila veća, a imala je i znatno veći proračun od poljskog Biuroa Szyfrów, uspjeli su konstruirati vrlo snažne strojeve (tzv. bombe) pomoću kojih su pokušavali dekriptirati poruke šifrirane Enigmom. Nakon što su svladali tehniku koju su koristili Poljaci, grupa iz Bletchley Parka, predvođena Alanom Turingom, izmislila je još neke nove tehnike. Jedna od slabosti, ne same Enigme, već njezina korištenja u praksi, bilo je korištenje "predvidljiivih ključeva". Tako su operateri često za ključ za poruku koristili tri susjedna slova na tipkovnici. Pored toga, Turing je pronašao efikasan način za dešifriranje Enigme korištenjem metode vjerojatne riječi. Sve aktivnosti unutar Bletchley Parka su bile prekrivene velom tajnosti punih 30 godina. Tek je 1974. godine britanska vlada dozvolila objavljivanje prvih informacija vezanih uz britansko razbijanje Enigme.

5.4 Stroj $C - 36$

Švođanin ruskog podrijekla Boris Hagelin tvorac je niza naprava za šifriranje koje su u širokoj uporabi bile sredinom 20. stoljeća. On je prvi čovjek koji se obogatio zahvaljujući kriptologiji. Vjerojatno najpoznatiji njegov izum je stroj $C - 36$ iz 1936. godine, koji je u američkoj vojsci imao naziv M-209.



Slika 5.4: Stroj $C-36$

Osnovne komponente ovog stroja bile su 6 rotora s po 17, 19, 21, 23, 25 i 26 slova, te "kavez" koji je imao 27 šipki montiranih u obliku vodoravnog cilindra koji se okreće.

6 Literatura

[1] A. Dujella, M. Maretić: Kriptografija, Udžbenik Sveučilišta u Zagrebu, Element, Zagreb, 2007

[2] N. Smart, Cryptography: An Introduction (3rd Edition), McGraw-Hill, Maidenhead, 2003

7 Sažetak

Kriptografija je znanost koja osigurava sigurnu komunikaciju između pošiljatelja i primatelja poruke. Ljudi su kroz povijest pokušali osmisliti neslomljivu šifru. Najstarija šifra jest Cezarova, dok je prva ideja šifiranja bila vezana za supstituciju. Za sigurnu komunikaciju pošiljatelja i primatelja potrebno je osmisliti dobar ključ i način šifriranja poruke. Također su se kroz povijest su se stvarale mnoge naprave koje bi osigurale sigurnu komunikaciju. Postoje monoalfabetske i polialfabetske šifre. U današnje vrijeme u kojemu sve je teže osigurati zašititu podataka, ali kriptografija je dosta napredovala kao i kriptoanalitičari.

Ključne riječi: komunikacija, otvoreni tekst, šifrat, kriptografja, šifriranje, kriptosustav, kriptoanaliza, primatelj, pošiljatelj, frekvencija

8 Životopis

Rođena sam 18. prosinca 1991. godine u Siklosu. Svoje osnovno školsko obrazovanje započinjem 1998. godine u Osnovnoj školi Ivana Filipovića u Osijeku. Nakon završetka, 2006. godine upisujem opću gimnaziju u Osijeku. Budući da sam već u osnovnoj školi razvila zanimanje za matematiku, upisujem 2010. godine Sveučilišni nastavnički studij matematike i informatike na Odjelu za matematiku u Osijeku.