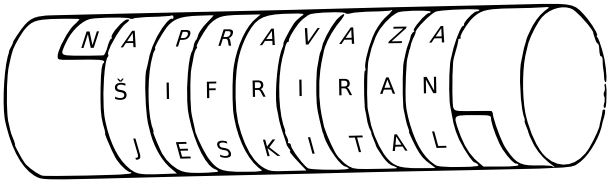
1. Klasična kriptografija

1.1 Osnovni pojmovi

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".

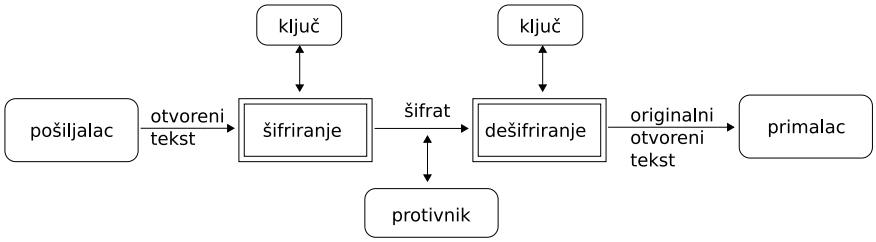
Neki elementi kriptografije bili su prisutni već kod starih Grka. Naime, Spartanci su u 5. stoljeću prije Krista upotrebljavali napravu za šifriranje zvanu *skital*. To je bio drveni štap oko kojeg se namotavala vrpca od pergamenta, pa se na nju okomito pisala poruka. Nakon upisivanja poruke, vrpca bi se odmotala, a na njoj bi ostali izmiješani znakovi koje je mogao pročitati samo onaj tko je imao štap jednake debljine.



Slika 1.1: *Skital*

Osnovni zadatak kriptografije je omogućiti dvjema osobama (zvat ćemo ih *pošiljalac* i *primalac* - u kriptografskoj literaturi za njih su rezervirana imena Alice i Bob) komuniciranje preko nesigurnog komunikacijskog kanala (telefonska linija, računalna mreža, ...) na način da treća osoba (njihov protivnik - u literaturi se najčešće zove Eva ili Oskar), koja može nadzirati komunikacijski kanal, ne može razumjeti njihove poruke. Poruku koju pošiljalac želi poslati primaocu zvat ćemo *otvoreni tekst* (engl. plaintext). To može biti tekst na njihovom materinjem jeziku, numerički podatci ili bilo što drugo. Pošiljalac transformira otvoreni tekst koristeći unaprijed dogovoreni *ključ* (engl. key). Taj postupak se naziva *šifriranje*, a dobiveni rezultat *šifrat* (engl. ciphertext) ili *kriptogram*. Nakon toga pošiljalac pošalje šifrat preko nekog komunikacijskog kanala. Protivnik prisluškujući može doznati sadržaj šifrata, ali ne može odrediti otvoreni tekst. Za razliku od njega, primalac

koji zna ključ kojim je šifrirana poruka može *dešifrirati* šifrat i odrediti otvoreni tekst.



Slika 1.2: *Shema klasične kriptografije*

Za razliku od dešifriranja, *kriptoanaliza* ili *dekriptiranje* je znanstvena disciplina koja se bavi proučavanjem postupaka za čitanje skrivenih poruka bez poznavanja ključa. *Kriptologija* je pak grana znanosti koja obuhvaća kriptografiju i kriptoanalizu.

Kriptografski algoritam ili *šifra* je matematička funkcija koja se koristi za šifriranje i dešifriranje. Općenito, radi se o dvije funkcije, jednoj za šifriranje, a drugoj za dešifriranje. Te funkcije preslikavaju osnovne elemente otvorenog teksta (najčešće su to slova, bitovi, grupe slova ili bitova) u osnovne elemente šifrata, i obratno. Funkcije se biraju iz određene familije funkcija u ovisnosti o ključu. Skup svih mogućih vrijednosti ključeva nazivamo *prostor ključeva*. *Kriptosustav* se sastoji od kriptografskog algoritma, te svih mogućih otvorenih tekstova, šifrata i ključeva. Dakle, imamo sljedeću formalnu definiciju.

Definicija 1.1. *Kriptosustav* je uređena petorka $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$, gdje je $\mathcal{P}$ konačan skup svih mogućih osnovnih elemenata otvorenog teksta, $\mathcal{C}$ konačan skup svih mogućih osnovnih elemenata šifrata, $\mathcal{K}$ konačan skup svih mogućih ključeva, $\mathcal{E}$ skup svih funkcija šifriranja i $\mathcal{D}$ skup svih funkcija dešifriranja. Za svaki $K \in \mathcal{K}$ postoji funkcija šifriranja $e_K \in \mathcal{E}$ i odgovarajuća funkcija dešifriranja $d_K \in \mathcal{D}$. Pritom su $e_K : \mathcal{P} \to \mathcal{C}$ i $d_K : \mathcal{C} \to \mathcal{P}$ funkcije sa svojstvom da je $d_K(e_K(x)) = x$ za svaki $x \in \mathcal{P}$.

Najvažnije svojstvo u definiciji je $d_K(e_K(x)) = x$. Iz njega slijedi da funkcije e_K moraju biti injekcije. Zaista, ako bi bilo

$$e_K(x_1) = e_K(x_2) = y,$$

za dva različita otvorena teksta x_1 i x_2, onda primalac ne bi mogao odrediti treba li y dešifrirati u x_1 ili x_2, tj. $d_K(y)$ ne bi bilo definirano. U skladu s tim, ako je $\mathcal{P} = \mathcal{C}$, onda su funkcije e_K permutacije.

Kriptosustave obično klasificiramo s obzirom na sljedeća tri kriterija:

1. **Tip operacija koje se koriste pri šifriranju**

   Imamo podjelu na *supstitucijske šifre* u kojima se svaki element otvorenog teksta (bit, slovo, grupa bitova ili slova) zamjenjuje s nekim drugim elementom, te *transpozicijske šifre* u kojima se elementi otvorenog teksta permutiraju (premještaju). Npr. ako riječ TAJNA šifriramo u XIWOI, načinili smo supstituciju, a ako je šifriramo u JANAT, načinili smo transpoziciju. Primjer transpozicijske šifre je već spomenuti skital. Postoje također i kriptosustavi koji kombiniraju ove dvije metode.

2. **Način na koji se obrađuje otvoreni tekst**

   Ovdje razlikujemo *blokovne šifre*, kod kojih se obrađuje jedan po jedan blok elemenata otvorenog teksta koristeći jedan te isti ključ K, te *protočne šifre* (engl. stream cipher) kod kojih se elementi otvorenog teksta obrađuju jedan po jedan koristeći pritom paralelno generirani niz ključeva (engl. keystream).

3. **Tajnost i javnost ključeva**

   Ovdje je osnovna podjela na *simetrične kriptosustave* i *kriptosustave s javnim ključem*. Kod simetričnih ili konvencionalnih kriptosustava, ključ za dešifriranje se može izračunati poznavajući ključ za šifriranje i obratno. Ustvari su ovi ključevi najčešće identični. Sigurnost ovih kriptosustava leži u tajnosti ključa. Zato se oni zovu i *kriptosustavi s tajnim ključem*.

   Kod kriptosustava s javnim ključem ili asimetričnih kriptosustava ključ za dešifriranje se ne može (barem ne u nekom razumnom vremenu) izračunati iz ključa za šifriranje. Ovdje je ključ za šifriranje *javni ključ*. Naime, bilo tko može šifrirati poruku pomoću njega, ali samo osoba koja ima odgovarajući ključ za dešifriranje (*privatni* ili *tajni ključ*) može dešifrirati tu poruku. Ideju javnog ključa prvi su javno iznijeli Whitfield Diffie i Martin Hellman 1976. godine, kada su dali prijedlog rješenja problema razmjenjivanja ključeva za simetrične kriptosustave putem nesigurnih komunikacijskih kanala.

Sada ćemo dati nekoliko općih napomena o kriptoanalizi.

Osnovna pretpostavka kriptoanalize je da kriptoanalitičar zna koji se kriptosustav koristi. To se naziva *Kerckhoffsovo načelo*, po Nizozemcu Augustu Kerckhoffsu (1835-1903), autoru važne knjige “Vojna kriptografija”. Naravno, ova pretpostavka u konkretnom slučaju ne mora biti točna, ali mi ne želimo da nam

sigurnost kriptosustava leži na "klimavoj" pretpostavci da naš protivnik ne zna koji kriptosustav koristimo. Čak i ukoliko kriptoanalitičar treba provjeriti nekoliko mogućih kriptosustava, time se kompleksnost procedure bitno ne mijenja. Dakle, pretpostavljamo da tajnost šifre u potpunosti leži u ključu.

Razlikujemo četiri osnovna nivoa kriptoanalitičkih napada.

1. **Samo šifrat**

   Kriptoanalitičar posjeduje samo šifrat od nekoliko poruka šifriranih pomoću istog algoritma. Njegov je zadatak otkriti otvoreni tekst od što više poruka ili u najboljem slučaju otkriti ključ kojim su poruke šifrirane.

2. **Poznati otvoreni tekst**

   Kriptoanalitičar posjeduje šifrat neke poruke, ali i njemu odgovarajući otvoreni tekst. Njegov je zadatak otkriti ključ ili neki algoritam za dešifriranje poruka šifriranih tim ključem.

3. **Odabrani otvoreni tekst**

   Kriptoanalitičar ima mogućnost odabira teksta koji će biti šifriran, te može dobiti njegov šifrat. Ovaj napad je jači od prethodnoga, ali je manje realističan.

4. **Odabrani šifrat**

   Kriptoanalitičar je dobio pristup alatu za dešifriranje, pa može odabrati šifrat, te dobiti odgovarajući otvoreni tekst. Ovaj napad je tipičan kod kriptosustava s javnim ključem. Tu je zadatak kripoanalitičara otkriti ključ za dešifriranje (tajni ključ).

(5.) **Potkupljivanje, ucjena, krađa i slično**

   Ovaj napad ne spada doslovno u kriptoanalizu, ali je vrlo efikasan i često primjenjivan u kombinaciji s "pravim" kriptoanalitičkim napadima.

Naravno, možemo se pitati koliko je realno da će kriptoanalitičar biti u prilici primijeniti 2., 3. ili 4. vrstu napada. Na prvi pogled to izgleda dosta nerealno. Međutim, tu treba imati u vidu činjenicu da je kriptoanalitičar već nekako došao u posjed šifrata koji nije bio njemu namjenjen. Dakle, svakako on (ili njegova organizacija) posjeduje izvjesne sposobnosti koje mu mogu pomoći i oko drugih vrsta kriptoanalitičkih napada.

1.2 Supstitucijske šifre

Gaj Julije Cezar

Znameniti se rimski vojskovođa i državnik Gaj Julije Cezar u komunikaciji sa svojim prijateljima koristio 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, C $\mapsto$ F itd.). Pretpostavljamo da se alfabet ciklički nastavlja, tj. da nakon zadnjeg slova Z, ponovo dolaze A, B, C. Ako bismo 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

U daljnjim primjerima koristit ćemo se engleskim (međunarodnim) 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 (tj. kriptosustavi) istog oblika s pomakom različitim od 3. Da bismo Cezarovu šifru precizno definirali u smislu Definicije 1.1, uvest 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 njegovim ostatkom pri dijeljenju s 26. Koristit ćemo oznake $a +_{26} b$ ili $(a + b) \bmod 26$, te analogno za oduzimanje i množenje. Npr. $(10 + 20) \bmod 26 = 30 - 26 = 4$, $(10 - 20) \bmod 26 = -10 + 26 = 16$. Skup $\mathbb{Z}_{26}$, uz operacije $+_{26}$ i $\cdot_{26}$, zadovoljava aksiome matematičke strukture koja se naziva *prsten*. To znači da su operacije zbrajanja i množenja zatvorene (rezultat je ponovo iz $\mathbb{Z}_{26}$), komutatitivne ($a +_{26} b = b +_{26} a$, $a \cdot_{26} b = b \cdot_{26} a$) i asocijativne ($(a +_{26} b) +_{26} c = a +_{26} (b +_{26} c)$, $(a \cdot_{26} b) \cdot_{26} c = a \cdot_{26} (b \cdot_{26} c)$), vrijedi distributivnost množenja prema zbrajanju ($(a +_{26} b) \cdot_{26} c = (a \cdot_{26} c) +_{26} (b \cdot_{26} c)$).

Broj 0 je neutralni element za zbrajanje ($a +_{26} 0 = 0 +_{26} a = a$), te svaki element a ima suprotni element (aditivni inverz) $-a$ (za $a \neq 0$ to je broj $26 - a$, jer vrijedi $a +_{26} (26 - a) = (26 - a) +_{26} a = 26 \bmod 26 = 0$). Nadalje, broj 1 je neutralni element za množenje ($a \cdot_{26} 1 = 1 \cdot_{26} a = a$), no samo neki elementi a imaju multiplikativni inverz a^{-1}, tj. element za koji vrijedi $a \cdot_{26} a^{-1} = a^{-1} \cdot_{26} a = 1$. Uvedimo još jednu oznaku: ako dva cijela broja a i b daju isti ostatak pri dijeljenju s 26, to ćemo zapisivati s $a \equiv b \pmod{26}$ i govoriti da su a i b *kongruentni* modulo 26. Potpuno analogno se definira skup $\mathbb{Z}_m$ i operacije na njemu za proizvoljan prirodan broj m.

Primijetimo da na ovom mjestu zamjena slova brojevima još nije bila nužna (mogli bismo sve definirati u terminima slova i njihovog pomicanja unutar alfabeta, te pojasniti što se događa kad "preskočimo" zadnje slovo), no uskoro će korištenje ovog matematičkog rječnika postati nužno.

Dakle, *Cezarovu šifru* možemo definirati na sljedeći način:

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

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

Kao što smo već objasnili, šifra je definirana na $\mathbb{Z}_{26}$ 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
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

U Cezarovoj su šifri osnovni elementi (simboli) otvorenog teksta slova (odnosno njihovi numerički ekvivalenti), a ključ K određuje za koliko mjesta (udesno) ćemo pomicati slova pri šifriranju. Očito je $d_K(e_K(x)) = x$, kao što se zahtijeva u definiciji kriptosustava. 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 1.1. Dekriptirati šifrat PWNUYTLWFKNOF dobiven Cezarovom šifrom.

Rješenje. Budući da je prostor ključeva jako mali (ima ih 26) zadatak možemo riješiti "grubom silom", tj. tako da ispitamo sve moguće ključeve, sve dok ne dođemo do nekog smislenog teksta. Za $d_0, d_1, d_2, \ldots$ dobivamo redom:

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

Dakle, ključ je $K = 5$, a otvoreni tekst je KRIPTOGRAFIJA. ♢

Da bismo dobili barem malo sigurniju šifru, možemo promatrati funkcije za šifriranje koje će uključivati više od 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:

Neka je $\mathcal{P} = \mathcal{C} = \mathbb{Z}_{26}$, te neka je

$$\mathcal{K} = \{(a, b) \in \mathbb{Z}_{26} \times \mathbb{Z}_{26} \,:\, (a, 26) = 1\}.$$

Za $K = (a, b) \in \mathcal{K}$ definiramo

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

Ova šifra se naziva afinom zato što su funkcije šifriranja i dešifriranja afine. Provjerimo je li uvjet $d_K(e_K(x)) = x$ zadovoljen. Zaista,

$$d_K(e_K(x)) = d_K(ax + b) = a^{-1}(ax + b - b) = x.$$

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 djelitelj od a i 26 jednak 1 (to pišemo: $(a, 26) = 1$). Prikažimo te brojeve zajedno s njihovim inverzima:

a	1	3	5	7	9	11	15	17	19	21	23	25
a^{-1}	1	9	21	15	3	19	7	23	11	5	17	25

Primjer 1.2. Neka je $K = (7, 3)$. Šifrirati otvoreni tekst ZADAR.

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

$$\begin{aligned} 25 \cdot 7 + 3 &\equiv 22 \pmod{26}, \\ 0 \cdot 7 + 3 &\equiv 3 \pmod{26}, \\ 3 \cdot 7 + 3 &\equiv 24 \pmod{26}, \\ 17 \cdot 7 + 3 &\equiv 18 \pmod{26}. \end{aligned}$$

pa je šifrat WDYDS. ♢

Primjer 1.3. Dekriptirati šifrat

OZWHRYEZCVWFCTPCUWRCFPYHWI

dobiven afinom šifrom.

Rješenje. Imamo $12 \cdot 26 = 312$ mogućih ključeva. To je još uvijek premalo, pa bismo uz pomoć računala sigurno mogli primijeniti "grubu silu", kao u Primjeru 1.1.

No, postoji i elegantniji način ukoliko znamo kojim je jezikom pisan otvoreni tekst. Recimo da nam je poznato da je u ovom slučaju otvoreni tekst pisan hrvatskim jezikom. Frekvencijom slova u hrvatskom, a i nekim drugim jezicima, detaljnije ćemo se pozabaviti malo kasnije. Zasad nam je potrebna samo činjenica da su najfrekventnija slova u hrvatskom jeziku A, I, O, E, N, i to upravo tim redoslijedu. U našem šifratu uočavamo da su najfrekventnija slova C i W, koja se javljaju po 4 puta. Iako je naš šifrat prekratak, možemo ipak očekivati da su ova dva slova šifrati od A, I, O, E ili N. Pa pogledajmo kakve smo sreće.

Imamo $e_K(\mathrm{A}) = a \cdot 0 + b = b$, $e_K(\mathrm{I}) = 8a + b$. Pretpostavimo da je $e_K(\mathrm{A}) = \mathsf{C}$ i $e_K(\mathrm{I}) = \mathsf{W}$. Dobivamo da je $b = 2$ i $8a + b \equiv 22 \pmod{26}$, odakle je $a = 9$. (Općenito se linearne kongruencije rješavaju pomoću (proširenog) Euklidova algoritma o kojem će biti više riječi kasnije, no u slučaju malog modula, kao što je naš modul 26, dovoljno je uvrstiti sve dopustive (invertibilne) a-ove, te provjeriti koji zadovoljava kongruenciju.) Dakle, dobili smo da je $e_K(x) = 9x + 2 \bmod 26$. Tada je $d_K(y) = 3(y - 2) \bmod 26$. Primijenimo li funkciju d_K na naš šifrat, dobivamo otvoreni tekst (s umetnutim razmacima i dijakritičkim znakovima):

KRIPTOGRAFIJA ZNAČI TAJNOPIS. ♢

Cezarova i afina šifra su specijalni slučajevi *supstitucijske šifre*, koja je definirana na sljedeći način:

Neka je $\mathcal{P} = \mathcal{C} = \mathbb{Z}_{26}$. Prostor ključeva $\mathcal{K}$ se sastoji od svih permutacija skupa $\{0, 1, 2, ..., 25\}$. Za svaku permutaciju $\pi \in \mathcal{K}$ definiramo

$$e_\pi(x) = \pi(x), \quad d_\pi(y) = \pi^{-1}(y),$$

gdje je π^{-1} inverzna permutacija od π.

Dakle, umjesto tablice *otvoreni tekst - šifrat* koja odgovara Cezarovoj šifri i kod koje smo za alfabet šifrata (drugi redak u pripadnoj tablici) imali D, E, F, . . . , Z, A, B, C; možemo za alfabet šifrata izabrati bilo koju permutaciju slova A, B, . . . , Z; te svako slovo otvorenog teksta zamijeniti (supstituirati) sa slovom koje se u tablici nalazi ispod njega.

Ovdje imamo čak $26! = 1 \cdot 2 \cdot 3 \cdots 26 \approx 4 \cdot 10^{26}$ mogućih ključeva, tako da je napad ispitivanjem svih mogućih ključeva praktički nemoguć, čak i uz pomoć računala. Međutim, supstitucijsku šifru je moguće dosta lako dekriptirati koristeći statistička svojstva jezika na kojem je pisan otvoreni tekst. Osnovna metoda je *analiza frekvencija 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* (parovima slova) i *trigramima* (nizovima od tri slova) 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 tekstu (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 5 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. Ovakvu situaciju u kojoj praktički istovremeno do otkrića značajnih za kriptografiju dođu znanstvenici koji žele što prije objaviti svoje rezultate i dobiti za njih priznanje, te ljudi iz obavještajnih ili komercijalnih institucija koje ne žele ili ne smiju odmah objaviti svoje rezultate, susrećemo često u povijesti kriptografije sve do današnjih dana (npr. pitanje prvenstva kod otkrića diferencijalne kriptoanalize ili kriptosustava s javnim ključem).

Navest ćemo osnovne podatke o frekvenciji slova, bigrama i trigrama za hrvatski, engleski i njemački jezik. Pritom smatramo da u tekstu nema interpunkcijskih znakova ni razmaka između riječi (u protivnom bi kriptoanaliza bila puno lakša), te da su slova Č, Ć, Đ, Dž, Lj, Nj, Š, Ž iz hrvatske abecede zamijenjena na prije opisani način slovima iz međunarodnog alfabeta.

Podatci za hrvatski jezik su dobiveni analizom tekstova iz dnevnog tiska dostupnog na internetu, dok su podatci za engleski i njemački jezik preuzeti iz literature [5, 114].

Frekvencija slova u hrvatskom jeziku (u promilima)

A	I	O	E	N	S	R	J	T	U	D	K	V	L	M	P	C	Z	G	B	H	F
115	98	90	84	66	56	54	51	48	43	37	36	35	33	31	29	28	23	16	15	8	3

Frekvencija slova u engleskom jeziku (u promilima)

E	T	A	O	I	N	S	H	R	D	L	C	U	M	W	F	G	Y	P	B	V	K	J	Q	X	Z
127	91	82	75	70	67	63	61	60	43	40	28	28	24	23	22	20	20	19	15	10	8	2	1	1	1

Frekvencija slova u njemačkom jeziku (u promilima)

E	N	I	R	S	A	T	D	H	U	L	G	O	C	M	B	F	W	K	Z	P	V	J	Y	X	Q
175	98	77	75	68	65	61	48	42	42	35	31	30	27	26	19	17	15	15	11	10	9	3	1	0	0

Najfrekventniji bigrami u hrvatskom jeziku su:

JE (2.7%), NA (1.5%), RA, ST, AN, NI, KO, OS, TI, IJ, NO, EN, PR (1.0%).

Ovdje je važno uočiti da je JE najfrekventniji bigram, iako J nije među najfrekventnijim slovima. Više od pola pojavljivanja slova J otpada na bigram JE. Druga zanimljivost je da su svi najfrekventniji bigrami oblika suglasnik-samoglasnik ili samoglasnik-suglasnik, osim bigrama ST i PR. Konačno, najfrekventniji *recipročni bigrami* su NA i AN (1.5% i 1.4%), te NI i IN (1.3% i 0.9%). Jedino kod ovih dvaju parova su frekvencije obaju bigrama barem 0.9%.

Daleko najfrekventniji trigram u hrvatskom jeziku je IJE (0.6%). Slijede (s frekvencijama između 0.3% i 0.4%): STA, OST, JED, KOJ, OJE, JEN.

U engleskom jeziku najfrekventniji bigrami su

TH (3.2%), HE (2.5%), AN, IN, ER, RE, ON, ES, TI, AT (1.2%),

a trigrami THE (3.5%), ING (1.1%), AND (1.0%), ION, TIO, ENT, ERE, HER (0.7%).

U njemačkom jeziku najfrekventniji bigrami su

ER (4.1%), EN (4.0%), CH (2.4%), DE, EI, ND, TE, IN, IE, GE (1.5%),

a trigrami EIN (1.2%), ICH (1.1%), NDE (0.9%), DIE, UND, DER, CHE, END (0.8%).

Primjer 1.4. Dekriptirati šifrat

```
TQCWT QCKIQ RWNOQ OBCEW OQVKB UKAPK OQOQB CQPQA
JGDUQ EQORW TSJGR WEQKY WGTWC JKRBI KZGVO GBQ
```

dobiven supstitucijskom šifrom ako je poznato da je otvoreni tekst na hrvatskom jeziku.

(Zbog preglednosti se kod duljih šifrata obično stavlja razmak nakon svakog petog slova - to naravno nema nikakve veze s razmacima u otvorenom tekstu, za koje smo se dogovorili da ćemo ih zanemarivati kod šifriranja.)

Rješenje. Napravit ćemo (istovremeno) analizu frekvencija slova i bigrama tako da za svako slovo u alfabetu napišemo sve njegove sljedbenike u šifratu (za zadnje slovo u šifratu stavimo *). Dobivamo sljedeću tablicu:

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

Iz tablice iščitavamo da su najfrekventnija slova:

Q (13), K (7), O (7), W (7), B, C, G, R, T, E, J,

a najfrekventniji bigrami:

OQ (4), QO (3), RW (3), BC, EQ, JG, QC, TQ, WT.

Logično je pretpostaviti da je $e(\mathrm{A}) = \mathrm{Q}$. Uočavamo također recipročne bigrame OQ i QO, što nas navodi na $e(\mathrm{N}) = \mathrm{O}$. Nadalje, većina pojavljivanja slova R vezana je uz bigram RW, dok je W jedno od najfrekventnijih slova. To nas vodi na pretpostavku da je $e(\mathrm{J}) = \mathrm{R}$ i $e(\mathrm{E}) = \mathrm{W}$. Pokušajmo otkriti šifrat čestog bigrama ST (najčešćeg od neotkrivenih). Najozbiljniji kandidati su BC i JG. Možemo uzeti neki od njih, pa vidjeti što ćemo dobiti. Mi ćemo krenuti s BC, jer frekvencije od B i C dobro odgovaraju očekivanim frekvencijama od S i T. Dakle, uzmimo da je $e(\mathrm{S}) = \mathrm{B}$ i $e(\mathrm{T}) = \mathrm{C}$. Od najfrekventnijih slova u hrvatskom jeziku, još nismo odgonetnuli šifrate od I i O. Glavni kandidati su K i G, i to upravo tim

redoslijedom. Pa uzmimo da je $e(\mathrm{I}) = \mathsf{K}$ i $e(\mathrm{O}) = \mathsf{G}$. Rezimirajmo ono što smo dosad pretpostavili:

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	Q				W				K	R				O	G				B	C						

Ubacimo ove pretpostavke u polazni šifrat:

```
TQCWT QCKIQ RWNOQ OBCEW OQVKB UKAPK OQOQB CQPQA
 ate  ati a je na nst e na is  i  i nanas ta a

JGDUQ EQORW TSJGR WEQKY WGTWC JKRBI KZGVO GBQ
 o  a  anje    oj e ai  eo et  ijs  i o n osa
```

Sada već imamo dovoljno elemenata otvorenog teksta da možemo postupno odgonetavati čitave riječi (npr. prva riječ: “matematika”, zadnja riječ: “odnosa”). Konačno dobivamo otvoreni tekst:

> Matematika je znanstvena disciplina nastala proučavanjem
> brojeva i geometrijskih odnosa.

Alfabet šifrata izgleda ovako:

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

Uočavamo pojavljivanje riječi “kriptografija” unutar alfabeta šifrata. Radi se o varijanti supstitucijske šifre koja se naziva *Cezarova šifra s ključnom riječi*. U njoj ključ predstavlja ključna riječ (u ovom slučaju *KRIPTOGRAFIJA*), te broj (u ovom slučaju *8*) koji označava poziciju (između 0 i 25) na kojoj počinjemo pisati ključnu riječ (bez ponavljanja slova). Naravno, da smo znali da je riječ upravo o ovoj varijanti, dekriptiranje bi nam bilo još lakše, no i bez toga nismo imali puno problema. ♢

Možemo zaključiti da je usprkos velikom prostoru ključeva, supstitucijska šifra vrlo laka za kriptoanalizu. To je bilo poznato već početkom 15. stoljeća, kada je u Italiji počela uporaba tzv. *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. Primjerice, ako kod šifriranja slova pomoću dvoznamenkastih brojeva naiđemo na nizove

$$12\ \ 17\ \ 37\ \ 23\ \ 57 \quad \text{i} \quad 12\ \ 17\ \ 42\ \ 23\ \ 57,$$

onda je prilično izvjesno da 37 i 42 predstavljaju isto slovo otvorenog teksta, pa ih možemo "spojiti" u analizi frekvencija.

1.3 Vigenèreova šifra

Blaise de Vigenère

Kod supstitucijske šifre svakom slovu otvorenog teksta odgovara jedinstveno slovo šifrata. Takve šifre se zovu *monoalfabetske*. Prikazat ćemo sada Vigenèreovu šifru koja spada u *polialfabetske šifre*. Naime, kod nje se svako slovo otvorenog teksta može preslikati u jedno od m mogućih slova (gdje je m duljina ključa), u ovisnosti o svom položaju unutar otvorenog teksta.

Francuski diplomat Blaise de Vigenère objavio je 1586. godine knjigu "Traicte de Chiffres" u kojoj se nalazilo sve što se u to vrijeme znalo o kriptografiji (ali gotovo ništa o kriptoanalizi). U njoj je opisano više originalnih polialfabetskih kriptosustava. Kriptosustav koji se danas naziva *Vigenèreova šifra* definiran je na sljedeći način.

Neka je m fiksan prirodan broj. Definiramo $\mathcal{P} = \mathcal{C} = \mathcal{K} = \mathbb{Z}_{26}^m$. Za ključ $K = (k_1, k_2, \ldots, k_m)$, definiramo

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

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

Primjer 1.5. Neka je $m = 4$ i ključna riječ *BROJ*. Njezin numerički ekvivalent je ključ $K = (1, 17, 14, 9)$. Pretpostavimo da je otvoreni tekst KRIPTOLOGIJA, čiji je numerički ekvivalent $(10, 17, 8, 15, 19, 14, 11, 14, 6, 8, 9, 0)$. Šifriranje se provodi na sljedeći način:

	1	*17*	*14*	*9*	*1*	*17*	*14*	*9*	*1*	*17*	*14*	*9*
	10	17	8	15	19	14	11	14	6	8	9	0
$+_{26}$												
	11	8	22	24	20	5	25	23	7	25	23	9

Dakle, šifrat je LIWYUFZXHZXJ. Uočimo da se prvo slovo O preslikalo u F, a drugo u X. ♢

Primjer 1.5 može se ilustrirati i ovako:

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

Vidimo da se ovdje ključ ponavlja unedogled pa prema podjeli šifara, s obzirom na način na koji se obrađuje otvoreni tekst, ovu šifru možemo shvatiti kao primjer blokovne šifre. Postoje i druge varijante Vigenèreove šifre. Jedna takva (sigurnija od originalne) je ona s *autoključem* (engl. autokey), u kojoj otvoreni tekst generira ključ. Naime, originalni ključ se koristi samo za šifriranje prvog bloka od m slova, dok se za šifriranje daljnjih blokova koristi prethodni blok otvorenog teksta. Time ova šifra spada u protočne šifre.

Primjer 1.6. Sve isto kao u Primjeru 1.5, ali s autoključem.

Rješenje. Pri šifriranju možemo koristiti tzv. *Vigenèreov kvadrat*.

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

Ako npr. slovo K treba šifrirati ključem *B*, onda pogledamo stupac koji počinje s K i redak koji počinje s *B*. U presjeku je šifrat L. Dobivamo:

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

♢

Vigenèreova šifra jedan je od najpopularnijih kriptosustava u povijesti. Spomenimo da je bila u širokoj uporabi tijekom Američke revolucije, krajem 18. stoljeća, a korištena je i u Američkom građanskom ratu. Čak je godine 1917. u uglednom časopisu "Scientific American" objavljeno da je ovu šifru "nemoguće razbiti". To, naravno, nije bilo točno jer su kriptoanalitičari već pola stoljeća prije toga poznavali metode za napad na Vigenèreovu šifru.

Recimo sada nešto o kriptoanalizi Vigenèreove šifre. Prvi korak je određivanje duljine ključne riječi. Prikazat ćemo dvije metode. Prva metoda se naziva *Kasiskijev test* i uveo ju je Friedrich Kasiski 1863. godine, a koristio ju je otprilike u isto vrijeme i Charles Babbage (začetnik ideje računala). Metoda se zasniva na činjenici da će dva identična odsječka otvorenog teksta biti šifrirana na isti način ukoliko se njihove početne pozicije razlikuju za neki višekratnik od m, gdje je m duljina ključa. Obrnuto, ako uočimo dva identična odsječka u šifratu, duljine barem 3, tada je vrlo vjerojatno da oni odgovaraju identičnim odsječcima otvorenog teksta (podudarnost odsječaka duljine 2 lako može biti i slučajna, dok je kod odsječaka veće duljine to puno manje vjerojatno).

U Kasiskijevom testu u šifratu tražimo parove identičnih odsječaka duljine barem 3, te (ako takvi postoje) zabilježimo udaljenosti između njihovih početnih položaja. Ako na takav način dobijemo udaljenosti $d_1, d_2, d_3, \ldots$, onda je razumna pretpostavka da m dijeli, ako ne sve, a onda barem većinu d_i-ova. Nakon što odredimo m, nalazimo se u sličnoj situaciji kao kod Cezarove šifre. Naime, ako pogledamo samo ona slova koja su šifrirana pomakom za k_1 slova (a ako znamo m, onda znamo i koja su to slova), onda su ona šifrirana običnom Cezarovom šifrom. Situacija je ipak nešto teža nego kod obične Cezarove šifre, zbog toga što to ovdje nisu uzastopna slova u otvorenom tekstu, pa njihovim dešifriranjem nećemo dobiti smisleni tekst. Zato ćemo opisati još jednu metodu za razbijanje Vigenèreove šifre.

Druga metoda za određivanje duljine ključa koristi tzv. indeks koincidencije. Taj je pojam uveo 1920. godine William Friedman u knjizi "Indeks koincidencije i njegove primjene u kriptografiji", koja se smatra jednom od najvažnijih publikacija u povijesti kriptologije.

Neka je $x = x_1 x_2 \cdots x_n$ niz od n slova. *Indeks koincidencije* od x, u oznaci $I_c(x)$, definira se kao vjerojatnost da su dva slučajna elementa iz x jednaka.

Neka su $f_0, f_1, \ldots, f_{25}$ redom (apsolutne) frekvencije od A, B, C, ..., Z u x. Dva elementa iz x možemo odabrati na $\frac{n(n-1)}{2}$ načina, a za svaki $i = 0, 1, \ldots, 25$ postoji $\frac{f_i(f_i-1)}{2}$ načina dvostrukog odabira i-tog slova u alfabetu. Stoga vrijedi formula

$$I_c(x) = \frac{\sum_{i=0}^{25} f_i(f_i-1)}{n(n-1)}.$$

Pretpostavimo sada da x predstavlja neki tekst na hrvatskom jeziku. Označimo očekivane vjerojatnosti pojavljivanja slova A, B, ..., Z u hrvatskom jeziku redom s $p_0, p_1, \ldots, p_{25}$ (vidi ranije navedene frekvencije slova u promilima). Ako je n dovoljno velik, za očekivati je da će vrijediti

$$I_c(x) \approx \sum_{i=0}^{25} p_i^2 \approx 0.064$$

(vjerojatnost da su oba slova A je $p_0^2 \approx 0.115^2$, da su oba B je $p_1^2 \approx 0.015^2$, itd.). Isti zaključak vrijedi i ukoliko je x šifrat dobiven iz otvorenog teksta na hrvatskom jeziku pomoću neke monoalfabetske šifre. Tu će se pojedinačne vjerojatnosti ispremiještati, ali će veličina $\sum_i p_i^2$ ostati nepromijenjena.

Pretpostavimo sada da imamo šifrat $y = y_1 y_2 \cdots y_n$ koji je dobiven Vigenèreovom šifrom. Rastavimo y na m podnizova $z_1, z_2, \ldots, z_m$ tako da y napišemo po stupcima, u matricu dimenzija $m \times \frac{n}{m}$ (ako m ne dijeli n, možemo nadopuniti y na proizvoljan način ili promatrati "krnju matricu" s nepotpunim zadnjim retkom). Redci ove matrice su upravo traženi podnizovi $z_1, z_2, \ldots, z_m$. Ako je m jednak duljini ključne riječi, onda su elementi istog retka matrice šifrirani pomoću istog slova ključa. Na primjer, prvi redak sadrži prvo, $(m+1)$-vo, $(2m+1)$-vo ... slovo šifrata, a sva su ta slova šifrirana pomoću k_1. Zato bi indeksi koincidencije $I_c(z_i)$, za $i = 1, \ldots, m$, trebali biti približno jednaki 0.064. S druge strane, ako m nije duljina ključne riječi, onda će z_i-ovi izgledati kao više-manje slučajni nizovi slova, budući da su dobiveni pomacima pomoću različitih slova ključa. Primijetimo da za potpuno slučajni niz r imamo $I_c(r) \approx 26 \cdot (\frac{1}{26})^2 = \frac{1}{26} \approx 0.038$. Ove dvije vrijednosti $\kappa_p = 0.064$ i $\kappa_r = 0.038$ (p = *plaintext* = otvoreni tekst, r = *random* = slučajan) su dovoljno daleko jedna od druge, tako da ćemo najčešće na ovaj način moći odrediti točnu duljinu ključne riječi (ili potvrditi pretpostavku dobivenu Kasiskijevom metodom). Napomenimo da je u engleskom jeziku $\kappa_p = 0.065$, u njemačkom 0.076, u francuskom 0.078, u talijanskom 0.074, a u španjolskom 0.078 (vidi [5, Poglavlje 16]). Odavde zaključujemo da za primjenu ove metode nije nužno znati na kojem je jeziku pisan otvoreni tekst. Jedina bitna pretpostavka jest da se za jezik na kojemu je pisan otvoreni tekst veličina κ_p značajno razlikuje od 0.038.

Primjer 1.7. Dekriptirati šifrat dobiven Vigenèreovom šifrom:

```
GSIQI TUKQI EAOHR VUGLT AZGHX UHLPJ MRTTN QRBZI
AVBTG QTBYM YAIVO MZTAI XJBTE DEWVQ WADVW GOOKN
QNTCI PEGPY BOKUS ECNWE LLCPZ UMIVW FUIJM YATUE
XISLM ZTNPG UJHTM ERXJS YSIVW ABGVW FDTZI LNTIE
DEFJM FAMPN QZBRS DIZPR MLGVK FEDZX MVXVQ MJXWS
LEEQR MAEPR UJXIM FNT
```

Primijenimo najprije Kasiskijev test. Uočavamo nekoliko trigrama koji se dvaput pojavljuju u šifratu. To su MYA s početkom na pozicijama 50 i 115 ($115-50 = 65 = 5 \cdot 13$), MZT s početkom na pozicijama 56 i 125 ($125 - 56 = 69 = 3 \cdot 23$), EDE ($160 - 65 = 95 = 5 \cdot 19$), IVW ($143 - 108 = 35 = 5 \cdot 7 \cdot 11$) i VWF ($149 - 109 = 40 = 5 \cdot 8$). Odavde se kao najvjerojatnija duljina ključne riječi nameće broj $m = 5$, koji dijeli sve osim jedne od razlika početnih pozicija ponovljenih trigrama.

Pogledajmo hoćemo li pomoću indeksa koincidencije doći do istog zaključka. Za $m = 1$ je $I_c = 0.040$; za $m = 2$ su indeksi 0.037 i 0.040; za $m = 3$ su 0.038, 0.048 i 0.038; za $m = 4$ su 0.036, 0.038, 0.044 i 0.036, dok za $m = 5$ dobivamo indekse 0.057, 0.052, 0.066, 0.076 i 0.066. Sada već s prilično velikom sigurnošću možemo zaključiti da je duljina ključne riječi jednaka 5.

Sljedeće je pitanje kako odrediti ključnu riječ ukoliko znamo njezinu duljinu. Tu nam može pomoći *međusobni indeks koincidencije dvaju nizova*.

Definicija 1.2. Neka su $x = x_1x_2 \cdots x_n$ i $y = y_1y_2 \cdots y_{n'}$ dva niza od n, odnosno n' slova. *Međusobni indeks koincidencije* od x i y, u oznaci $MI_c(x, y)$, definira se kao vjerojatnost da je slučajni element od x jednak slučajnom elementu od y. Ako frekvencije od A, B, C, ... , Z u x i y označimo s $f_0, f_1, \ldots, f_{25}$, odnosno $f'_0, f'_1, \ldots, f'_{25}$, onda je

$$MI_c = \frac{\sum_{i=0}^{25} f_i f'_i}{nn'}.$$

Neka je sada m duljina ključne riječi, a neka su podnizovi $z_1, z_2, \ldots, z_m$ dobiveni iz šifrata y kao prije. Pretpostavimo da je $K = (k_1, k_2, \ldots, k_m)$ ključna riječ i pokušajmo ocijeniti indeks $MI_c(z_i, z_j)$. Promotrimo proizvoljno slovo u z_i i proizvoljno slovo u z_j. Procijenimo vjerojatnost da su oba ova slova jednaka A. Prvo slovo A smo dobili pomakom za k_i, a drugo pomakom za k_j. Vjerojatnost da pomakom za k_i dobijemo slovo A približno je jednaka vjerojatnosti s kojom se u hrvatskom jeziku pojavljuje slovo čiji je numerički ekvivalent $-k_i \bmod 26$. Dakle, vjerojatnost, da su oba promatrana slova jednaka A, približno je jednaka $p_{-k_i}p_{-k_j}$,

da su oba slova B, približno je jednaka $p_{1-k_i}p_{1-k_j}$, itd. (operacije u indeksima su modulo 26). Dakle, imamo ocjenu

$$MI_c(z_i, z_j) \approx \sum_{h=0}^{25} p_{h-k_i}p_{h-k_j} = \sum_{h=0}^{25} p_h p_{h+k_i-k_j}$$

(pomakom indeksa suma se ne mijenja). Uočimo da ova ocjena ovisi samo o razlici $k_i - k_j \bmod 26$, koju ćemo zvati *relativni pomak* od z_i i z_j. Također, vrijedi $\sum_{h=0}^{25} p_h p_{h+q} = \sum_{h=0}^{25} p_h p_{h-q}$, što znači da za pomak q dobivamo istu ocjenu kao i za pomak $26 - q$. Stoga je dovoljno promatrati pomake između 0 i 13. To je (za hrvatski jezik) napravljeno u sljedećoj tablici:

relativni pomak	očekivana vrijednost od MI_c
0	0.064
1	0.039
2	0.031
3	0.031
4	0.044
5	0.040
6	0.039
7	0.033
8	0.040
9	0.042
10	0.036
11	0.036
12	0.036
13	0.039

Važno je uočiti da ako je pomak jednak 0, onda je ocjena 0.064, a ako je pomak različit od 0, onda su ocjene između 0.031 i 0.044 – dakle, bitno manje. Ovo zapažanje može se iskoristiti za određivanje vrijednosti $q = k_i - k_j$.

Pretpostavimo da smo fiksirali z_i, pa promotrimo efekt šifriranja z_j sa slovima A, B, C, ... , Z (tj. pomakom za $0, 1, 2, \ldots, 25$ mjesta). Tako dobivene nizove označimo sa $z_j^0, z_j^1, \ldots, z_j^{25}$. Za $g = 0, 1, \ldots, 25$ izračunamo indeks $MI_c(z_i, z_j^g)$ po formuli

$$MI_c(x, y^g) = \frac{\sum_{i=0}^{25} f_i f'_{i-g}}{nn'}.$$

Za $g \equiv q \pmod{26}$, MI_c bi trebao biti blizu 0.064, a za $g \not\equiv q \pmod{26}$ trebao bi varirati uglavnom između 0.031 i 0.044.

Na ovaj način možemo utvrditi relativne pomake bilo koja dva podniza z_i i z_j. Nakon što to učinimo, ostaje nam samo 26 mogućih ključnih riječi koje onda možemo ispitati jednu po jednu.

No, malom modifikacijom ove metode, do ključne riječi možemo doći učinkovitije, ukoliko nam je poznato na kojem je jeziku pisan otvoreni tekst. Umjesto međusobnog indeksa koincidencije nizova z_i i z_j^g, računat ćemo $MI_c(x, z_j^g)$, gdje je x niz koji odgovara tipičnom tekstu na jeziku otvorenog tekta. Pretpostavimo da nam je poznato (ili da to barem naslućujemo) da je otvoreni tekst pisan na hrvatskom jeziku. To znači da su relativne frekvencije f_i/n za x približno jednake p_i, pa je

$$MI_c(x, z_j^g) \approx \frac{\sum_{i=0}^{25} p_i f'_{i-g}}{n'}.$$

Očekujemo da je $MI_c(x, z_j^g) \approx 0.064$ ako je $g \equiv -k_j \pmod{26}$, a u protivnom da je $MI_c(x, z_j^g) < 0.045$.

Prema tome, da bismo odredili j-to slovo k_j ključne riječi K, postupamo na sljedeći način. Za $0 \leq g \leq 25$ izračunamo

$$M_g = \frac{\sum_{i=0}^{25} p_i f'_{i-g}}{n'}.$$

Odredimo h takav da je $M_h = \max\{M_g \,:\, 0 \leq g \leq 25\}$, te stavimo $k_j \equiv -h \pmod{26}$.

Nastavak primjera 1.7: Već smo zaključili da je $m = 5$. Za $j = 1, 2, 3, 4, 5$ izračunajmo vrijednosti $M_0, M_1, \ldots M_{25}$. Npr. za $j = 0$ je

$$M_0 = \frac{1}{44}(0.115 \cdot 3 + 0.015 \cdot 1 + 0.028 \cdot 0 + \cdots + 0.023 \cdot 1) \approx 0.0310.$$

Sve tražene vrijednosti nalaze se u sljedećoj tablici.

j	vrijednosti od M_g za $g = 0, 1, 2, \ldots, 25$						
1	0.0310	0.0341	0.0425	0.0427	0.0340	0.0386	0.0439
	0.0342	0.0400	0.0417	0.0476	0.0290	0.0266	0.0350
	0.0636	0.0440	0.0335	0.0304	0.0400	0.0327	0.0361
	0.0364	0.0389	0.0457	0.0395	0.0373		
2	0.0616	0.0421	0.0291	0.0271	0.0449	0.0406	0.0368
	0.0302	0.0423	0.0498	0.0411	0.0312	0.0316	0.0432
	0.0421	0.0382	0.0315	0.0485	0.0375	0.0373	0.0345
	0.0414	0.0410	0.0316	0.0254	0.0383		
3	0.0407	0.0369	0.0388	0.0439	0.0296	0.0336	0.0375
	0.0650	0.0355	0.0332	0.0313	0.0500	0.0407	0.0392
	0.0271	0.0393	0.0417	0.0363	0.0385	0.0250	0.0474
	0.0408	0.0404	0.0261	0.0415	0.0391		
4	0.0347	0.0321	0.0335	0.0289	0.0378	0.0510	0.0339
	0.0303	0.0267	0.0429	0.0393	0.0464	0.0250	0.0403
	0.0385	0.0496	0.0262	0.0330	0.0462	0.0643	0.0396
	0.0357	0.0344	0.0382	0.0450	0.0454		
5	0.0472	0.0419	0.0431	0.0333	0.0420	0.0380	0.0371
	0.0346	0.0398	0.0396	0.0338	0.0303	0.0394	0.0418
	0.0380	0.0243	0.0362	0.0467	0.0537	0.0212	0.0312
	0.0416	0.0681	0.0359	0.0330	0.0274		

Iz tablice iščitavamo redom:

- Za $j = 1$ imamo $h = 14$, $M_{14} = 0.0619$, pa je $k_1 = -14 \bmod 26 = 26 - 14 = 12$;
- Za $j = 2$ imamo $h = 0$, $M_0 = 0.0666$, pa je $k_2 = 0$;
- Za $j = 3$ imamo $h = 7$, $M_7 = 0.0677$, pa je $k_3 = 19$;
- Za $j = 4$ imamo $h = 19$, $M_{19} = 0.0633$, pa je $k_4 = 7$;
- Za $j = 5$ imamo $h = 22$, $M_{22} = 0.0636$, pa je $k_5 = 4$.

Stoga je ključna riječ *MATHE*, a traženi otvoreni tekst glasi:

```
USPJE HURJE SAVAN JUNEP OZNAT IHSIF ARAMJ ERISE
OVIMC ETIRI MAPOK AZATE LJIMA REDOM KAKOS UOVDJ
ENAVE DENIU PORNO SCUPA ZLJIV IMPOS TUPCI MAANA
LIZEI NTUIC IJOMI SRECO MSPOS OBNOS TDASE ZNABA
REMCI TATIJ EZIKO RIGIN ALNOG TEKST AVEOM AJEPO
ZELJN AALIN IJEBI TNA
```

ili, s umetnutim dijakritičkim znakovima (“kvačicama”), razmacima i interpunkcijom:

> Uspjeh u rješavanju nepoznatih šifara mjeri se ovim četirima pokazateljima, redom kako su ovdje navedeni: upornošću, pažljivim postupcima analize, intuicijom i srećom. Sposobnost da se zna barem čitati jezik originalnog teksta veoma je poželjna, ali nije bitna.

Tako glase (prema prijevodu iz [50]) prve dvije rečenice “Udžbenika za rješavanje vojnih šifara” autora Parkera Hitta, jednog od najpoznatijih američkih kriptografa iz vremena Prvog svjetskog rata. Koliko je u njima Hitt bio u pravu, možda može prosuditi i čitatelj ove knjige nakon što pokuša samostalno riješiti neke od zadataka na kraju poglavlja.