Polialfabetske supstitucijske šifre

Kobašević, Valentina

Master's thesis / Diplomski rad

2019

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:126:255999

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

Valentina Kobašević

Polialfabetske supstitucijske šifre

Diplomski rad

Osijek, 2019.

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

Valentina Kobašević

Polialfabetske supstitucijske šifre

Diplomski rad

Mentor: doc. dr. sc. Ivan Soldo

Osijek, 2019.

Sadržaj

Uvod

Kriptografija je znanstvena disciplina koja se bavi proučavanjem metoda za slanje poruka u takvom obliku da ih onaj kome su namijenjene može pročitati. Osnovni zadatak je omogućiti dvjema osobama (*pošiljalac* i *primalac*) komuniciranje preko nesigurnog komunikacijskog kanala na način da neka treća osoba (*protivnik*), koja može nadzirati komunikacijski kanal, ne može razumjeti njihove poruke.

Poruku koju pošiljalac želi poslati primaocu zovemo *otvoreni tekst*. Pošiljalac transformira otvoreni tekst koristeći unaprijed dogovoreni *ključ*. Taj postupak zove se *šifriranje* ili *kriptiranje*, a dobiveni tekst *šifrat* ili *kriptogram*. Nakon toga pošiljalac pošalje šifrat preko nekog komunikacijskog kanala, a protivnik prisluškujući može doznati sadržaj šifrata, ali ne može odrediti otvoreni tekst. Za razliku od njega, primalac zna ključ kojim je poruka šifrirana i može dešifrirati šifrat i odrediti otvoreni tekst.

Kriptoanaliza ili *dekriptiranje* je znanstvena disciplina koja se bavi proučavanjem postupaka za čitanje skrivenih poruka bez poznavanja ključa. Grana znanosti koja obuhvaća kriptografiju i kriptoanalizu naziva se *kriptologija*.

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, 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. Prema [3], vrijedi sljedeća definicija:

Definicija 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 elemenata otvorenog teksta;*
2. $\mathcal{C}$ *je konačan skup svih mogućih osnovnih elemenata šifrata;*
3. $\mathcal{K}$ *je konačan skup svih mogućih ključeva;*
4. $\mathcal{E}$ *je skup svih funkcija šifriranja;*
5. $\mathcal{D}$ *je skup svih funkcija dešifriranja;*

6. *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 otvoreni tekst* $x \in \mathcal{P}$.

Najvažnije svojstvo u definiciji je $d_K(e_K(x)) = x$ iz čega slijedi kako te funkcije moraju biti injekcije.

Kriptosustavi se obično klasificiraju obzirom na sljedeća tri kriterija:

1. Obzirom na tip operacija koje se koriste pri šifriranju:
   (a) *Supstitucijske šifre*: svaki element otvorenog teksta zamjenjuje se s nekim drugim elementom, prema unaprijed utvrđenoj transformaciji. Ovisno o broju transformacija, one mogu biti monoalfabetske i polialfabetske.
   (b) *Transpozicijske šifre*: elementi otvorenog teksta se premještaju, tj. permutiraju.
   (c) Kombinacija supstitucijskih i transpozicijskih šifri.
2. Obzirom na način na koji se obrađuje otvoreni tekst:
   (a) *Blokovne šifre*: obrađuje se jedan po jedan blok elemenata otvorenog teksta koristeći jedan te isti ključ.
   (b) *Protočne šifre*: elementi otvorenog teksta obrađuju se jedan po jedan koristeći pritom paralelno generirani niz ključeva (engl. *keystream*).
3. Obzirom na tajnost ključeva:
   (a) *Simetrični kriptosustavi*: ključ za dešifriranje može se izračunati poznavajući ključ za šifriranje i obratno. Ovi su ključevi najčešće identični, pa sigurnost ovih kriptosustava leži u tajnosti ključa. Zato se oni zovu i *kriptosustavi s tajnim ključem.*
   (b) *Asimetrični kriptosustavi*: ključ za dešifriranje ne može se u nekom razumnom vremenu izračunati iz ključa za šifriranje. Ovdje je ključ za šifriranje javan, pa se zato oni zovu i *kriptosustavi s javnim ključem.* 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.

Naravno, osnovna je pretpostavka da kriptoanalitičar zna koji se kriptosustav koristi. Svaka usmjerena radnja kriptoanalitičara zove se *napad*. Razlikuju se četiri osnovne vrste napada:

1. *Napad poznatim šifratom*: 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. *Napad poznatim otvorenim tekstom*: 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. *Napad odabranim otvorenim tekstom*: kriptoanalitičar ima mogućnost odabira teksta koji će biti šifriran, te može dobiti njegov šifrat. Na taj način, dobrim odabirom skupa poruka, može dobiti što više informacija o upotrebljenom ključu. Ovaj napad jači je od prethodnoga, ali je manje realističan.

4. *Napad odabranim šifratom*: kriptoanalitičar je dobio pristup alatu za dešifriranje, pa može odabrati šifrat i dobiti odgovarajući otvoreni tekst. Ovaj napad je tipičan kod kriptosustava s javnim ključem. Tu je zadatak kriptoanalitičara otkriti ključ za dešifriranje, tj. tajni ključ.

   Postoji još jedan (neprimjeren) oblik napada:

5. *Napad potkupljivanjem, ucjenama, krađama i slično*: ovaj napad ne spada u kriptoanalizu, ali je vrlo efikasan i često primjenjivan u kombinaciji s ranije navedenim kriptoanalitičkim napadima.

Cilj je ovog diplomskog rada opisati povijest nekih od najpoznatijih polialfabetskih supstitucijskih šifri, kao i njihovu kriptoanalizu. Kao dio uvoda definiraju se osnovni pojmovi iz kriptografije potrebni za razumijevanje ostatka ovog rada. Nadalje, obrađene su najpoznatije polialfabetske supstitucijske šifre kroz povijest: Albertijeva šifra, Trithemiusova šifra, Vigenèreova šifra, Beaufortova šifra, Playfairova šifra, Šifra četiri kvadrata, Šifra dva kvadrata i Hillova šifra.

Kako su tema ovog rada polialfabetske supstitucijske šifre, za neke metode koje su opisane u radu bitno je poznavati frekvenciju slova za pojedini jezik. Tako

frekvencija slova od najfrekventnijih do najmanje frekventnih izražena u promilima (1‰ = 0.1%) u hrvatskom jeziku iznosi kako slijedi: $A(115)$, $I(98)$, $O(90)$, $E(84)$, $N(66)$, $S(56)$, $R(54)$, $J(51)$, $T(48)$, $U(43)$, $D(37)$, $K(36)$, $V(35)$, $L(33)$, $M(31)$, $P(29)$, $C(28)$, $Z(23)$, $G(16)$, $B(15)$, $H(8)$, $F(3)$. Najfrekventniji bigrami u hrvatskom jeziku su: $JE(27)$, $NA(15)$, $RA(15)$, ST, AN, NI, KO, OS, TI, IJ, NO, EN, $PR(10)$. Zanimljivo je uočiti da je najfrekventniji bigram JE iako slovo J nije među najfrekventnijim slovima. Najfrekventniji recipročni bigrami su $NA(15)$ i $AN(14)$, te $NI(13)$ i $IN(9)$. Najfrekventniji trigram u hrvatskom jeziku je $IJE(6)$ te STA, OST, JED, KOJ, OJE, JEN s frekvencijama između 3‰ i 4‰. Često je otvoreni tekst pisan i engleskim i njemačkim jezikom. Stoga je za pravilno dešifriranje potrebno poznavati i frekvencije slova u tim jezicima, što je moguće vidjeti primjerice u [3].

Dodatno, uvodi se korespodencija između slova engleskog alfabeta (A – Z) koji se smatra međunarodnim alfabetom i cijelih brojeva (0 – 25) na sljedeći način:

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

Ukoliko se bude radilo s otvorenim tekstom na hrvatskom jeziku, onda se hrvatska slova s dijakritičkim znakovima mijenjaju s onima bez njih. Razlog korištenja numeričkog ekvivalenta slova leži u načinu na kojeg neki kriptosustavi šifriraju i dešifriraju otvoreni tekst – koristeći upravo numeričku reprezentaciju slova.

1 Polialfabetske supstitucijske šifre

Polialfabetska supstitucijska šifra predstavlja napredak nad monoalfabetskim supstitucijskim šiframa utoliko što se svako slovo otvorenog teksta može šifrirati u nekoliko različitih slova šifrata. Drugim riječima, šifriranje ne koristi jedan supstitucijski alfabet nego više njih. Ovo poglavlje predstavlja najznačajnije takve kriptosustave kroz povijest. Na primjerima ilustriramo njihovo djelovanje i opisujemo mogućnosti napada na takve kriptosustave.

1.1 Albertijeva šifra

Leon Battista Alberti, vanbračno dijete talijanskog plemića (nije poznato tko mu je majka), rođen je 1404. godine u Genovi. Razvio je metodu šifriranja koja je donijela revoluciju u područje kriptografije na zapadu. Albertijeva šifra, opisana u njegovoj raspravi o šifriranju *De Cifris* 1467. godine, prva je polialfabetska šifra. Raspravu je napisao za prijatelja Leonarda Datija ali ona nije bila tiskana u 15. stoljeću.

Slika 1: *Leon Battista Alberti*[1]

Poznat je po svome radu u arhitekturi, pisanju i slikanju, ali najviše se istaknuo u području kriptologije gdje je, prema [4], dobio naziv "otac zapadnjačke kriptologije". Albertijeva šifra tradicionalno se sastojala od dva koncentrična metalna diska – jednog pokretnog i jednog statičnog – pri čemu se unutarnji mogao rotirati. Svaki

[1] 14. veljače 1404. – 25. travnja 1472.; Izvor: Trinity College

od diskova podijeljen je na 24 jednake ćelije. S vanjske strane vanjskog diska bila su popisana velika slova latinskog pisma, odnosno engleske abecede izuzev slova `J`, `U`, `W`, `H`, `K` i `Y`. Alberti je smatrao da su navedena slova nepotrebna (jer se u latinskom jeziku nisu puno koristila) ili da se mogu zamijeniti drugim slovima. Osim slova abecede, tamo su se nalazili i brojevi od 1 do 4 koji bi se koristili zajedno s knjigom u kojoj su bile zapisane ranije definirane fraze (njih 336) koje su se preslikavale na četveroznamenkaste kombinacije tih brojeva. Ovi brojevi mogu se koristiti i kao upute za rotiranje diska tijekom postupka šifriranja kako je opisano u *drugoj metodi šifriranja* u nastavku ovog potpoglavlja. Unutarnji disk sadržavao je mala slova latinskog pisma, odnosno engleske abecede u nasumičnom poretku izuzev slova `u`, `w` i `j`, ali uključujući `et` (što se vjerojatno odnosilo na znak `&`). Ovakva naprava naziva se Albertijev disk za šifriranje te je vidljiva na *Slici 2*.

Slika 2: *Albertijev disk za šifriranje*[2]

Dakle, korištena slova, brojke i znakovi u vanjskom, odnosno unutrašnjem disku su sljedeći:

- vanjski disk: `A B C D E F G I L M N O P Q R S T V X Z 1 2 3 4`;
- unutrašnji disk: `g k l n p r t v z & x y s o m q i h f d b a c e`.

Poznate su dvije bazične metode za šifriranje koristeći Albertijev disk objašnjene u nastavku.

[2]Izvor: Wikimedia

Metoda 1. Prvi korak šifriranja priprema je otvorenog teksta iz kojeg je potrebno izbaciti ili zamijeniti slova koja se ne nalaze na vanjskom disku. Ovakav dizajn korišten je da bi se dodatno smanjila mogućnost pojavljivanja uzoraka, odnosno da bi se šifrat dodatno osigurao od frekvencijske analize. Mala slova unutarnjeg diska koriste se kao indeksna slova. Na početku se izabere jedno slovo unutarnjeg diska kao indeksno te se tijekom šifriranja (svaku riječ, svakih nekoliko riječi ili na proizvoljnim mjestima) mijenja slovo iz vanjskog diska koje se na njega preslikava. Pri promjeni slova, što se odnosi i na sam početak procesa, u šifrat se velikim slovom zapisuje ono slovo na koje se izabrano indeksno unutarnjeg diska preslikava u ostatku šifrata (ili do pojavljivanja sljedećeg velikog slova).

Metoda 2. U otvoreni tekst na proizvoljna mjesta ubacuju se brojevi 1–4 (ili njihove kombinacije) kojima je potrebno definirati značenje u smislu promjene preslikavanja slova. Tako, primjerice, šifriranje broja 2 može značiti rotaciju unutarnjeg diska (pomak preslikavanja) za dva mjesta u smjeru kazaljke na satu – ili suprotno od smjera kazaljke na satu, ovisno o definiciji. Šifriranje broja 14 tako može značiti, primjerice, rotaciju diska za pet ili za tri mjesta (zbroj ili razlika brojeva 1 i 4) u nekom od smjerova. U ovoj se metodi slova vanjskog diska koriste kao indeksna slova, a kako šifriranje ovisi o rotiranju prouzročenom brojevima, u šifrat se pri promjeni preslikavanja ne zapisuje veliko slovo koje se preslikava.

Primjer 1. *Šifrirajmo otvoreni tekst*

POLIALFABETSKA SUPSTITUCIJSKA ŠIFRA SVAKA JE ŠIFRA KOJA SE BAZIRA NA SUPSTITUCIJI KORISTEĆI VIŠE ALFABETA

koristeći prvu metodu šifriranja primjenom Albertijevog diska.

Rješenje:

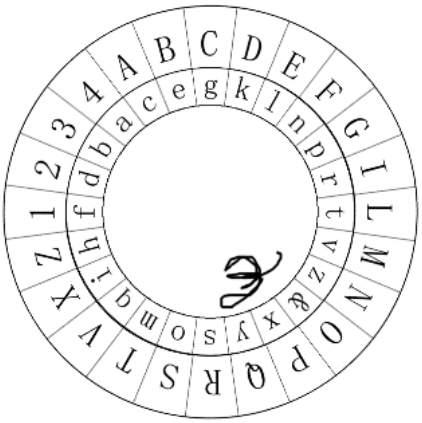
Prvi korak priprema je otvorenog teksta za šifriranje Albertijevom šifrom, pa tako izbacivanjem hrvatskih dijakritičkih znakova i proizvoljnom zamjenom slova

$$\mathtt{j} \mapsto \mathtt{i}, \mathtt{u} \mapsto \mathtt{v}, \mathtt{k} \mapsto \mathtt{c}$$

kojom se i dalje može iščitati otvoreni tekst dobije se:

POLIALFABETSCA SVPSTITVCIISCA SIFRA SVACA IE SIFRA COIA SE BAZIRA NA SVPSTITVCIII CORISTECI VISE ALFABETA.

Neka je indeksno slovo sa unutarnjeg diska primjerice slovo `m`*. Uzme li se da za prvu riječ vrijedi preslikavanje* `T` $\mapsto$ `m` *(prikazano na Slici 3), tada se prva riječ otvorenog teksta šifrira na sljedeći način:* `POLIALFABETSCA` $\mapsto$ `Tx&trctncelmogc`*. Analogno se diskovi mogu okretati za sljedeće riječi kao posljedica biranja slova koja se preslikavaju u ranije odabrano indeksno slovo* `m` *iz unutarnjeg diska.*



Slika 3: *Albertijev disk za šifriranje postavljen tako da vrijedi preslikavanje* $T \mapsto m$[3]

Kako je u opisu metode spomenuto, promjena preslikavanja može se dogoditi neovisno o početku riječi, odnosno može biti proizvoljne učestalosti. Neka se u ovom primjeru preslikavanja mijenjaju za svaku veću riječ, a manje riječi neka se spajaju sa susjednim većim riječima. Neka zbog toga u ovom primjeru vrijede sljedeća preslikavanja, a time i šifriranja:

- `G` $\mapsto$ `m`*, pa vrijedi:* `SVPSTITVCIISCA` $\mapsto$ `Gekbegqgkxqqexz`*;*
- `D` $\mapsto$ `m`*, pa vrijedi:* `SIFRA` $\mapsto$ `Dlfiky`*;*
- `V` $\mapsto$ `m`*, pa vrijedi:* `SVACAIE` $\mapsto$ `Vsmaeapk`*;*
- `X` $\mapsto$ `m`*, pa vrijedi:* `SIFRA` $\mapsto$ `Xynkxb`*;*
- `N` $\mapsto$ `m`*, pa vrijedi:* `COIASE` $\mapsto$ `Ntqypdz`*;*
- `L` $\mapsto$ `m`*, pa vrijedi:* `BAZIRANA` $\mapsto$ `Lvtkobtit`*;*
- `F` $\mapsto$ `m`*, pa vrijedi:* `SVPSTITVCIII` $\mapsto$ `Fglagkiklyiii`*;*

[3]Izvor: Venetian Cryptography

- `Q` $\mapsto$ `m`, *pa vrijedi:* `CORISTECI` $\mapsto$ `Qnsqzihrnz`;
- `A` $\mapsto$ `m`, *pa vrijedi:* `VISE` $\mapsto$ `Avarf`;
- `O` $\mapsto$ `m`, *pa vrijedi:* `ALFABETA` $\mapsto$ `Onyznpvdn`.

Konačno, dobivamo šifrat:

`Tx&trctncelmogcGekbegqgkxqqexzDlfikyVsmaeapkXynkxbNtqypdz LvtkobtitFglagkiklyiiiQnsqzihrnzAvarfOnyznpvdn`.

Primjer 2. *Šifrirajmo otvoreni tekst*

`POLIALFABETSKA SUPSTITUCIJSKA ŠIFRA SVAKA JE ŠIFRA KOJA SE BAZIRA NA SUPSTITUCIJI KORISTEĆI VIŠE ALFABETA`

koristeći drugu metodu šifriranja primjenom Albertijevog diska.

Rješenje:

Prvi korak priprema je otvorenog teksta za šifriranje Albetrijevom šifrom ekvivalentno Primjeru 1 tako da je polazni otvoreni tekst:

`POLIALFABETSCA SVPSTITVCIISCA SIFRA SVACA IE SIFRA COIA SE BAZIRA NA SVPSTITVCIII CORISTECI VISE ALFABETA`.

Neka se primjerice `A` *preslikava u* `m`. *Također, neka se između svake dvije riječi umjesto razmaka nađe broj* $1-4$ *koji će, primjerice, označavati pomak unutarnjeg diska u smjeru obrnutom od kazaljke na satu. Tada je otvoreni tekst sljedećeg oblika:*

`POLIALFABETSCA2SVPSTITVCIISCA4SIFRA2SVACA1IE4SIFRA1COIA 3SE4BAZIRA2NA2SVPSTITVCIII3CORISTECI1VISE1ALFABETA`.

Sada vrijede sljedeća preslikavanja, a time i šifriranja:

- `A` $\mapsto$ `m` *(početno stanje), pa vrijedi:* `POLIALFABETSCA` $\mapsto$ `lkcamcdmqftrim`;
- `A` $\mapsto$ `i` *(pomak za 2), pa vrijedi:* `SVPSTITVCIISCA` $\mapsto$ `v&pvzez&feevfi`;
- `A` $\mapsto$ `b` *(pomak za 4), pa vrijedi:* `SIFRA` $\mapsto$ `ynkxb`;
- `A` $\mapsto$ `c` *(pomak za 2), pa vrijedi:* `SVACA` $\mapsto$ `oqcgc`;
- `A` $\mapsto$ `e` *(pomak za 1), pa vrijedi:* `IE` $\mapsto$ `tn`;

- `A` $\mapsto$ `n` *(pomak za 4), pa vrijedi:* `SIFRA` $\mapsto$ `fxzhn`*;*
- `A` $\mapsto$ `p` *(pomak za 1), pa vrijedi:* `COIA` $\mapsto$ `tqyp`*;*
- `A` $\mapsto$ `v` *(pomak za 3), pa vrijedi:* `SE` $\mapsto$ `cy`*;*
- `A` $\mapsto$ `y` *(pomak za 4), pa vrijedi:* `BAZIRA` $\mapsto$ `sytfky`*;*
- `A` $\mapsto$ `o` *(pomak za 2), pa vrijedi:* `NA` $\mapsto$ `eo`*;*
- `A` $\mapsto$ `q` *(pomak za 2), pa vrijedi:* `SVPSTITVCIII` $\mapsto$ `tzntvcvzhccc`*;*
- `A` $\mapsto$ `f` *(pomak za 3), pa vrijedi:* `CORISTECI` $\mapsto$ `brzk&xcbk`*;*
- `A` $\mapsto$ `d` *(pomak za 1), pa vrijedi:* `VISE` $\mapsto$ `slxe`*;*
- `A` $\mapsto$ `b` *(pomak za 1), pa vrijedi:* `ALFABETA` $\mapsto$ `bpkbagsb`*.*

Konačno, dobivamo šifrat:

`lkcamcdmqftrimv&pvzez&feevfiynkxboqcgctnfxzhn`
`tqypcysytfkyeotzntvcvzhcccbrzk&xcbkslxebpkbagsb`*.*

Alberti je, prema [4], smatrao da je njegova šifra neprobojna. Svoje je pretpostavke bazirao na tome kako funkcionira frekvencijska analiza teksta. Ona je bila jedina tada znana tehnika za napad na neki kriptosustav te je bila vrlo efikasna za dekriptiranje monoalfabetskih šifri. Zaista, u usporedbi s ostalim kriptosustavima tog vremena, Albertijeva šifra nije se mogla razbiti bez znanja o metodi šifriranja što uključuje poredak slova u unutarnjem disku, učestalost promjene preslikavanja vanjskog na unutarnji disk, veličina i smjer pomaka pri promjeni preslikavanja, itd. Razlog se svodi na to da je distribucija frekvencija slova u šifratu dobivenom Albertijevom šifrom bila skrivena.

Primjer 3. *Dešifrirajmo šifrat*

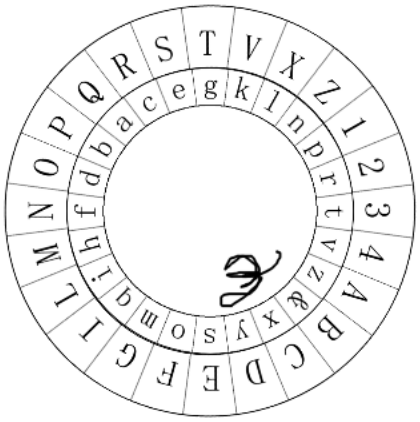
`Tx&trctncelmogcGekbegqgkxqqexzDlfikyVsmaeapkXynkxbNtqypdz`
`LvtkobtitFglagkiklyiiiQnsqzihrnzAvarfOnyznpvdn`

dobiven Albertijevom šifrom iz otvorenog teksta na hrvatskom jeziku. Neka je, dodatno, poznato da je šifrat dobiven prvom metodom šifriranja primjenom Albertijevog diska uz `m` *kao indeksno slovo unutarnjeg diska.*

Rješenje:

Kako je `T` *prvo veliko slovo šifrata i jer je znano da je* `m` *indeksno slovo unutarnjeg diska, za dešifriranje prvog dijela šifrata* `Tx&trctncelmogc` *potrebno je postaviti Albertijev disk tako da vrijedi preslikavanje* $\texttt{T} \mapsto \texttt{m}$ *kao na Slici 3. Iz tako postavljenog diska vidljivo je kako se navedeni dio šifrata dešifrira u dio otvorenog teksta* `POLIALFABETSCA`.

Sljedeće veliko slovo u šifratu je slovo `G` *pa je za nastavak dešifriranja potrebno Albertijev disk postaviti kao na Slici 4 tako da vrijedi preslikavanje* $\texttt{G} \mapsto \texttt{m}$. *Iz tako postavljenog diska vidljivo je da se dio šifrata* `Gekbegqgkxqqexz` *dešifrira u dio otvorenog teksta* `SVPSTITVCIISCA`.



Slika 4: *Albertijev disk za šifriranje postavljen tako da vrijedi preslikavanje* $\texttt{G} \mapsto \texttt{m}$[4]

Analogno dešifriramo i ostatak šifrata te dobivamo:

`POLIALFABETSCASVPSTITVCIISCASIFRASVACAIESIFRACOIASE`
`BAZIRANASVPSTITVCIIICORISTECIVISEALFABETA`.

Dodajući razmake, dijakritičke znakove i zamjenom svih slova koje Albertijeva šifra zamijeni u pripremi otvorenog teksta za šifriranje dobije se sljedeći otvoreni tekst:

`POLIALFABETSKA SUPSTITUCIJSKA ŠIFRA SVAKA JE ŠIFRA KOJA SE`
`BAZIRA NA SUPSTITUCIJI KORISTEĆI VIŠE ALFABETA`.

[4]Izvor: Venetian Cryptography

1.2 Trithemiusova šifra

Polialfabetske substitucijske šifre doživjele su sljedeći pozitivan korak pojavom prve tiskane knjige o kriptologiji kao dio skupa radova nazvanih *Polygraphiae libri sex, loannis Trithemii abbatis Peapolitani, quondam Spanheimensis, ad Maximilianum Caesarem* koju je napisao jedan od najpoznatijih intelektualaca svojeg vremena, Johannes Trithemius, njemački benediktinski redovnik. Knjigu je napisao 1508. godine, a tiskana je 1518. godine nakon njegove smrti. Prema [4], bavio se alkemijom i magijom što je doprinijelo tome da postane jedna od najpoznatijih osoba u okultnim znanostima, dok je zbog svog znajačajnijeg (konkretnijeg) znanstvenog rada – u područjima povijesti, teologije i kriptografije – dobio nadimak "otac bibliografije".

Slika 5: *Johannes Trithemius*[5]

U navedenom se radu po prvi puta pojavljuje kvadratna tablica koja se sastoji od slova, tzv. "tableau". Takva tablica osnovni je oblik polialfabetske substitucije jer odjednom prikazuje sve alfabete nekog sustava šifriranja. Sadržaj tablice obično su nizovi istih slova pomaknuti u različite pozicije u odnosu na alfabet otvorenog teksta, kao što je na Albertijevom disku unutarnji alfabet bio pomaknut za određen broj pozicija u odnosu na vanjski. U tablici su oni jednoliko poredani tako da svaki redak označava alfabet pomaknut za jedno mjesto ulijevo u odnosu na onaj prošli. Svaki redak, dakle, nudi drugačiji skup supstitucija u odnosu na alfabet otvorenog teksta koji je na vrhu. Kako redaka može biti samo onoliko koliko ima slova u

[5] 1. veljače 1462. – 13. prosinca 1516.; Izvor: Amazon

abecedi, tablica je kvadratna. Najjednostavnija takva tablica je ona koja koristi običan alfabet kao početni – što je upravo tablica kakvu je Trithemius koristio i koju je nazvao "tabula recta" (*Tablica 1*).

Trithemiusova šifra koristi tabulu rectu tako da se otvoreni tekst šifrira na način da je prvo slovo otvorenog teksta šifrirano slovom koje je na presjeku retka s tim slovom (iz otvorenog teksta) i prvog stupca. Zatim, drugo slovo otvorenog teksta šifrira se slovom koje je na presjeku retka s tim slovom (iz otvorenog teksta) i drugog stupca. Postupak se analogno ponavlja po slovima otvorenog teksta i stupcima tabule recte, a kada se dođe do zadnjeg stupca tablice ponovno se krene od prvoga koji predstavlja originalni alfabet.

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

Tablica 1: *Trithemiusova tabula recta*

Primjer 4. *Šifrirajmo otvoreni tekst*

POLIALFABETSKA SUPSTITUCIJSKA ŠIFRA SVAKA JE ŠIFRA KOJA SE BAZIRA NA SUPSTITUCIJI KORISTEĆI VIŠE ALFABETA

koristeći Trithemiusovu šifru.

Rješenje:

Prvi korak priprema je otvorenog teksta za šifriranje. Kod šifriranja Trithemiusovom šifrom nije potrebno izbacivati slova kao što je to kod Albertijeve šifre. Iz otvorenog teksta izbacuju se razmaci i dijakritički znakovi, pa on izgleda kako slijedi:

`POLIALFABETSKASUPSTITUCIJSKASIFRASVAKAJESIFRA`
`KOJASEBAZIRANASUPSTITUCIJIKORISTECIVISEALFABETA.`

Primjenom Tablice 2 dio otvorenog teksta `POLIALFABETSKA` *šifrira se u* `PPNLEQLHJNDDWN`.

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

Tablica 2: *Šifriranje otvorenog teksta* ***`POLIALFABETSKA`*** *Trithemiusovom šifrom*

Analogno se šifrira i ostatak otvorenog teksta, pa je krajnji rezultat sljedeći šifrat:

`PPNLEQLHJNDDWNGJFJLBNPYFHRKBULJWGZDJULVRGXVISD`
`IEWPCAAAKUESGZCYCEUGIRYAADIMEPRDCJXLWJGSNJLPFN.`

Da bi se uspješno izvršio napad na šifrat dobiven Trithemiusovom šifrom, potrebno je jedino znati da je upravo njome šifriran. Kako se postupkom šifriranja

šifrat dobiva pomicanjem udesno po stupcima tabule recte, tako se dešifriranje obavlja suprotnom radnjom, odnosno pomicanjem ulijevo te se, kada se dođe do prvog stupca tablice, ponovno krene od zadnjega. Obzirom da se prvo slovo Trithemiusovom šifrom šifrira prvim stupcem, dešifriranju/napadu se također pristupa od prvog stupca.

Primjer 5. *Dešifrirajmo šifrat*

PPNLEQLHJNDDWNGJFJLBNPYFHRKBULJWGZDJULVRGXVISD
IEWPCAAAKUESGZCYCEUGIRYAADIMEPRDCJXLWJGSNJLPFN.

dobiven Trithemiusovom šifrom iz otvorenog teksta na hrvatskom jeziku.

Rješenje:

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

Tablica 3: *Napad na šifrat* ***PPNLEQLHJNDDWN*** *dobiven Trithemiusovom šifrom*

Primjenom Tablice 3 šifrat PPNLEQLHJNDDWN *dešifriramo u* POLIALFABETSKA. *Analogno dešifriramo i ostatak šifrata te dobivamo:*

POLIALFABETSKASUPSTITUCIJSKASIFRASVAKAJESIFRA
KOJASEBAZIRANASUPSTITUCIJIKORISTECIVISEALFABETA.

Dodajući razmake i dijakritičke znakove dobije se polazni otvoreni tekst:

POLIALFABETSKA SUPSTITUCIJSKA ŠIFRA SVAKA JE ŠIFRA
KOJA SE BAZIRA NA SUPSTITUCIJI KORISTEĆI VIŠE ALFABETA.

Tabula recta vrlo je praktična pri šifriranju i dešifriranju, no isti postupak mogao je biti napravljen koristeći Albertijev disk za šifriranje uz rotaciju unutarnjeg diska nakon šifriranja svakog slova otvorenog teksta. Upravo to bitna je razlika između Albertijeve i Trithemiusove šifre, tj. za šifriranje svakog slova otvorenog teksta Trithemiusovom šifrom koristi se novi alfabet. Trithemiusova šifra vrlo je važan korak u razvoju sigurnih šifri, no zbog nedostatka bilo kakvog ključa za šifriranje i dešifriranje zapravo je vrlo laka za razbiti jer svaka poruka – svaki otvoreni tekst – šifriran njome koristi u potpunosti istu metodu.

1.3 Vigenèrova šifra

Kako je već navedeno u *Potpoglavljima 1.1 i 1.2*, prva dva značajna koraka za polialfabetske šifre napravili su Alberti i Trithemius koji su bili vrlo poznati. Sljedeći značajan korak napravio je čovjek koji nije ostavio puno traga iza sebe, talijan Giovan Battista Bellaso. Zna se da je rođen u Bresciai 1505. godine u plemićkoj obitelji, te da je 1553. godine izdao knjižicu pod nazivom *La Cifra del Sig. Giovan Battista Bellaso.*

Slika 6: *Giovan Battista Bellaso*[6]

[6]1505. – ?; Izvor: Twitter

U toj je knjižici, prema [4], sugerirao korištenje ključa za polialfabetske šifre koji se jednostavno pamti i lako može zamijeniti – on ga je nazvao "countersign" – a koji se može sastojati od proizvoljnog broja riječi bilo kojeg jezika. Napisao je kako se iznad otvorenog teksta treba, slovo po slovo, napisati ključ i ponavljati ga dok se ne dođe do kraja otvorenog teksta.

Tako bi, primjerice, iznad otvorenog teksta `POLIALFABETSKA SUPSTITUCIJSKA SIFRA` uz ključ `BELLASO SIFRA` njegova metoda izgledala kako slijedi:

```
BELLASOSIFRABE LLASOSIFRABELL ASOSI
POLIALFABETSKA SUPSTITUCIJSKA SIFRA.
```

Slovo ključa koje je upareno s nekim slovom otvorenog teksta indicira alfabet tabule recte koji se treba koristiti za šifriranje tog slova otvorenog teksta. Točnije, slovo šifrata nalazi se na presjeku retka koji je predstavljen slovom otvorenog teksta i stupca koji je predstavljen slovom ključa. U navedenom primjeru slovo `P` šifriralo bi se slovom alfabeta koje odgovara slovu `B`, slovo `O` slovom alfabeta koje odgovara slovu `E`, te analogno za sva ostala slova. Ovakav sustav dopušta veliku fleksibilnost jer se sve poruke – odnosno otvoreni tekstovi – više nisu morali šifrirati jednom od samo nekoliko standardno korištenih kombinacija alfabeta. Svakome kome se šalje neki šifrat mogao se dodijeliti poseban ključ, a ako se smatralo da je ključu ugrožena sigurnost, jednostavno bi se zamijenio drugim. Ovakav način korištenja ključeva u kriptografiji brzo je bio prepoznat i postavio je temelje za današnje kompleksnije sustave koji koriste razne kombinacije ključeva koji se izmijenjuju u nekim vremenskim intervalima. Štoviše, kombinirajući miješane alfabete Albertija i šifriranje jednog po jednog slova Trithemiusa te dodajući svoju ideju o ključevima, Bellaso je stvorio moderne koncepte polialfabetskih supstitucijskih šifri. Međutim, kasnije je u 19. stoljeću Bellasova šifra pogrešno pripisana Blaise de Vigenèru, francuskom diplomatu i kriptografu.

Blaise de Vigenère rođen je 1523. godine u Saint–Pourçainu u Francuskoj. Sa 17 godina stupio je u diplomatsku službu, gdje je proveo 30 godina. Pet godina proveo je u Wormskom saboru (njem. *Reichstag zu Worms*) kao mlađi tajnik. S 24 godine stupio je u službu Vojvode od Neversa. Godine 1549. bio je u dvogodišnjoj diplomatskoj misiji u Rimu gdje je dolazio u kontakt s knjigama o kriptografiji – čitao je Trithemiusove i Bellasove knjige, kao i neobjavljene rukopise Albertija. S 47 godina odlazi u mirovinu i tada piše preko 20 knjiga, uključujući i *Traicté de Chiffres* 1585. godine. U toj knjizi opisuje prethodno ilustriranu šifru koju je prvi

definirao Bellaso, zbog čega mu se ona kasnije pogrešno pripisala.

Slika 7: *Blaise de Vigenère*[7]

Kako je već objašnjeno, Vigenèrovom šifrom šifrira se koristeći tabulu rectu, koja je zbog toga i popularnosti same šifre bila još nazivana i *Vigenèrovim kvadratom* ili *Vigenèrovom tablicom.* Obzirom da se za svako slovo otvorenog teksta koristi jedan od alfabeta iz tabule recte koji odgovara uparenom mu slovu ključa, to znači da se iz tabule recte ovom metodom koriste samo alfabeti koji odgovaraju nekom od slova iz ključa (a ostali zanemaruju).

Primjer 6. *Šifrirajmo otvoreni tekst*

POLIALFABETSKA SUPSTITUCIJSKA ŠIFRA SVAKA JE ŠIFRA KOJA SE BAZIRA NA SUPSTITUCIJI KORISTEĆI VIŠE ALFABETA. NAJPOZNATIJA TAKVA ŠIFRA POVIJESNO JE PRIPISANA KRIVOJ OSOBI, A TAKO ODREĐENA NOMENKLATURA OSTALA JE DO DANAS. KOMBINIRAJUĆI MIJEŠANE ALFABETE I ŠIFRIRANJE JEDNOG PO JEDNOG SLOVA TE DODAJUĆI IDEJU O KLJUČEVIMA, STVORENI SU MODERNI KONCEPTI POLIALFABETSKIH SUPSTITUCIJSKIH ŠIFRI

koristeći Vigenèrovu šifru.

Rješenje:

Navedeni otvoreni tekst pripremljen za šifriranje izgleda kako slijedi:

[7] 5. travnja 1523. – 19. veljače 1596.; Izvor: Wikipedia

POLIALFABETSKASUPSTITUCIJSKASIFRASVAKAJESIFRAKOJASEBAZIRA
NASUPSTITUCIJIKORISTECIVISEALFABETANAJPOZNATIJATAKVASIFRA
POVIJESNOJEPRIPISANAKRIVOJOSOBIATAKOODREDENANOMENKLATURA
OSTALAJEDODANASKOMBINIRAJUCIMIJESANEALFABETEISIFRIRANJE
JEDNOGPOJEDNOGSLOVATEDODAJUCIIDEJUOKLJUCEVIMASTVORENISU
MODERNIKONCEPTIPOLIALFABETSKIHSUPSTITUCIJSKIHSIFRI.

Uz to, neka je VIGENERE *ključ za šifriranje. Zapisivanjem ključa koji se ponavlja iznad otvorenog teksta, dobije se:*

VIGENEREVIGENEREVIGENEREVIGENEREVIGENEREVIGENEREVIGENEREV
POLIALFABETSKASUPSTITUCIJSKASIFRASVAKAJESIFRAKOJASEBAZIRA

IGENEREVIGENEREVIGENEREVIGENEREVIGENEREVIGENEREVIGENEREVI
NASUPSTITUCIJIKORISTECIVISEALFABETANAJPOZNATIJATAKVASIFRA

GENEREVIGENEREVIGENEREVIGENEREVIGENEREVIGENEREVIGENEREVI
POVIJESNOJEPRIPISANAKRIVOJOSOBIATAKOODREDENANOMENKLATURA

GENEREVIGENEREVIGENEREVIGENEREVIGENEREVIGENEREVIGENEREV
OSTALAJEDODANASKOMBINIRAJUCIMIJESANEALFABETEISIFRIRANJE

IGENEREVIGENEREVIGENEREVIGENEREVIGENEREVIGENEREVIGENERE
JEDNOGPOJEDNOGSLOVATEDODAJUCIIDEJUOKLJUCEVIMASTVORENISU

VIGENEREVIGENEREVIGENEREVIGENEREVIGENEREVIGENEREVI
MODERNIKONCEPTIPOLIALFABETSKIHSUPSTITUCIJSKIHSIFRI

Koristeći navedene parove slova otvorenog teksta i ključa i preslikavajući ih u tabuli recti, dio otvorenog teksta POLIALFABETSKA *šifrira se s* KWRMNPWEWMZWXE. *Tablica 4 prikazuje način šifriranja navedenog dijela otvorenog teksta, a analogno se šifrira i ostatak istog. Krajnji rezultat sljedeći je šifrat:*

KWRMNPWEWMZWXEJYKAZMGYTMEAQEFMWVVABEXEAINQLVNOFNVAKFNDZVV
VGWHTJXDBAGVNZOJZOWGITMQQYINPWEWMZEAEATJHTEGMAEOIQZNWZJMI
VSIMAINVUNRTIMKQYEAEBVDDUNBWFFDIZEXSFHMMJIAEESHMTOYEKYMI
UWGECEEMJSQEEENSUQOMEMMIPYPMDMEMYEAIRPAIHIGIZWDNXMEEENZ
RKHASXTJRKHASXWGWBEGIUSYIPYPMZHZRASXPAYXMBMZEJXQWXIAMJY
HWJIERZOJVIICXZTJTOEYJRFZBYOVLJYKAZMGYTMEAQMUWZJMQ.

U *Tablici 4* vidljivo je kako se zaista koriste samo alfabeti (stupci) koji pripadaju slovima korištenog ključa – u ovom slučaju, VIGENERE. Prema tome, zanimljivo

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

Tablica 4: *Šifriranje otvorenog teksta* `POLIALFABETSKA` *Vigenèrovom šifrom koristeći* `VIGENERE` *kao ključ*

je primijetiti kako se Trithemiusova šifra može interpretirati kao Vigenèrova šifra s ključem `ABCDEFGHIJKLMNOPQRSTUVWXYZ` (cijelim osnovnim alfabetom engleskog jezika).

Dešifriranje, uz poznavanje ključa i šifrata, obrnuti je postupak takav da se iznad šifrata napiše ključ koji se ponavlja za cijeli šifrat. Za svaki par slova šifrata i ključa u stupcu koji odgovara slovu ključa nađe se slovo koje odgovara slovu šifrata. Potom se iščita slovo retka u kojem se nađeno slovo šifrata nalazi i upravo je ono pripadajuće slovo otvorenog teksta. Da bi se dobio cijeli otvoreni tekst, postupak se ponavlja na isti način za svaki par slova šifrata i ključa.

Prema [3], Vigenèrova šifra može se opisati i algebarski sljedećom definicijom:

Definicija 2. *Neka je m fiksan prirodan broj. Definiramo $\mathcal{P} = \mathcal{C} = \mathcal{K} = \mathbb{Z}_{26}$. Za ključ $K = (k_1, k_2, \ldots, k_m)$ definiramo funkcije šifriranja i dešifriranja:*

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

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

gdje nam $+_{26}$ *i* $-_{26}$ *označavaju operacije zbrajanja i oduzimanja modulo* 26.

Dakle, slova otvorenog teksta pomiču se za $k_1, k_2, \ldots, k_m$ mjesta u ovisnosti o tome na kojem se mjestu u otvorenom tekstu nalaze – odnosno, pomak ovisi o ostatku koji se dobije kada se pozicija slova podijeli s duljinom ključa m. Ovakvom metodom može se Vigenèrovu šifru interpretirati u smislu da su joj osnovni elementi otvorenog teksta i šifrata "blokovi" od po m slova unatoč tome što se šifriranje i dešifriranje provode slovo po slovo.

Glavna slabost Vigenèrove šifre ponavljanje je njenog ključa tijekom procesa šifriranja, pa se kriptoanaliza Vigenèrove šifre svodi na određivanje duljine ključa. Ukoliko osoba koja vrši napad nad šifratom odredi duljinu ključa, dešifriranje se svodi na primjenu jednostavne supstitucijske šifre (konkretno, Cezarove šifre). Dvije su najpoznatije metode pristupa određivanju duljine ključa – Kasiskijev i Friedmanov test.

Kasiskijev test uveo je Friedrich Kasiski 1863. godine – bio je to prvi objavljeni općeniti napad na šifre koje funkcioniraju poput Vigenèrove bez prethodnog znanja o šifratu ili početnom otvorenom tekstu. Iako je Kasiski bio prvi koji je objavio svoju metodu, postoje dokazi da su je i drugi bili svjesni i ranije. Tako je primjerice 1854. godine Charles Babbage prozvao John Hall Brock Thwaitesa, koji je tvrdio da je stvorio novu vrstu šifre, da je zapravo koristio Vigenèrovu šifru koju je samo malo modificirao. Thwaites ga je zbog toga izazvao da, temeljem otvorenog teksta iz Shakespearove knjige i njegovog šifrata, ukoliko se zaista radi o modificiranoj Vigenèrovoj šifri, odredi ključ šifriranja. Babbage je uskoro otkrio da su ključevi bile riječi "two" i "combined". Nikad nije objasnio korištenu metodu, no istraživanja njegovih bilješki pokazuju da je koristio metodu kasnije objavljenu kao Kasiskijeva metoda još od 1846. godine. Metoda se zasniva na činjenici da će dva identična segmenta otvorenog teksta biti šifrirana na isti način ukoliko se njihove početne pozicije razlikuju za neki višekratnik od m, gdje je m duljina ključa. U šifratu se traže parovi identičnih segmenata duljine barem 3, te (ako takvi postoje) zabilježavaju se udaljenosti između njihovih početnih položaja. Ako se na takav način dobiju udaljenosti $d_1, d_2, \ldots$, onda je razumna pretpostavka da duljina ključa m dijeli većinu d_i-ova. Nakon što se odredi m, dolazi se do slične situacije kao kod Cezarove šifre. Naime, ako se pogledaju samo ona slova koja su šifrirana pomakom za k_1 slova (a ako je poznat m, onda se zna i koja su to slova), onda su ona šifrirana

običnom Cezarovom šifrom. Međutim, situacija je ipak nešto teža nego kod obične Cezarove šifre jer to ovdje nisu uzastopna slova u otvorenom tekstu, pa se njihovim dešifriranjem ne dobiva smisleni tekst. Zbog toga je značajna još jedna metoda za razbijanje Vigenèrove šifre.

Friedmanov test za određivanje duljine ključa koristi tzv. indeks koincidencije. Taj pojam uveo je William Friedman 1920. godine u knjizi "Indeks koincidencije i njegove primjene u kriptografiji", a test mjeri nejednakost frekvencija slova šifrata kako bi se izvršio uspješan napad na šifrat. Vrijedi sljedeća definicija.

Definicija 3. *Neka je $x = x_1, x_2, \ldots, x_n$ 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 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 odabira dvaput i-tog slova. Dakle, vrijedi sljedeća formula:*

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

Neka x predstavlja neki tekst na hrvatskom jeziku i neka su očekivane vjerojatnosti pojavljivanja slova `A,B,...,Z` u hrvatskom jeziku redom $p_0, p_1, \ldots, p_{25}$ (vjerojatnosti navedene u *Uvodu* ovog rada). Ako je n dovoljno velik, za očekivati je da će vrijediti:

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

jer je vjerojatnost da su oba slova `A` jednaka $p_0^2 \approx 0.115^2 = 0.013225$, oba slova `B` jednaka $p_1^2 \approx 0.015^2 = 0.000225$, oba slova `C` jednaka $p_2^2 \approx 0.028^2 = 0.000784$, i tako dalje.

Neka je dodatno šifrat $y = y_1 y_2 \ldots y_n$ dobiven šifriranjem Vigenèrovom šifrom i neka je rastavljen na m podnizova $z_1, z_2, \ldots, z_m$ tako da se y napiše, po stupcima, u matricu dimenzija $m \times (n/m)$. Ako m ne dijeli n, y se može nadopuniti na proizvoljan način ili je moguće promatrati "krnju matricu" s nepotpunim zadnjim stupcem. Retci ove matrice su upravo traženi podnizovi $z_1, z_2, \ldots, z_m$. Ako je m jednak duljini ključa, 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 svi indeksi koincidencije $I_c(z_i)$ trebali biti približno jednaki 0.064. S druge strane, ako m nije duljina ključa, onda će z_i-ovi izgledati kao većinom slučajni nizovi slova budući da su dobiveni pomacima pomoću različitih slova ključa. Treba primijetiti da za potpuno slučajni niz slova vrijedi:

$$I_c \approx 26 \cdot \left(\frac{1}{26}\right)^2 = \frac{1}{26} \approx 0.038.$$

Ove dvije vrijednosti, $k_p = 0.064$ (za otvoreni tekst) i $k_r = 0.038$ (za nasumičan niz slova), dovoljno su daleko jedna od druge, pa će se najčešće na ovaj način moći odrediti točna duljina ključa (odnosno, potvrditi pretpostavka dobivena pomoću Kasiskijevog testa).

Postavlja se pitanje kako odrediti sam ključ ukoliko je poznata njegova duljina, pri čemu pomaže međusobni indeks koincidencije dvaju nizova definiran kako slijedi:

Definicija 4. *Neka su $x = x_1, x_2, \ldots, x_n$ i $y = y_1, y_2, \ldots, y_{n'}$ 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 vrijedi:*

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

Neka je m duljina ključa, $K = (k_1, k_2, \ldots, k_m)$ ključ i neka su podnizovi z_1, z_2, $\ldots$, z_m dobiveni iz šifrata kao prije. Potrebno je promotriti proizvoljno slovo u z_i i proizvoljno slovo u z_j i procijeniti vjerojatnost da su oba ova slova jednaka `A`. Prvo slovo `A` dobije se pomakom k_i, a drugo pomakom k_j. Vjerojatnost da se pomakom za k_i dobije slovo `A` približno je jednaka vjerojatnosti s kojom se u hrvatskom jeziku pojavljuje slovo čiji je numerički ekvivalent $-k_i \pmod{26}$. Dakle, vjerojatnost da su oba promatrana slova jednaka `A`, uz napomenu da su operacije u indeksima modulo 26, približno je jednaka $p_{-k_i} p_{-k_j}$, da su oba slova `B` približno je jednaka $p_{1-k_i} p_{1-k_j}$, i tako dalje. Dakle, vrijedi ocjena

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

odnosno, pomakom indeksa suma se ne mijenja. Ova ocjena ovisi samo o razlici $k_i - k_j \pmod{26}$ koja se naziva relativni pomak od z_i i z_j i označava s $q = k_i - k_j$.

Također, vrijedi

$$\sum_{h=0}^{25} p_h p_{h+q} = \sum_{h=0}^{25} p_h p_{h-q}$$

jer $h-q \pmod{26} = h-(26-q) \pmod{26} = h-26+q \pmod{26} = h+q \pmod{26}$, što znači da se za pomak q dobiva ista ocjena kao i za pomak $26-q$. Stoga je dovoljno promatrati pomake između 0 i 13. Za hrvatski jezik, ako je relativni pomak $q = 0$, onda je $MI_c = 0.064$. Za ostale $q \in \{1, \ldots, 13\}$ vrijednost od MI_c je između 0.031 i 0.044.

Uz pretpostavku da se fiksira niz z_i, potrebno je promotriti efekt šifriranja z_j sa slovima $\mathtt{A}, \mathtt{B}, \mathtt{C}, \ldots, \mathtt{Z}$, tj. pomakom za $0, 1, 2, \ldots, 25$ mjesta. Tako dobiveni nizovi neka su označeni sa $z_j^0, z_j^1, \ldots, z_j^{25}$. Za $g = 0, 1, \ldots, 25$ izračunava se indeks $MI_c(z_i, z_j^g)$ po formuli:

$$MI_c(z_i, z_j^g) = \frac{\sum_{i=0}^{25} f_i f_{i-g}}{nn'}.$$

Ako je $g \equiv -k_j \pmod{26}$, onda bi trebalo vrijediti $MI_c(z_i, z_j^g) \approx 0.064$; u protivnom bi trebao varirati između 0.031 i 0.044. Na ovaj način moguće je utvrditi relativne pomake bilo koja dva podniza z_i i z_j. Nakon što se to učini, ostaje samo 26 mogućih ključeva koji se mogu ispitati jedan po jedan. Međutim, malom modifikacijom ove metode do ključa je moguće doći efikasnije ukoliko je poznato na kojem je jeziku pisan otvoreni tekst. Umjesto međusobnog indeksa koincidencije nizova z_i i z_j^g tada bi se računao $MI_c(x, z_j^g)$ gdje je x niz koji odgovara tipičnom tekstu na jeziku otvorenog teksta. Uz pretpostavku da je otvoreni tekst pisan na hrvatskom jeziku, relativne frekvencije $\frac{f_i}{n}$ približno su jednake vrijednostima p_i, pa vrijedi:

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

Očekivanje je 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 bi se odredilo j-to slovo k_j ključa, za $0 \leq g \leq 25$ računa se:

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

Zatim se odredi l takav da je $M_l = \max\{M_g : 0 \leq g \leq 25\}$, te se stavi $l \equiv -k_j \pmod{26}$, odnosno $-k_j \equiv l \pmod{26}$.

Primjer 7. *Dešifrirajmo šifrat*

KWRMNPWEWMZWXEJYKAZMGYTMEAQEFMWVVABEXEAINQLVNOFNVAKFNDZVV
VGWHTJXDBAGVNZOJZOWGITMQQYINPWEWMZEAEATJHTEGMAEOIQZNWZJMI
VSIMAINVUNRTIMKQYEAEBVDDUNBWFFDIZEXSFHMMJIAEESHMTOYEKYMI
UWGECEEMJSQEEENSUQOMEMMIPYPMDMEMYEAIRPAIHIGIZWDNXMEEENZ
RKHASXTJRKHASXWGWBEGIUSYIPYPMZHZRASXPAYXMBMZEJXQWXIAMJY
HWJIERZOJVIICXZTJTOEYJRFZBYOVLJYKAZMGYTMEAQMUWZJMQ

dobiven Vigenèrovom šifrom iz otvorenog teksta na hrvatskom jeziku.

Rješenje:

Najprije treba odrediti duljinu ključne riječi, zbog čega se primjenjuje Kasiskijev test. Analizom frekvencije slova uočavaju se neki trigrami koji se ponavljaju u šifratu:

- `NPW` *na pozicijama 5 i 85, pa je njihov razmak:* $85 - 5 = 80 = 2^4 \cdot 5$*;*
- `WMZ` *na pozicijama 9 i 89, pa je njihov razmak:* $89 - 9 = 80 = 2^4 \cdot 5$*;*
- `YEA` *na pozicijama 131 i 203, pa je njihov razmak:* $203 - 131 = 72 = 2^3 \cdot 3^2$*;*
- `IPY` *na pozicijama 194 i 250, pa je njihov razmak:* $250 - 194 = 56 = 2^3 \cdot 7$*;*
- `ZOJ` *na pozicijama 71 i 287, pa je njihov razmak:* $287 - 71 = 216 = 2^3 \cdot 3^3$*;*
- `TME` *na pozicijama 23 i 319, pa je njihov razmak:* $319 - 23 = 296 = 2^3 \cdot 37$*;*
- `EAE` *na pozicijama 92 i 132, pa je njihov razmak:* $132 - 92 = 40 = 2^3 \cdot 5$*;*
- `ASX` *na pozicijama 229, 237 i 259, pa su njihovi razmaci:* $237 - 229 = 8 = 2^3$, $259 - 237 = 22 = 2 \cdot 11$, $259 - 229 = 30 = 2 \cdot 3 \cdot 5$.

Obzirom na navedene razmake, kako je 2^3 *dio većine njih, postoji sumnja da je duljina ključa* $m = 2^3 = 8$*. Nadalje, potrebno je provjeriti dobije li se i pomoću*

indeksa koincidencije isti zaključak. Podjelom našega šifrata na odgovarajući broj podnizova i računanjem indeksa koincidencije dobivamo:

$$m = 1 : 0.0496$$
$$m = 2 : 0.0475, 0.077$$
$$m = 3 : 0.0479, 0.0467, 0.0505$$
$$m = 4 : 0.0497, 0.0758, 0.0578, 0.0792$$
$$m = 5 : 0.0448, 0.0452, 0.0513, 0.0592, 0.0541$$
$$m = 6 : 0.0478, 0.0754, 0.0465, 0.0707, 0.0485, 0.0714$$
$$m = 7 : 0.055, 0.0527, 0.0453, 0.0481, 0.0407, 0.0527, 0.0444$$
$$m = 8 : 0.0581, 0.0883, 0.0476, 0.0963, 0.0756, 0.1012, 0.0793, 0.061.$$

Najbliža vrijednost ciljanoj 0.064 *postiže se za* $m = 8$*. Zaključak je da indeks koincidencije sugerira kako je ključ duljine* $m = 8$*, no ne potvrđuje to zasigurno jer niti jedna postignuta vrijednost nije točno* 0.064 *što može biti indikator da otvoreni tekst odnosno šifrat trebaju biti dulji kako bi primjena indeksa koincidencije dala točnije rezultate. Uz pretpostavku da zaista vrijedi* $m = 8$*, sljedeći je korak određivanje samog ključa koristeći međusobni indeks koincidencije dvaju nizova. Ukoliko se ispostavi da je pretpostavljen krivi* m*, otvoreni tekst koji će se dobiti dešifriranjem neće biti smislen. Dakle, podjelom se dobiju sljedeći podnizovi:*

$z_1 =$ `KWKEVNVVDJQWJOMNKDDMHMENMEADZJGYZXQHJJZKEM`
$z_2 =$ `WMAAAQAVBZQMHIIVQDIMMIMSIMINRRWIRMWWVTBAAQ`
$z_3 =$ `RZZQBLKGAOYZTQVUYUZJTUJUPYHXKKBPABXJIOYZQ`
$z_4 =$ `MWMEEVFWGWIEEZSNENEIOWSQYEIMHHEYSMIIIEOMM`
$z_5 =$ `NXGFXNNHVGNAGNIRABXAYGQOPAGEAAGPXZAECYVGU`
$z_6 =$ `PEYMEODTNIPEMWMTEWSEEEEMMIIESSIMPEMRXJLYW`
$z_7 =$ `WJTWAFZJZTWAAZAIBFFEKCEEDRZEXXUZAJJZZRJTZ`
$z_8 =$ `EYMVINVXOMETEJIMVFHSYEEMMPWNTWSHYXYOTFYMJ`.

Sada se za $j = 1, \ldots, 8$ *računaju vrijednosti* $M_0, \ldots, M_{25}$*. Primjerice, duljina podniza* z_1 *jednaka je* 42 *i za* $j = 1$ *dobiva se:*

$$M_0 = \frac{\sum_{i=0}^{25} p_i f_i'}{42} = \frac{p_0 f_0' + p_1 f_1' + \ldots + p_{25} f_{25}'}{42}$$
$$= \frac{0.115 \cdot 1 + 0.015 \cdot 0 + \ldots + 0.023 \cdot 3}{42} \approx 0.0392,$$

$$M_1 = \frac{\sum_{i=0}^{25} p_i f'_{i-1}}{42} = \frac{p_0 f'_{25} + p_1 f'_0 + \ldots + p_{25} f'_{24}}{42}$$
$$= \frac{0.115 \cdot 3 + 0.015 \cdot 1 + \ldots + 0.023 \cdot 1}{42} \approx 0.0472.$$

Analogno nastavimo dalje i za svaki $j = 1, \ldots, 8$ *odgovarajući* M_g*-ovi za* $g = 0, \ldots, 25$ *navedeni su u sljedećoj tablici:*

j	M_g
1	0.0392, 0.0472, 0.0339, 0.0293, 0.049, **0.0597**, 0.0326, 0.0344, 0.039, 0.0414, 0.0407, 0.0334, 0.0267, 0.0363, 0.0463, 0.0313, 0.0407, 0.0429, 0.039, 0.0312, 0.0315, 0.0339, 0.0463, 0.0406, 0.0345, 0.0379
2	0.0507, 0.0435, 0.0397, 0.0322, 0.0396, 0.0406, 0.0353, 0.0319, 0.0415, 0.0446, 0.0354, 0.0267, 0.0352, 0.0497, 0.0533, 0.0205, 0.0209, 0.0417, **0.0741**, 0.0345, 0.027, 0.0307, 0.0535, 0.0366, 0.0304, 0.0292
3	0.0342, 0.0409, 0.0387, 0.0406, 0.0365, 0.0405, 0.0362, 0.0332, 0.0282, 0.0408, 0.0505, 0.0409, 0.0337, 0.0324, 0.0422, 0.0428, 0.0424, 0.0343, 0.0375, 0.048, **0.0548**, 0.0377, 0.026, 0.0295, 0.0362, 0.0402
4	0.0513, 0.0377, 0.0389, 0.0262, 0.0502, 0.046, 0.0458, 0.0356, 0.0385, 0.0372, 0.0438, 0.0262, 0.0372, 0.0422, 0.0462, 0.028, 0.0368, 0.0332, 0.0479, 0.0227, 0.0235, 0.0377, **0.076**, 0.0317, 0.0275, 0.0309
5	0.0465, 0.0288, 0.0445, 0.0405, 0.0456, 0.0362, 0.0369, 0.0381, 0.0466, 0.0348, 0.0288, 0.0422, 0.0384, **0.0578**, 0.0458, 0.036, 0.027, 0.0402, 0.028, 0.0362, 0.0498, 0.0401, 0.035, 0.0309, 0.0385, 0.0258
6	0.052, 0.0317, 0.0421, 0.0277, 0.0466, 0.042, 0.0433, 0.0354, 0.0358, 0.0368, 0.0431, 0.0369, 0.0276, 0.035, 0.0455, 0.0383, 0.0387, 0.0412, 0.0415, 0.022, 0.0231, 0.0369, **0.0753**, 0.0328, 0.0301, 0.0376
7	0.0456, 0.0425, 0.0232, 0.036, 0.0533, 0.0437, 0.0264, 0.0317, 0.0414, **0.0597**, 0.0437, 0.0387, 0.0361, 0.0382, 0.0422, 0.0453, 0.0324, 0.046, 0.0394, 0.0311, 0.0357, 0.05, 0.0343, 0.0204, 0.0245, 0.0376
8	0.0397, 0.0339, 0.0439, 0.0291, 0.0388, 0.0461, 0.0447, 0.04, 0.0347, 0.0338, 0.0381, 0.0351, 0.0324, 0.0403, 0.043, 0.0367, 0.0448, 0.0396, 0.0357, 0.0302, 0.0317, 0.046, **0.061**, 0.034, 0.0278, 0.0379

Tablica 5: *Tablica indeksa* M_g

Uočimo kako smo u Tablici 5 podebljali najveće vrijednosti indeksa M_g*, pa redom imamo:*

- *za* $j = 1$ *je* $l = 5$*, pa je* $k_1 = -5 \pmod{26} = 21$*;*
- *za* $j = 2$ *je* $l = 18$*, pa je* $k_2 = -18 \pmod{26} = 8$*;*

- *za* $j = 3$ *je* $l = 20$, *pa je* $k_3 = -20 \pmod{26} = 6$;
- *za* $j = 4$ *je* $l = 22$, *pa je* $k_4 = -22 \pmod{26} = 4$;
- *za* $j = 5$ *je* $l = 13$, *pa je* $k_5 = -13 \pmod{26} = 13$;
- *za* $j = 6$ *je* $l = 22$, *pa je* $k_6 = -22 \pmod{26} = 4$;
- *za* $j = 7$ *je* $l = 9$, *pa je* $k_7 = -9 \pmod{26} = 17$;
- *za* $j = 8$ *je* $l = 22$, *pa je* $k_8 = -22 \pmod{26} = 4$.

Prema dobivenim brojevima koristeći korespodenciju između slova i cijelih brojeva koja je objašnjena u Uvodu, zaključujemo da je ključ riječ VIGENERE. *Otvoreni tekst može se dobiti postupkom dešifriranja uz poznavanje ključa koristeći Vigenèrov kvadrat kako je ranije opisano (u stupcu se nađe slovo ključa, u Tablici 1 se za taj stupac nađe slovo šifrata te je rezultantno slovo jednako odgovarajućem retku). Primjerice, za slovo* V *ključa i slovo* K *šifrata dobije se slovo* P *otvorenog teksta. Analogno, dobivamo otvoreni tekst:*

POLIALFABETSKASUPSTITUCIJSKASIFRASVAKAJESIFRAKOJASEBAZIRA
NASUPSTITUCIJIKORISTECIVISEALFABETANAJPOZNATIJATAKVASIFRA
POVIJESNOJEPRIPISANAKRIVOJOSOBIATAKOODREDENANOMENKLATURA
OSTALAJEDODANASKOMBINIRAJUCIMIJESANEALFABETEISIFRIRANJE
JEDNOGPOJEDNOGSLOVATEDODAJUCIIDEJUOKLJUCEVIMASTVORENISU
MODERNIKONCEPTIPOLIALFABETSKIHSUPSTITUCIJSKIHSIFRI.

Dodavanjem razmaka, interpunkcijskih i dijakritičkih znakova otvoreni tekst glasi:

POLIALFABETSKA SUPSTITUCIJSKA ŠIFRA SVAKA JE ŠIFRA KOJA SE BAZIRA NA SUPSTITUCIJI KORISTEĆI VIŠE ALFABETA. NAJPOZNATIJA TAKVA ŠIFRA POVIJESNO JE PRIPISANA KRIVOJ OSOBI, A TAKO ODREĐENA NOMENKLATURA OSTALA JE DO DANAS. KOMBINIRAJUĆI MIJEŠANE ALFABETE I ŠIFRIRANJE JEDNOG PO JEDNOG SLOVA TE DODAJUĆI IDEJU O KLJUČEVIMA, STVORENI SU MODERNI KONCEPTI POLIALFABETSKIH SUPSTITUCIJSKIH ŠIFRI.

1.4 Beaufortova šifra

Postoji puno kriptosustava baziranih na Vigenèrovoj šifri. Jedan od najpoznatijih takvih izumio je Sir Francis Beaufort, irski časnik u Britanskoj kraljevskoj

ratnoj mornarici.

Slika 8: *Sir Francis Beaufort*[8]

Beaufortova šifra bazirana je, prema [6] i [7], na Beaufortovom kvadratu vidljivom u *Tablici 6* koji izgleda poput Vigenèrovog kvadrata (*Tablica 1*) sa sljedećom bitnom razlikom: retci u Beaufortovom kvadratu su retci iz Vigenèrovog kvadrata ali je svaki redak napisan u obrnutom redoslijedu. Kao što su u Vigenèrovom kvadratu prvi redak i stupac identični onima koji služe kao indeksni redak i stupac (odnosno, "vanjski" redak i stupac kvadrata), tako su u Beaufortovom kvadratu to prvi redak i zadnji stupac. Koristeći Beaufortov kvadrat, šifriranje i dešifriranje svodi se na isti postupak preslikavanja kao i u Vigenèrovoj šifri:

- šifriranje: slovo šifrata nalazi se na presjeku retka Beaufortovog kvadrata koji je predstavljen slovom otvorenog teksta i stupca koji je predstavljen slovom ključa;
- dešifriranje: u stupcu koji odgovara slovu ključa nađe se slovo koje odgovara slovu šifrata; redak u kojem se nalazi to slovo šifrata upravo je pripadajuće slovo otvorenog teksta.

Primjer 8. *Šifrirajmo otvoreni tekst*

```
POLIALFABETSKA SUPSTITUCIJSKA ŠIFRA SVAKA JE ŠIFRA
KOJA SE BAZIRA NA SUPSTITUCIJI KORISTEĆI VIŠE ALFABETA
```

[8] 27. svibnja 1774. – 17. prosinca 1857.; Izvor: Wikipedia

koristeći Beaufortovu šifru.

Rješenje:

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

Tablica 6: *Beaufortov kvadrat*

Navedeni otvoreni tekst pripremljen za šifriranje Beaufortovom šifrom izgleda kako slijedi:

POLIALFABETSKASUPSTITUCIJSKASIFRASVAKAJESIFRAKOJA
SEBAZIRANASUPSTITUCIJIKORISTECIVISEALFABETA.

Tekst je očišćen od dijakritičkih znakova. Uz to, neka je BEAUFORT *ključ za šifriranje. Zapiše li se ključ s ponavljanjem iznad otvorenog teksta, dobije se:*

BEAUFORTBEAUFORTBEAUFORTBEAUFORTBEAUFORTBEAUFORTB
POLIALFABETSKASUPSTITUCIJSKASIFRASVAKAJESIFRAKOJA

EAUFORTEAUFORTEAUFORTEAUFORTEAUFORTEAUFORTB
SEBAZIRANASUPSTITUCIJIKORISTECIVISEALFABETA

U Tablici 7 prikazano je šifriranje dijela otvorenog teksta POLIALFABETSKA *primjenom Beaufortove šifre. Dobiva se dio šifrata* QSLCFZWTCITMPO*. Analogno nasta-*

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

Tablica 7: *Šifriranje dijela otvorenog teksta*

vimo dalje i slijedi šifrat:

```
QSLCFZWTCITMPOJNQWTCYITBKWKUXWWKBWVUPOAXTMFLFY
FCBWEVFNZKBRAMZDJMJXUWNXZDPVIMYSTBWMSYFZWTCITU.
```

Kriptoanaliza Beaufortove šifre, odnosno napad na šifrat dobiven njome, izvodi se potpuno analogno kriptoanalizi Vigenèrove šifre koristeći Kasiskijev i Friedmanov test kao što je ilustrirano u *Primjeru 7.*

1.5 Playfairova šifra

Sir Charles Wheatstone, engleski znanstvenik i izumitelj, imao je iznimno kreativan um – konstruirao je električni telegraf prije Morsea, izumio je vrstu male ručne harmonike (engl. *concertina*), proučavao je podvodnu telegrafiju, napisao nekoliko znanstvenih radova u području akustike, proveo brojne pokuse sa strujom, popularizirao metodu iznimno preciznog mjerenja otpora struje koja se i danas koristi. Službeno je bio profesor eksperimentalne filozofije King's College sveučilišta u Londonu, no bio je toliko sramežljiv da je rijetko predavao.

Slika 9: *Sir Charles Wheatstone i Barun Lyon Playfair*[9]

Još jedan njegov izum bila je šifra u telegrafiji koja nosi ime njegovog prijatelja baruna Lyon Playfaira od St. Andrewsa. Playfair je bio znanstvenik i javna ličnost Viktorijanskog doba u Engleskoj. Prema [4], na večeri u siječnju 1854. godine kojoj su prisustvovali princ Albert, muž kraljice Ujedinjenog Kraljevstva Viktorije i tadašnji državni tajnik te budući premijer Lord Palmerston, a čiji je domaćin bio predsjednik vladajućeg vijeća Lord Granville, Playfair je demonstrirao nešto što je nazočnima predstavio kao "Wheatstonova novootkrivena simetrična šifra". Nekoliko dana kasnije kada je Playfair bio u Dublinu primio je dva kratka pisma od Palmerstona i Granvilla u kojima su se nalazili šifrati dobiveni koristeći objašnjeni im sustav, što je pokazalo da su ga obojica brzo svladala.

Sam kriptosustav je prvi u povijesti koji je bio bigramski – rezultat šifriranja dva uzastopna slova ovisi o oba slova, odnosno o njihovoj kombinaciji. Wheatstone je shvatio da šifra, objašnjena u nastavku, jednako dobro može funkcionirati koristeći pravokutnik kao što može koristeći kvadrat, no s vremenom su svi koristili samo kvadrat. Upravo taj kvadrat, odnosno 5×5 matrica slova, ključna je za za šifriranje i dešifriranje. Prema [1], postoje dvije njezine varijante:

- trivijalna varijanta, odnosno ona u kojoj nema ključa; u tom slučaju matrica slova izgleda kako slijedi:

[9] 6. veljače 1802. – 19. listopada 1875.; Izvor: British photographic history
18. studenog 1873. – 17. veljače 1874.; Izvor: Wikimedia Commons

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

- permutirana matrica slova pri čemu je permutacija bazirana na ključu ili nekoj frazi koja se dobije tako da se u matricu upisuju slova iz ključa ili fraze bez duplikata te se ostatak matrice, ukoliko nije zastupljeno svih 26 slova, popunjava nedostajućim slovima prema abecednom redu; tako primjerice, ako je ključ `PLAYFAIR`, matrica slova izgleda kako slijedi:

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

Ukoliko se otvoreni tekst šifrira Playfairovom šifrom, obično se koristi druga varijanta jer je jednostavno sigurnija. Budući da u matricu stane 25 slova, ako je otvoreni tekst pisan engleskim jezikom, slova `I` i `J` se poistovjećuju odnosno šifriraju jednako. Također, prema [3], ukoliko je otvoreni tekst na hrvatskom jeziku, poistovjećuju se slova `V` i `W` da se izbjegnu mogući neporazumi kod dešifriranja.

Šifriranje se vrši tako da se najprije otvoreni tekst podijeli na blokove od po dva slova. Ukoliko se neki od blokova sastoji od jednakih slova, između njih se doda primjerice slovo `X`. Također, ukoliko se tim postupkom dobije neparna duljina teksta, na kraju se dodaje slovo `X` kako bi se i zadnji blok sastojao od dva slova. Nadalje, ovisno o položaju slova u matrici, kod šifriranja bloka od dva slova mogu nastupiti sljedeća tri slučaja:

- slova se nalaze u istom retku – zamjenjuju se slovima koja se nalaze za jedno mjesto udesno, ciklički, tj. iza slova u zadnjem stupcu dolazi slovo iz prvog stupca koje pripada istom retku; primjerice, za ranije navedenu matricu slova dobivenu ključem `PLAYFAIR` imamo preslikavanja `KG` $\mapsto$ `MH`, `YF` $\mapsto$ `FP`, `ZU` $\mapsto$ `UV`;

- slova se nalaze u istom stupcu – zamjenjuju se slovima koja se nalaze za jedno mjesto ispod, ciklički, tj. iza slova u zadnjem retku dolazi slovo iz prvog retka koje pripada istom stupcu; primjerice, za ranije navedenu matricu slova dobivenu ključem PLAYFAIR dobiva se SC $\mapsto$ XK, RV $\mapsto$ GL, VL $\mapsto$ LR;

- slova se ne nalaze niti u istom retku niti u istom stupcu – zamjenjuju se slovima koja čine preostala dva vrha pravokutnika kojeg tvore slova polaznog bloka pri čemu je redoslijed određen tako da najprije ide ono slovo koje se nalazi u istom retku kao prvo slovo u polaznom bloku; primjerice (za ranije navedenu matricu slova dobivenu ključem PLAYFAIR): IQ $\mapsto$ BN, CO $\mapsto$ RS, DS $\mapsto$ CT.

Primjer 9. *Šifrirajmo otvoreni tekst*

POLIALFABETSKA SUPSTITUCIJSKA ŠIFRA SVAKA JE ŠIFRA
KOJA SE BAZIRA NA SUPSTITUCIJI KORISTEĆI VIŠE ALFABETA

koristeći Playfairovu šifru.

Rješenje:

Navedeni otvoreni tekst pripremljen za šifriranje Playfairovom šifrom izgleda kako slijedi:

PO LI AL FA BE TS KA SU PS TI TU CI JS KA SI
FR AS VA KA JE SI FR AK OJ AS EB AZ IR AN AS UP
ST IT UC IX JX IK OR IS TE CI VI SE AL FA BE TA.

Tekst je očišćen od dijakritičkih znakova i obzirom da se u matrici slova I *i* J *poistovjećuju, zbog riječi "supstituciji" bilo je potrebno ubaciti slova* X*. Uz to, neka je* PLAYFAIR *ključ za šifriranje pa matrica slova izgleda kako slijedi:*

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

Temeljem otvorenog teksta pripremljenog za šifriranje i navedene matrica slova, vrijedi: PO $\mapsto$ LN, LI $\mapsto$ PR, AL $\mapsto$ YA, FA $\mapsto$ PY, BE $\mapsto$ IH, ...

Konačno, dobiveni šifrat je

LNPRYAPYIHNTHYNXYNNDNZDRCNHYNCLDYQWLHYENNCLDYHNR
YQHIFWRBPQYQPITNDNXICUCUCEVGCNNMDRURNKYAPYIHQF.

Dešifriranje se vrši kao obrnuti postupak šifriranju:

- ako se slova nalaze u istom retku – zamjenjuju se slovima koja se nalaze za jedno mjesto ulijevo, ciklički, tj. iza slova u prvom stupcu dolazi slovo iz zadnjeg stupca koje pripada istom retku;

- ako se slova nalaze u istom stupcu – zamjenjuju se slovima koja se nalaze za jedno mjesto iznad, ciklički, tj. iza slova u prvom retku dolazi slovo iz zadnjeg retka koje pripada istom stupcu;

- ako se slova ne nalaze niti u istom retku niti u istom stupcu – kao i kod šifriranja, zamjenjuju se slovima koja čine preostala dva vrha pravokutnika kojeg tvore slova polaznog bloka pri čemu je redoslijed određen tako da najprije ide ono slovo koje se nalazi u istom retku kao prvo slovo u polaznom bloku.

Postupak se analogno provodi za cijeli šifrat.

Primjer 10. *Dešifrirajmo šifrat*

LNPRYAPYIHNTHYNXYNNDNZDRCNHYNCLDYQWLHYENNCLDYHNR
YQHIFWRBPQYQPITNDNXICUCUCEVGCNNMDRURNKYAPYIHQF

dobiven Playfairovom šifrom s ključem PLAYFAIR *iz otvorenog teksta na hrvatskom jeziku.*

Rješenje:

Prvi korak priprema je šifrata za dešifriranje, pa tako podjelom šifrata u blokove dobivamo:

LN PR YA PY IH NT HY NX YN ND NZ DR CN HY NC LD
YQ WL HY EN NC LD YH NR YQ HI FW RB PQ YQ PI TN
DN XI CU CU CE VG CN NM DR UR NK YA PY IH QF.

Obzirom da je PLAYFAIR *ključ za šifriranje, matrica slova izgleda kako slijedi:*

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

Temeljem šifrata pripremljenog za dešifriranje i navedene matrice slova, vrijedi: LN $\mapsto$ PO, PR $\mapsto$ LI, YA $\mapsto$ AL, PY $\mapsto$ FA, IH $\mapsto$ BE, ...

Konačno, dobiveni otvoreni tekst je

PO LI AL FA BE TS KA SU PS TI TU CI JS KA SI
FR AS VA KA JE SI FR AK OJ AS EB AZ IR AN AS UP
ST IT UC IX JX IK OR IS TE CI VI SE AL FA BE TA.

Dodavanjem dijakritičkih znakova i izbacivanjem slova X *koji su dodani radi postupka šifriranja, dobiveni otvoreni tekst je*

POLIALFABETSKA SUPSTITUCIJSKA ŠIFRA SVAKA JE ŠIFRA
KOJA SE BAZIRA NA SUPSTITUCIJI KORISTEĆI VIŠE ALFABETA.

Ova šifra ima nekoliko značajnih prednosti nad ostalima u tom dobu. Bigramska je pa se u šifratu izgube jednoslovne riječi poput "a" koje utječu na frekvencije i na pola se smanjuje broj elemenata dostupan frekvencijskoj analizi – otvoreni tekst od 100 slova imat će 50 bigrama. Štoviše, broj bigrama puno je veći od broja individualnih slova (za 26 slova postoji 676 bigrama) te su njihove frekvencije ujednačenije od frekvencija slova. Iz ovih razloga, dugo vremena se smatrala sigurnom, čak i neprobojnom. Ipak, analiza frekvencije bigrama kod dugih šifrata dobiva na točnosti pa za takve tekstove ova šifra postaje nesigurnom i ranjiva je na napad.

Metoda vjerojatne riječi

Ukoliko se radi o kraćem šifratu, napad na njega može se, prema [3] i [7], napraviti koristeći tzv. metodu vjerojatne riječi. Metoda se sastoji u tome da se napravi lista riječi ili fraza za koje se pretpostavlja da se nalaze u otvorenom tekstu, te da se u šifratu pronađe segment čija se struktura podudara sa strukturom vjerojatne riječi – ponavljanje bigrama, određeni razmak među njima. Kod rastavljanja vjerojatne riječi ili fraze na bigrame treba uzeti u obzir sve mogućnosti u ovisnosti o tome gdje

se taj tekst može nalaziti unutar poruke. Ovakav napad je često vrlo efikasan jer, budući da je poznat šifrat, može se pretpostaviti da je već poduzeta uspješna akcija presretanja poruke pa nije nerealno za pretpostaviti da se naslućuje i nešto o njezinom mogućem sadržaju. Također, često su poznate neke informacije o strukturi poruke poput zaglavlja, kome je naslovljena, tko ju je potpisao i slično. U praksi se ovakav napad sprječava tako da se vjerojatne riječi najprije "kodiraju" – zamijene nekim drugim riječima ili kombinacijama slova koje ne nalikuju međusobno jedna na drugu unatoč tome što su vjerojatne riječi potencijalno vrlo slične – a tek nakon toga šifriraju.

Primjer 11. *Dešifrirajmo šifrat*

LNPRYAPYIHNTHYNXYNNDNZDRCNHYNCLDYQWLHYENNCLDYHN
RYQHIFWRBPQYQPITNDNXICUCUCEVGCNNMDRURNKYAPYIHQF

dobiven Playfairovom šifrom iz otvorenog teksta na hrvatskom jeziku.

Rješenje:

Za potrebe primjera, pretpostavit će se da otvoreni tekst vjerojatno sadrži riječi POLIALFABETSKA SUPSTITUCIJSKA*, odnosno odvojeno na blokove:*

PO LI AL FA BE TS KA SU PS TI TU CI JS KA.

Uočava se ponavljanje bigrama KA *te razmak od 6 blokova između. Ukoliko se šifrat podijeli na blokove, on izgleda kako slijedi:*

LN PR YA PY IH NT HY NX YN ND NZ DR CN HY NC LD
YQ WL HY EN NC LD YH NR YQ HI FW RB PQ YQ PI TN
DN XI CU CU CE VG CN NM DR UR NK YA PY IH QF

U šifratu se najviše, i to tri puta, pojavljuju bigrami HY *i* YQ*. Broj blokova između pojavljivanja bigrama* HY *iznosi 6 i 4, a bigrama* YQ *7 i 4, što temeljem bigrama* HY *upućuje da bi* ***LN PR YA PY IH NT HY NX YN ND NZ DR CN HY*** *mogao biti šifrat od* ***PO LI AL FA BE TS KA SU PS TI TU CI JS KA****. Temeljem pretpostavki da vrijede šifriranja* PO $\mapsto$ LN*,* LI $\mapsto$ PR*,* AL $\mapsto$ YA*,* CI $\mapsto$ DR *i* FA $\mapsto$ PY*, može se početi konstruirati matrica slova do na permutaciju redaka ili stupaca:*

P	L	A	Y	F
IJ	R	_	C	D
N	O	_	_	_

Ovakva matrica vrijedi uz pretpostavku da PO *i* LN *čine pravokutnik. Kako su onda slova* P *i* L *u istom retku, pretpostavlja se da* LI *i* PR *također čine pravokutnik. Nadalje, zbog pojavljivanja slova* A *u* AL $\mapsto$ YA *pretpostavljamo da su slova* L *i* Y *u istom retku. Također, iz toga da su* I *i* R *u istom retku slijedi da su zbog* CI $\mapsto$ DR *slova* C *i* D *također elementi tog retka – a nalaze se na njegovom kraju. Posljednje, zbog onoga što je do sada popunjeno, pogleda li se* FA $\mapsto$ PY*, očito je da su sva navedena slova dio istog retka pa se slovo* F *dodaje na njegov kraj.*

Kako je poznato da se radi o šifratu koji je šifriran Playfairovom šifrom, te kako su slova P, L, A, Y, F, I, R *iz različitih dijelova abecede, jasno je da je taj redak dio ključa i da se radi o prvom retku matrice slova. Obzirom da se nakon njih slova pojavljuju abecednim redom, pretpostavlja se kako je ključ* PLAYFAIR *te da cijela matrica slova izgleda kako slijedi:*

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

Temeljem navedene matrice, korištenjem opisanog postupka dešifriranja, vrijedi: LN $\mapsto$ PO*,* PR $\mapsto$ LI*,* YA $\mapsto$ AL*,* PY $\mapsto$ FA*,* IH $\mapsto$ BE*, ...*

Konačno, cijeli otvoreni tekst dodavanjem dijakritičkih znakova, zamjenom I *sa* J *gdje je to potrebno i izbacivanjem nepotrebnih slova* X *glasi:*

POLIALFABETSKA SUPSTITUCIJSKA ŠIFRA SVAKA JE ŠIFRA
KOJA SE BAZIRA NA SUPSTITUCIJI KORISTEĆI VIŠE ALFABETA.

Nastavno na Playfairovo dobivanje šifriranih pisama od Palmerstona i Granvilla, prema [4], Wheatstone i Playfair su objasnili ovaj kriptosustav visokom dužnosniku Ujedinjenog Kraljevstva zaduženom za vanjske poslove ističući njegovu tadašnju najveću prednost – da šifrati dva bloka od po dva slova koja imaju jedno slovo zajedničko ne nalikuju jedan drugome. Također, istakli su da se, kada se proces svlada, otvoreni tekst može šifrirati jako brzo i jednostavno. Kada je spomenuti visoki dužnosnik komentirao kako je sustav ipak prekompliciran, Wheatstone je predložio da tri od četiri nasumična dječaka iz obližnje osnovne škole može naučiti šifrirati ovim sustavom u 15 minuta, na što je visoki dužnosnik odvratio: *"To je*

vrlo lako moguće, ali nikad ne biste naučili dužnosnike dodijeljene ambasadama u inozemstvu".

Kako je ova šifra bila praktična jer za šifriranje nije potreban neki dodatan uređaj ili alat, a ključ se brzo i lako mogao promijeniti, Playfair je na spomenutoj večeri 1854. godine sugerirao princu Albertu da se koristi kao kriptosustav za šifriranje na bojnom polju u nadolazećem Krimskom ratu. Ne postoje dokazi da se ovaj sustav u njemu zaista i koristio, ali postoje izvještaji da se koristio u Burskom ratu (još nazvan i Lažni rat).

Playfairova nesebična borba za kriptosustav njegova prijatelja Wheatstona nenamjerno je prouzročila da se ovaj kriptosustav popularizira kao Playfairov sve do danas čime je Wheatstone lišen svojeg kriptografskog nasljeđa.

1.6 Šifra četiri kvadrata

Félix-Marie Delastelle[10] bio je francuski kriptograf. Njegov otac, koji je bio zapovjednik broda, nestao je 1843. godine na moru. Delastelle je pohađao fakultet do 1860. godine, a nakon napuštanja obrazovanja radio je 40 godina u lokalnoj luci u skladištu carinske službe, te se svo to vrijeme amaterski bavio kriptografijom. Nakon odlaska u mirovinu 1900. godine unajmio je sobu u hotelu u kojoj je do svibnja 1901. napisao 150 stranica dugačku knjigu *Traité Élémentaire de Cryptographie*. Nakon što je dobio vijest o iznenadnoj smrti svoga brata i sam je umro u travnju 1902. godine, a njegova knjiga izdana je tri mjeseca nakon njegove smrti.

Delastellova knjiga je predstavila neke nove kriptosustave, uključujući šifru četiri kvadrata što je posebno zanimljivo jer se pretpostavlja da Delastelle nije bio svjestan Playfairove šifre. Šifra četiri kvadrata može se smatrati njenom varijantom. Također, fascinantno je da je jedan amaterski kriptograf svojom knjigom dao značajan doprinos kriptografiji u vrijeme kada su veća postignuća u tom području postizali profesionalni časnici, diplomati i akademici. D. Kahn u [5] opisuje jednu od šifri koje je Delastelle predstavio u svojoj knjizi kao "kriptosustav od visoke važnosti u kriptologiji".

Šifra četiri kvadrata, prema [2], bigramska je šifra koja koristi četiri kvadrata, odnosno 5×5 matrice slova, da bi se šifrirali i dešifrirali blokovi od po dva slova. Kvadrati su slični onima iz Playfairove šifre pri čemu su dva kvadrata trivijalno

[10] 2. siječnja 1840. – 2. travnja 1902.

generirana (bez ključne riječi – i to gornji lijevi i donji desni), dok su dva (gornji desni i donji lijevi) generirani koristeći dva različita ključa ili fraze.

Šifriranje se provodi podjelom otvorenog teksta na blokove od po dva slova, dodavanjem slova `X` na kraju ukoliko otvoreni tekst sadrži neparan broj slova i generiranjem četiri kvadrata kako je prethodno opisano – dva su trivijalna, a dva se generiraju poput kvadrata u Playfairovoj šifri koristeći ključeve ili fraze (opisano u *Poglavlju 1.5*). Kao i kod Playfairove šifre, slova `I` i `J` se poistovjećuju odnosno šifriraju jednako. Nadalje, za svaki se blok slova u gornjem lijevom kvadratu nalazi prvo slovo, u donjem desnom kvadratu drugo slovo, dok se rezultantni šifrat tvori iz preostala dva vrha pravokutnika kojeg tvore slova polaznog bloka – prvo slovo se uzima iz gornjeg desnog, a drugo iz donjeg lijevog kvadrata.

Primjer 12. *Šifrirajmo otvoreni tekst*

`POLIALFABETSKA SUPSTITUCIJSKA ŠIFRA SVAKA JE ŠIFRA`
`KOJA SE BAZIRA NA SUPSTITUCIJI KORISTEĆI VIŠE ALFABETA.`

koristeći šifru četiri kvadrata.

Rješenje:

Navedeni otvoreni tekst pripremljen za šifriranje šifrom četiri kvadrata izgleda kako slijedi:

`PO LI AL FA BE TS KA SU PS TI TU CI JS KA SI FR`
`AS VA KA JE SI FR AK OJ AS EB AZ IR AN AS UP`
`ST IT UC IJ IK OR IS TE CI VI SE AL FA BE TA.`

Tekst je očišćen od dijakritičkih znakova, a kako sadrži paran broj slova, na kraj nije potrebno dodavati slovo `X`*.*

Neka su ključevi za šifriranje `DELASTELLE` *i* `CETIRI`*. Matrice slova, odnosno četiri kvadrata, izgledaju kako slijedi:*

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

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

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

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

Temeljem otvorenog teksta pripremljenog za šifriranje i generiranih kvadrata, vrijedi: PO $\mapsto$ MN, LI $\mapsto$ MA, AL $\mapsto$ DH, FA $\mapsto$ TC, BE $\mapsto$ SE, ...

Dobivamo šifrat:

MNMADHTCSEQSTRUQKURFUSADCSTRRDBOLOVCTRGIRDBOSA
MFLOERSVBSLHLOUNRQFSQRFFGFISCSUIADYAUTDHTCSEOI.

Dešifriranje se, uz poznavanje ključeva, vrši kao obrnuti postupak šifriranju, odnosno za svaki blok slova iz šifrata se kao i kod šifriranja generiraju četiri kvadrata te se u gornjem desnom kvadratu pronalazi prvo slovo, a u donjem lijevom kvadratu drugo slovo šifrata. Rezultantni blok otvorenog teksta su slova koja čine preostala dva vrha pravokutnika – prvo se slovo uzima iz gornjeg lijevog, a drugo iz donjeg desnog kvadrata. Analogno se postupak provodi za cijeli šifrat.

Primjer 13. *Dešifrirajmo šifrat*

MNMADHTCSEQSTRUQKURFUSADCSTRRDBOLOVCTRGIRDBOSA
MFLOERSVBSLHLOUNRQFSQRFFGFISCSUIADYAUTDHTCSEOI

dobiven šifrom četiri kvadrata s ključevima DELASTELLE *i* CETIRI *iz otvorenog teksta na hrvatskom jeziku.*

Rješenje:

Prvi korak generiranje je četiri kvadrata temeljem danih ključeva koji izgledaju kako slijedi:

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

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

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

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

Sljedeći korak podjela je šifrata u blokove slova kako slijedi:

MN MA DH TC SE QS TR UQ KU RF US AD CS TR
RD BO LO VC TR GI RD BO SA MF LO ER SV BS LH LO
UN RQ FS QR FF GF IS CS UI AD YA UT DH TC SE OI.

Temeljem šifrata pripremljenog za dešifriranje i generiranih kvadrata, vrijedi: MN $\mapsto$ PO*,* MA $\mapsto$ LI*,* DH $\mapsto$ AL*,* TC $\mapsto$ FA*,* SE $\mapsto$ BE*, . . .*

Dobivamo otvoreni tekst:

PO LI AL FA BE TS KA SU PS TI TU CI JS KA SI FR
AS VA KA JE SI FR AK OJ AS EB AZ IR AN AS UP
ST IT UC IJ IK OR IS TE CI VI SE AL FA BE TA.

Odnosno, dodavanjem dijakritičkih znakova otvoreni tekst je

POLIALFABETSKA SUPSTITUCIJSKA ŠIFRA SVAKA JE ŠIFRA
KOJA SE BAZIRA NA SUPSTITUCIJI KORISTEĆI VIŠE ALFABETA.

Kriptoanaliza šifre četiri kvadrata slična je drugim bigramskim šiframa – ukoliko je šifrat dugačak, ranjiv je na analizu frekvencije bigrama. Ova šifra jača je od Playfairove šifre utoliko što može šifrirati blokove koji se sastoje od dva ista slova, te u šifratu može generirati blok od dva ista slova. Također, može šifrirati slovo otvorenog teksta u samog sebe – ovo svojstvo se naziva transparentnost i koristan je sigurnosni atribut ukoliko se ne pojavljuje prečesto – što se u Playfairovom kriptosustavu ne može dogoditi. Dodatno, za razliku od Playfaira gdje se inverzni

blokovi bigrama šifriraju u inverzne blokove bigrama – primjerice, bigrami `AB` i `BA` će šifriranjem Playfairovom šifrom postati bigrami oblika `XY` i `YX` pri čemu su `X` i `Y` neka dva slova – kod šifre četiri kvadrata se to neće dogoditi. Međutim, jedna od mana koju napad na ovaj kriptosustav može iskoristiti je da se za neke riječi dobiva isto slovo šifrata neovisno o ključu. Na primjer, za riječ "teret" otvorenog teksta, bez obzira na ključeve kojima su generirani gornji desni i donji lijevi kvadrat, prvo i treće slovo šifrata će biti isto jer se slova `T` i `R` nalaze u istom retku trivijalnog kvadrata i oba imaju slovo `E` u nasuprotnom kutu pravokutnika. Stoga, iako će slovo u donjem lijevom kutu pravokutnika biti različito, ono u gornjem desnom biti će jednako. Ista logika primijenjuje se i ukoliko drugo slovo tih bigrama nije jednako ali se nalazi u istom stupcu trivijalnog kvadrata. Dakle, ako su prva slova dva bloka šifrata jednaka, protivnik koji izvodi napad zna da prva slova bloka moraju biti u istom retku, a druga u istom stupcu u trivijalnom kvadratu – a kako je trivijalni kvadrat uvijek isti, uspješan napad se izvršava postupkom eliminacije mogućnosti. Jedan način za anulirati navedenu manu ovog kriptosustava je modificirati ga tako da se sva četiri kvadrata generiraju koristeći neke ključeve ili fraze. Na taj način se poredak slova u svim kvadratima permutira pa nije moguće pretpostaviti da su neka dva slova dio istog retka ili stupca kvadrata.

1.7 Šifra dva kvadrata

Šifra dva kvadrata, nazvana još i "dvostruki Playfair", nastala je nakon šifre četiri kvadrata – čija je varijanta – radi bržeg i jednostavnijeg šifriranja i dešifriranja uz zadržavanje više razine sigurnosti od Playfairove šifre. Bigramska je šifra koja koristi dva kvadrata, odnosno 5×5 matrice slova, koje se generiraju koristeći ključeve ili fraze analogno kvadratu u Playfairovoj šifri odnosno gornjem desnom i donjem lijevom kvadratu u šifri četiri kvadrata.

Šifriranje se provodi podjelom otvorenog teksta na blokove od po dva slova, dodavanjem slova `X` na kraju ukoliko otvoreni tekst sadrži neparan broj slova i generiranjem dva kvadrata kako je opisano koristeći ključeve ili fraze. Postoje dvije varijante ove šifre ovisno o poziciji kvadrata – jedan se kvadrat može nalaziti ispod drugoga ili pored njega. Rezultirajući šifrat ovisi o odabiru odgovarajuće varijante šifre. Kao i kod šifre četiri kvadrata, slova `I` i `J` se poistovjećuju odnosno šifriraju jednako. Svako se slovo otvorenog teksta može šifrirati u samog sebe, a u šifratu se može generirati blok od dva ista slova – što su sve prednosti zbog kojih je šifra

dva kvadrata sigurnija od Playfairove šifre. Nadalje, za svaki se blok slova u gornjem/lijevom kvadratu nalazi prvo, a u donjem/desnom kvadratu drugo slovo, dok se rezultantni šifrat tvori iz preostala dva vrha pravokutnika kojeg tvore slova polaznog bloka – prvo se slovo uzima iz gornjeg/lijevog, a drugo iz donjeg/desnog kvadrata.

Primjer 14. *Šifrirajmo otvoreni tekst*

POLIALFABETSKA SUPSTITUCIJSKA ŠIFRA SVAKA JE ŠIFRA
KOJA SE BAZIRA NA SUPSTITUCIJI KORISTEĆI VIŠE ALFABETA

koristeći šifru dva kvadrata.

Rješenje:

Navedeni otvoreni tekst pripremljen za šifriranje šifrom dva kvadrata izgleda kako slijedi:

PO LI AL FA BE TS KA SU PS TI TU CI JS KA SI FR
AS VA KA JE SI FR AK OJ AS EB AZ IR AN AS UP
ST IT UC IJ IK OR IS TE CI VI SE AL FA BE TA.

Tekst je očišćen od dijakritičkih znakova, a kako sadrži paran broj slova, na kraj nije potrebno dodavati slovo X*. Neka su ključevi za šifriranje* DVA *i* KVADRATA*. Matrice slova, odnosno dva kvadrata, ovisno o varijanti šifre izgledaju kako slijedi:*

- *ako se jedan kvadrat nalazi ispod drugoga:*

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

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

- *ako se jedan kvadrat nalazi pored drugoga:*

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

Temeljem otvorenog teksta pripremljenog za šifriranje i generiranih kvadrata, ovisno o varijanti šifre, vrijedi:

- *ako se jedan kvadrat nalazi ispod drugoga:*
  PO $\mapsto$ QN, LI $\mapsto$ MH, AL $\mapsto$ BI, FA $\mapsto$ GV, BE $\mapsto$ BE, ...

  Konačno, dobivamo šifrat:

  QNMHBIGVBETSMKPYTNRMPZAMISMKRLIVCPAVMKHFRLIVDA
  MMCPFTCXIRDPCPXNPEEFXTGMERORISSFAMAHSEBIGVBERR.

- *ako se jedan kvadrat nalazi pored drugoga:*
  PO $\mapsto$ PO, LI $\mapsto$ LI, AL $\mapsto$ MD, FA $\mapsto$ VC, BE $\mapsto$ HD, ...

  Konačno, dobivamo šifrat:

  POLIMDVCHDTSDIYNPSOPZNOATFDINPVFRRVADIIENPVFAK
  OIRREBXRCFRKRRPXHNITEXOCCTCMTFIQOALAHQMDVCHDCP.

Dešifriranje se, uz poznavanje ključeva, vrši identično šifriranju zbog simetrične naravi ove šifre.

Primjer 15. *Dešifrirajmo šifrat*

POLIMDVCHDTSDIYNPSOPZNOATFDINPVFRRVADIIENPVFAK
OIRREBXRCFRKRRPXHNITEXOCCTCMTFIQOALAHQMDVCHDCP

dobiven šifrom dva kvadrata s ključevima DVA *i* KVADRATA *iz otvorenog teksta na hrvatskom jeziku.*

Rješenje:

Prvi korak generiranje je dva kvadrata temeljem danih ključeva i ovisno o varijanti šifre kako slijedi:

- *ako se jedan kvadrat nalazi ispod drugoga:*

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

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

- *ako se jedan kvadrat nalazi pored drugoga:*

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

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

Sljedeći korak podjela je šifrata u blokove slova kako slijedi:

PO LI MD VC HD TS DI YN PS OP ZN OA TF DI NP VF
RR VA DI IE NP VF AK OI RR EB XR CF RK RR PX
HN IT EX OC CT CM TF IQ OA LA HQ MD VC HD CP.

Temeljem šifrata pripremljenog za dešifriranje i generiranih kvadrata, ovisno o varijanti šifre, vrijedi:

- *ako se jedan kvadrat nalazi ispod drugoga:*
  PO $\mapsto$ QN, LI $\mapsto$ MH, MD $\mapsto$ NA, VC $\mapsto$ AB, HD $\mapsto$ HD, ...

Konačno, dobivamo otvoreni tekst:

QNMHNAABHDTSAGUQTNMSUSMRTFAGMQCBTAAVAGHFMQCBDA
MMTAFTZACFPATARUEQEFGUMFDFCMTFHSMRMVHQNAABHDAS.

- *ako se jedan kvadrat nalazi pored drugoga:*
  PO $\mapsto$ PO, LI $\mapsto$ LI, MD $\mapsto$ AL, VC $\mapsto$ FA, HD $\mapsto$ BE, ...

  Konačno, dobivamo otvoreni tekst:

  POLIALFABETSKASUPSTITUCIISKASIFRASVAKAIESIFRAK
  OIASEBAZIRANASUPSTITUCIIIKORISTECIVISEALFABETA.

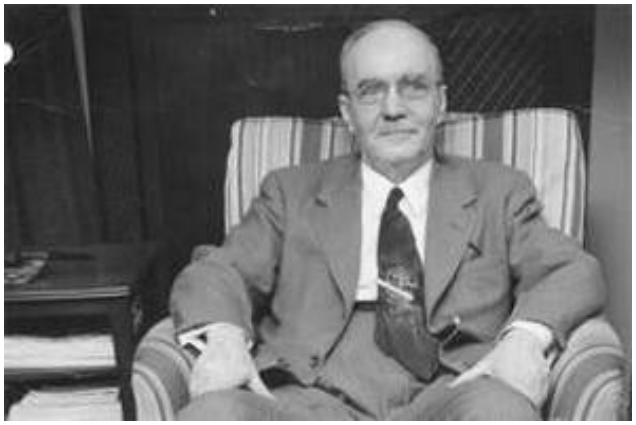
Kako dobiveni otvoreni tekst u varijanti šifre gdje se jedan kvadrat nalazi ispod drugoga nema smisla, zaključujemo da se šifrat koji dešifriramo dobio koristeći varijantu u kojoj se kvadrati nalaze jedan pored drugoga. Zbog toga, dodavanjem dijakritičkih znakova i zamjenom slova I *sa* J *gdje je to potrebno, otvoreni tekst je*

POLIALFABETSKA SUPSTITUCIJSKA ŠIFRA SVAKA JE ŠIFRA
KOJA SE BAZIRA NA SUPSTITUCIJI KORISTEĆI VIŠE ALFABETA.

Značajno je u *Primjeru 14* primijetiti kako su se prva dva bigrama, za varijantu kada je jedan kvadrat pored drugog, preslikali sami u sebe jer su se prvo i drugo slovo iz bloka našli u istom retku. Analogno se događa i u prvoj varijanti ove šifre, kada se jedan kvadrat nalazi ispod drugoga, ukoliko se prvo i drugo slovo iz bloka nađu u istom stupcu. Kako je navedeno u *Potpoglavlju 1.6*, to se svojstvo naziva transparentnost i uz umjereno pojavljivanje doprinosi sigurnosti kriptosustava. Međutim, mana šifre dva kvadrata je prečesto pojavljivanje transparentnosti, čak oko 20%. Protivnik koji napada ovaj kriptosustav može iskoristiti toliko visoku mogućnost pojave transparentnosti zbog kojih se, kada se sekvencijalno pojave, počinju nazirati dijelovi riječi. Temeljem njih protivnik može raditi na izgradnji kvadrata – matrica slova – odnosno pronalaska ključa i otkriti ostale bigrame šifrata. Osim toga, šifra dva kvadrata je, kao i ostale bigramske šifre, za dugačke šifrate ranjiva na analizu frekvencije bigrama.

1.8 Hillova šifra

Lester S. Hill, američki matematičar i profesor koji je predavao na nekoliko značajnih sveučilišta te se interesirao za primjene matematike u komunikacijskim tehnologijama, 1929. je godine izumio kriptosustav baziran na linearnoj algebri kod kojeg se m uzastopnih slova otvorenog teksta zamjenjuje s m slova u šifratu – što se naziva poligramskom šifrom. Ako broj slova otvorenog teksta nije djeljiv s m,



Slika 10: *Lester S. Hill*[11]

poruka se nadopunjuje da bi se mogla podijeliti u blokove od po m slova. Bila je to prva praktična poligramska šifra koja je mogla šifrirati više od tri slova odjednom.

Prema [3], elementi alfabeta su uređene m-torke elemenata iz $\mathbb{Z}_{26}$. Preciznije, to su elementi iz $M_{1,m}(\mathbb{Z}_{26})$ – matrice s elementima iz $\mathbb{Z}_{26}$ s jednim retkom i m stupaca. Prostor ključeva skup je svih invertibilnih kvadratnih $m \times m$ matrica s elementima iz $\mathbb{Z}_{26}$, tj. $GL(m, \mathbb{Z}_{26})$. Treba napomenuti da je matrica $A \in M_{m\times m}(\mathbb{Z}_{26})$ invertibilna ako i samo ako vrijedi $(det(A), 26) = 1$. Ključ može biti eksplicitno definiran matricom ili implicitno riječju odnosno frazom koja se pretvori u matricu. Ukoliko dana riječ ili fraza sadrži m^2 slova, ona je točno dugačka onoliko slova koliko je potrebno za generiranje matrice ključa. Ako je dulja, slova koja ostanu nakon m^2 se odbacuju, a ukoliko je kraća, nadopunjuje se proizvoljnim slovima.

Šifriranje se provodi tako da za dio otvorenog teksta $X \in M_{1,m}(\mathbb{Z}_{26})$ i ključ $K \in GL(m, \mathbb{Z}_{26})$, odgovarajući dio šifrata iznosi $e_K(X) = X \cdot K$. S druge strane, dešifriranje se provodi tako da za dio šifrata $Y \in M_{1,m}(\mathbb{Z}_{26})$ i ključ $K \in GL(m, \mathbb{Z}_{26})$, odgovarajući dio otvorenog teksta iznosi $d_K(Y) = Y \cdot K^{-1}$.

Primjer 16. *Šifrirajmo otvoreni tekst* `POLIALFABETSKA` *Hillovom šifrom s* $m = 3$ *ako je ključ fraza* `HILL POLIGRAMSKA SIFRA`.

Rješenje:

Navedeni otvoreni tekst, obzirom da je $m = 3$*, pripremljen za šifriranje Hillovom šifrom izgleda kako slijedi:*

[11] 18. siječnja 1891. – 9. siječnja 1961.; Izvor: Wikipedia

POL IAL FAB ETS KAX.

Kako duljina teksta nije djeljiva sa m*, dopunjen je slovom* X*. Za samo šifriranje potrebno je još svako slovo šifrata zamijeniti njegovim numeričkim ekvivalentom, odnosno pozicijom u alfabetu, pri čemu se* A *mijenja sa* 0*,* B *sa* 1*,* C *sa* 2*, . . . ,* Z *sa* 25*. Obzirom da je ključ zadan implicitno, potrebno je i u njemu svako slovo zamijeniti njegovom pozicijom u alfabetu. Također, obzirom da sadrži više od* 9 *slova, pri generiranju matrice ključa u obzir se uzima samo sljedeći dio zadanog ključa, a ostatak odbacuje:* HILLPOLIG*. Dakle, vrijedi:*

$$K = \begin{bmatrix} 7 & 8 & 11 \\ 11 & 15 & 14 \\ 11 & 8 & 6 \end{bmatrix}.$$

Matrica K *je invertibilna jer* $det(K) = -297 = 15 \pmod{26}$*, pa vrijedi:*

$$(det(K), 26) = (15, 26) = 1.$$

Šifriranje:

$$\texttt{POL}: \quad \begin{bmatrix} 15 & 14 & 11 \end{bmatrix} \begin{bmatrix} 7 & 8 & 11 \\ 11 & 15 & 14 \\ 11 & 8 & 6 \end{bmatrix} =_{26} \begin{bmatrix} 16 & 2 & 11 \end{bmatrix},$$

$$\texttt{IAL}: \quad \begin{bmatrix} 8 & 0 & 11 \end{bmatrix} \begin{bmatrix} 7 & 8 & 11 \\ 11 & 15 & 14 \\ 11 & 8 & 6 \end{bmatrix} =_{26} \begin{bmatrix} 21 & 22 & 24 \end{bmatrix},$$

$$\texttt{FAB}: \quad \begin{bmatrix} 5 & 0 & 1 \end{bmatrix} \begin{bmatrix} 7 & 8 & 11 \\ 11 & 15 & 14 \\ 11 & 8 & 6 \end{bmatrix} =_{26} \begin{bmatrix} 20 & 22 & 9 \end{bmatrix},$$

$$\texttt{ETS}: \quad \begin{bmatrix} 4 & 19 & 18 \end{bmatrix} \begin{bmatrix} 7 & 8 & 11 \\ 11 & 15 & 14 \\ 11 & 8 & 6 \end{bmatrix} =_{26} \begin{bmatrix} 19 & 19 & 2 \end{bmatrix},$$

$$\texttt{KAX}: \quad \begin{bmatrix} 10 & 0 & 23 \end{bmatrix} \begin{bmatrix} 7 & 8 & 11 \\ 11 & 15 & 14 \\ 11 & 8 & 6 \end{bmatrix} =_{26} \begin{bmatrix} 11 & 4 & 14 \end{bmatrix},$$

gdje nam $=_{26}$ *označava jednakost modulo* 26 *po svakom elementu matrice koja je rezultat umnoška matrica.*

Sada jednostavno brojevima pridružimo slova i dobivamo šifrat QCLVWYUWJTTC-LEO.

S druge strane, ukoliko je poznat ključ K, dešifriranje se provodi koristeći inverznu matricu K^{-1}. U ovom slučaju:

$$K^{-1} = \begin{bmatrix} 7 & 8 & 11 \\ 11 & 15 & 14 \\ 11 & 8 & 6 \end{bmatrix}^{-1} = \frac{1}{297} \cdot \begin{bmatrix} 22 & -40 & 53 \\ -88 & 79 & -23 \\ 77 & -32 & -17 \end{bmatrix}.$$

Kako je $297 = 11 \pmod{26}$*, i taj broj je u nazivniku, pitamo se za koji* x *vrijedi* $11 \cdot x = 1 \pmod{26}$*. Dobivamo* $x = 19$*. Sada je*

$$K^{-1} =_{26} 19 \cdot \begin{bmatrix} 22 & 12 & 1 \\ 16 & 1 & 3 \\ 25 & 20 & 9 \end{bmatrix} =_{26} \begin{bmatrix} 2 & 20 & 19 \\ 18 & 19 & 5 \\ 7 & 16 & 15 \end{bmatrix}.$$

Dešifriranje:

$$\texttt{QCL}: \quad \begin{bmatrix} 16 & 2 & 11 \end{bmatrix} \begin{bmatrix} 2 & 20 & 19 \\ 18 & 19 & 5 \\ 7 & 16 & 15 \end{bmatrix} =_{26} \begin{bmatrix} 15 & 14 & 11 \end{bmatrix},$$

$$\texttt{VWY}: \quad \begin{bmatrix} 21 & 22 & 24 \end{bmatrix} \begin{bmatrix} 2 & 20 & 19 \\ 18 & 19 & 5 \\ 7 & 16 & 15 \end{bmatrix} =_{26} \begin{bmatrix} 8 & 0 & 11 \end{bmatrix},$$

$$\texttt{UWJ}: \quad \begin{bmatrix} 20 & 22 & 9 \end{bmatrix} \begin{bmatrix} 2 & 20 & 19 \\ 18 & 19 & 5 \\ 7 & 16 & 15 \end{bmatrix} =_{26} \begin{bmatrix} 5 & 0 & 1 \end{bmatrix},$$

$$\texttt{TTC}: \quad \begin{bmatrix} 19 & 19 & 2 \end{bmatrix} \begin{bmatrix} 2 & 20 & 19 \\ 18 & 19 & 5 \\ 7 & 16 & 15 \end{bmatrix} =_{26} \begin{bmatrix} 4 & 19 & 18 \end{bmatrix},$$

$$\texttt{LEO}: \quad \begin{bmatrix} 11 & 4 & 14 \end{bmatrix} \begin{bmatrix} 2 & 20 & 19 \\ 18 & 19 & 5 \\ 7 & 16 & 15 \end{bmatrix} =_{26} \begin{bmatrix} 10 & 0 & 23 \end{bmatrix}.$$

Konačno, otvoreni tekst je onaj polazni tekst kojega se i šifriralo, tj. `POLIALFABETSKAX`*, odnosno* `POLIALFABETSKA`*.*

Hillov kriptosustav s 3×3 matricama ($m = 3$) skriva ne samo sve informacije o frekvencijama slova, već i o frekvencijama bigrama. Za $m \geq 4$ nestaju i frekvencije trigrama, a za $m \geq 5$ Hillov kriptosustav može se smatrati gotovo potpuno sigurnim – napad poznavanjem samo šifrata postaje praktički neizvediv.

Međutim, ako je poznat m – koji dijeli broj slova šifrata – i barem m različitih matrica iz $M_{1,m}(\mathbb{Z}_{26})$ odnosno m-torki otvorenog teksta:

$$x_i = (x_{i1}, x_{i2}, \ldots, x_{im}), \quad y_i = (y_{i1}, y_{i2}, \ldots, y_{im}),$$

takvih da je $y_i = e_K(x_i), i = 1, 2, \ldots, m$, moguće je odrediti ključ K. Neka su $X = [x_{ij}]$ i $Y = [y_{ij}]$ dvije $m \times m$ matrice. Tada, ako je matrica X invertibilna, ključ K izračunava se na sljedeći način:

$$Y = X \cdot K \Rightarrow K = X^{-1} \cdot Y.$$

Ako X nije invertibilna matrica, protivniku koji izvršava napad na ovaj kriptosustav biti će potreban neki drugi skup od m parova otvorenog teksta i šifrata.

S druge strane, ako m nije poznat, pretpostavljajući da nije jako velik, napad se može iskušavati za $m \in \{2, 3, \ldots\}$ redom dok se ne pronađe ključ. Ako pretpostavljena vrijednost od m nije točna, onda $m \times m$ matrica dobivena na prethodno opisani način neće biti u skladu s daljnjim parovima otvorenog teksta i šifrata.

Primjer 17. *Odredimo ključ K ako je Hillovom šifrom iz otvorenog teksta* `POTRES` *dobiven šifrat* `TUJLYK`*.*

Rješenje:

Očito vrijedi da je $m \in \{1, 2, 3, 6\}$. Razumno je pretpostaviti da je m jednako 2 *ili* 3*.*

Pokušajmo najprije s $m = 2$. Tada, koristeći korespodenciju između slova šifrata i njihovih numeričkih ekvivalenata, vrijedi:

$$\texttt{PO} \mapsto \texttt{TU}: \quad \begin{bmatrix}15 & 14\end{bmatrix} = \begin{bmatrix}19 & 20\end{bmatrix},$$

$$\texttt{TR} \mapsto \texttt{JL}: \quad \begin{bmatrix}19 & 17\end{bmatrix} = \begin{bmatrix}9 & 11\end{bmatrix},$$

$$\texttt{ES} \mapsto \texttt{YK}: \quad \begin{bmatrix}4 & 18\end{bmatrix} = \begin{bmatrix}24 & 10\end{bmatrix}.$$

Odaberimo

$$X = \begin{bmatrix}15 & 14\\ 19 & 17\end{bmatrix}.$$

Ova matrica je invertibilna jer je $det(X) = -11 =_{26} 15$ i $(15, 26) = 1$, te je

$$X^{-1} = \begin{bmatrix}15 & 6\\ 23 & 1\end{bmatrix}.$$

Sada po K rješavamo matričnu jednadžbu $Y = X \cdot K$ za

$$Y = \begin{bmatrix} 19 & 20 \\ 9 & 11 \end{bmatrix},$$

i imamo

$$K = X^{-1} \cdot Y = \begin{bmatrix} 1 & 2 \\ 4 & 3 \end{bmatrix}.$$

Dobiveni ključ provjeravamo na trećem paru:

$$\begin{bmatrix} 4 & 18 \end{bmatrix} \cdot K = \begin{bmatrix} 4 & 18 \end{bmatrix} \begin{bmatrix} 1 & 2 \\ 4 & 3 \end{bmatrix} = \begin{bmatrix} 24 & 10 \end{bmatrix},$$

te zaključujemo da smo na početku dobro pretpostavili da je $m = 2$. Dakle, ključ je

$$K = \begin{bmatrix} 1 & 2 \\ 4 & 3 \end{bmatrix}.$$

Zbog svoje prirode i različitosti od prethodnih kriptosustava, za Hillovu šifru se može reći da je na granici između klasične i moderne kriptografije.

Zaključak

Polialfabetske supstitucijske šifre vrlo su značajne za kriptologiju kao znanost zbog svog dugog vijeka razvijanja od oko 5 stoljeća. Radi potrebe tajnosti poruka, bile su to značajne ratne strategije koje su okosnica uspješnosti na bojištu ili jednostavno hobiji kriptografskih amatera poput Félix-Marie Delastella, te radi potrebe trećih strana da izvrše uspješne napade nad istima, u tom velikom vremenskom periodu došlo je do razvoja raznovrsnih kriptosustava od kojih je svaki pokušao ispraviti neku manu prethodnoga. Te mane obično su se otkrivale novim težnjama i naporima za uspješnim napadima na pojedine šifrate.

Uz nadolazeće moderno digitalno doba, kriptosustavi navedeni u ovom radu, kao i još neki značajni sustavi poput protočnih šifri, bili su nužna baza za razvoj modernih sigurnosnih računalnih sustava koji danas pokreću sve aspekte ljudskog života i od kojih očekujemo da sigurno skladište naše osobne podatke.

Literatura

[1] D. Bishop, *Introduction to Cryptography with Java Applets*, Jones and Bartlett Publishers, Sudbury, 2003.

[2] W. M. Bowers, *Digraphic substitution: The Playfair cipher, the four square cipher*, American Cryptogram Association, SAD, 1959.

[3] A. Dujella, M. Maretić, *Kriptografija*, Element, Zagreb, 2007.

[4] D. Kahn, *The Code-Breakers: The Story of Secret Writing*, The Macmillan Company, New York, 1967.

[5] D. Kahn, *The Codebreakers: The Comprehensive History of Secret Communication from Ancient Times to the Internet*, Scribner, New York, 1996.

[6] J. Rothe, *Complexity Theory and Cryptology: An Introduction to Cryptocomplexity*, Springer-Verlag, New York, 2005.

[7] A. Salomaa, *Public-Key Cryptography*, Springer-Verlag, New York, 1990.

Sažetak

Polialfabetske supstitucijske šifre, od kojih je prva bila Albertijeva šifra, predstavile su značajan napredak nad monoalfabetskim supstitucijskim šiframa u pogledu korištenja više supstitucijskih alfabeta u postupku šifriranja. Svaka sljedeća koja je nastala pokušala je popraviti neku ranjivost prethodne. Tako je Trithemiusova šifra za svako slovo teksta koristila drugi alfabet. Vigenèrova šifra više nije imala linearno kretanje po tablici slova (tzv. tabuli recti) kao što je to Trithemiusova imala, dok je Beaufortova šifra bila varijanta Vigenèrove šifre. Playfairova šifra predstavila je novi pogled na problem šifriranja koristeći bigrame i 5×5 matrice slova. Šifra četiri kvadrata može se smatrati njenim sigurnijim proširenjem jer sličnu logiku primijenjuje na četiri takve matrice, dok je šifra dva kvadrata pokušaj da se dobije najbolje od ta dva kriptosustava – veća sigurnost od Playfairove šifre uz jednostavnije šifriranje i dešifriranje od šifre četiri kvadrata. Na kraju, potpuno nov pogled na problem šifriranja i dešifriranja pružio je Hill sa svojom šifrom koja je bazirana na linearnoj algebri.

Ključne riječi

Polialfabetska supstitucijska šifra, Albertijeva šifra, Trithemiusova šifra, Vigenèrova šifra, Beaufortova šifra, Playfairova šifra, šifra četiri kvadrata, šifra dva kvadrata, Hillova šifra

Summary

Polyalphabetic substitution ciphers, from which the first one was Alberti cipher, were an advancement over monoalphabetic substitution ciphers simply because of their use of multiple alphabets in the encipherment process. Each one that followed the Alberti cipher tried to improve a vulnerability that the previous one possessed. The Trithemius cipher used a different alphabet for every letter that it processed, the Vigenère cipher didn't have linear movement over the so-called tabula recta, while the Beaufort cipher is considered to be a variant of the Vigenère cipher. Furthermore, the Playfair cipher had a new perspective of the encipherment problem using bigrams and 5×5 letter matrix. The four-square cipher can be considered as an extension of the Playfair cipher with improved security because it applies a similar logic to four such matrices, while the two-square cipher attempts to obtain the best of these two cryptosystems – better text encryption then the Playfair cipher while being easier to use then the four-square cipher. Finally, a completely new perspective on the encipherment problem was provided by Hill's cipher based on linear algebra.

Keywords

Polyalphabetic substitution cipher, Alberti cipher, Trithemius cipher, Vigenère cipher, Beaufort cipher, Playfair cipher, four-square cipher, two-square cipher, Hill cipher

Životopis

Zovem se Valentina Kobašević i rođena sam 18. veljače 1994. godine u Vinkovcima. Pohađala sam Osnovnu školu Ivana Gorana Kovačića u Štitaru te sam osnovnoškolsko obrazovanje završila 2008. godine. Iste godine upisala sam opću gimnaziju u Županji. 2012. godine završila sam srednjoškolsko obrazovanje i upisala sveučilišni nastavnički studij matematike i informatike na Odjelu za matematiku Sveučilišta Josipa Jurja Strossmayera u Osijeku. Trenutno radim u Gimnaziji Županja i OŠ Mate Lovraka u Županji.