Supstitucijske šifre

Klobučar, Josipa

Sveučilište J.J. Strossmayera u Osijeku
Odjel za matematiku
Sveučilišni preddiplomski studij matematike

Josipa Klobučar

Supstitucijske šifre

Završni rad

Osijek, 2016.

Sveučilište J. J. Strossmayera u Osijeku
Odjel za matematiku
Preddiplomski studij matematike

Josipa Klobučar

Supstitucijske šifre

Završni rad

Voditelj: izv.prof.dr.sc. Ivan Matić

Osijek, 2016.

Sažetak. U ovom završnom radu ćemo se, kao što to i naslov kaže, baviti supstitucijskim šiframa te njihovim dešifrifanjem i primjerom primjene u informatici. U prvom poglavlju baviti ćemo se supstitucijskim šiframa i definirati ćemo nekoliko načina kako ih napraviti. Uz svaki dio napravit ćemo i primjere pomoću elngleske i hrvatske abecede
U drugom poglavlju bavit ćemo se dešifriranjem supstitucijskih šifri, dok ćemo u trećm vidjeti primjenu u tehnologiji koju svakodnevno koristimo.

Ključne riječi: supstitucijske šifre, jednostavene supstitucijske šifre, pomaknuta šifra, šifre s datumskim pomakom, šifriranje ključnom riječju, Pigpen šifra, Polybiusov kvadrat, nasumične supstitucijske šifre, Shadowljev kôd, dešifriranje, CrypticSMS, TimePIN

Abstract. This final thesis paper is about substitution ciphers and their use in informational technology. The first chapter will reflect on substitution ciphers, how to create them, and with each of those examples will be provided using the Croatian and the English alphabet. The second chapter will describe the decoding process of said substitution ciphers, while the third chapter will show examples of such ciphers being used in everyday technology.

Key words: substitution ciphers, simple substitution ciphers, date shift ciphers, key word ciphers,the pigpen cipher, the Polybius checkerboard, random substitution ciphers, the Shadow's code, deciphering, CrypticSMS, TimePIN

Sadržaj

1 Uvod

Kriptografija je prevođenje razgovijetnoga teksta (jasan, otvoreni tekst), ili bilo kakvog drugoga skupa podataka, u nerazgovijetan tekst (kriptirani tekst, kriptogram ili šifrat), kako bi ga jedino onaj koji posjeduje unaprijed utvrđen ključ za odgonetanje (dešifriranje) mogao prevesti u izvorni, razgovijetni tekst. Zadaća je kriptografije da omogući dvjema osobama (pošiljatelj i primatelj) očuvanje tajnosti poruka, čak i u komunikaciji nesigurnim komunikacijskim kanalom (npr. računalna mreža), koji je dostupan trećim osobama.

Supstitucijske šifre susrećemo u svakodnevnom životu: točke i povlake u Morseovoj abecedi, kombinacije Brailleovog pisma, znakovni jezik, komunikaciji bubnjevima afričkih plemena... To, naravno, nisu šifre, ali su primjer zamjene slova i riječi sa simbolima.

Kriptografija se stoljećima primjenjivala za osiguravanje tajnosti pretežito vojne i diplomatske komunikacije. U predznanstvenome razdoblju klasične kriptografije, postupci kriptiranja svodili su se na različite domišljate kombinacije razmještanja znakova unutar teksta ili na njihovu zamjenu (supstitucija). Dio kriptologije koji se bavi postupcima odgonetanja poruka bez poznavanja ključa naziva se kriptoanalizom.

Danas, u doba razmjene poruka globalnim računalnim i komunikacijskim mrežama, kriptografija se široko primjenjuje: bilo da se želi osigurati privatnost poruka, ili se time nastoji zaštititi njihova tajnost. U oba se slučaja kriptografija bavi podatcima u digitalnom obliku, postupci kriptiranja i dekriptiranja matematičke su naravi, a provode se automatski, uz pomoć računala. Zbog toga se suvremena kriptologija uglavnom oslanja na računarstvo, a znatno je potpomognuta teorijom brojeva.

2 Supstitucijske šifre

U supstitucijskoj šifri, poredak slova ostaje isti, ali se za svako slovo koristi drugo slovo, ili neka vrsta simbola. Takve šifre zovu se supstitucijske jer nešto supstituira (mijenja) svako slovo poruke. Supstitucijske i transpozicijske šifre mogu se kombinirati na razne načine, no kôd tada postaje previše kompliciran i vrlo je lako pogriješiti u kôdiranju i dekôdiranju poruke. Profesionalni kriptografi ograničavaju riječ "kôd" na pojam tajnog pisanja u kojem se cijele riječi ili fraze supstituiraju drugim riječima. U ovom radu pratit ćemo uobičajenu praksu korištenja riječi "kôd" kao drugu riječ za pojam šifre.

Većina sljedećih supstitucijskih šifri su monoalfabetske. To znači da svako slovo ima jedno i samo jedno supstitucijsko slovo ili znak. Ako je kôd za slovo T slovo K, onda svaki puta kada se pojavi slovo K u šifri, ono znači slovo T, i niti jedno drugo slovo osim K nema to značenje.

Velika prednost supstituiranja je da se ono lako pamti. Ako uz sebe imate abecedni ključ šifre, netko ga može pronaći i ukrasti vam ga, i na taj način pročitati sve šifrirane poruke. Kôd tada postaje potpuno bezvrijedan. Ali ako ključ šifre zapamtite, nitko ga ne može ukrasti. Jedna od najjednostavnijih i najstarijih supstitucijskih šifri kreira se pisanjem abecede standardnim redom, a onda ispod toga obrnutim redom.

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

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

Tablica 1: U tablici vidimo kako se zapisuje jednostavna supstitucijska šifra

Svako slovo odgovara onome točno ispod njega (ili iznad). Poruka kao **MYRTLE HAS BIG FEET** bi se pisala u obliku:

NBIGOV SZH YRT UVVG

ili ako grupirate slova u četverce:

NBIG OVSZ HYRT UVVG.

Promotrite kako se riječ "big" ponovno javlja na početku kôdiranog teksta. Iako je puka slučajnost, ovakve stvari vrlo su česte u šifriranom pisanju. Ponekad izazivaju velike probleme kriptoanalitičarima jer ih oni shvate kao tragove za dešifriranje, no zapravo ih samo odvedu s pravog puta.

Još jedna jednostavna metoda jest numerirati slova abecede unaprijed (A=1, B=2, C=3 itd.) ili unatrag (A=26, B=25, C=24 itd). Tada se brojevi koriste umjesto slova. Za razlikovanje jednoznamenkastih od dvoznamenkastih brojeva koriste se crtice. Obje ove metode abeceda unatrag i numeriranje slova vrlo su riskantne za korištenje. Toliko su poznate da ih vjerojatno i vaši neprijatelji koriste. Potrebna je samo minuta do dvije za testiranje šifre kako bi se ustanovilo je li korištena jednostavna supstitucija. Sustavi koji su opisani u nastavku superiorni su u odnosu na ove jednostavnije.

Primjer 2.1. *Kako bi pomoću jednostavnih supstitucija napisali rečenicu:*

NAJČEŠĆE JEDEM GROŽĐE

Uzmimo za ovaj primjer numeriranje slova unazad:

A	*B*	*C*	*Č*	*Ć*	*D*	*Dž*	*Đ*	*E*	*F*	*G*	*H*	*I*	*J*	*K*
30	*29*	*28*	*27*	*26*	*25*	*24*	*23*	*22*	*21*	*20*	*19*	*18*	*17*	*16*

L	*Lj*	*M*	*N*	*Nj*	*O*	*P*	*R*	*S*	*Š*	*T*	*U*	*V*	*Z*	*Ž*
15	*14*	*13*	*12*	*11*	*10*	*9*	*8*	*7*	*6*	*5*	*4*	*3*	*2*	*1*

Čitajući iz tablice dobivamo:

13117282272622 1722252213 2091012723.

2.1 Pomaknuta šifra

Pomaknuta šifra zove se još i **Cezarova šifra**, jer ju je koristio rimski car Julije Cezar za tajne državne poruke. Jednostavne su za kôdiranje i dekôdiranje.

Broj pomaka, kojeg znate samo vi i vaši prijatelji (i koji se može mijenjati po potrebi) govori za koliko slova unaprijed je potrebno pomaknuti abedecu za šifriranje poruke. Primjerice, ako je broj pomaka 7, potrebno je abecedu za šifriranje poruke započeti slovom 7 mjesta udaljenim od slova A, i tako za svako slovo abecede. Nakon što se šifra dovrši, ona izgleda ovako:

T	U	V	W	X	Y	Z	A	B	C	D	E	F
A	B	C	D	E	F	G	H	I	J	K	L	M

G	H	I	J	K	L	M	N	O	P	Q	R	S
N	O	P	Q	R	S	T	U	V	W	X	Y	Z

Tablica 2: U tablici vidimo kako se zapisuje jednostavna supstitucijska šifra s pomakom

Za kôdiranje poruke, slovo iz gornjeg reda potrebno je zamijeniti slovom točno ispod njega, tako da slova iz riječi **MYRTLE**, pomaknuta 7 mjesta unaprijed, glase **TFYASL**. Za dekôdiranje prouke, potrebno je naći slovo u donjem redu i zamijeniti ga onim točno iznad njega.

Pošto su ovakve poruke temeljene na jednostavnim abedednim pravilima, potrebno je uništiti ključ po kôdiranju ili dekôdiranju poruke, kako bi spriječili da ključ dopadne u krive ruke.

Povremeno određene riječi čistom slučajnošću postaju neka sasvim druga riječ kada se kôdira, kao npr. riječ COLD (hladno). Pokušajte ju kôdirati pomakom od 3 mjesta. Ili riječ PECAN (vrsta oraha) pomakom od 4 mjesta, ili SLEEP (spavati) s pomakom od 9 mjesta. Što je dulja riječ, manja je vjerojatnost da će njena šifra biti smislena riječ. Jedna od najduljih takvih riječi u engleskom jeziku je ABJURER, koja pomakom od 13 mjesta postaje riječ NOWHERE (nigdje).

Primjer 2.2. *Kako bi pomoću pomaka napisali rečenicu:*

NAJČEŠĆE JEDEM GROŽĐE

Uzmimo za ovaj primjer abeceda kreće sa slovom F, tj s pomakom 10:

F	*G*	*H*	*I*	*J*	*K*	*L*	*Lj*	*M*	*N*	*Nj*	*O*	*P*	*R*	*S*
A	*B*	*C*	*Č*	*Ć*	*D*	*Dž*	*Đ*	*E*	*F*	*G*	*H*	*I*	*J*	*K*

Š	*T*	*U*	*V*	*Z*	*Ž*	*A*	*B*	*C*	*Č*	*Ć*	*D*	*Dž*	*Đ*	*E*
L	*Lj*	*M*	*N*	*Nj*	*O*	*P*	*R*	*S*	*Š*	*T*	*U*	*V*	*Z*	*Ž*

Čitajući iz tablice dobivamo:

FPĆŠŽLTŽ ĆŽUŽE BJHOZŽ .

2.2 Šifre s datumskim pomakom

Kako bi šifriranu poruku što više otežali za dešifriranje bez ključa, moguće je broj pomaka mijenjati za svako slovo. Jedan od načina je korištenjem nadnevka kada je poruka poslana. Na primjer da želite poslati poruku 21. listopada 1973. Listopad je 10. mjesec u godini, i nadnevak tada možemo pisati po američkom sustavu kao 10-21-73. Uklanjanjem crtica dobije se broj 1002173. Taj broj tada treba ponavljati iznad svakog slova poruke:

102173	102	173	1021
MYRTLE	HAS	BIG	FEET

Tablica 3: U tablici vidimo kako se zapisuje jednostavna supstitucijska šifra s datumskim pomakom

Za kôdiranje poruke, slovo M potrebno je pomaknuti za jedno mjesto, i ono tada postaje N. Y se ne pomiče (zbog broja 0), te ostaje Y. R se pomiče za 2 mjesta, i postaje T, i tako dalje za sva slova poruke. Ako pomak ide dalje od slova Z, nastavlja se od početka abecede. Konačna poruka, korištenjem ključa 102173 i grupiranjem slova u grupe od četiri, dalje sljedeći rezultat:

NYTU SHIA UCPJ GEGU.

Za dekôdiranje poruke, potrebno je napisati ključ iznad poruke i pomake u abecedu odraditi unatrag. Ako pomak ide dalje od slova A, potrebno je vratiti se na kraj abecede i nastaviti prema nazad. Ova šifra nije monoalfabetska. Posljednja riječ od četiri slova, FEET, u šifriranoj poruci postaje GEGU, tako da je 'EE' iz FEET zamijenjeno s 'EG', što šifre s datumskim pomakom čini izrazito složenim za probijanje. datum, već se on može zamijeniti bilo kojim brojem.

Primjer 2.3. *Kako bi pomoću datumskog pomaka napisali rečenicu:*

NAJČEŠĆE JEDEM GROŽĐE

Uzmimo za ovaj primjer pomak datuma 8-5-2015 odnosno 050815:

05081505	*05081*	*505081*
NAJČEŠĆE	*JEDEM*	*GROŽĐE*

Pomičući se po abecedi za točno onoliko mjesta koliki je broj iznad slova dobivamo:

NDJHFŽĆJ JJDLjN LRTŽLF.

2.3 Šifriranje ključnom riječju

Jednostavan način za kreiranje supstitucijske abecede za šifriranje je korištenjem ključne riječi ili fraze. Uzmimo za primjer da je dogovoreni ključ JUPITER. Ispod ispisane abecede potrebno je ispisati riječ JUPITER i onda nastaviti s preostalim slovima abecede:

A	B	C	D	E	F	G	H	I	J	K	L	M
J	U	P	I	T	E	R	A	B	C	D	F	G

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
H	K	L	M	N	O	Q	S	V	W	X	Y	Z

Tablica 4: U tablici vidimo kako se zapisuje jednostavna supstitucijska šifra uz pomoć ključne riječi

Ključne riječi lako se pamte, i svaka riječ automatski kreira drugačiju supstitucijsku šifru. Kôdiranje i dekôdiranje vrše se na isti način kao u prethodno opisanim metodama.

U ovome se sustavu slova V, X, Y i Z ne mijenjaju, jer riječ JUPITER nema slova koja idu dalje od slova U. Ako koristite riječ koja sadrži slovo Y, ona će promijeniti cijelu abecedu osim slova Z. Potrebno je da riječ korištena za šifriranje nema slova koja se ponavljaju.

Ukoliko se riječ šifriranja mijenja svaki tjedan, teško je usuglasiti se koja će riječ biti korištena u svakoj prilici. Jedan od načina za lakši dogovor je korištenje svima dostupnih i pristupačnih novina ili magazina za pronalazak ključnih riječi. Potrebno je odabrati riječ koja može poslužiti za supstituciju, zabilježiti broj stranice na kojoj se riječ nalazi, redak i redni broj riječi na stranici. Taj podatak može se onda ostaviti na kraju šifriranog teksta. Primjerice, broj 205-17-8 znači da se ključna riječ nalazi na 205. stranici, u 17. redu i da je u tom redu ta riječ 8. po redu.

Primjer 2.4. *Kako bi pomoću jednostavnih supstitucija napisali rečenicu:*

NAJČEŠĆE JEDEM GROŽĐE

Uzmimo za ovaj primjer abeceda kreće sa slovom F, tj. s pomakom 10:

A	*B*	*C*	*Č*	*Ć*	*D*	*Dž*	*Đ*	*E*	*F*	*G*	*H*	*I*	*J*	*K*
S	*V*	*J*	*E*	*T*	*L*	*O*	*A*	*B*	*C*	*Č*	*Ć*	*D*	*Dž*	*Đ*

L	*Lj*	*M*	*N*	*Nj*	*O*	*P*	*R*	*S*	*Š*	*T*	*U*	*V*	*Z*	*Ž*
F	*G*	*H*	*I*	*K*	*Lj*	*M*	*N*	*Nj*	*P*	*R*	*Š*	*U*	*Z*	*Ž*

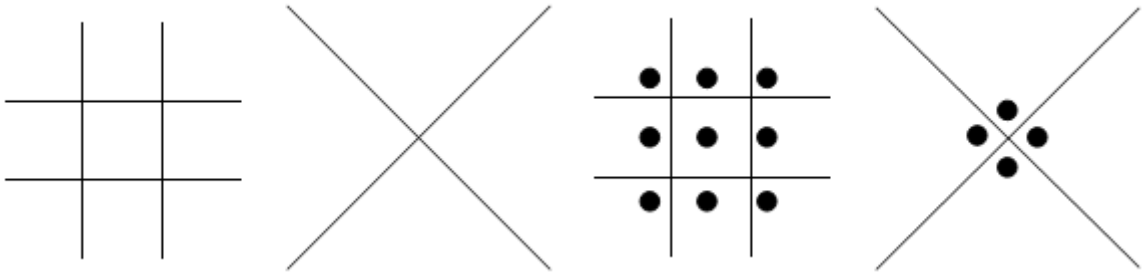
Čitajući iz tablice dobijemo:

ISDEBPTB DžBLBH ČNLjŽAB.

2.4 Pigpen šifra

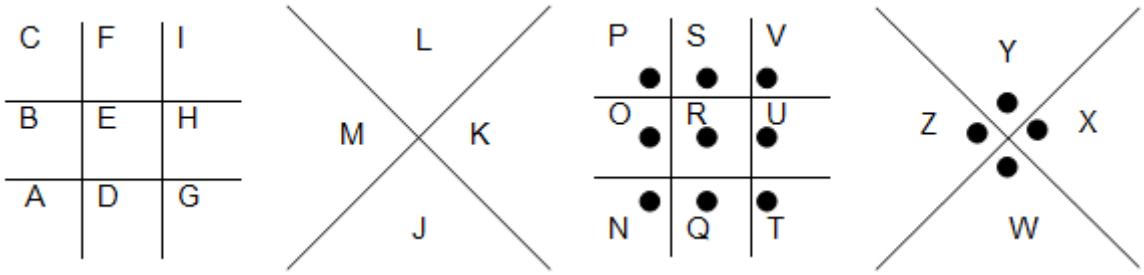
Pigpen (svinjac) šifra dobija svoje ime po načinu na koji se slova odvajaju linijama, kao svinje u svinjcu. Poznata je i kao masonska šifra, koju je koristilo društvo masona više od stotinu godina. Koristili su ju i vojnici Konfederacije u Američkom građanskom ratu.

Nacrtajte polje kao za igru iks-oks (tic tac toe, križić-kružić) i veliki kosi križ (slovo X), i onda ponovite crteže, s tim da svaki odjeljak označite točkom:



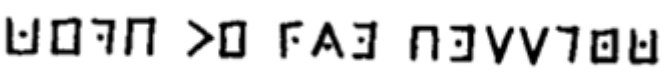
Slika 1: Na slici vidimo kako se izgleda osnovni oblik Pigpen šifre

Abecedu ispišite u sve odjeljke na crtežima. Budući da je ovaj način šifriranja relativno popularan, dobra je ideja slova ispisati nekim neuobičajenim poretkom. Na sljedećoj slici, slova idu prema gore u svakom stupcu iks-oks tablice, stupci idu prema desno, a u X uzorku idu u smjeru obrnutom od kazaljke na satu, s početkom u donjem odjeljku:



Slika 2: Na slici vidimo kako se izgleda osnovni oblik Pigpen šifre uz raspored slova abecene po vlastitoj želji

Poruka se tada slaže tako da se svako slovo poruke supstituira malim crtežom odjeljka u kojem se slovo nalazi. Poruka **SEND ME TWO DOLLARS** u pigpen šifri izgleda ovako:



Slika 3: Na slici vidimo primjer šifata

2.5 Polybiusov kvadrat

Polybius je bio starogrčki pisac koji je predložio metodu supstitucije svakog slova različitim dvoznamenkastim brojem. Abeceda se ispisuje u matricu 5×5 s numeriranim retcima i stupcima:

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

Tablica 5: U tablici vidimo kako se zapisuje Polybiusov kvadrat

Primijetite kako slova Y i Z dijele posljednju ćeliju tablice. Također česti slučajevi su da slova I i J dijele ćeliju tablice. Kontekst poruke trebao bi biti dovoljan da se odredi je li za poruku potrebno slovo Y ili Z. Za kôdiranje, potrebno je zamijeniti slovo s brojvanom oznakom retka i stupca u kojem se slovo nalazi. Na prvom mjestu nalazi se broj retka, a onda i broj stupca. Primjerice, slovo Q postaje 42, slovo J 25, itd. Riječ **WATERMELON** kôdirana postaje:

53-11-45-15-43-33-15-32-35-34.

Dekôdiranje se vrši na način da se pročita broj, prva znamenka označava red, a druga stupac. Npr. 53 je peti redak, treći stupac, u kojem se nalazi slovo W.

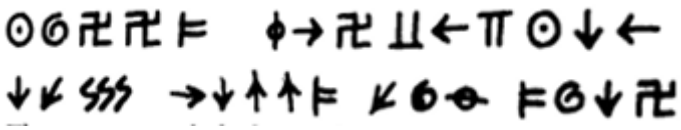
2.6 Nasumične supstitucijske šifre

Sve dosad pregledane supstitucijske šifre koristile su abecedu ispisanu prema određenim pravilima. Njihova prednost je ta što ne morate nositi njihov ključ sa sobom za dekôdiranje poruke.

Nasumična supstitucijska šira je konstruirana bez ikakvih pravila ili planova. Ispišete abecedu, i uz svaki njen znak stavite bilo koje slovo, broj ili znak. Iako gubitkom ključa gubite i način dekôdiranja poruka, nasumične supstitucijske šifre puno su teže za probijanje od šifri temeljenih na jednostavnim sustavima.

Deseci i deseci detektivskih priča i romana koristile su nasumične šifre kao bitne dijelove svojih radnji. Jedna od najpoznatijih je kratka priča Arthura Conana Doylea, "The Adventure of Dancing Men", u kojoj detektiv Sherlock Holmes razbija nasumičnu šifru koristeći nacrtane čovječuljke za svako slovo abecede. Još jedna slična priča je ona Edgara Allana Poea, "The Gold Bug", u kojoj šifra koristi brojeve i razne simbole.

Nasumična šifra može se složiti dodavanjem bilo kojeg simbola svakom od slova. Primjerice, ako poruku **MERRY CHRISTMAS AND HAPPY NEW YEAR** kôdirate simbolima, ona će izgledati vrlo tajnovito:



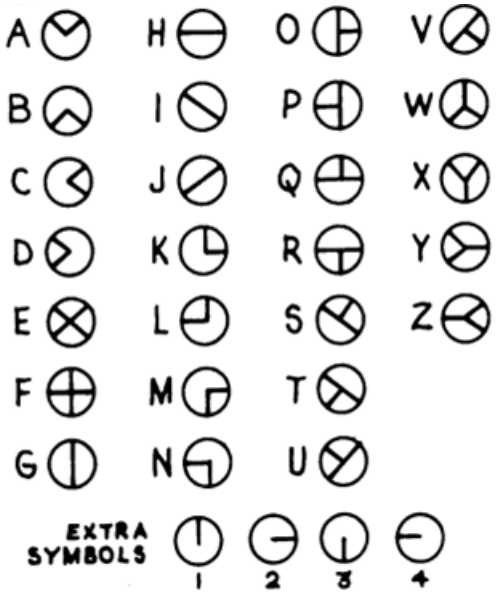
Slika 4: Na slici vidimo kako se izgleda primjer kôdiranja simbolima

Čudni simboli ne čine poruku težom za dekôdiranje od onih pisanih slovima i brojevima. Sljedeće poglavlje prikazat će kako kriptoanalitičari rjevavaju šifre za koje ne znaju je li korištena abeceda ili ne.

Slika 5: Na slici vidimo kako se izgleda abeceda kôdirana simbolima

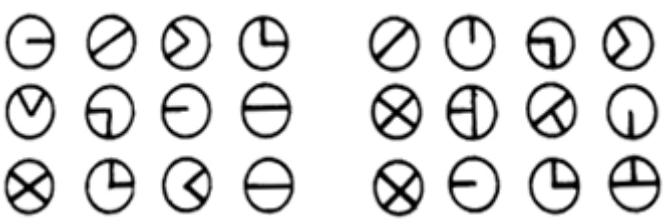
2.7 Shadowljev kôd

U 30-im godinama prošlog stoljeća, misteriozni borac protiv zločina imena Shadow bio je junak popularnih časopisa i još popularnije radijske emisije. Shadow, obučen u crno, neprimjetno se kretao kroz tamu kako bi se borio protiv sila zla. Priče o Shadowu pisao je Maxwell Grant (pseudonim tvorca Shadowa, Waltera B. Gibsona) i često je u njih uključivao neobične šifrirane poruke. Ova šifra iz kratke novele naslova "The Chain of Death" jedna je od najboljih.



Slika 6: Shadowljev kôd

Abeceda sa slike pokazuje četiri dodatna simbola na dnu tablice, koji se mogu ubaciti na bilo koje mjesto u šifriranom tekstu. Svaki od ta četiri simbola pokazuje kako se stranica na kojoj je napisan šifrirani tekst mora okrenuti za nastavak dekôdiranja, sve dok se ne dođe do sljedećeg od tih simbola. Crtica u tim simbolima pokazuje koja od stranica papira treba biti gornja stranica. Primjerice, ako se u tekstu pojavi simbol označen s brojem 3 u tablici, znači da je papir potrebno okrenuti naopako, tako da donja strana postane gornja. Ako se u nastavku teksta pojavi simbol broj 2, potrebno je papir okrenuti ulijevo, tako da desni rub stranice postaje gornji rub, i tako dalje. Poruka **I AM IN DANGER. SEND HELP** može izgledati ovako:



Slika 7: Primjer korištenja Shadowljeva kôda

Poruka nam govori da je prije početka dekôdiranja papir potrebno okrenuti ulijevo, i nakon dekôdiranja sljedeća četiri znaka, dolazimo do sljedećeg simbola koji pokazuje da papir treba okrenuti u normalni položaj, i tako sve dok ne dođemo do kraja poruke.

2.8 Šifriranje hrvatske abecede

U prethodnim poglavljima prikazano je kako možemo šifrirati ako abecedu uzmemo doslovno sa svim karakterističnim slovima za hrvatsku abecedu, dok ću u ovom obraditi i vezu između hrvatke i engleske abecede.

Ne postoje stroga pravila šifriranja slova karakteristična za hrvatsku abecedu. Kao i kod svakog postupka šifriranja sve ovisi o dogovoru između pošiljatelja i primatelja.

Najprihvaćeniji standard je takav da se koriste isključivo slova engleske abecede, te se č i ć pisu kao c, š kao s, đ kao dj, ž kao z, dok se lj, nj i dž tretiraju kao par slova odnosno lj, nj i dz. Radeći na ovaj način unosimo težinu dešifriranja jer za dva slova koristimo isti znak ili za jedno slovo dva znaka no o tome nešto više u idućem poglavlju.

A	B	C	Č	Ć	D	Dž	Đ	E	F	G	H	I	J	K
A	B	C	C	C	D	DZ	DJ	E	F	G	H	I	J	K

L	Lj	M	N	Nj	O	P	R	S	Š	T	U	V	Z	Ž
L	LJ	M	N	NJ	O	P	R	S	S	T	U	V	Z	Z

Tablica 6: U tablici vidimo izmjene hrvatske abecede

Provjerimo kako bi jedan od ranijih primjer izgledao šifriranjem na ovaj nain:

Primjer 2.5. *Kako bi pomoću pomaka napisali rečenicu:*

NAJČEŠĆE JEDEM GROŽĐE

Uzmimo za ovaj primjer abeceda kreće sa slovom F, tj s pomakom 10, te uzmimo u obzir da smo hrvatsku abecedu prilagodili engleskoj. Tada rečenica koju šifriramo glasi:

***NAJCESCE JEDEM GROZDJE**:*

F	*G*	*H*	*I*	*J*	*K*	*L*	*M*	*N*	*O*	*P*	*Q*	*R*
A	*B*	*C*	*D*	*E*	*F*	*G*	*H*	*I*	*J*	*K*	*L*	*M*

S	*T*	*U*	*V*	*W*	*X*	*Y*	*Z*	*A*	*B*	*C*	*D*	*E*
N	*O*	*P*	*Q*	*R*	*S*	*T*	*U*	*V*	*W*	*X*	*Y*	*Z*

Čitajući iz tablice dobivamo:

***IVEXZNXZ EZYZH BMJUYEZ**.*

2.9 Primjena u svakodnevnom životu

Primjena kriptografije je još uvijek najraširenija u vojne svrhe, ali razvojem informatike, tehnologije i Interneta kao prijenosnika poruka i informacija javlja se potreba za zaštitom istih. U vrijeme kada svakodnevno izbijaju skandali oko neovlaštenog nadzora i krađe podataka potreba za njihovom zaštitom veća je nego ikad. Neke od učinkovitijih metoda zaštita podataka upravo se mogu naći u šifriranju.

Iako se za zaštitu baza podataka i općenito sadržajem važnije baze koriste inačice RSA ili DES sustava, za osobne potrebe prosječnog korisnika zaštitu osobnih podataka može se izvršiti jednostavnim šifriranjem.

2.9.1 Jednostavni primjeri kriptografske metode

Kriptografija se temelji na jednoj sveobuhvatnoj premisi: potrebi za šifrom koja je pouzdana, prijenosna, i koja može kriptirati tekst koji se kroz bilo koji način kriptoanalize ne može riješiti korištenjem postojeće tehnologije. Kroz stoljeća, bilo je mnogo pokušaja kreiranja jednostavnih šifri koje mogu ispuniti zadane ciljeve. S iznimkom jednokratne metode koja nije lako prenosiva, uspjeh je bio relativno skroman.

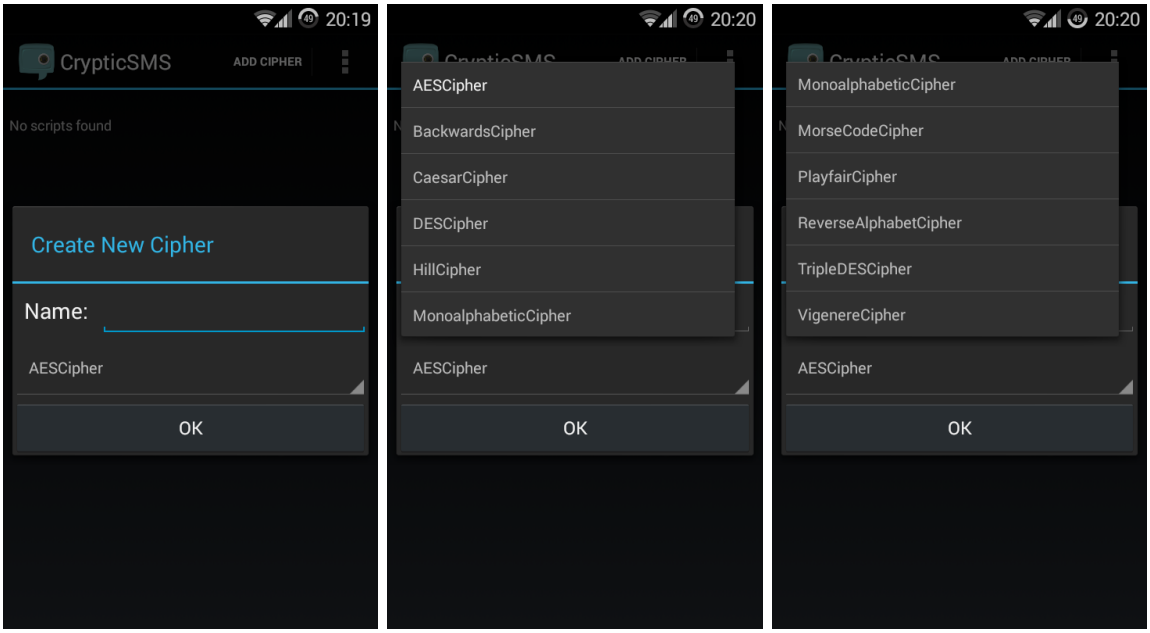
Iako naizgled jednostavne i zastarjele s tehnološkog stajalita, supstitucijske šifre izvor su enigmatske zabave za velik broj ljubitelja enigmatike diljem svijeta.

2.9.1.1 CrypticSMS

Koliko je kriptografija potrebna i zanimljiva za korištenje pokazuje broj dostupnih aplikacija za kriptiranje poruka između korisnika. Aplikacije kao takve koriste osim jednostavnih supstitucijskih šifri, polialfabetske šifre i slične zamjene (npr. korištenje ASCII kôda).

U slijedećem primjeru vidjet ćemo aplikaciju za razmjenu poruka koja ima mogućnost šifriranja i dešifriranja pomoću jednostavnih supstitucijskih šifri.

U početnom zaslonu aplikacije pritiskom na Add Cipher u gornjem desnom kutu zaslona kreira se novi šifrat. Pri kreiranju izabire se njegovo ime i vrsta (8a). Zatim se odabire jedan od mogućih načina za kriptiranje (8b i 8c).

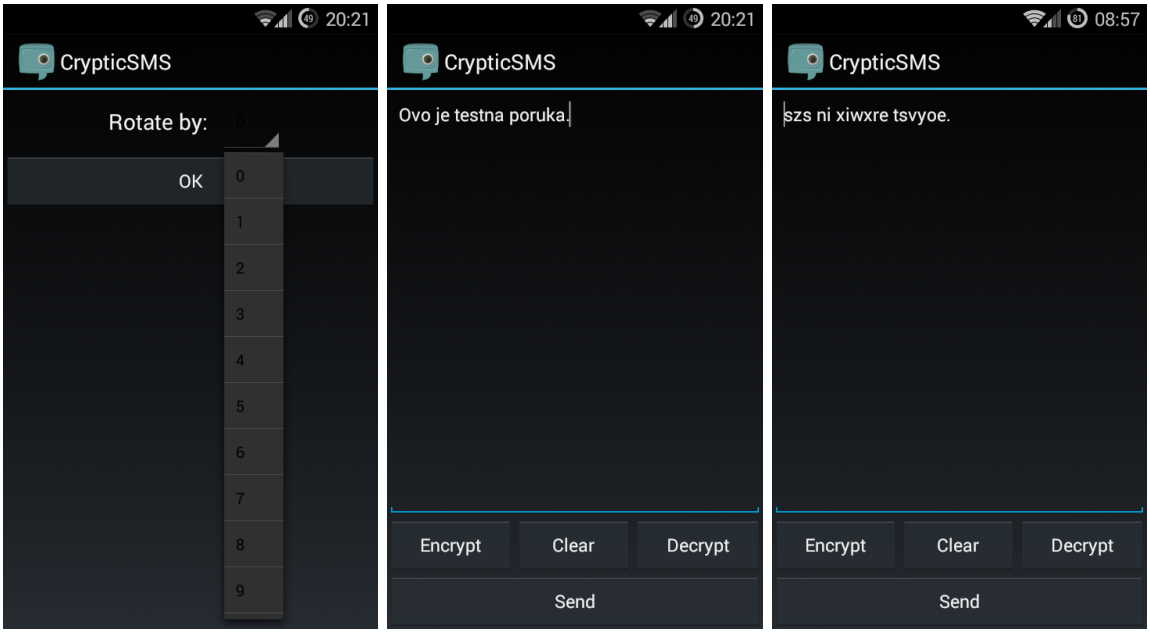


(a) Kreiranje novog šifrata (b) Dostupni načini šifriranja (c) Dostupni načini šifriranja

Slika 8: Snimke počenih zaslona aplikacije CrypticSMS

Kao primjer uzet ćemo Cezarovu šifru koja je obrađena u prethodnim poglavljima rada. Nakon odabranog načina šifriranja, odabiremo koliki pomak želimo kreirati u odnosu na osnovnu alfanumeričku abecedu. Za ovaj primjer uzet je pomak od 4 znaka. Nakon odabira pomaka unosimo tekst koji želimo kriptirati te za kriptiranje stisnemo tipku s oznakom

Encrypt.



(a) Odabir pomaka (b) Početni tekst poruke (c) Kriptirani tekst

Slika 9: Kriptiranje pomoću Cezarove šifre

Kriptiranu poruku tada možemo poslati pritiskom na tipku Send, prilikom čega mobilni uređaj ponudi na koji načine je dostupno slanje poruke.

Aplikacija, ukoliko to način šifriranja zahtijeva, nudi mogućnost kreiranja vlastite abecede i ključne riječi. Na isti način nudi i mogućnost dekriptiranja poruka.

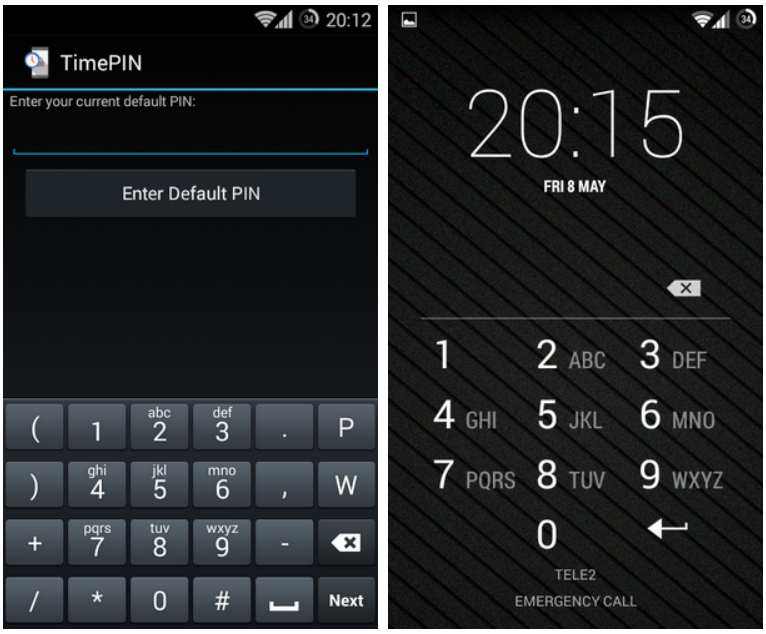
Postoje i aplikacije poput Pig Pen i Pigpen Keyboard dodatak Multiling tipkovnici koje nude mogućnost šifriranja uz pomoć pigpen šifre, ali one nemaju mogućnost vlastitog odabira rasporeda slova abecede nego samo jedan zadani raspored, te time ne koriste sav potencijal ove "slikovite" šifre.

2.9.1.2 TimePIN

Sam primjer govori koliko se kriptografija kao takva širi i u svakodnevnom životu običnog čovjeka. Radi se o aplikaciji TimePIN za uređaje bazirane na trenutno najraširenijem operacijskom sustavu za mobilne uređaje Android.

Aplikacija radi na principu ograničavanja pristupa uređaju korištenjem trenutnog vremena prema satu samoga uređaja ili varijacija na vrijeme (zrcaljenje, sa zadanim pomakom, duplanje unosa i obrnuti redoslijed). Također osim vremena aplikacija koristi i datum.

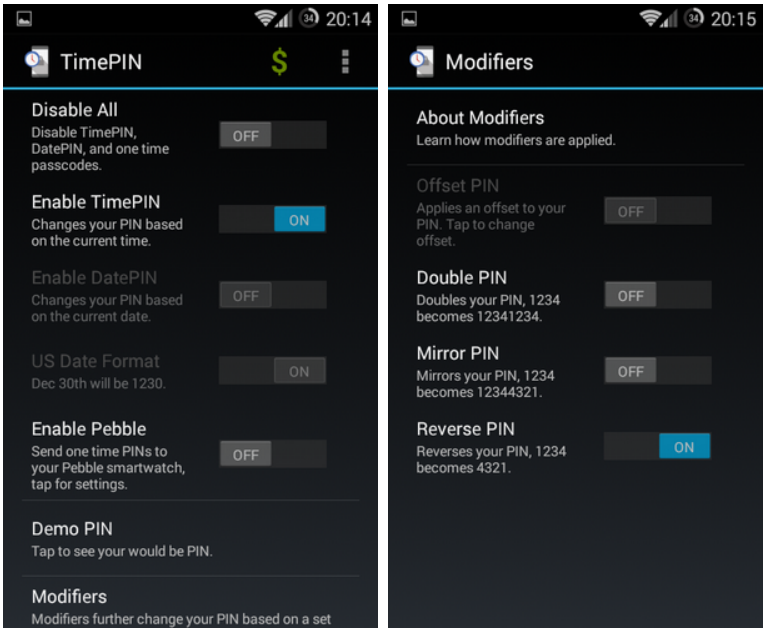
Kako bi ograničio pristup postavkama, prilikom pristupa istima potrebno je unijeti kontrolni PIN broj poznat samo vlasniku uređaja.



(a) Unos privatnog ključa (b) Zaključani zaslon

Slika 10: Snimke zaslona aplikacije TimePIN

Aplikacija omogućava korištenje supstitucijske šifre gdje je lozinka za pristup uređaju zapravo trenutno vrijeme upisano unatrag. Osim toga moguće je koristiti i šifru gdje se može unjeti proizvoljni pomak, npr ako je točno vrijeme 20:23, a proizvoljni pomak -101 tada šifra za otključavanje postaje 1922 (2023-101=1922). Od nasumičnih opcija šifriranja dostupno je zrcaljenje (npr ako je 20:23 onda je pin 20233202) i udvostručavanje unosa (20232023).



(a) Izbor oblika ključa (b) Izbor šifrata

Slika 11: Snimke zaslona aplikacije TimePIN

Na tržištu, naravno, postoje slične aplikacije ali princip rada je isti: korištenje jednostavnih šifrata kako bi se omogućila privatnost.

3 Dešifriranje supstitucijskih šifri

Brzo rješavanje jednostavnih supstitucijskih šifri umjetnost je koja zahtijeva veliko znanje i iskustvo. U ovom poglavlju prikazati ćemo nekoliko smjernica i kako se zapravo rješavaju kriptogrami koji se pojavljuju kao zagonetke u mnogim novinama, tjedno u The Saturday Review. Takvi kriptogrami zadržavaju originalni raspored slova, riječi i interpunkcijskih znakova, što olakšava njihovo rješavanje.

Za početak, nekoliko važnih činjenica o engleskom jeziku:

1. Najčešće korišteno slovo u engleskom jeziku je slovo E, a redom za njim slova T, A, O, i N (E je također najčešće slovo u njemačkom, talijanskom i španjolskom jeziku, ali ovaj podatak ne vrijedi za mnoge druge svjetske jezike, kao što je primjerice ruski, u kojem je najčešće slovo O).

2. Slovo koje se najčešće javlja na kraju riječi je E.

3. Slovo s kojim riječi najčešće počinju je T.

4. Slovo koje stoji samo po sebi kao riječ u rečenici je najčešće I ili A, i u rijetkim prilikama O.

5. Riječ s dva slova koja se najčešće javlja u rečenici je OF, a zatim TO i IN.

6. Najčešće korištena riječ od tri slova je THE, a zatim AND.

7. Poslije Q uvijek dolazi U.

8. Suglasnik koji najčešće dolazi iza samoglasnika je N.

9. Najčešći bigrami su redom: LL, EE, SS, OO, TT, FF, RR, NN, PP i CC.

10. Najčešća riječ od četiri slova je THAT.

Napomena: riječ THAT ima ista slova na početku i na kraju. Kada se isto slovo više puta javlja u jednoj riječi, radi se o riječi koja je uzorak. U rješavanju kriptograma, takve riječi imaju neprocjenjivu vrijednost.

Na primjer, pretpostavimo da se u kriptogramu javlja riječ XPP. Vrlo je vjerojatno da je to česta i uobičajena riječ kao što su ALL, SEE ili TOO, iako bi mogla biti i jedna od rjeđe korištenih riječi, kao što su ODD, ADD, BOO, INN, EGG, ZOO i još mnogo drugih. Kao što smo već spomenuli, XYZX je vrlo vjerojatno riječ THAT.

Uzorak od pet slova kao što je BDCKC je vjerojatno riječ THERE, ili WHERE ili THESE, iako postoji mogućnost da je jedna od stotina manje korištenih riječi kao što su NIECE, ROSES, NOSES, OMAHA ili IRENE.

Uzorak ABCDB je vjerojatno WHICH. RDMMRJ je uzorak u kojem se dva slova, R i M ponavljaju, i po svemu sudeći, radi se o riječi LITTLE. Manje vjerojatne mogućnosti su SNEESH, SWOOSH i TWEETS.

Iskusni rješavatelj kriptograma će brzo prepoznati riječi uzorke kao što su TOMORROW, PEOPLE, BANANA, BEGINNING, COMMITTEE i mnoge druge. Ako je kriptogram nečiji citat, popraćen imenom autora, iskusniji rješavatelji će RBKJDRLDKMD prepoznati kao SHAKESPEARE.

Jedan od najvrjednijih alata kojima se kriptograf-amater može služiti je tablica najčešćih riječi-uzoraka, složenih na način da se uzorak može brzo pronaći, i naučiti riječi koje su najčešća rješenja. Kratka lista ovakvih tablica uključena je u knjizi *"Secret and urgent"* Fletchera Pratta. Potpune liste (za sve glavne svjetske jezike) su u računalnim programima vladinih kriptoanalitičara. 1971. godine Jack Levine, profesor matematike na sveučilištu North Carolina State, objavio je popis od 184 tisuće riječi-uzoraka duljine od dva do devet slova. Popis je složilo računalo i prošireno je 1972. godine s riječima od deset do šesnaest slova. Riječi koje nemaju uzorak objavljene su još prije 1957. godine u knjizi *"A List of Words Containing No Repeated Letters"*.

Još jedan kriptografima koristan popis je tzv. obrnuti rječnik. Za razliku od klasičnog rječnika u kojima su riječi abecedno složene prema slovima na koja one počinju, u obrnutom rječniku one su abecedno složene prema slovima na koje završavaju. Ako znate riječ koja završava na CION, u rječniku ćete potražiti riječi koje počinju na NOIC. A. F. Brown, profesor lingvistike na sveučilištu u Pennsylvaniji, predvodio je slaganje upravo takvog rječnika objavljenog 1963. godine u 8 svezaka naslova *"Normal and Reverse English Word List"* s preko 350 tisuća unosa. Slični rječnici objavljeni su i u Francuskoj, Grčkoj, Rusiji, Italiji i mnogim drugim državama.

Tehnika rješavanja kriptograma sastoji se od pogađanja određenih riječi, te supstitucijom slova u šifriranoj riječi kako bi se istražilo je li pogađanje dalo smislenu riječ, ili vodi u besmislenu kombinaciju slova. Ako se dogodi potonje, potrebno je krenuti dalje s novom rječju. *"The Gold Bug"* sadrži odličan opis kako riješiti kriptogram, a detaljnije informacije mogu se naći u knjizi *"Cryptanalysis"* autorice Helen Gaines.

Proučimo jednostavan, poznat citat iz djela popularnog engleskog pisca:

ZU HO UD CUZ ZU HO ZSGZ AE ZSO JKOEZAUC

Kriptogram je tako kratak da se ne možemo osloniti na informaciju da je slovo E najčešće slovo u engleskom jeziku. Najbolji način pristupa ovom kriptogramu je kroz riječ ZSGZ, u kojoj se slovo Z ponavlja na početku i kraju, te je ona stoga najbolji kandidat za riječ THAT. Primijenimo supstituciju otkrivenu kroz tu riječ na ostatak teksta:

T-	- -	- -	- -T	T-	- -	THAT	- -	TH-	- - - -T- - -
ZU	HO	UD	CUZ	ZU	HO	ZSGZ	AE	ZSO	JKOEZAUC

Tablica 7: U tablici vidimo kako slovo Z zapravo znači T u ovom slučaju

Na dobrom smo tragu, jer sada možemo zaključiti da je ZSO gotovo sigurno riječ THE, a ZU je gotovo sigurno TO. S novootkrivenim slovima E i O dobijamo:

TO	- E	O -	- OT	TO	- E	THAT	- -	THE	- - - ET-O-
ZU	HO	UD	CUZ	ZU	HO	ZSGZ	AE	ZSO	JKOEZAUC

Tablica 8: U tablici vidimo kako slovo U zapravo znač O, a O je E u ovom slučaju

Četvrta riječ završava na OT. Ovdje postoji mnogo mogućnosti. C, prvi simbol riječi, ne može biti H jer je H već otkriveno slovo (mijenja ga slovo S u kriptogramu). Primijetite kako posljednja riječ kriptograma završava slovom C. TION je čest završetak riječi u engleskom jeziku. Ako supstituiramo TION u posljednjoj riječi, C postaje N, i tada CUZ postaje NOT. Dodamo li nova slova I i N u poruku, kriptirana rečenica ima puno više smisla:

TO	- E	O -	NOT	TO	- E	THAT	I-	THE	- - - E-TION
ZU	HO	UD	CUZ	ZU	HO	ZSGZ	AE	ZSO	JKOEZAUC

Tablica 9: U tablici vidimo kako se uz pomoću karateristika jezika otkriva dio šifre

AE ne može biti IT, jer je T već otkriveno slovo. IF stilski ne pristaje između THAT i THE, ali IS odgovara, pa ako dodamo S u rješenje, poruka glasi:

TO	- E	O -	NOT	TO	- E	THAT	IS	THE	- - - ESTION
ZU	HO	UD	CUZ	ZU	HO	ZSGZ	AE	ZSO	JKOEZAUC

Tablica 10: U tablici vidimo kako se uz pomoću karateristika jezika otkriva dio šifre

Uz opću kulturu i temeljno poznavanje engleske književnosti, jedino rješenje koje se nameće je Hamletov popularni citat iz istoimene drame Williama Shakespearea **TO BE OR NOT TO BE THAT IS THE QUESTION** (Biti ili ne biti, pitanje je sad). Iako vrlo jednostavan za rješavanje, ovaj kriptogram daje općenitu sliku o otkrivanju slova i rješavanju riječi i rečenica šifriranih jednostavnim supstitucijskim kôdovima.

Claude E. Shannon, američki matematičar koji je osnovao komunikacijsku teoriju, granu moderne matematike, napisao je važan rad 1949. godine (*"Communication Theory of Secrecy Systems"*, Bell Technical Journal, October, 1949) u kojem je pokazao da ako kriptogram ima 30 ili više slova, gotovo je sigurno da može imati jedinstveno rješenje. Ako ima 20 ili manje znakova, postoji mogućnost da ima više od jednog rješenja.

Slavni njemački filozof i matematičar Gottfried Leibnitz je pokazao da je rješavanje kriptograma slično rješavanju znanstvenih problema. Ako znanstvenik ima dvije ili tri nepovezane činjenice o prirodi koje mora objasniti teorijom, smislit će na desetke ispravnih teorija, isto kao što kriptograf može osmisliti na desetke rješenja za jednu kratku riječ. Ali ako postoji velik broj činjenica koje treba objasniti, situacija nije puno drugačija od rješavanja dugog kriptograma. Nije jednostavno osmisliti jednu teoriju koja će objasniti stotine različitih činjenica koje su prethodno bile tajanstvene i nejasne. Kada se osmisli teorija koja objašnjava sve činjenice, vjerojatno je ispravna i točna, iz razloga sličnog onom koji pojašnjava da je rješenje dugog kriptograma točno ako ispravno dekriptira sve simbole i znakove.

Jedno od najvećih znanstvenih otkrića u povijesti sadrži pravi prirodni kôd onaj genetski. On nosi plan za razvoj živih bića kroz dvije isprepletene molekule DNA u jezgri svake žive stanice. Genetski kôd ima abecedu od samo četiri simbola, od kojih svaki označava različitu kemikaliju. Te četiri kemikalije složene su kroz DNA molekule u grupe od po tri člana. Te trojke su "riječi" nevjerojatno duge "rečenice" koja govori svakoj stanici u organizmu što točno treba raditi i kakva joj je uloga.

Edgar Allan Poe u svom djelu *"The Gold Bug"* i u svojem eseju o kriptografiji je pojasnio da svaka šifra koju osmisli "ljudska domišljatost" se isto tako može probiti istom tom ljudskom domišljatošću. Poe je u pravu, uz nekoliko ispravaka. Šifra mora biti praktična, to jest, proces šifriranja i točnog dešifriranja ne smije trajati predugo. Uz to, kriptoanalitičar mora imati dovoljnu količinu kôdiranog teksta na kojem može raditi, kao i dovoljno vremena. Da je Poe sve ovo uzeo u obzir, njegova teorija još uvijek nije niti potpuno točna niti potpuno netočna.

U svakom slučaju, moguće je stvoriti neprobojne šifre koje su nepraktične, osim u iznimnim situacijama. *"The Codebreakers"* posvećuje poglavlje izvanrednom stroju kojeg je izumio Amerikanac Gilbert S. Vernam. Njegov uređaj proizvodi neprobojnu šifru jer koristi ono što kriptografi zovu jednostruki sustav. Uređaj koristi jedan te isti potpuno nasumični ključ samo jednom, i nikada više. U Kahnovom odličnom članku o kriptologiji u *"The Encyclopedia Americana"* opisan je jednostavan jednostruki sustav, šifra koju su koristili komunistički agenti u 2. svjetskom ratu koja je uistinu neprobojna. Zašto se onda ne koristi češće? Zato što njena kompliciranost i potreba za generiranjem ključa za svaku šifru nije praktična za svakodnevnu uporabu.

Niže je ilustracija Rudyarda Kiplinga za djelo *"The First Letter"*, jednu od priča u njegovoj slavnoj knjizi za djecu *"Just So Stories"*. Slika prikazuje kljovu od bjelokosti u kojoj su izrezbarene slike o djevojčici imena Taffimai. Kipling kaže da su čudni simboli s obje strane magična runska slova, no oni su zapravo simboli za supstitucijsku šifru.

Možete li pročitati Kiplingovu šifru?
Napomena: postoji nekoliko specifičnih pravopisnih izmjena u izvornom tekstu: YOU je napisano kao U, W je ili izostavljeno ili zamijenjeno s OU, F zamjenjuje V, a I se koristi umjesto Y. Uz to, A, G, O i T imaju svaki po dva simbola, a H ima tri.
Tekst s lijeve strane započinje ovako: **THIS IS THE STORY OF TAFFIMAI, ALL RITTEN OUT ON AN OLD TUSK**.

Slika 12: "The First Letter"

Literatura

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

[2] H. Fouche Gaines, Cryptanalysis a study of ciphers and their solution, Dover Publication, New York, 1956.

[3] M. Gardner, Codes, ciphers and secret writing, Dover Publications, Inc. New York, 1972.

[4] I. Matić, Uvod u teoriju brojeva, skripta, Odjel za matematiku, Sveučilište J.J. Strossmayera, Osijek, 2013.

[5] Ž. Panian, Poslovna informatika, Koncepti, metode i tehnologija, Potecon d.o.o, Zagreb, 2001.

[6] J. R. Vacca, Computer and Information Security Handbook, Morgan Kaufmann, Waltham, Massachusetts, 2013.

[7] http://web.zpr.fer.hr/ergonomija/2005/galinovic/literatura.html, 20.9.2015

[8] http://www.enciklopedija.hr/natuknica.aspx?ID=33988, 27.4.2016.

[9] https://hr.wikipedia.org/wiki/Kriptografija, 24.7.2015.