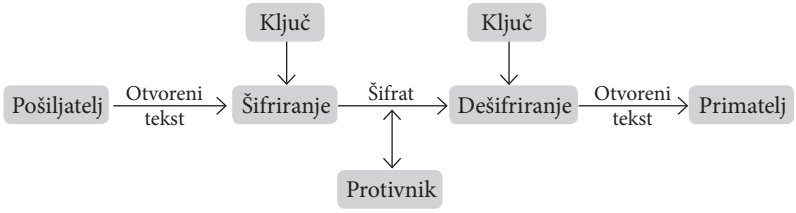
SKRIVENE PORUKE

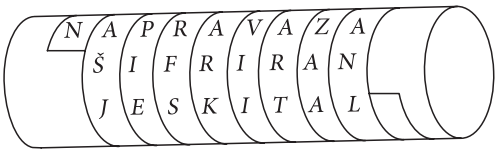
Andreja Igrec, Čakovec

Ljudi su od davnina željeli sigurno komunicirati. Poruke koje su slali bilo je potrebno zaštiti tako da samo primatelj može doznati njezin sadržaj. Kroz povijest su se načini prenošenja poruka mijenjali, ali problem zaštite sadržaja ostao je isti. Načinima slanja poruka u takvome obliku da ih može pročitati samo onaj kome su namijenjene bavi se znanstvena disciplina *kriptografija*. Sama riječ *kriptografija* grčkog je podrijetla i može se prevesti kao *tajnopis*. Poruka koju pošiljatelj želi poslati u kriptografiji se naziva *otvoreni tekst*. Kako bi zaštitio sadržaj poruke, pošiljatelj transformira otvoreni tekst pomoću unaprijed dogovorenog *ključa*. Taj postupak naziva se šifriranje, a rezultat je šifrirana poruka, tj. šifrat ili *kriptogram*. Šifrat se zatim šalje primatelju. Protivnik može prisluškivanjem doznati tekst šifrata, ali ako ne posjeduje dogovoreni ključ, ne može saznati otvoreni tekst (tj. sadržaj poruke). Za razliku od protivnika, primatelj zna ključ kojim je poruka šifrirana pa može *dešifrirati* šifrat te na taj način odrediti otvoreni tekst. Na slici 1. prikazana je shema kriptografije.



Slika 1. Shema kriptografije

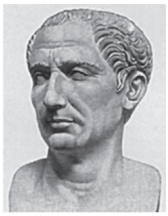
Kriptografija je bila prisutna već u vrijeme starih Grka. Spartanci su u 5. stoljeću prije Krista koristili jednostavnu napravu za šifriranje – *skital*. To je bio drveni štap oko kojega se namatala vrpca od kože ili pergamenta, onako kako je to prikazano na slici 2. Pošiljatelj na toj namotanoj vrpci napiše poruku, a kad se ta vrpca odmota, na njoj je samo niz naizgled besmislenih slova. Sada glasnik odnosi odmotanu vrpcu primatelju, a primatelj čita tekst poruke tako što tu vrpcu omota oko skitala jednakog promjera kao što je promjer skitala pošiljatelja. Dakle, ključ je bio skital određenog promjera.



Slika 2. Skital s omotanom vrpcom i napisanom porukom

Postoji podatak da se 404. godine prije Krista pred Lisandrom Spartancem pojavio glasnik, jedini od petorice koji je preživio mukotrpan put iz Perzije. Glasnik mu je predao vrpcu sa slovima, a Lisandar je pomoću skitala tako doznao da ga Farnabas Perzijski kani napasti. Zahvaljujući skitalu Lisandar se mogao pripremiti za napad i uspješno ga odbiti.

Šifriranjem se služio i znameniti rimski vojskovođa i državnik Gaj Julije Cezar. On je u komunikaciji sa svojim prijateljima poruke šifrirao tako da je slova otvorenog teksta zamijenio slovima koja su se nalazila tri mjesta dalje od njih u abecedi[1]. Koristimo li današnju englesku abecedu, slovo A bismo zamijenili slovom D, slovo B slovom E i tako dalje. U tablici se nalazi današnja engleska abeceda, a ispod nje je napisana šifrirana abeceda, tj. ispod svakog slova originalne abecede nalazi se slovo kojim se to slovo originalne abecede zamjenjuje prilikom šifriranja. Ovakav način šifriranja naziva se ***Cezarova šifra***.



Slika 3. Gaj Julije Cezar

Originalna abeceda	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
Šifrirana abeceda	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

Primjer 1. Šifrirajmo poznatu Cezarovu izreku *Veni Vidi Vici* pomoću Cezarove šifre.

Rješenje: Otvoreni tekst glasi: VENI VIDI VICI

Pomoću gornje tablice zamijenimo slova pa dobivamo: YHQL YLGL YLFL

Dakle, šifrat glasi: YHQL YLGL YLFL

Zadatak 1. Šifrirajte tekst GAJ JULIJE CEZAR pomoću Cezarove šifre.

Zadatak 2. Dešifrirajte šifrat DOHD LDFWD HVW ako je poznato da je šifriranje izvršeno Cezarovom šifrom.

Zadatak 3. Dešifrirajte šifrat DWODQWLGD MH VWYDUQD ako je poznato da je šifriranje izvršeno Cezarovom šifrom.

Cezarova šifra s vremenom je postala manje sigurna jer su uz razvoj kriptografije napredovale i metode za čitanje skrivenih poruka bez poznavanja ključa. Zbog toga se javila potreba za smišljanjem jače, nove šifre. Jednu takvu šifru razvio je u 16. stoljeću Blaise de Vigenère. ***Vigenèreova šifra*** umjesto jedne šifrirane abecede koristi 26 šifriranih abeceda.

Slika 4. Blaise de Vigenère

Prvi korak u šifriranju ovom šifrom je crtanje Vigenèreovog kvadrata prikazanog na slici 5. U prvom retku napisana je originalna engleska abeceda, a ispod nje 26 šifriranih abeceda napisanih na način da je svaka od njih pomak-

[1]O šifriranju pomoću Cezarove i Vigenèreove šifre možete pročitati i u članku *Kako šifrirati poruku?* autorice Jelene Hunjadi u prošlom broju Matke

Otvorena abeceda:	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
1	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
2	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
3	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
4	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
5	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
6	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
7	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
8	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
9	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
10	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
11	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
12	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
13	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
14	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
15	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
16	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
17	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
18	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
19	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
20	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
21	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
22	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
23	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
24	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
25	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
26	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

Slika 5. Vigenèreov kvadrat

nuta za jedno slovo u odnosu na prethodnu. Ako na primjer posegnemo za šifriranom abecedom broj 2, onda slovo A šifriramo kao C, no ako to učinimo pomoću abecede broj 12, onda isto slovo šifriramo kao M. Po Vigenèreovoj metodi različita se slova poruke šifriraju pomoću različitih redaka (tj. različitih šifriranih abeceda) njegova kvadrata. Na primjer, pošiljatelj može prvo slovo poruke šifrirati pomoću 5. retka, drugo pomoću 17. retka, treće pomoću 23. retka, i tako dalje. Da bi odgonetnuo poruku, primatelj mora znati pomoću kojeg je retka Vigenèreovog kvadrata šifrirano koje slovo. Dakle, mora postajati nekakvo dogovoreno pravilo o izmjeni redaka. To pravilo bilo je sadržano u nekoj ključnoj riječi koja je bila poznata samo pošiljatelju i primatelju. Pokažimo na primjeru kako se šifrira Vigenèreovom šifrom.

Primjer 2. Šifrirajmo BLAISE DE VIGENERE Vigenèreovom šifrom uz dogovorenu ključnu riječ CVIJET.

Rješenje: Otvoreni tekst glasi: BLAISE DE VIGENERE, a ključna riječ je: CVIJET

Kako bismo šifrirali zadani tekst, prvo ključnu riječ ispisujemo više puta iznad teksta poruke tako da se iznad svakog slova otvorenog teksta nalazi jedno slovo ključne riječi:

C	V	I	J	E	T	C	V	I	J	E	T	C	V	I	J
B	L	A	I	S	E	D	E	V	I	G	E	N	E	R	E

Kako šifriramo pojedino slovo otvorenog teksta, govori nam slovo ključnog teksta koje se nalazi iznad tog slova. Dakle, prvo slovo otvorenog teksta, B, šifriramo pomoću šifrirane abecede koja počinje ključnim slovom C. To je 2. šifrirana abeceda i po toj abecedi slovu B odgovara slovo D.

Drugo slovo otvorenog teksta, L, šifriramo pomoću šifrirane abecede koja počinje ključnim slovom V. To je 21. šifrirana abeceda i po toj abecedi slovu L odgovara slovo G. Na isti način šifriramo ostala slova otvorenog teksta:
Treće slovo otvorenog teksta, A, šifriramo pomoću 8. šifrirane abecede. (A→I)
Četvrto slovo, I, šifriramo pomoću 9. šifrirane abecede. (I→R)
Peto slovo, S, pomoću 4. šifrirane abecede. (S→W)
Isto tako ostala slova:
(E→X), (D→F), (E→Z), (V→D), (I→R), (G→K), (E→X), (N→P), (E→Z), (R→Z), (E→N)
Na kraju dobivamo šifrat: DGIRWX FZ DRKXPZZN

Zadatak 4. Šifrirajte tekst DIJAMANTI SU SKRIVENI UNUTAR POTPETICE pomoću Vigenèreove šifre, uz dogovorenu ključnu riječ KRIPTOGRAFIJA.

Zadatak 5. Dešifrirajte šifrat FFTXFAGKERICIUL ako je poznato da je šifriranje izvršeno Vigenèreovom šifrom pomoću ključne riječi KRIPTOGRAFIJA.

Zadatak 6. Dešifrirajte šifrat EVFDEYJTYQBUROYPNNINI ako je poznato da je šifriranje izvršeno Vigenèreovom šifrom pomoću ključne riječi PENKALA.

Osim Vigenèreove šifre, jedna od ideja poboljšanja šifriranja je i ***Playfairova šifra***. Playfairovu je šifru 1854. godine smislio britanski znanstvenik Charles Wheatstone, a ime je dobila po njegovom prijatelju barunu Playfairu od St. Andrewsa koji ju je popularizirao. Playfairova šifra temelji se na tablici slova, koja se konstruira koristeći ključnu riječ. Na primjer, ako je ključna riječ PLAYFAIR, onda tablica izgleda ovako (slika desno):

Budući da u tablicu 5 × 5 stane 25 slova, a engleska abeceda sadrži 26 slova, dogovor je da se slova I i J poistovjete, tj. šifriraju se jednako. (U slučaju da je otvoreni tekst na hrvatskom jeziku, onda se poistovjećuju slova V i W kako bi se izbjegli mogući nesporazumi prilikom dešifriranja.) Dakle, 5 × 5 tablicu popunjavamo na sljedeći način: prvo upisujemo ključnu riječ tako da pišemo svako slovo samo jednom (npr. ako se slovo A pojavljuje više puta, upisat ćemo samo ono prvo, a ostala ćemo preskočiti), a zatim upisujemo redom ostala slova abecede uz preskakivanje slova koja su već se pojavila u ključnoj riječi. Nakon što smo napravili 5 × 5 tablicu uz pomoć dogovorene ključne riječi, možemo šifrirati poruku. Tekst poruke najprije treba podijeliti na blokove po dva susjedna slova. Pritom treba paziti da se niti jedan blok ne sastoji od dva jednaka slova, te da tekst ima paran broj slova. Ukoliko se u tekstu pojavi blok s dva jednaka slova ili je u tekstu neparan broj slova, oba problema možemo riješiti umetanjem npr. slova X. Ovisno o položaju slova iz blokova u 5 × 5 tablici, kod šifriranja bloka od dva slova mogu nastupiti tri slučaja:

Slika 6. Charles Wheatstone

Slika 7. Barun Playfair

- Ako se slova iz bloka u tablici pojavljuju u istome retku, zamjenjujemo ih slovima koja se nalaze za jedno mjesto udesno. Npr. u našem bismo slučaju imali sljedeće zamjene: CR→DB, ST→TN, FP→PL.
- Ako se slova iz bloka u tablici pojavljuju u istome stupcu, zamjenjujemo ih slovima koja se nalaze za jedno mjesto ispod. Npr. OV→VL, GR→OG, PI→IE.
- Ako se slova iz bloka u tablici ne nalaze u istome retku ili stupcu, onda pogledamo pravokutnik koji određuju ta dva slova te ih zamijenimo s preostala dva vrha tog pravokutnika. Redoslijed zamjenskih slova određen je tako da prvo dođe slovo koje se nalazi u istome retku kao prvo slovo u polaznome bloku. Npr. OC→SR, HY→KA, PD→FI, HJ→EB.

Primjer 3. Šifrirajmo riječ CRYPTOGRAPHY pomoću Playfairove šifre s ključnom riječi PLAYFAIR.

Rješenje: Otvoreni tekst glasi CRYPTOGRAPHY, a ključna je riječ PLAYFAIR.

Prvo podijelimo otvoreni tekst na blokove po dva slova:

CR YP TO GR AP HY

5 × 5 tablica jednaka je gornjoj tablici jer je ključna riječ ista.

Sada zamijenimo blokove slova:

Blok CR: slova C i R nalaze se u istome retku pa šifrirani blok glasi DB.

Blok YP: slova Y i P nalaze se također u istome retku pa njihov šifrirani blok glasi FL.

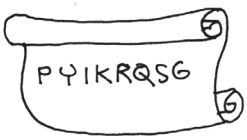
Na isti način mijenjaju se blokovi TO→NQ i AP→YL.

Blok GR: slova G i R nalaze se u istome stupcu pa šifrirani blok glasi OG.

Blok HY: gledamo pravokutnik koji čine slova H i Y. Šifrirani blok tada je KA.

Na kraju dobijemo šifrat: DB FL NQ OG YL KA.

Zadatak 7. Šifrirajte riječ MATHEMATICS pomoću Playfairove šifre uz dogovorenu ključnu riječ PLAYFAIR.



Zadatak 8. Dešifrirajte šifrat PYIKRQSG ako je poznato da je šifriranje izvršeno Playfairovom šifrom pomoću ključne riječi PLAYFAIR. (Uputa: slova I i J se poistovjećuju.)

Zadatak 9. Dešifrirajte šifrat IRTOKPAYTI ako je poznato da je šifriranje izvršeno Playfairovom šifrom pomoću ključne riječi PLAYFAIR. (Uputa: slova I i J se poistovjećuju.)

Playfairova šifra bila je standardna šifra u britanskoj vojsci za vrijeme 1. svjetskog rata, a čak je bila korištena i u američkoj vojsci u 2. svjetskom ratu, ali za šifriranje manje važnih poruka.

Daljnjim razvojem kriptografije nastala je 1929. godine ***Hillova šifra*** koju je izumio Lester Hill. Ova šifra temelji se na invertibilnim matricama. Matricu možemo zamisliti kao tablicu brojeva. Primjer jedne invertibilne matrice 3 × 3 (što znači da matrica ima 3 retka i 3 stupca):

$$\begin{bmatrix} 5 & 8 & 22 \\ 2 & 5 & 24 \\ 10 & 20 & 17 \end{bmatrix}$$

Šifriranje Hillovom šifrom provodi se na način da se najprije slova teksta gupiraju po tri. Ukoliko broj slova otvorenog teksta nije djeljiv brojem 3, trebamo dodati onoliko slova koliko nedostaje da bismo mogli imati 3 slova u svakome bloku. Najčešće se dopiše zadnje slovo teksta tako da se mogu formi-

rati blokovi od po 3 slova. (Slova dijelimo u blokove po tri zbog toga što smo izabrali matricu 3×3. U slučaju da je izabrana matrica s više od tri retka i stupaca, npr. 5 redaka i stupaca, onda bismo grupirali po pet slova.) Zatim se svako slovo teksta zamijeni rednim brojem tog slova u abecedi. U sljedećoj tablici prikazana su slova engleske abecede i brojevi kojima odgovara pojedino slovo.

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

Nakon što smo blokove zamijenili brojevima, brojčane blokove množimo zadanom matricom. Dobijemo nove brojeve kojima opet, uz pomoć gornje tablice, pridružimo slova i dobijemo šifrat. Pokažimo na konkretnom primjeru kako se šifrira Hillovom šifrom.

Primjer 4. Šifrirajmo tekst SKRIVAM SE Hillovom šifrom i koristeći istu gornju matricu.

Rješenje: Otvoreni tekst glasi: SKRIVAM SE. Koristit ćemo gornju matricu i tablicu.

Podijelimo slova u blokove od 3 slova: SKR IVA MSE.

Zamijenimo blokove brojevima (zapravo matricama s jednim retkom i tri stupca):

Blok SKR zamjenjujemo matricom $\begin{bmatrix}18 & 10 & 17\end{bmatrix}$.

Blok IVA zamjenjujemo matricom $\begin{bmatrix}8 & 21 & 0\end{bmatrix}$.

Blok MSE zamjenjujemo matricom $\begin{bmatrix}12 & 18 & 4\end{bmatrix}$.

Sada računamo umnožak dobivenih matrica sa zadanom matricom:

Matrice množimo prema sljedećem pravilu:

$$\begin{bmatrix}a & b & c\end{bmatrix}\cdot\begin{bmatrix}d & e & f\\ g & h & i\\ j & k & l\end{bmatrix}=\begin{bmatrix}ad+bg+cj & ae+bh+ck & af+bi+cl\end{bmatrix}$$

$$\begin{bmatrix}18 & 10 & 17\end{bmatrix}\cdot\begin{bmatrix}5 & 8 & 22\\ 2 & 5 & 24\\ 10 & 20 & 17\end{bmatrix}=\begin{bmatrix}280 & 534 & 925\end{bmatrix}$$

$$\begin{bmatrix}8 & 21 & 0\end{bmatrix}\cdot\begin{bmatrix}5 & 8 & 22\\ 2 & 5 & 24\\ 10 & 20 & 17\end{bmatrix}=\begin{bmatrix}82 & 169 & 680\end{bmatrix}$$

$$\begin{bmatrix}12 & 18 & 4\end{bmatrix}\cdot\begin{bmatrix}5 & 8 & 22\\ 2 & 5 & 24\\ 10 & 20 & 17\end{bmatrix}=\begin{bmatrix}136 & 266 & 764\end{bmatrix}$$

Brojevi u dobivenim matricama veći su od 26. Kako imamo 26 slova, trebamo pronaći ostatke pri dijeljenju tih brojeva brojem 26, a nakon toga tim ostatcima pridružiti slova pomoću gornje tablice.

280 : 26 = 10 i ostatak 20, a broj 20 odgovara slovu U.
534 : 26 = 20 i ostatak 14, a broj 14 odgovara slovu O.
925 : 26 = 35 i ostatak 15, a broj 15 odgovara slovu P.

82 : 26 = 3 i ostatak 4, a broj 4 odgovara slovu E.
169 : 26 = 6 i ostatak 13, a broj 13 odgovara slovu N.
680 : 26 = 26 i ostatak 4, a broj 4 odgovara slovu E.

136 : 26 = 5 i ostatak 6, a broj 6 odgovara slovu G.
266 : 26 = 10 i ostatak 6, a broj 6 odgovara slovu G.
764 : 26 = 29 i ostatak 10, a broj 10 odgovara slovu K.

Dakle, šifrat glasi UOPENEGGK.

Zadatak 10. Šifrirajte riječ UTORAK Hillovom šifrom koristeći istu matricu kao i u primjeru 4.

Ovo su samo neke od šifra koje su se razvile tijekom povijesti. Do današnjeg dana pojavilo se još mnogo šifra koje su složenije. Budućnost kriptografije danas je povezana s budućnošću računala. Računala su sve brža i brža, a razvoj svega vezanog uz njih sve je teže pratiti.

Literatura:

1. Singh, S. (2003.). Šifre (Kratka povijest kriptografije). Zagreb: Mozaik knjiga
2. Dujella, A., Maretić, M. (2007.). *Kriptografija*. Zagreb: Element
3. http://web.math.pmf.unizg.hr/~duje/kript/osnovni.html (17. 10. 2015.)
4. http://web.math.pmf.unizg.hr/~duje/kript/supst.html (17. 10. 2015.)
5. http://web.math.pmf.unizg.hr/~duje/kript/vigener.html (17. 10. 2015.)
6. http://web.math.pmf.unizg.hr/~duje/kript/playfair.html (17. 10. 2015.)
7. https://hr.wikipedia.org/wiki/Kriptografija (17. 10. 2015.)

Rješenja zadataka provjerite na stranici 285.