Kriptografija i kriptoanaliza

izv. prof. dr. sc. Ante Đerek i prof. dr. sc. Marin Golub

listopad 2025.

Sadržaj

1. Uvod u kriptografiju i kriptoanalizu
2. Simetrični kriptosustavi (DES, 3DES, IDEA, AES)
3. Funkcije za izračunavanje sažetka poruke (MD5, SHA)
4. Autentifikacijsko kriptiranje
5. Napadi na kriptosustave, kriptoanaliza
6. Asimetrični kriptosustavi (RSA, ECC)
   - Digitalni potpis: RSA digitalni potpis i DSA
7. Kriptografija prilagođena računalima s ograničenim mogućnostima (Lightweight Crypto)
8. Kvantna i post-kvantna kriptografija

Literatura

[1] Christof Paar, Jan Pelzl, ***Understanding Cryptography***, Springer-Verlag Berlin Heidelberg, 2009.

[2] L. Budin, M. Golub, D. Jakobović, L. Jelenković, *Sigurnost računalnih sustava*, poglavlje u knjizi ***Operacijski sustavi***, Element, Zagreb, 3. izdanje 2013.

[3] ***Sigurnost računalnih sustava, zbirka studentskih radova***, dostupno na Internet adresi: http://sigurnost.zemris.fer.hr

1.
Uvod u kriptografiju i kriptoanalizu

- Osnovni pojmovi
- Prijetnje i napadi
- Podjela kriptografskih algoritama
- Jesu li i koliko su kriptografski algoritmi sigurni?

Osnovni pojmovi

Kriptologija = kriptografija + kriptoanaliza

Kriptografija

- znanstvena disciplina (ili umjetnost?) sastavljanja poruka sa ciljem skrivanja sadržaja poruka

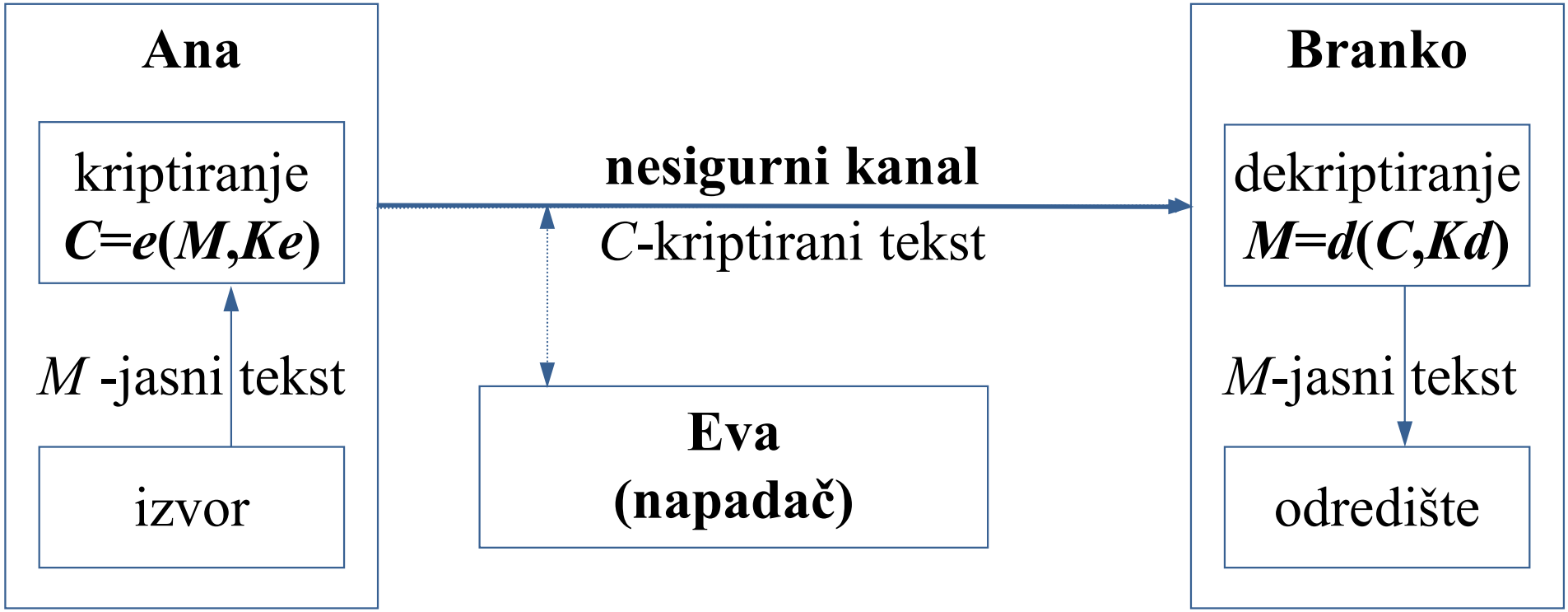
Kriptoanaliza

- znanstvena disciplina koja se bavi analizom skrivenih aspekata sustava i koristi se kako bi se ispitala (ili narušila) sigurnost kriptografskog sustava

Kriptoanaliza

- izvedenica iz grčkih riječi
  - *kryptós* – skriven i
  - *analýein* – rastavljati
- analiza informacijskog sustava u svrhu pronalaska skrivenih aspekata sustava
- obuhvaća primjerice
  - diferencijalnu kriptoanalizu
  - linearnu kriptoanalizu
  - analizu propusta u implementaciji
- uspješnost kriptoanalize ocjenjuje se uspoređivanjem s napadom grubom silom odnosno ispitivanjem svih mogućih ključeva

Osnovni pojmovi i oznake



Na ovom će se predmetu pojmovi kriptiranje i šifriranje koristiti na sljedeći način:

- šifriranje/dešifriranje - klasična kriptografija
- kriptiranje/dekriptiranje - moderna kriptografija

Kratko ponavljanje gradiva iz predmeta Sigurnost računalnih sustava

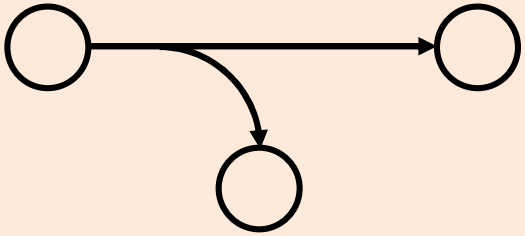
Osnovni pojmovi

identifikacija = predstavljanje

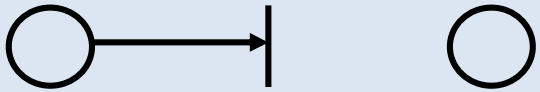
autentifikacija = identifikacija + verifikacija

autorizacija = autentifikacija + provjera prava pristupa

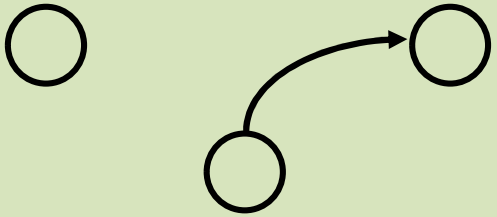
Prijetnje i napadi



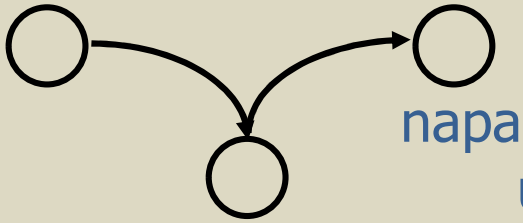
1. prisluškivanje
2. prekidanje



3. lažno predstavljanje



4. ponovno odašiljanje snimljenih starih paketa
5. modifikacija paketa



napad čovjek u sredini

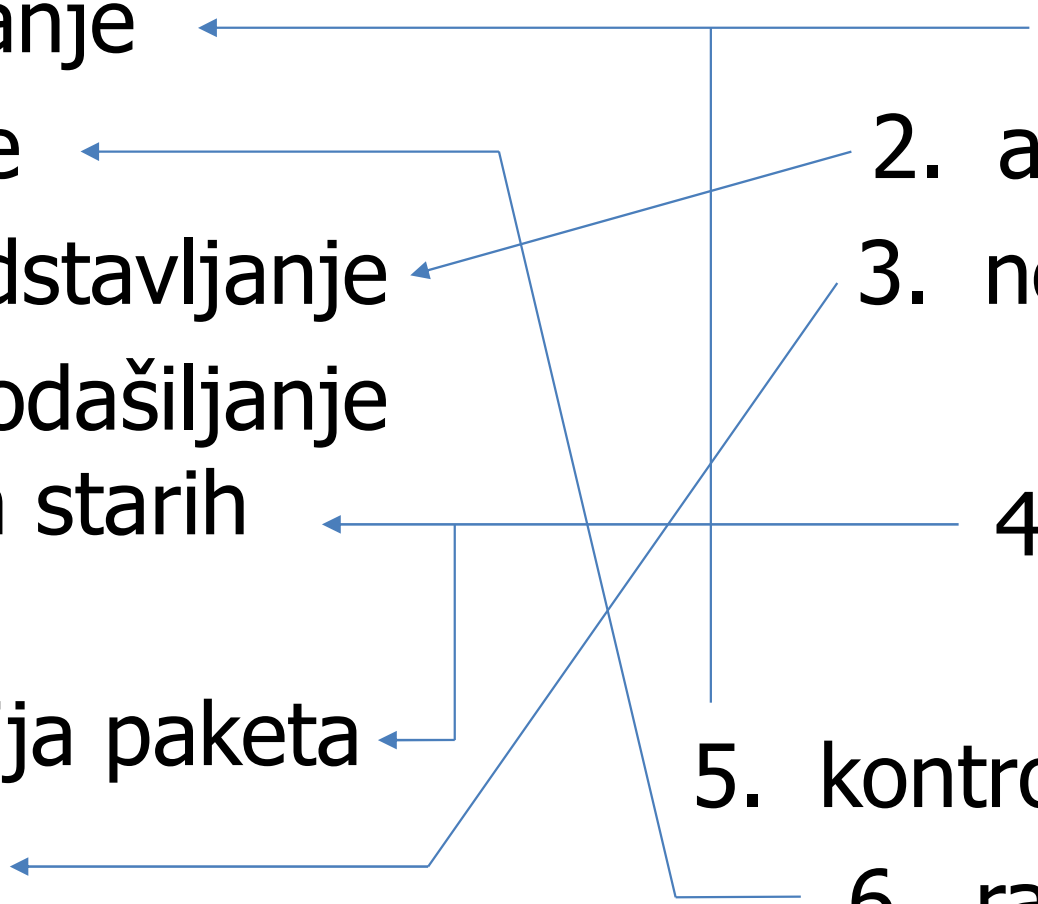
6. poricanje

Prijetnje i napadi

1. prisluškivanje
2. prekidanje
3. lažno predstavljanje
4. ponovno odašiljanje snimljenih starih paketa
5. modifikacija paketa
6. poricanje

Sigurnosni zahtjevi

1. tajnost
2. autentičnost
3. neporecivost
4. integritet
5. kontrola pristupa
6. raspoloživost



Sigurnosni zahtjev: **povjerljivost**

- pojam koji se koristi primjerice u kratici *CIA*
  (engl. *Confidentiality, Integrity and Availability*)
- sigurnosni zahtjev koji štiti informacije od neautoriziranog pristupa
  - tj. samo autorizirani korisnici smiju pristupiti osjetljivim podacima
- ostvaruje se kombinacijom autentičnosti i tajnosti ali i provjerom prava pristupa
- povjerljivost ≠ tajnost
  - mada se ta dva pojma često poistovjećuju
  - povjerljivost se može ostvariti uz pomoć tajnosti
- ali, može se ostvariti i bez tajnosti, npr.:
  - samo uz pomoć osiguravanja autentičnosti i provjere prava pristupa

Podjela kriptografskih algoritama

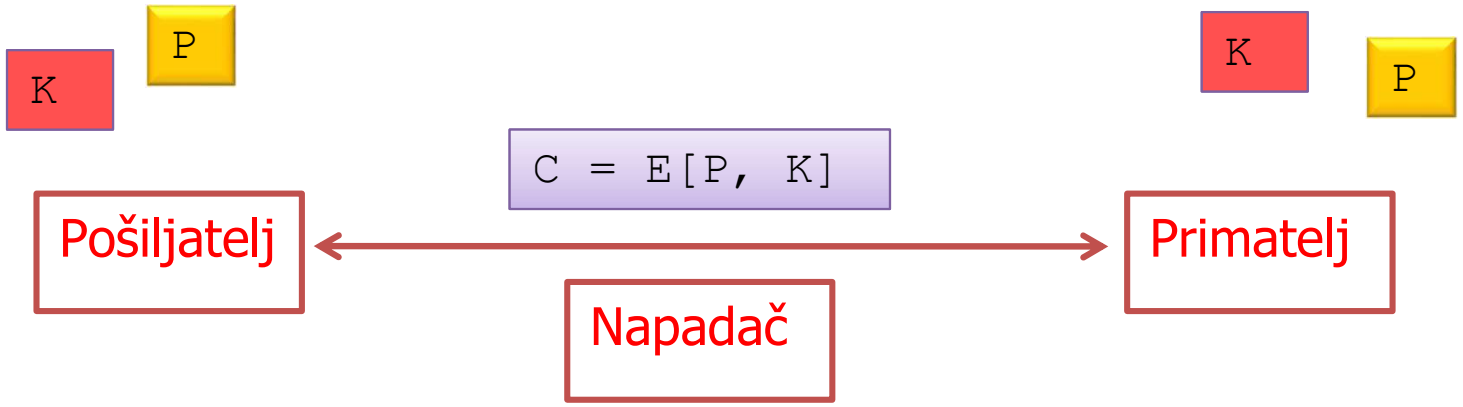
- Klasični
  - supstitucija
  - transpozicija
- Mehanički strojevi
- Moderni
  - simetrični
    - blok (AES, DES, PRINCE, PRESENT, Twofish, RC6, ...)
    - protočni ili kriptiranje toka podataka (Salsa20, Trivium, Mickey, Grain, Achterbahn, Rakaposhi, ...)
    - $Ke = Kd = \boldsymbol{K}$ (simetrični, sjednički ili tajni ključ)
  - asimetrični
    - $Ke \neq Kd$ (***P*** - javni i ***S*** - privatni ključ)
  - funkcije za izračunavanje sažetka poruke (*hash*)

Jesu li i koliko su kriptoalgoritmi sigurni?

- postoje specijalizirana računala za napad grubom silom na DES kriptosustav: COPACOBANA (*A Cost-Optimized PArallel COde Breaker*)
- 12.12.2009. faktoriziran RSA-768
- na kvantnom računalu je riješen problem faktoriziranja velikih brojeva i problem diskretnog logaritma
- 17.8.2004. - kineski i francuski znanstvenici su objavili članak pod naslovom: "*Kolizija za hash funkcije: MD4, MD5, Haval-128 i RIPEMD*"
- 13.2.2005. - kineski znanstvenici: "*Collision Search Attacks on SHA-1* "
- napadi koji koriste sporedna svojstva uređaja (*Side-Channel Attacks*, SCA)

2.
Simetrični kriptosustavi

Simetrična enkripcija



Kerckhoffov princip

- Kriptosustav mora biti siguran i onda kada su sve informacije o kriptosustavu javno poznate, osim tajnog ključa.

- Simetrični kriptosustavi temelje se na jednostavnoj logičkoj operaciji isključivo ILI (XOR):

$$C = M \oplus K \qquad M = C \oplus K$$

$$\boldsymbol{M = (M \oplus K) \oplus K}$$

- ONE TIME PAD – jednokratna bilježnica

Savršena povjerljivost

- Claude Shannon, 1946
- jednokratna bilježnica pruža *savršenu povjerljivost:*
  - za svaku poruku $m \in \{0,1\}^n$ i šifrat $c \in \{0,1\}^n$ i vrijedi:

$$P_{k \leftarrow \{0,1\}^n}(E(m,k) = c) = \frac{1}{2^n}.$$

- jednokratna bilježnica u praksi:

Izvor: www.cryptomuseum.com

Jednokratna bilježnica – nedostaci

- Ključ
  - mora se generirati potpuno i uistinu slučajno!
  - mora biti jednako velik kao i poruka!
  - smije se koristiti najviše jednom!

$$c_1 = m_1 \oplus k$$
$$c_2 = m_2 \oplus k$$
$$c_1 \oplus c_2 = m_1 \oplus m_2$$

- Moguće je na predvidiv način izmijeniti poruku (engl. *malleable encryption)* !
  - naravno, samo ako nam je poznata kriptirana poruka

$$c_1 = OTP(m_1, k) = m_1 \oplus k$$

$$c_2 = c_1 \oplus m_1 \oplus m_2 = m_1 \oplus k \oplus m_1 \oplus m_2 = m_2 \oplus k = OTP(m_2, k)$$

Klasična kriptografija

- nećemo se baviti klasičnom kriptografijom, no, ipak ćemo navesti nekoliko primjera

Šifriranje uz pomoć papira i olovke

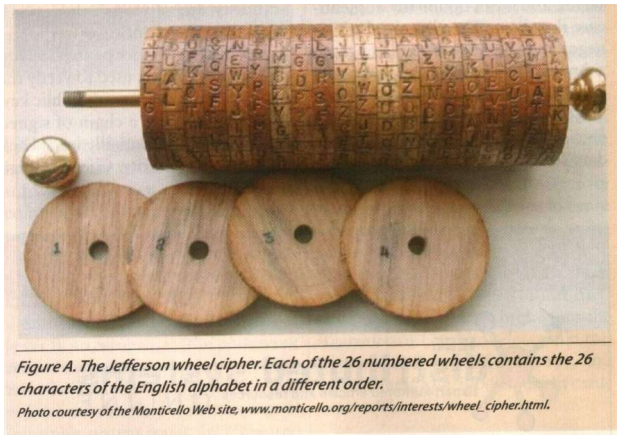
- supstitucijske šifre
  - Cezarova šifra
  - Vigenèreova šifra (1586.)
  - Playfairova šifra (1854.)
  - Hillova šifra (1929.)
- transpozicijske šifre

Šifriranje uz pomoć naprava

- Jeffersonov kotač (krajem 18. stoljeća Thomas Jefferson)
- električni stroj za kodiranje (1915. Edward Hugh Hebern)
- Enigma (1918. Artur Scherbius)
- C-36 (1936. Boris Hagelin)
  - u američkoj vojsci ta je naprava nosila naziv M-209

Naprave za šifriranje

Enigma
(1918. Artur Scherbius)



Jeffersonov kotač
(krajem 18. stoljeća Thomas Jefferson)

električni stroj za kodiranje
(1915. Edward Hugh Hebern)

C-36
(1936. Boris Hagelin)
- u američkoj vojsci ta je naprava nosila naziv M-209

Primjer supstitucijske šifre:
Cezarova šifra

- najjednostavnija i najčešće korištena šifra
- monoalfabetska šifra: svako slovo se mijenja drugim slovom za jednak pomak, gdje je pomak ključ

Pomak = 3

Jasni tekst:	a	b	c	č	ć	d	đ	e	f	g	h	i	j	k	l	m	n	o	p	r	s	š	t	u	v	z	ž
Šifra:	Č	Ć	D	Đ	E	F	G	H	I	J	K	L	M	N	O	P	R	S	Š	T	U	V	Z	Ž	A	B	C

Jasni tekst:	A	U	T	O
Šifra:	Č	Ž	Z	S

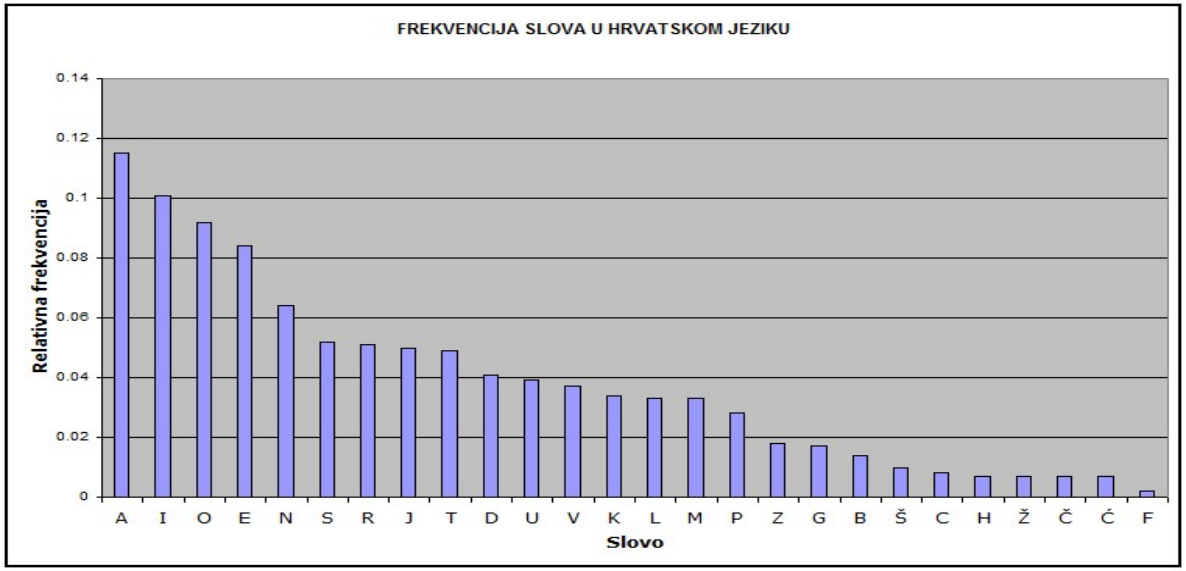
- jednostavan napad frekvencijskom analizom ako je poznat jezik

Frekvencijska analiza (1/4)

- uzeti u obzir frekvenciju slova (u promilima):

Tablica 1. Frekvencija slova u hrvatskom jeziku

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



Izvor: wikipedia.org

... a prebrojali smo najfrekventnije znakove u nekom tekstu koji je šifriran supstitucijskom šifrom:

```
Z 51
P 54
D 56
R 60
W 78
O 91
```

Frekvencijska analiza (2/4)

- ako znamo da je poruka šifrirana Cezarovom šifrom možemo uz pomoć frekvencijske analize iz šifrata:

```
VWZWUO UG FOEQCPGPO: RAJOMRIOPW ZPQSGDPG ERUW XG DRZWPW
PGKDRCRZEW W SJQZPIGDW JOMIRU KJIOPZEG EJRM DOZPOIQ GCGEPJRPGKDWEG,
JOXQDOJZPIO PG WDFRJVOXWUZEG W ERVQDWEOXWUZEG PGKDRCRHWUG
MOZDRIODQ DO JGMQCPOPWVO WZPJOMWIODUO, ZPIOJOPW DRIO MDODUO EJRM
VGSUQDOJRSDR LJWMDOPO WZPJOMWIODUO, JOMIWUOPW HRZLRSOJZPIR W
UOIDW ZGEPRJ EJRM WDRIOXWUG PG SRLJWDRZWPW QEQLDRV JOMIRUQ SJQZPIO,
AWPW QZPODRIO IWZREWK OEOSGVZEWK IJWUGSDRZPW W GPWXEWK EJWPGJWUO,
VUGZPR EJWPWXERH JOMVWZCUODUO W LJRLWPWIODUO PG UGSDOERZPW ZIWK
DUGDWK XCODRIO W AWPW LREJGPOXEO ZDOHO KJIOPZERH SJQZPIO.
Q WZLQDUGDUQ VWZWUG FOEQCPGPO RZCODUOVR ZG DO DOZG PGVGCUDG
IJWUGSDRZPW ERUG SOCUG JOMIWUOVR: IRSGXO ZVR DOXWRDOCDO
IWZRERZERCZEO W WZPJOMWIOXEO QZPODRIO Z WMIJZDWV DOZPOIDWXWVO W
ZPQSGDPWVO, XIJZPR LRIGMODO Z HRZLRSOJZPIRV, WMIJZDR RJHODWMWJODO W
VGSUQDOJRSDR LJGLRMDOPCUWIO.
```

Frekvencijska analiza (3/4)

- dobiti nešto što nalikuje na tekst na hrvatskom jeziku:

```
.I.I.A .. .A...N.NA: O..A.O.ANI .N...EN. .O.I .. EO.INI
N..EO.O..I I ....N..EI .A..O. ...AN... ..O. EA.NA.. ....N.ON..EI..,
.A..EA..N.A N. IE.O..A.I.... I .O..EI.A.I.... N..EO.O.I..
.A.EO.AE. EA .....NANI.A I.N.A.I.AE.A, .N.A.ANI EO.A .EAE.A ..O.
.....EA.O.EO ..I.EANA I.N.A.I.AE.A, .A..I.ANI .O..O.A..N.O I
.A.EI ...NO. ..O. IEO.A.I.. N. .O..IEO.INI ....EO. .A..O.. ....N.A,
.INI ..NAEO.A .I.O.I. A.A.....I. ..I...EO.NI I .NI..I. ..IN..I.A,
....NO ..INI..O. .A..I...AE.A I ..O.INI.AE.A N. ...EA.O.NI ..I.
E..EI. ..AEO.A I .INI .O...NA..A .EA.A ...AN..O. ....N.A.
. I...E..E.. .I.I.. .A...N.NA O..AE.A.O .. EA EA.. N.....E.
..I...EO.NI .O.. .A... .A..I.A.O: .O...A ..O EA.IOEA.EA
.I.O.O..O...A I I.N.A.I.A..A ..NAEO.A . I....EI. EA.NA.EI.I.A I
.N...ENI.A, ....NO .O...AEA . .O..O.A..N.O., I....EO O..AEI.I.AEA I
.....EA.O.EO ....O.EAN..I.A.
```

- nisu sva slova pogođena jer je premali tekst
  - što ima više teksta, lakše ga je dešifrirati

Frekvencijska analiza (4/4)

- frekvencija slova na hrvatskom i engleskom jeziku:

A	I	O	E	N	S	R	J	T	D	U	V	K	L	M	P	Z	G	B	Š	C	H	Ž	Č	Ć	F
117	104	94	85	64	53	50	49	47	42	40	38	37	35	34	27	18	17	15	10	7	6	5	4	3	1

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

- frekvencija bigrama:

  HR: 2.8% **je**; 1.5% **na**; 1% **an st an ni ko os ti ij no en**

  EN: 3.2% **th**; 2.5% **he**; 1.2% **an in er re on es ti at**

- frekvencija trigrama:

  HR: 0.6% **ije**; 0.3-0.4% **sta ost jed koj oje jen**

  EN: 3.5% **the**; 1.1% **ing**; 1% **and**; 0.7% **ion tio ent ...**

Drugi primjer supstitucijske šifre:
Vigenèreova šifra

- polialfabetska šifra: niz od nekoliko Cezarovih šifri s različitim pomacima
- postupak šifriranja: $S_i = A_i + K_i \mod(\text{broj\_slova}=27)$

```
                                1 1 1 1 1 1 1 1 1 1 2 2 2 2 2 2 2
            0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6
Alfabet (A): a b c č ć d đ e f g h i j k l m n o p r s š t u v z ž

Ključ = „ključ” = {13, 14, 12, 23, 3}

Jasni tekst: A U T O M O B I L    L=14   u=23
  Ključ (K): k l j u č k l j u   (14 + 23) mod 27= 37 mod 27 = 10 = H
  Šifra (S): K H E K P Č M U H
```

Treći primjer supstitucijske šifre:
Playfairova šifra

- polialfabetska, bigramska šifra: šifriraju se parovi znakova
- ako je neparan broj slova, dodaje se neko slovo npr. Ž
- koristi se matrica 5x5 slova (ako ima više slova, neka se poistovjećuju, npr. DĐ i SŠ) koja se stvara na temelju ključa (neka je ključ = „OVOJEKLJUČ”):

```
Alfabet: a b c č ć d đ e f g h i j k l m n o p r s š t u v z ž

   O  V  J  E  K    Pravila:
   L  U  Č  A  B    1. par slova u istom retku posmiču se udesno (npr. AU=BČ)
   C  Ć  DĐ F  G    2. par slova u istom stupcu posmiču se dolje (OR=LO)
   H  I  M  N  P    3. par slova čine pravokutnik i mijenjaju se sa slovima na
   R  SŠ T  Z  Ž       suprotnim stranama pravokutnika (npr. TO=RJ ili BI=UP)

Jasni tekst: AU TO MO BI LŽ
      Šifra: BČ RJ HJ UP BR
```

Četvrti primjer supstitucijske šifre:
Hillova šifra

- poligramska šifra: šifrira se m znakova
- ako duljina poruke nije djeljiva s m zadnji blok treba nadopuniti
- ključ K je matrica m x m

											1	1	1	1	1	1	1	1	1	1	2	2	2	2	2	2
	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5
Alfabet (***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

Neka je $m = 3$ i $K = K^{-1} = \begin{bmatrix} 5 & 8 & 22 \\ 2 & 5 & 24 \\ 10 & 20 & 17 \end{bmatrix}$ Jasni tekst: subota (18,20,1,14,19,0)

Šifriranje: $(18\ 20\ 1)\begin{bmatrix} 5 & 8 & 22 \\ 2 & 5 & 24 \\ 10 & 20 & 17 \end{bmatrix} = (140\ 264\ 893)\ mod\ 26 = (10\ 4\ 9) =$ k e j

$(14\ 19\ 0)\begin{bmatrix} 5 & 8 & 22 \\ 2 & 5 & 24 \\ 10 & 20 & 17 \end{bmatrix} = (108\ 207\ 764)\ mod\ 26 = (4\ 25\ 10) =$ e z k

Šifra: kejezk (10,4,9,4,25,10)

Hillova šifra – postupak dešifriranja

- za dešifriranje koristi se inverz matrice *K*, tj. K^{-1}
- izvorno autor predlaže da je $K = K^{-1}$
  - ali se time značajno smanjuje prostor svih mogućih ključeva

											1	1	1	1	1	1	1	1	1	2	2	2	2	2	2
	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5
Alfabet (**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

$$K = K^{-1} = \begin{bmatrix} 5 & 8 & 22 \\ 2 & 5 & 24 \\ 10 & 20 & 17 \end{bmatrix}$$

Šifra: kejezk (10,4,9,4,25,10)

Dešifriranje: $(10\ 4\ 9)\begin{bmatrix} 5 & 8 & 22 \\ 2 & 5 & 24 \\ 10 & 20 & 17 \end{bmatrix} = (148\ 280\ 469)\ mod\ 26 = (18\ 20\ 1) =$ s u b

$(4\ 25\ 10)\begin{bmatrix} 5 & 8 & 22 \\ 2 & 5 & 24 \\ 10 & 20 & 17 \end{bmatrix} = (170\ 357\ 858)\ mod\ 26 = (14\ 19\ 0) =$ o t a

Jasni tekst: subota (18,20,1,14,19,0)

Primjer transpozicijske šifre:
Stupčana transpozicija

- umjesto zamjene znakova koristi zamjenu položaja elemenata otvorenog teksta
- frenkvencije znakova šifrata su jednake kao i kod jasnog teksta
- ključ je permutacijski niz od *m* elemenata
- jasni tekst se upisuje u pravokutnik po retcima, a jedan redak ima *m* znakova
- zadnji redak se nadopunjuje proizvoljnim znakovima

```
Jasni tekst: danas je lijep dan

      Ključ: 3 2 5 1 4
Jasni tekst: d a n a s
             j e l i j
             e p d a n

Šifra: aiaaepdjesjnnld
```

- u stupcu 1 piše „aia” i tako počinje šifrirani tekst
- u stupcu 2 piše „aep” pa se tako nastavlja šifrat
- slijedi „dje”, itd.