

## **Sigurnost računalnih sustava**

# **Osnove kriptografije i kriptanalize**

doc. dr. sc. Ante Đerek

doc. dr. sc. Stjepan Groš

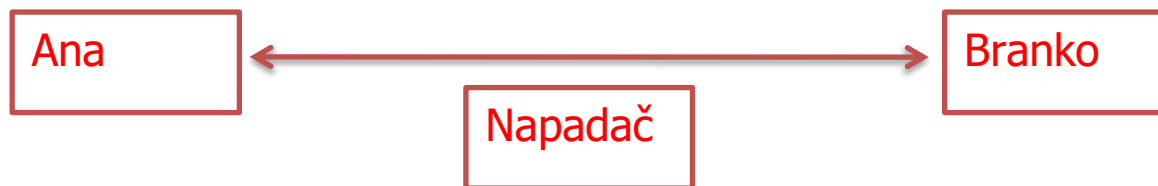
izv. prof. dr. sc. Miljenko Mikuc

izv. prof. dr. sc. Marin Vuković

# Dodatna literatura

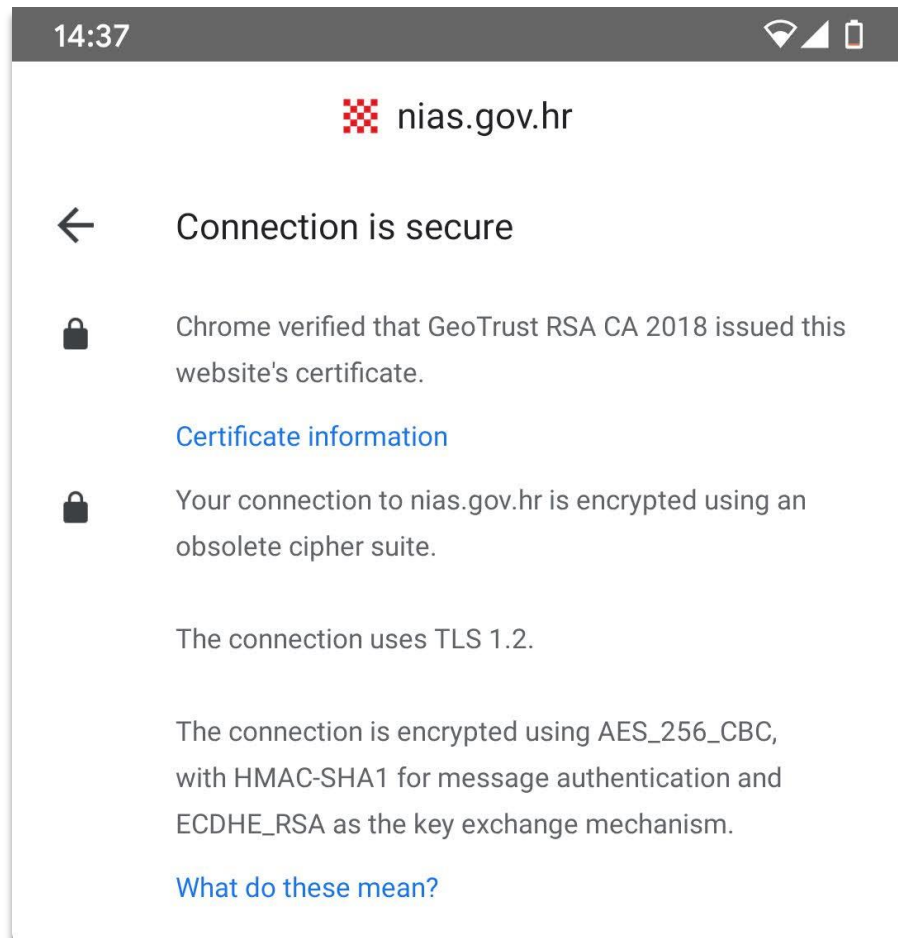
- Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone (1996.), *Handbook of Applied Cryptography*, CRC Press
- Andrej Dujella, Marcel Maretić (2007.), *Kriptografija*

## Problem: *Sigurna* komunikacija putem nesigurnog kanala



- *Povjerljivost*: može li napadač saznati sadržaj komunikacija?
- *Integritet*: može li napadač promijeniti sadržaj komunikacije?
- *Autentifikacija*: može li Ana biti sigurna da komunicira baš s Brankom i obrnuto?
- ...

# Naš cilj: Usvojiti osnovne pojmove moderne kriptografije



- Simetrične šifre
- Kriptografske *funkcije sažetka*
- Kodovi za integritet poruke
  
- Asimetrične šifre
- Digitalni potpisi
- Diffie-Hellmanova razmjena ključeva

Osnove kriptografije i kriptanalize

# Klasična kriptografija

# Cezarova šifra



NAPADAMO U ZORU

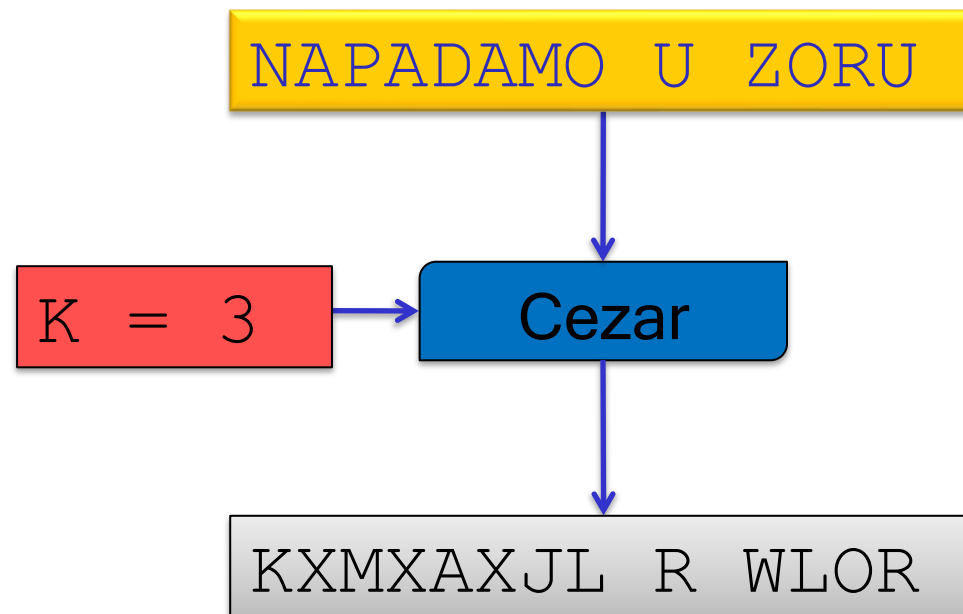
KXXAXJL R WLOR

ABCDEFGHIJKLMNOPQRSTUVWXYZ

XYZABCDEFGHIJKLMNOPQRSTUVWXYZ

# Cezarova šifra s *ključem*

- Svako slovo u *izvornom tekstu* zamjeni sa slovom koje dolazi K pozicija ispred



# Gruba sila (osnovni algoritam kriptanalize)

- Isprobaj sve moguće ključeve, dešifriraj poruku i pogledaj ima li rezultat smisla

QRI Z KZ JZEV SILKV

RSJ A LA KAFW TJMLW

K = 1

STK B MB LBGX UKNMX

K = 2

TUL C NC MCHY VLONY

K = 3

UVM D OD NDIZ WMPOZ

K = 4

VWN E PE OEJA XNQPA

K = 5

WXO F QF PFKB YORQB

K = 6

XYP G RG QGLC ZPSRC

K = 7

YZQ H SH RHMD AQTSO

K = 8

ZAR I TI SINE BRUTE

K = 9

Malo mogućih različitih ključeva znači nesiguran sustav!

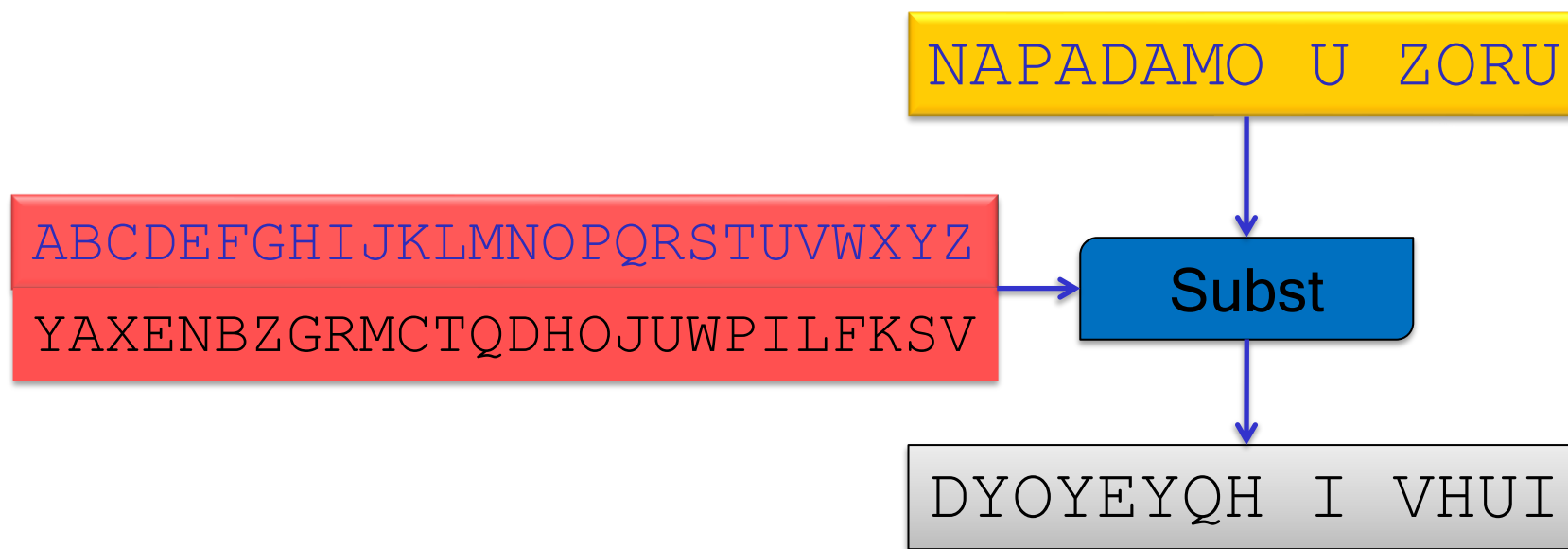


# Kerckhoffov princip

- Kriptosustav mora biti siguran čak i kada su javno poznati svi detalji rada sustava osim samih ključeva!

Pazite se *security-by-obscurity* pristupa u kriptografiji!

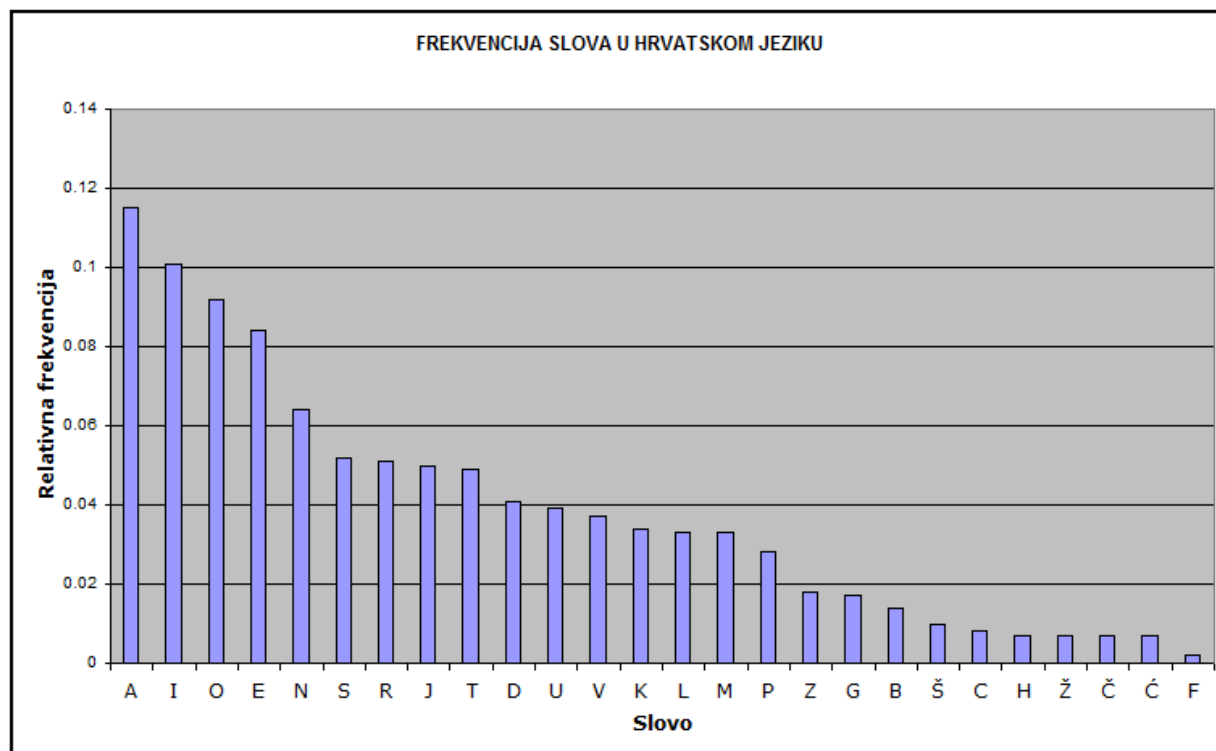
# Supstitucijska šifra



403291461126605635584000000 različitih ključeva!

VWZWUO UG FOEQCPGPO: RAJOMRIOPW ZPQSGDPG ERUW XG DRZWPW  
PGKDRCRZEW W SJQZPIGDW JOMIRU KJIOPZEG EJRM DOZPOIQ GCGEPJRPGKDWE,  
JOXQDOJZPIO PG WDFRJVOXWUZEG W ERVQDWEQXWUZEG PGKDRCRHWUG  
MOZDRIODQ DO JGMQCPWPVVO WZPJOMWIODUO, ZPIOJOPW DRIO MDODUO EJRM  
VGSUQDOJRSDR LJWMDOPW WZPJOMWIODUO, JOMIWUOPW HRZLRSOJZPIR W  
UOIDW ZGEPRJ EJRM WDRIQXWUG PG SRLJWDRZWPW QEQLDRV JOMIRUQ SJQZPIO,  
AWPW QZPODRIO IWZREW OEOSGVZEWK IJWUGSDRZPW W GPWKEWK 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  
IWZRERZERCEO W WZPJOMWIOXEO QZPODRIO Z WMIJZDWV DOZPOIDWXWVO W  
ZPQSGDPWVO, XIJZPR LRIGMODO Z HRZLRSOJZPIRV, WMIJZDR RJHODWMWJODO W  
VGSUQDOJRSDR LJGLRMDOPCUWIO.

# Frekvencijska analiza



Izvor: wikipedia.org

...

Z 51

P 54

D 56

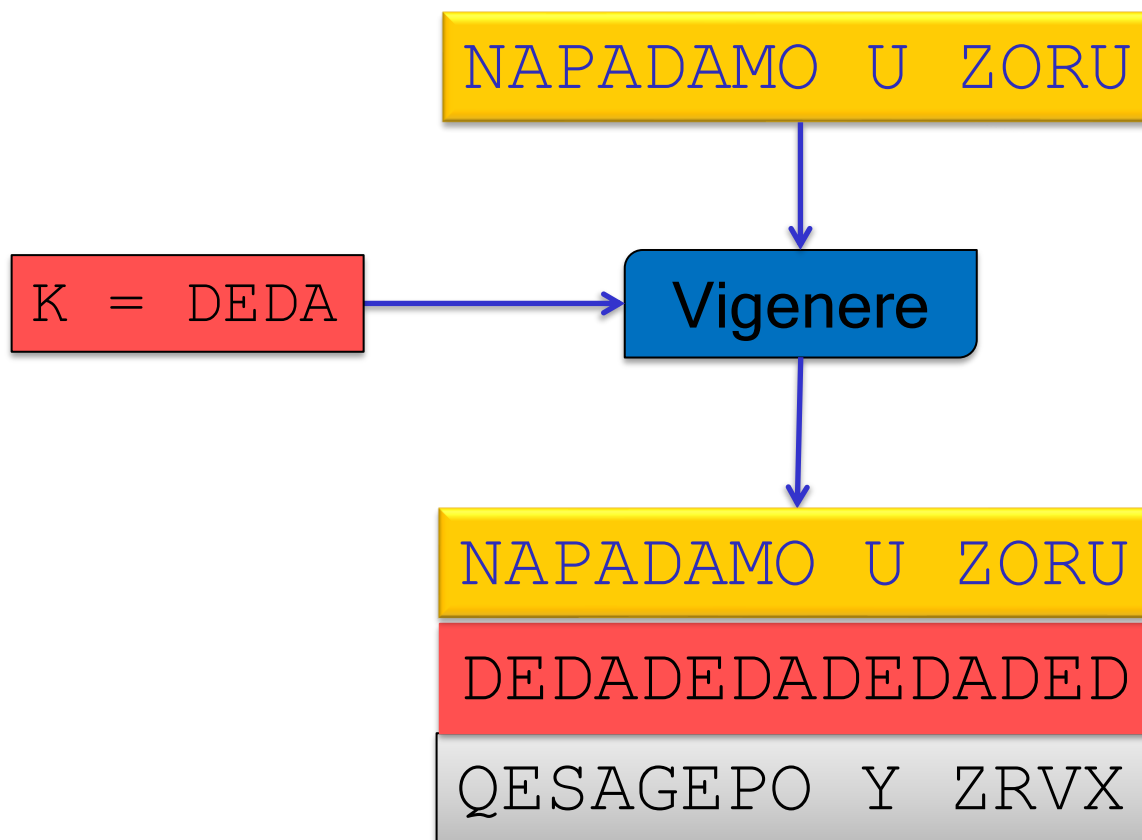
R 60

W 78

O 91

```
.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.
```

# Vigenèereova šifra – *le chiffre indéchiffrable*



# Kriptoanaliza Vigenèereove šifre

NIROJBBDLALUKZEUANH**RBZ**NBAUIRZUEEMZELOIOCFN  
NYIUISKHOOKUSLIHJRVSSBEOI**QGZ**WOINRWASYKFKQU  
ZOARZAWUDRELTQUTFHMOKFRZIUOAQYTWASKIOFNXMB  
CHPSLEHQONUMOKBCHPSLESKHOOKUGJJDFATNNBAOUM  
GRFZTRTBTHSAJSSXAAIUGNKARZVBRZZIOOUGZOAMPA  
LRNFMFDIANBRNJNPPQOZOASGITT**QGZ**JVZTJBRZ FVJJ  
ZZIHORVOEAQYTWOPAWNHYELTNXKSOYONPVZIIKESK  
DPPQONPSHZIVKTVNPM**QGZ**WOIADSURZVBBHZI**VSS**GNP  
VZBITOJOHBKZJENSJOHWRHPEENNYTJIDZIDKHNKSI  
KRJJZSJFSSUKSISOCLOFXAAMHYLKAMPAJPQUPJTHBA  
OJZZEKECTALORZITVHNNKEMOHDLTOWAHHIUIOUKSE  
SGCLARTAHAGXVBTRQOHDQASUVZAITPTTJFNIAMJSHF  
EGAJALUESGOTLZTJBMNYEOAMGSFTDSEMJMKVSIKDO  
ORZILLOIKDBLIK**RBZ**UOJBMNBOEEBGSNOMGCJOMGLOAU  
OSPKNYKPLRQAJIRZ**RBZ**HBADKZASUAMUVBSHF**VSS**MOM  
OARZAWNHIINAHYTVDDTTJMZ**VSS**SUPPVDFAOARMOTP  
NJASSSBONIYBRTNNURHAMOZJRZTAJMDJJVNZXOENNV  
RFPNFBTKPIWA

- Traženje vjerojatnih duljina ključa  
*Kasiskijevim testom*
- Frekvencijska analiza fragmenata koji odgovaraju istom znaku ključa

# Vigenèreova šifra – napad poznatim tekstom

```
RIYH: RXOE UOMEW <VNFV.YEDVU@FQI.CR>  
DJ: JDEEBRX GDFC <EKTZPME.BRAJ@AED.RM>  
JEWJQTD: XRLJSU  
P BISGOSL KRUAOYLAX UAPRDFA QK PDMS LMSYN.
```

```
RIYH: RXOE UOMEW . . .
```

```
FROM: ANTE DEREK . . .
```

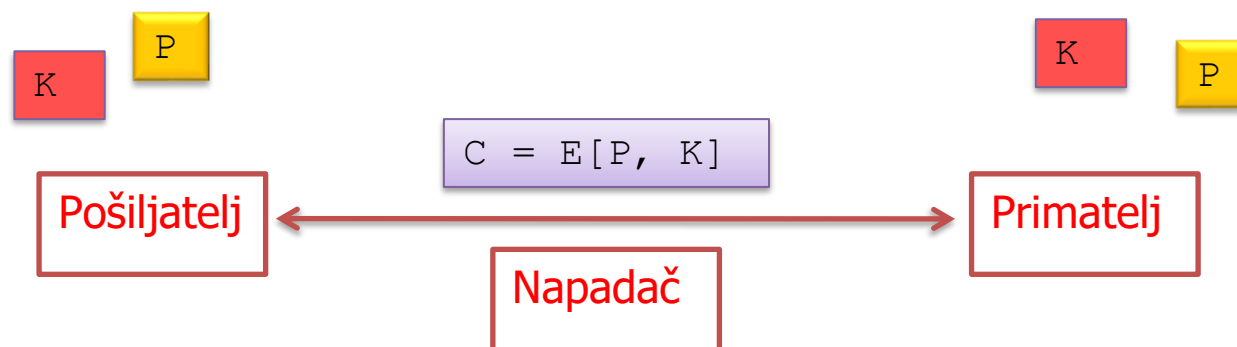
```
MRKV??RKVA?RKVAM
```



Osnove kriptografije i kriptanalize

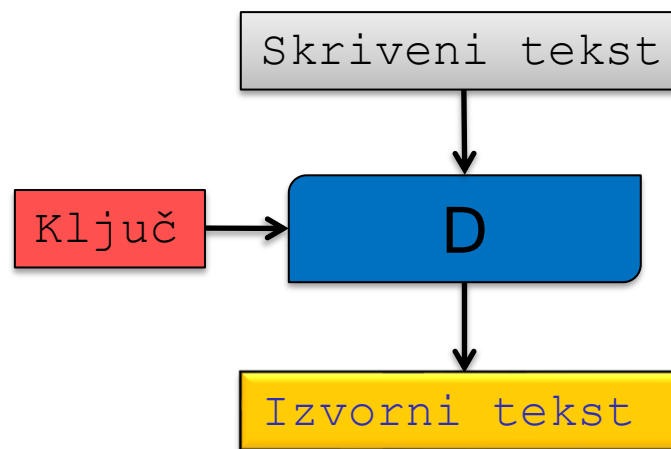
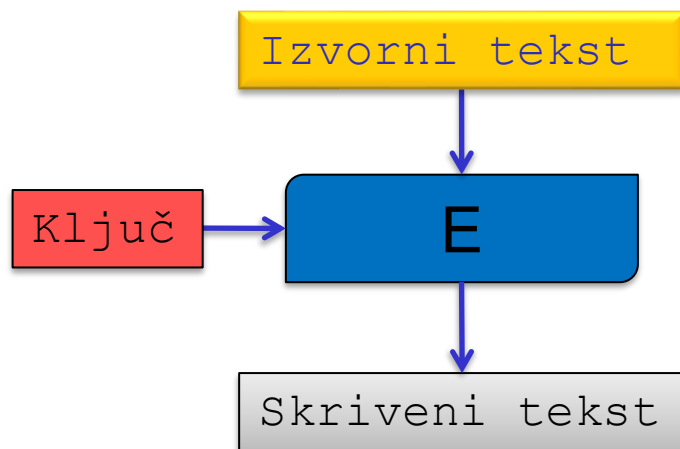
# Simetrične šifre

# Kako osigurati povjerljivost komunikacije?



# Simetrična šifra

- Poruka ili izvorni tekst ili otvoreni tekst (*plaintext*)
- Šifrat ili skriveni test (*ciphertext*)



# Simetrična šifra – definicija

Neka su  $K$ ,  $M$  i  $C$  konačni skupovi – *prostor ključeva*, *prostor izvornih tekstova* i *prostor skrivenih tekstova*.

*Simetrična šifra* je par algoritama  $E$  i  $D$

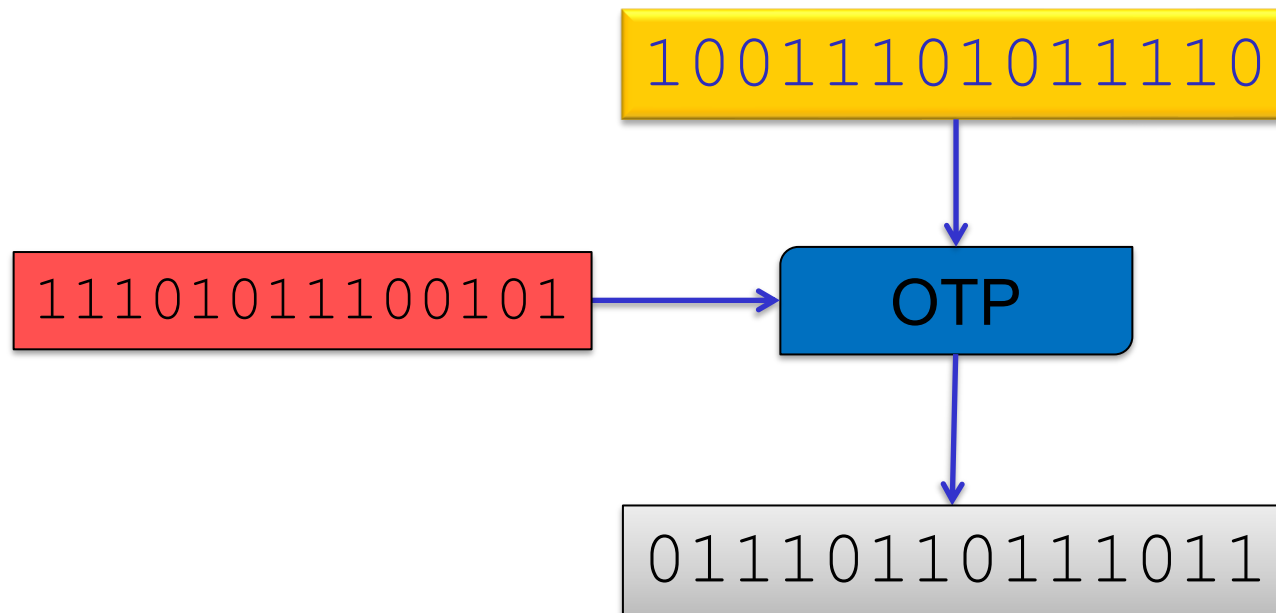
$$E: M \times K \rightarrow C, D: C \times K \rightarrow M$$

gdje za svaki  $k \in K$  i  $m \in M$  vrijedi

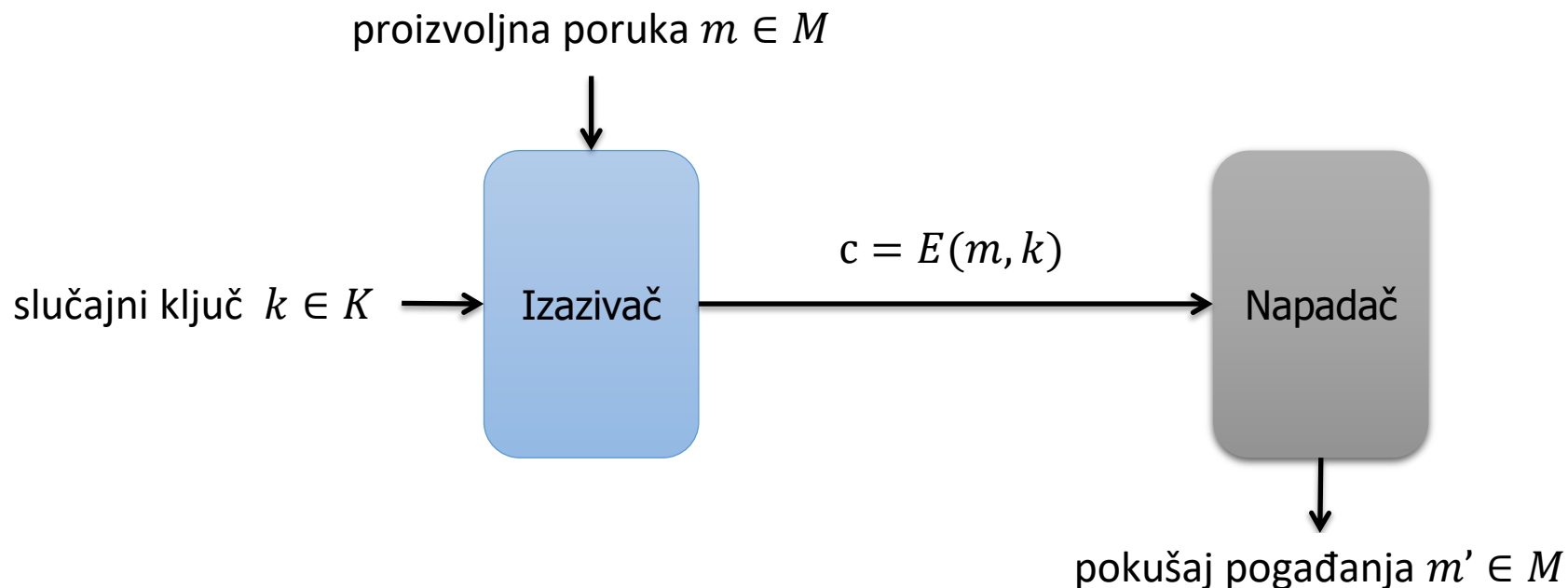
$$D(E(m, k), k) = m.$$

# Jednokratna bilježnica (*one-time pad*)

- $M = K = C = \{0, 1\}^n$
- $E(m, k) = m \oplus k$
- $D(c, k) = c \oplus k$



## Savršena povjerljivost (*perfect secrecy*), Claude Shannon (1946)



Šifra pruža *savršenu povjerljivost* ako je za **svakog napadača** šansa da pogodi poruku jednaka  $1/|M|$  (bez obzira na algoritam napadača, vrijeme izvršavanja, računalne resurse, itd.).

# Savršena povjerljivost (Claude Shannon, 1946)

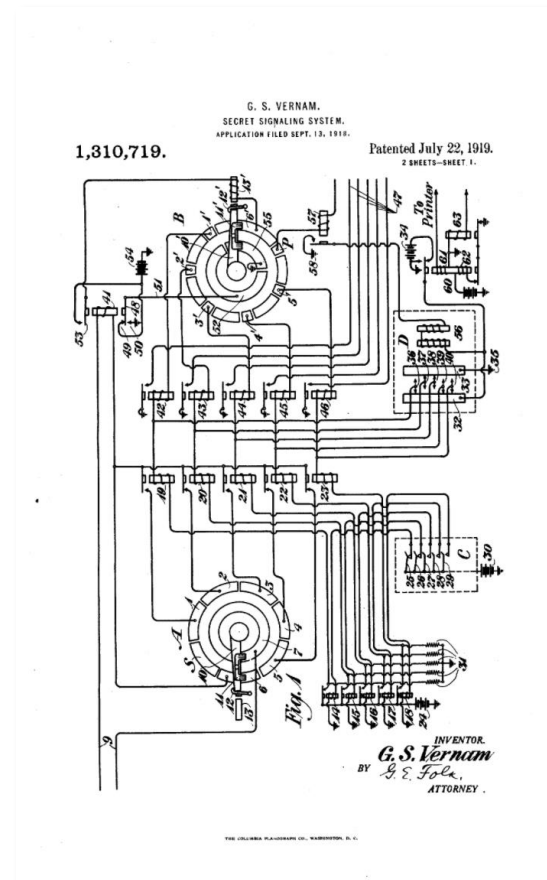
Jednokratna bilježnica pruža *savršenu povjerljivost*: za svaku poruku  $m \in \{0, 1\}^n$  i šifrat  $c \in \{0, 1\}^n$  i vrijedi

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

# Jednokratna bilježnica u praksi



Izvor: [www.cryptomuseum.com](http://www.cryptomuseum.com)



Izvor: [uspto.gov](http://uspto.gov)



# Jednokratna bilježnica – nedostatci

- Ključ mora biti jednako velik kao i poruka!
- Ključ se smije koristiti najviše jednom!
  - $c_1 = m_1 \oplus k$
  - $c_2 = m_2 \oplus k$
  - $c_1 \oplus c_2 = m_1 \oplus m_2$

# Jednokratna bilježnica – nedostatci

- Ne štiti integritet poruke (kao niti jedna šifra sama po sebi)!
- Moguće je na predvidiv način izmijeniti poruku (*malleable encryption*)!

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

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



# Fleksibilnije definicije sigurnosti

*Što je cilj napada?*

- odrediti tajni ključ  $k$
- odrediti poruku  $m$
- odrediti neki dio poruke  $m$
- odrediti bilo kakvu informaciju o poruci  $m$
- ...

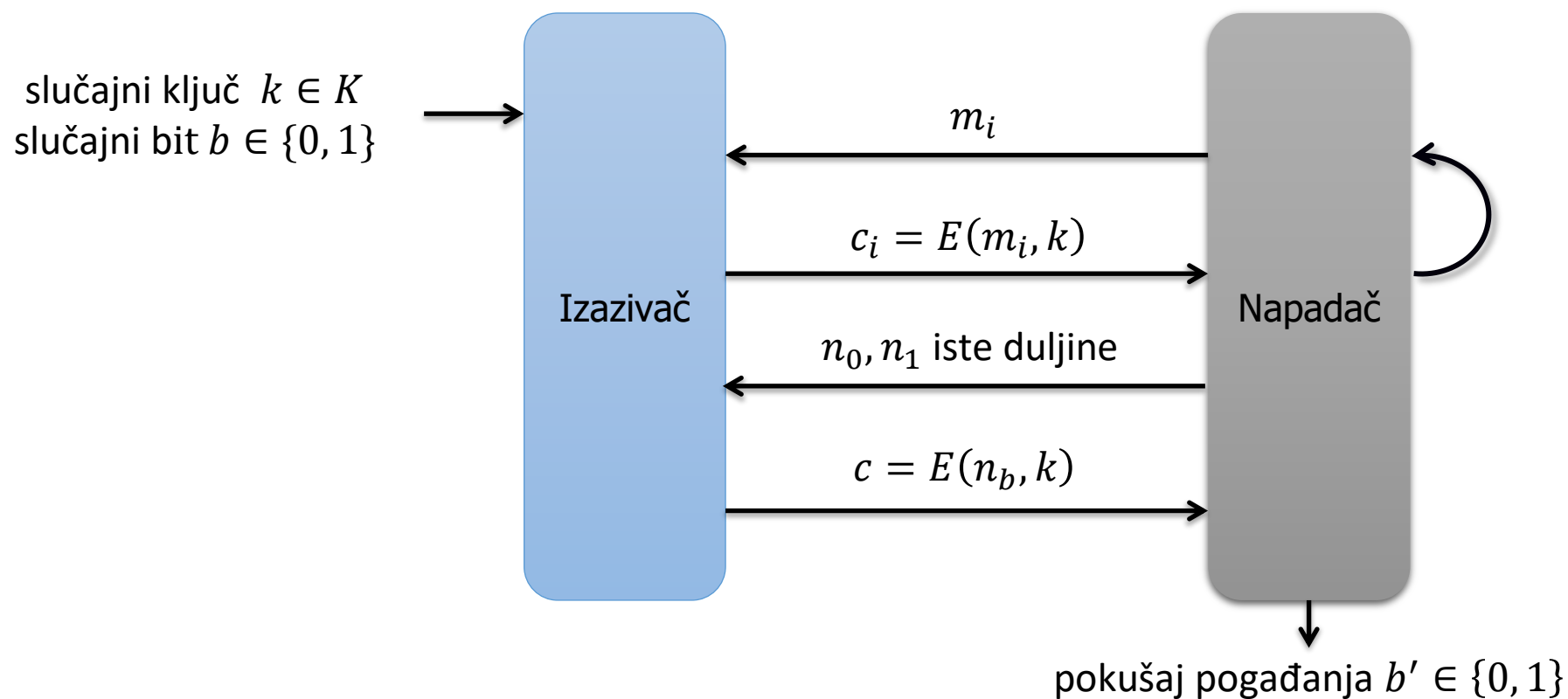
# Fleksibilnije definicije sigurnosti

*Što napadač ima na raspolaganju?*

- samo jedan skriveni tekst
- puno parova  $(m_i, c_i)$  gdje je  $c_i = E(m_i, k)$ 
  - Napad poznatim izvornim tekstom / *known plaintext attack*
- mogućnost da dobije  $c_i = E(m_i, k)$  za  $m_i$  po izboru
  - Napad odabranim izvornim tekstom / *chosen plaintext attack*
- mogućnost da dobije  $m_i = D(c_i, k)$  za  $c_i$  po izboru
  - Napad odabranim skrivenim tekstom / *chosen ciphertext attack*
- ...

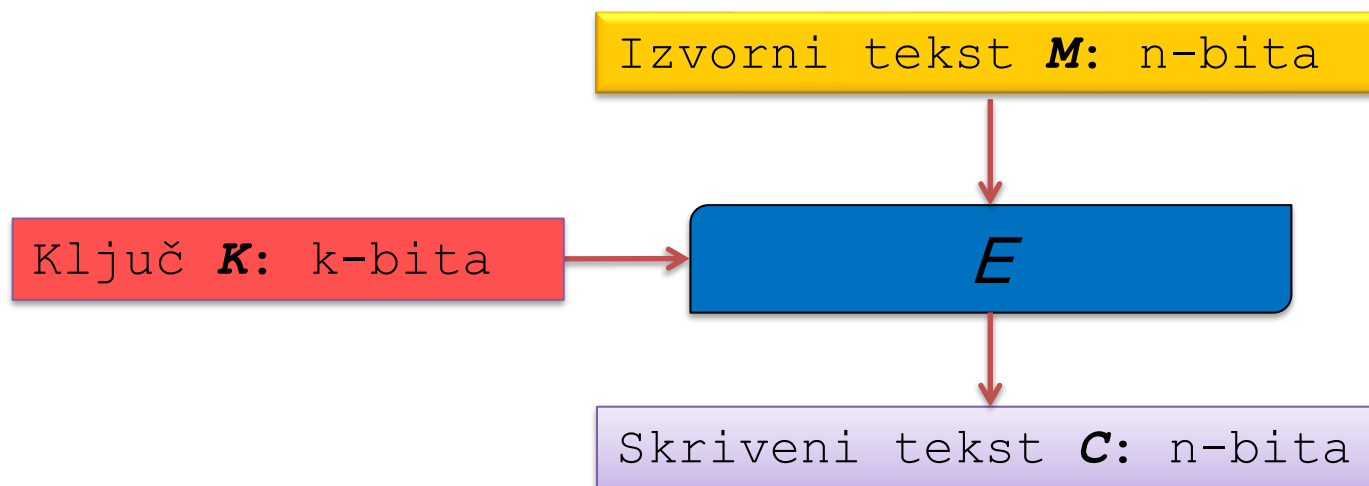
# Primjer definicije sigurnosti šifre

Semantička sigurnost od napada odabranim izvornim tekstom (*semantic security under chosen-plaintext attack*): Niti jedan algoritam koji koristi razumne resurse ne može pobijediti u sljedećoj igri s vjerojatnošću nezanemarivo većom od jedne polovine.



# Blok šifra (*block cipher*)

- $M = C = \{0, 1\}^n$
- $K = \{0, 1\}^k$
- $E$  i  $D$  deterministički algoritmi



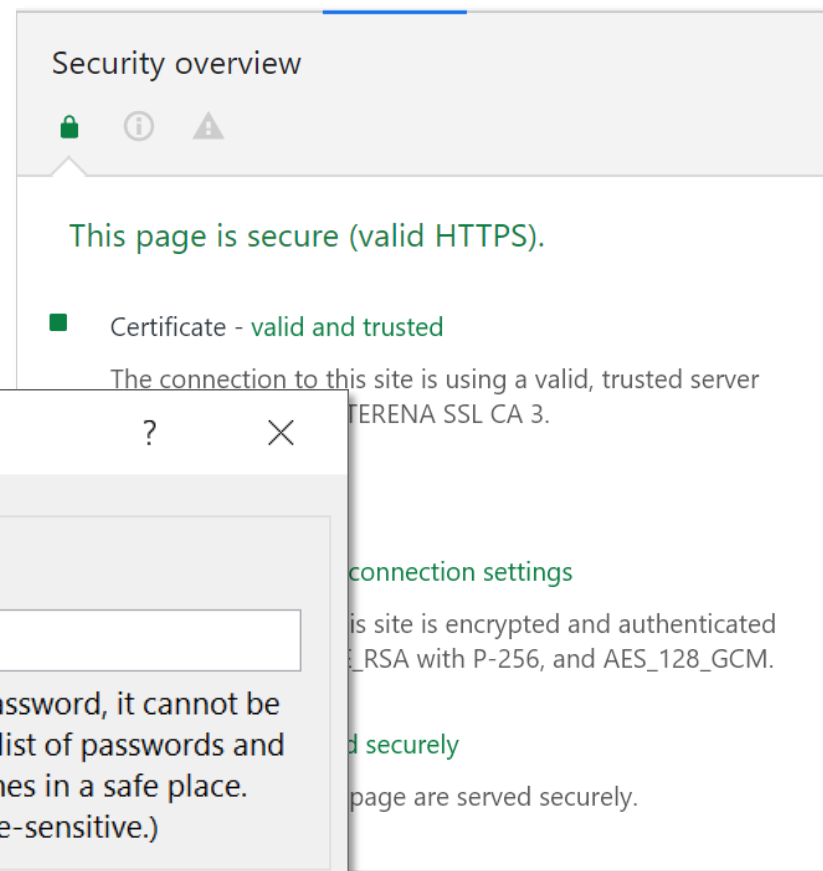
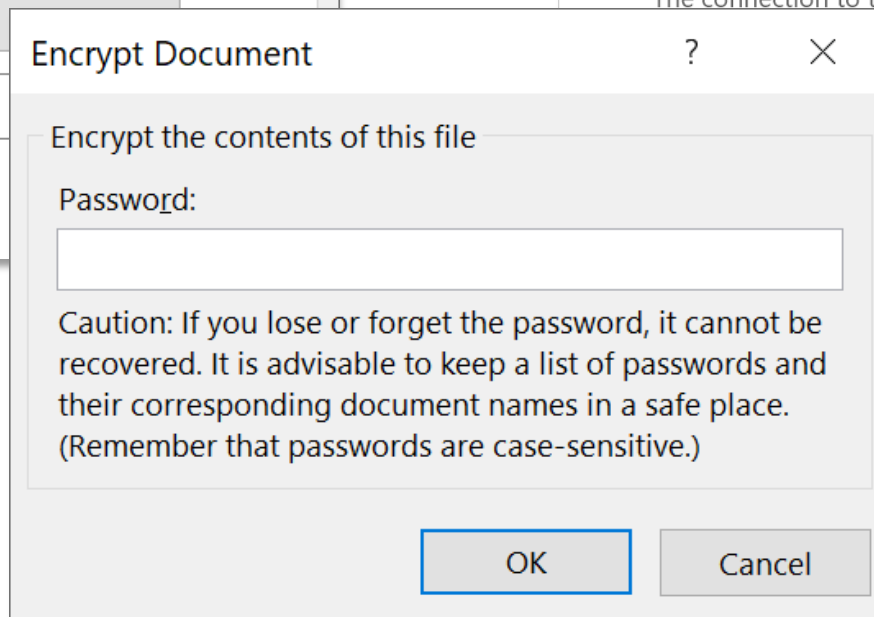
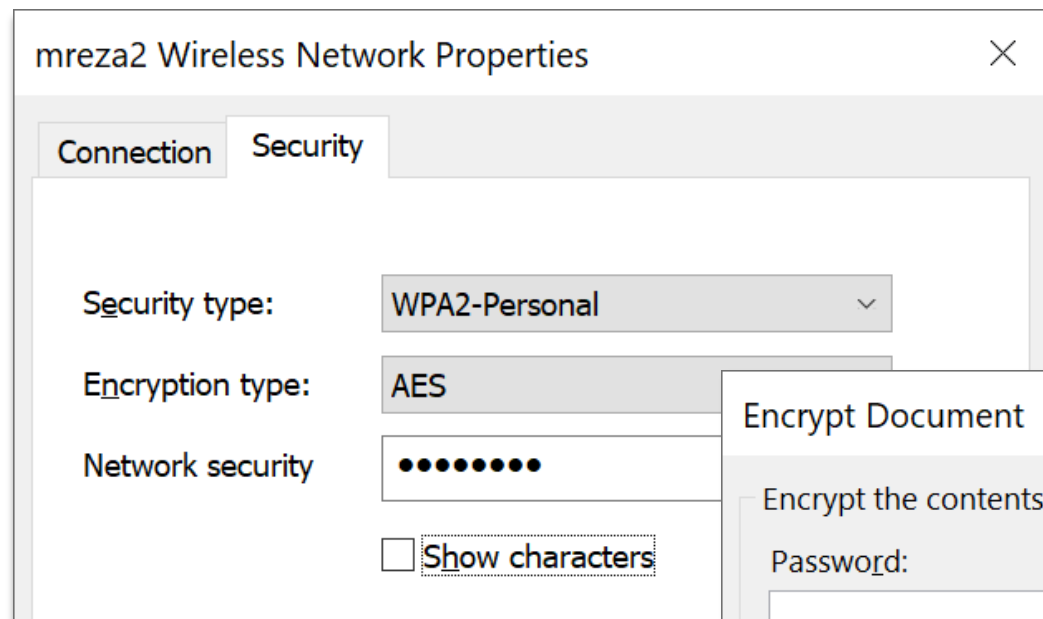
# Primjeri blok šifri

- DES (1970-te)
  - $n=64$   $k=56$ , dugogodišnji standard, danas potpuno nesiguran zbog malog ključa
- 3DES (1970-te)
  - $n=64$   $k=168$ , trostruki DES, veća sigurnost s istom šifrom
- IDEA (1991)
  - $n=64$ ,  $k=128$
- Blowfish (1993)
  - $n=64$ ,  $k=32-448$
- AES (1999)
  - $n=128$   $k=128, 192, 256$ , standard od 2002., vrlo široko korišten

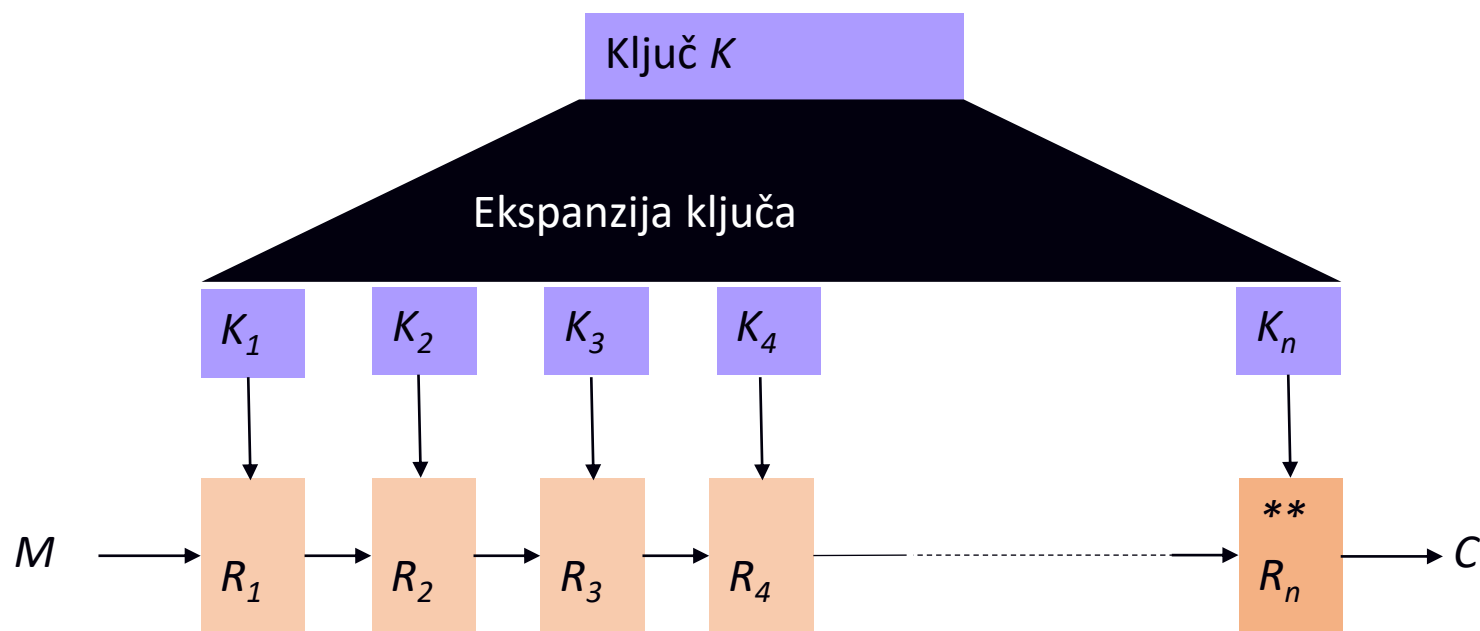
# Napredni kriptosustav – AES

- Natječaj za novi standard je raspisao NIST 1999. godine
- Pobjednik sustav *Rijndael* (autori Vincent Rijmen i Joan Daemen)
- Jednostavna struktura!
- Parametri:
  - Veličina bloka: 128 bitova
  - Veličine ključa: 128, 192 ili 256 bitova



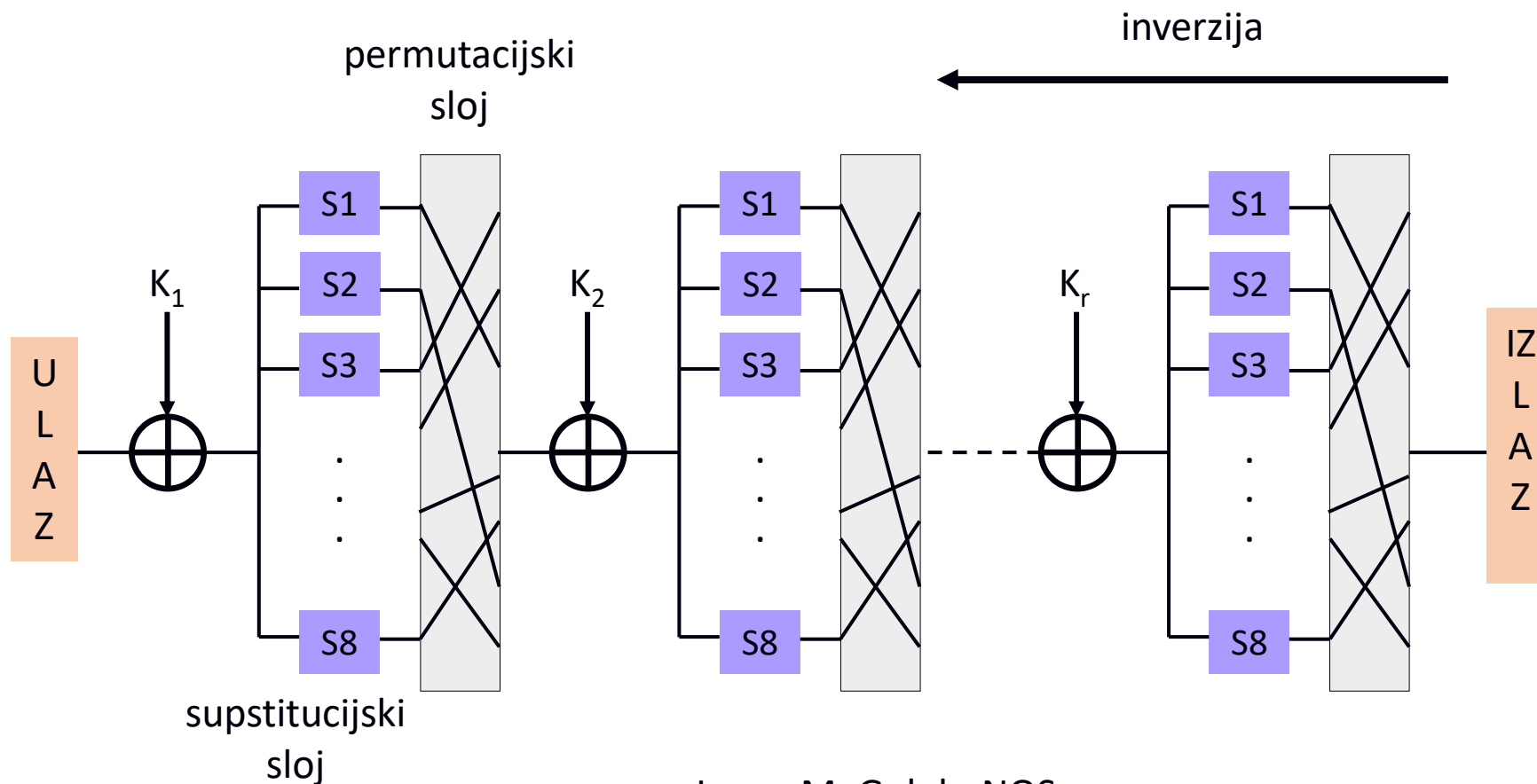


# AES – runde



Izvor: M. Golub, NOS

# AES – supstitucijsko-permutacijska mreža

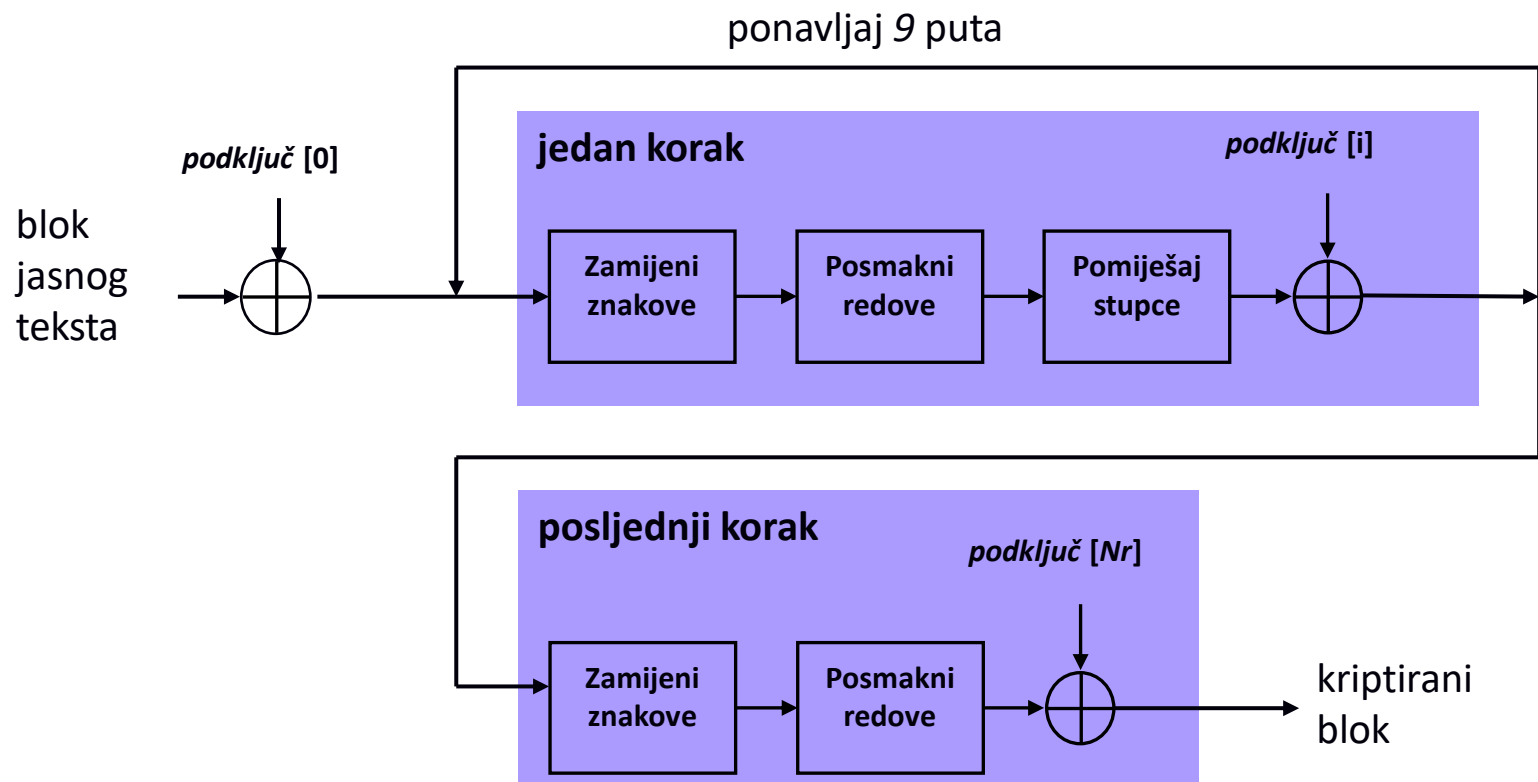


Izvor: M. Golub, NOS

# AES128 – blok

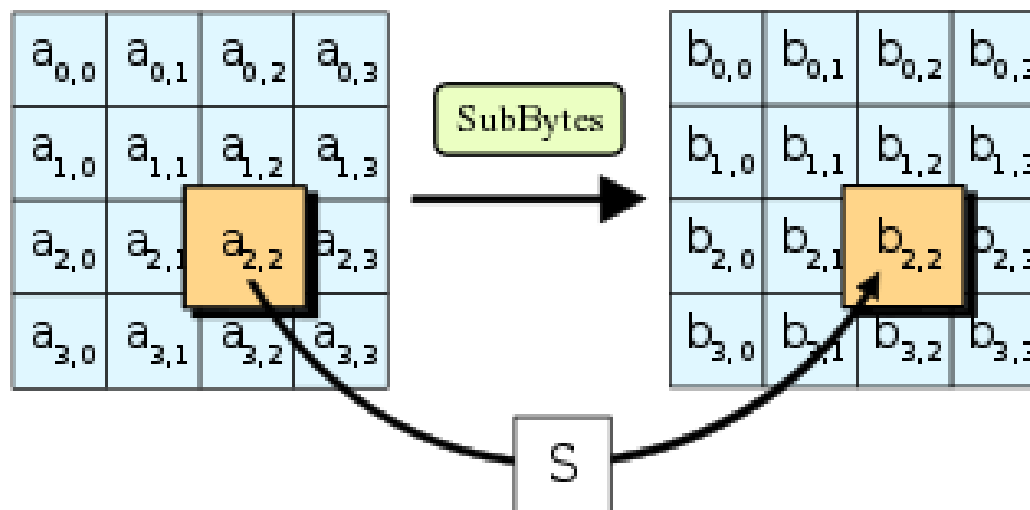
$a_{00}$	$a_{01}$	$a_{02}$	$a_{03}$
$a_{10}$	$a_{11}$	$a_{12}$	$a_{13}$
$a_{20}$	$a_{21}$	$a_{22}$	$a_{23}$
$a_{30}$	$a_{31}$	$a_{32}$	$a_{33}$

# AES128 – postupak (de)šifriranja



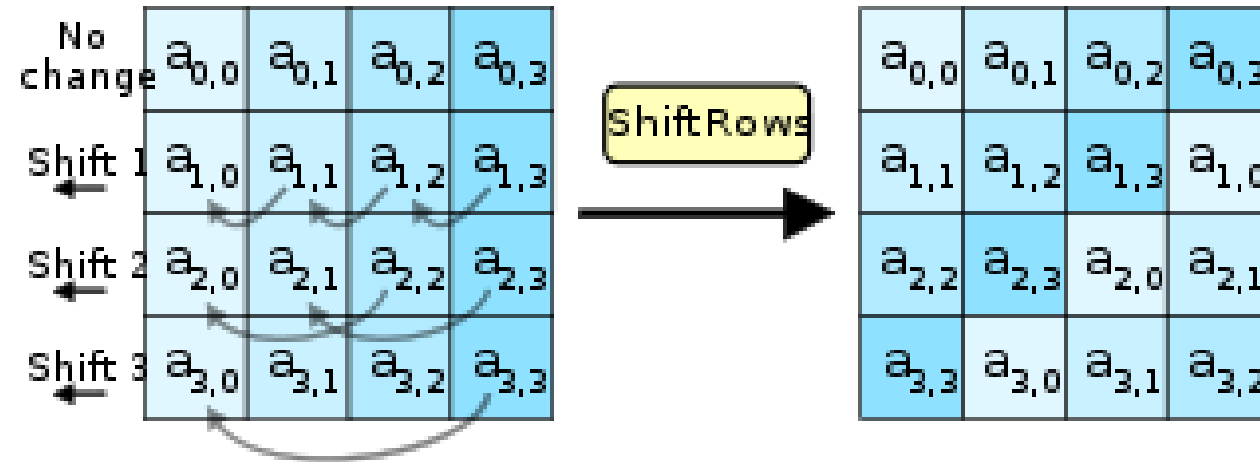
Izvor: M. Golub, NOS

# AES128 – Zamijeni znakove



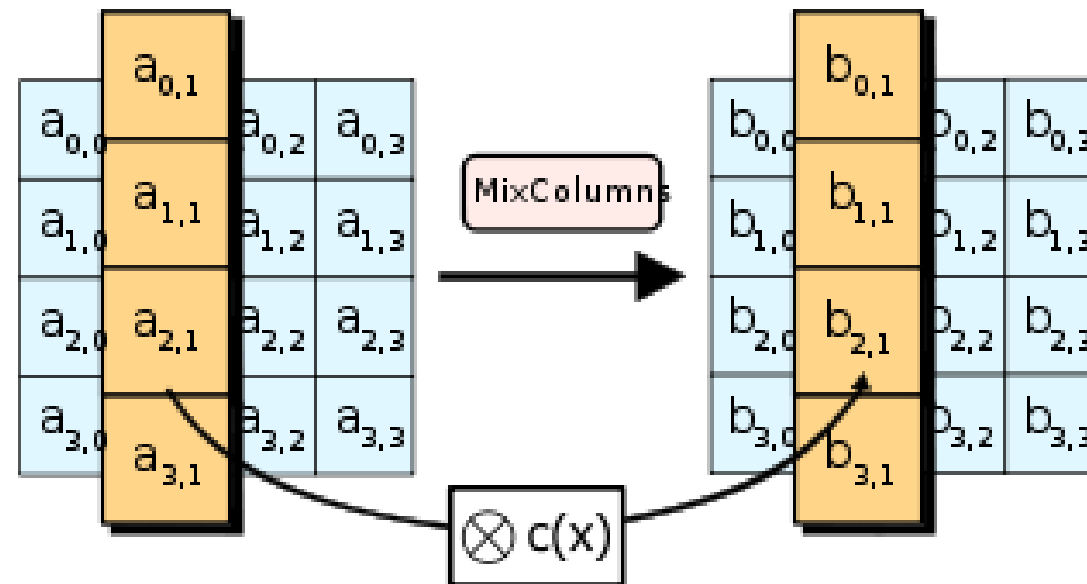
Izvor: wikipedia.org

# AES128 – Posmakni redove



Izvor: wikipedia.org

# AES128 – Pomiješaj stupce



Izvor: wikipedia.org



# AES128 – Pomiješaj stupce

$$\begin{bmatrix} s_{0i}' \\ s_{1i}' \\ s_{2i}' \\ s_{3i}' \end{bmatrix} = \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \begin{bmatrix} s_{0i} \\ s_{1i} \\ s_{2i} \\ s_{3i} \end{bmatrix}$$

- „zbrajanje” i „množenje” se vrše u polju  $GF(2^8)$
- „zbrajanje” i „množenje” u  $GF(2^8)$  imaju svojstva potrebna za invertibilnost matričnog množenja

# Konačno polje $\text{GF}(2^8)$

- Elementi polja su polinomi oblika:

$$a_7x^7 + a_6x^6 + \cdots + a_1x + a_0, a_i \in \{0, 1\}$$

- Svaki bajt  $(a_7a_6a_5a_4a_3a_2a_1a_0)_2$  je predstavljen odgovarajućim polinomom.
- Aritmetičke operacije:
  - zbrajanje: XOR
  - Množenje: binarno množenje polinoma modulo fiksni ireducibilni polinom  $g(x) = x^8 + x^4 + x^3 + x + 1$ , nekoliko *shift* i XOR operacija

Nije tajni sastojak za sigurnost već za jednostavnost i efikasnost (*citation needed*)!

# Zašto ovakav dizajn?

$a_{00}$	$a_{01}$	$a_{02}$	$a_{03}$
$a_{10}$	$a_{11}$	$a_{12}$	$a_{13}$
$a_{20}$	$a_{21}$	$a_{22}$	$a_{23}$
$a_{30}$	$a_{31}$	$a_{32}$	$a_{33}$

- The linear mixing layer:** guarantees high diffusion over multiple rounds.
- The non-linear layer:** parallel application of S-boxes that have optimum worst-case nonlinearity properties.
- The key addition layer:** A simple EXOR of the Round Key to the intermediate State.

Izvor: AES Proposal: Rijndael  
Joan Daemen, Vincent Rijmen, 2003.

# Programsko ostvarenje algoritma AES

- NE preporuča se vlastita programska implementacija zbog mogućih i vrlo vjerojatnih propusta
- koristiti raspoloživa i provjerena programska ostvarenja poput:
  - Openssl: [https://github.com/openssl/openssl/blob/master/crypto/aes/aes\\_x86core.c](https://github.com/openssl/openssl/blob/master/crypto/aes/aes_x86core.c)

# Sklopovska potpora algoritmu AES

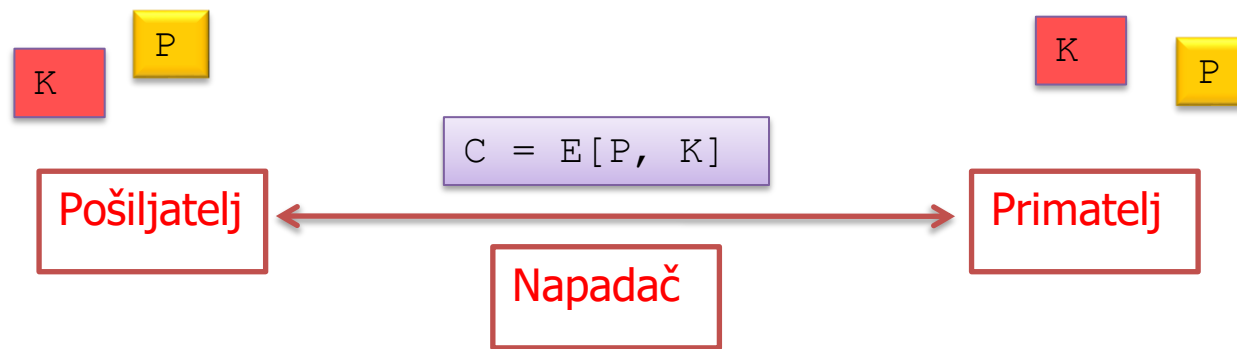
- Intel (slično i AMD)
- aesenc, aesenclast: jedna runda AES-a
  - 128-bitni registri:
  - xmm1=state, xmm2=ključ za rundu
  - aesenc xmm1, xmm2 ; rezultat u xmm1
  - aeskeygenassist: stvaranje podključeva
- 5 procesorskih ciklusa po bajtu, brzina se mjeri u GB/s

Osnove kriptografije i kriptanalize

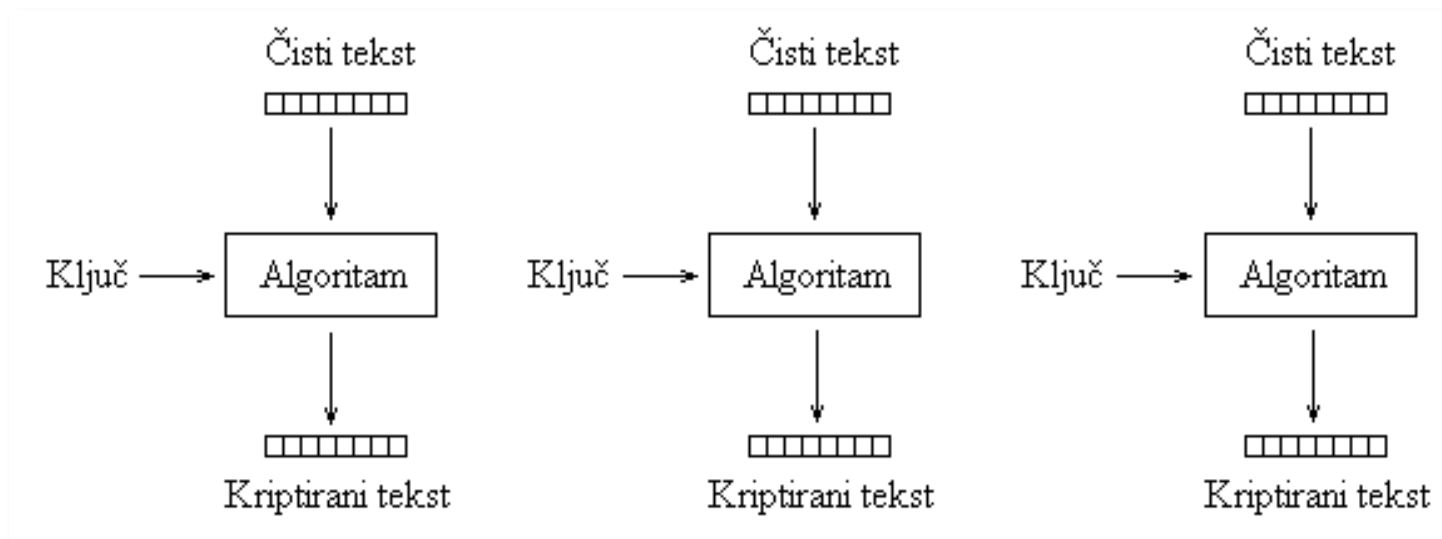
# Načini šifriranja

## Protočne šifre

# Kako šifrirati poruku proizvoljne duljine?



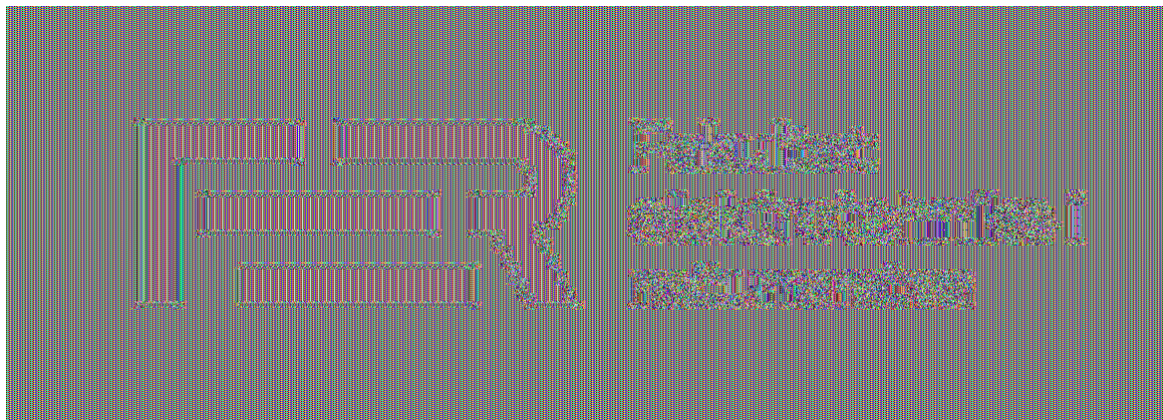
# Načini šifriranja ECB – *Electronic Codebook*



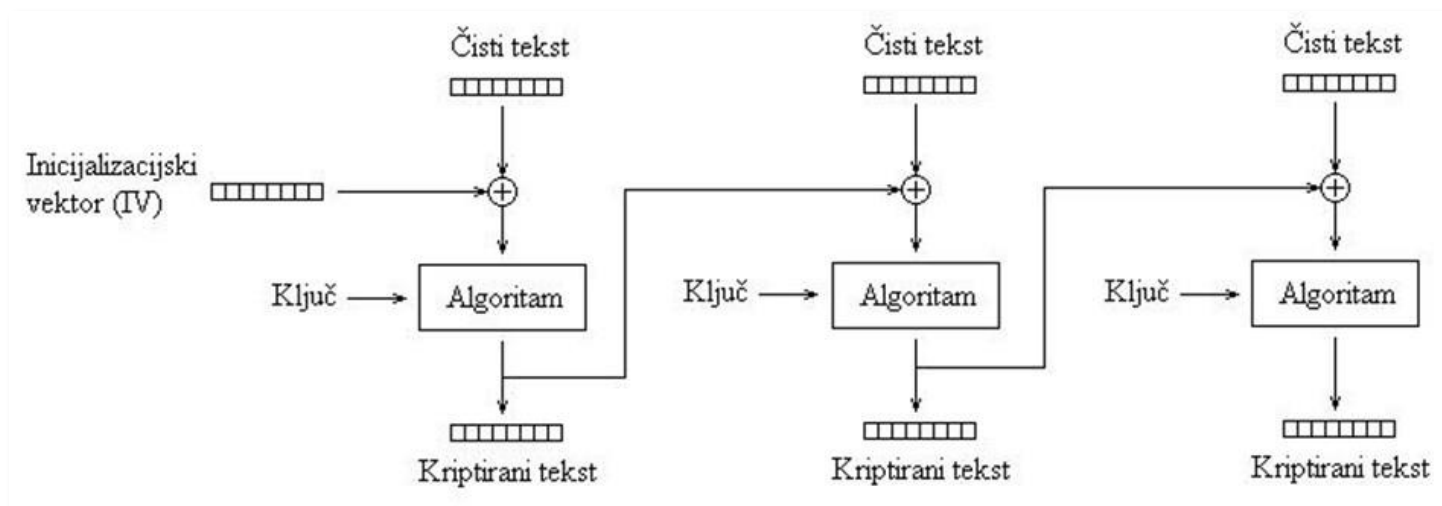
Izvor: Budin, Golub, Jakobović,  
Jelenković, Operacijski sustavi



# Načini šifriranja ECB – *Electronic Codebook*

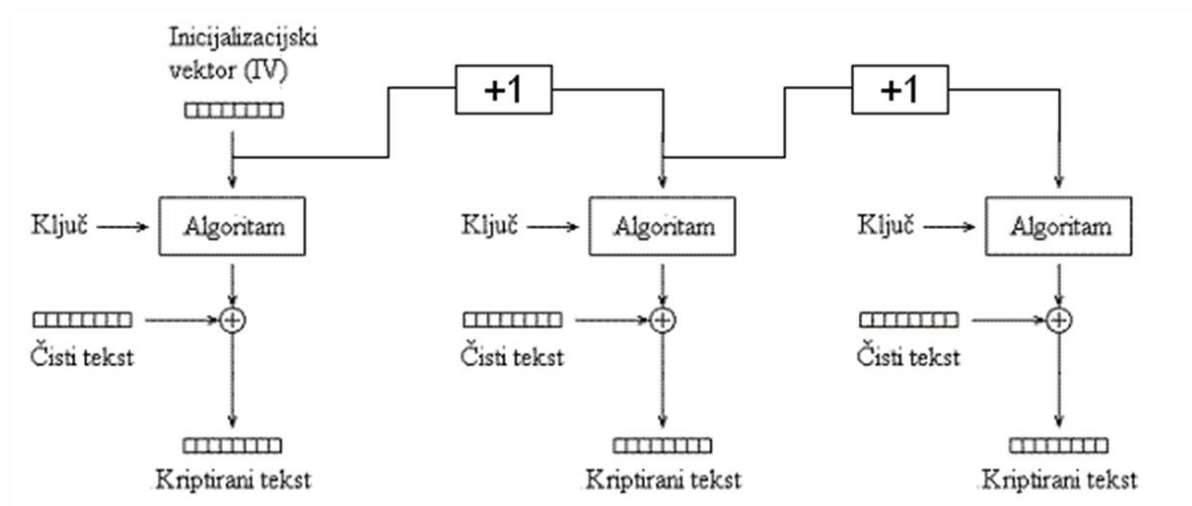


# Načini šifriranja CBC – *Cipher Block Chaining*



Izvor: Budin, Golub, Jakobović,  
Jelenković, Operacijski sustavi

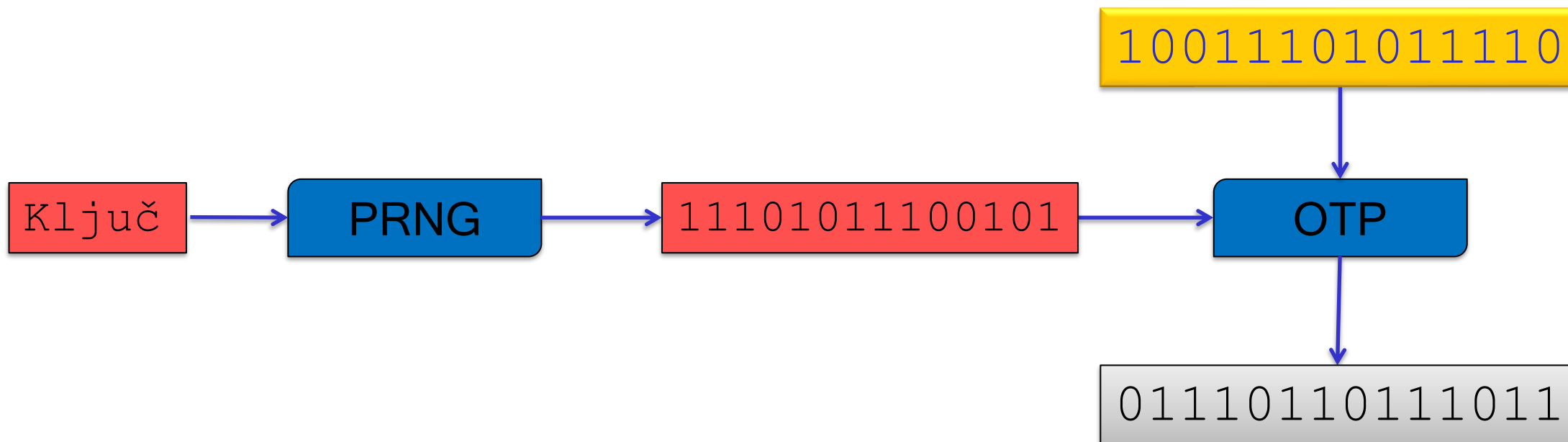
# Načini šifriranja CTR – *Counter Mode*



Izvor: Budin, Golub, Jakobović,  
Jelenković, Operacijski sustavi

# Protočna šifra (*stream cipher*)

Generator pseudoslučajnih brojeva na temelju ključa generira niz bitova koji se XOR-a s izvornim tekstom



# Primjeri protočnih šifri

- **RC4 (1987)**
  - ključ veličine 40–2048 bitova
  - vrlo široko korišten, mnoštvo poznatih slabosti
- **CSS (1996)**
  - 40-bitni ključ
  - zaštita sadržaja na DVD-ovima
  - potpuno razbijen 1999. godine
- **Salsa20/ChaCha (2005)**
  - ključ 128 ili 256 bitova
  - podržan u TLS-u
  - alternativa AES-u zbog boljih performansi na uređajima gdje sklopovlje ne implementira AES

Osnove kriptografije i kriptanalize

# Kriptanaliza blok šifri

# Sigurnost simetričnih šifri

- Apsolutne dokaze sigurnosti nemamo 😞
  - Relativni dokazi sigurnosti: Ako je  $F$  sigurna pseudoslučajna fukncija onda je  $F$ -CTR semantički sigurna od napada odabranim izvornim tekstom.
- Procjena sigurnosti:
  - Otpornost na poznate napade
  - Sigurnost pojednostavljenih verzija šifre
  - Principi dizajna
  - ...
- *Efektivna veličina ključa* je  $b$  ako najbolji poznati napad radi red veličine  $2^b$  koraka

# Kriptoanaliza blok šifri – gruba sila

- neka je poznato nekoliko parova  $m_j, c_j = E(m_j, k)$
- algoritam radi sljedeće:
  - za svaki mogući ključ  $k_i$
  - ako je  $c_j = E(m_j, k_i)$  onda ispiši  $k_i$



# Napadi grubom silom na DES

- DES Challenge 1 (1997.)
  - distributed.net, 3 mjeseca
- DES Challenge 2 (1998.)
  - EFF specijalizirani hardware (DeepCrack), 3 dana i 250 K\$
- DES Challenge 3 (1999.)
  - kombinirano pretraživanje, 22 sata
- COPACABANA (2006.)
  - 120 FPGA modula, 7 dana 10 K\$

```
Identifier: DES-Challenge-III
Cipher: DES
Start: January 18, 1999 9:00 AM PST
Prize: $10,000
IV: da 4b be f1 6b 6e 98 3d
Plaintext: See you in Rome (second AES Conference, March
22-23, 1999)
```

Ciphertext:

```
bd 0d de 91 99 60 b8 8a 47 9c b1 5c 23 7b 81 18 99 05
45 bc de 82 01 ab 53 4d 6f 1c b4 30 63 3c ee cd 96 2e
07 c6 e6 95 99 9c 96 46 5a 95 70 02 02 70 98 bd 41 c2
88 a9 f0 2f 8b e5 48 20 d2 a8 a0 6b bf 93 de 89 f6 e2
52 fd 8a 25 eb d0 7d 96 83 ee a4 2d c8 8d 1b 71
```

Izvor: [rsa.com](http://rsa.com)

# Napad grubom silom na AES128

- duljina ključa = 128 bita
- broj različitih ključeva =  $2^{128}$
- pretpostavke
  - Svi Bitcoin rudari razbijaju AES za to specijaliziranim hardware-om
  - Trenutni (2021) hash rate Bitcoin mreže 100 EH/s
  - $10^{20}$  ključeva po sekundi
- gotovi smo za oko  $3.4 * 10^{18}$  sekundi
- 100 milijardi godina

# Linearna kriptanaliza

- Iskorištava linearne zavisnosti pojedinih bitova poruke, ključa i šifrata:

$$m[1, 17, 34] \oplus c[14, 31] \oplus k[3, 29, 51] = 1.$$

- Ako zavisnost uvijek vrijedi onda se duljina ključa efektivno smanjuje za jedan bit.
- Što je veća pristranost (*bias*) to se više može ubrzati napad.

# Linearna kriptanaliza DES-a

- Matsui (1994.)
- Dvije zavisnosti koje vrijede s pristranošću  $\varepsilon = 1.19 * 2^{-21}$ .
- Krajnji rezultat je napad koji:
  - Treba  $2^{43}$  poznatih parova poruka/šifrat
  - Radi  $2^{43}$  koraka šifriranja
  - Uspijeva s vjerojatnošću 85%

$$\begin{aligned} &P_H[7, 18, 24] \oplus F_1(P_L, K_1)[7, 18, 24] \oplus C_H[15] \oplus C_L[7, 18, 24, 29] \oplus \\ &F_{16}(C_L, K_{16})[15] \\ &= K_3[22] \oplus K_4[44] \oplus K_5[22] \oplus K_7[22] \oplus K_8[44] \oplus K_9[22] \oplus K_{11}[22] \oplus \\ &K_{12}[44] \oplus K_{13}[22] \oplus K_{15}[22], \end{aligned}$$

$$\begin{aligned} &C_H[7, 18, 24] \oplus F_{16}(C_L, K_{16})[7, 18, 24] \oplus P_H[15] \oplus P_L[7, 18, 24, 29] \oplus \\ &F_1(P_L, K_1)[15] \\ &= K_{14}[22] \oplus K_{13}[44] \oplus K_{12}[22] \oplus K_{10}[22] \oplus K_9[44] \oplus K_8[22] \oplus K_6[22] \oplus \\ &K_5[44] \oplus K_4[22] \oplus K_2[22]. \end{aligned}$$

Izvor: Matsui, M. „The first experimental cryptanalysis of the data encryption standard”, 1994.

# Diferencijalna kriptanaliza

- Analiza kako promjene poruke utječu na promjene šifrata. Posebno, analiza S-kutija koje su često jedini nelinearni dio šifre.

$$\Delta_x = b_1 \oplus b_2, \Delta_y = S(b_1) \oplus S(b_2)$$

- Na temelju puno parova poruka s fiksnom razlikom  $\Delta_x$  napadač može analizom razlika šifrata smanjiti prostor pretraživanja (podrazumijeva napad odabranim izvornim tekstom)

# Diferencijalna kriptanaliza DES-a

- Biham, Shamir (1990.)
- DES reduciran na 6 rundi
  - 240 parova poruka/šifrat, par sekundi
- DES reduciran na 8 rundi
  - 50000 parova poruka/šifrat, par minuta
- Potpuni DES
  - zahtjeva  $2^{58}$  koraka 😊
  - „Even a minimal change of one entry in one of the DES S boxes can make DES easier to break.”

The entire algorithm was published in the Federal Register [2], but the design considerations, which we present here, were not published at that time. The design took advantage of knowledge of certain cryptanalytic techniques, most prominently the technique of “differential cryptanalysis,” which were not known in the published literature. After discussions with NSA, it was decided that disclosure of the design considerations would reveal the technique of differential cryptanalysis, a powerful technique that can be used against many ciphers. This in turn would weaken the competitive advantage the United States enjoyed over other countries in the field of cryptography.

Izvor: Coppersmith, D. „The Data Encryption Standard (DES) and its strength against attacks”, 1994

# AES danas smatramo sigurnim

- Najbolji napad na AES-128 radi u  $2^{126.1}$  koraka
- Najbolji napad na AES-192 radi u  $2^{189.7}$  koraka
- Najbolji napad na AES-256 radi u  $2^{254.4}$  koraka

A. Bogdanov (KU Leuven), D. Khovratovich (MS Research Redmond), C. Rechberger (France Telecom), Biclique Cryptanalysis of the Full AES, ASIACRYPT, 2011.

Osnove kriptografije i kriptanalize

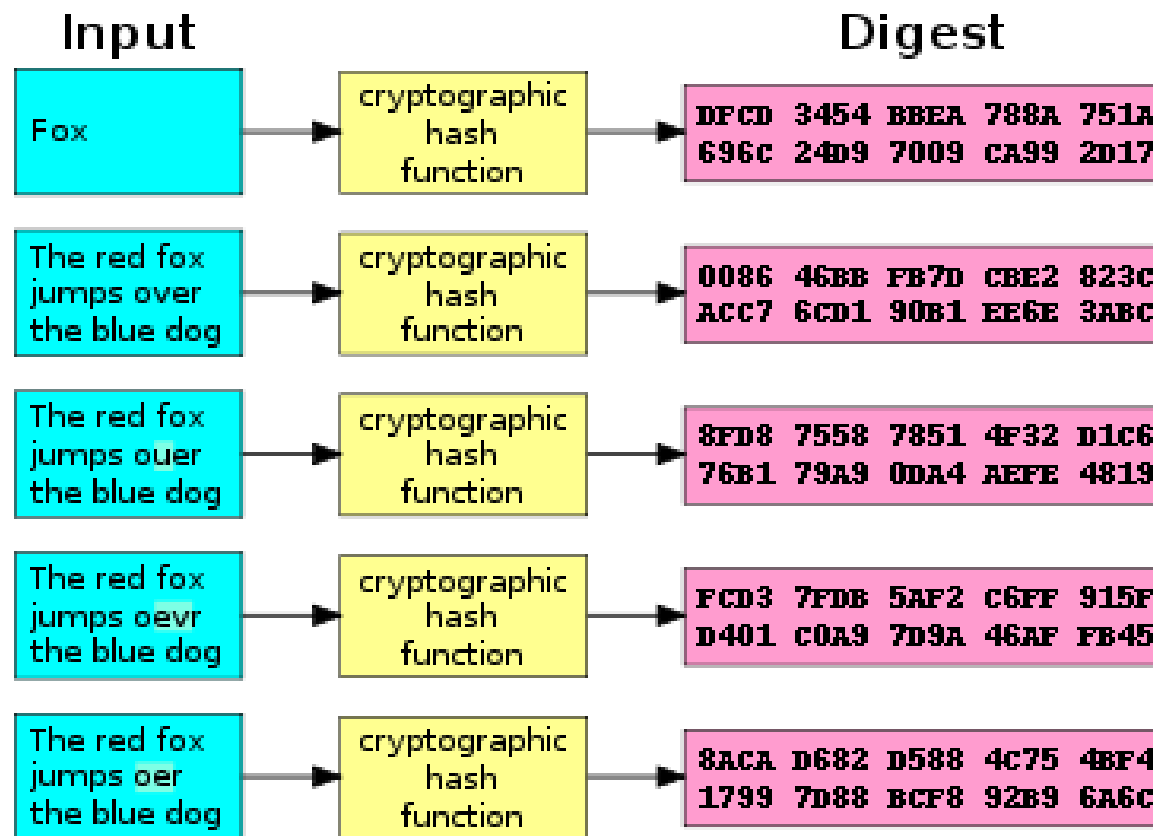
# Kriptografske funkcije sažetka



# Kriptografska funkcija sažetka (*hash*)

$H$  je deterministički algoritam  $H: \{0,1\}^* \rightarrow \{0,1\}^n$  koji proizvoljnoj *poruci* pridružuje *sažetak* fiksne duljine.

```
$ echo -n "fer" | shasum
cef48cb4569d34364e0e86067efa14fbe9b4591e -
$ echo -n "fer" | shasum
cef48cb4569d34364e0e86067efa14fbe9b4591e -
$ echo -n "Fer" | shasum
4514751a6511a102351de1f2b6abf0d6633c401f -
$ shasum big.txt
0c496df552232e34beaba1e15046f87e147d14f6 big.txt
$ shasum empty.txt
da39a3ee5e6b4b0d3255bfeef95601890afd80709 empty.txt
```



Izvor: wikipedia.org

# Funkcije sažetka – sigurnost

- Želimo da se ponaša „kao da je potpuno slučajna” te da sažetak dokumenta u praksi jedinstveno određuje originalni dokument.
- Kriptografska funkcija sažetka  $H$  je *otporna na kolizije* ako je praktički nemoguće pronaći dvije različite poruke  $x$  i  $y$  takve da vrijedi  $H(x) = H(y)$ .

Kolizije uvijek postoje, ali ih je jako teško pronaći!

# Funkcije sažetka – sigurnost

- Nije svaka hash funkcija kriptografska hash funkcija!
- *Checksum* (CRC32, CRC64, ...) nije kriptografska hash funkcija!

# Funkcije sažetka – primjene

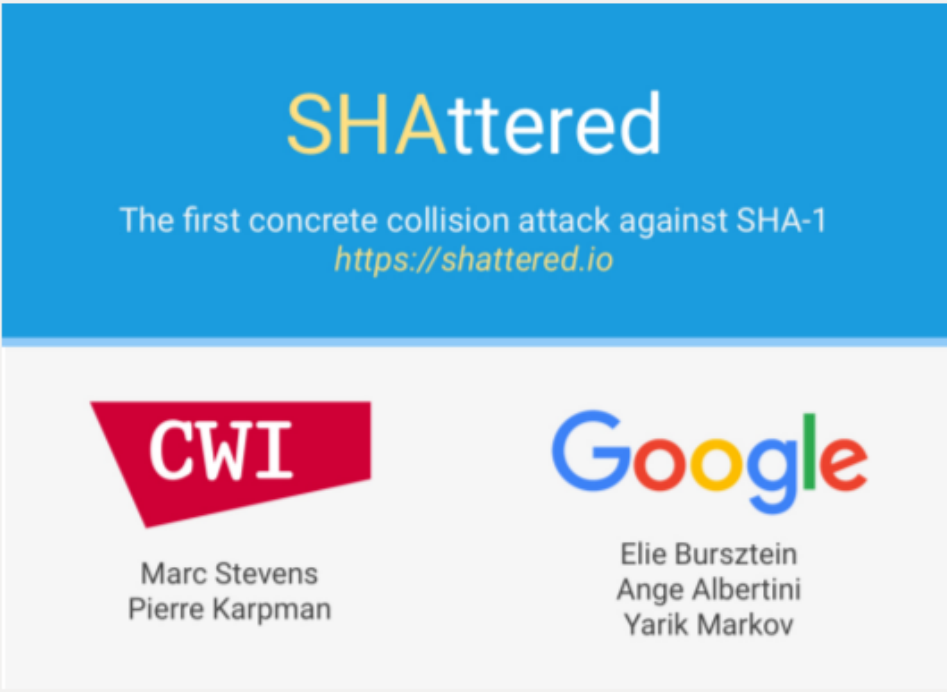
- Integritet datoteka: Spremate važnu datoteku na FER web kako bi je dohvatili s drugog računala. Kako možete biti sigurni da administratori nisu promijenili vašu datoteku?
- Deduplikacija: Odredite koliko različitih datoteka postoji na disku vašeg računala i pronađite sve duplikate.

# Funkcije sažetka – primjene u kriptografiji

- Integritet poruka
- Zaštita zaporki
- Deriviranje ključeva iz zaporki
- Generiranje pseudoslučajnih brojeva
- Digitalni potpisi
- *Proof-of-work* kod kriptovaluta
- ...

# Hash funkcije – napad grubom silom

- Algoritam:
  1. Izaberi slučajnu poruku  $m$
  2. Izračunaj  $h = H(m)$  i zapamti par  $(h, m)$
  3. Ako smo već vidjeli  $(h, m')$  gdje je  $m' \neq m$  onda smo gotovi
  4. Skoči na korak 1.
- Iz paradoksa rođendana (*birthday paradox*) slijedi da je, u očekivanju, potrebno oko  $1.2 * 2^{\frac{n}{2}}$  iteracija da se pronađe kolizija.



SHattered


The first concrete collision attack against SHA-1  
<https://shattered.io>

CWI

Marc Stevens  
Pierre Karpman

Google

Elie Bursztein  
Ange Albertini  
Yarik Markov



SHattered

The first concrete collision attack against SHA-1  
<https://shattered.io>

CWI

Marc Stevens  
Pierre Karpman

Google

Elie Bursztein  
Ange Albertini  
Yarik Markov

```

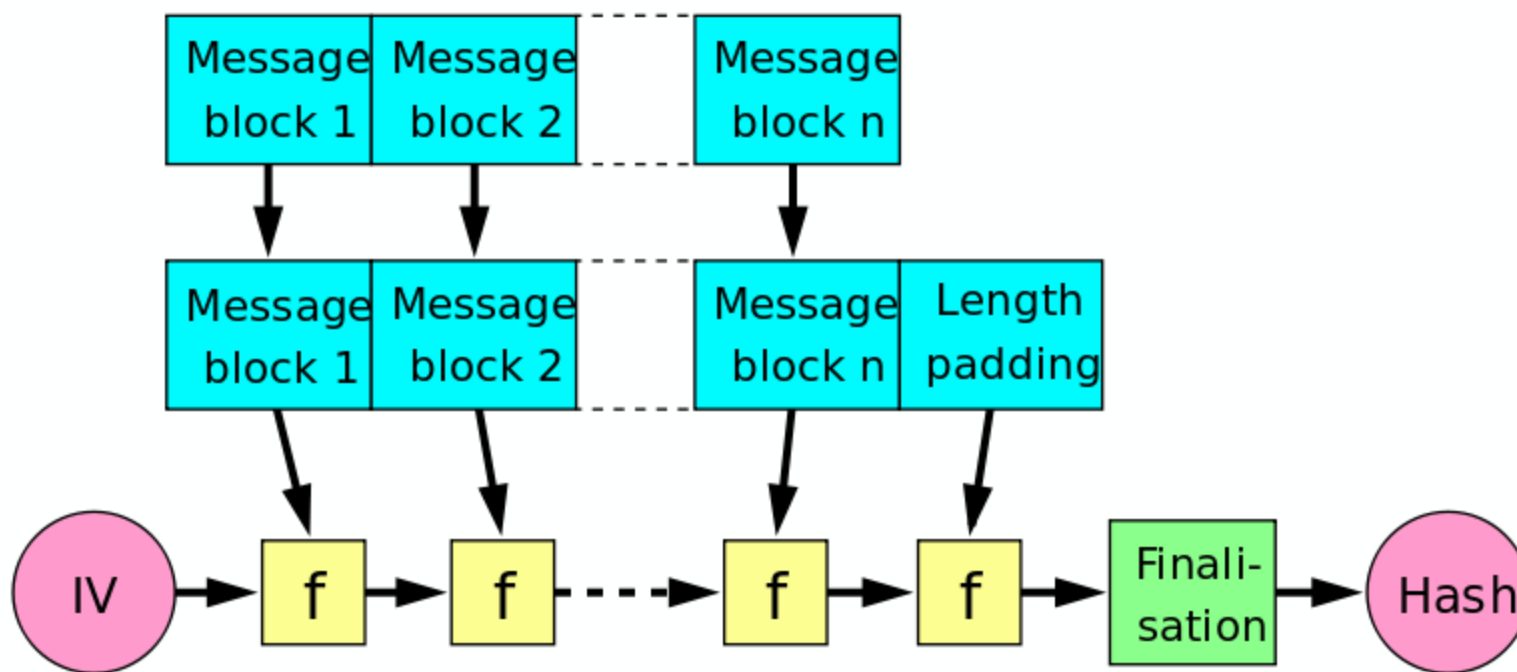
└─ sha1sum *.pdf
38762cf7f55934b34d179ae6a4c80cadccb7f0a 1.pdf
38762cf7f55934b34d179ae6a4c80cadccb7f0a 2.pdf
└─ /tmp/sha1
└─ sha256sum *.pdf
2bb787a73e37352f92383abe7e2902936d1059ad9f1ba6daaa9c1e58ee6970d0 1.pdf
d4488775d29bdef7993367d541064dbdda50d383f89f0aa13a6ff2e0894ba5ff 2.pdf

```

0.64G
8-11h



# Merkle–Damgård konstrukcija



Izvor: wikipedia.org

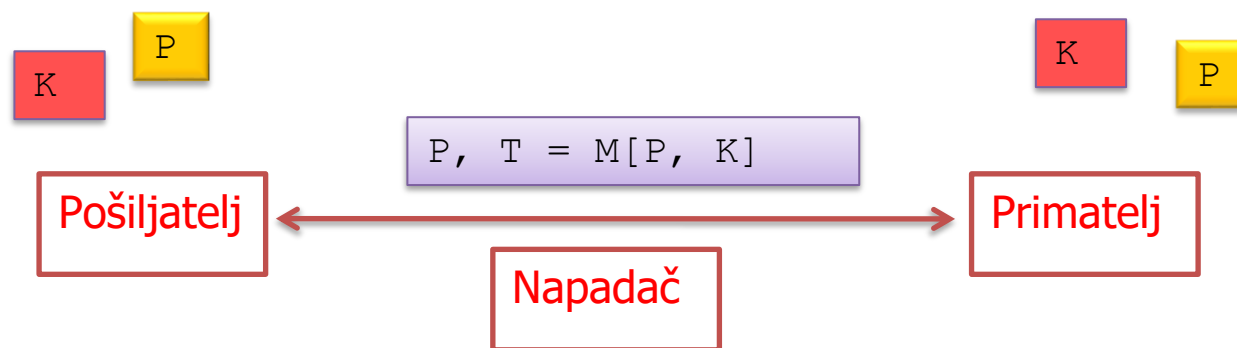
# Primjeri kriptografskih funkcija sažetka

- MD5 (1992)
  - izlaz 128 bita, smatra se potpuno nesigurnom
- SHA-1 (1993)
  - izlaz 160 bita, smatra se nesigurnom
- SHA-256 / SHA-512 (2001)
  - dio NIST standarda
- SHA-3 (2015)
  - razne veličine izlaza
  - dio NIST standarda
  - spužvasta konstrukcija
  - pripada Keccak obitelji sustava

Osnove kriptografije i kriptanalize

# Kodovi za integritet poruke

# Kako osigurati integritet komunikacije?



# Kod za integritet poruke

$M$  je deterministički algoritam  $M: \{0, 1\}^* \times \{0, 1\}^k \rightarrow \{0, 1\}^n$  koji proizvoljnoj *poruci* i *ključu* pridružuje *oznaku* (eng. *tag*) fiksne duljine.

*Message Authentication Code (MAC)* ili *Message Integrity Code (MIC)*

## Sigurnost koda za integritet poruke – neformalno

- Kod za integritet poruke je siguran ako je vrlo teško krivotvoriti oznaku, odnosno generirati ispravnu oznaku za proizvoljnu poruku.
- ... čak i ako napadač ima na raspolaganju mnogo parova  $(m_i, t_i)$  gdje je  $t_i = M(m_i, k)$ .

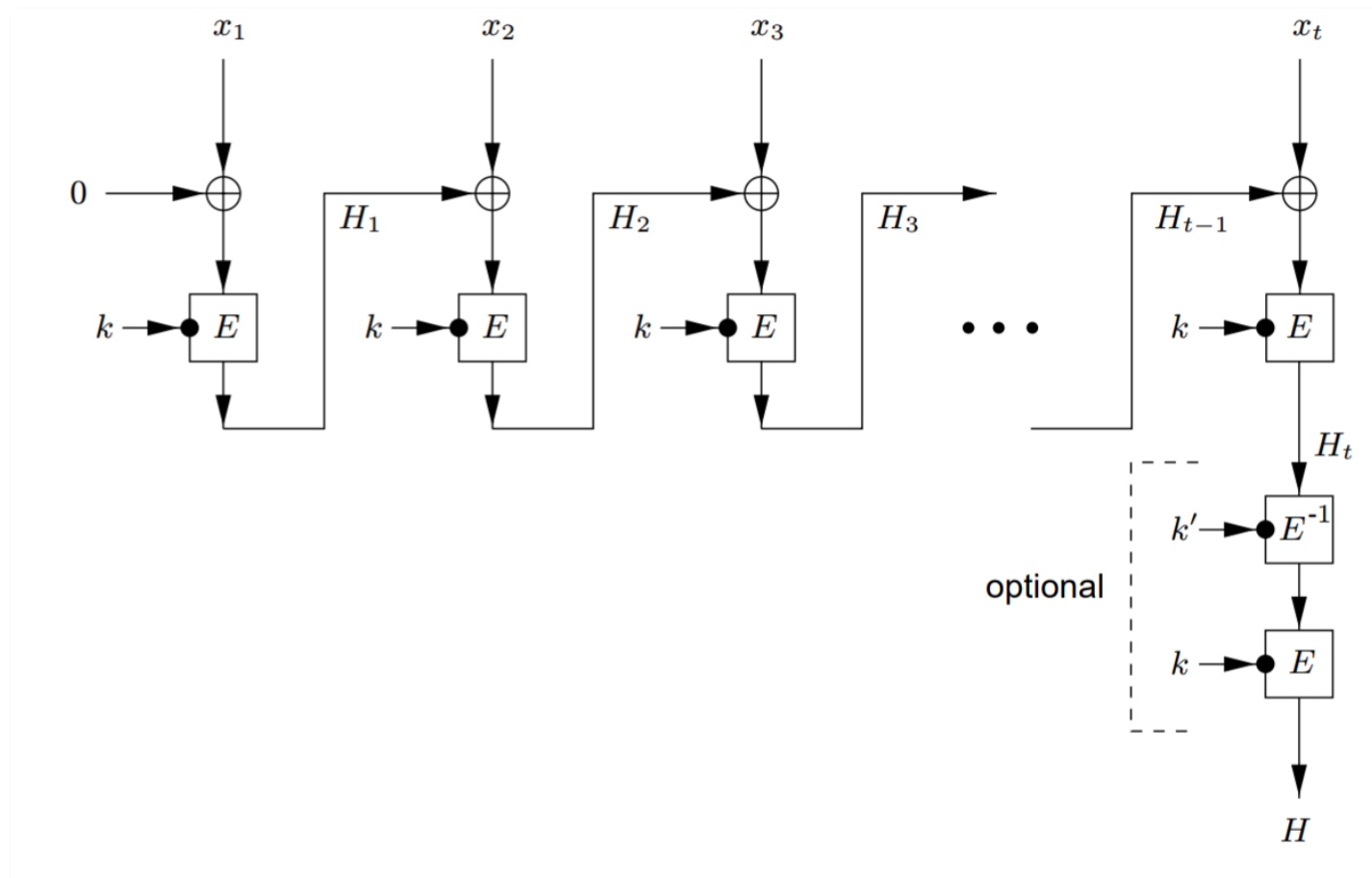
# HMAC – MAC pomoću hash funkcija

- Primjena kriptografskih hash funkcija
- Definiran u RFC2104

$$HMAC(m, k) = H(k \oplus opad || H(K \oplus ipad || m))$$

# MAC pomoću blok šifre

- Primjer: CBC-MAC





# Primjeri kodova za integritet poruka

- HMAC konstrukcija
  - bazirana na kriptografskim funkcijama sažetka
- CBC-MAC, OMAC, PMAC konstrukcije
  - bazirani na blok šiframa
- Poly1305 (2005.)
  - baziran na univerzalnim funkcijama sažetka (*universal hashing*) i blok šiframa

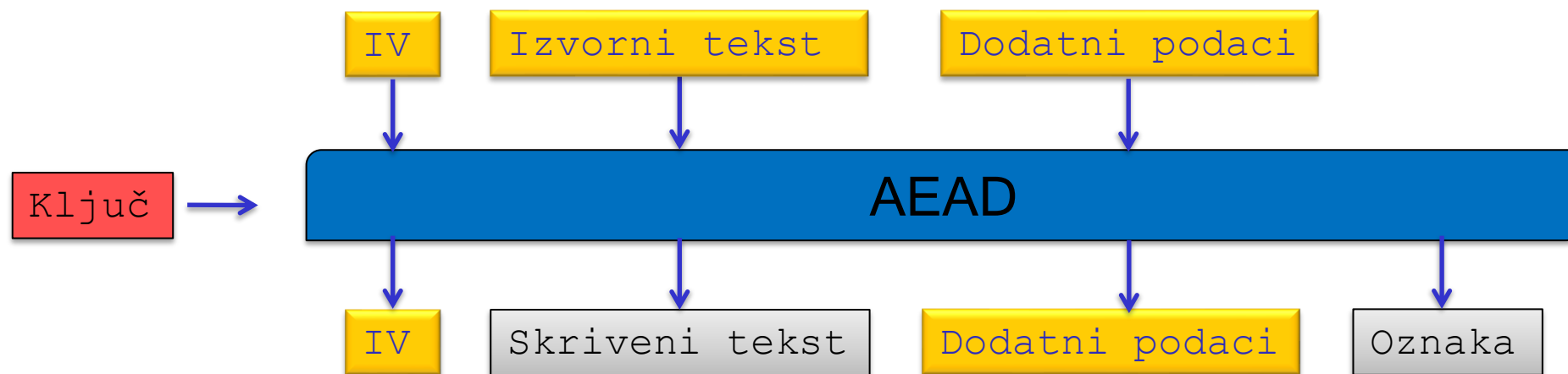
# Povjerljivost i integritet?

- Encrypt-and-MAC:  $E(m, k_1), M(m, k_2)$ 
  - SSH, generalno nesigurna konstrukcija
- MAC-then-Encrypt:  $E(m || M(m, k_2), k_1)$ 
  - Stare verzije TLS-a, 802.11i, može biti nesigurno, POODLE napad (CVE-2014-3566)
- Encrypt-then-MAC:  $c = E(m, k_1), M(c, k_2)$ 
  - IPSec, TLS nakon verzije 1.2

Ključevi  $k_1$  i  $k_2$  moraju biti različiti!

# Autentificirana šifra

- Pruža svojstva povjerljivosti i integriteta u jednom paketu
- *Authenticated-Encryption with Associated-Data*
- Primjer: AES-GCM



# Preporuke

- Koristiti provjerena programska ostvarenja algoritama
  - NIKAKO se NE preporuča vlastita implementacija
- NE koristiti način kriptiranja ECB
- IV generirati slučajno
- NE koristiti stalno isti simetrični ključ
- Gotovo uvijek je potrebno osigurati i integritet

# Hvala!