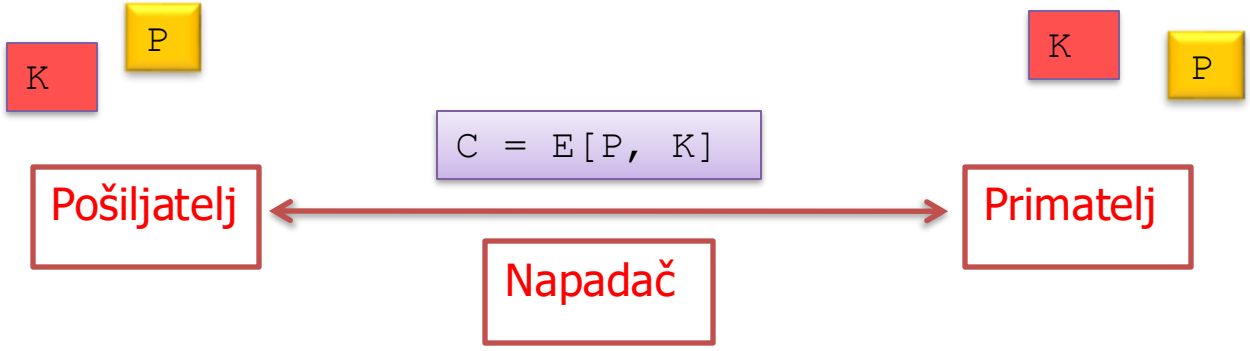
Ponavljanje: Simetrična enkripcija

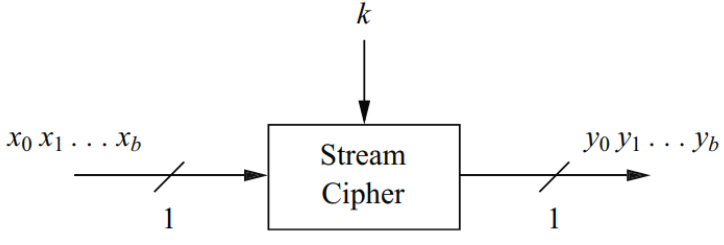


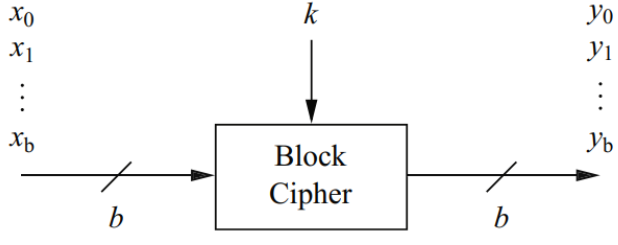
Ponavljanje: Simetrična enkripcija – definicija

- Neka su K, M i C konačni skupovi – prostor ključeva, prostor jasnih tekstova i prostor skrivenih tekstova.
- Simetrična enkripcija je par algoritama E i D ($E: M \times K \to C$, $D: C \times K \to M$) gdje za svaki $k \in K$ i $m \in M$ vrijedi
- $$D(E(m,k),k) = m.$$

Ponavljanje: vrste simetrične enkripcije

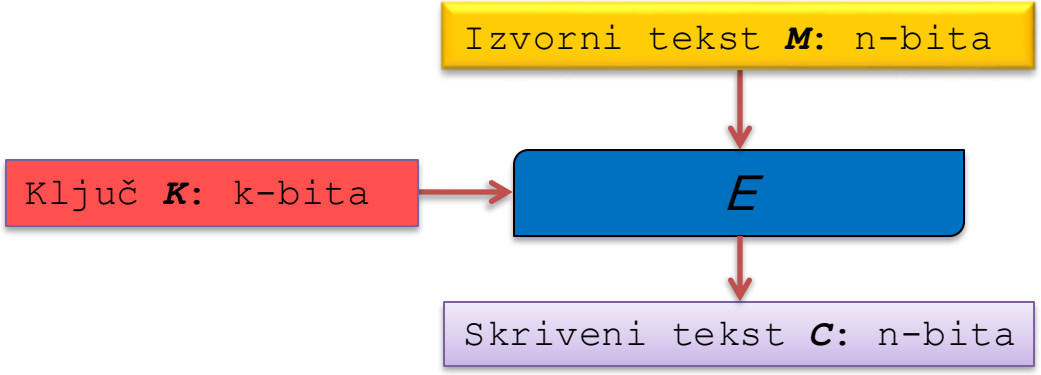
- Protočna enkripcija (*eng. stream cipher)*
  - Kriptira se jedan po jedan bit.
- Sustavi kriptiranja bloka (*eng. block cipher*)
  - Kriptiraju se blokovi fiksne duljine.



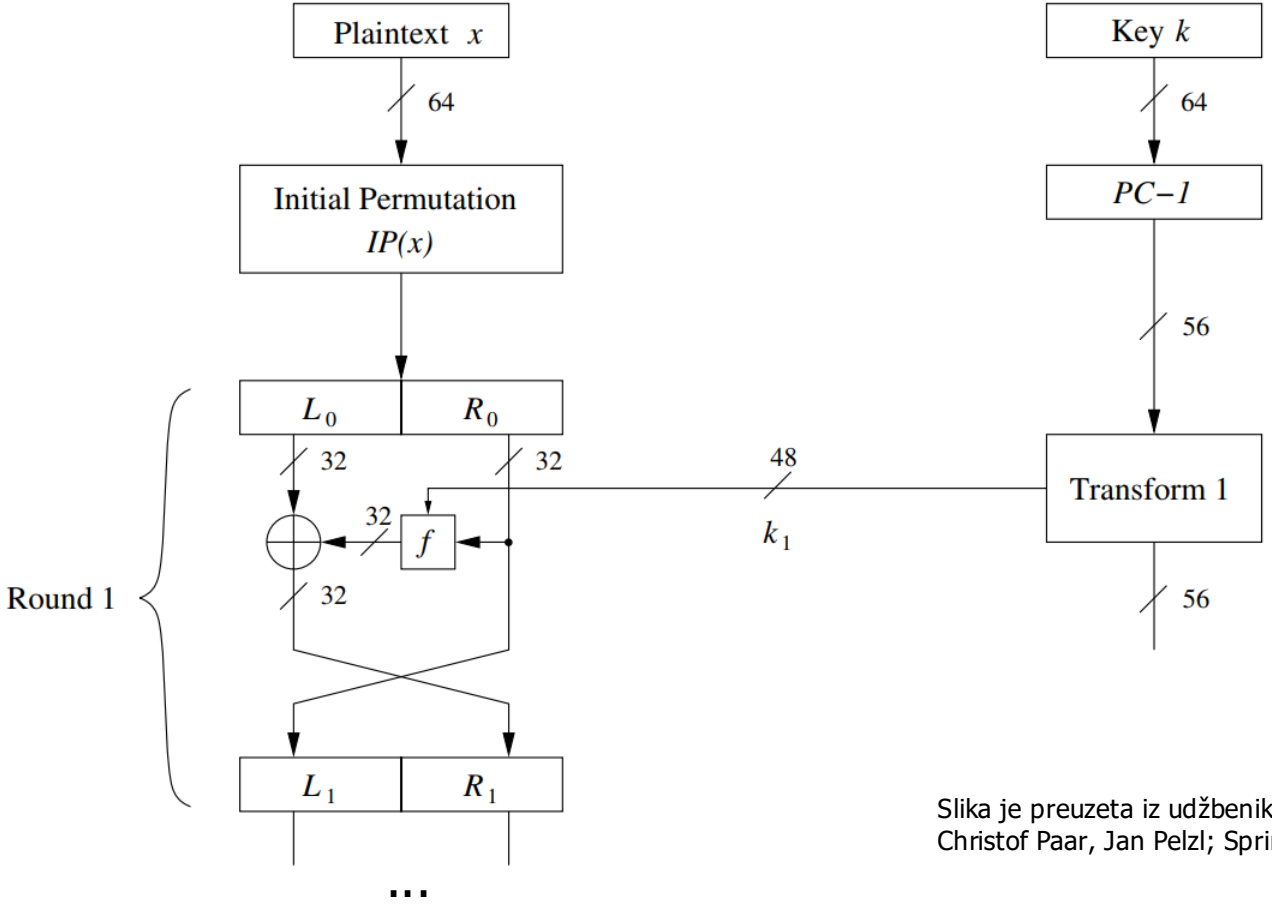


Ponavljanje: sustav kriptiranja bloka

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

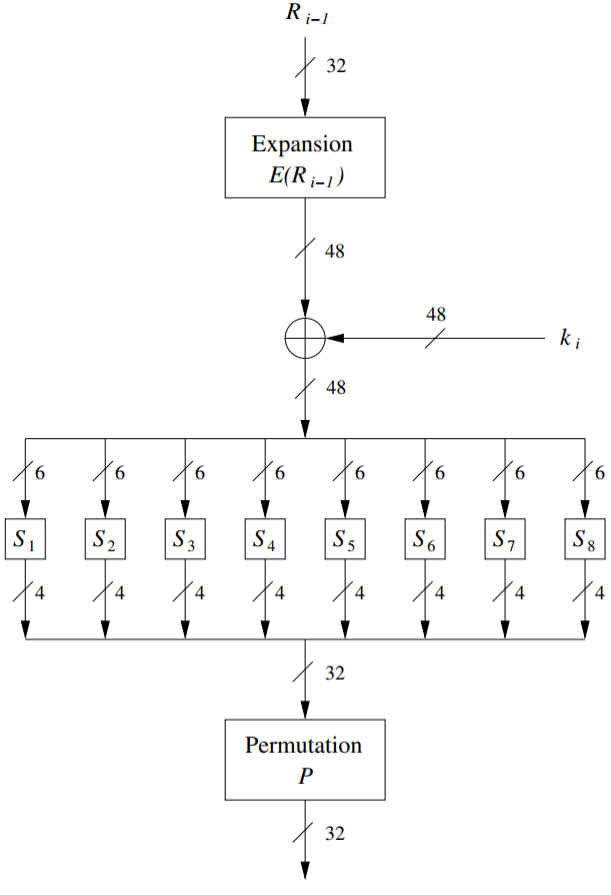


Ponavljanje: DES – Feistelova mreža



Slika je preuzeta iz udžbenika: ***Understanding Cryptography***, Christof Paar, Jan Pelzl; Springer-Verlag Berlin Heidelberg, 2009.

Ponavljanje: DES – Funkcija f



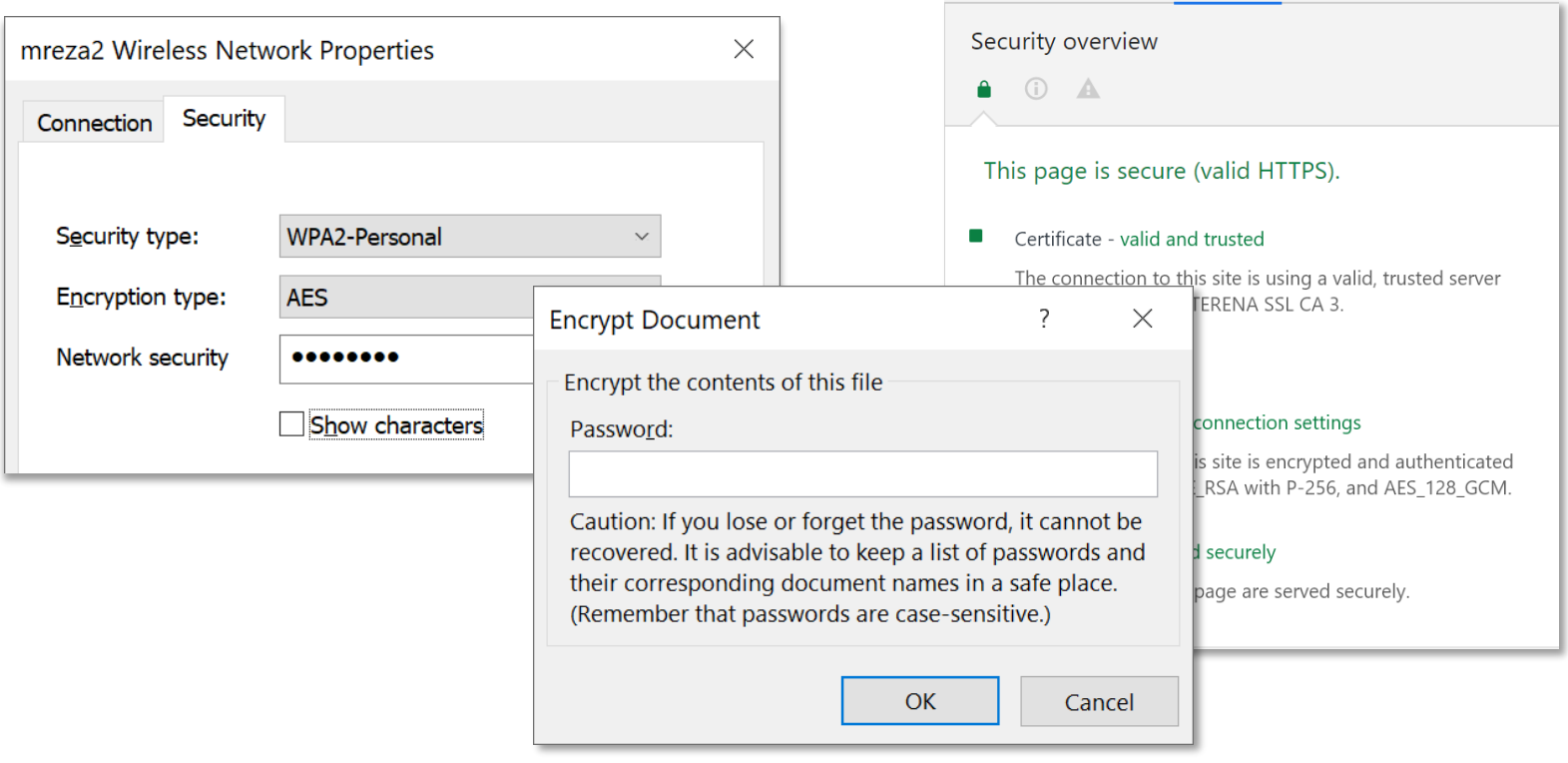
Slika je preuzeta iz udžbenika: ***Understanding Cryptography***, Christof Paar, Jan Pelzl; Springer-Verlag Berlin Heidelberg, 2009.

Zadatak: DES-bez-S

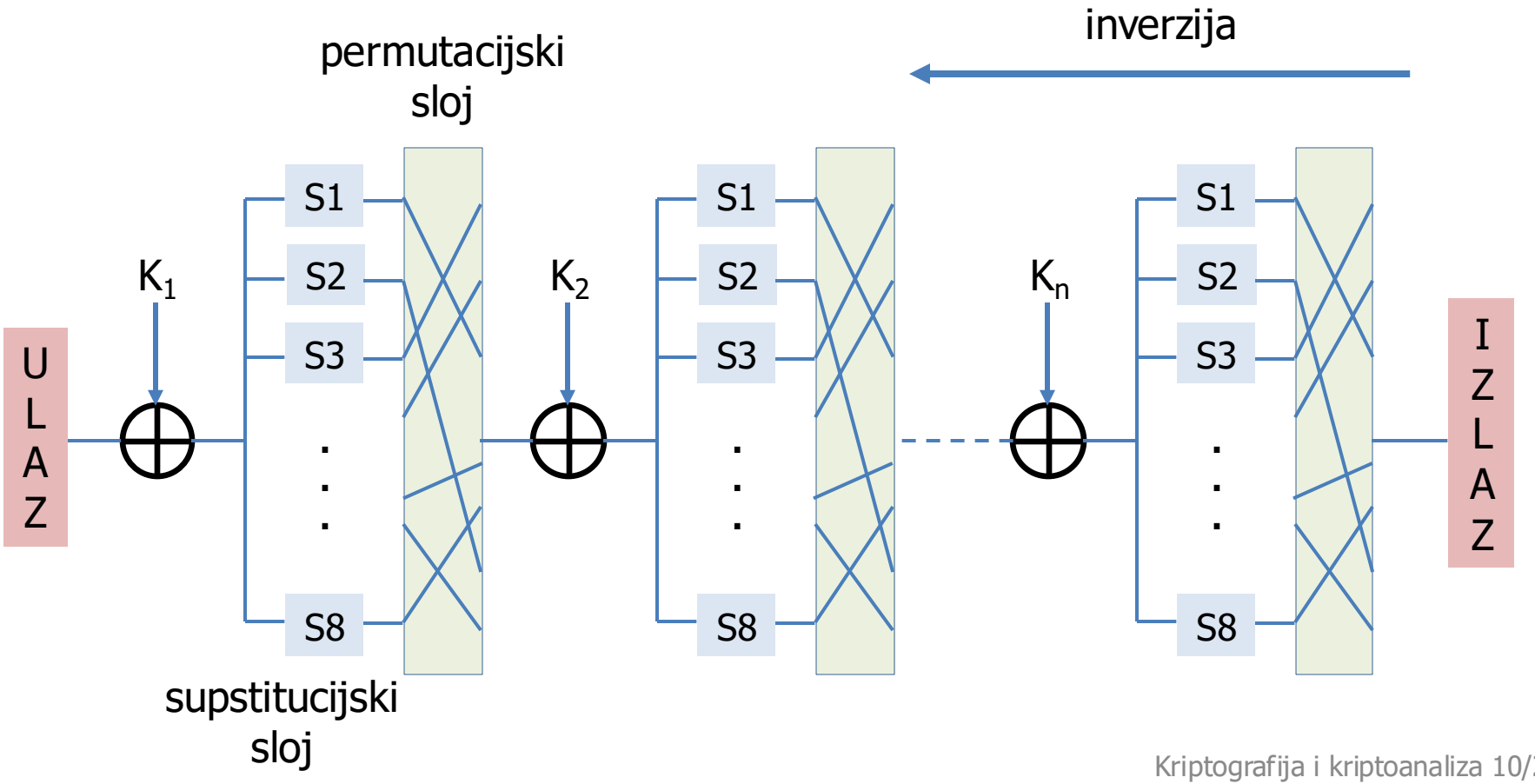
- Sustav DES-bez-S je identičan DES-u osim što nema S-tablice.
- Zadano je nekoliko stotina parova M_i, $C_i = DES\text{–bez–S}(M_i, K)$, pronađite način da dekriptirate nove poruke kriptirane ključem K.

Napredni kriptosustav (AES)

- Natječaj za novi standard je raspisao NIST 1997. godine
- Pobjednik sustav *Rijndael* (autori Vincent Rijmen i Joan Daemen)
- Jednostavna struktura!
- Parametri:
  - Veličina bloka: 128 bitova
  - Veličine ključa: 128, 192 ili 256 bitova


mreza2 Wireless Network Properties
Connection
Security
Security type:
WPA2-Personal
Encryption type:
AES
Network security
Show characters
Security overview
This page is secure (valid HTTPS).
Certificate - valid and trusted
The connection to this site is using a valid, trusted server
TERENA SSL CA 3.
connection settings
is site is encrypted and authenticated
RSA with P-256, and AES_128_GCM.
securely
page are served securely.
Encrypt Document
Encrypt the contents of this file
Password:
Caution: If you lose or forget the password, it cannot be recovered. It is advisable to keep a list of passwords and their corresponding document names in a safe place. (Remember that passwords are case-sensitive.)
OK
Cancel

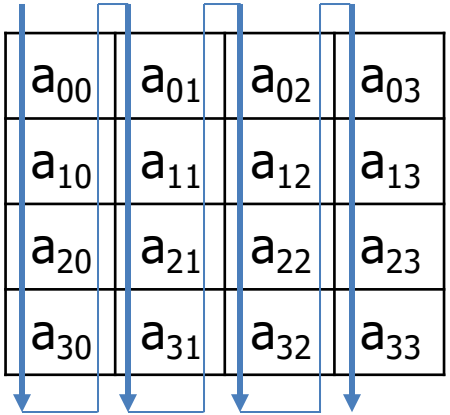
AES: supstitucijsko-permutacijska mreža



Blok

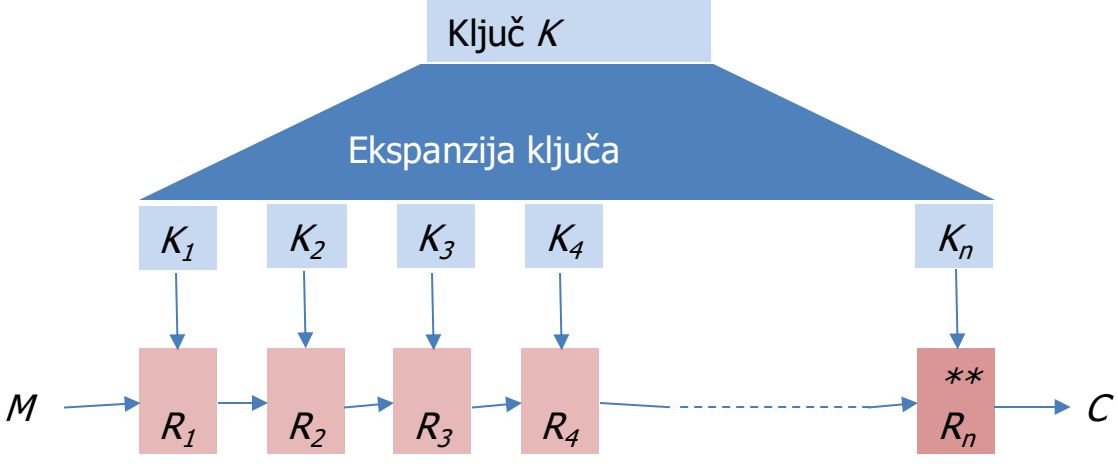
- veličina bloka: 128 bita (AES)
  - izvorni algoritam Rijndael dopušta veličine bloka od 128, 192 ili 256 bita nezavisno od veličine ključa
- pravokutni niz bajtova u četiri retka i četiri stupca $Nb = 4$
- na sličan način se tretira i ključ koji je također smješten u pravokutni niz bajtova u četiri retka, a broj stupaca ovisi o veličini ključa: $Nk = 4, 6,$ ili 8
- broj koraka Nr :

Nr	$Nb = 4$
$Nk = 4$	10
$Nk = 6$	12
$Nk = 8$	14

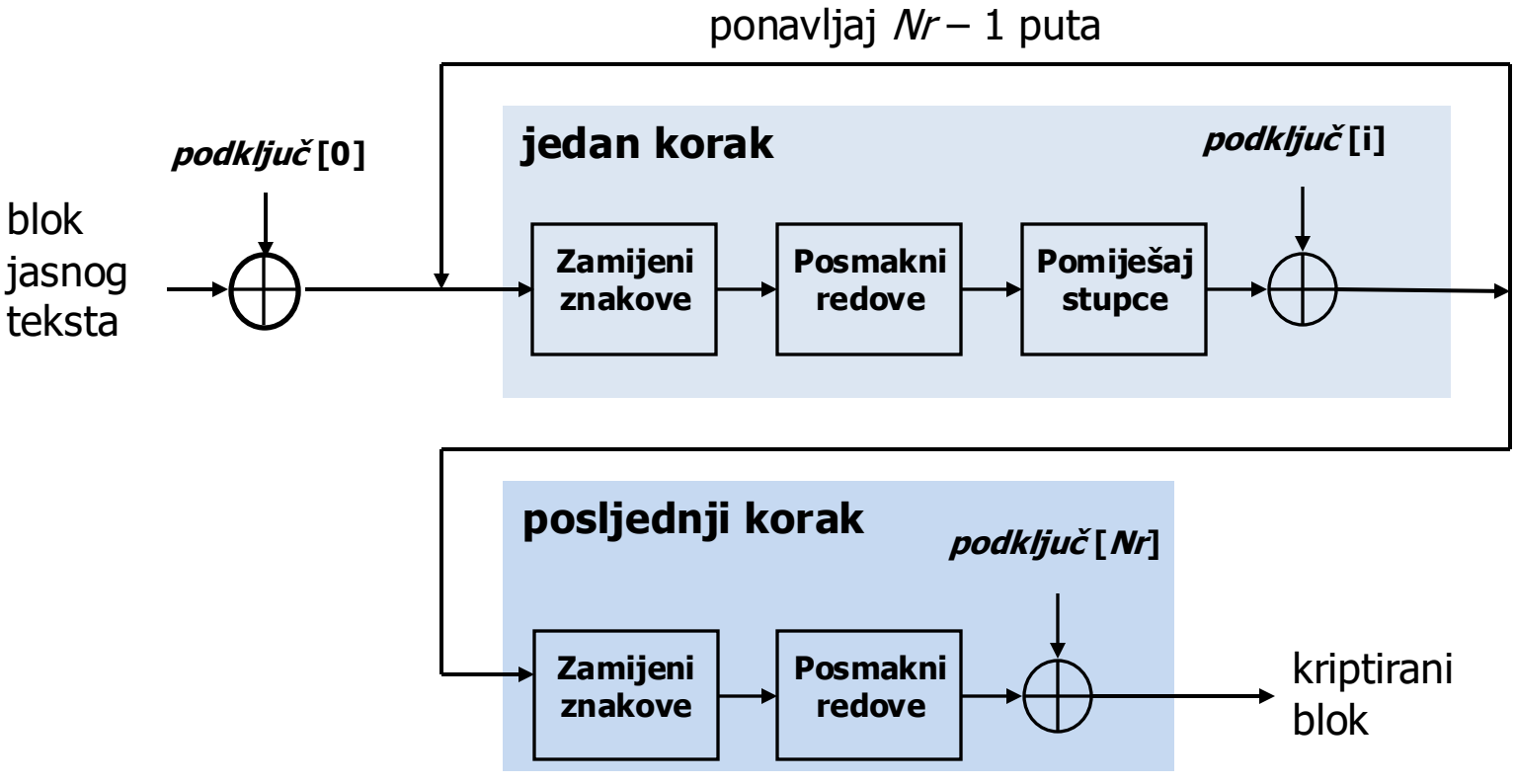


- redoslijed punjenja bloka
  - po stupcima

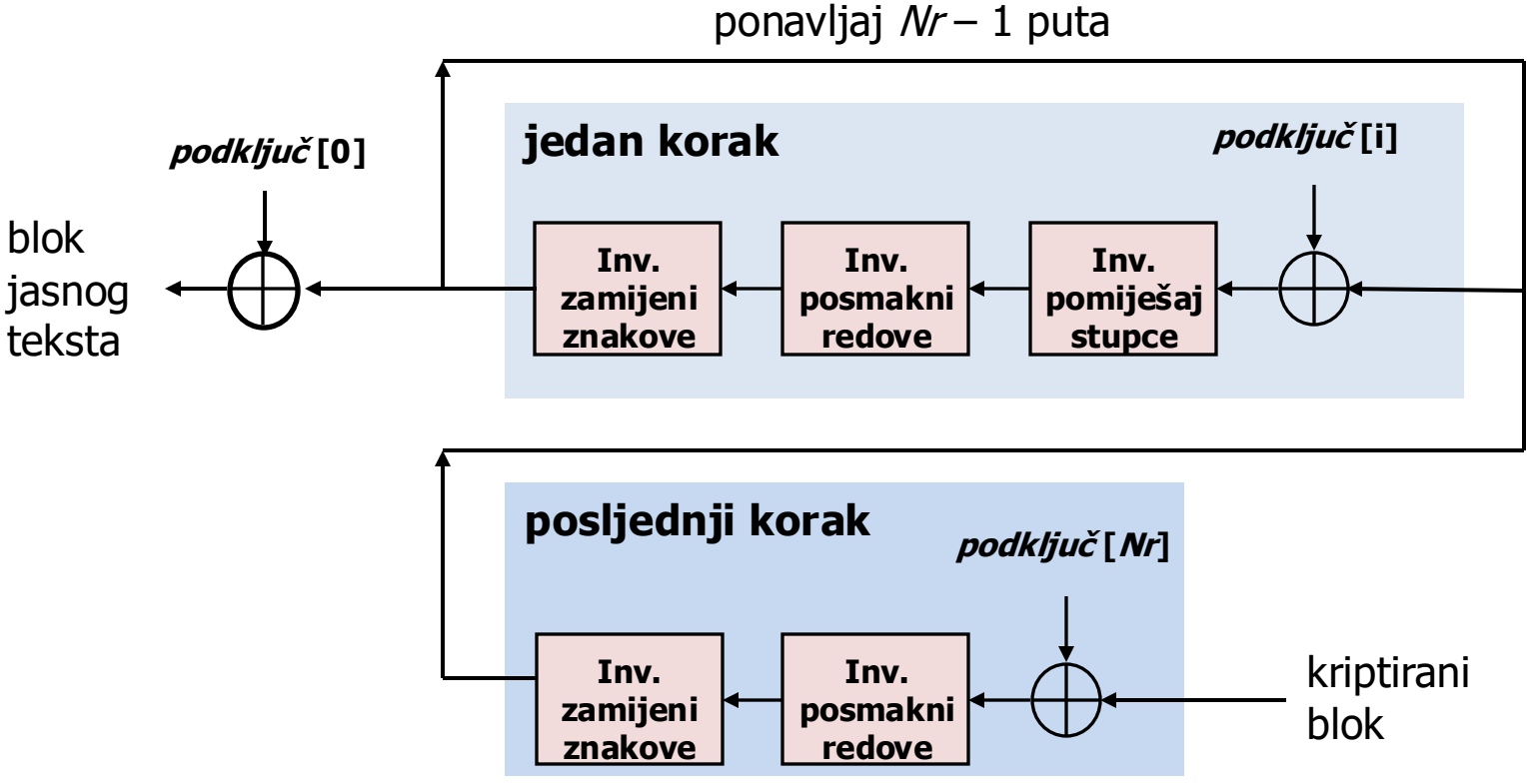
AES – runde



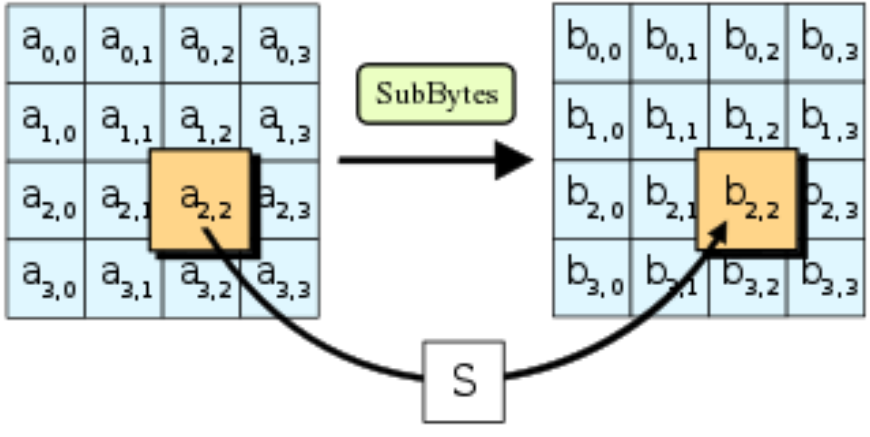
AES – postupak kriptiranja



AES – postupak dekriptiranja

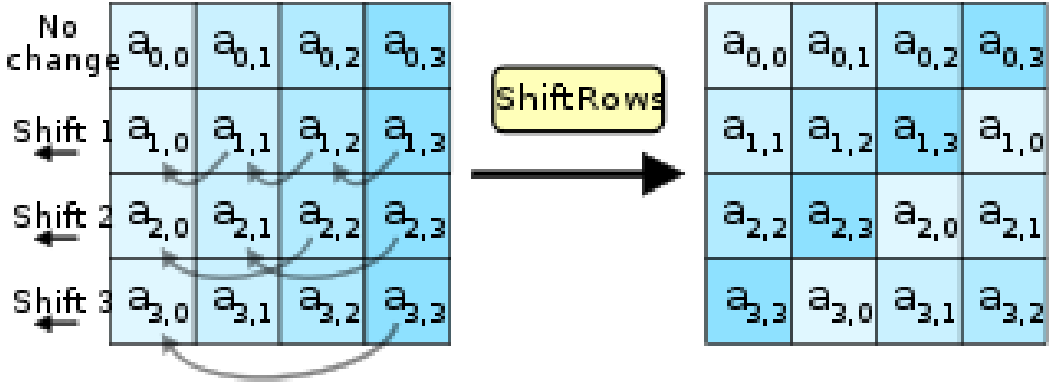


AES128 – Zamijeni znakove



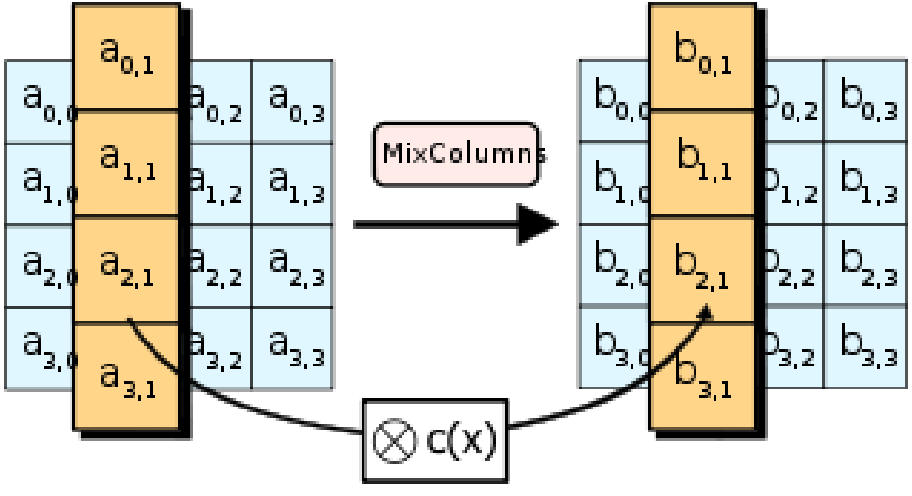
Izvor: wikipedia.org

AES128 – Posmakni redove



Izvor: wikipedia.org

AES128 – Pomiješaj stupce



Izvor: wikipedia.org

Funkcije koje koristi algoritam AES

- *zamijeni znakove*

$$\text{znak} = \text{Sbox}[\text{znak}]$$

- *dodaj podključ*

$$\text{blok} = \text{blok} \oplus \text{podključ}[i]$$

- *posmakni redove*
  - rotira (kružno posmiče) znakove ulijevo i to u drugom, trećem i četvrtom redu bloka (*C1*, *C2* i *C3*) za unaprijed poznati broj mjesta koji ovisi o *Nb*
  - prvi red (*C0*) se ne posmiče

N_b	C_1	C_2	C_3
4	1	2	3
6	1	2	3
8	1	3	4

Funkcije koje koristi algoritam AES

- *pomiješaj stupce*
  - množi se stupac po stupac bloka (tako da se svaki stupac promatra kao četveročlani polinom) s fiksnim polinomom
    $a(x) = 03_H x^3 + 01_H x^2 + 01_H x + 02_H$ modulo x^4+1
  - odnosno, za svaki stupac bloka računa se stupac novog stanja:

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

AES – detalji koji nisu jako bitni

- Supstitucijske tablice imaju jednostavan matematični opis: inverz i afina funkcija u $GF\ (2^8)$.
- Ekspanzija ključa nešto složenija nego kod DES-a: XOR i supstitucijske tablice.
- Dizajn omogućuje vrlo efikasne softverske i hardverske implementacije.

Podsjetnik: Shannonova načela

- Difuzija
  - svaki bit jasnog teksta kao i svaki bit tajnog ključa treba utjecati na mnogo bitova kriptiranog teksta
  - promjena samo jednog bita jasnog teksta mora uzrokovati promjenu (statistički) polovicu bitova kriptiranog teksta
  - ostvaruje se primjerice permutacijom i u više koraka algoritma
- Konfuzija
  - međuzavisnost kriptiranog i jasnog teksta je previše složena da bi se mogla iskoristiti za razbijanje kriptosustava
  - svaki bit kriptiranog teksta treba ovisiti o više bitova ključa ali tako da se pritom prikrije veza između njih
  - ostvaruje se primjerice supstitucijom, tj. supstitucijskim tablicama

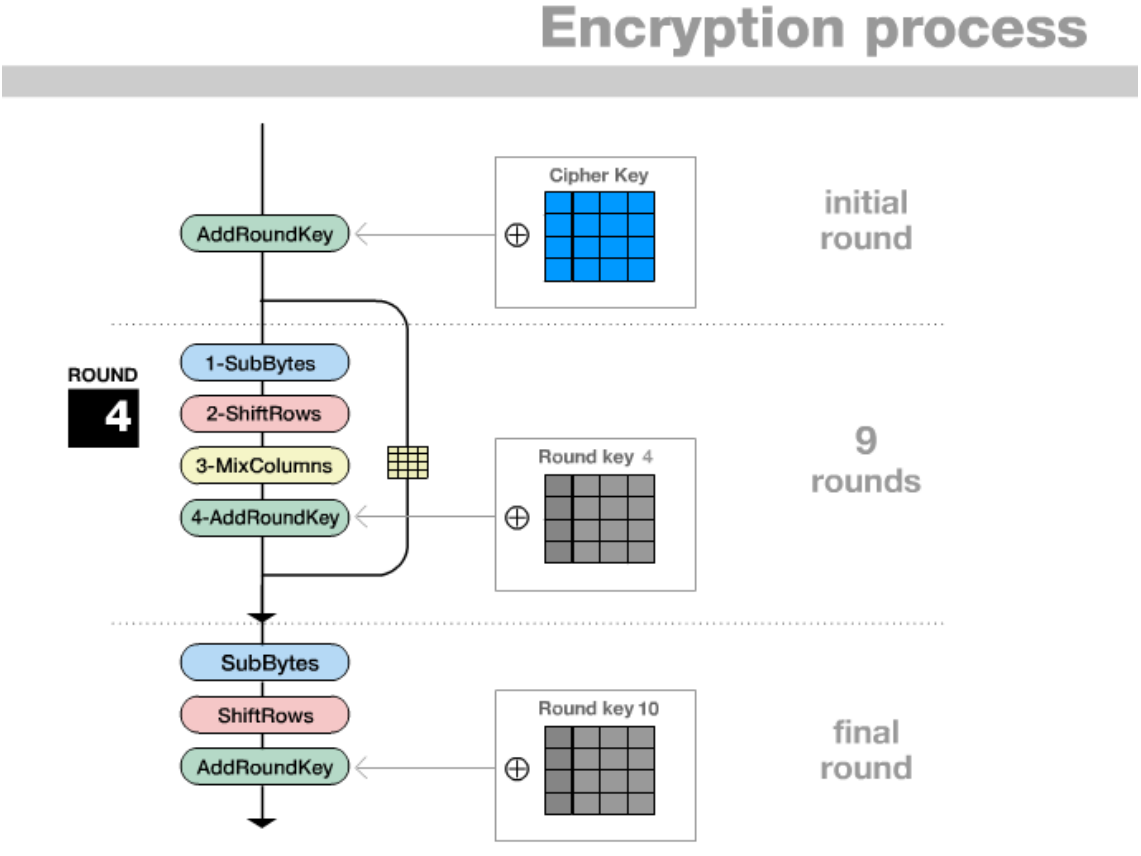
Zašto ovakav dizajn?

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.

Simulacija AES-a



https://www.youtube.com/watch?v=mlzxpkdXP58

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

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

Primjer *uspješnog* napada na AES

- reducirani AES-128 na 8 rundi sa složenošću $\mathbf{2^{124.9}}$

- potpuni AES-128 sa složenošću $\mathbf{2^{126.1}}$
- potpuni AES-192 sa složenošću $\mathbf{2^{189.7}}$
- potpuni AES-256 sa složenošću $\mathbf{2^{254.4}}$

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

Zadatak

- Razmatrajte 1AES – AES sa samo jednom rundom.
  - Pokažite da je nesiguran tako da opišete postupak koji će na temelju M i C=1AES(M, K) odrediti ključ K.

Zadatak

- Za one koji žele više: Razmatrajte AES bez jedne od operacija i pokažite da je nesiguran.
  - Ako je dostupno puno parova M_i, C_i onda je moguće dekriptirati bilo koju poruku.

Ponavljanje? Grupe

Grupe. Grupa je matematička struktura koja se sastoji od nepraznog skupa G i binarne operacije $\circ : G \times G \to G$. To znači da je za svaka dva elementa $x, y \in G$ definiran njihov umnožak $x \circ y \in G$. Pri tome zahtjevamo da vrijede sljedeća svojstva

1) **Asocijativnost.** Za sve $x, y, z \in G$ vrijedi

$$(x \circ y) \circ z = x \circ (y \circ z).$$

2) **Postojanje neutralnog elementa.** Postoji element $e \in G$ takav da za svaki $x \in G$ vrijedi

$$e \circ x = x \circ e = x.$$

3) **Postojanje inverznog elementa.** Za svaki $x \in G$ postoji element $x^{-1} \in G$ takav da je

$$x \circ x^{-1} = x^{-1} \circ x = e.$$

Ako je k tome za svaka dva elementa $x, y \in G$ ispunjeno $x \circ y = y \circ x$, onda za G kažemo da je **komutativna** ili **Abelova** grupa.

Izvor: N. Elezović, Linearna algebra 1

Primjeri grupa

- $(\mathbb{Z}, +)$ je grupa
- $(\mathbb{Q} \setminus \{0\}, *)$ je grupa
- $(\mathbb{Z}_N, +)$ je grupa
- $(\mathbb{Z}_N^*, *)$ je grupa
- …

- $(\mathbb{N}, +)$ nije grupa
- $(\mathbb{Q}, *)$ nije grupa
- $(\mathbb{Z}_N, *)$ nije grupa ako je N složen.
- …

Ponavljanje? Polja

Polje. Sljedeća važna matematička struktura jest polje. Polje čini neprazni skup X na kojemu su definirane dvije operacije i koje zadovoljavaju svojstva koja ćemo navesti u nastavku. Operacije ćemo označiti s $+$ i s $\cdot$ iako to ne moraju biti klasične operacije zbrajanja i množenja. Zahtijevamo da bude ispunjeno sljedeće:

1) $(X, +)$ je (aditivna) Abelova grupa,
2) $(X^*, \cdot)$ je (multiplikativna) Abelova grupa, pri čemu je $X^* = X \setminus \{0\}$,
3) vrijede zakoni distribucije, za sve $x, y, z \in X$

$$(x + y) \cdot z = x \cdot z + y \cdot z$$
$$x \cdot (y + z) = x \cdot y + x \cdot z$$

Izvor: N. Elezović, Linearna algebra 1

Primjeri polja

- $(\mathbb{Q}, +, *)$ je polje
- $(\mathbb{R}, +, *)$ je polje
- $(\mathbb{Z}_p, +, *)$ je polje ako je p prost broj
- …

- $(\mathbb{Z}, +, *)$ nije polje
- $(\mathbb{Z}_n, +, *)$ nije polje ako je n složen
- …

Zadatak: DES-bez-S

- Sustav DES-bez-S je identičan DES-u osim što nema S-tablice.
- Zadano je nekoliko stotina parova M_i, $C_i = DES\text{–bez–S}(M_i, K)$, odredite ključ K.

Konačno polje $GF\ (2^8)$

- elementi polja su polinomi oblika:

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

- svaki bajt $a_7a_6a_5a_4a_3a_2a_1a_0$ (niz od 8 bitova) je predstavljen odgovarajućim polinomom

- *zbrajanje* - isključivo ILI
- *množenje* - binarno množenje polinoma modulo fiksni ireducibilni polinom

  $g(x) = x^8 + x^4 + x^3 + x + 1 \equiv 11B_H$