# ADVANCED ENCRYPTION STANDARD (AES)

**Conf.univ.dr. Ana Cristina Dăscălescu**
**Conf.univ.dr. Radu Boriga**

- În ianuarie 1997, NIST a organizat un concurs de criptografie deschis cercetătorilor din întreaga lume, având ca subiect crearea unui nou standard, care să înlocuiască DES.

- Regulile concursului erau:
  - algoritmul să fie un cifru bloc simetric
  - algoritmul trebuia să suporte chei de 128, 192 şi 256 biţi
  - algoritmul trebuia să se poată implementa atât hardware, cât şi software
  - algoritmul trebuia să fie un standard public sau oferit cu licenţă nediscriminatorie

- În august 1998 NIST a selectat cinci finaliști pe criterii de securitate, eficiență, flexibilitate și cerințe de memorie.

- Finaliștii au fost:
  - **Rijndael** (Joan Daemen și Vincent Rijmen - 86 de voturi)
  - **Serpent** (Ross Anderson, Eli Biham, Lars Knudsen - 56 voturi)
  - **Twofish** (echipa condusă de Bruce Schneier - 31 voturi)
  - **RC6** (RSA Laboratories - 23 voturi)
  - **MARS** (IBM - 13 voturi)

- **Rijndael** se bazează pe teoria câmpului Galois, octeții fiind reprezentați ca elemente în câmpul finit extins $GF(2^8)$.

- Pentru reprezentarea câmpului finit $GF(2^8)$ se poate alege reprezentarea clasică polinomială, cu impact pozitiv asupra complexităţii implementării.
- Octetul $b$, format din biţii $b_7b_6b_5b_4b_3b_2b_1b_0$ și scris sub forma hexazecimală, este considerat ca fiind un polinom de gradul $7$ având coeficienţii egali cu $0$ sau $1$:

$$f(x) = b_7x^7 + b_6x^6 + b_5x^5 + b_4x^4 + b_3x^3 + b_2x^2 + b_1x + b_0$$

- Operaţia de adunare este definită ca suma a două polinoame în care coeficienţii se adună modulo $2$ şi corespunde aplicării operatorului XOR asupra celor doi octeţi corespondenţi.

- Operaţia de înmulţire corespunde produsului a două polinoame modulo un polinom ireductibil $f$ de grad $8$, care pentru AES este:

$$f(X) = 1 + X + X^3 + X^4 + X^8$$

- Câmpul $\mathrm{GF}(2^8)$ definit de polinomul

$$f(X) = 1 + X + X^3 + X^4 + X^8$$

reprezintă mulțimea polinoamelor din clasa de resturi $f(X)$.

- **Exemplu:**

$\{57\} = \{01010111\} = X^6 + X^4 + X^2 + X + 1$

$\{83\} = \{10000011\} = X^7 + X + 1$

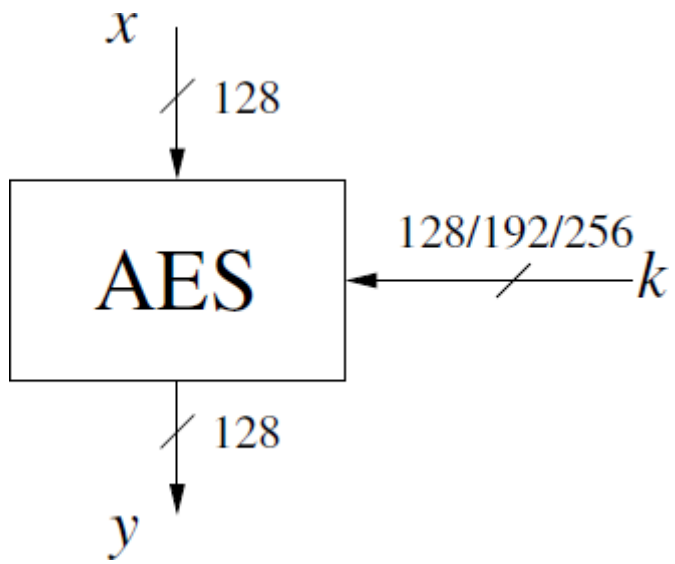
$\{57\} \bullet \{83\} = (X^{13} + X^{11} + X^9 + X^8 + X^6 + X^5 + X^4 + X^3 + 1)$
$mod\ (X^8 + X^4 + X^3 + X + 1) = X^7 + X^6 + 1 = \{11000001\}$

$\{57\} \bullet \{83\} = \{11000001\} = \{C1\}$

- În proiectarea AES s-a ţinut cont de trei criterii:
  - rezistenţa împotriva tuturor atacurilor cunoscute;
  - viteza mare pe un mare număr de platforme (aproximativ 40-50 MB/s);
  - simplicitatea proiectării.

- AES foloseşte substituţii şi permutări!

- Toate operaţiile sunt la nivel de octet, pentru a permite implementări eficiente hardware şi software.




| Lungimea cheii (biți) | Numărul de runde |
|---|---|
| 128 | 10 |
| 192 | 12 |
| 256 | 14 |

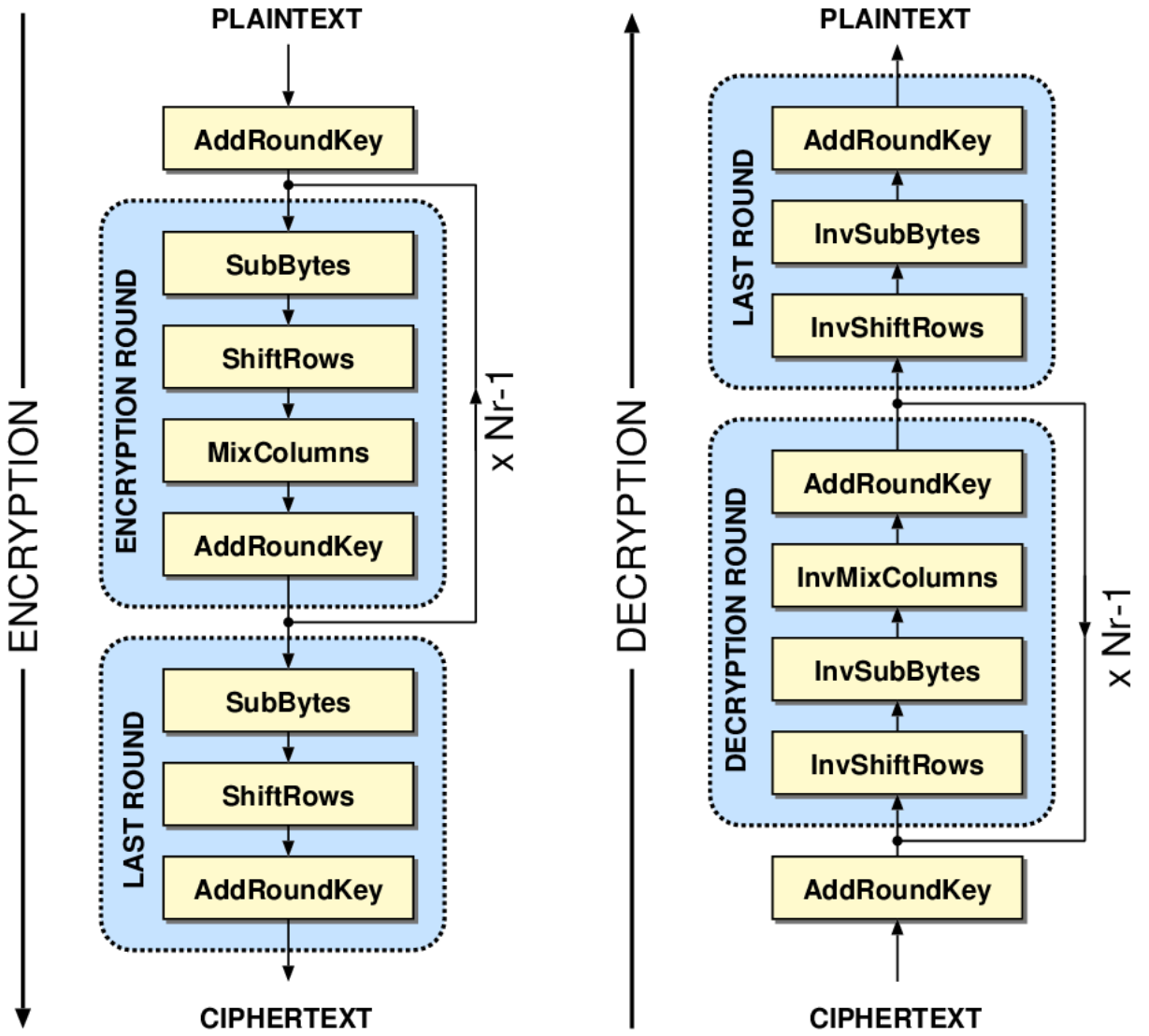
- Vectorul de stare se inițializează cu blocul de 128/192/256 biți din textul clar în ordinea coloanelor, având 4 linii și 4/6/8 coloane.
- O cheie de criptare se va reprezenta în mod similar.
- O stare pentru un bloc de 128 biți și o cheie tot de 128 biți sunt structurate astfel:

| | | | |
|---|---|---|---|
| $A_0$ | $A_4$ | $A_8$ | $A_{12}$ |
| $A_1$ | $A_5$ | $A_9$ | $A_{13}$ |
| $A_2$ | $A_6$ | $A_{10}$ | $A_{14}$ |
| $A_3$ | $A_7$ | $A_{11}$ | $A_{15}$ |

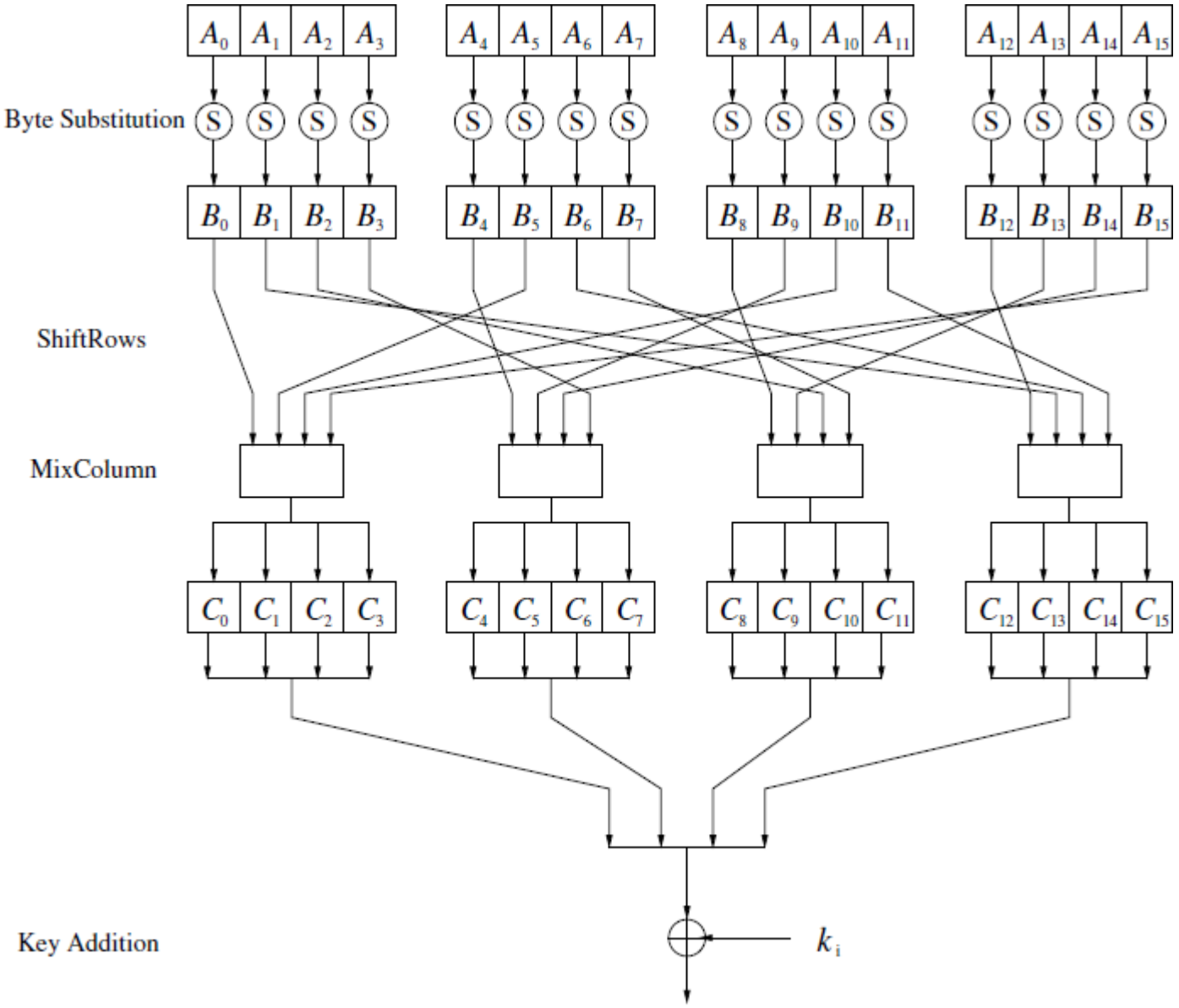
| | | | |
|---|---|---|---|
| $k_0$ | $k_4$ | $k_8$ | $k_{12}$ |
| $k_1$ | $k_5$ | $k_9$ | $k_{13}$ |
| $k_2$ | $k_6$ | $k_{10}$ | $k_{14}$ |
| $k_3$ | $k_7$ | $k_{11}$ | $k_{15}$ |

- Fiecare rundă are la intrare o stare și folosește o cheie de rundă.

- În afara rundei finale, fiecare rundă este formată din 4 transformări.



## STRUCTURA UNEI RUNDE



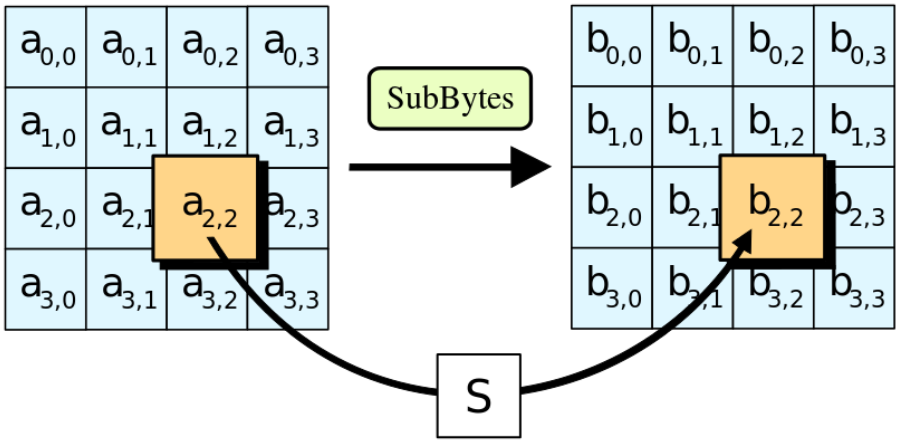
## ➢ Transformarea SubBytes(stare)

| x \ y | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | A | B | C | D | E | F |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 63 | 7C | 77 | 7B | F2 | 6B | 6F | C5 | 30 | 01 | 67 | 2B | FE | D7 | AB | 76 |
| 1 | CA | 82 | C9 | 7D | FA | 59 | 47 | F0 | AD | D4 | A2 | AF | 9C | A4 | 72 | C0 |
| 2 | B7 | FD | 93 | 26 | 36 | 3F | F7 | CC | 34 | A5 | E5 | F1 | 71 | D8 | 31 | 15 |
| 3 | 04 | C7 | 23 | C3 | 18 | 96 | 05 | 9A | 07 | 12 | 80 | E2 | EB | 27 | B2 | 75 |
| 4 | 09 | 83 | 2C | 1A | 1B | 6E | 5A | A0 | 52 | 3B | D6 | B3 | 29 | E3 | 2F | 84 |
| 5 | 53 | D1 | 00 | ED | 20 | FC | B1 | 5B | 6A | CB | BE | 39 | 4A | 4C | 58 | CF |
| 6 | D0 | EF | AA | FB | 43 | 4D | 33 | 85 | 45 | F9 | 02 | 7F | 50 | 3C | 9F | A8 |
| 7 | 51 | A3 | 40 | 8F | 92 | 9D | 38 | F5 | BC | B6 | DA | 21 | 10 | FF | F3 | D2 |
| 8 | CD | 0C | 13 | EC | 5F | 97 | 44 | 17 | C4 | A7 | 7E | 3D | 64 | 5D | 19 | 73 |
| 9 | 60 | 81 | 4F | DC | 22 | 2A | 90 | 88 | 46 | EE | B8 | 14 | DE | 5E | 0B | DB |
| A | E0 | 32 | 3A | 0A | 49 | 06 | 24 | 5C | C2 | D3 | AC | 62 | 91 | 95 | E4 | 79 |
| B | E7 | C8 | 37 | 6D | 8D | D5 | 4E | A9 | 6C | 56 | F4 | EA | 65 | 7A | AE | 08 |
| C | BA | 78 | 25 | 2E | 1C | A6 | B4 | C6 | E8 | DD | 74 | 1F | 4B | BD | 8B | 8A |
| D | 70 | 3E | B5 | 66 | 48 | 03 | F6 | 0E | 61 | 35 | 57 | B9 | 86 | C1 | 1D | 9E |
| E | E1 | F8 | 98 | 11 | 69 | D9 | 8E | 94 | 9B | 1E | 87 | E9 | CE | 55 | 28 | DF |
| F | 8C | A1 | 89 | 0D | BF | E6 | 42 | 68 | 41 | 99 | 2D | 0F | B0 | 54 | BB | 16 |

Transformarea este o substituție neliniară care operează pe octeți. Tabela de substituție (S-box) este o matrice inversabilă formată din compunerea a două transformări:

1. Fiecare octet $b \neq 0$ este înlocuit cu inversul său $b^{-1} \in GF(2^8)$
2. Rezultatul este modificat printr-o transformare afină peste $Z_2$

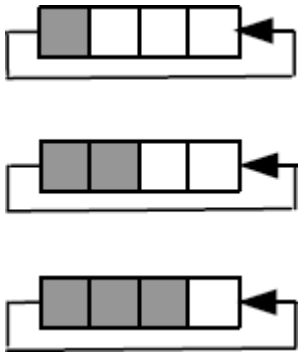
$$\begin{pmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \\ b_4 \\ b_5 \\ b_6 \\ b_7 \end{pmatrix} \equiv \begin{pmatrix} 1&0&0&0&1&1&1&1 \\ 1&1&0&0&0&1&1&1 \\ 1&1&1&0&0&0&1&1 \\ 1&1&1&1&0&0&0&1 \\ 1&1&1&1&1&0&0&0 \\ 0&1&1&1&1&1&0&0 \\ 0&0&1&1&1&1&1&0 \\ 0&0&0&1&1&1&1&1 \end{pmatrix} \begin{pmatrix} b'_0 \\ b'_1 \\ b'_2 \\ b'_3 \\ b'_4 \\ b'_5 \\ b'_6 \\ b'_7 \end{pmatrix} + \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{pmatrix} \quad \text{mod } 2$$



## ➢ Transformarea ShiftRows(stare)

- Liniile stării curente sunt rotite circular spre stânga cu 0, 1, 2 și 3 poziții.

| | | | |
|---|---|---|---|
| $B_0$ | $B_4$ | $B_8$ | $B_{12}$ |
| $B_1$ | $B_5$ | $B_9$ | $B_{13}$ |
| $B_2$ | $B_6$ | $B_{10}$ | $B_{14}$ |
| $B_3$ | $B_7$ | $B_{11}$ | $B_{15}$ |



| | | | |
|---|---|---|---|
| $B_0$ | $B_4$ | $B_8$ | $B_{12}$ |
| $B_5$ | $B_9$ | $B_{13}$ | $B_1$ |
| $B_{10}$ | $B_{14}$ | $B_2$ | $B_6$ |
| $B_{15}$ | $B_3$ | $B_7$ | $B_{11}$ |

## ➢ Transformarea MixColumns(stare)

- Fiecare coloană a stării este privită ca un polinom de gradul 3 cu coeficienți în $GF(2^8)$, fiind apoi înmulțită cu polinomul

$$c(X) = \{03\}X^3 + \{01\}X^2 + \{01\}X + \{02\}$$

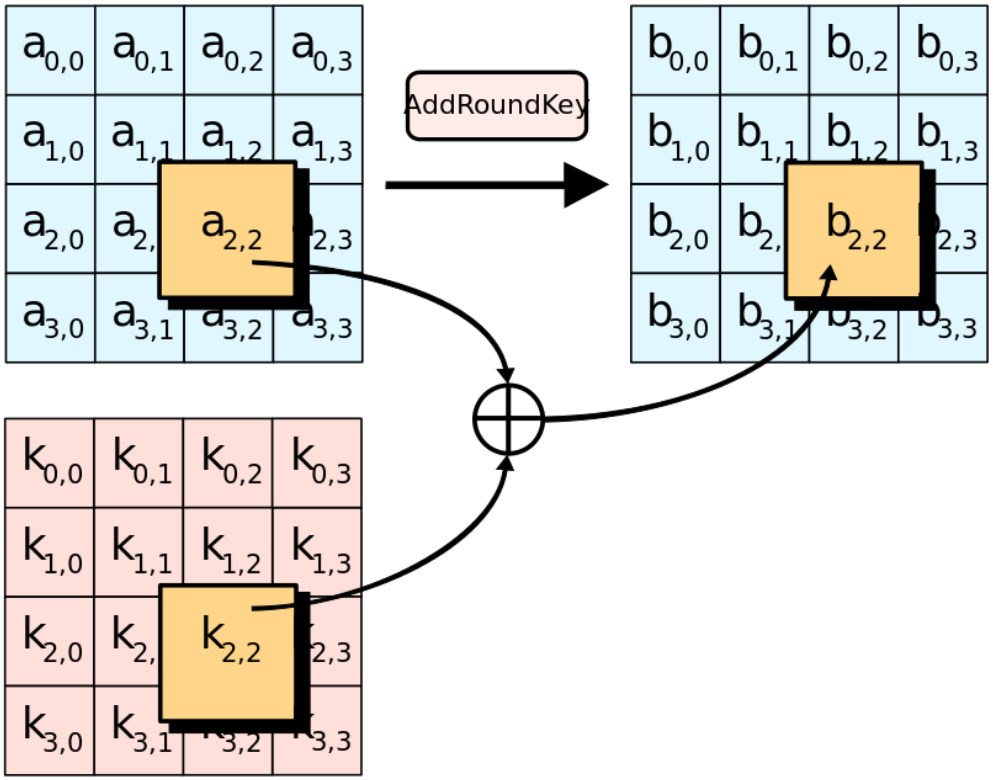
în algebra polinoamelor modulo $X^4 + 1$.

- O formă alternativă a operației **MixColumns** este:

$$\begin{pmatrix} C_0 \\ C_1 \\ C_2 \\ C_3 \end{pmatrix} = \begin{pmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{pmatrix} \begin{pmatrix} B_0 \\ B_5 \\ B_{10} \\ B_{15} \end{pmatrix}$$

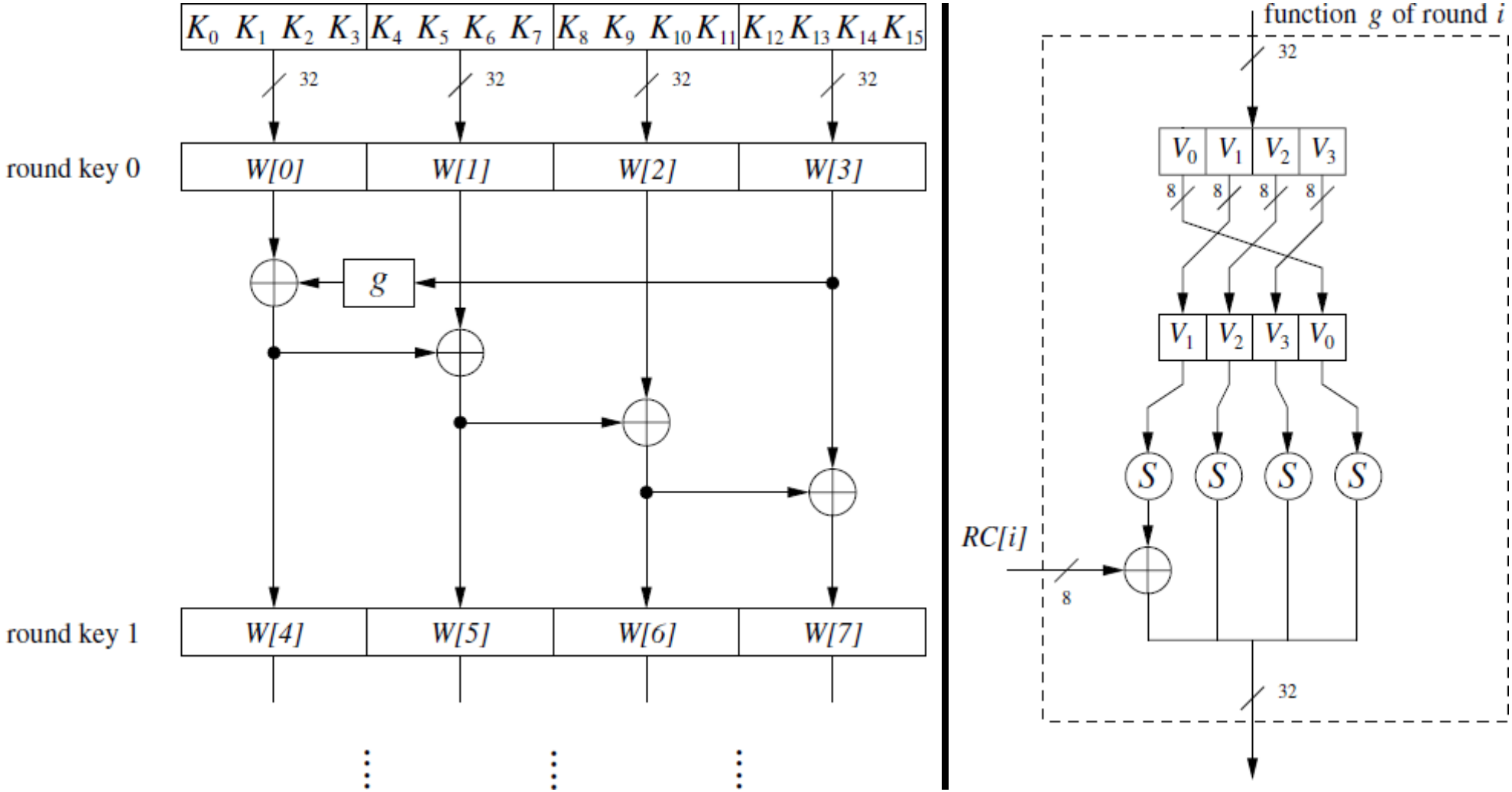
## ➢ Transformarea AddRoundKey(stare,cheie de rundă)

- Se aplică operația XOR între starea curentă și cheia de rundă.
- Cheia de rundă are lungime egală cu cea a cheii de criptare.



## ➢ Generarea cheilor de rundă

- Cheile de rundă sunt derivate din cheia de criptare.
- Numărul cheilor de rundă este mai mare cu 1 decât numărul de runde.
- Generarea cheilor de rundă se realizează la nivel de cuvânt, adică grupuri de 4 octeți.
- Cheile de rundă sunt un alt element de neliniaritate al AES-ului și îi atenuează simetria.


$K_0$ $K_1$ $K_2$ $K_3$
$K_4$ $K_5$ $K_6$ $K_7$
$K_8$ $K_9$ $K_{10}$ $K_{11}$
$K_{12}$ $K_{13}$ $K_{14}$ $K_{15}$
32
round key 0
W[0]
W[1]
W[2]
W[3]
g
round key 1
W[4]
W[5]
W[6]
W[7]
function g of round i
$V_0$ $V_1$ $V_2$ $V_3$
8
$V_1$ $V_2$ $V_3$ $V_0$
S
RC[i]

## ➢ Performanțe AES

| Round | | Number of bits that differ |
|---|---|---|
| | 0123456789abcdeffedcba9876543210<br>0023456789abcdeffedcba9876543210 | 1 |
| 0 | 0e3634aece7225b6f26b174ed92b5588<br>0f3634aece7225b6f26b174ed92b5588 | 1 |
| 1 | 657470750fc7ff3fc0e8e8ca4dd02a9c<br>c4a9ad090fc7ff3fc0e8e8ca4dd02a9c | 20 |
| 2 | 5c7bb49a6b72349b05a2317ff46d1294<br>fe2ae569f7ee8bb8c1f5a2bb37ef53d5 | 58 |
| 3 | 7115262448dc747e5cdac7227da9bd9c<br>ec093dfb7c45343d689017507d485e62 | 59 |
| 4 | f867aee8b437a5210c24c1974cffeabc<br>43efdb697244df808e8d9364ee0ae6f5 | 61 |
| 5 | 721eb200ba06206dcbd4bce704fa654e<br>7b28a5d5ed643287e006c099bb375302 | 68 |
| 6 | 0ad9d85689f9f77bc1c5f71185e5fb14<br>3bc2d8b6798d8ac4fe36a1d891ac181a | 64 |
| 7 | db18a8ffa16d30d5f88b08d777ba4eaa<br>9fb8b5452023c70280e5c4bb9e555a4b | 67 |
| 8 | f91b4fbfe934c9bf8f2f85812b084989<br>20264e1126b219aef7feb3f9b2d6de40 | 65 |
| 9 | cca104a13e678500ff59025f3bafaa34<br>b56a0341b2290ba7dfdfbddcd8578205 | 61 |
| 10 | ff0b844a0853bf7c6934ab4364148fb9<br>612b89398d0600cde116227ce72433f0 | 58 |

## ➢ Avantaje AES

- AES se poate implementa pe un dispozitiv Smart Card, folosind un spaţiu redus de memorie RAM şi un număr redus de cicluri.

- Transformarea din cadrul unei runde este paralelă prin proiectare, ceea ce constituie un avantaj pentru viitoarele procesoare.

- AES nu foloseşte componente criptografice externe, cum ar fi cutii de substituție sau biţi aleatori.

- AES nu foloseşte operaţiuni aritmetice, ci doar operaţii la nivel de şiruri de biţi.

# ➢ Criptanaliza AES

- **Forța brută**
  - Cheia secretă poate avea lungimi de 128, 192 sau 256 de biți, deci un atac de tip forță brută nu poate fi efectuat într-un timp util!

- **Criptanaliză**
  - Singurul atac criptanalitic cunoscut (atacul bipartit) nu pune în pericol securitatea AES, deoarece complexitatea sa este $2^{126.1}$/ $2^{189.7}$/$2^{254.4}$.

- **Atacuri de tip side-channel**
  - Se bazează pe deficiențele de implementare ale unui algoritm de criptare.
  - Au fost publicate mai multe atacuri de acest tip, dar majoritatea sunt greu de aplicat în practică.