ĐẠI NAM
UNIVERSITY

Bài 6

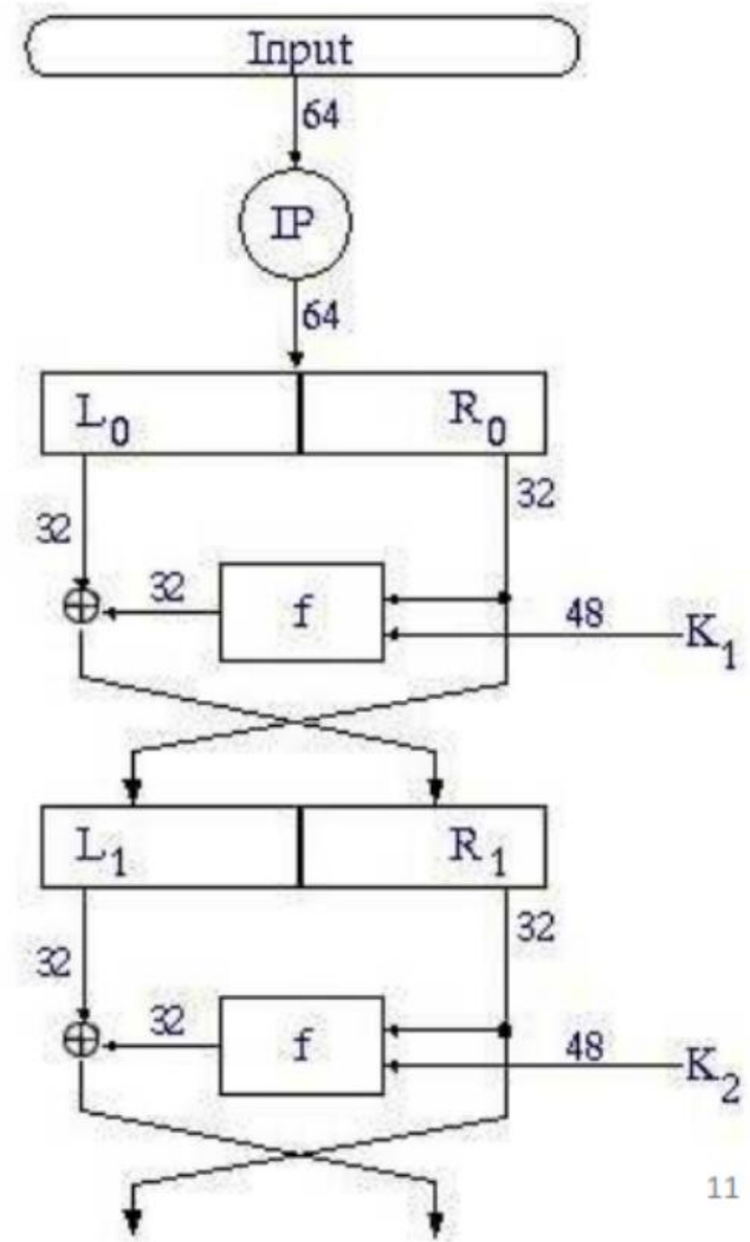
THUẬT TOÁN AES

TS. Trần Đăng Công

Tel: 0964981451

Email: congtd@dainam.edu.vn

- **Thuật toán DES:**
  - $IP(x) = L_0R_0$
  - $L_i = R_{i-1}$
  - $R_i = L_{i-1} \oplus f(R_{i-1}, K_i)$
  - $y = IP^{-1}(R_{16}L_{16})$



Thuật toán DES: 02 bài

1. Truyền - Nhận văn bản có mã hóa DES

2. Truyền - Nhận file có mã hóa DES

1. Giới thiệu

2. Thuật toán AES

4. Luyện tập

- AES (Advanced Encryption Standard), là một thuật toán mã hóa đối xứng, khối được Mỹ áp dụng làm tiêu chuẩn mã hóa năm 2001 thay thế DES.
- Thuật toán được xây dựng dựa trên Rijndael Cipher phát triển bởi 2 nhà mật mã học người Bỉ (Joan Daemen và Vincent Rijmen).

FIPS 197

Federal Information Processing Standards Publication

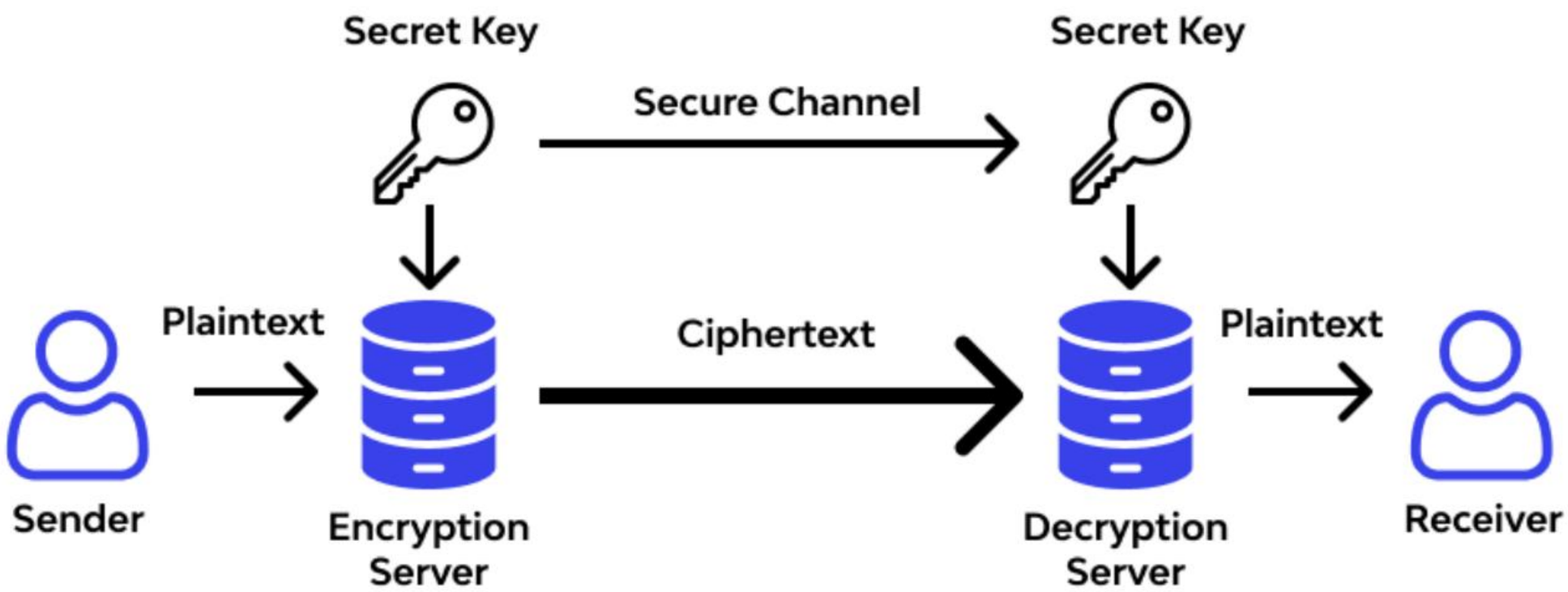
Advanced Encryption Standard (AES)

Category: Computer Security **Subcategory: Cryptography**

Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8900

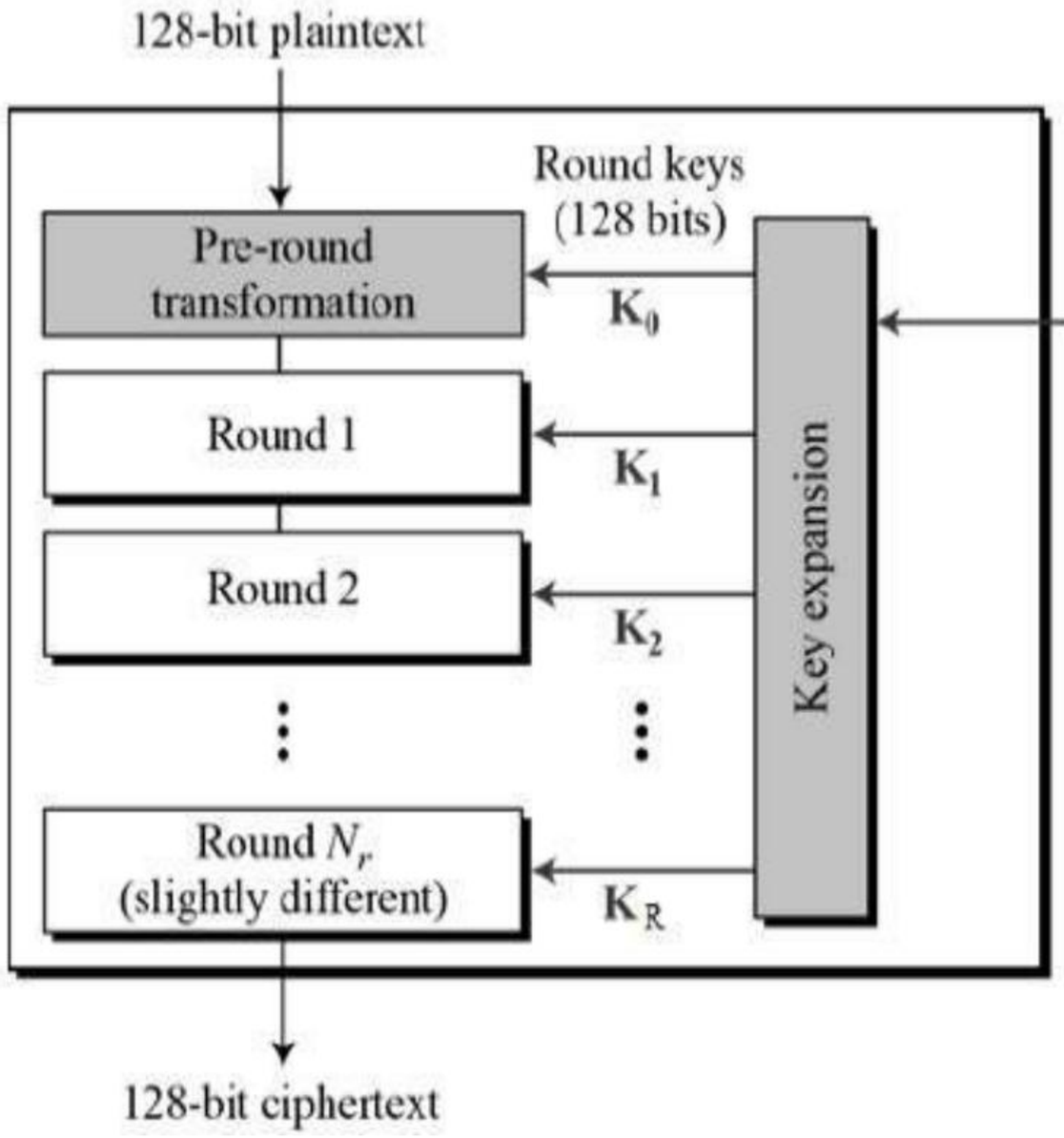
This publication is available free of charge from:
https://doi.org/10.6028/NIST.FIPS.197-upd1

Published November 26, 2001; Updated May 9, 2023


AES Algorithm Working
Secret Key
Secret Key
Secure Channel
Plaintext
Ciphertext
Plaintext
Sender
Encryption Server
Decryption Server
Receiver

- AES mã hóa dữ liệu theo khối có kích thước 128 bit (16 byte).
- Kích thước khóa có thể là 128 bit, 192 bit hoặc 256 bit. Kích thước khóa này xác định số vòng lặp (rounds) mà thuật toán thực hiện.
- Vòng Lặp (Rounds):
  - Với khóa 128 bit: 10 vòng lặp.
  - Với khóa 192 bit: 12 vòng lặp.
  - Với khóa 256 bit: 14 vòng lặp.

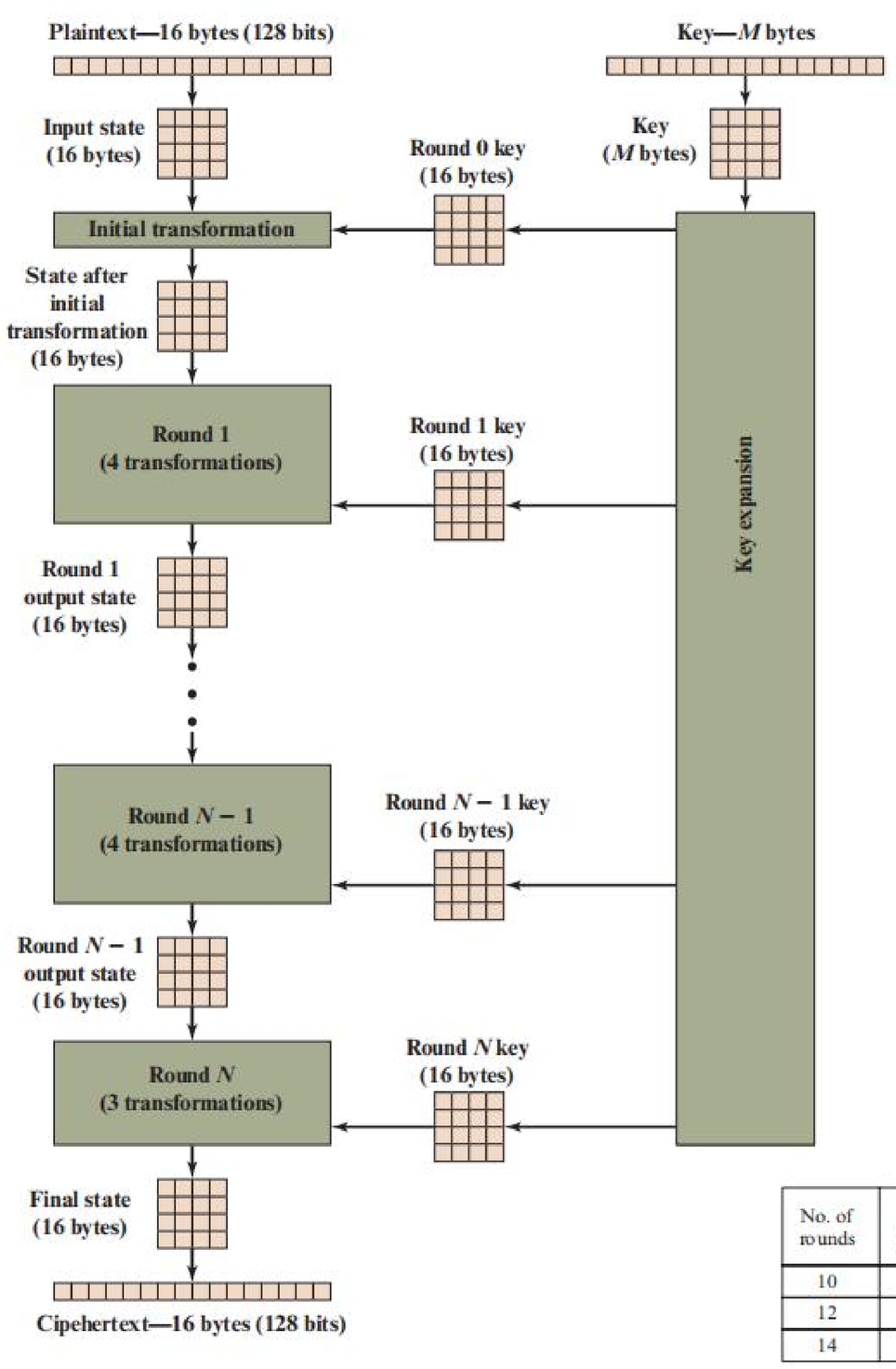
CẤU TRÚC AES



R	Key size
10	128
12	192
14	256

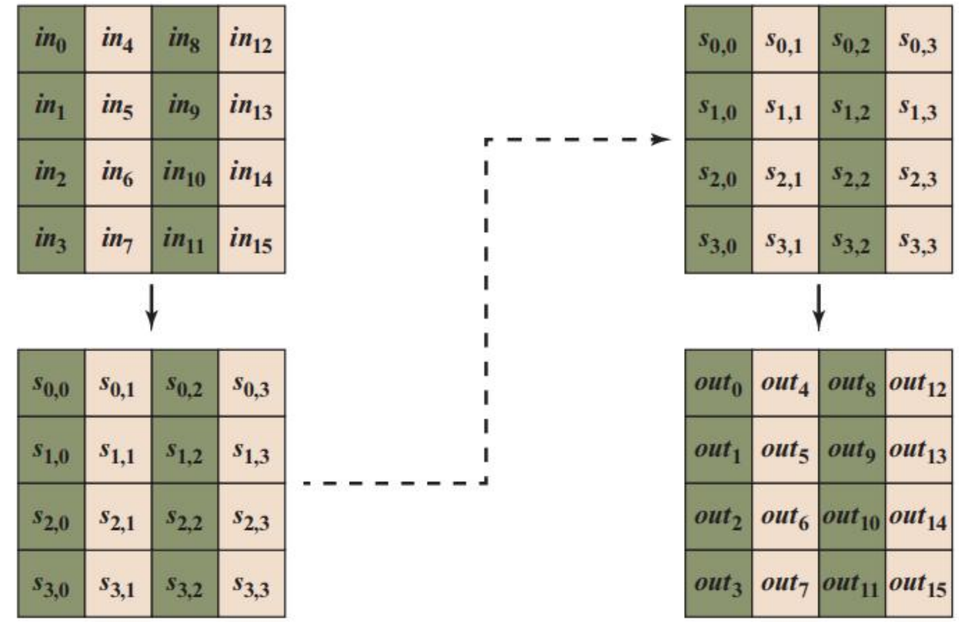
Relationship between number of rounds(R) and cipher key size

CẤU TRÚC AES

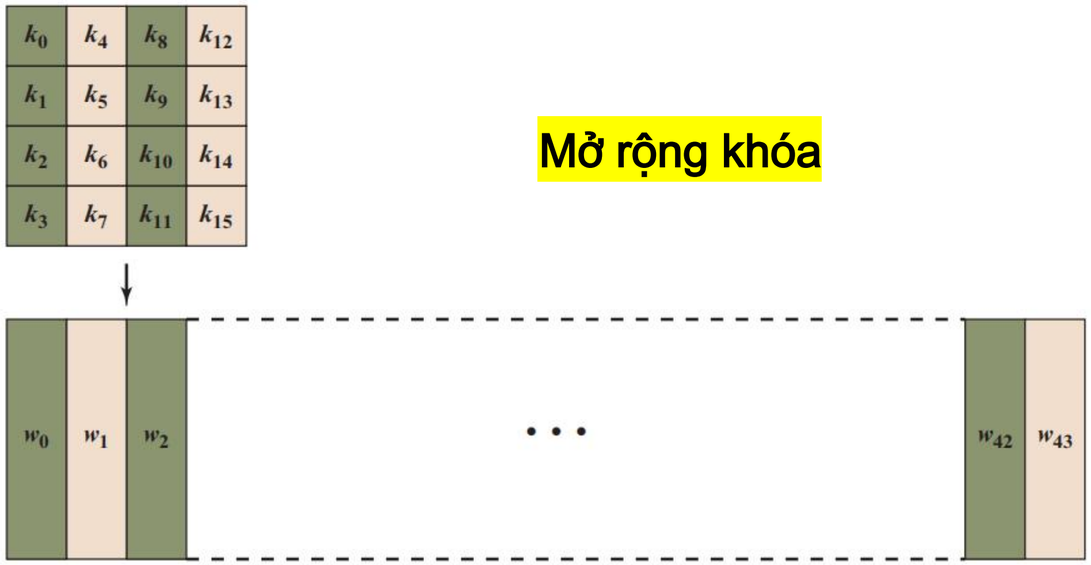


No. of rounds	Key Length (bytes)
10	16
12	24
14	32

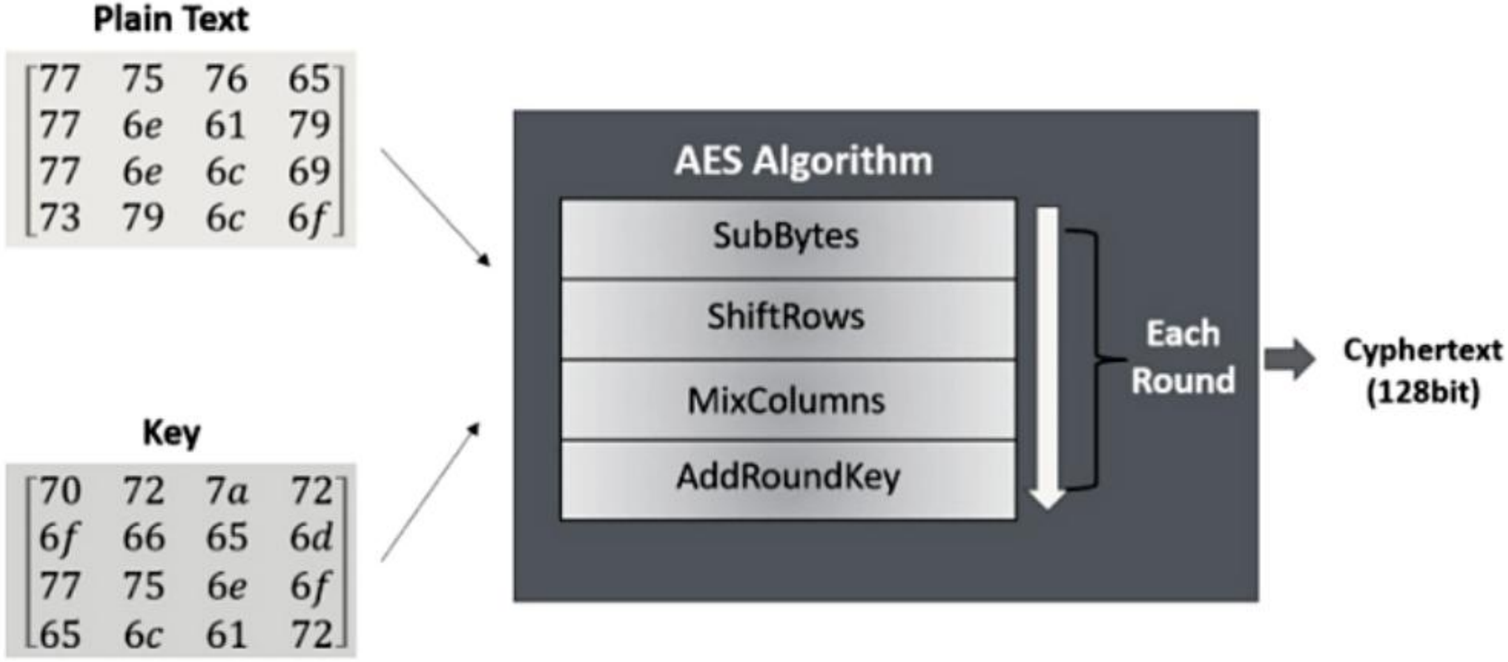
Ma trận trạng thái



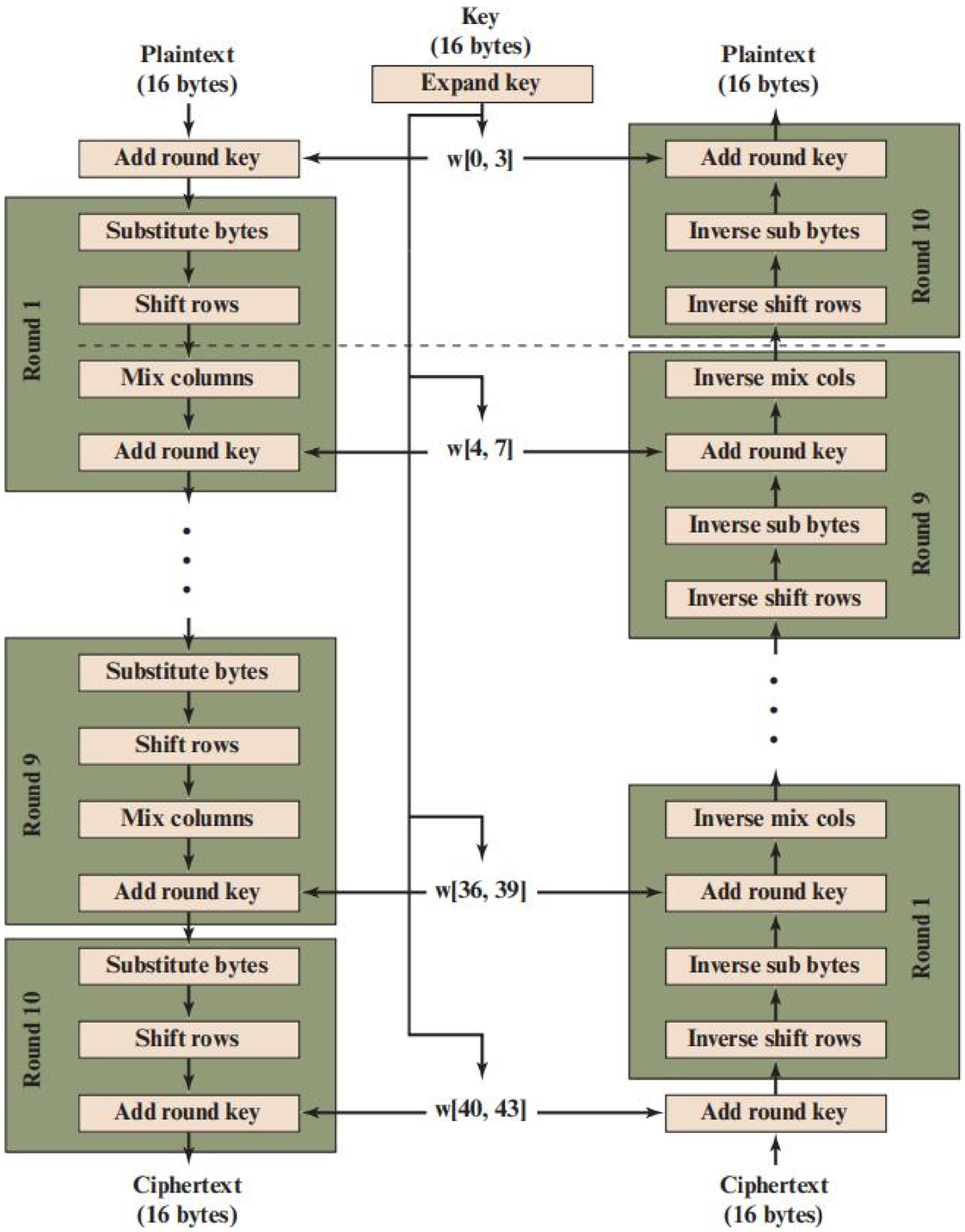
Mở rộng khóa

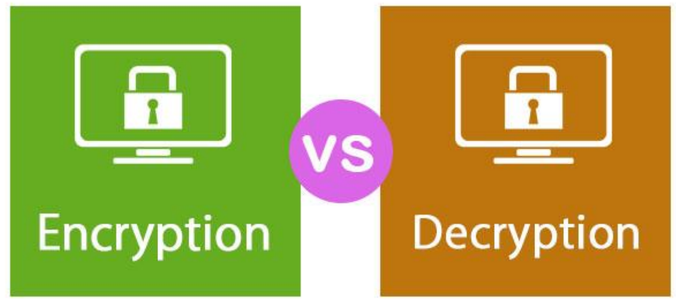


- Các phép toán trong thuật toán AES đều thực hiện trong một trường hữu hạn của các byte. Mỗi khối dữ liệu đầu vào 128 bits (16 bytes), có thể xếp thành 4 cột, mỗi cột 4 phần tử hay một ma trận 4x4 của các bytes, nó gọi là ma trận trạng thái.



THUẬT TOÁN AES





6.2 AES STRUCTURE

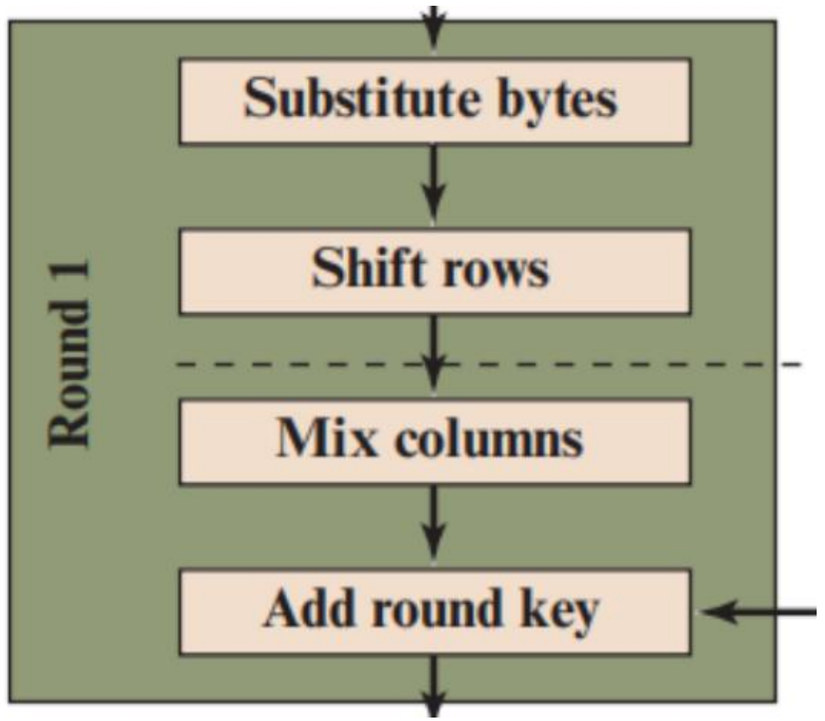
General Structure

Figure 6.1 shows the overall structure of the AES encryption process. The cipher takes a plaintext block size of 128 bits, or 16 bytes. The key length can be 16, 24, or 32 bytes (128, 192, or 256 bits). The algorithm is referred to as AES-128, AES-192, or AES-256, depending on the key length.

The input to the encryption and decryption algorithms is a single 128-bit block. In FIPS PUB 197, this block is depicted as a 4×4 square matrix of bytes. This block is copied into the **State** array, which is modified at each stage of encryption or decryption. After the final stage, **State** is copied to an output matrix. These operations are depicted in Figure 6.2a. Similarly, the key is depicted as a square matrix of bytes. This key is then expanded into an array of key schedule words. Figure 6.2b shows the expansion for the 128-bit key. Each word is four bytes, and the total key schedule is 44 words for the 128-bit key. Note that the ordering of bytes within a matrix is by column. So, for example, the first four bytes of a 128-bit plaintext input to the encryption cipher occupy the first column of the **in** matrix, the second four bytes occupy the second column, and so on. Similarly, the first four bytes of the expanded key, which form a word, occupy the first column of the **w** matrix.

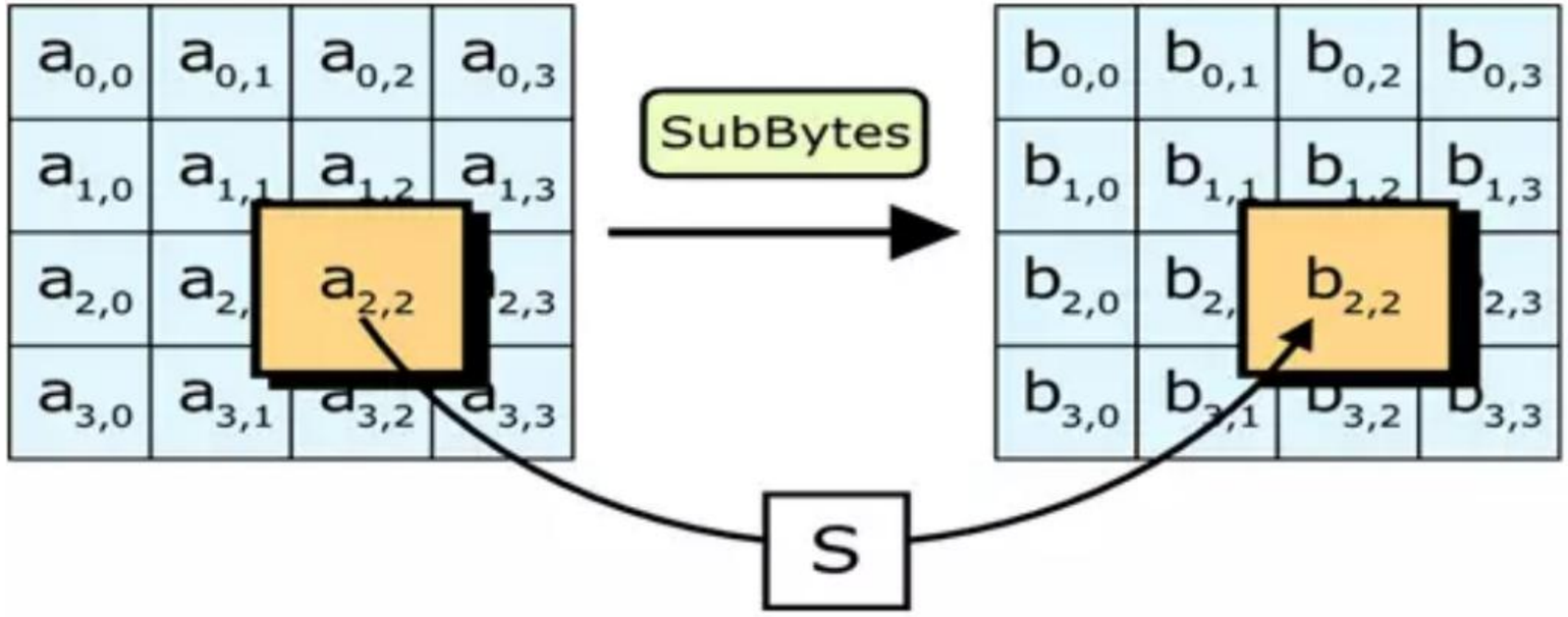
4 giai đoạn thực hiện:

- Substitute bytes
- Shift Rows
- Mix Columns
- AddRoundKey



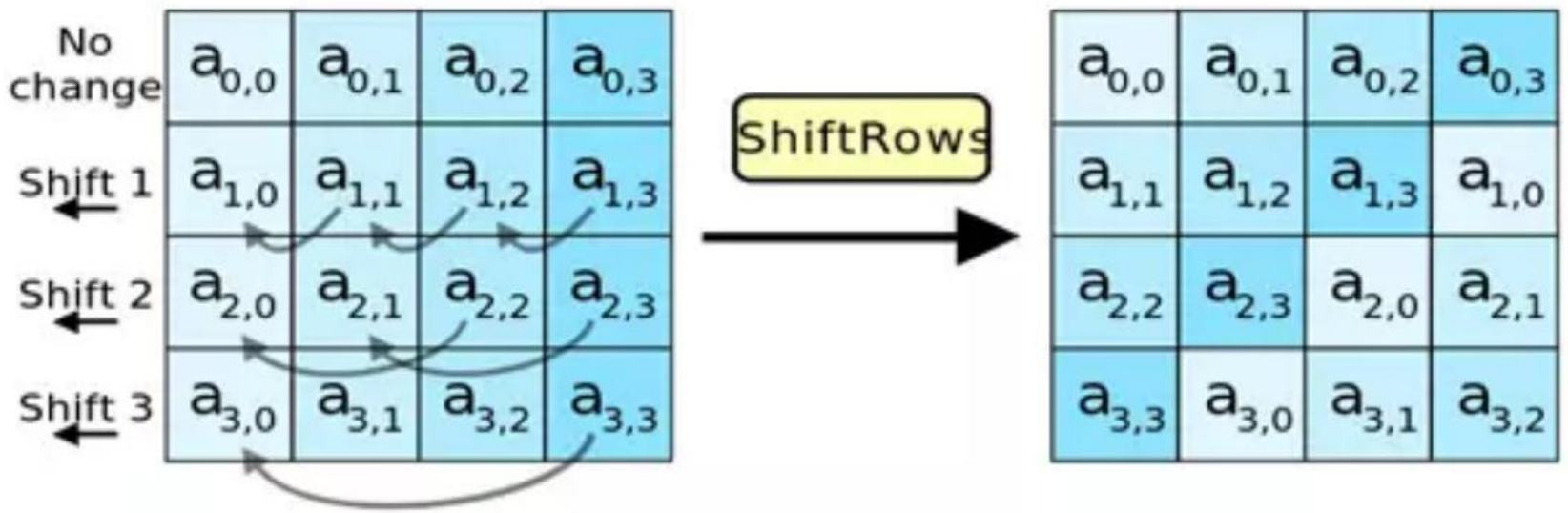
Substitute bytes:

- Biến đổi SubBytes() thay thế mỗi byte riêng rẽ của state $S_{r,c}$ bằng một giá trị mới $S'_{r,c}$ sử dụng bảng thay thế (S - box) được xây dựng ở trên.



Shift Rows:

- $S'_{r,c} = S_{r,(c + shift(r, Nb)) \bmod Nb}$ $(Nb = 4)$



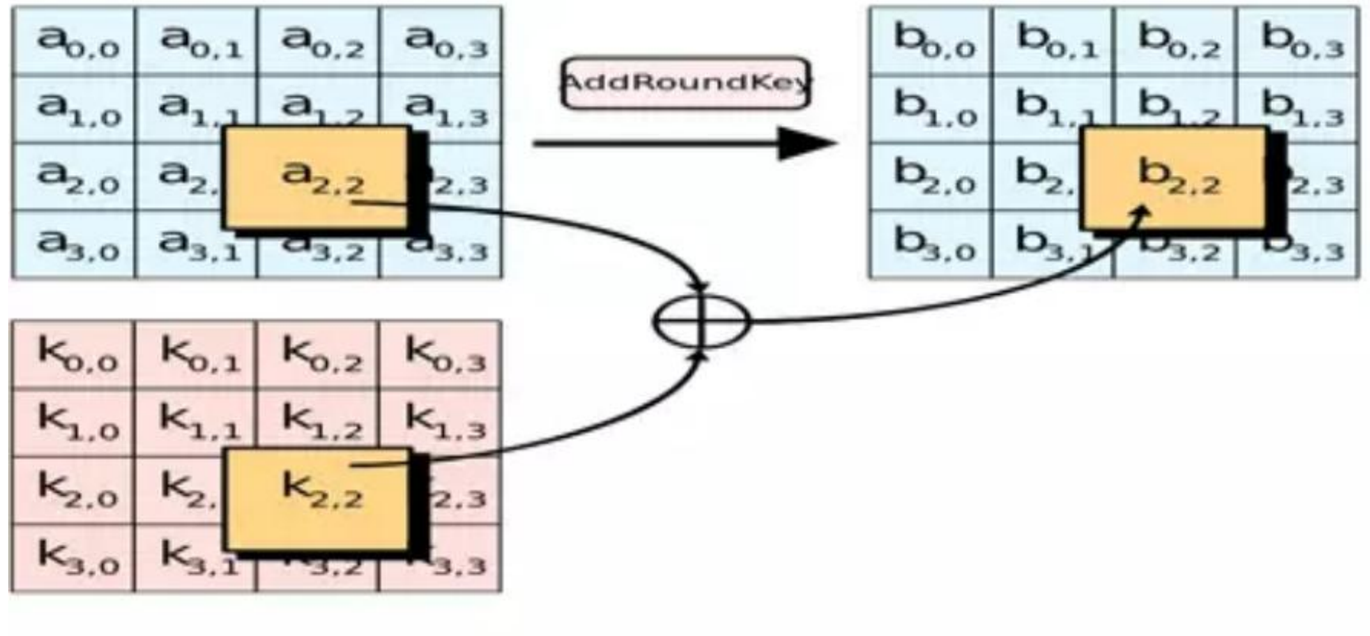
Mix Columns:

- Biến đổi MixColumns() tính toán trên từng cột của state. Các cột được coi như là đa thức trong trường GF(28) và nhân với một đa thức *a(x)*.

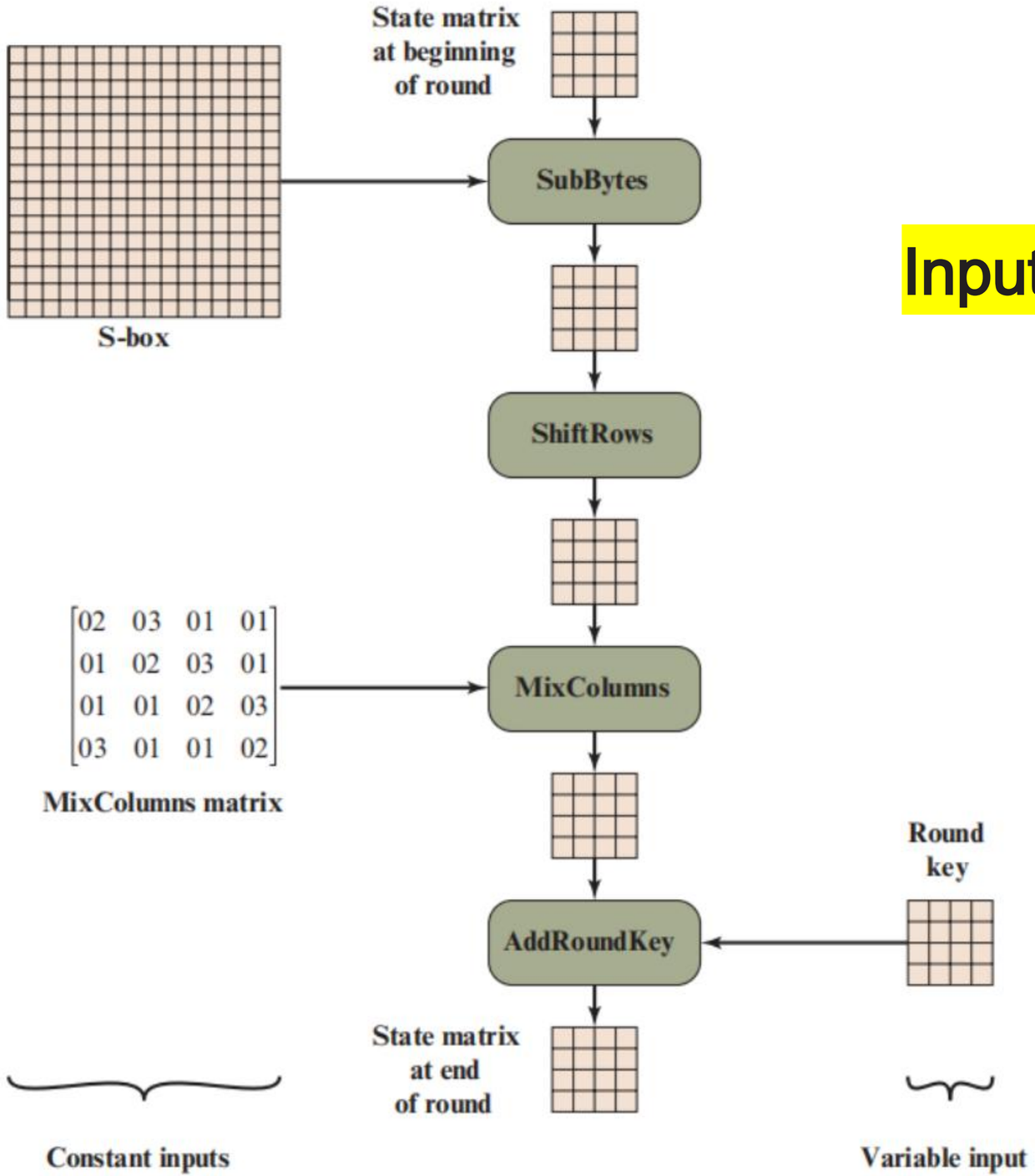
$$\begin{bmatrix} S'_{0,c} \\ S'_{1,c} \\ S'_{2,c} \\ S'_{3,c} \end{bmatrix} = \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \begin{bmatrix} S_{0,c} \\ S_{1,c} \\ S_{2,c} \\ S_{3,c} \end{bmatrix}$$

AddRoundKeys:

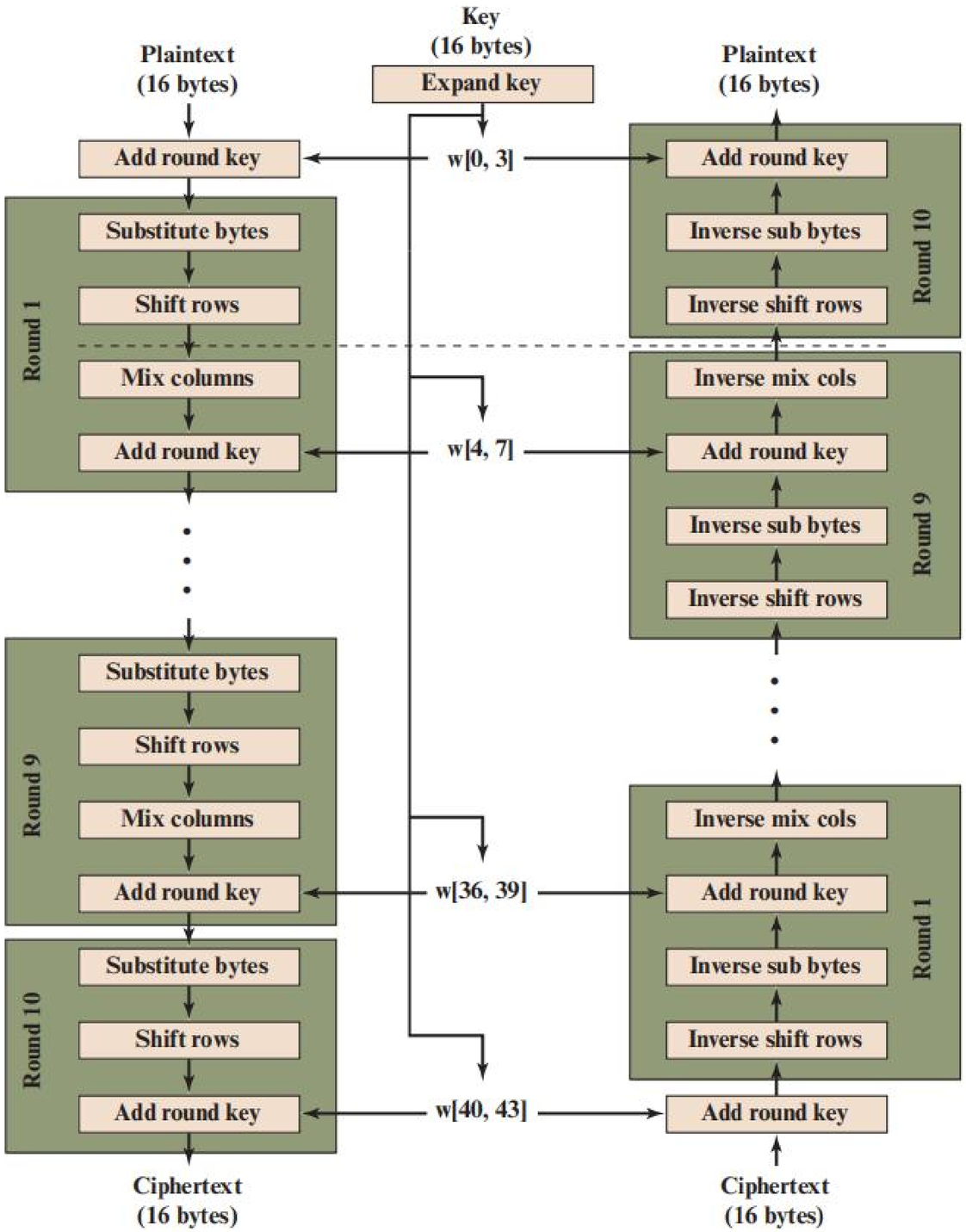
- Được áp dụng từ vòng lặp thứ 1 tới vòng lặp N_r. Trong biến đổi Addroundkey(), một khóa vòng được cộng với state bằng một phép XOR.



Inputs for Single AES Round



THUẬT TOÁN AES



Xem lại sơ đồ thuật toán

Mở rộng khóa - AES Expand key:

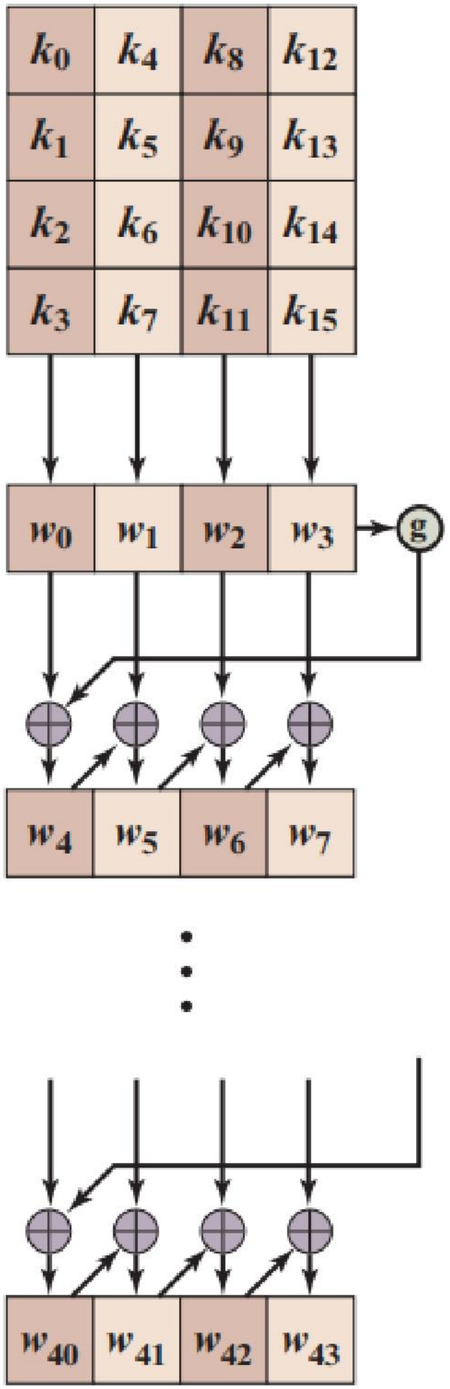
- AES Key Expansion là quá trình tạo ra các khóa vòng từ khóa chính ban đầu. Nó đảm bảo rằng mỗi vòng lặp trong quá trình mã hóa và giải mã có một khóa riêng biệt, giúp tăng cường độ bảo mật và làm cho thuật toán AES trở nên mạnh hơn.

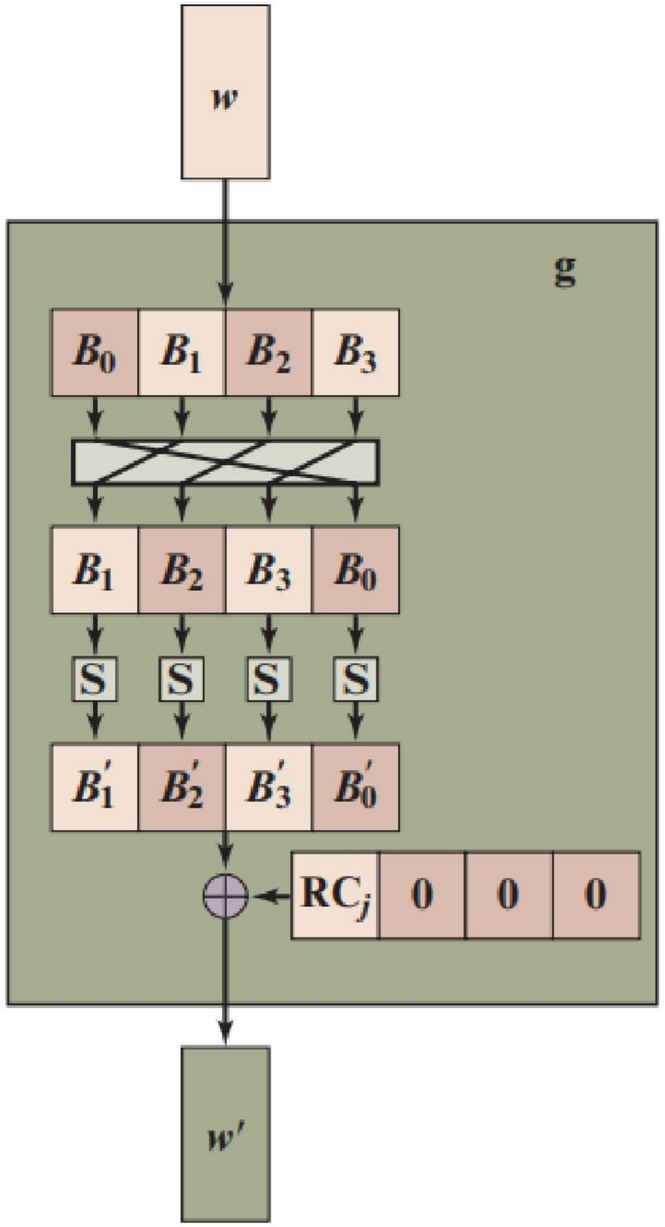
6.4 AES KEY EXPANSION

Key Expansion Algorithm

The AES **key expansion** algorithm takes as input a four-word (16-byte) key and produces a linear array of 44 words (176 bytes). This is sufficient to provide a four-word round key for the initial AddRoundKey stage and each of the 10 rounds of the cipher. The pseudocode on the next page describes the expansion.

The key is copied into the first four words of the expanded key. The remainder of the expanded key is filled in four words at a time. Each added word **w**[i] depends on the immediately preceding word, **w**[i − 1], and the word four positions back, **w**[i − 4]. In three out of four cases, a simple XOR is used. For a word whose position in the **w** array is a multiple of 4, a more complex function is used. Figure 6.9 illustrates the generation of the expanded key, using the symbol g to represent that complex function. The function g consists of the following subfunctions.





Sơ đồ thuật toán mở rộng khóa

Key Size (bits)	Cipher	Number of Alternative Keys	Time Required at 10^9 Decryptions/s	Time Required at 10^{13} Decryptions/s
56	DES	$2^{56} \approx 7.2 \times 10^{16}$	2^{55} ns = 1.125 years	1 hour
128	AES	$2^{128} \approx 3.4 \times 10^{38}$	2^{127} ns = 5.3×10^{21} years	5.3×10^{17} years
168	Triple DES	$2^{168} \approx 3.7 \times 10^{50}$	2^{167} ns = 5.8×10^{33} years	5.8×10^{29} years
192	AES	$2^{192} \approx 6.3 \times 10^{57}$	2^{191} ns = 9.8×10^{40} years	9.8×10^{36} years
256	AES	$2^{256} \approx 1.2 \times 10^{77}$	2^{255} ns = 1.8×10^{60} years	1.8×10^{56} years
26 characters (permutation)	Monoalphabetic	$2! = 4 \times 10^{26}$	2×10^{26} ns = 6.3×10^{9} years	6.3×10^{6} years

SUMMARY

- Hoạt động của thuật toán AES
- Cơ chế sinh khóa

LAB LUYỆN TẬP

https://www.javatpoint.com/aes-algorithm-in-cpp

https://github.com/SergeyBel/AES

HOMEWORK

- Xây dựng chương trình thực hiện thuật toán AES với ứng dụng nhắn tin
- Xây dựng chương trình thực hiện thuật toán AES với file dữ liệu

ĐẠI NAM
UNIVERSITY