Advanced Encryption Standard (AES)

AES

- The Advanced Encryption Standard (AES) is a symmetric block cipher adopted by the U.S. government
- is currently the most widely used encryption algorithm worldwide
- it replaced the Data Encryption Standard (DES) due to DES's insufficient key length.

Key Features and Background

Feature	Description
Type	Symmetric Block Cipher
Block Size	Fixed at 128 bits (16 bytes)
Key Lengths	Variable: 128, 192, or 256 bits
Rounds	Variable, depending on key length: 10 (for 128-bit key), 12 (for 192-bit key), or 14 (for 256-bit key)
Structure	Not a Feistel cipher (unlike DES); it's based on a Substitution-Permutation Network (SPN).
Origin	Developed by two Belgian cryptographers, Joan Daemen and Vincent Rijmen, as the Rijndaelalgorithm.

AES Structure and State

- AES operates on a single 128-bit block of data, which is represented as a 4×4 array of bytes (since 128 bits=16 bytes). This 4×4 array is called the State.

$$\text{State} = \begin{pmatrix} s_{0,0} & s_{0,1} & s_{0,2} & s_{0,3} \\ s_{1,0} & s_{1,1} & s_{1,2} & s_{1,3} \\ s_{2,0} & s_{2,1} & s_{2,2} & s_{2,3} \\ s_{3,0} & s_{3,1} & s_{3,2} & s_{3,3} \end{pmatrix}$$

- The encryption process consists of an Initial Round, N–1 Main Rounds, and a Final Round, where N is the total number of rounds.

The Four Main Round Transformations

- Each main round (except the final one) involves four distinct, invertible transformations applied sequentially to the 16 bytes of the State:
- SubBytes (Substitution)
- ShiftRows (Permutation)
- MixColumns (Diffusion)
- AddRoundKey (Key Mixing)

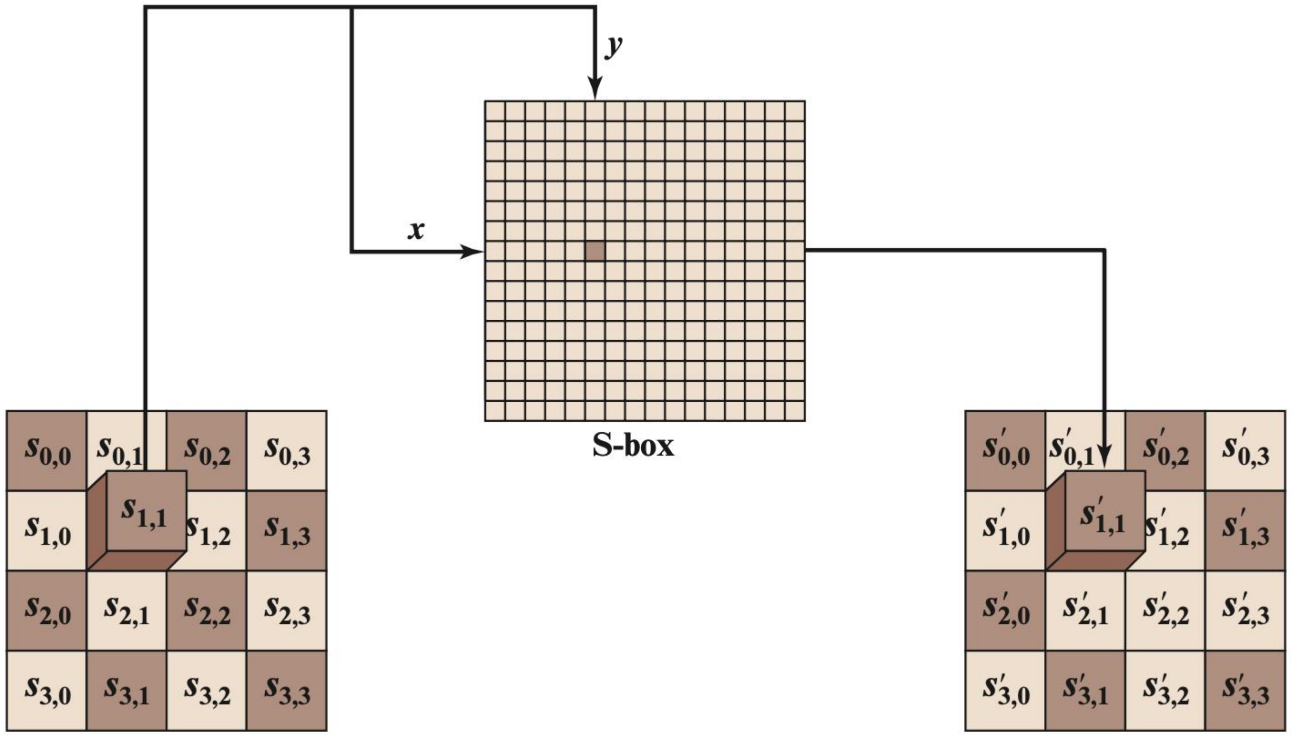
SubBytes (Substitution)

- What it does: It performs a non-linear byte substitution on each byte of the State independently.

- Mechanism: Each byte is replaced by another byte using a single fixed look-up table called the S-box.

- Purpose: Provides confusion (makes the relationship between the key and the ciphertext complex).

Substitution byte transformation


y
x
S-box
$s_{0,0}$ $s_{0,1}$ $s_{0,2}$ $s_{0,3}$
$s_{1,0}$ $s_{1,1}$ $s_{1,2}$ $s_{1,3}$
$s_{2,0}$ $s_{2,1}$ $s_{2,2}$ $s_{2,3}$
$s_{3,0}$ $s_{3,1}$ $s_{3,2}$ $s_{3,3}$
$s'_{0,0}$ $s'_{0,1}$ $s'_{0,2}$ $s'_{0,3}$
$s'_{1,0}$ $s'_{1,1}$ $s'_{1,2}$ $s'_{1,3}$
$s'_{2,0}$ $s'_{2,1}$ $s'_{2,2}$ $s'_{2,3}$
$s'_{3,0}$ $s'_{3,1}$ $s'_{3,2}$ $s'_{3,3}$

(a) Substitute byte transformation

ShiftRows (Permutation)

- What it does: It cyclically shifts the bytes in the last three rows of the State.

- Mechanism: Row 0 is shifted by 0 bytes (no shift). Row 1 is shifted left by 1 byte. Row 2 is shifted left by 2 bytes. Row 3 is shifted left by 3 bytes.

- Purpose: Provides diffusion across the columns (spreads the influence of each byte across the entire block).

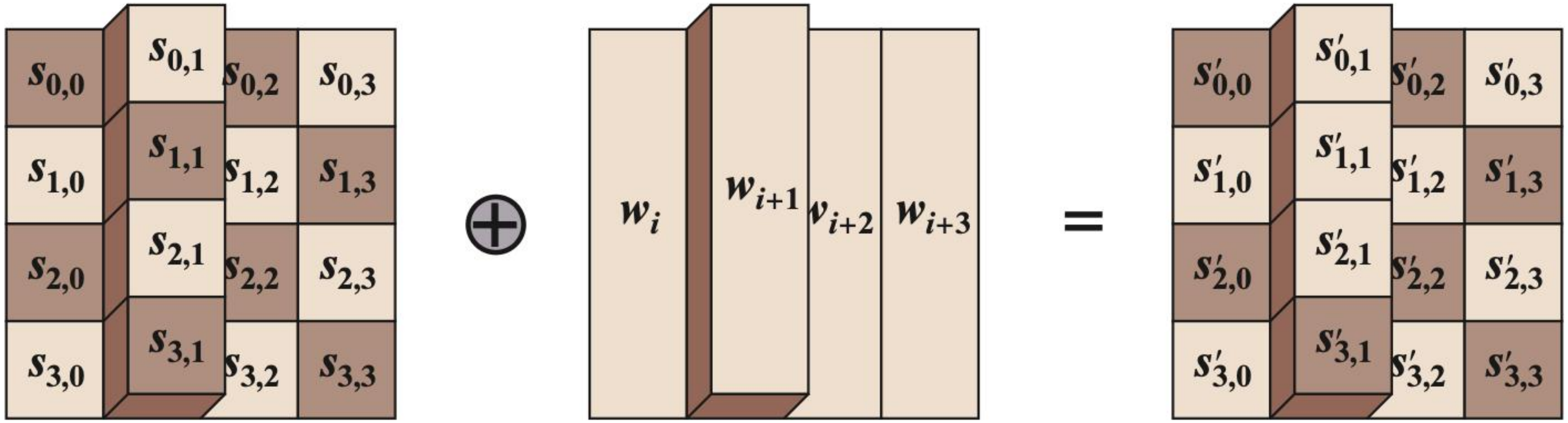
MixColumns (Diffusion)

- What it does: It operates on the four bytes of each column independently.
- Mechanism: Each column is transformed using a linear matrix multiplication over the finite field GF(2^8).
- Purpose: Provides robust diffusion by mixing the bytes within each column. This step is omitted in the Final Round.

AddRoundKey (Key Mixing)

- What it does: The 128-bit round key is combined with the State.
- Mechanism: The 128-bit Round Key is XORed ($\oplus$) with the 128-bit State.
- Purpose: Incorporates the key material into the encryption process. This is the only step that uses the secret key bits.

Add round key transformation


$s_{0,0}$ $s_{0,1}$ $s_{0,2}$ $s_{0,3}$
$s_{1,0}$ $s_{1,1}$ $s_{1,2}$ $s_{1,3}$
$s_{2,0}$ $s_{2,1}$ $s_{2,2}$ $s_{2,3}$
$s_{3,0}$ $s_{3,1}$ $s_{3,2}$ $s_{3,3}$
$\oplus$
w_i w_{i+1} w_{i+2} w_{i+3}
=
$s'_{0,0}$ $s'_{0,1}$ $s'_{0,2}$ $s'_{0,3}$
$s'_{1,0}$ $s'_{1,1}$ $s'_{1,2}$ $s'_{1,3}$
$s'_{2,0}$ $s'_{2,1}$ $s'_{2,2}$ $s'_{2,3}$
$s'_{3,0}$ $s'_{3,1}$ $s'_{3,2}$ $s'_{3,3}$

AES Key Expansion (Key Schedule)

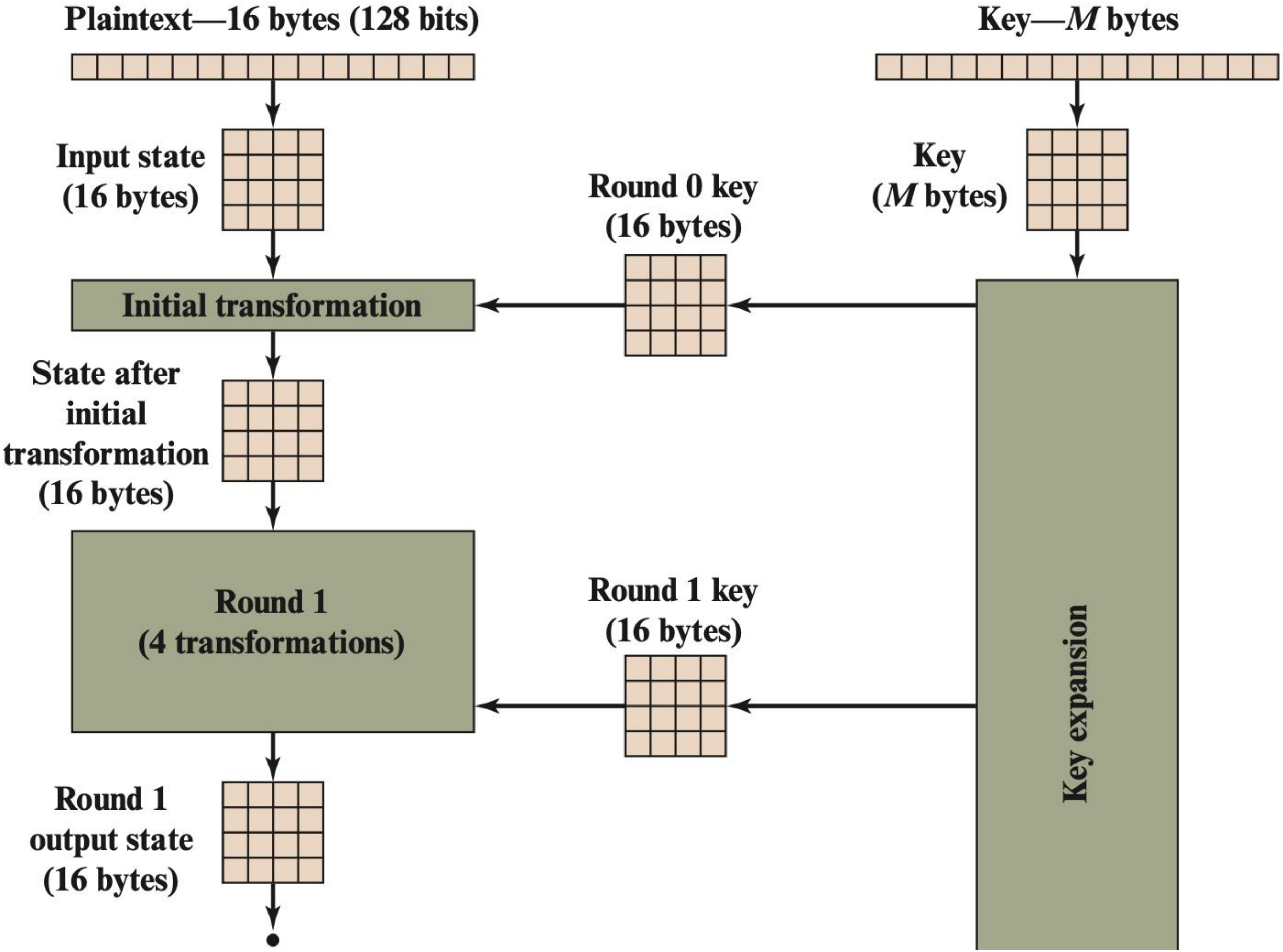
- The Key Schedule is the algorithm that takes the initial secret key (128, 192, or 256 bits) and generates the required number of Round Keys (each 128 bits) for the N rounds of encryption.

Key Length	Rounds (N)	Round Keys Needed
128-bit	10	11 (Initial Round Key + K_1 to K_{10})
192-bit	12	13
256-bit	14	15

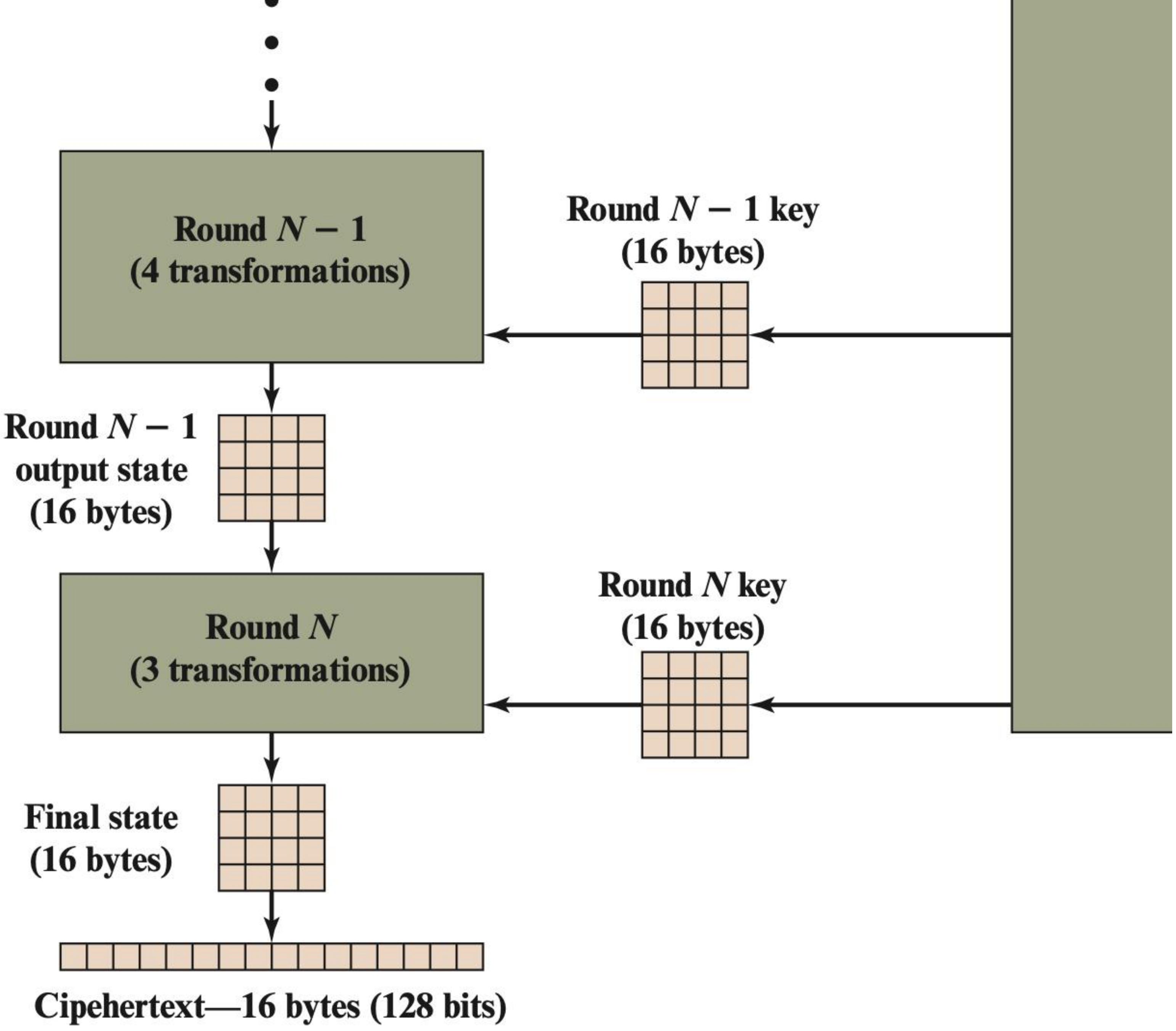
Encryption Flow: AES encryption process for a 128-bit block

- Start: Input a 128-bit plaintext block and an initial key.
- Initial Round: AddRoundKey (using K_0)
- Main Rounds (Rounds 1 to N-1): (Repeated 9, 11, or 13 times)
  - SubBytes, ShiftRows, MixColumns, AddRoundKey
- Final Round (Round N): (Note: MixColumns is omitted here)
- Output: 128-bit ciphertext block.

AES Encryption Process


Plaintext—16 bytes (128 bits)
Key—*M* bytes
Input state (16 bytes)
Key (*M* bytes)
Round 0 key (16 bytes)
Initial transformation
State after initial transformation (16 bytes)
Round 1 (4 transformations)
Round 1 key (16 bytes)
Key expansion
Round 1 output state (16 bytes)

AES Encryption Process



AES vs DES

Feature	**AES (Advanced Encryption Standard)**	**DES (Data Encryption Standard)**
Current Status	Modern Standard (Secure)	Obsolete (Insecure)
Structure	Substitution-Permutation Network (SPN)	Feistel Cipher
Block Size	128 bits (Fixed)	64 bits (Fixed)
Key Length	128, 192, or 256 bits (Variable)	64 bits (56 effective bits)
Number of Rounds	10, 12, or 14 (Depends on key size)	16 (Fixed)
Speed	Generally faster in both hardware and software	Slower than AES