

SYMMETRIC CIPHERS

ADVANCED ENCRYPTION STANDARD

Contents

- 1) AES Origins
- 2) AES Structure
- 3) AES Key Expansion
- 4) An AES Example
- 5) AES Decryption

1. AES Origins

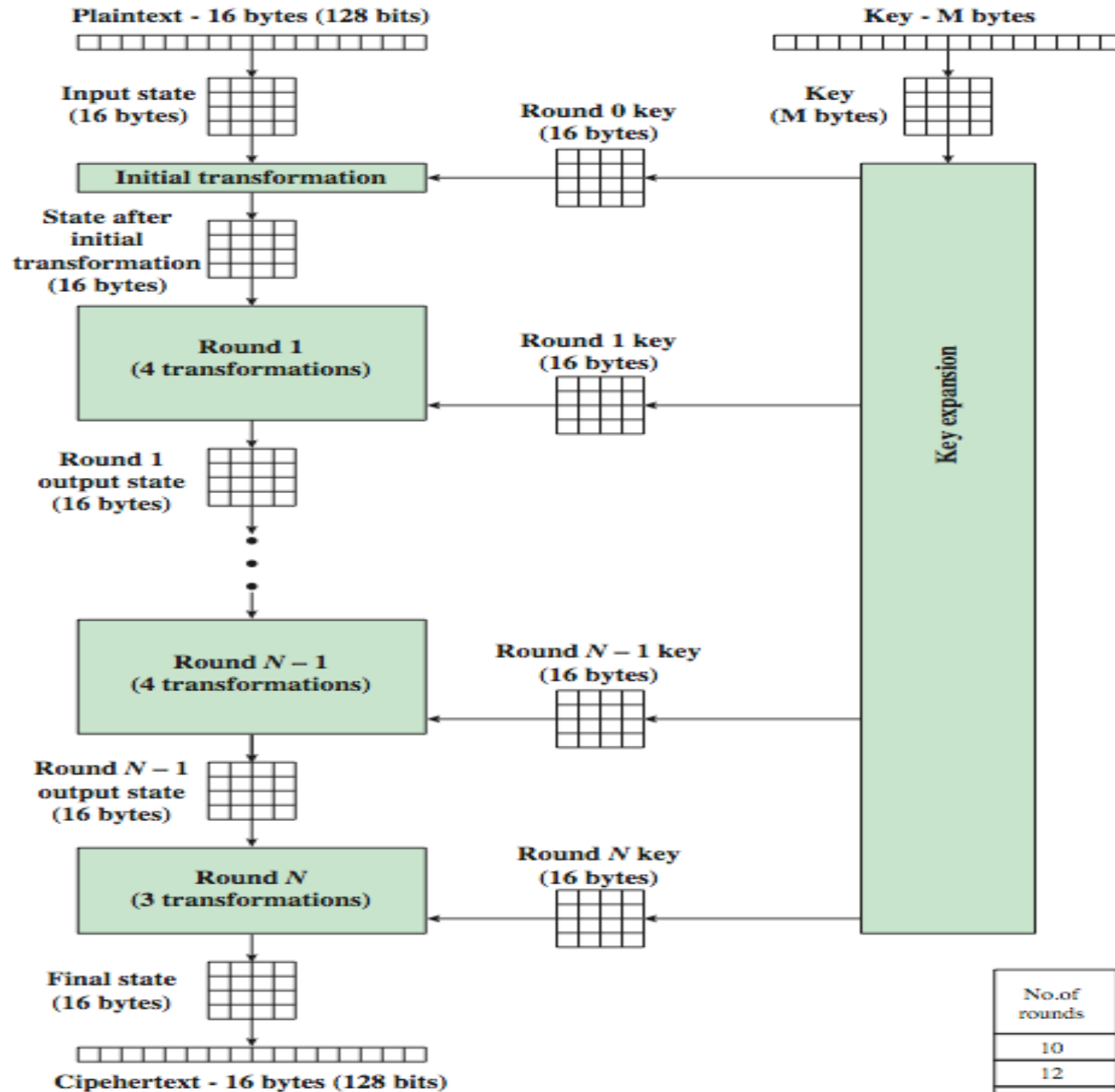
AES Origins

- Clear a replacement for DES was needed have theoretical attacks that can break it have demonstrated exhaustive key search attacks
- Can use Triple-DES – but slow, has small blocks

The AES Cipher - Rijndael

- Designed by Rijmen-Daemen in Belgium
- has 128/192/256 bit keys, 128 bit data
- Designed to have:
 - resistance against known attacks
 - speed and code compactness on many CPUs
 - design simplicity

AES E

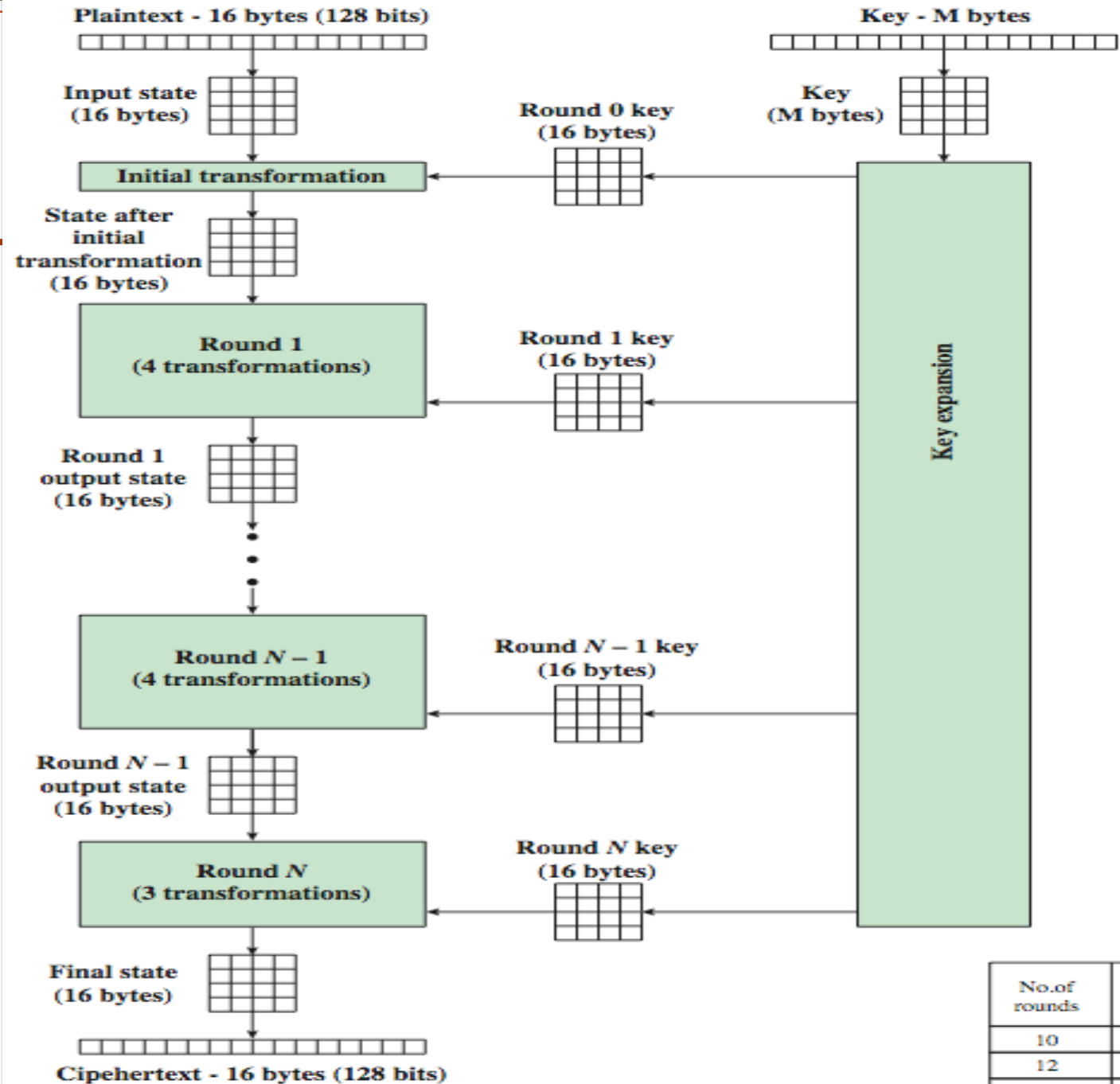


2. AES Structure

AES Structure

- Plaintext block size: 128 bits.
- Key length: 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

| Chiều dài khoá (bit) | 128 | 192 | 256 |
|-------------------------------|-----|-----|-----|
| Kích thước khối (bit) | 128 | 128 | 128 |
| Số vòng mã (vòng) | 10 | 12 | 14 |
| Chiều dài khoá phụ (bit) | 128 | 128 | 128 |
| Chiều dài khoá mở rộng (byte) | 176 | 208 | 240 |



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

Detailed Structure

- 128-bit block as consisting of a 4×4 matrix of bytes, arranged as follows:

$$\begin{bmatrix} \text{byte}_0 & \text{byte}_4 & \text{byte}_8 & \text{byte}_{12} \\ \text{byte}_1 & \text{byte}_5 & \text{byte}_9 & \text{byte}_{13} \\ \text{byte}_2 & \text{byte}_6 & \text{byte}_{10} & \text{byte}_{14} \\ \text{byte}_3 & \text{byte}_7 & \text{byte}_{11} & \text{byte}_{15} \end{bmatrix}$$

- The 4×4 matrix of bytes shown above is referred to as the **state array** in AES

Detailed Structure



(a) Input, state array, and output

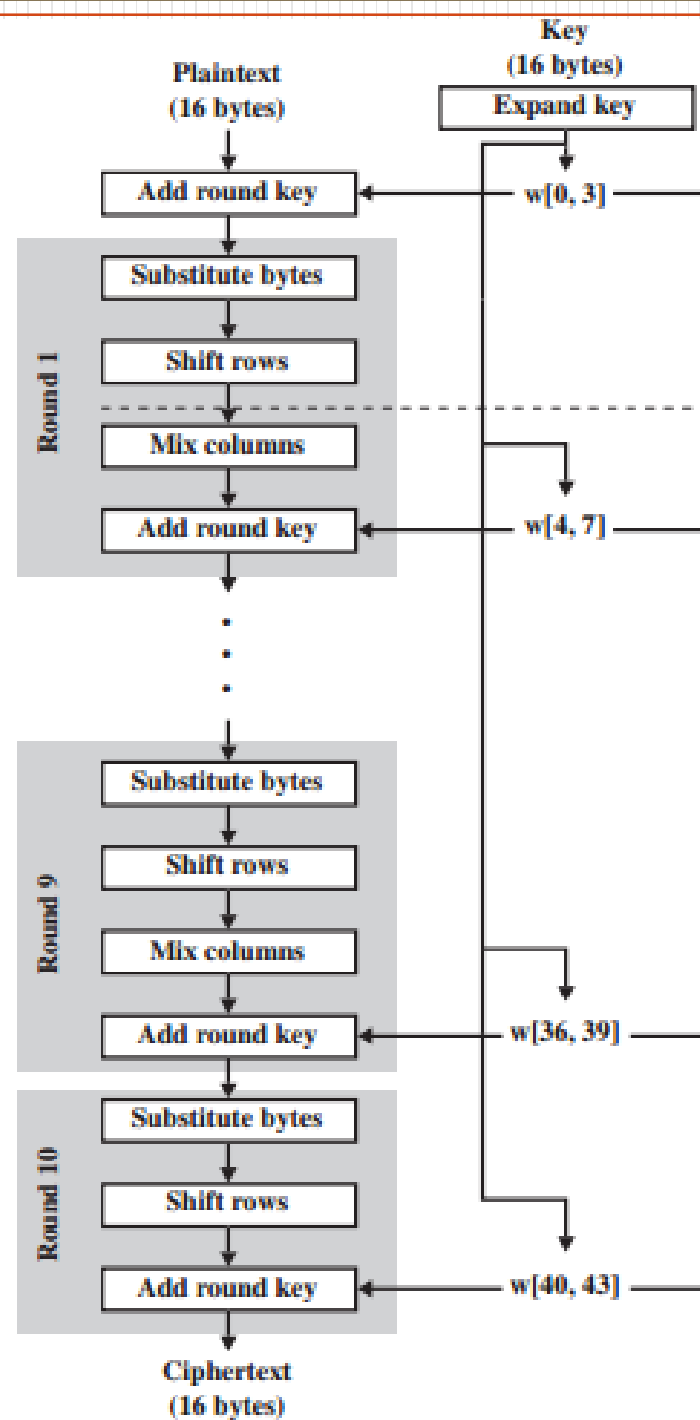
Detailed Structure

- The key is depicted as a square matrix of bytes
- This key is then expanded into an array of key schedule words
- Each **word** is **four bytes**, and the total key schedule is 44 words for the 128-bit key



(b) Key and expanded key

Detailed Stru



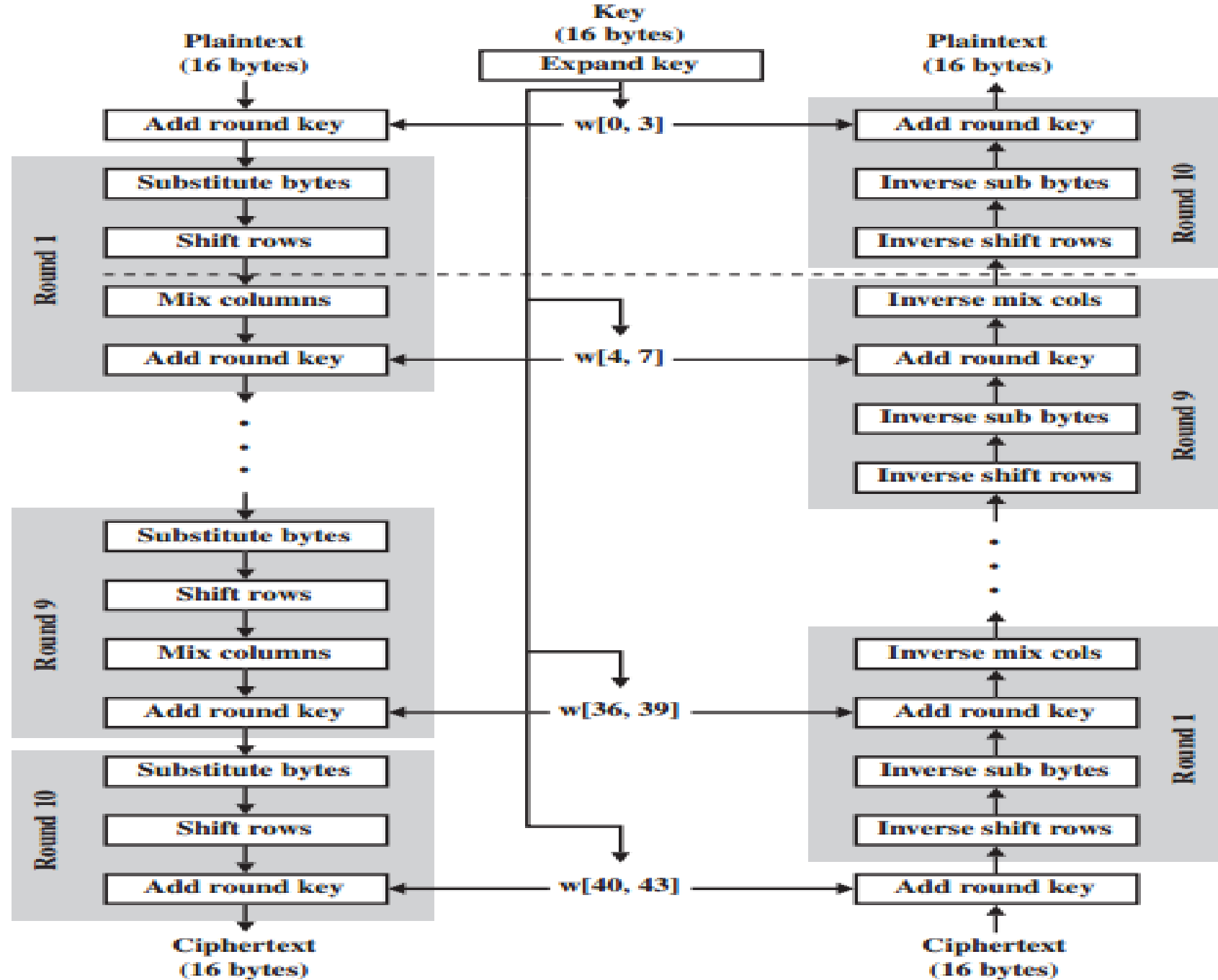
Detailed Structure

Four different stages are used, one of permutation and three of substitution:

- **Substitute bytes:** Uses an S-box to perform a byte-by-byte substitution of the block
- **Shift Rows:** A simple permutation
- **Mix Columns:** A substitution that makes use of arithmetic over
- **Add Round Key:** A simple bitwise XOR of the current block with a portion of the expanded key

Detailed Structure

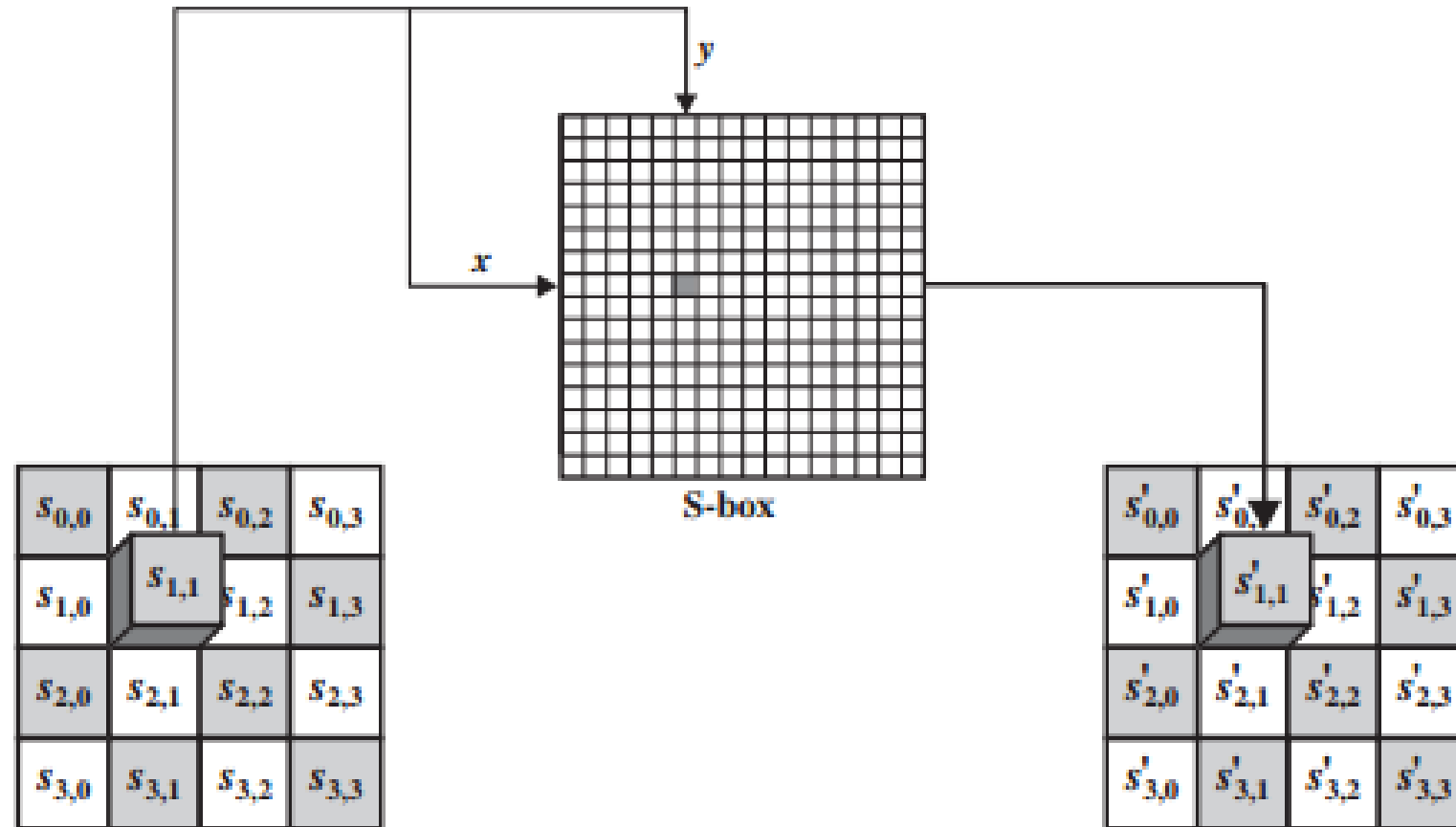
- For both encryption and decryption, the cipher begins with an Add Round Key stage, followed by nine rounds that each includes all four stages, followed by a tenth round of three stages.
- Only the Add Round Key stage makes use of the key



a. Substitute Bytes Transformation

- Each individual byte of State is mapped into a new byte in S-Box
- The leftmost 4 bits of the byte are used as a row value and the rightmost 4 bits are used as a column value.
- These row and column values serve as indexes into the S-box to select a unique 8-bit output value

Substitute Bytes Transformation (cont.)



| | | <i>y</i> | | | | | | | | | | | | | | | |
|----------|---|----------|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|
| | | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | A | B | C | D | E | F |
| <i>x</i> | 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 |

Substitute Bytes Transformation

- For example, the hexadecimal value {95} references row 9, column 5 of the S-box, which contains the value .Accordingly, the value is mapped into the value.
- Here is an example of the SubBytes transformation:

| | | | | | | | | |
|----|----|----|----|---|----|----|----|----|
| EA | 04 | 65 | 85 | → | 87 | F2 | 4D | 97 |
| 83 | 45 | 5D | 96 | | EC | 6E | 4C | 90 |
| 5C | 33 | 98 | B0 | | 4A | C3 | 46 | E7 |
| F0 | 2D | AD | C5 | | 8C | D8 | 95 | A6 |

b. ShiftRows Transformation

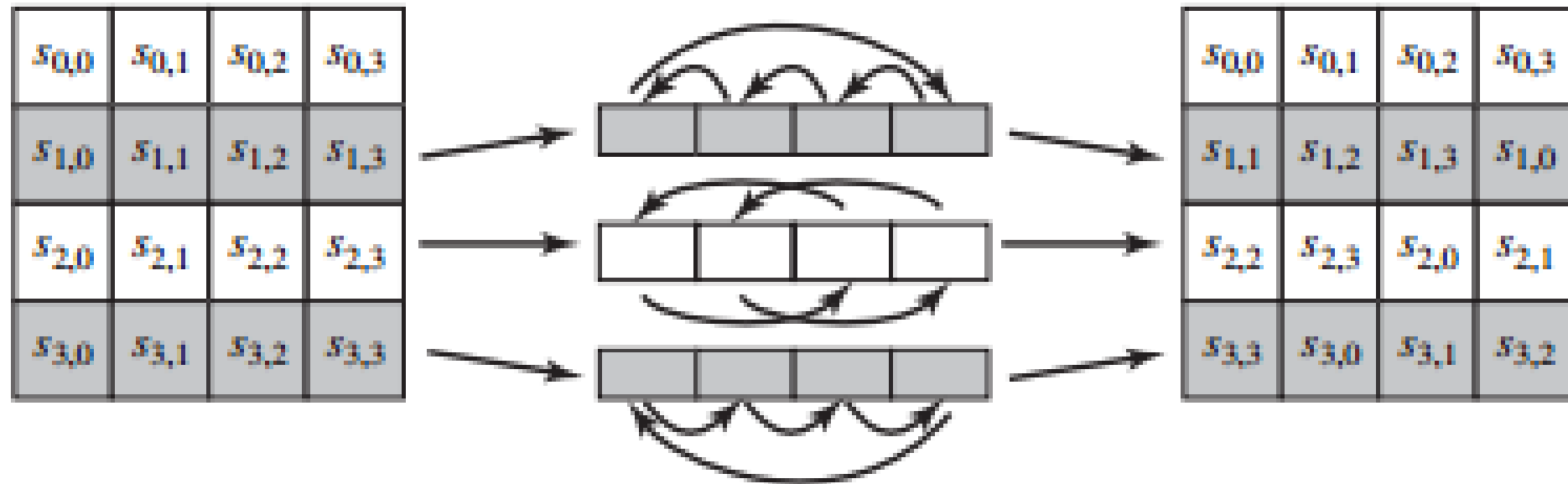
- The forward shift row transformation, called ShiftRows.
- The first row of State is not altered. For the second row, a 1-byte circular left shift is performed. For the third row, a 2-byte circular left shift is performed. For the fourth row, a 3-byte circular left shift is performed

| | | | |
|----|----|----|----|
| 87 | F2 | 4D | 97 |
| EC | 6E | 4C | 90 |
| 4A | C3 | 46 | E7 |
| 8C | D8 | 95 | A6 |

→

| | | | |
|----|----|----|----|
| 87 | F2 | 4D | 97 |
| 6E | 4C | 90 | EC |
| 46 | E7 | 4A | C3 |
| A6 | 8C | D8 | 95 |

ShiftRows Transformation



(a) Shift row transformation

c. MixColumns Transformation

- Each byte of a column is mapped into a new value that is a function of all four bytes in that column. The transformation can be defined by the following matrix multiplication on State

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

MixColumns Transformation

- the individual additions and multiplications are performed in $GF(2^8)$.

$$s'_{0,j} = (2 \cdot s_{0,j}) \oplus (3 \cdot s_{1,j}) \oplus s_{2,j} \oplus s_{3,j}$$

$$s'_{1,j} = s_{0,j} \oplus (2 \cdot s_{1,j}) \oplus (3 \cdot s_{2,j}) \oplus s_{3,j}$$

$$s'_{2,j} = s_{0,j} \oplus s_{1,j} \oplus (2 \cdot s_{2,j}) \oplus (3 \cdot s_{3,j})$$

$$s'_{3,j} = (3 \cdot s_{0,j}) \oplus s_{1,j} \oplus s_{2,j} \oplus (2 \cdot s_{3,j})$$

| | | | |
|----|----|----|----|
| 87 | F2 | 4D | 97 |
| 6E | 4C | 90 | EC |
| 46 | E7 | 4A | C3 |
| A6 | 8C | D8 | 95 |



| | | | |
|----|----|----|----|
| 47 | 40 | A3 | 4C |
| 37 | D4 | 70 | 9F |
| 94 | E4 | 3A | 42 |
| ED | A5 | A6 | BC |

d. Add Round Key Transformation

- XOR state with 128-bits of the round key

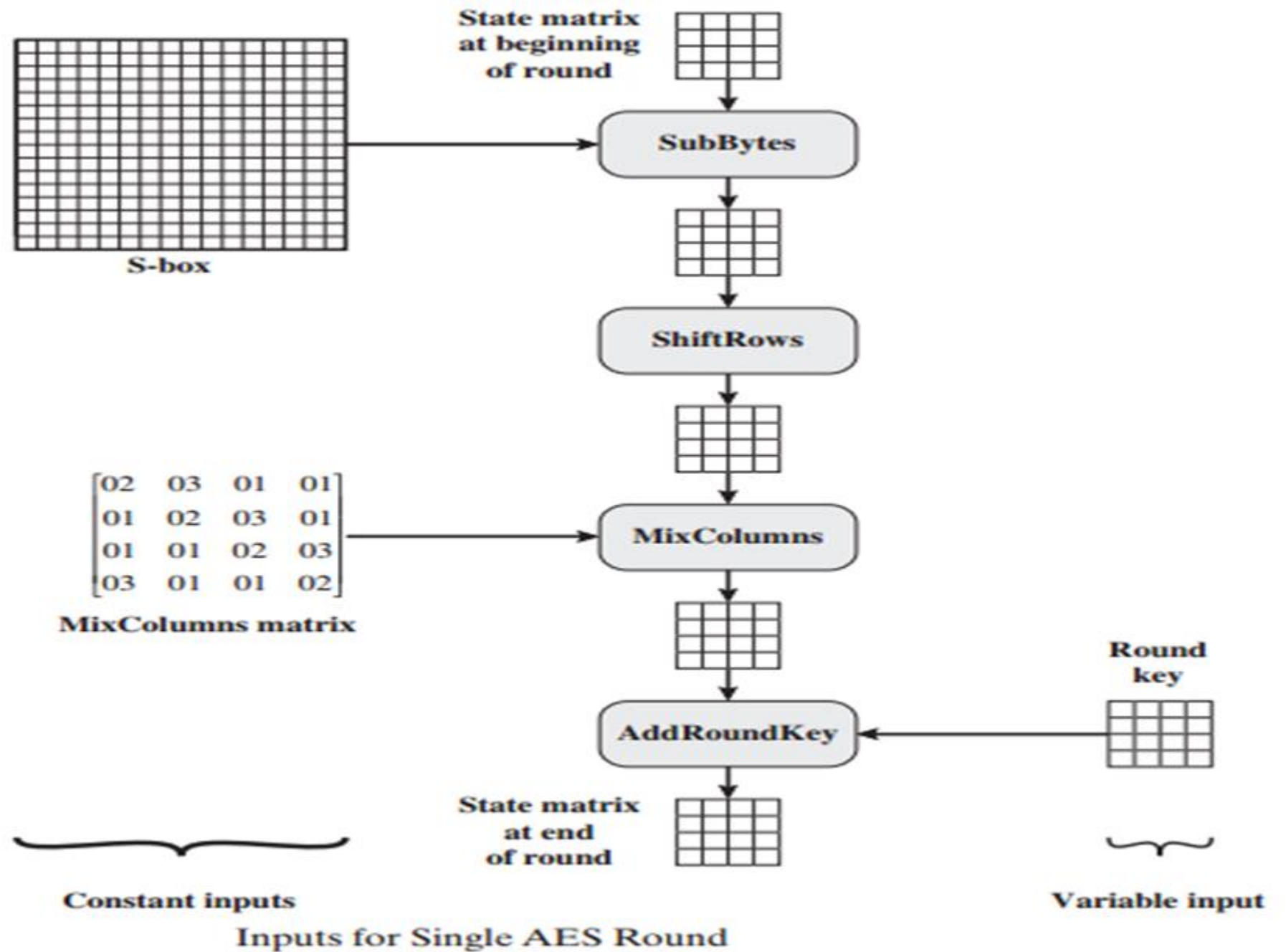
| | | | |
|----|----|----|----|
| 47 | 40 | A3 | 4C |
| 37 | D4 | 70 | 9F |
| 94 | E4 | 3A | 42 |
| ED | A5 | A6 | BC |

 \oplus

| | | | |
|----|----|----|----|
| AC | 19 | 28 | 57 |
| 77 | FA | D1 | 5C |
| 66 | DC | 29 | 00 |
| F3 | 21 | 41 | 6A |

 $=$

| | | | |
|----|----|----|----|
| EB | 59 | 8B | 1B |
| 40 | 2E | A1 | C3 |
| F2 | 38 | 13 | 42 |
| 1E | 84 | E7 | D6 |



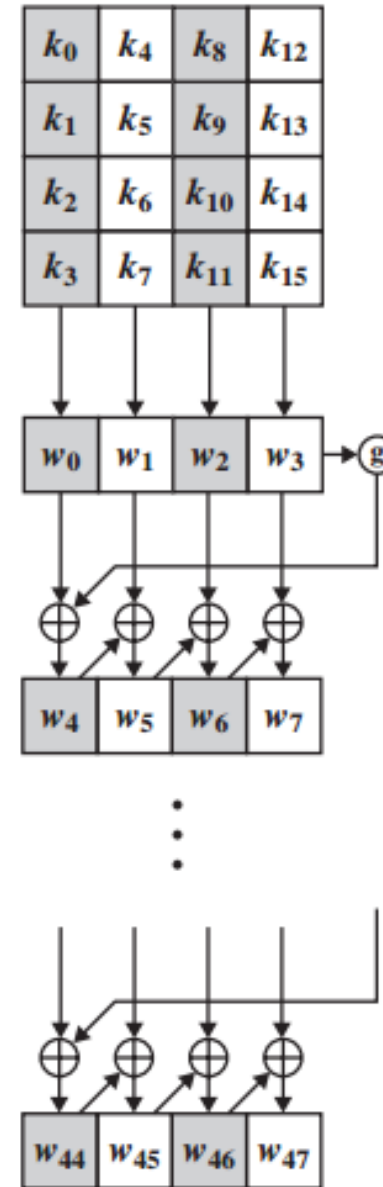
3. Aes Key Expansion

Key Expansion Algorithm

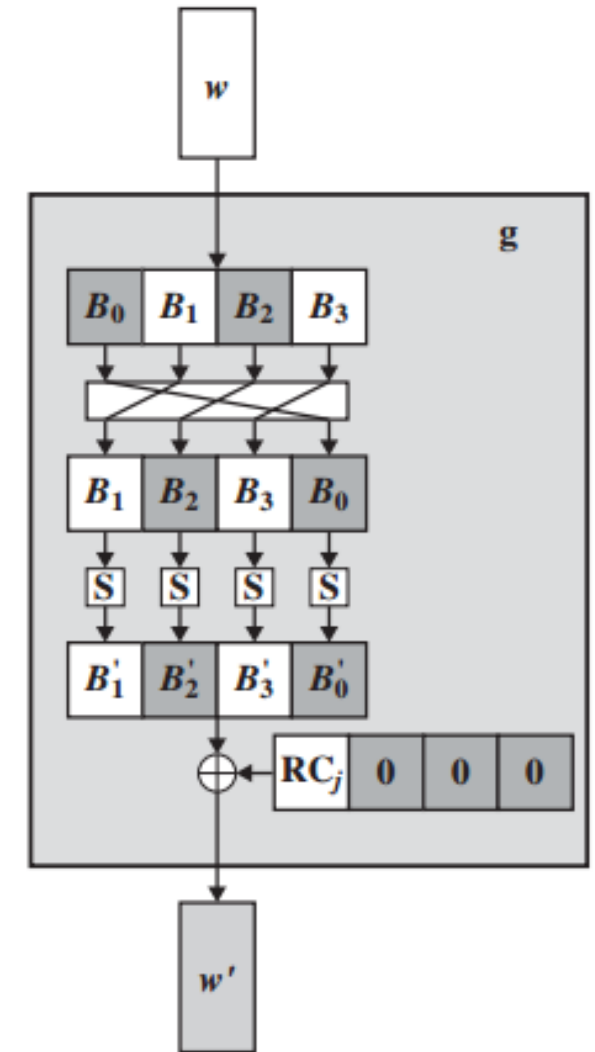
- Input a four-word (16-byte) key and produces a linear array of 44 words (176 bytes).
- This is sufficient to provide a four-word round key for the initial Add Round Key stage and each of the 10 rounds of the cipher.

Key Expansion Algo

- $w[i] = w[i-1] \oplus w[i-4]$.
- For a word whose position in the warray is a multiple of 4: a more complex function is used (g)



(a) Overall algorithm



(b) Function g

Key Expansion Algorithm

| | | | | | | | | | | |
|-------|----|----|----|----|----|----|----|----|----|----|
| j | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
| RC[j] | 01 | 02 | 04 | 08 | 10 | 20 | 40 | 80 | 1B | 36 |

- For example, suppose that the round key for round 8 is

EA D2 73 21 B5 8D BA D2 31 2B F5 60 7F 8D 29 2F

Then the first 4 bytes (first column) of the round key for round 9 are calculated as follows:

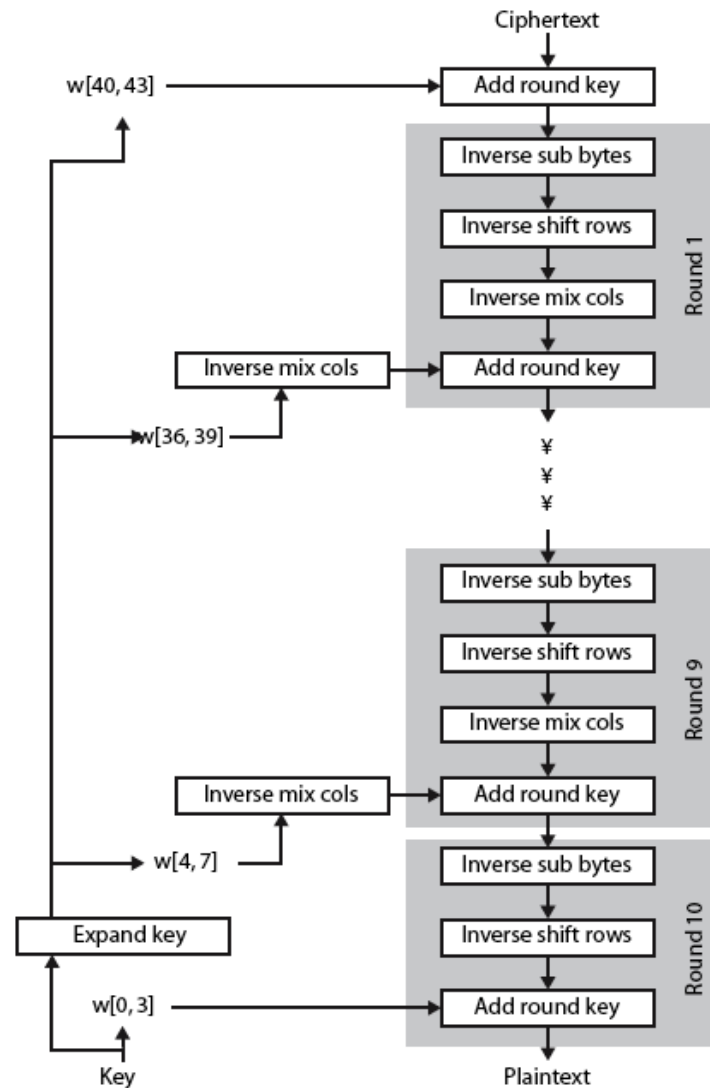
| i (decimal) | temp | After RotWord | After SubWord | Rcon (9) | After XOR with Rcon | w[i-4] | w[i] = temp \oplus w[i-4] |
|-------------|----------|---------------|---------------|----------|---------------------|----------|-----------------------------|
| 36 | 7F8D292F | 8D292F7F | 5DA515D2 | 1B000000 | 46A515D2 | EAD27321 | AC7766F3 |

4. AN AES EXAMPLE

-
- For this example, the plaintext is a hexadecimal palindrome. The plaintext, key, and resulting ciphertext are

| | |
|-------------|-----------------------------------|
| Plaintext: | 0123456789abcdef fedcba9876543210 |
| Key: | 0f1571c947d9e8590cb7add6af7f6798 |
| Ciphertext: | ff0b844a0853bf7c6934ab4364148fb9 |

AES Decryption



Inverse Substitute Bytes

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

(b) Inverse S-box

Inverse Shift Row Transformation

- The inverse shift row transformation, called InvShiftRows, performs the circular shifts in the opposite direction for each of the last three rows, with a 1-byte circular right shift for the second row, and so on

Inverse Mix Column Transformation

$$\begin{bmatrix} 0E & 0B & 0D & 09 \\ 09 & 0E & 0B & 0D \\ 0D & 09 & 0E & 0B \\ 0B & 0D & 09 & 0E \end{bmatrix} \begin{bmatrix} s_{0,0} & s_{0,1} & s_{0,2} & s_{0,3} \\ s_{1,0} & s_{1,1} & s_{1,2} & s_{1,3} \\ s_{2,0} & s_{2,1} & s_{2,2} & s_{2,3} \\ s_{3,0} & s_{3,1} & s_{3,2} & s_{3,3} \end{bmatrix} = \begin{bmatrix} s'_{0,0} & s'_{0,1} & s'_{0,2} & s'_{0,3} \\ s'_{1,0} & s'_{1,1} & s'_{1,2} & s'_{1,3} \\ s'_{2,0} & s'_{2,1} & s'_{2,2} & s'_{2,3} \\ s'_{3,0} & s'_{3,1} & s'_{3,2} & s'_{3,3} \end{bmatrix}$$

Inverse Add Round Key Transformation

- The inverse add round key transformation is identical to the forward add round key transformation, because the XOR operation is its own inverse

Thanks