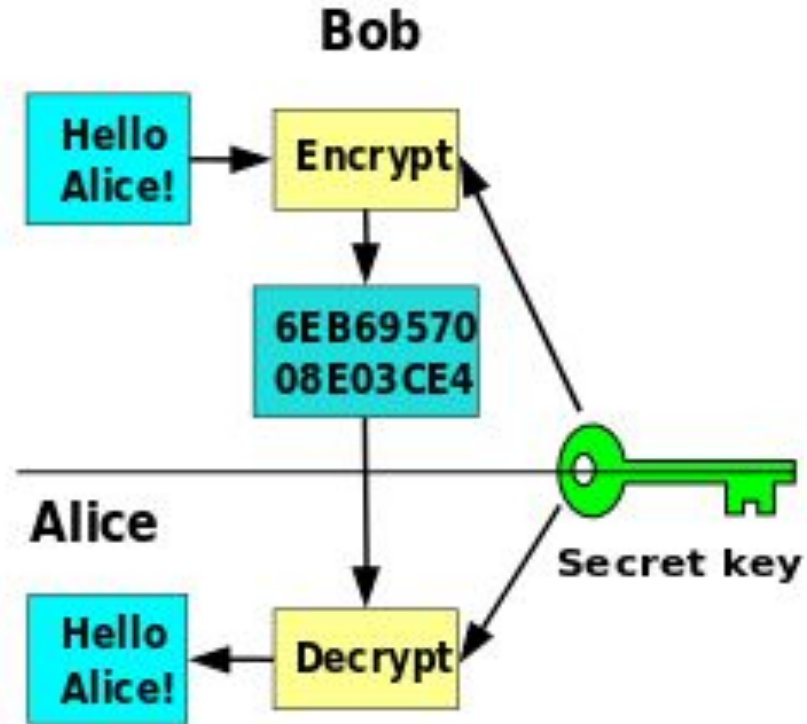# Cryptography

# Cryptography

Cryptography is the study of secure communications techniques that allow only the sender and intended recipient of a message to view its contents.
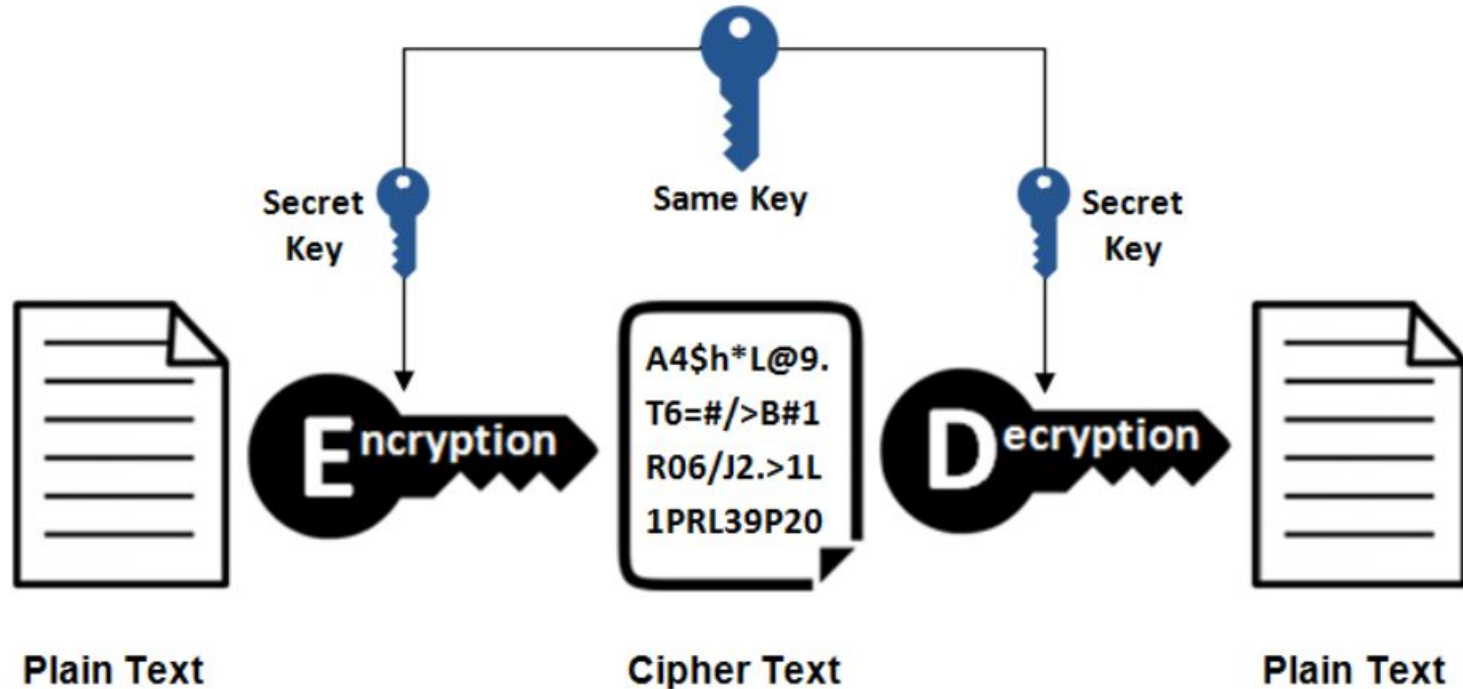
ABC (meaningful message) → ZYX(cipher)

# Cryptography

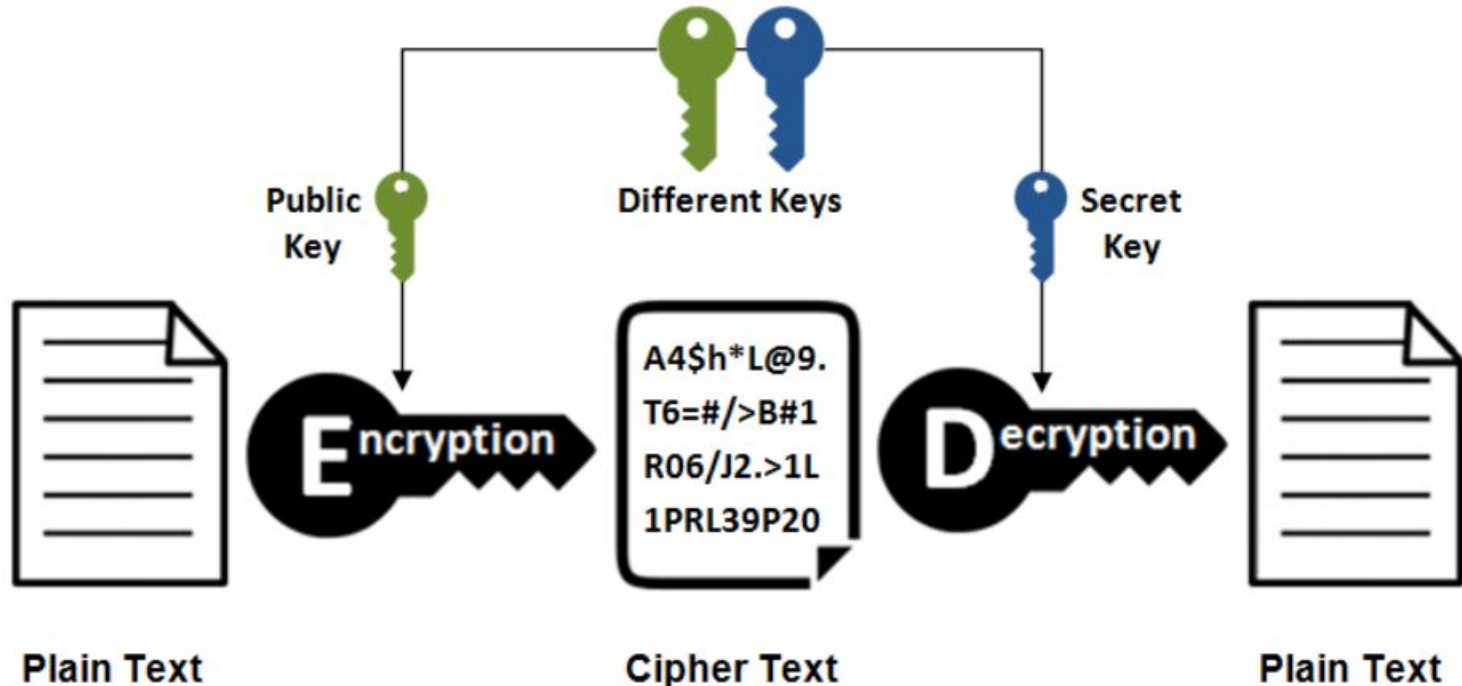# Symmetric vs Asymmetric Cryptography

## Symmetric Encryption

Secret Key

Same Key

Secret Key

**Plain Text**

**E**ncryption

Cipher Text

A4$h*L@9.
T6=#/>B#1
R06/J2.>1L
1PRL39P20

**D**ecryption

**Plain Text**

# Symmetric vs Asymmetric Cryptography

# What is AES?

- AES is an encryption standard chosen by the National Institute of Standards and Technology(NIST), USA to protect classified information. It has been accepted world wide as a desirable algorithm to encrypt sensitive data.

- It is a block cipher which operates on block size of 128 bits for both encrypting as well as decrypting.

- Each Round performs similar operations.

# Why AES?

- In 1990's the cracking of DES algorithm became possible.

- Around 50 hours of brute-forcing allowed to crack the message.

- NIST started searching for new feasible algorithm and proposed its requirement in 1997.

- In 2001 Rijndael algorithm designed by Rijment and Daemon of Belgium was declared as the winner of the competition.

- It met all Security, Cost and Implementation criteria.

# How Does AES work?

- AES basically repeats 4 major functions to encrypt data. It takes 128 bit block of data and a key and gives a ciphertext as output.The functions are:
  - Substitute Bytes
  - Shift Rows
  - Mix Columns
  - Add Key

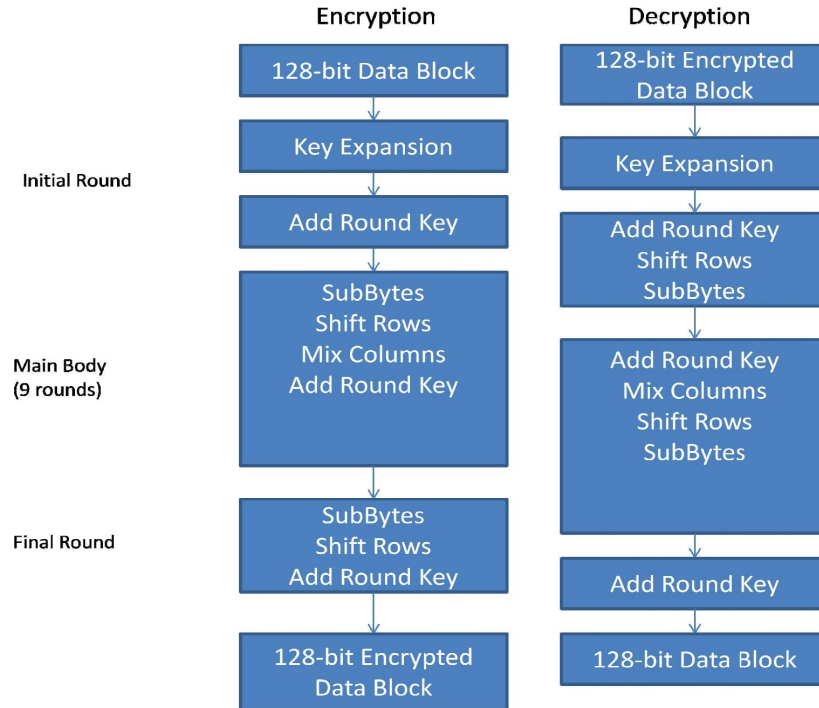# Steps for encryption and decryption



Figure 1 (Encryption on the left, Decryption on the right)

# Steps for encryption and decryption



Substitute Bytes

Shift Rows

Mix Columns

Add Round Key ← Round Key

Encryption Round

Inverse Mix Columns

Round Key → Add Round Key

Inverse Substitute Bytes

Inverse Shift Rows

Decryption Round
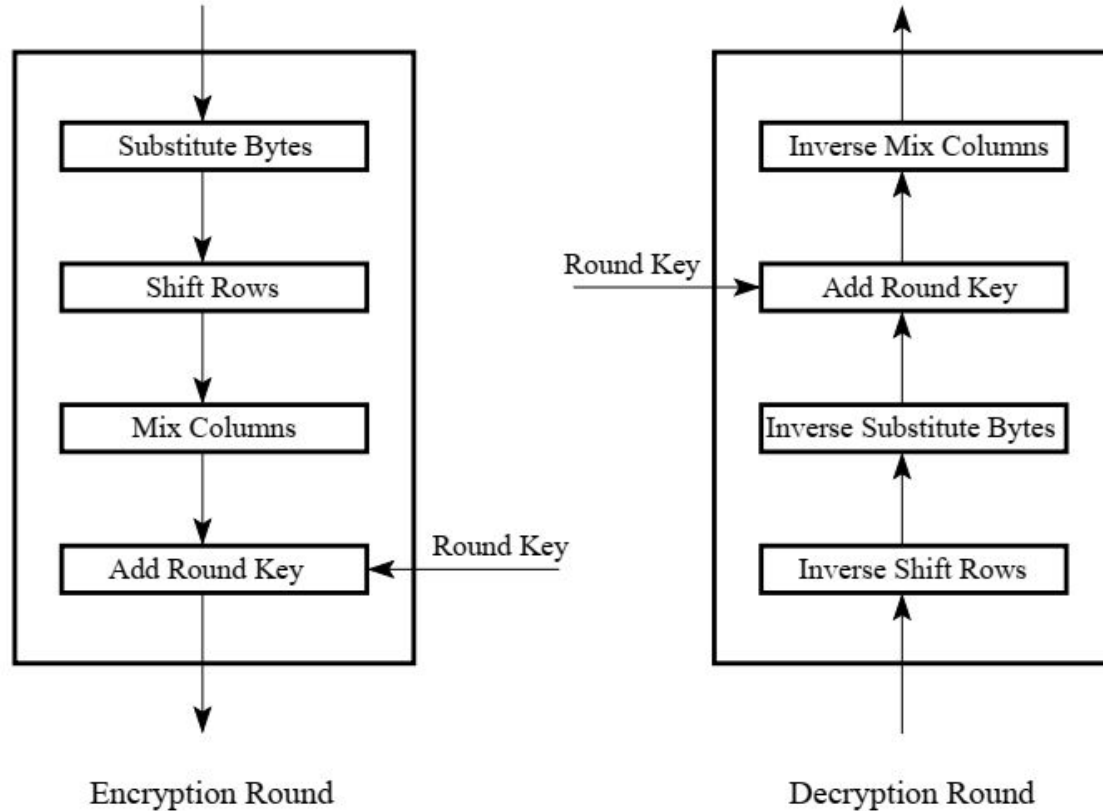
# Analysis of Steps: Key Expansion

- **Key Expansion:** In the key expansion process the given 128  bits cipher key is stored in a [4]x[4] byte matrix (16*8=128 bits) and then the four column words of the key matrix is expanded  into a schedule of 44 words (44*4=176 bytes) resulting in 11 round  keys.
- Number of round keys = $N_r$ + 1. Where $N_r$ is the number of  rounds (which is 10 in case of 128 bits key size). So, here, number round keys = 11.

# Analysis of Steps: Key Expansion
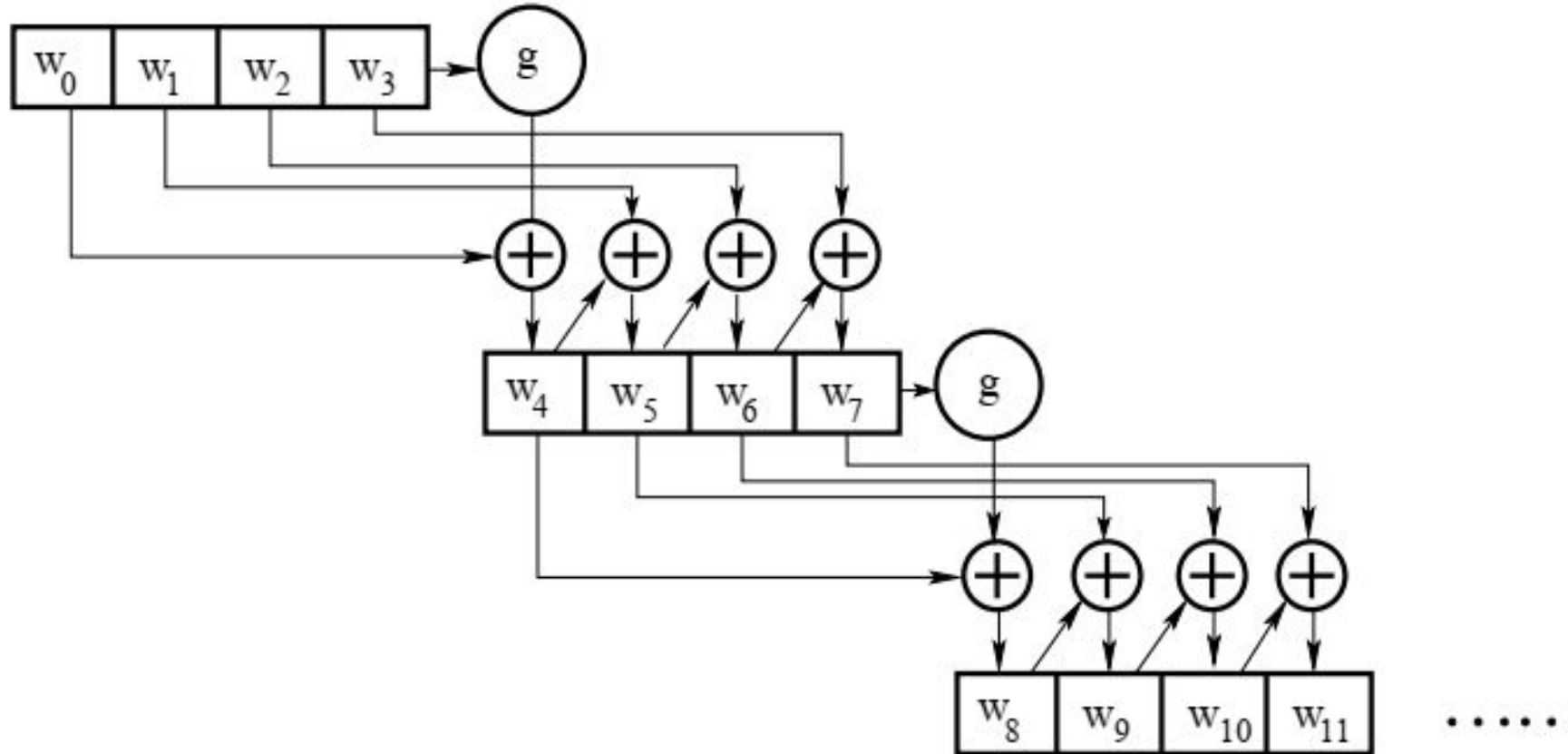
# Analysis of Steps: Substitute Bytes

**SubBytes:** Each element of the matrix is replaced by an element of the S-box matrix.
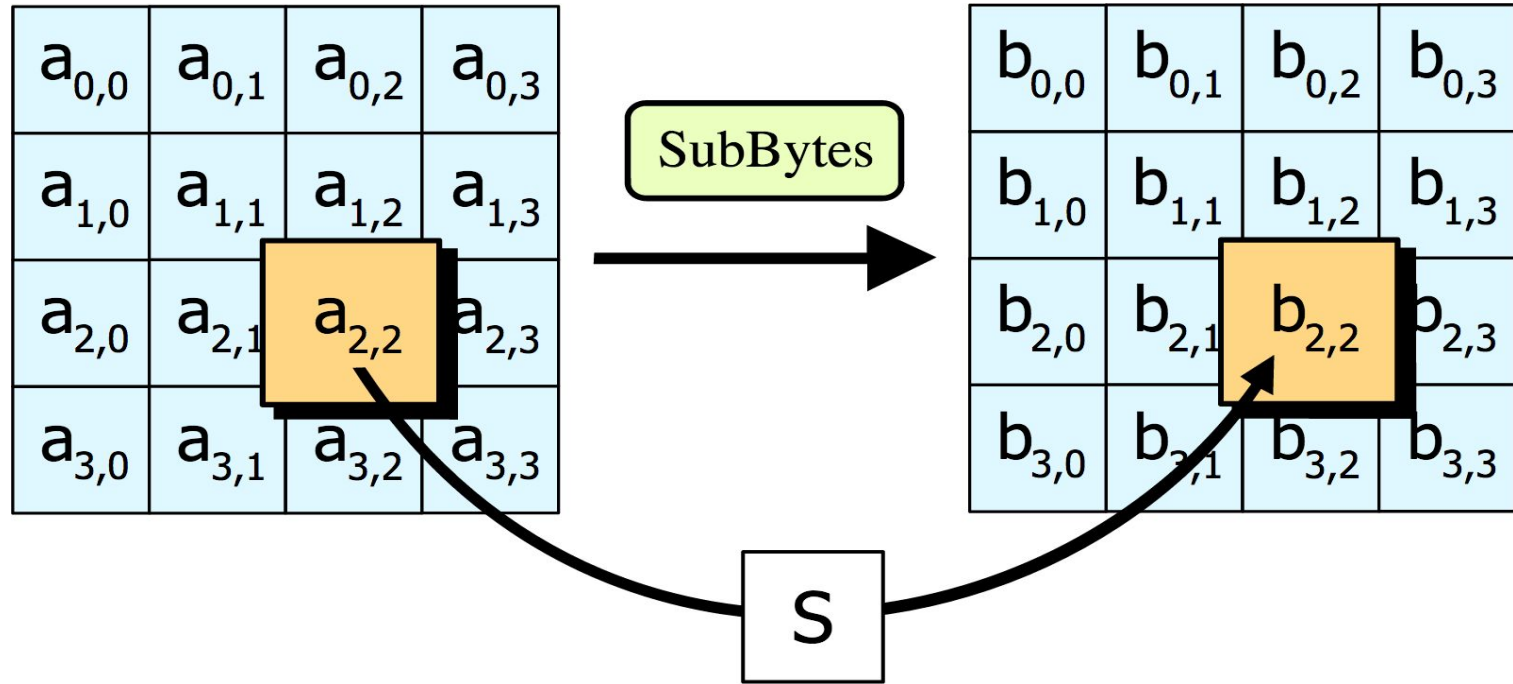
# Analysis of Steps: Substitute Bytes

**SubBytes:** Each element of the matrix is replaced by an element of the S-box matrix.

- The S-box is a special lookup table which is constructed from Galois fields.
- The Generating function used in this algorithm is $GF(2^8)$.
  - i.e., 256 values are possible
- The elements of the S-box are written in hexadecimal system.
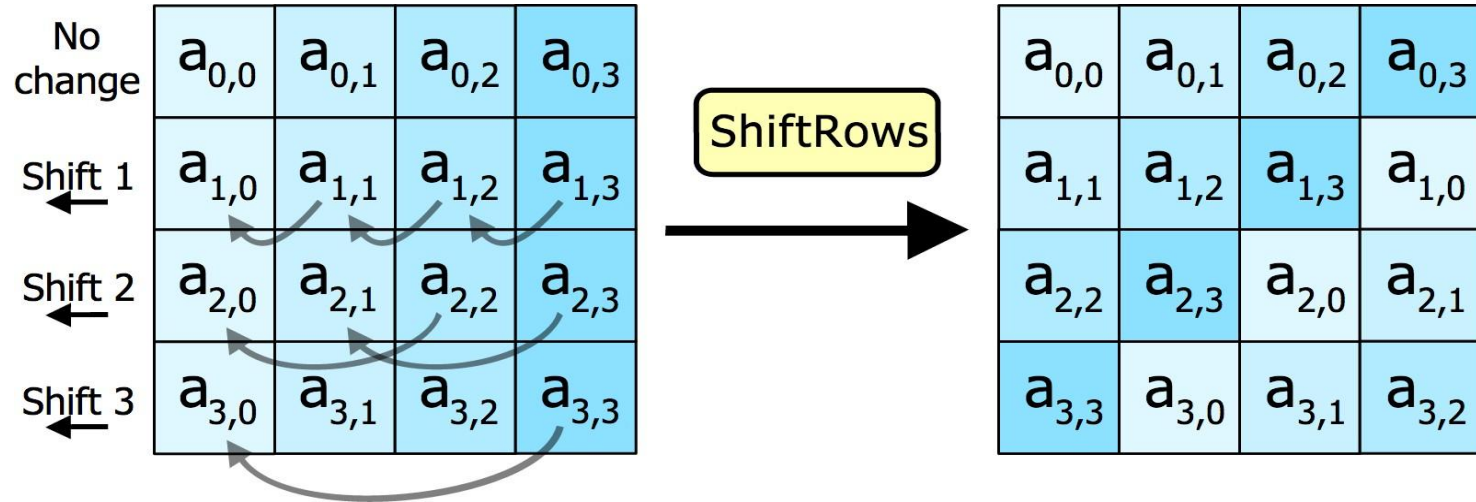
# Analysis of Steps: Substitute Bytes

**AES S-box**

|    | 00 | 01 | 02 | 03 | 04 | 05 | 06 | 07 | 08 | 09 | 0a | 0b | 0c | 0d | 0e | 0f |
|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|
| 00 | 63 | 7c | 77 | 7b | f2 | 6b | 6f | c5 | 30 | 01 | 67 | 2b | fe | d7 | ab | 76 |
| 10 | ca | 82 | c9 | 7d | fa | 59 | 47 | f0 | ad | d4 | a2 | af | 9c | a4 | 72 | c0 |
| 20 | b7 | fd | 93 | 26 | 36 | 3f | f7 | cc | 34 | a5 | e5 | f1 | 71 | d8 | 31 | 15 |
| 30 | 04 | c7 | 23 | c3 | 18 | 96 | 05 | 9a | 07 | 12 | 80 | e2 | eb | 27 | b2 | 75 |
| 40 | 09 | 83 | 2c | 1a | 1b | 6e | 5a | a0 | 52 | 3b | d6 | b3 | 29 | e3 | 2f | 84 |
| 50 | 53 | d1 | 00 | ed | 20 | fc | b1 | 5b | 6a | cb | be | 39 | 4a | 4c | 58 | cf |
| 60 | d0 | ef | aa | fb | 43 | 4d | 33 | 85 | 45 | f9 | 02 | 7f | 50 | 3c | 9f | a8 |
| 70 | 51 | a3 | 40 | 8f | 92 | 9d | 38 | f5 | bc | b6 | da | 21 | 10 | ff | f3 | d2 |
| 80 | cd | 0c | 13 | ec | 5f | 97 | 44 | 17 | c4 | a7 | 7e | 3d | 64 | 5d | 19 | 73 |
| 90 | 60 | 81 | 4f | dc | 22 | 2a | 90 | 88 | 46 | ee | b8 | 14 | de | 5e | 0b | db |
| a0 | e0 | 32 | 3a | 0a | 49 | 06 | 24 | 5c | c2 | d3 | ac | 62 | 91 | 95 | e4 | 79 |
| b0 | e7 | c8 | 37 | 6d | 8d | d5 | 4e | a9 | 6c | 56 | f4 | ea | 65 | 7a | ae | 08 |
| c0 | ba | 78 | 25 | 2e | 1c | a6 | b4 | c6 | e8 | dd | 74 | 1f | 4b | bd | 8b | 8a |
| d0 | 70 | 3e | b5 | 66 | 48 | 03 | f6 | 0e | 61 | 35 | 57 | b9 | 86 | c1 | 1d | 9e |
| e0 | e1 | f8 | 98 | 11 | 69 | d9 | 8e | 94 | 9b | 1e | 87 | e9 | ce | 55 | 28 | df |
| f0 | 8c | a1 | 89 | 0d | bf | e6 | 42 | 68 | 41 | 99 | 2d | 0f | b0 | 54 | bb | 16 |

**Inverse S-box**

|    | 00 | 01 | 02 | 03 | 04 | 05 | 06 | 07 | 08 | 09 | 0a | 0b | 0c | 0d | 0e | 0f |
|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|
| 00 | 52 | 09 | 6a | d5 | 30 | 36 | a5 | 38 | bf | 40 | a3 | 9e | 81 | f3 | d7 | fb |
| 10 | 7c | e3 | 39 | 82 | 9b | 2f | ff | 87 | 34 | 8e | 43 | 44 | c4 | de | e9 | cb |
| 20 | 54 | 7b | 94 | 32 | a6 | c2 | 23 | 3d | ee | 4c | 95 | 0b | 42 | fa | c3 | 4e |
| 30 | 08 | 2e | a1 | 66 | 28 | d9 | 24 | b2 | 76 | 5b | a2 | 49 | 6d | 8b | d1 | 25 |
| 40 | 72 | f8 | f6 | 64 | 86 | 68 | 98 | 16 | d4 | a4 | 5c | cc | 5d | 65 | b6 | 92 |
| 50 | 6c | 70 | 48 | 50 | fd | ed | b9 | da | 5e | 15 | 46 | 57 | a7 | 8d | 9d | 84 |
| 60 | 90 | d8 | ab | 00 | 8c | bc | d3 | 0a | f7 | e4 | 58 | 05 | b8 | b3 | 45 | 06 |
| 70 | d0 | 2c | 1e | 8f | ca | 3f | 0f | 02 | c1 | af | bd | 03 | 01 | 13 | 8a | 6b |
| 80 | 3a | 91 | 11 | 41 | 4f | 67 | dc | ea | 97 | f2 | cf | ce | f0 | b4 | e6 | 73 |
| 90 | 96 | ac | 74 | 22 | e7 | ad | 35 | 85 | e2 | f9 | 37 | e8 | 1c | 75 | df | 6e |
| a0 | 47 | f1 | 1a | 71 | 1d | 29 | c5 | 89 | 6f | b7 | 62 | 0e | aa | 18 | be | 1b |
| b0 | fc | 56 | 3e | 4b | c6 | d2 | 79 | 20 | 9a | db | c0 | fe | 78 | cd | 5a | f4 |
| c0 | 1f | dd | a8 | 33 | 88 | 07 | c7 | 31 | b1 | 12 | 10 | 59 | 27 | 80 | ec | 5f |
| d0 | 60 | 51 | 7f | a9 | 19 | b5 | 4a | 0d | 2d | e5 | 7a | 9f | 93 | c9 | 9c | ef |
| e0 | a0 | e0 | 3b | 4d | ae | 2a | f5 | b0 | c8 | eb | bb | 3c | 83 | 53 | 99 | 61 |
| f0 | 17 | 2b | 04 | 7e | ba | 77 | d6 | 26 | e1 | 69 | 14 | 63 | 55 | 21 | 0c | 7d |

# Analysis of Steps: Shift Rows

**Shift Rows:** In this step rows of the block are cylindrically shifted in left/right direction. The first row is untouched, the second one is shift by one, third one by two and the fourth one by three.

# Analysis of Steps: Shift Rows
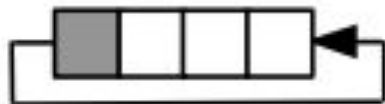
# Analysis of Steps: Mix columns

**Mix columns:** This is the most important part of the algorithm. It causes the flip of bits to spread all over the block. In this step the block is multiplied with a fixed matrix. The multiplication is a field multiplication in galois field.

For each row there are 16 multiplication, 12 XORs and a 4 byte output.

# Analysis of Steps: Mix columns

$$
\begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \times \begin{bmatrix} s_{0.0} & s_{0,1} & s_{0,2} & s_{0,3} \\ s_{1.0} & s_{1,1} & s_{1,2} & s_{1,3} \\ s_{2.0} & s_{2,1} & s_{2,2} & s_{2,3} \\ s_{3.0} & s_{3,1} & s_{3,2} & s_{3,3} \end{bmatrix} = \begin{bmatrix} s'_{0.0} & s'_{0,1} & s'_{0,2} & s'_{0,3} \\ s'_{1.0} & s'_{1,1} & s'_{1,2} & s'_{1,3} \\ s'_{2.0} & s'_{2,1} & s'_{2,2} & s'_{2,3} \\ s'_{3.0} & s'_{3,1} & s'_{3,2} & s'_{3,3} \end{bmatrix}
$$

# Analysis of Steps: Mix columns

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

$$
\begin{aligned}
s'_{0,j} &= (2 \bullet s_{0,j}) \oplus (3 \bullet s_{1,j}) \oplus s_{2,j} \oplus s_{3,j} \\
s'_{1,j} &= s_{0,j} \oplus (2 \bullet s_{1,j}) \oplus (3 \bullet s_{2,j}) \oplus s_{3,j} \\
s'_{2,j} &= s_{0,j} \oplus s_{1,j} \oplus (2 \bullet s_{2,j}) \oplus (3 \bullet s_{3,j}) \\
s'_{3,j} &= (3 \bullet s_{0,j}) \oplus s_{1,j} \oplus s_{2,j} \oplus (2 \bullet s_{3,j})
\end{aligned}
$$

**Predefine Matrix**   **State Array**   **New State Array**

# Analysis of Steps: Mix columns

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

# Analysis of Steps: Add round key

**Add round key:** In this step, each byte is XOR-ed with corresponding element of the key matrix.
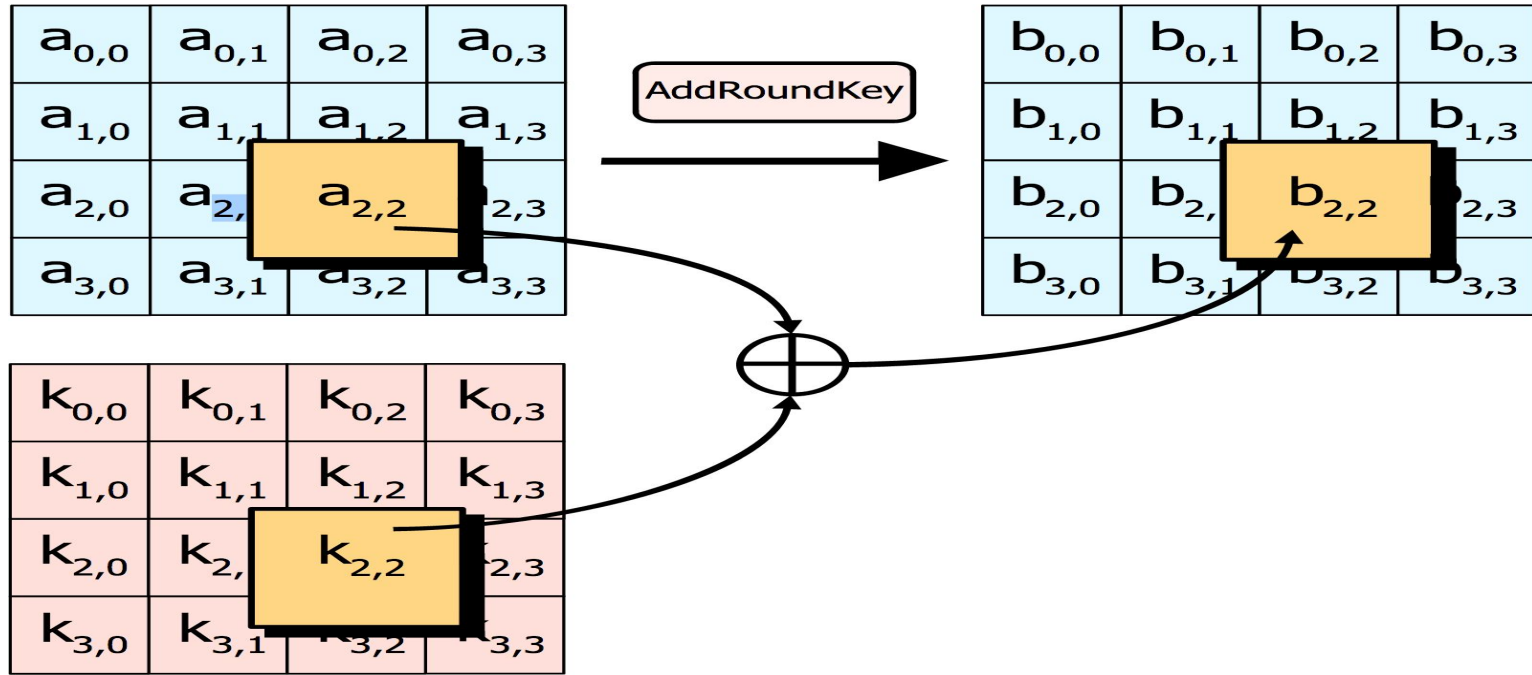
# RSA

# RSA

- RSA is one of the oldest asymmetric encryption algorithm.
- The acronym "RSA" comes from the surnames of Ron Rivest, Adi Shamir and Leonard Adleman.
- The security of RSA relies on the practical difficulty of factoring the product of two large prime numbers, the "factoring problem".

# RSA algorithm steps: Key-Generation

- Step-1: Select two large prime numbers p and q where p ≠ q
- Step-2: Calculate n = p · q
- Step-3: Calculate λ = LCM((p–1),(q–1))
- Step-4: Select e such that,
  - e is relatively prime to λ, i.e. gcd(e, λ) = 1
  - 1 < e < λ
- Step-5: Calculate d = ($e^{-1}$) (mod λ), so e · d = 1 (mod λ)
- Step-6: Public key = {e, n}, private key = {d, n}

# RSA algorithm steps: Encryption

- Let P be the plain text
- Find out the ciphertext C using the formula, $C = P^e \pmod{n}$ where, $P < n$

# RSA algorithm steps: Decryption

- Let C be the ciphertext
- Find out the plain text P using the formula, $P = C^d \pmod{n}$ where, $C < n$