Encryption

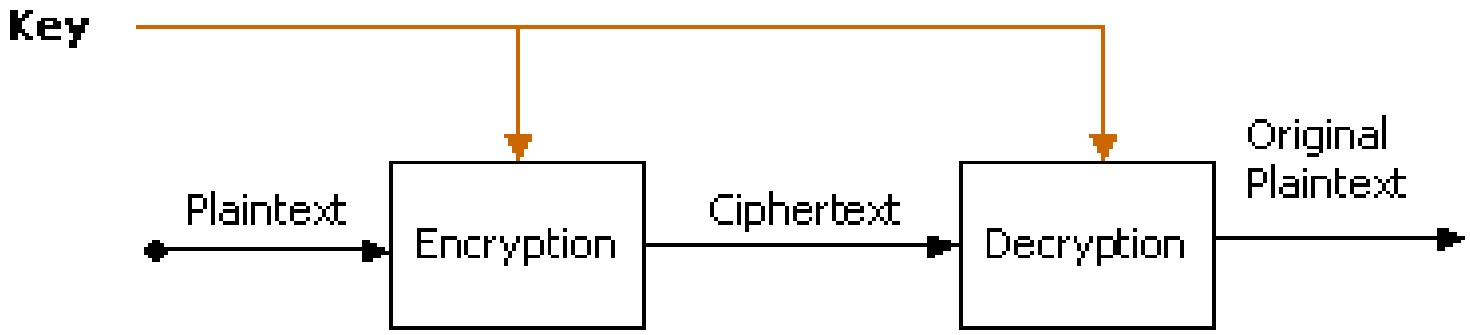
TOPICS

- Objectives
- RC4
- DES
- 3DES
- AES

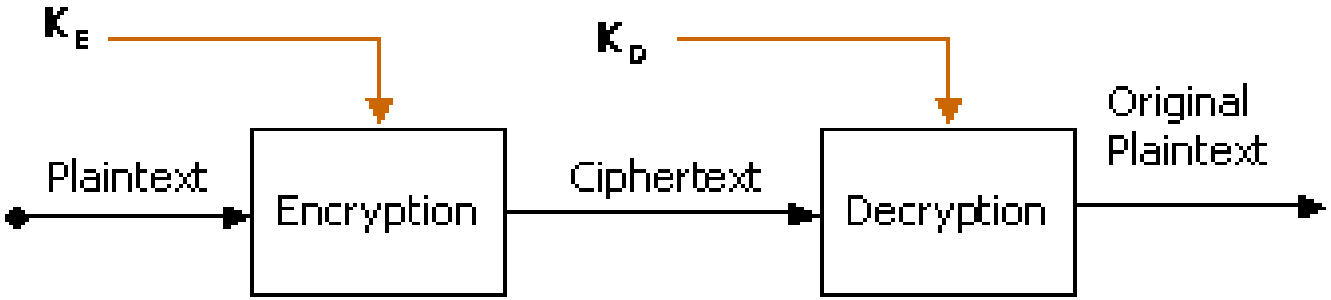
Objectives

- To understand the process of encryption and strong encryption algorithms.

Key Encryption Process



Secret Key Encryption



Public Key Cryptosystem



Block Ciphers vs Stream Cipher

- Block ciphers – ie. DES, 3DES, AES
  - Message is broken into blocks, each of which is then encrypted
  - Operate with a fixed transformation on large blocks of plaintext data
- Stream ciphers – ie. RC4
  - Process the message bit by bit (as a stream)
  - Operate with a time-varying transformation on individual plaintext digits

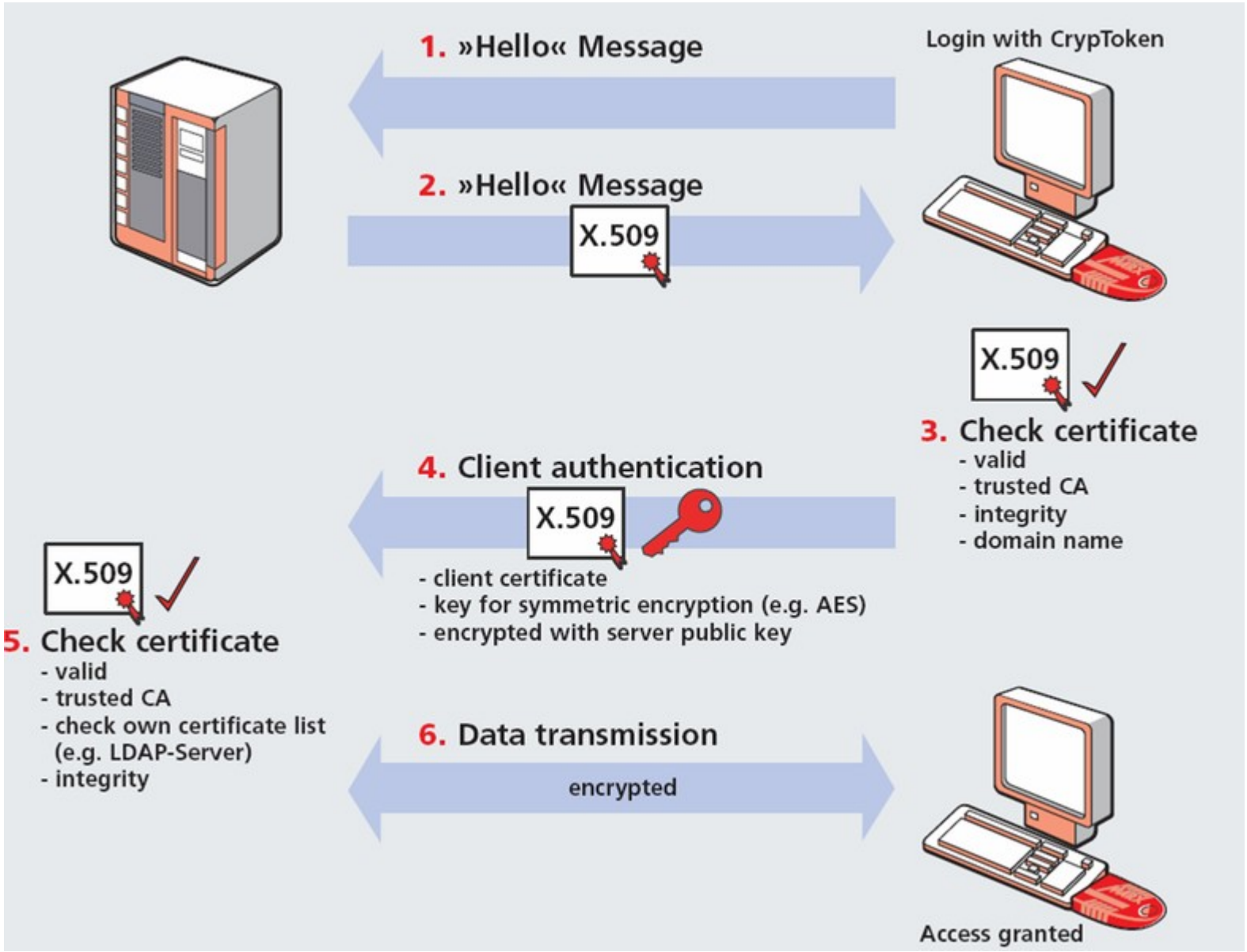
Confusion vs Diffusion

- Confusion: to make the relation between the plaintext and the ciphertext as complex as possibe
  - Caesar ciphers have poor confusion
  - Polyalphabetic substitutions and Vernam cipher have good confusion
- Diffusion: to spread the influence of the individual plaintext characters over as much of the ciphertext as possible, therefore hiding
  - Substitution ciphers
  - Transposition ciphers

Encryption Algorithm Characteristics

Name	Cipher Type	Key Size	Common Use
RC4	Stream	64,128 up to 256 bits	WEP,WPA (TKIP),SSL/TLS
DES	Block	64-bit (56-bit key + 8 Parity bits)	SSH, IPSec
3DES	Block	Three-Key Mode: 192-bit (168-bit key + 24 Parity bits) Two-Key Mode: 128-bit (112-bit key + 16 Parity bits)	SSL/TLS,SSH, IPSec
AES	Block	128,192,256-bits	802.11i-CCMP, SSH,PGP

Client Authentication SSL

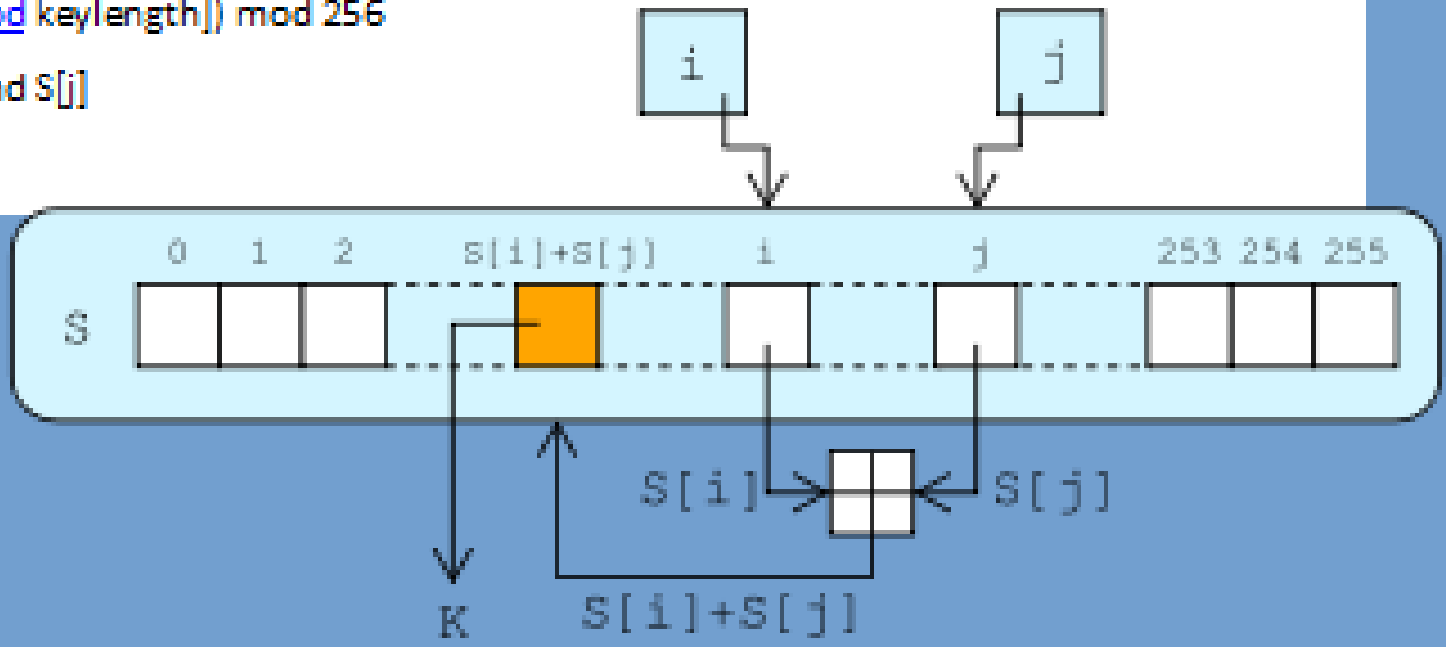


RC4

- RC4 was designed by Ron Rivest of RSA Security in 1987, it is officially termed “Rivest Cipher 4”.
- RC4 algorithm is capable of key lengths of up to 256 bits and is typically implemented in 64 bits, 128 bits and 256 bits.
- RC4 is used in WEP, TKIP, Secure Sockets Layer (SSL) , (TLS) Transport Layer Security

RC4
Key-Scheduling Alg.

```
for i from 0 to 255
    S[i] := i
endfor
j := 0
for i from 0 to 255
    j := (j + S[i] + key[i mod keylength]) mod 256
    swap values of S[i] and S[j]
endfor
```



RC4 – PRGA, Pseudo Random Generation Algorithm

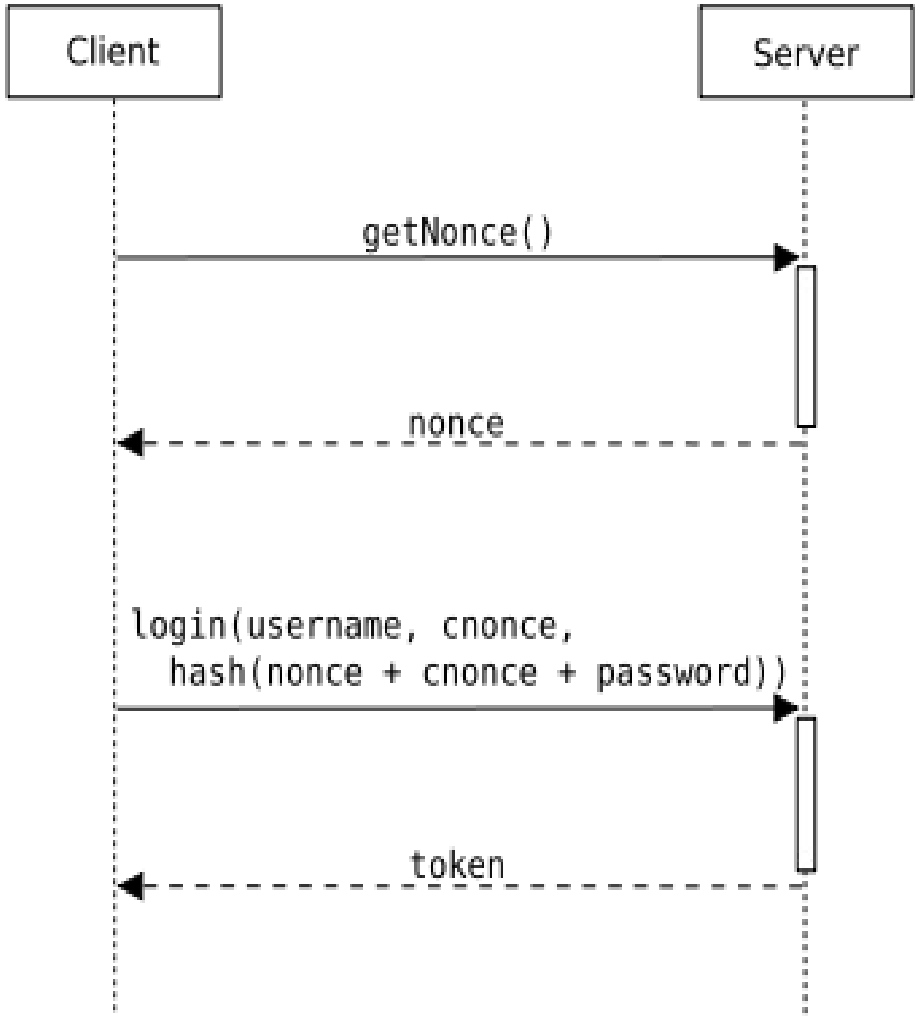
```
i := 0
j := 0
while GeneratingOutput:
    i := (i + 1) mod 256
    j := (j + S[i]) mod 256
    swap values of S[i] and S[j]
    K := S[(S[i] + S[j]) mod 256]
    output K
endwhile
```

RC4 Test Vector

Key	Keystream	Plaintext	Ciphertext
Key	eb9f7781b734ca72a719...	Plaintext	BBF316E8D940AF0AD3

Secret	04d46b053ca87b59...	Attack at dawn	45A01F645FC35B383552544B9BF5

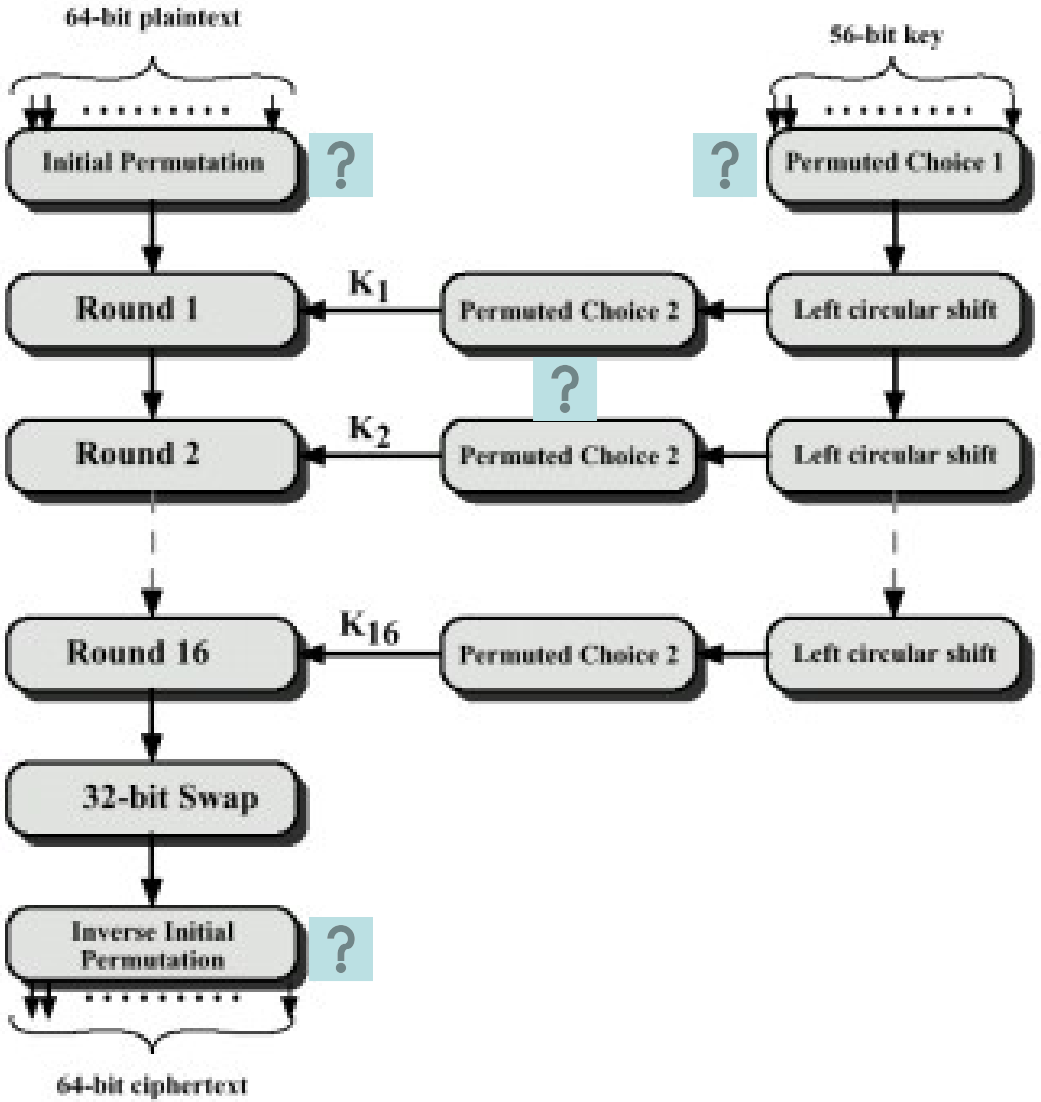
Cryptographic nonce



Data Encryption Standard (DES)

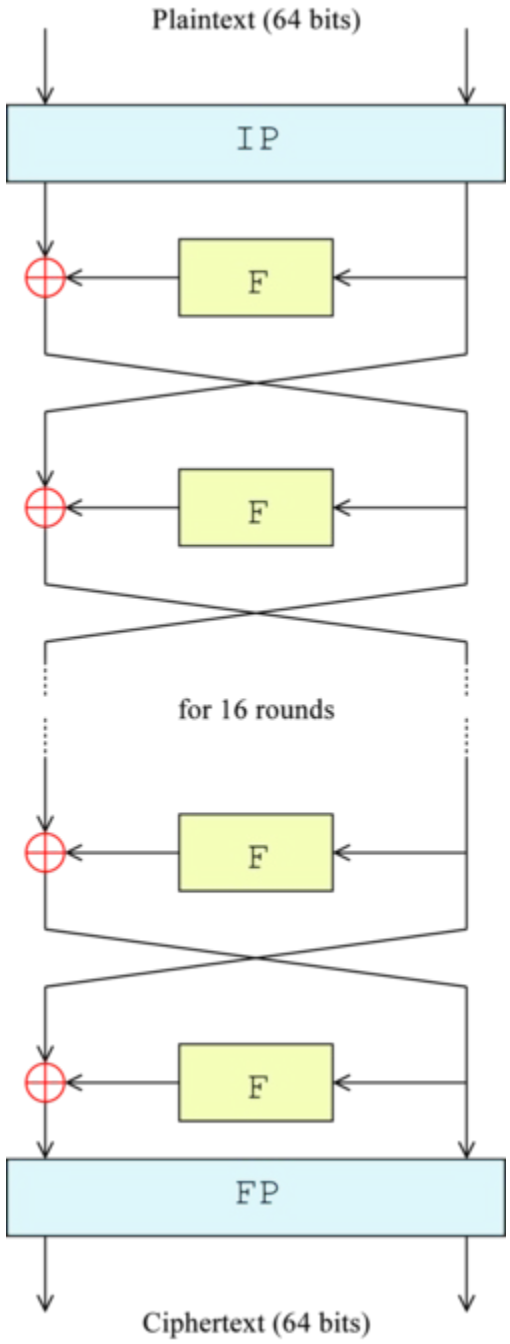
- Most widely-used secret-key encryption method
- Originally developed by IBM in 1970s, later adopted by U.S. government in 1977
- Encrypts 64-bit plaintext using a 56-bit key
- Relatively inexpensive to implement in hardware and widely available
- Largest users: financial transactions, PIN code generation, etc.

DES Algorithm



64-bit plaintext is divided into two halves. left half and right half, 32 bits each. 16 rounds.

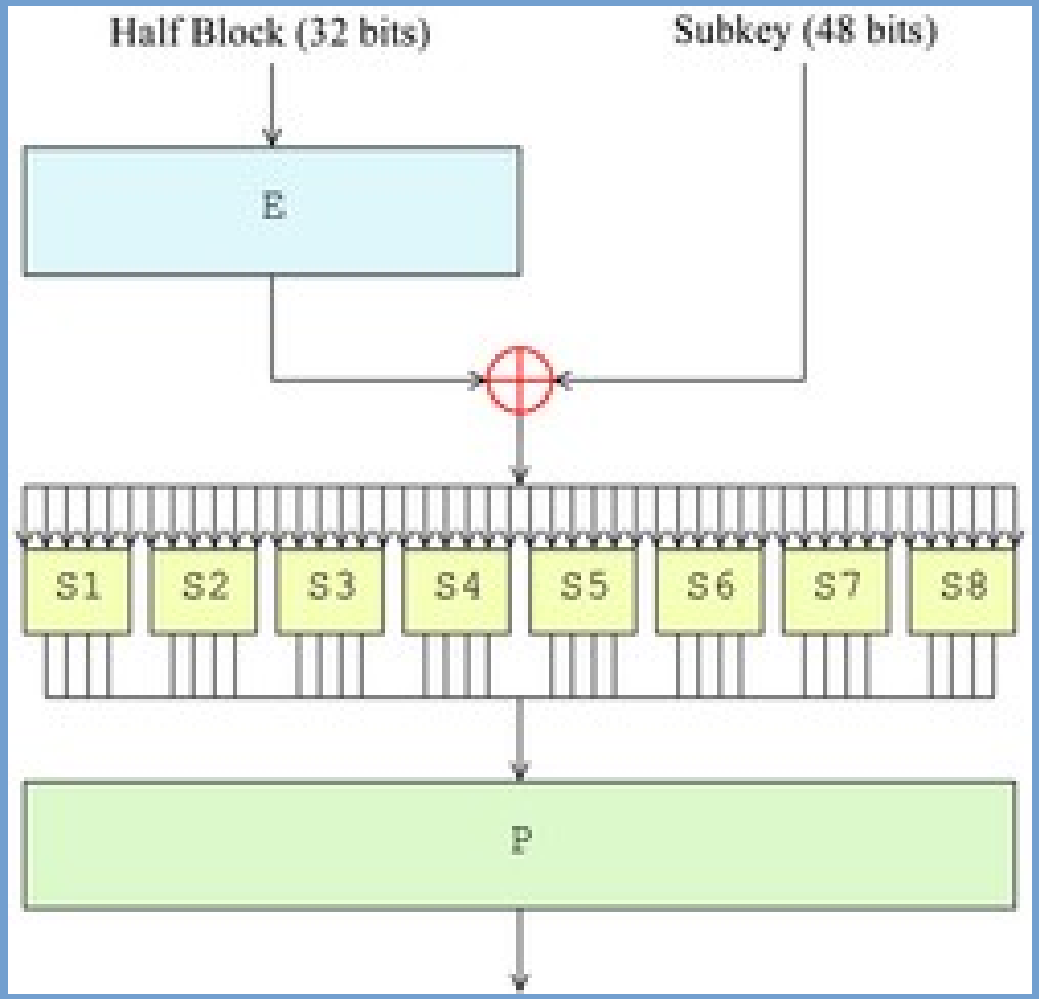
This example shows one half.


Plaintext (64 bits)
IP
F
F
for 16 rounds
F
F
FP
Ciphertext (64 bits)

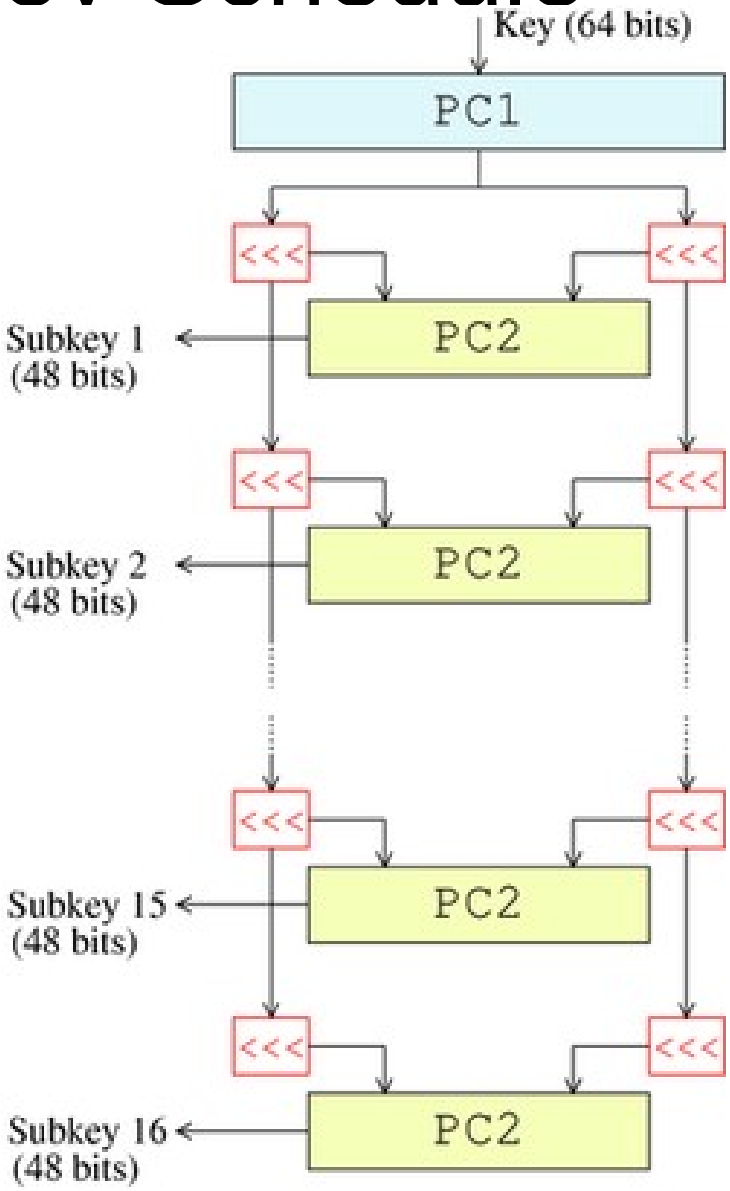
Feistel Function

1. Expansion
2. Key Mixing
3. Substitution
4. Permutation

Feistel Function (Expansion)

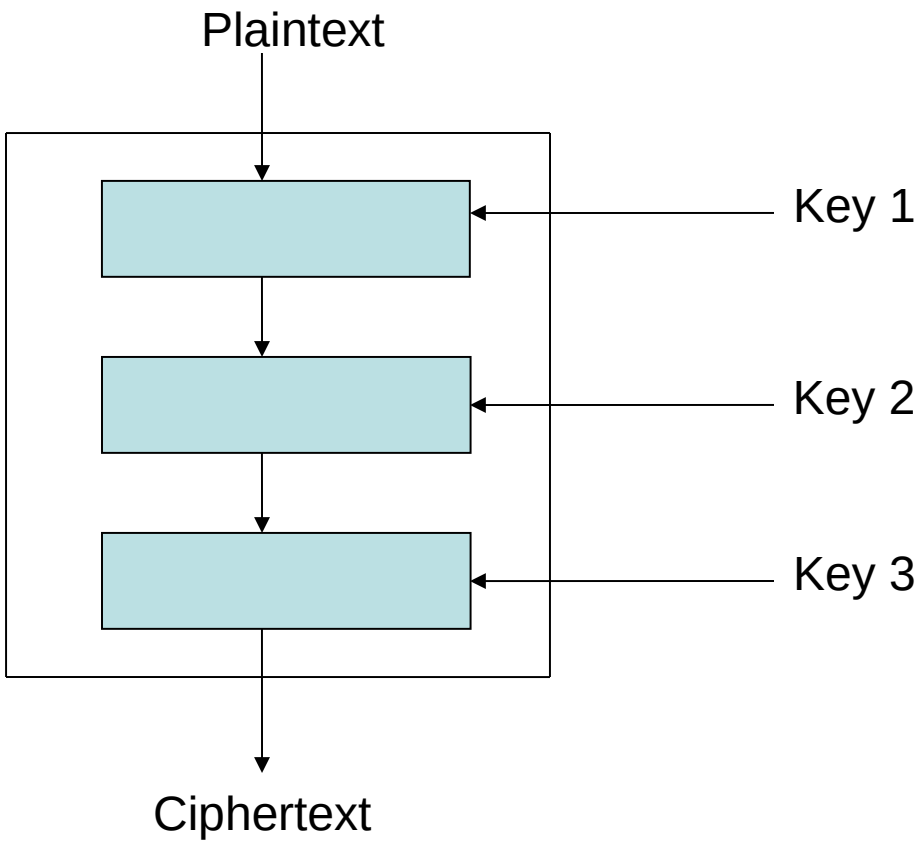


Kev Schedule



DES Cracking Time!

3DES Encryption Process



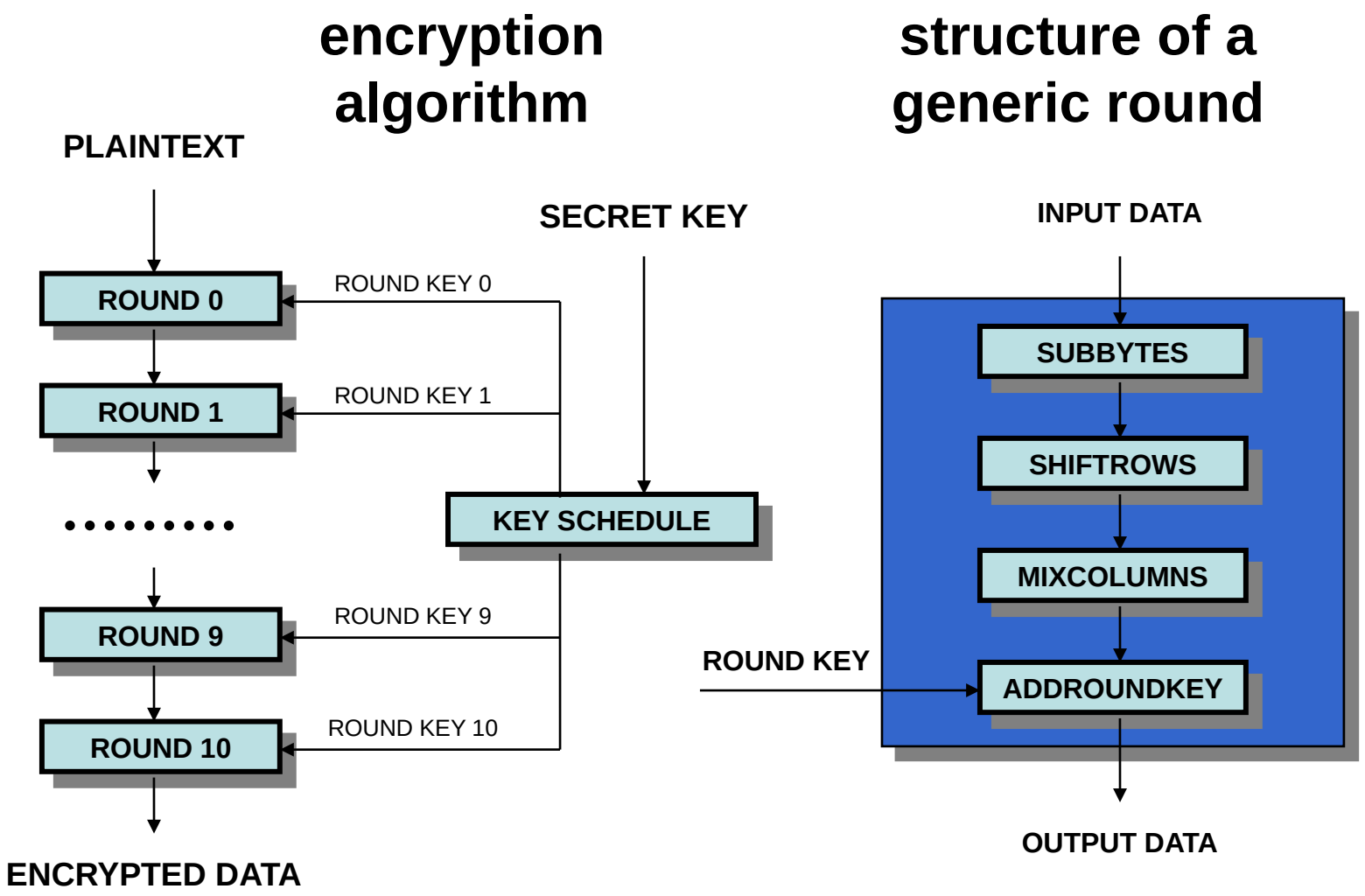
Advanced Encryption Standard
AES ENCRYPTION

- Rijndael is the selected (NIST competition) algorithm for AES (advanced encryption standard).
- Now standardized as FIPS-197
- It is a block cipher algorithm, operating on blocks of data.
- It needs a secret key, which is another block of data.

AES ENCRYPTION

- Performs encryption and the inverse operation, decryption (using the same secret key).
- It reads an entire block of data, processes it in rounds and then outputs the encrypted (or decrypted) data.
- Each round is a sequence of four inner transformations.
- The AES standard specifies 128-bit data blocks and 128-bit, 192-bit or 256-bit secret keys.

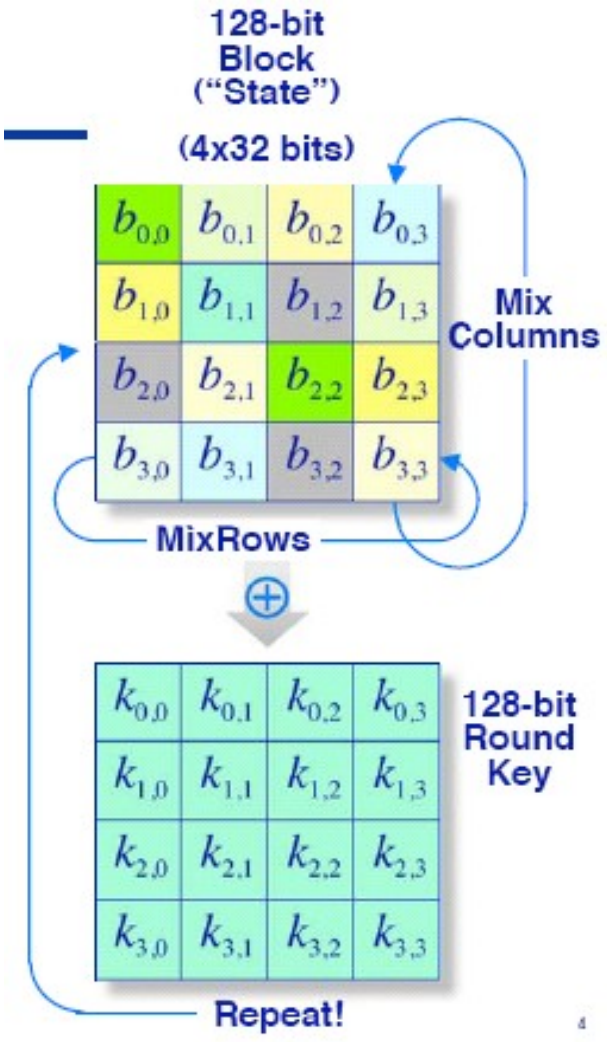
AES Algorithm – Encryption



AES Algorithm – Encryption
A little closer look

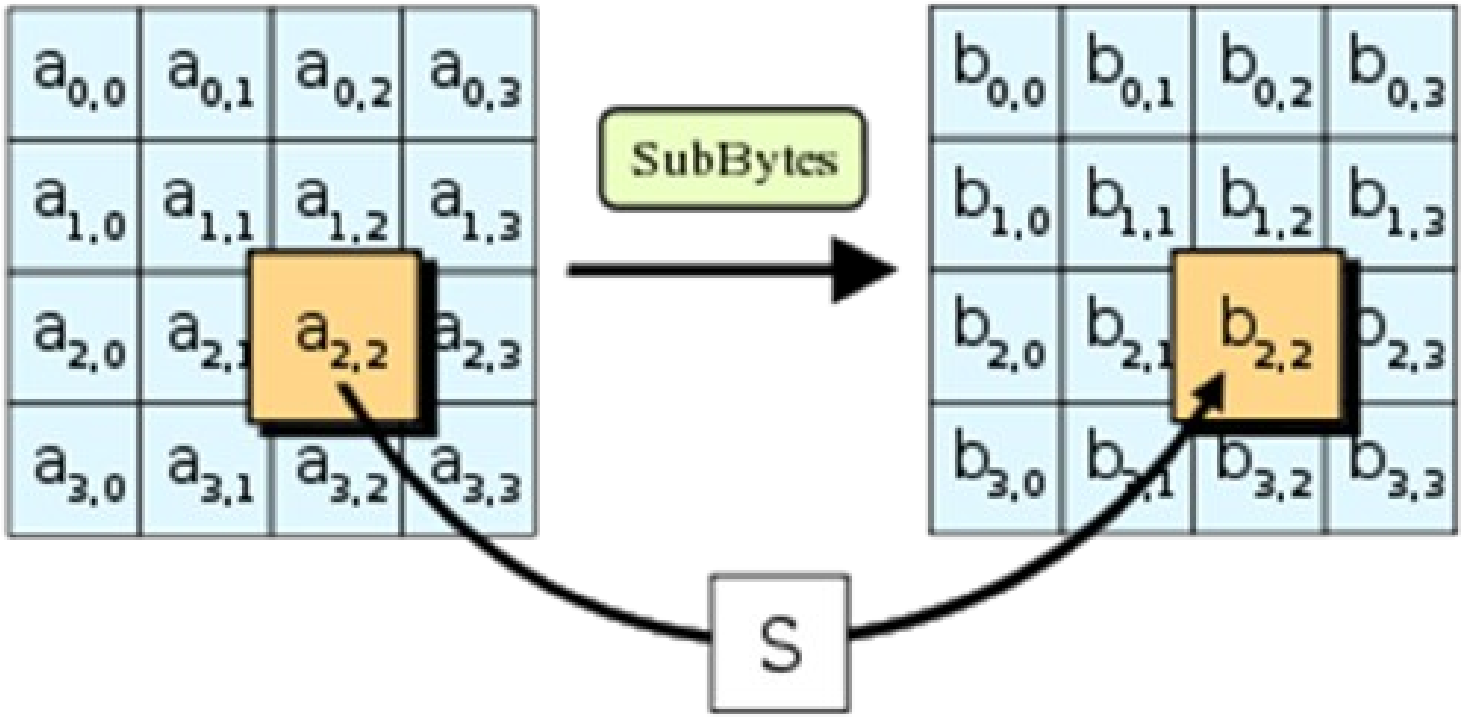
1. Perform a byte by byte substitution
2. Perform a row by row shift operation
3. Perform a column by column transformation
4. Perform a XOR with a round key

No of rounds = 10 for 128 bits
12 for 192 bits
14 for 256 bits



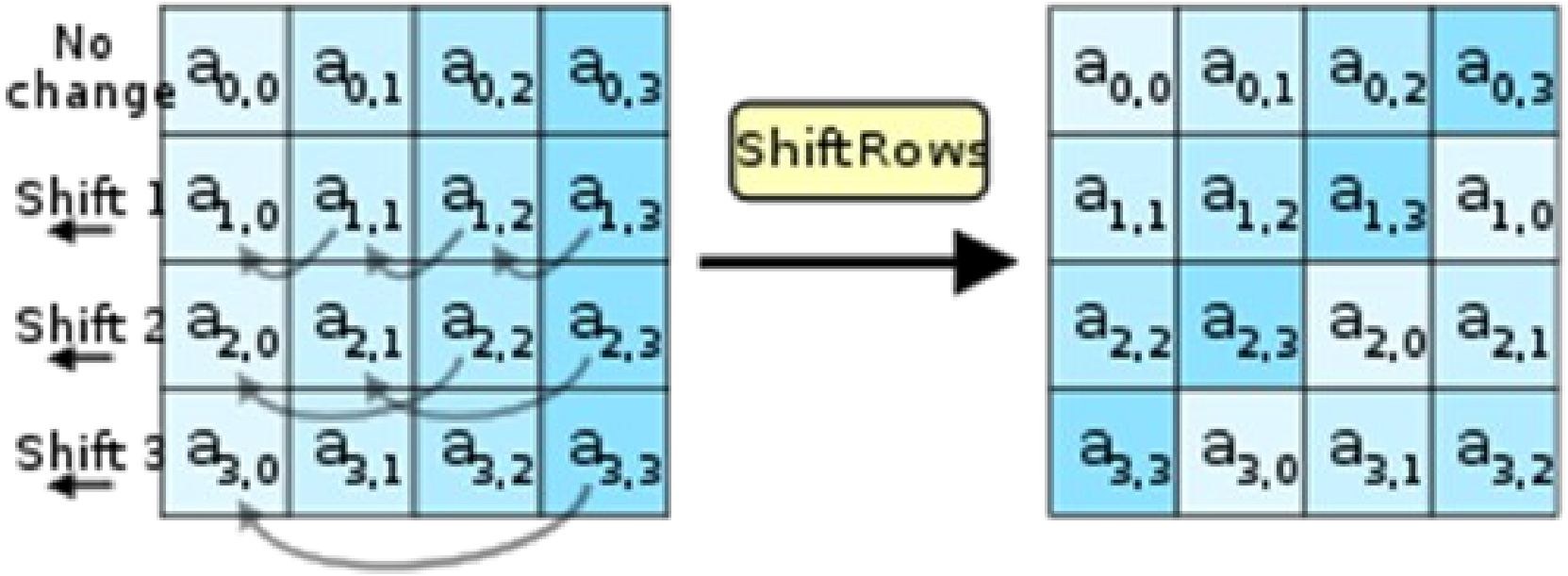
AES
Advanced Encryption Standard

1. The SubByte Step



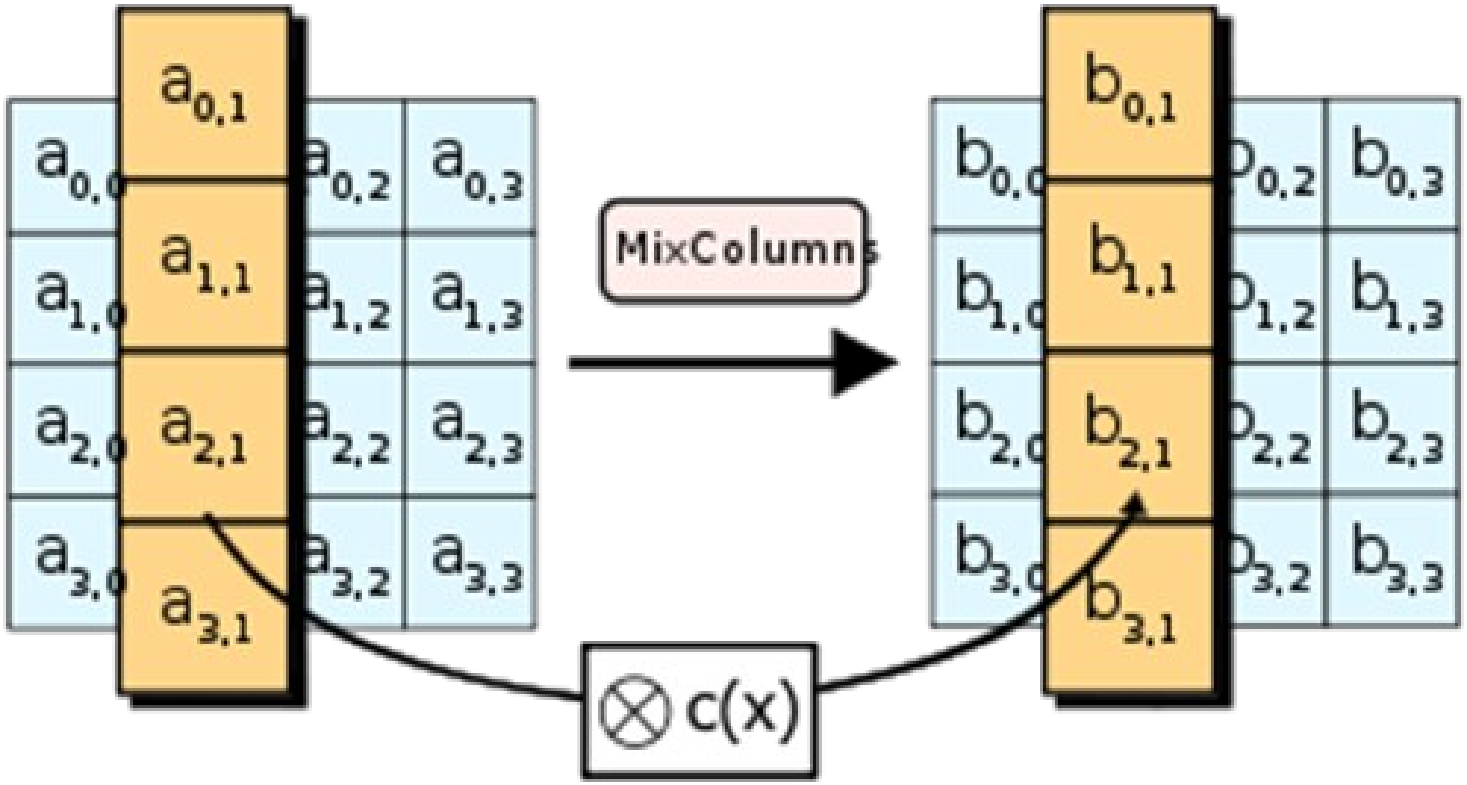
AES
Advanced Encryption Standard

2. The ShiftRow Step



AES
Advanced Encryption Standard

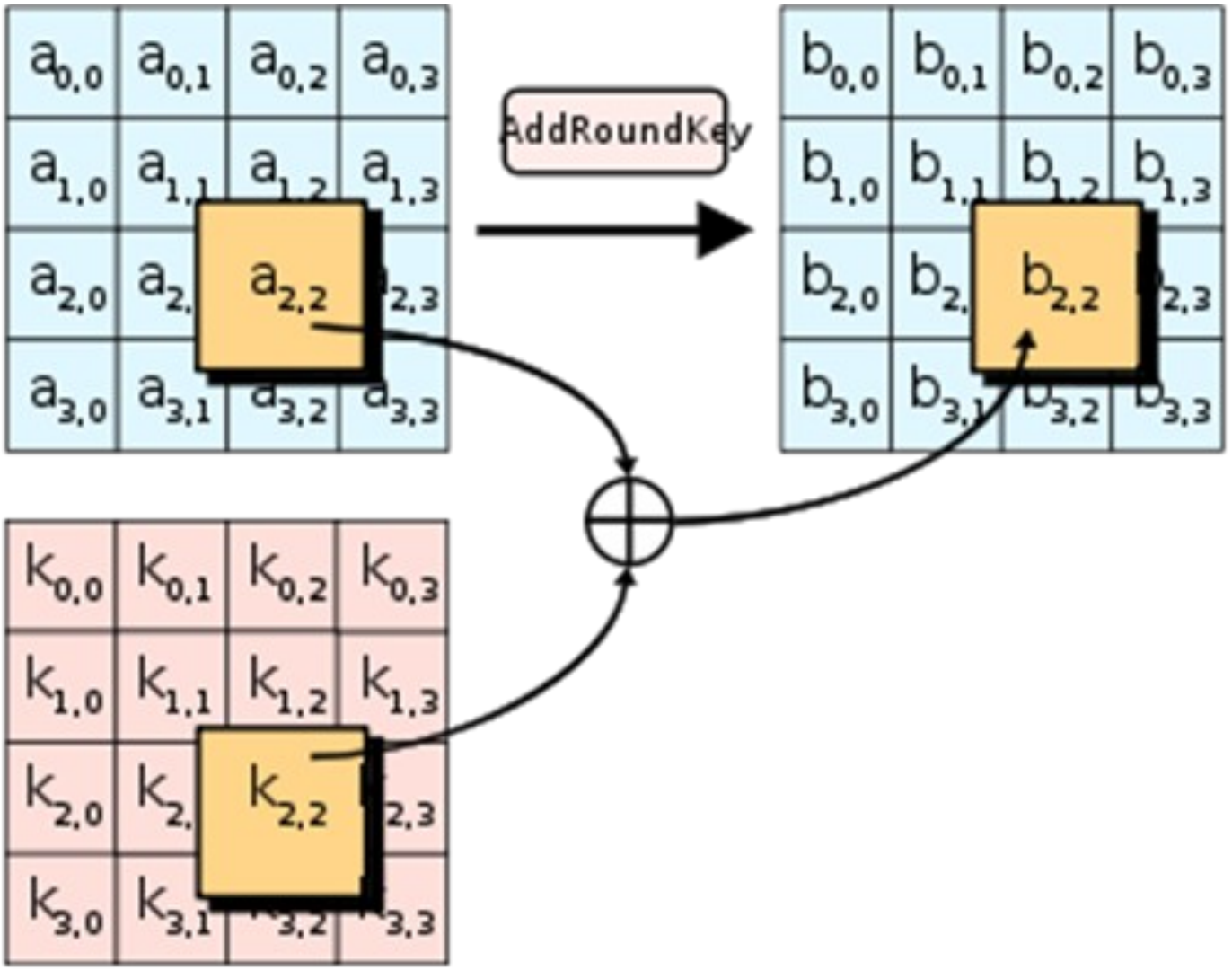
3. The MixColumns Step



multiplication operation

$$\begin{bmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{bmatrix}.$$

AES
The AddRoundKey step



Some facts about AES

- AES keys (128bits)

  340,000,000,000,000,000,000,000,000,000,000,000,000

  possible keys
- Suitable for a wide variety of platforms - ranging from smart cards to servers
- Much simpler, faster and more secure (than it’s predecessor 3DES)

AES ‘built-into’ products

- Navastream Crypto Phones
- PGP Mobile for the TREO 650
- Nokia’s solutions for mobile VPN client – AES 256



AES Cracking - 2006

- Assumptions
  - 3 GHz dedicated processor
  - 1 clock cycle per key generation
- 2^128 keys / 3E9 processes per second =
  - 1.13E29 seconds
  - 3.6E21 years, 3.6 Zy (Zetta years)
  - 3.6 Sextillion years

AES Cracking - Future

- 1 Week Decryption
- 5.6E32 Hz Processor, 560 MHz

Clock Cycles per Key Generation

Processor Speed Doubling Rate (Years)	1	4	8	16
0.5	38.8	155.3	310.7	621.3
1	77.7	310.7	621.3	1242.6
1.5	**116.5**	**466.0**	**932.0**	**1863.9**
2	155.3	621.3	1242.6	2485.3

Conclusion

- DES has been found to be vulnerable to brute-force attacks.
- 3DES, an encryption algorithm with three successive 56-bit keys, makes it a stronger solution but is much slower than DES.
- AES is currently still considered free from successful cryptanalytic attacks.