Lecture 6

Cryptography 3: block ciphers

Today: Block Ciphers

- Block ciphers: theory
- ECB mode & attacks
- CBC mode & attacks
- Feistel ciphers (...)
- (...)

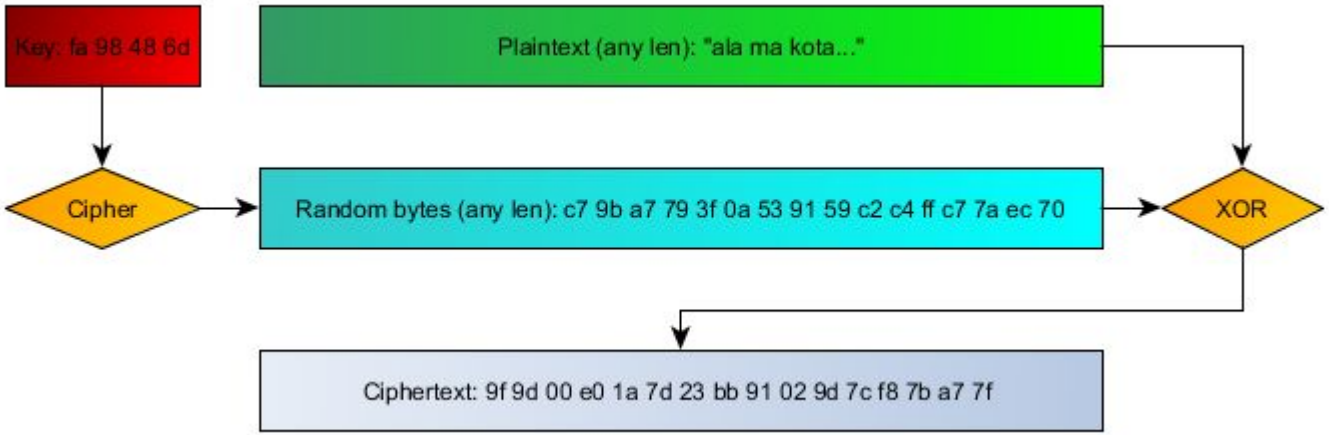
Block Ciphers

Block ciphers: theory

- Block ciphers vs stream ciphers
- Block encryption functions
- More theory

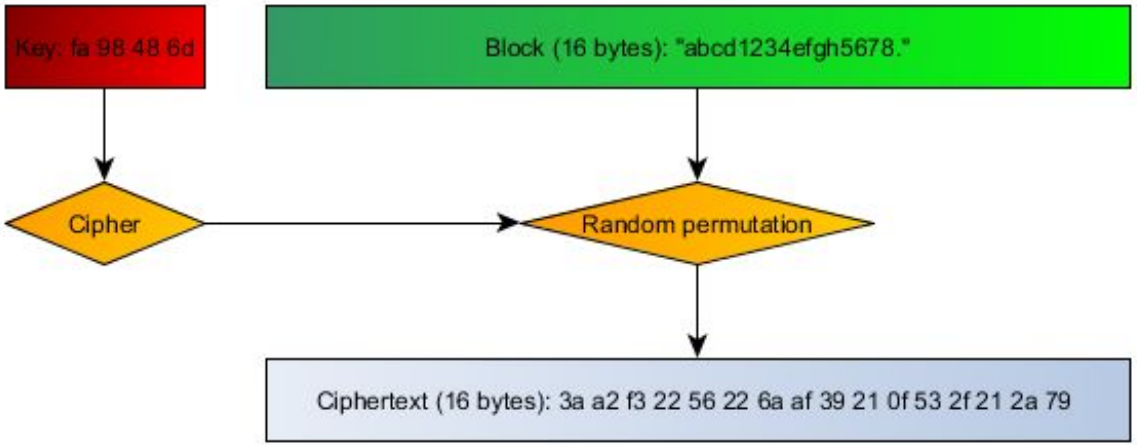
Stream cipher (simplified)

- Examples: RC4 (!), Salsa20, ChaCha, Spritz, VMPC (:P)
- "plaintext digits are encrypted with corresponding digits of the keystream, to give digits of ciphertext stream"



Block cipher (simplified)

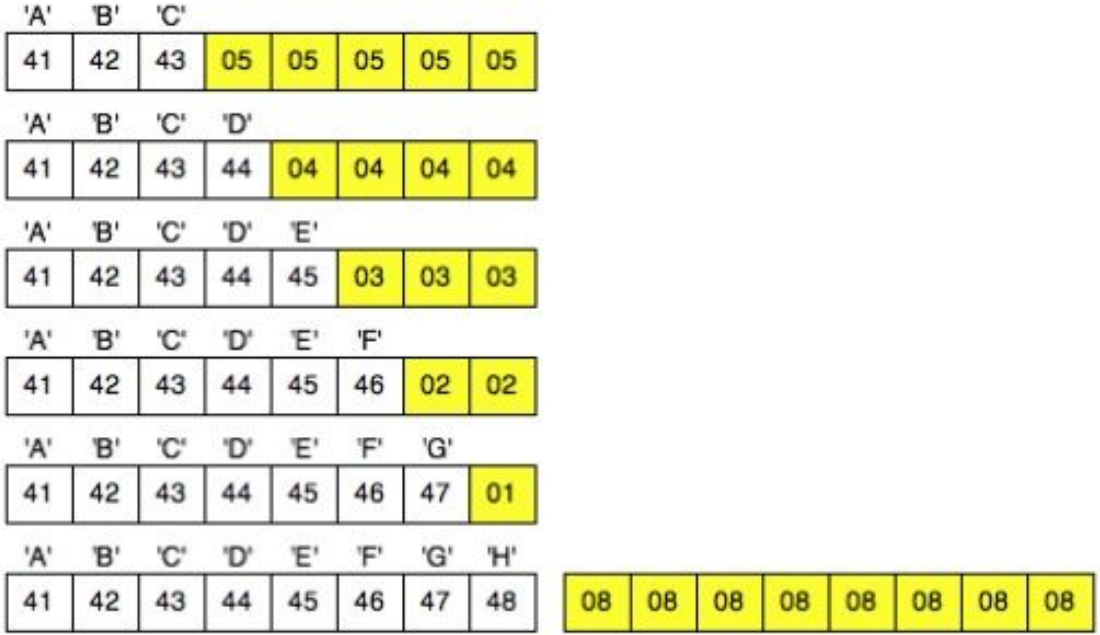
- Examples: [3]DES (obsolete), AES (!), Blowfish
- "algorithm operating on fixed-length groups of bits (blocks), with transformation specified by symmetric key"



PKCS#7 padding scheme

- Plaintext length must be multiple of block length
- What to do when it isn't?
- Padding schemes
- PKCS#7 padding scheme

PKCS#7 Valid Padding

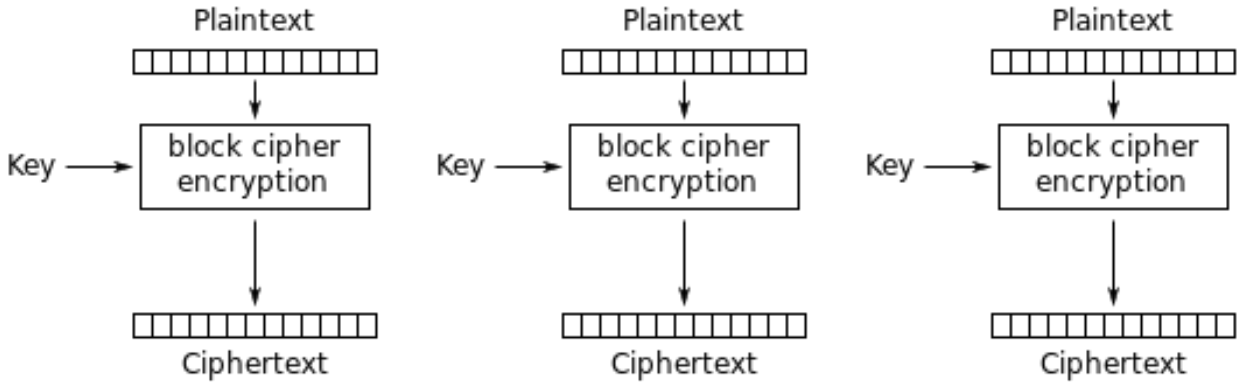


Cipher modes: ECB, CBC

OFB mode... CTR mode...

ECB Mode

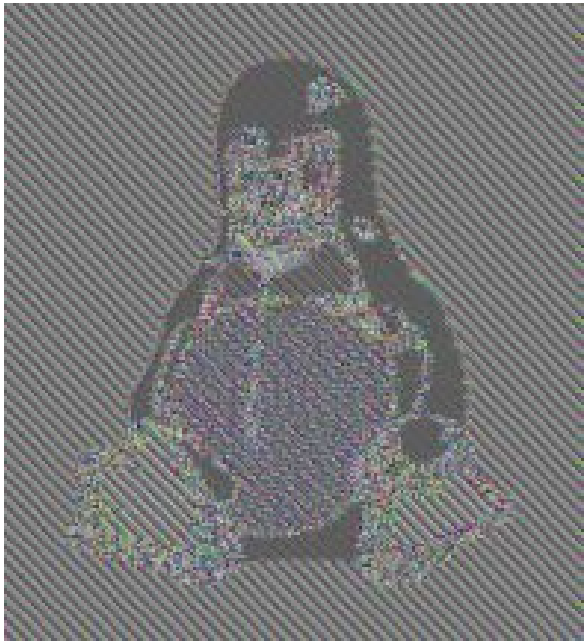
Simplest encryption mode possible

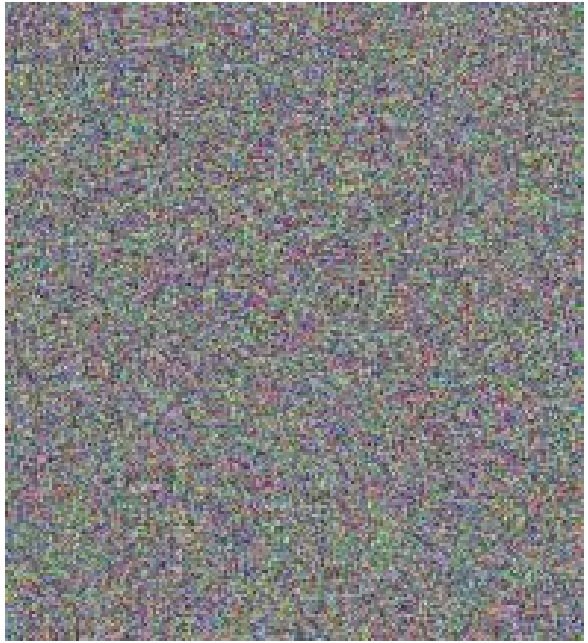


Electronic Codebook (ECB) mode encryption

ECB Mode

Obligatory penguin image

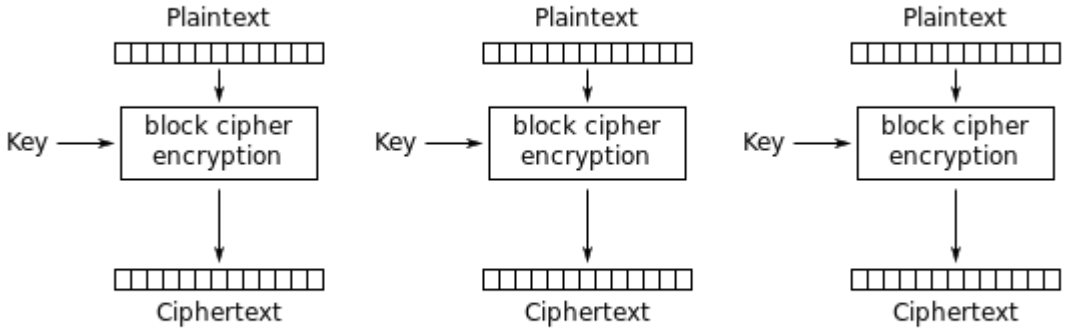




ECB mode attacks

https://uw2017.p4.team/ecb

ECB Mode Attack: Copy&Paste



Electronic Codebook (ECB) mode encryption

```
{'username': 'alamakota12345', 'is_admin': 'false'}
{'username': 'alamakota12345', 'is_admin': 'true'}
```

"Encryption is not authentication"

- What does it mean?
- Why?
- What is authentication?

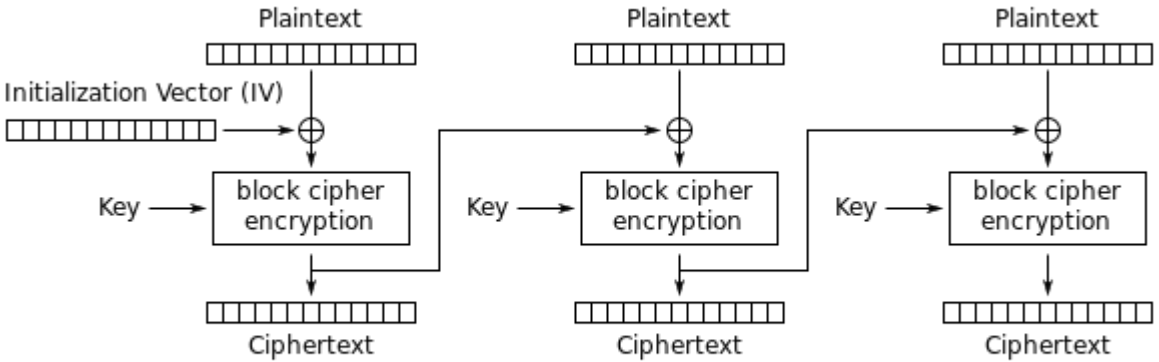
Off topic: so what is authentication?

- Hashes?
- Md5? Sha1? Sha256?
- Nope (why?)
- Message **Authentication** Codes
- HMAC construction

$$HMAC(K, m) = H\Big((K' \oplus opad) \mid\mid H\big((K' \oplus ipad) \mid\mid m\big)\Big)$$

CBC Mode

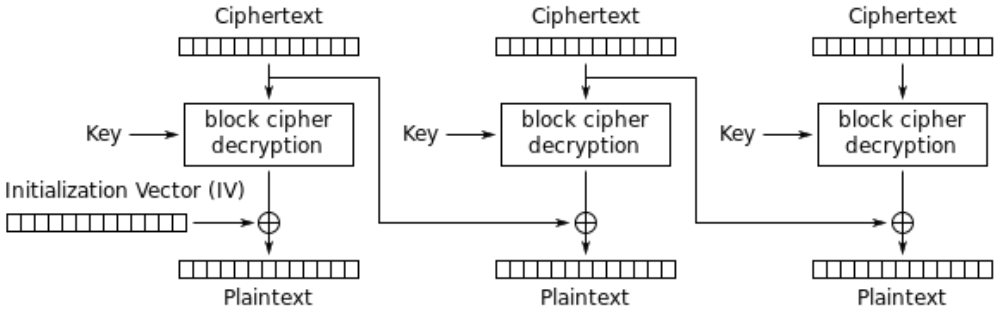
Cipher Block Chaining



Cipher Block Chaining (CBC) mode encryption

CBC mode attacks (byte flipping)

- Encryption is not authentication... again



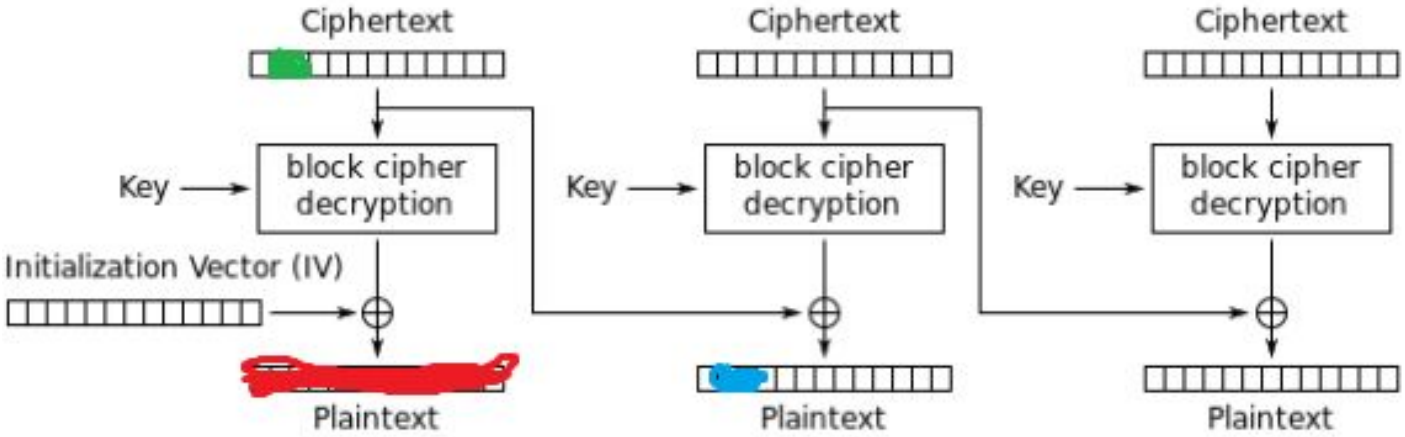
Cipher Block Chaining (CBC) mode decryption

- What if we can tamper with ciphertext?
  - What can we do with it?

CBC mode attack: ?

https://uw2017.p4.team/cbc

CBC Mode Attack: Byte Flipping



Cipher Block Chaining (CBC) mode decryption

```
{'username': 'alamakota12345', 'anything': 'true'}
{'username': 'f(3&3€Nf#;c]!ó', 'isadmin': 'true'}
```

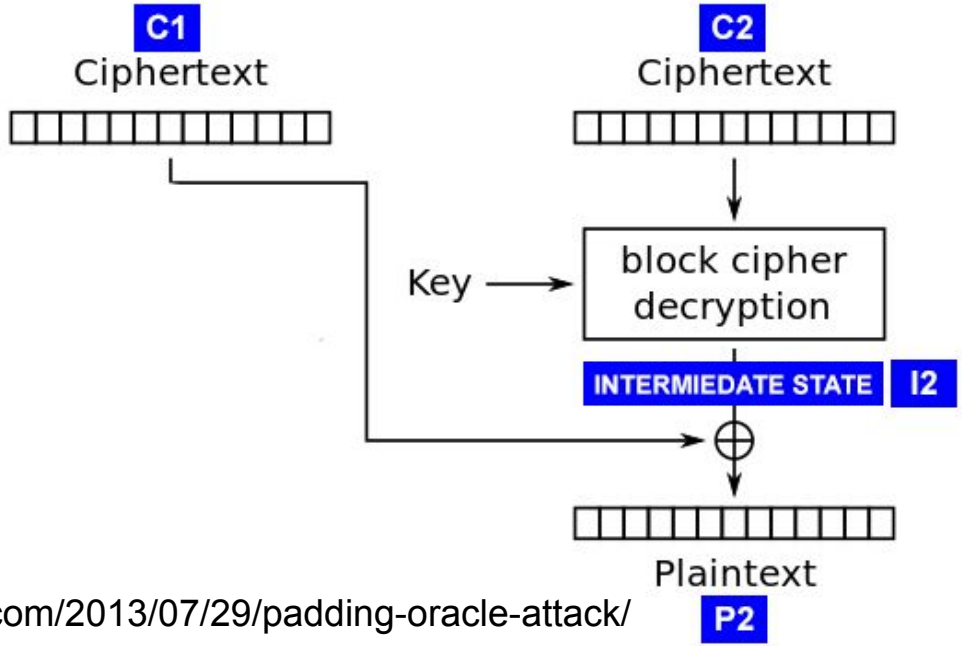
CBC Mode Attack: ?

```
def process_message(ciphertext):
    plaintext = decrypt_message(ciphertext)
    if plaintext == 'admin':
        return 'you are an admin'
    else:
        return 'you\'re not an admin'

def decrypt_message(ciphertext):
    if not padding_ok(ciphertext):
        raise new Exception('Invalid padding')
    return aes_decrypt(ciphertext)
```

Is something wrong with this code?

CBC Mode Attack: Padding oracle



http://robertheaton.com/2013/07/29/padding-oracle-attack/

I2 = C1 ^ P2
P2 = C1 ^ I2

P2[15] == 1?
I2[15] = ? C1[15] = ?

P2[14] == P2[15] == 1?
I2[14] = ? C1[14] = ?

Block ciphers: crypto building blocks

- Block ciphers => stream ciphers (CTR, OFB)
- Block ciphers => cryptographic hash function (1WCF)
- Block ciphers => CSPRNGs
- Block ciphers => PRP
- Block ciphers => MAC
- Block ciphers => AE (CCM, GCM, OCM...)

Block cipher design

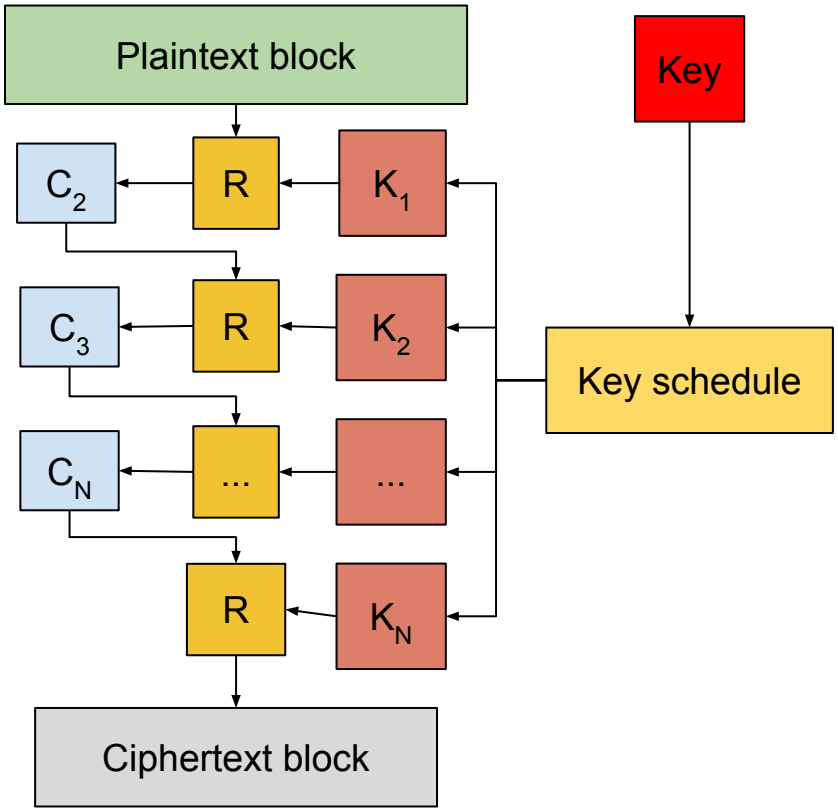
- Iterated block ciphers
  - Feistel ciphers
- Substitution-permutation ciphers

Attacks

- Slide attack
- Square attack

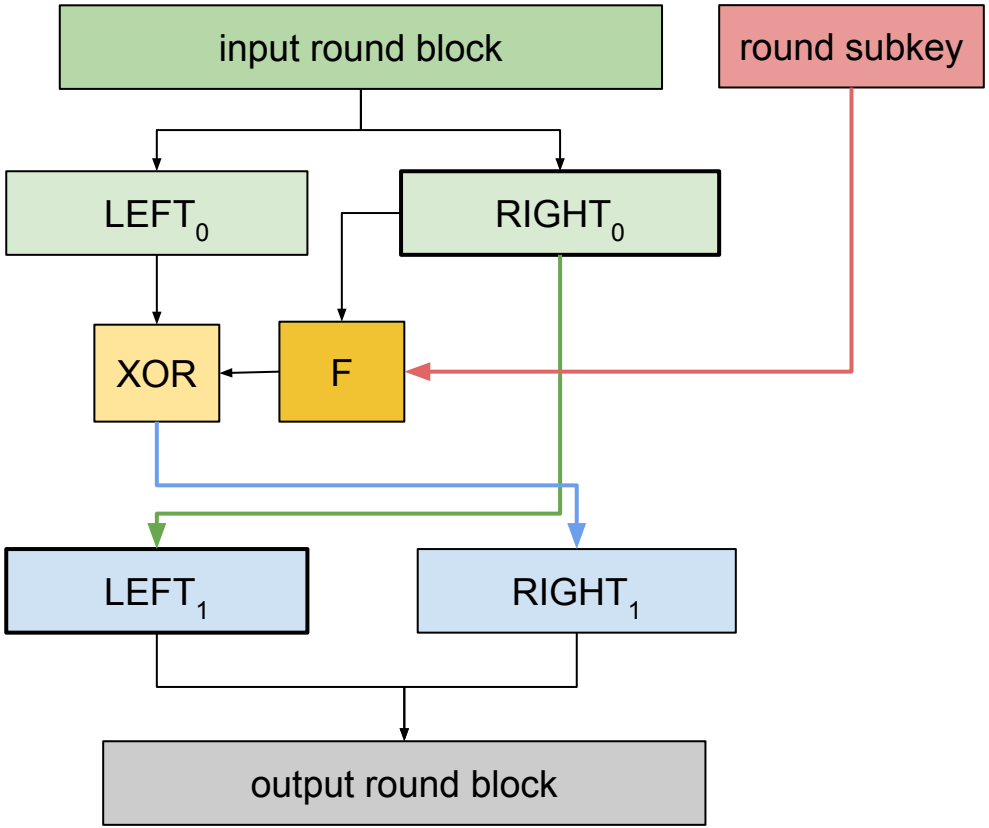
Iterated block ciphers

- Invertible round function: R
- Key schedule: K -> K_1,K_2,...,K_N
- C_{i+1}= R(K_i, C_i)
- P=C_1, C = C_{N+1}



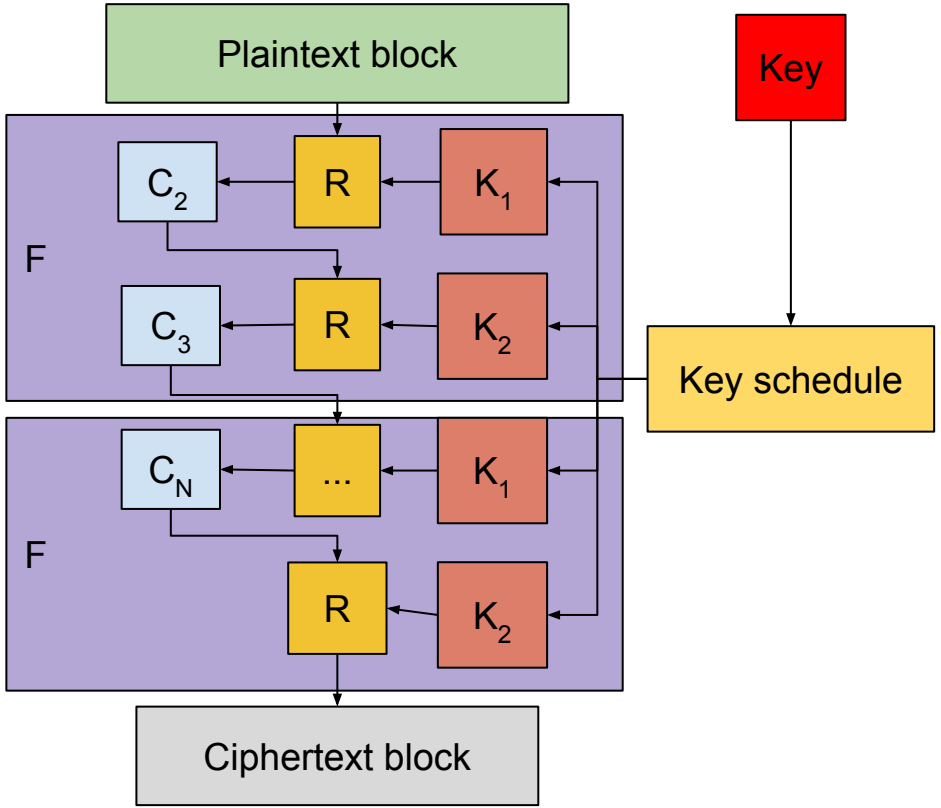
Feistel Ciphers

- Core function: F (not needed to be invertible)
- $LEFT_1 = RIGHT_0$

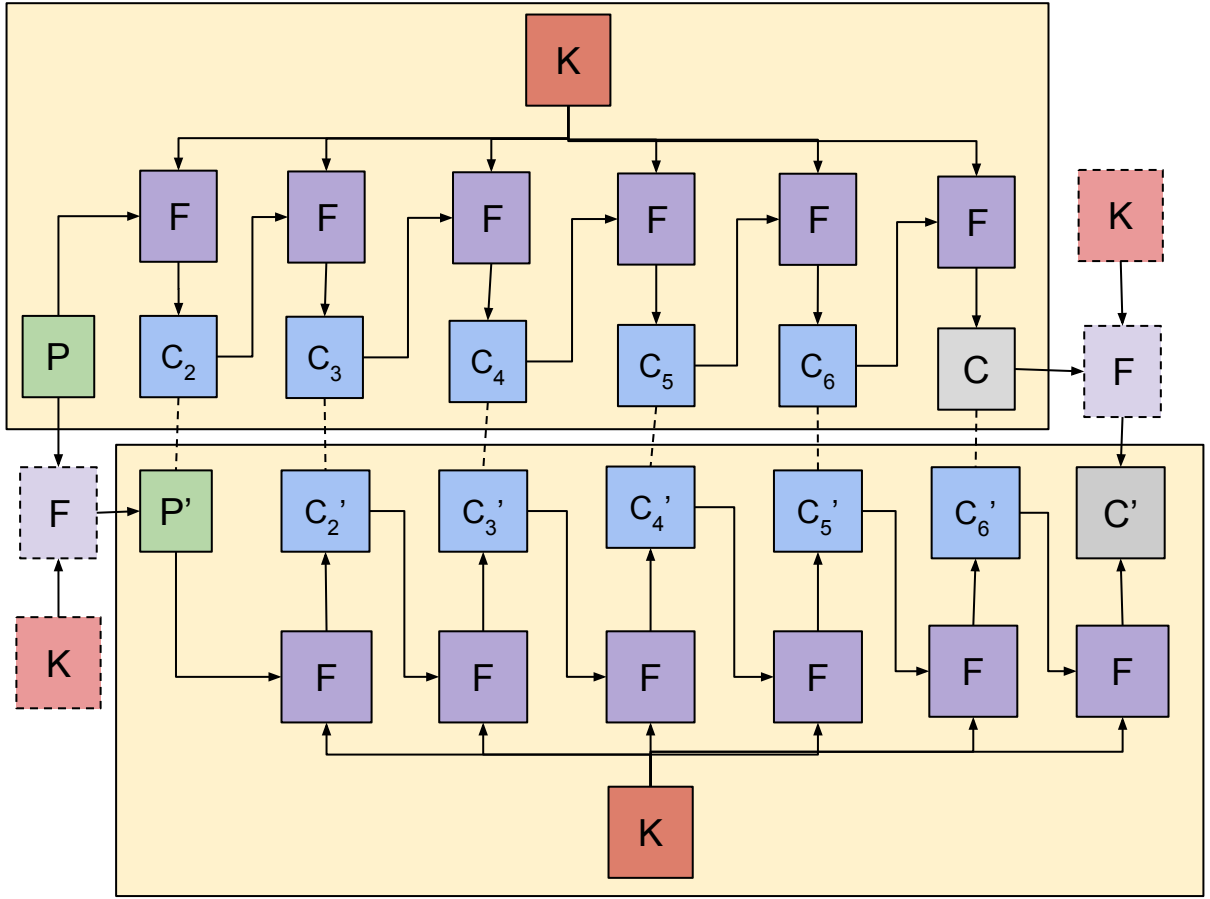


Slide attack

- Key schedule: periodic key
- Periodic part (F) vulnerable to known-plaintext attack
- N bit block: $2^{N/2}$ plaintext - ciphertext pairs

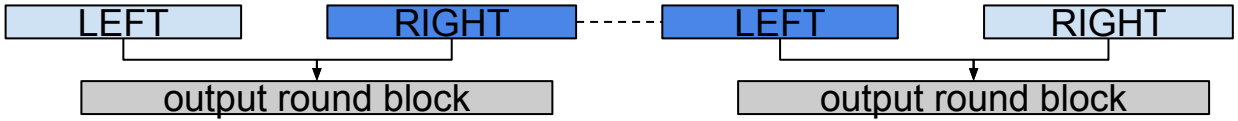


- (P, C),
  (P’,C’)
- P’ = F(K, P)
- C’ = F(K, P’)
- Time: 2^N !

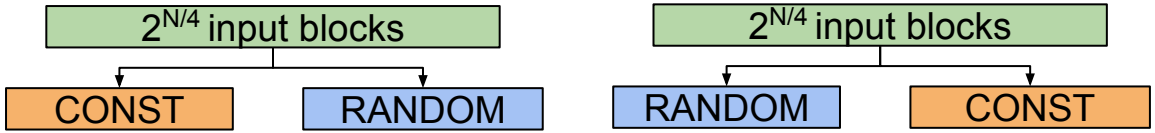


Slide attack on Feistel cipher

- Pair identification: RIGHT(C) = LEFT(C')

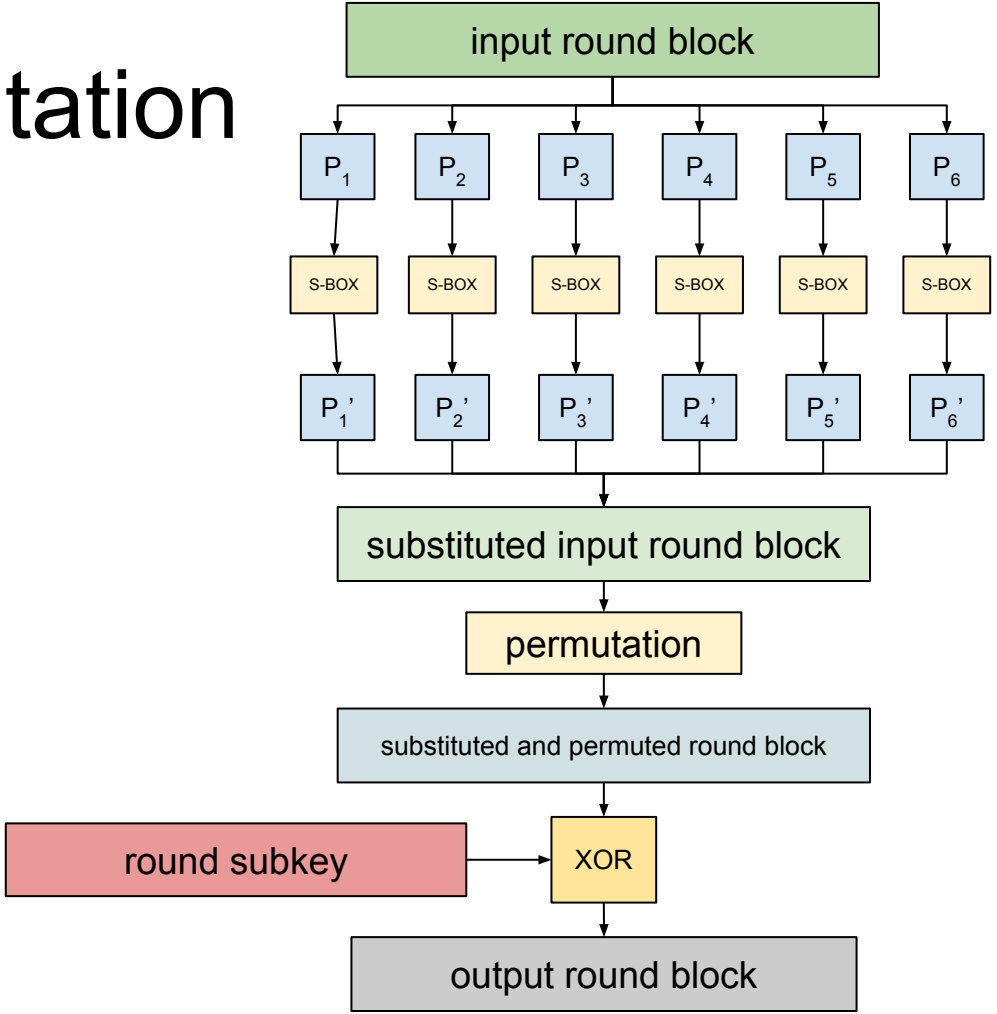


- Chosen plaintext: $2^{N/4}$: $P_i = b_i|a$, $2^{N/4}$: $P_i' = a|b_i$



Substitution-permutation ciphers

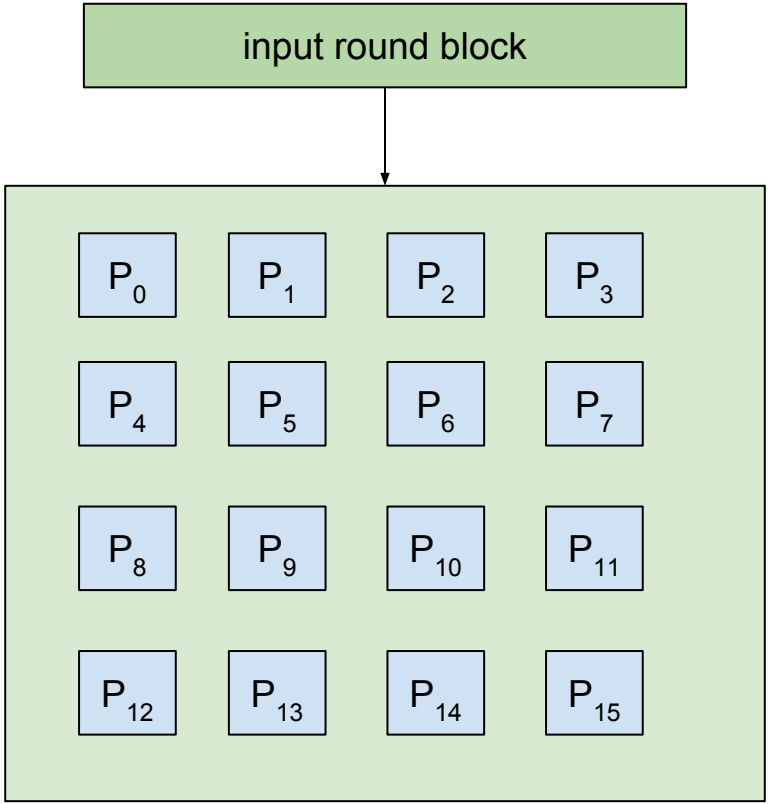
- S-Box
- P-Box
- Combine with key
- Confusion and diffusion



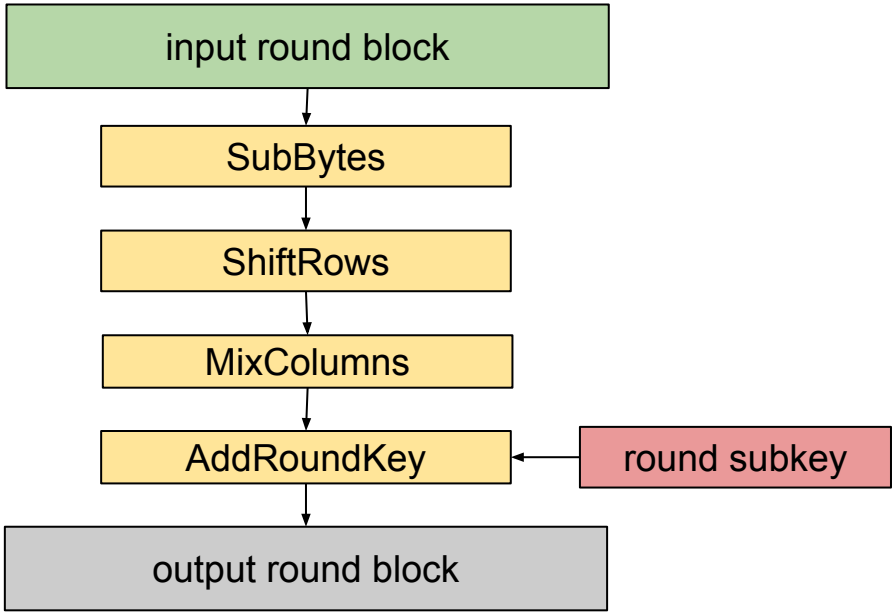
Square attacks

- Integral cryptanalysis
- AES (reduced to 4 rounds (from 10))
- Chosen plaintext

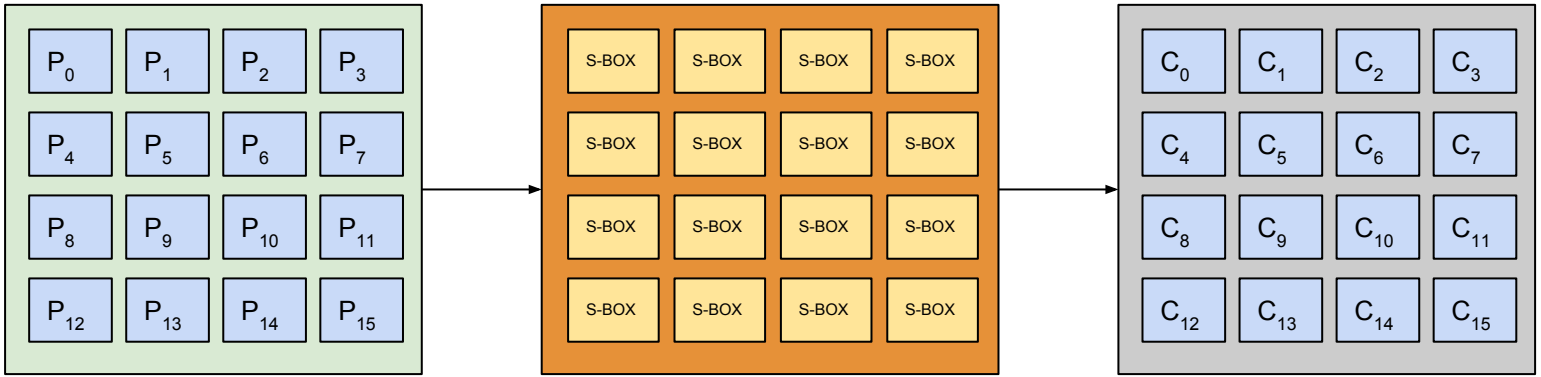
Square


input round block
P_0
P_1
P_2
P_3
P_4
P_5
P_6
P_7
P_8
P_9
P_{10}
P_{11}
P_{12}
P_{13}
P_{14}
P_{15}

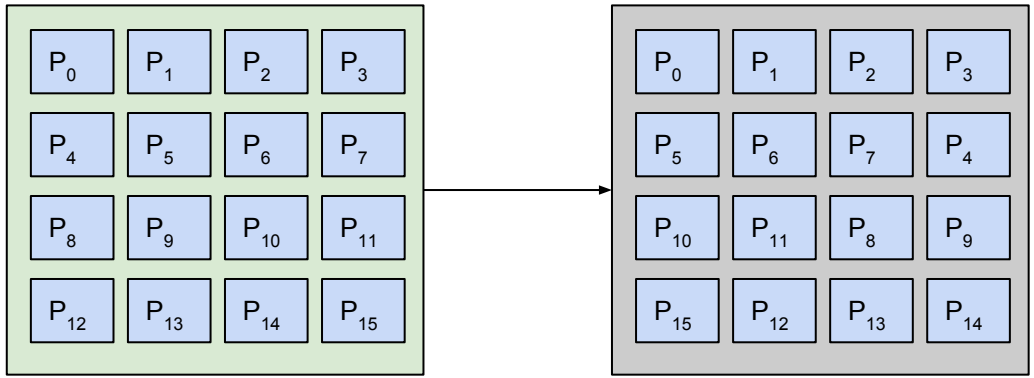
AES


input round block
SubBytes
ShiftRows
MixColumns
AddRoundKey
round subkey
output round block

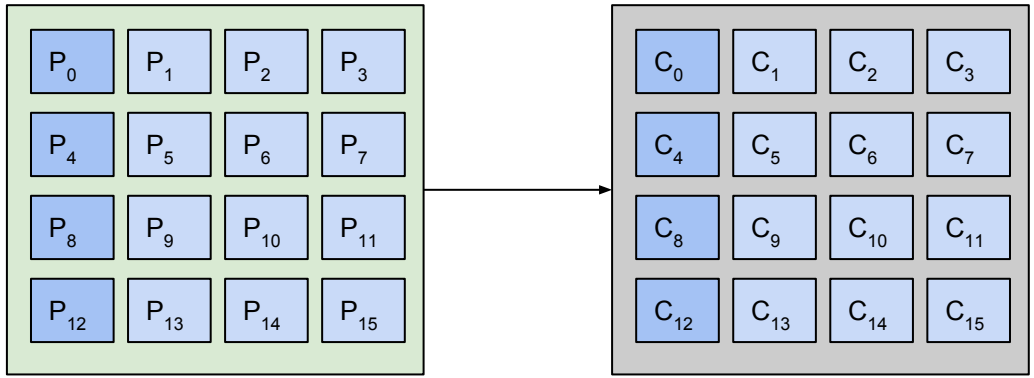
SubBytes


P0 P1 P2 P3
P4 P5 P6 P7
P8 P9 P10 P11
P12 P13 P14 P15
S-BOX S-BOX S-BOX S-BOX
S-BOX S-BOX S-BOX S-BOX
S-BOX S-BOX S-BOX S-BOX
S-BOX S-BOX S-BOX S-BOX
C0 C1 C2 C3
C4 C5 C6 C7
C8 C9 C10 C11
C12 C13 C14 C15

ShiftRows


P0 P1 P2 P3
P4 P5 P6 P7
P8 P9 P10 P11
P12 P13 P14 P15
P0 P1 P2 P3
P5 P6 P7 P4
P10 P11 P8 P9
P15 P12 P13 P14

MixColumns



$GF(2^8)$, $p(x) = P_{12}x^3+P_8x^2+P_4x+P_0$, $a(x) = 3x^3+x^2+x+2$, $p(x) * a(x)$, mod x^4+1

$C_0 = 2P_0 \oplus 3P_4 \oplus P_8 \oplus P_{12}$

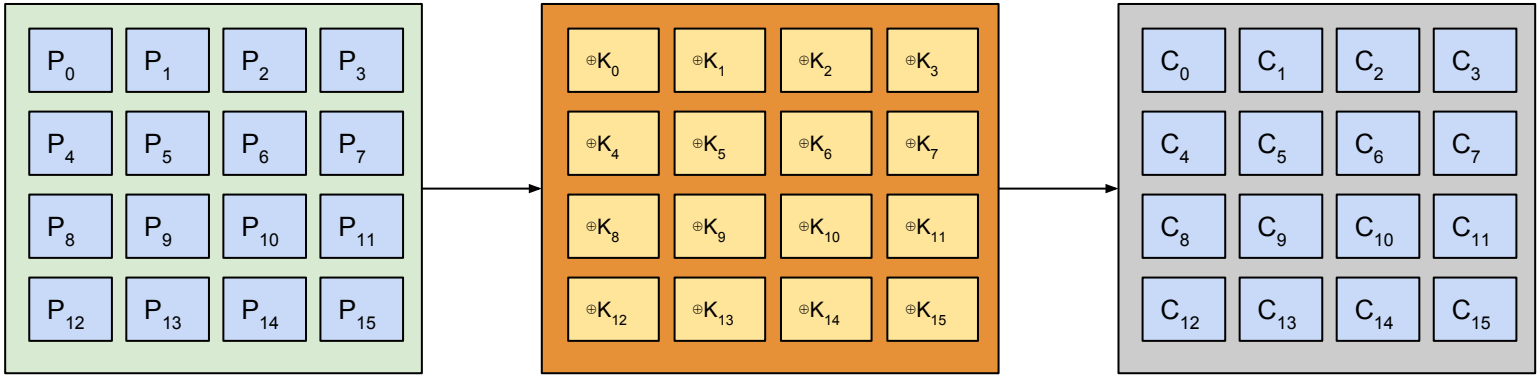
$C_4 = 2P_4 \oplus 3P_8 \oplus P_{12} \oplus P_0$

$C_8 = 2P_8 \oplus 3P_{12} \oplus P_0 \oplus P_4$

$C_{12} = 2P_{12} \oplus 3P_0 \oplus P_4 \oplus P_3$

Not present in last round

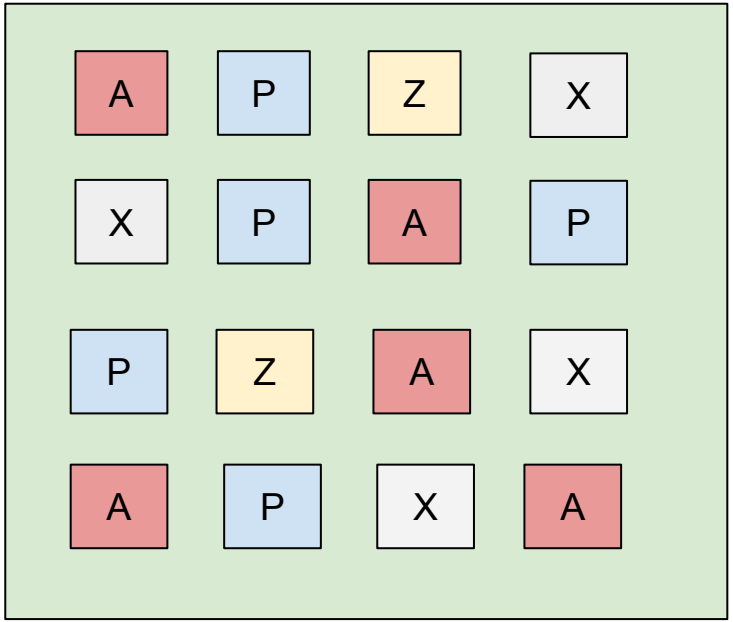
AddRoundKey



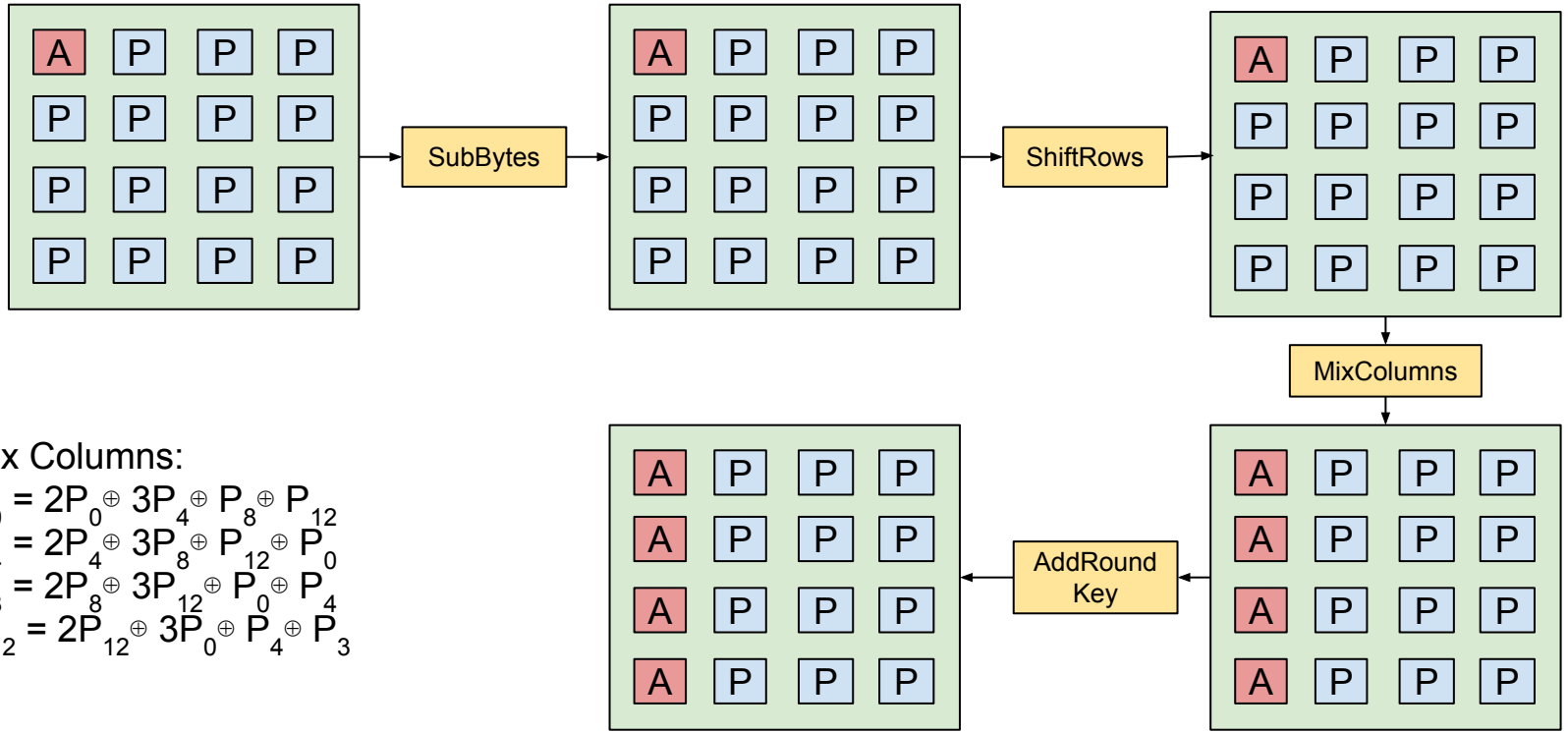
Active and passive byte states

- Set of plaintext
- Passive state: for each two plaintext the same square element
- Active state: for each two plaintext different square element
- Zero state: ⊕ elements from all plaintext = 0
  - 0⊕1⊕...⊕255 = 0

- Example:
  - 256 plaintext, first byte: 0,1,2,..,255, other bytes: 0
  - Before first round: top left element is active, other elements passive



Round 1



Mix Columns:

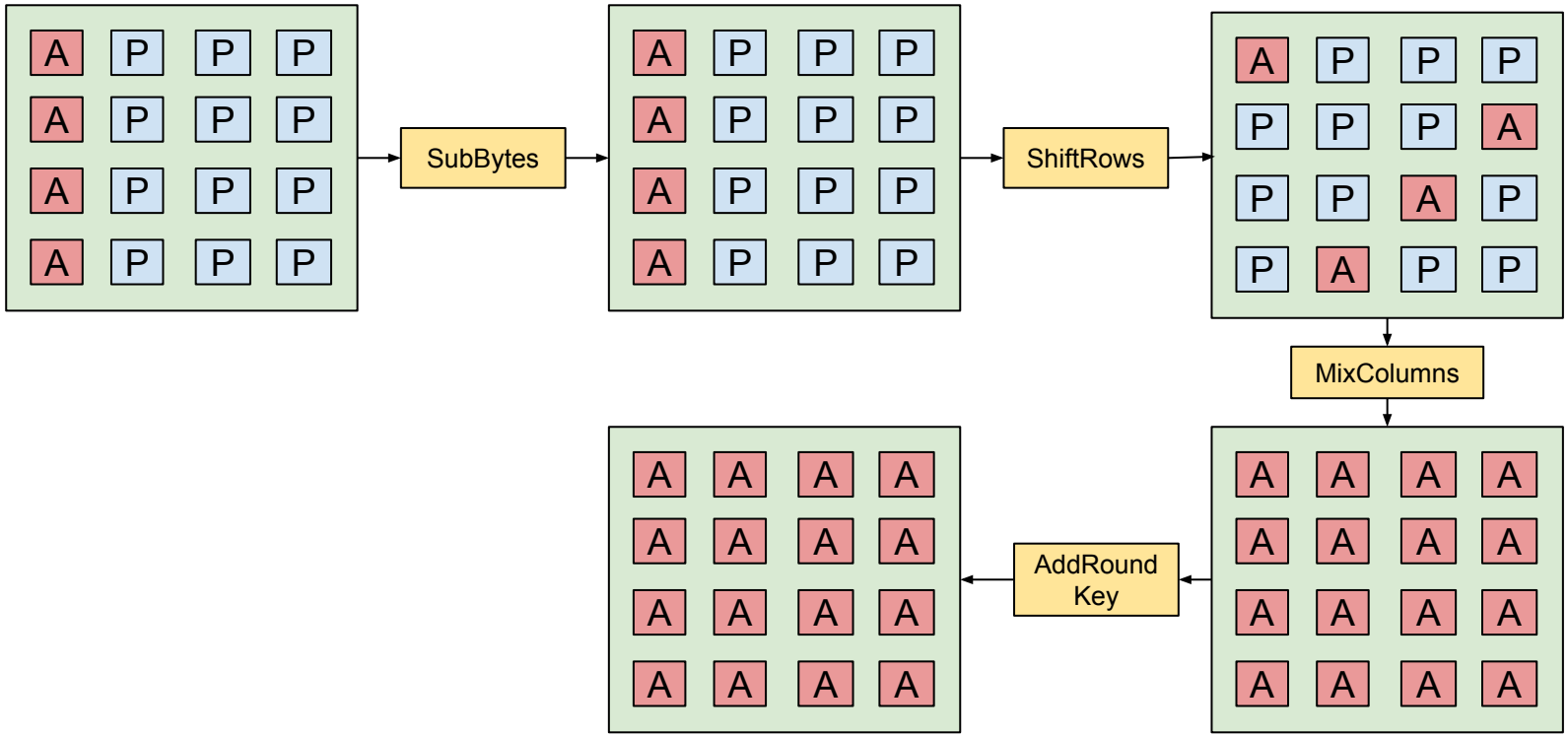
$C_0 = 2P_0 \oplus 3P_4 \oplus P_8 \oplus P_{12}$

$C_4 = 2P_4 \oplus 3P_8 \oplus P_{12} \oplus P_0$

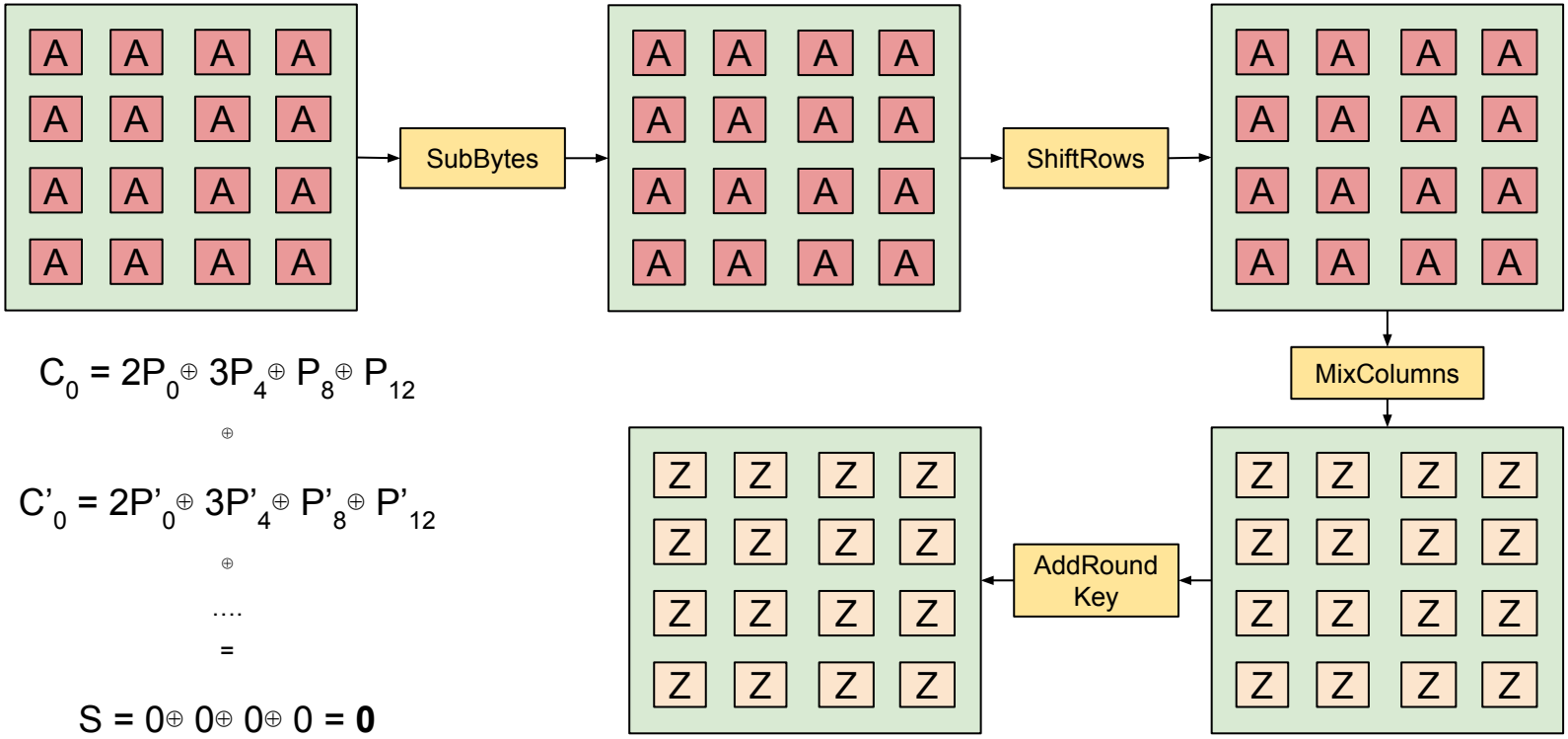
$C_8 = 2P_8 \oplus 3P_{12} \oplus P_0 \oplus P_4$

$C_{12} = 2P_{12} \oplus 3P_0 \oplus P_4 \oplus P_3$

Round 2


A P P P
A P P P
A P P P
A P P P
SubBytes
A P P P
A P P P
A P P P
A P P P
ShiftRows
A P P P
P P P A
P P A P
P A P P
MixColumns
A A A A
A A A A
A A A A
A A A A
AddRound Key
A A A A
A A A A
A A A A
A A A A

Round 3



$C_0 = 2P_0 \oplus 3P_4 \oplus P_8 \oplus P_{12}$

$\oplus$

$C'_0 = 2P'_0 \oplus 3P'_4 \oplus P'_8 \oplus P'_{12}$

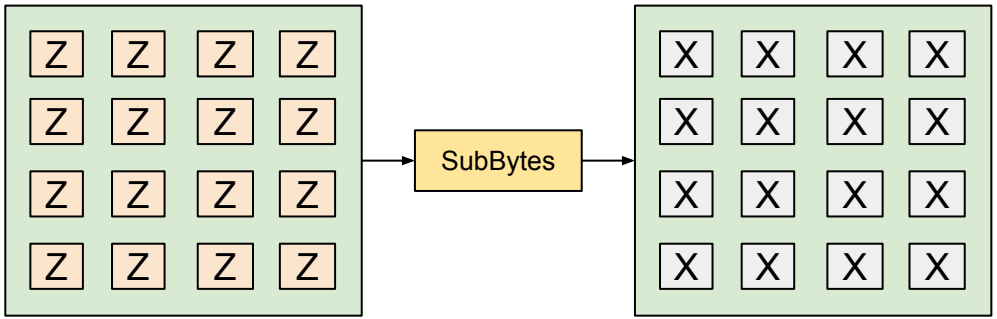
$\oplus$

....

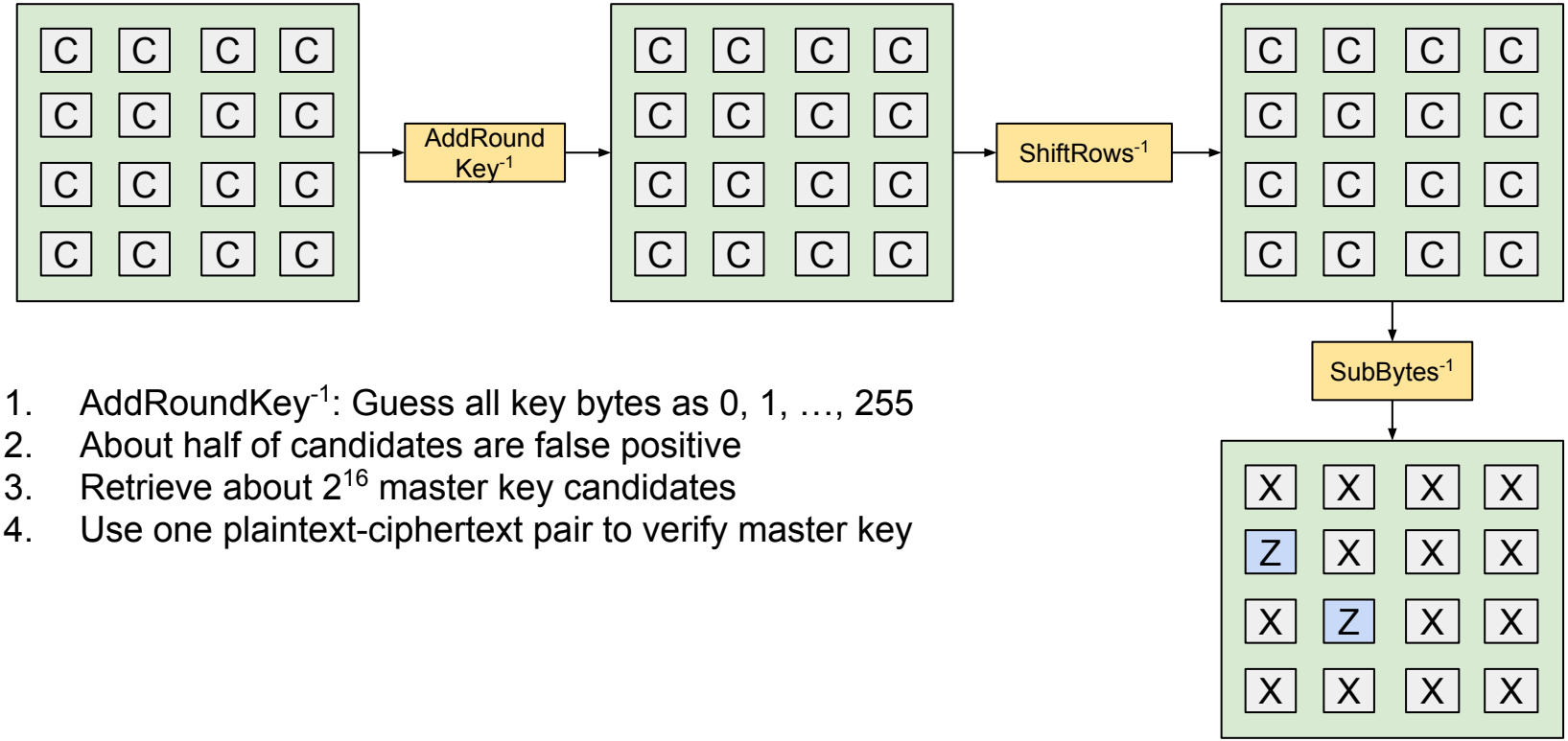
=

$S = 0 \oplus 0 \oplus 0 \oplus 0 = \mathbf{0}$

Round 4



Key byte guessing



1. AddRoundKey^{-1}: Guess all key bytes as 0, 1, …, 255
2. About half of candidates are false positive
3. Retrieve about 2^{16} master key candidates
4. Use one plaintext-ciphertext pair to verify master key

Bibliography

Joan Daemen and Vincent Rijmen, "AES Proposal: Rijndael"

Alex Biryukov and David Wagner, "Advanced Slide Attacks"

Bruce Schneier, "Applied Cryptography"