Block ciphers

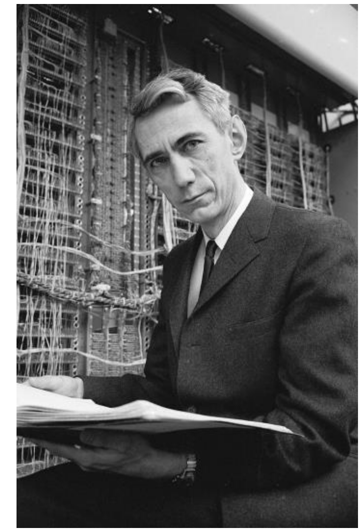
BMEVITMAV52

Information and Network Security

feher.gabor@tmit.bme.hu

History of cryptography
Modern cryptography

- Beginning with 1949
  - Claude Shannon:
    Communication Theory of Secrecy Systems
    - Solid theoretical basis for cryptography and for cryptanalysis
  - No more alphabets, but ‘bits’ and ‘bytes’



- 1975 DES – Data Encryption Standard
- 1976 Diffie-Hellman key exchange
- 1977 RSA

Block ciphers

- Definition
  - Function that transfers n-bit plaintext block to n-bit ciphertext block (n is the blocklength)
  - The function is parameterized by a k-bit key
  - One-to-one mapping (invertible)

- Symmetric key block ciphers
  - E(P,K)=C, D(C,K)=P
- Asymmetric key block ciphers
  - $E(P,K_1)=C$, $D(C,K_2)=P$

Well known symmetric block ciphers

- 1976: USA standard cipher: DES (Data Encryption Standard)
  - 64 bit block length, 56 bit key length
  - As of today it is insecure and slow
- 3DES: 3x DES cipher in a row
  - 2x not enough, 2 keys are already enough
  - 64 bit block length, 112 bit key length
  - Satisfactory security, but slow
- 2001: AES, the new cipher standard (Advanced Encryption Standard)
  - 128 bit block length, 128-192-256 bit key length
  - State of the art security and speed
- Other, less known ciphers
  - IDEA, Twofish, Blowfish, RC5

Requirements to modern ciphers

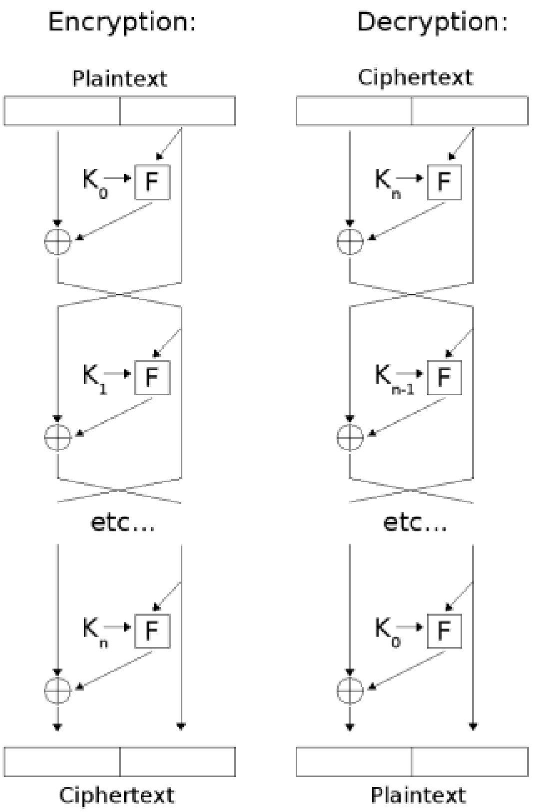
- Avalanche effect
  - Changing one bit in the input changes half of the output bits
- Completeness
  - Each ciphertext bit is a complex function of all the bits in the plaintext
- Efficiency
  - Using the same algorithm the plaintext and the ciphertext should be calculated fast

Product cipher

- Cloude Shannon (1949)
  - "confusion and diffusion"
    - Complex relationship between key and ciphertext
    - Redundancy of plaintext is dissipated
- Idea:
  - Build an encryption function from several simple functions (non satisfactory in alone)
    - Simple operations: transposition, translation, linear transformation, substitutions…
  - The result cipher should be more secure than the individual components

Feistel cipher

- Horst Feistel (IBM)
- Iterated product cipher
  - t-bit long blocks: L_0 and R_0
  - After r round, makes (R_r,L_r) from (L_0,R_0)
  - Round: $L_i=R_{i-1}$; $R_i=L_{i-1}\otimes f(R_{i-1},K_i)$
    - K_i is derived from the K key
    - $R_i=R_{i-2} \otimes f(R_{i-1},K_i)$
  - Decryption goes the same way, but the keys are used in reverse order. f should not need to be invertible!
- Blocks (f)
  - Permutation box (P box)
  - Substitution box (S box)



Feistel Cipher

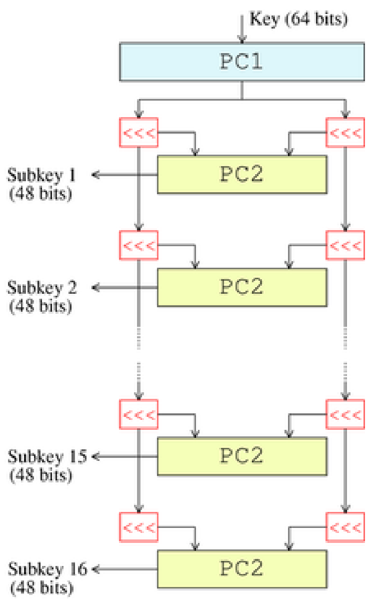
Data Encryption Standard (DES)

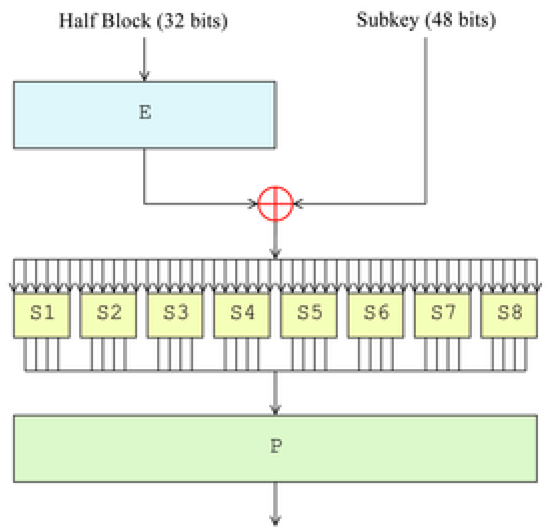
- History
  - In 1970s there was a need for a standard cipher
  - National Institute of Standards and Technology (NIST) issued a public request for standard cipher proposal
  - In 1977 January, after long debates the standard was accepted: modified Lucifer (Feistel) cipher

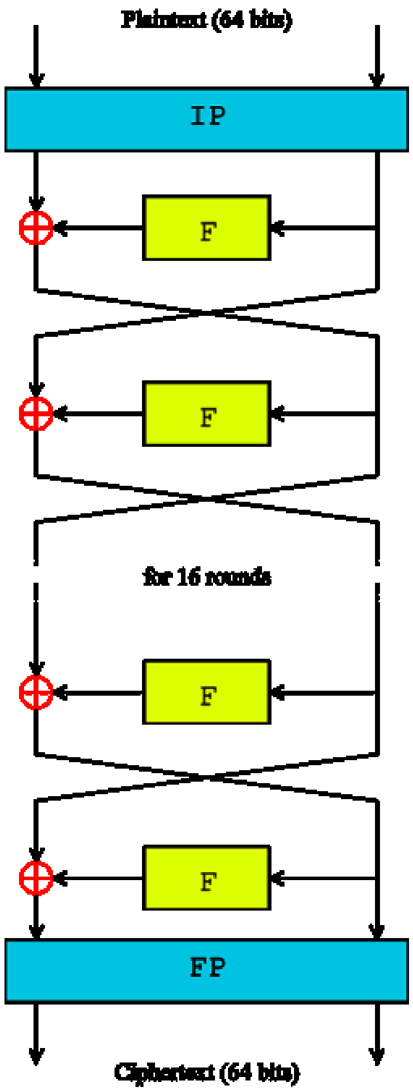
- Feistel cipher
  - 64 bit blocks
  - 56 (64) bit key (with 8 bit parity) transformed into 16 different 48 bit subkeys
  - 16 rounds, called stages
  - $f(R_{i-1},K_i) = P(S(E(R_{i-1}) \otimes K_i))$
    - P: Permutation (fixed), S: Substitution (non linar transformation), E: Expansion (fixed)
  - Before the first round, initial permutation (IP). After the last run IP inverse (FP) is performed

DES rounds

- Feistel (F) function







DES properties

- Complementation property`
  - If $y = E_K(x)$ then $y^* = E_{K^*}(x^*)$
  - Testing one key tells the result of the complement key as well
- Weak and semi-weak keys
  - Palindrome subkeys: $K_1=K_{16}$, $K_2=K_{15}$, …
  - Definition
    - Weak key K: $E_K(E_K(x)) = x$
      - also means that $(E_K = D_K)$
      - DES has 4 weak keys
    - Semi-weak key pair: K_1,K_2: $E_{K1}(E_{K2}(x)) = x$
      - also means that $(E_{K2} = D_{K1})$
      - DES has 6 semi-weak key pairs

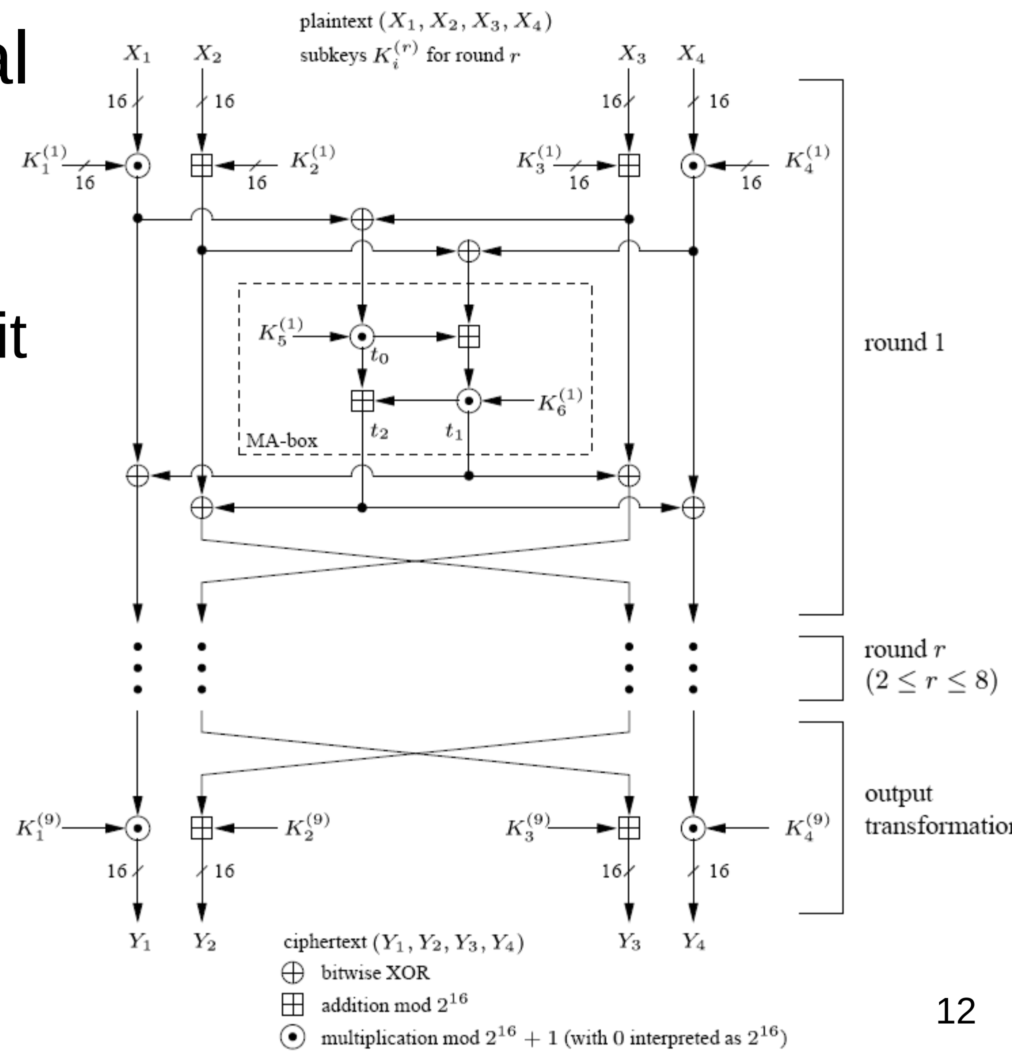
Brute force attack

- 56 bit security
  - DES can be break using brute force approach (testing all the keys)
    - 1997 DES Challenge: 96 days
    - 1998 DES Challenge II-1: 41 days
    - 1998 DES Challenge II-2: 56 hours ($250.000 cost)
    - 1999 DES Challenge III: 22 hours 15 minutes
  - In 1970s software solutions need years to break it
  - Today it is faster and we also have hardware implementations
  - “Chinese lottery” theory

- 56 bit security is not sufficient today!
- Besides DES was too slow

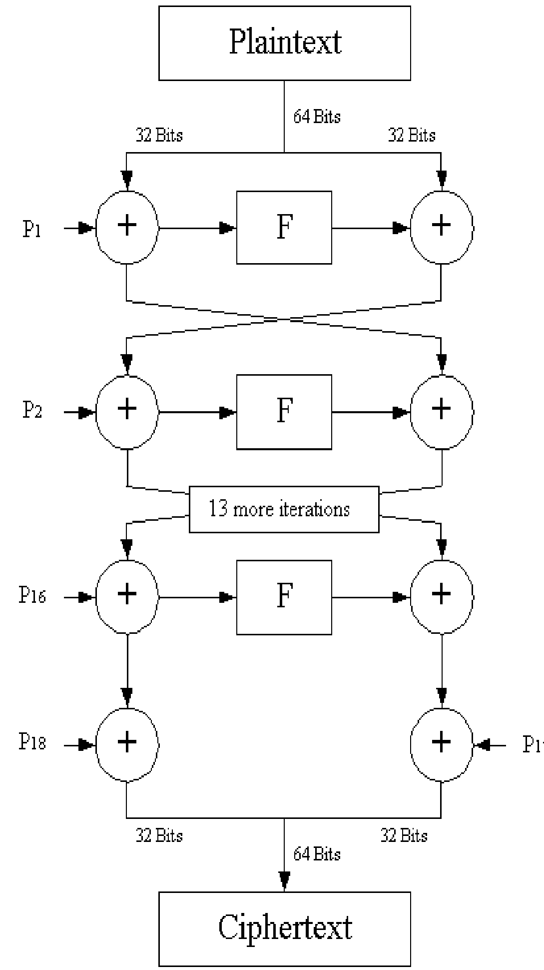
IDEA

- IDEA – International Data Encryption Algorithm
  - 64 bit blocks, 128 bit key
- Longer keys



Blowfish

- Blowfish – 1993 Bruce Schneier
  – Fast, compact, simple, secure
  – 64 bit blocks, 32-448 bit keys
- Feistel architecture (16 rounds)
- Large number of subkeys (better with infrequent key change) -> 4168 bytes



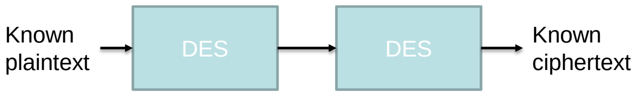
Make the key longer

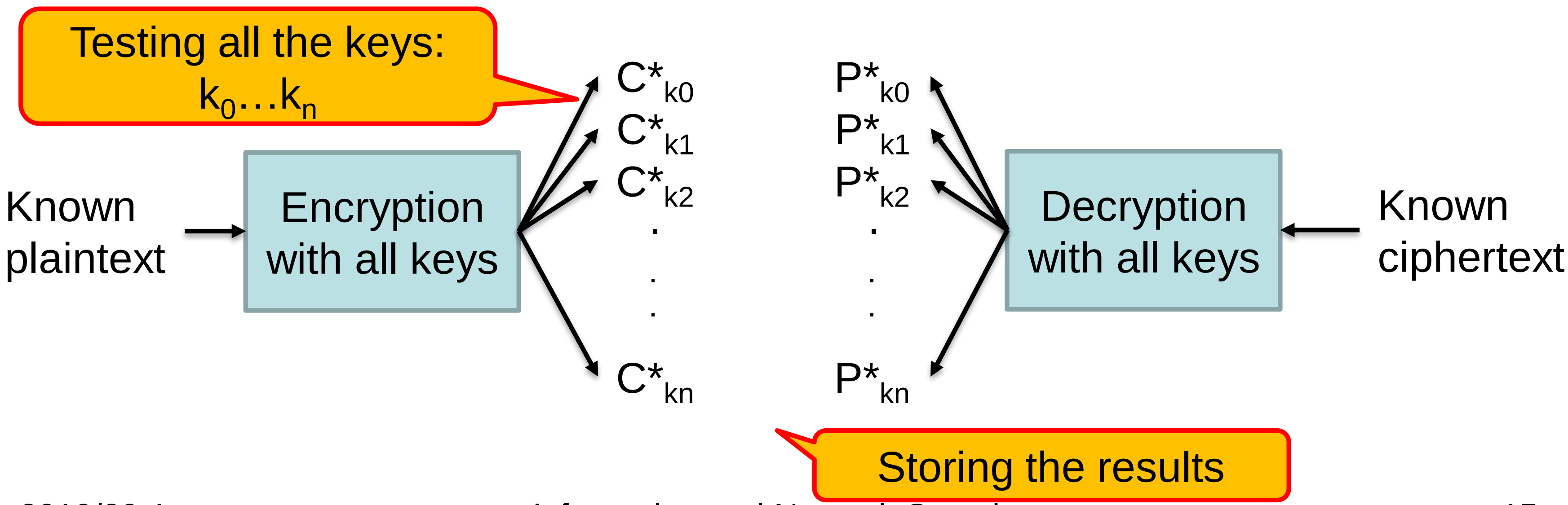
- Make the key longer
  - Using multiple encryptions with different keys

- Double encryption
  - $C = E_{K2}(E_{K1}(P))$
  - $P = D_{K1}(D_{K2}(C))$
  - If block algorithm is not a *group* - $C = E_{K2}(E_{K1}(P)) = E_{K3}(P)$ - then it would extend the keyspace. But later it turned out that using known plaintext attack (meet in the middle attack) it is only 2^{n+1} instead of 2^{2n}
  - Meet in the middle: E_{K1} (P) ? $D_{K2}(C)$

Meet in the Middle

- Meet in the middle attack
  - Known plaintext and ciphertext
  - Searching for the password
  - Assuming 2 cipher blocks





Meet in the middle (cont.)

- Testing all the keys, storing the results
  - Encryption: 2^x tests (x bit key length for the 1st cipher)
  - Decryption: 2^y tests (y bit key length for the 2nd cipher)
  - Testing and storing $2^x + 2^y$ keys altogether

- Matching
  - One of the encryption result using first key will match to the one of the decryption result using the second key
    - $C^*_{ka} = P^*_{kb}$

  This a,b is the key for the combined block encryption

- Complexity
  - Instead of testing 2^{x+y} keys, we tested $2^x + 2^y$ keys only. (+stored $2^x + 2^y$ keys)
  - 2DES: Instead of 2^{56+56} keys, it is just $2*2^{56}$ keys!

3DES

- Triple encryption – e.g. 3DES
    - $C = E_{K1}(D_{K2}(E_{K1}(P)))$
    - $P = D_{K1}(E_{K2}(D_{K1}(C)))$
  - – Doubles the key, but better then double encryption

- Triple encryption with independent keys
    - $C = E_{K1}(D_{K2}(E_{K3}(P)))$
    - $P = D_{K1}(E_{K2}(D_{K3}(C)))$
  - – Due to the meet in the middle attack it is not 2^{3n}, but a true 2^{2n} keyspace

3DES and Meet in the middle

- 3DES with 3 DES blocks
  - 2 groups: 1DES and 2DES -> 56 and 112 bit keys
  - Meet in the middle attack:
    - Instead of testing 2^{112+56} keys, it is just $2^{112} + 2^{56}$ keys

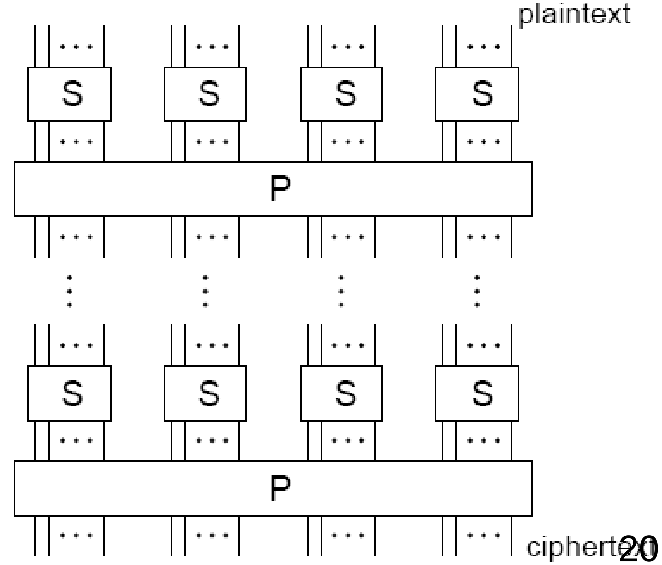
  - Effectively 3DES equals to a 112 bit key cipher

Need a new standard

- In 1997 NIST issued public request for a new cipher standard replacing 3DES
  - DES was subject to brute force attack
  - 3DES was too slow in software
  - Requirements:
    - 128 bit blocks
    - 128, 192, 256 bit keys
    - Speed is important
    - Run on embedded systems (limited resources)
- Among 15 candidates Rijndael was selected and became standard in 2001

Substitution-permutation network

- Product cipher example
- Iterated block cipher
  - Sequential repetition of a “round”
  - Each round has its own subkey (part of the key)
  - Invertible if the internal function in a round is a one-to-one mapping



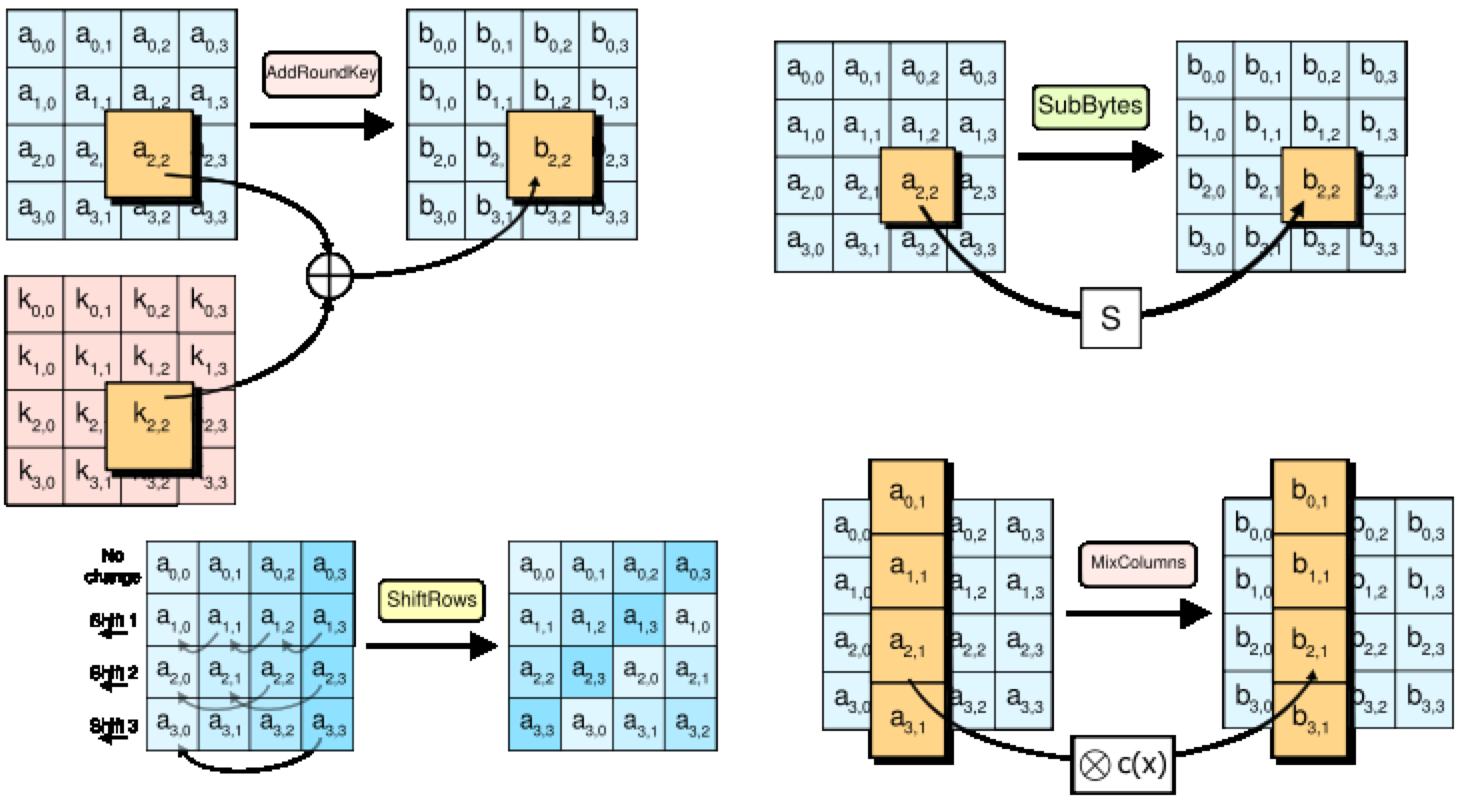
AES – Advanced Encryption Standard

- Joan Daemen and Vincent Rijmen: Belgian inventors
- Substitution-permutation network
- Works on 4x4 byte arrays called states
  - AddRoundKey — each byte of the state is combined with the round key; each round key is derived from the cipher key using a key schedule
  - SubBytes — a non-linear substitution step where each byte is replaced with another according to a lookup table
  - ShiftRows — a transposition step where each row of the state is shifted cyclically a certain number of steps
  - MixColumns — a mixing operation which operates on the columns of the state, combining the four bytes in each column using a linear transformation
    - AddRoundKey in the last round!
- It is also possible to transform stages into tables
  - 16 table lookups and 12 32 bit XOR operations, 4

- 128 bit keys: 10 rounds, 196 bit keys: 12 rounds and 256 bit keys: 14 rounds

AES stages

- Stages



Padding

- When the message is shorter than a block, padding should be used
  - Also good for hide the length of a message

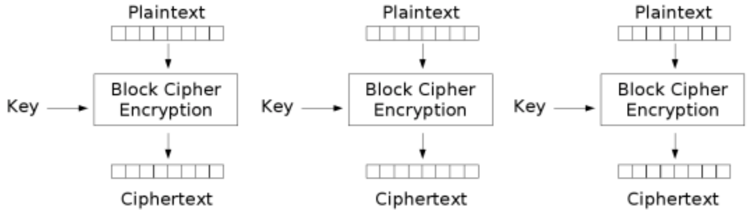
- Simple way:
  - Add 0 bytes to the end. Works for C style strings, but not for binary data
- Original DES method
  - One 1 bit followed by zeros. If message ends on a block border, then a whole padding block is added
- Last byte:
  - The last byte shows the length of the padding, the others are zero
- Random padding
  - The last byte shows the length of the padding, the others are random
- PKCS #5 (Public Key Cryptography Standards - Password-based Encryption Standard)
  - Padding with bytes showing the length of the padding

Block chaining

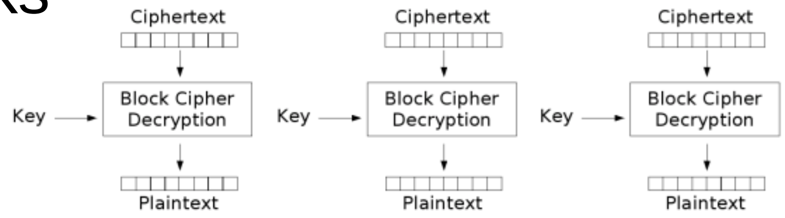
- Messages larger than a block should be encrypted block by block + block chaining
  - Modes of operation
- Modes of operation
  - Electronic Code Book (ECB)
  - Cipher-block Chaining (CBC)
  - Cipher feedback (CFB)
  - Output feedback (OFB)
  - Counter (CTR)

ECB – Electronic Codebook

- Properties
  - Same input – same output
  - Blocks are independent
    - Bit error affects the whole block, but no other blocks
    - Attack: replacing blocks



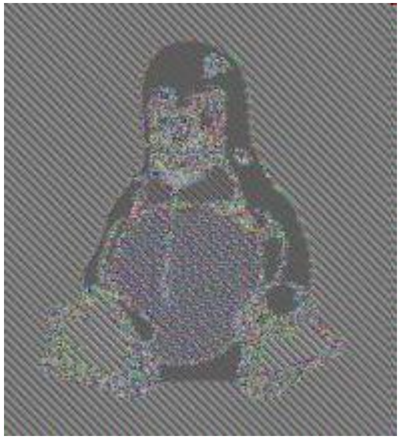
Electronic Codebook (ECB) mode encryption



Electronic Codebook (ECB) mode decryption

Insecurity of ECB

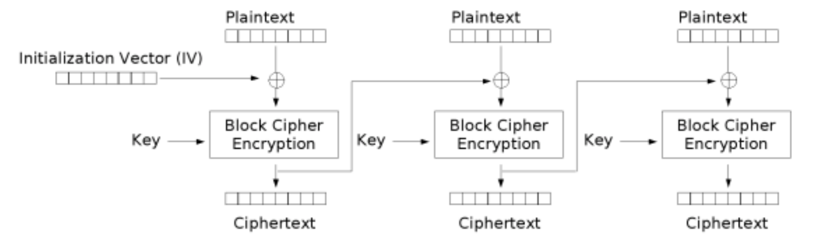
- Not recommended!
  - The output can be still recognized
  - Repeating or replacing blocks



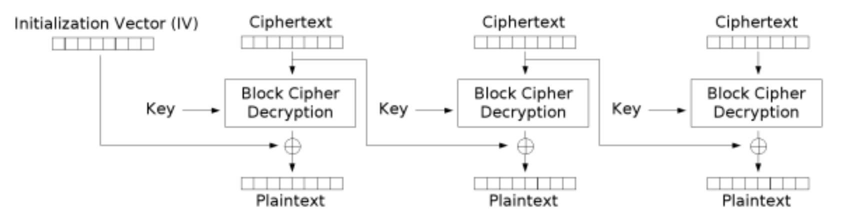
- Can be improved with random padding

CBC – Cipher-block Chaining

- Plaintext XORed with the previous ciphertext
  - Needs an Initialization Vector (IV)
  - IV should not be secret!
- Properties
  - Changing IV or key changes the output
  - No replacing, repeating attack anymore
  - Bit error affects the actual block + the next block
    - Possible attack
  - Change in the input changes all the output blocks



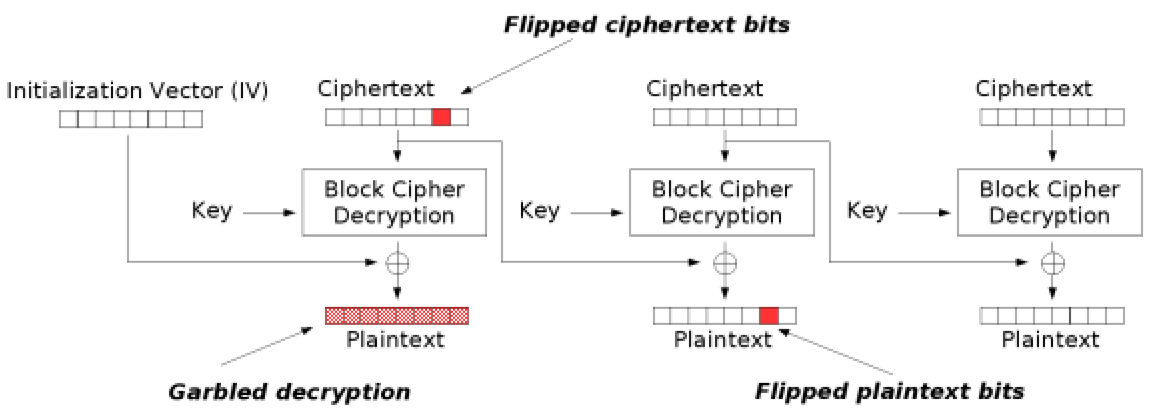
Cipher Block Chaining (CBC) mode encryption



Cipher Block Chaining (CBC) mode decryption

Error propagation in CBC

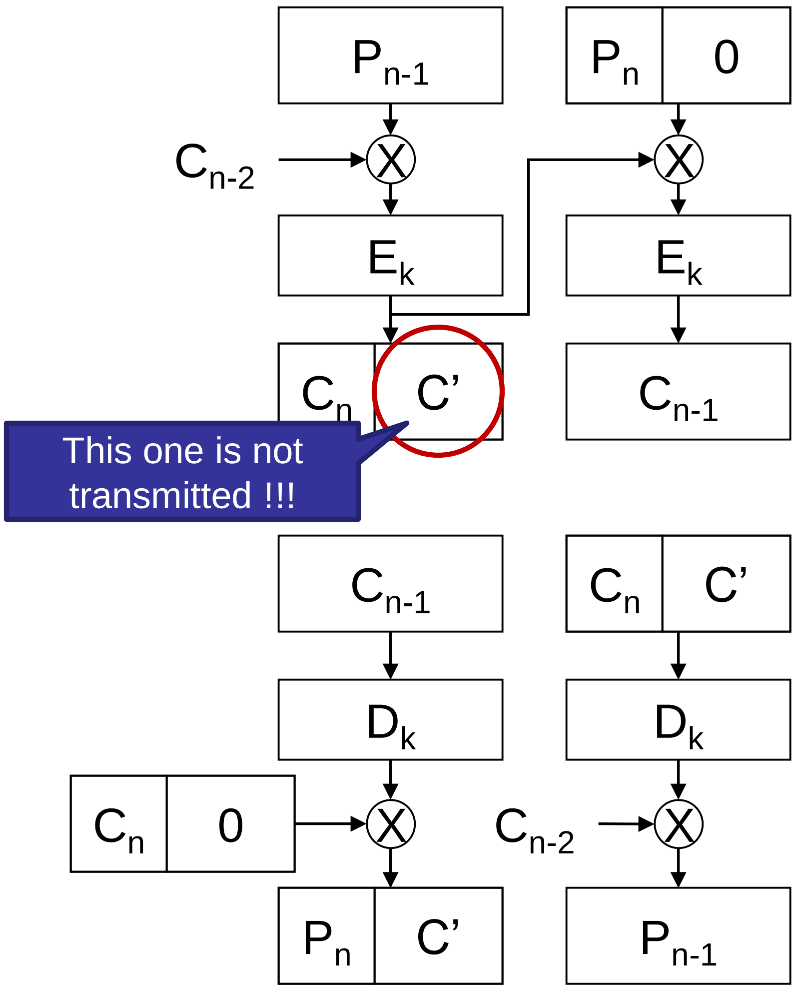
- Bit errors in the communication (e.g. wireless) or adversary's attack
- Bit error or bit insertion/removal



Modification attack or transmission error for CBC

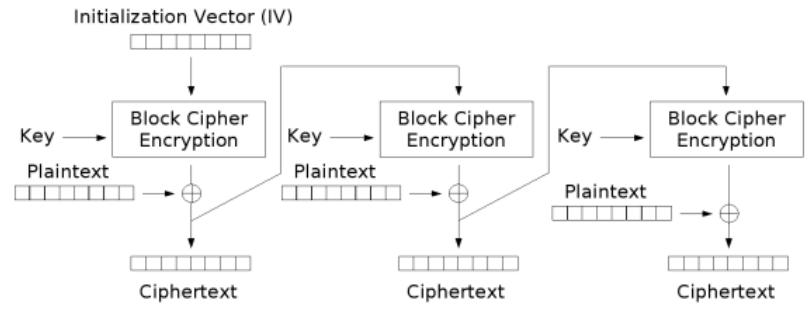
Ciphertext stealing

- CBC mode, that does not require padding
  - Encryption
    - Fill the last block with 0 bytes
    - Encryption using CBC
    - Swap the last 2 ciphertext blocks
    - Truncate the length of the last ciphertext
  - Decryption
    - If ciphertext is shorter than a block, then use the last bits of the last decrypted plaintext
    - Swap the last 2 ciphertext block
    - Truncate the length of the plaintext

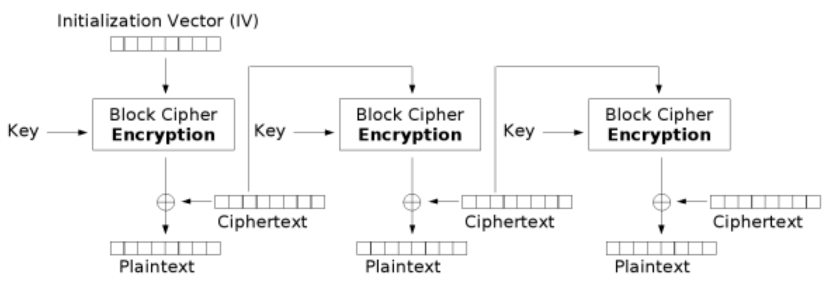


CFB – Cipher Feedback

- Generates a keystream – no padding
- Properties
  - Like CBC, but
  - 2 corrupted blocks
  - No decryption used!
    - Not suitable for asymmetric ciphers
  - CFB-r
    - Works on less bits than a whole block



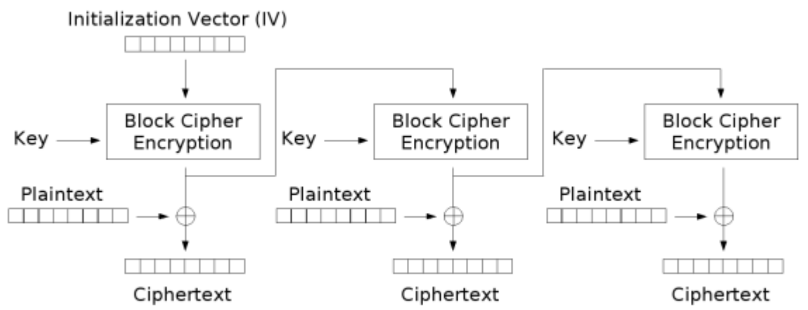
Cipher Feedback (CFB) mode encryption



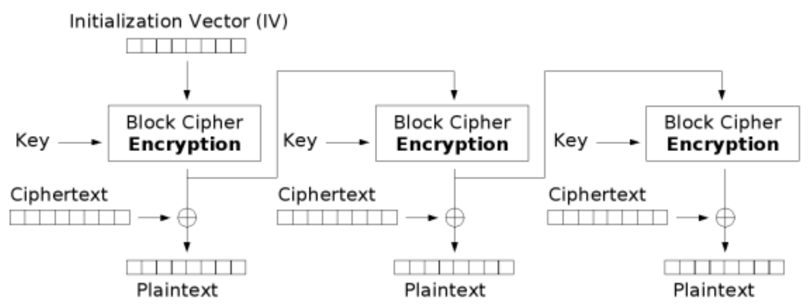
Cipher Feedback (CFB) mode decryption

OFB – Output Feedback

- Properties
  - Similar to CFB, but
  - Keystream is independent of the plaintext
  - Bit error affects only one bit in the output
  - OFB-r
  - Key and IV pair should not be reused



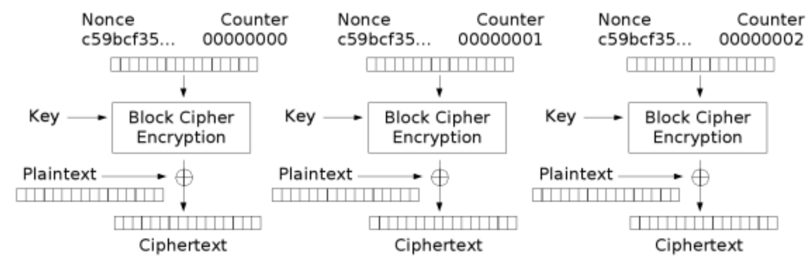
Output Feedback (OFB) mode encryption



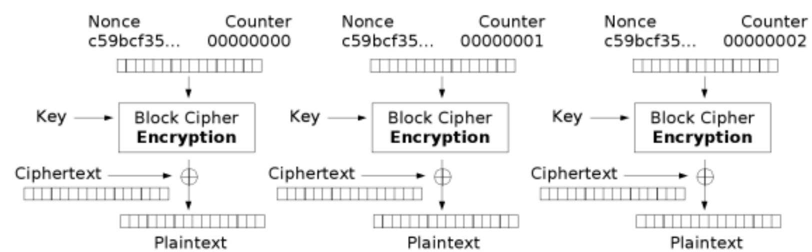
Output Feedback (OFB) mode decryption

CTR - Counter

- Uses a counter, no feedback
- Random access
- Nonce and key pair should not be reused!



Counter (CTR) mode encryption



Counter (CTR) mode decryption

- Problems with the same key
  - P1 XOR **K1** = C1
  - P2 XOR **K1** = C2
  - (P1 XOR K1) XOR (P2 XOR K1) = C1 XOR C2
  - P1 XOR P2 = C1 XOR C2

K1 XOR K1 = 0 !

No key here!

Authentication

- ECB, CBC, CFB and OFB make encryption, but no authentication
- Authentication + encryption
  - Authenticated-encryption with associated-data (AEAD)
  - Two-pass solutions
    - EAX mode
    - CCM - Counter with CBC-MAC
  - One-pass solutions
    - OCB - Offset Codebook Mode

References

- Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone, “Handbook of Applied Cryptography”, CRC Press, ISBN: 0-8493-8523-7
  - http://www.cacr.math.uwaterloo.ca/hac/
- Wikipedia - The free encyclopedia
  - http://www.wikipedia.org/
- AES animation
  - http://www.cs.bc.edu/~straubin/cs381-05/blockciphers/rijndael_ingles2004.swf