Symmetric Crypto Block Cipher

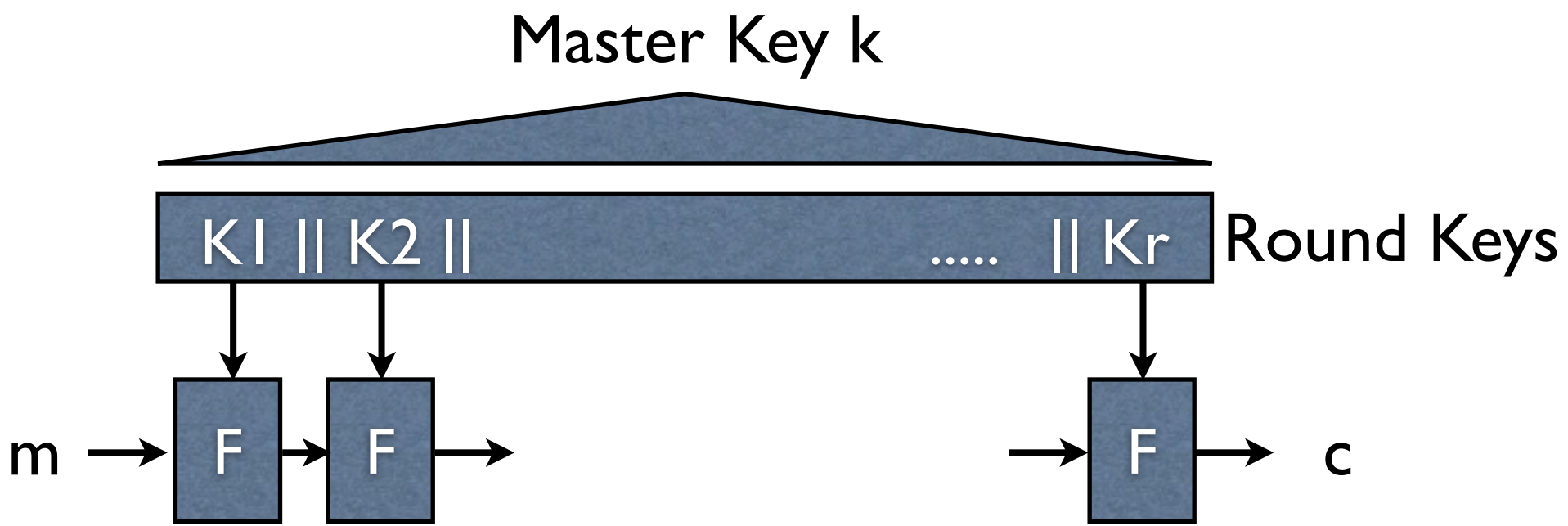
Pierre-Alain Fouque

Family of permutations

- Block cipher = family of 2^k substitutions on an alphabet of size 2^n indistinguable from randomly chosen substitutions
- Constructions:
  - Feistel scheme (DES)
  - SPN: Substitution-Permutation Network (AES)

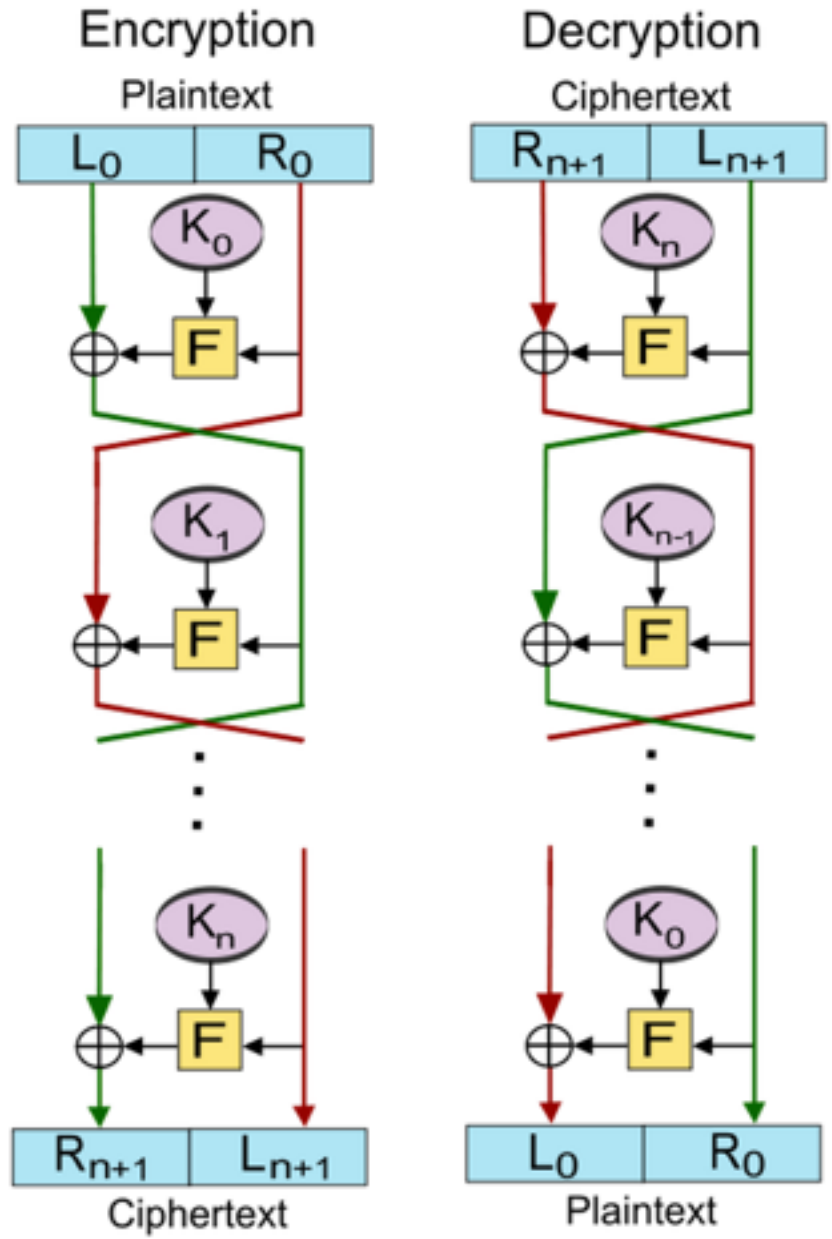
Block cipher

- Cipher (E,D) «eff. algs» such that D(k,E(k,m))=m
- Main drawback of stream cipher: lacks of theory to construct secure PRG
- Iterate many times a «small» round function F



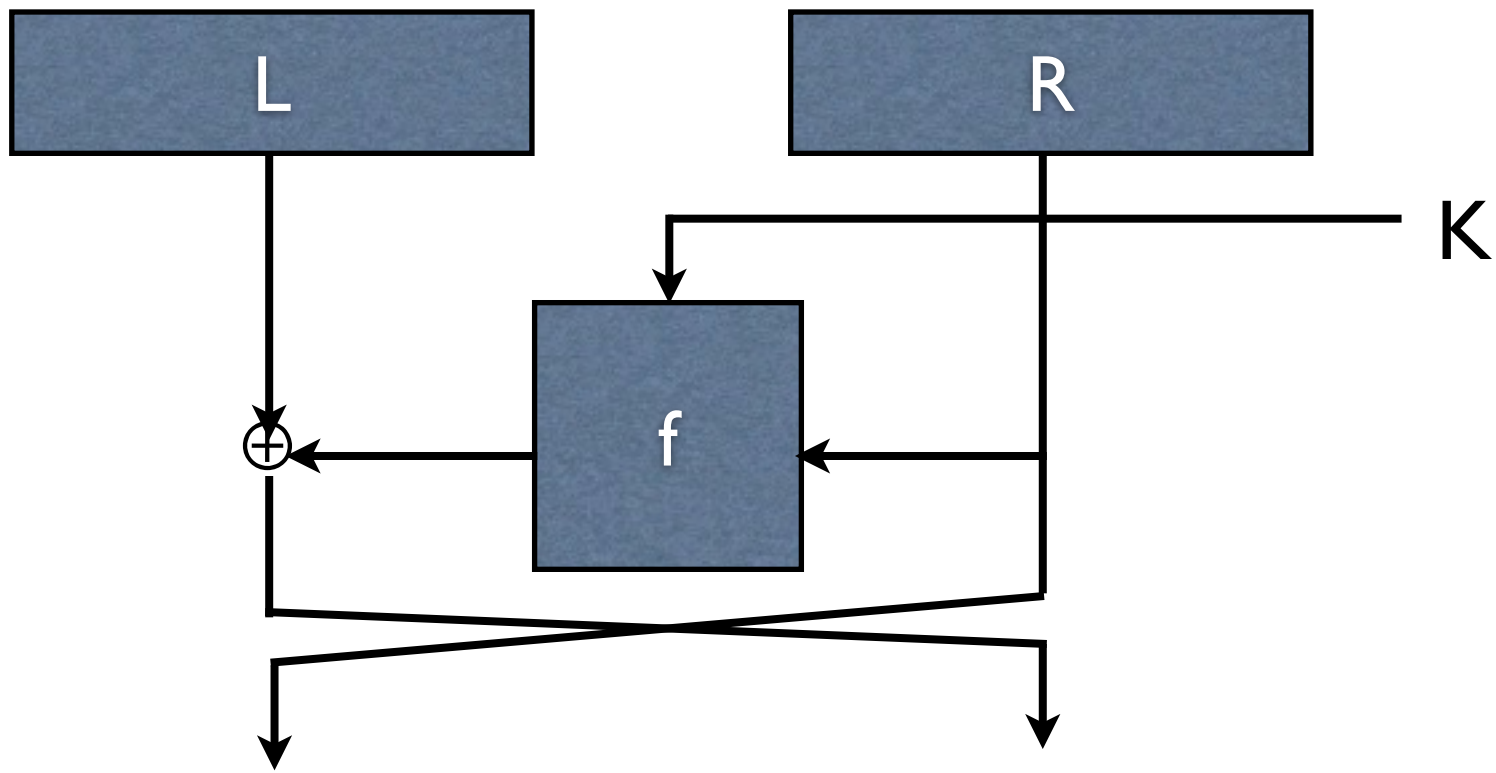
Data Encryption Standard

- DES (IBM 1973) and NBS (1977)
- Key Length: 56 bits
- Block Length: 64 bits
- 16 rounds with 48-bit round keys



Feistel scheme

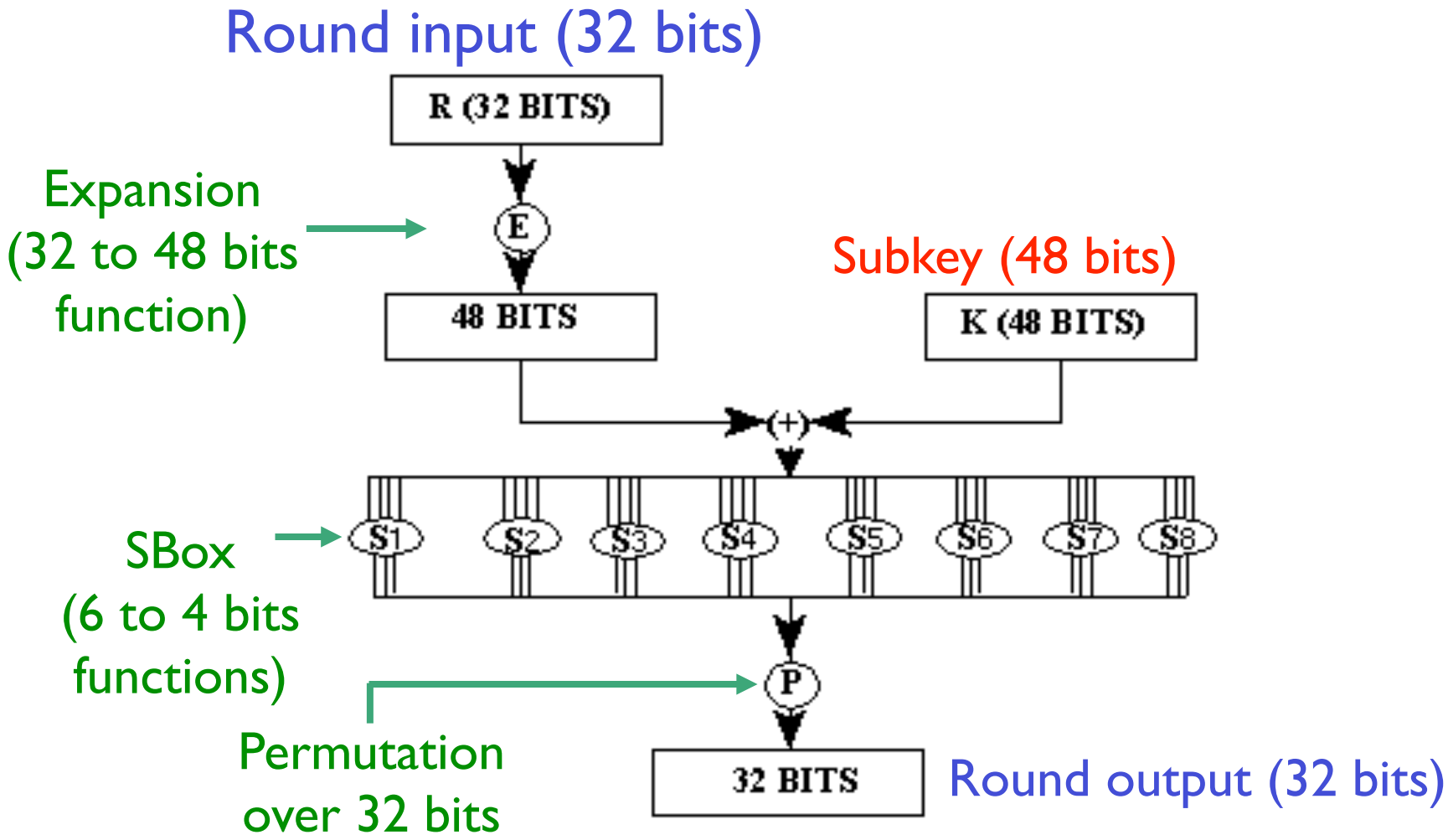
- Designed by Horst Feistel at IBM
- Transform random function to random permutation



Feistel security

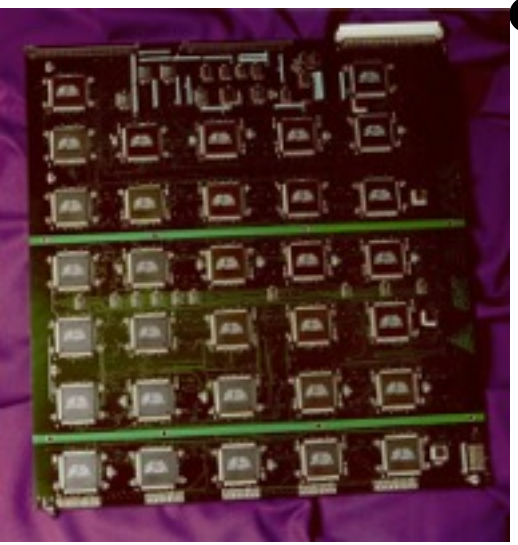
- Could you distinguish one-round Feistel ?
- Could you distinguish two-round Feistel ?
- Could you distinguish three-round Feistel ?

f function


Round input (32 bits)
R (32 BITS)
Expansion
(32 to 48 bits
function)
E
48 BITS
Subkey (48 bits)
K (48 BITS)
(+)
SBox
(6 to 4 bits
functions)
S1
S2
S3
S4
S5
S6
S7
S8
P
Permutation
over 32 bits
32 BITS
Round output (32 bits)

Attacks against DES

- Before 1990: attacks against round reduced version (less than 16 rounds)
- 1990-92: Differential cryptanalysis
- 1993-94: Linear cryptanalysis
- other attacks: Davies-Murphy, side-channel
- In practice, the most efficient attack is the exhaustive search (EFF, copacabana)

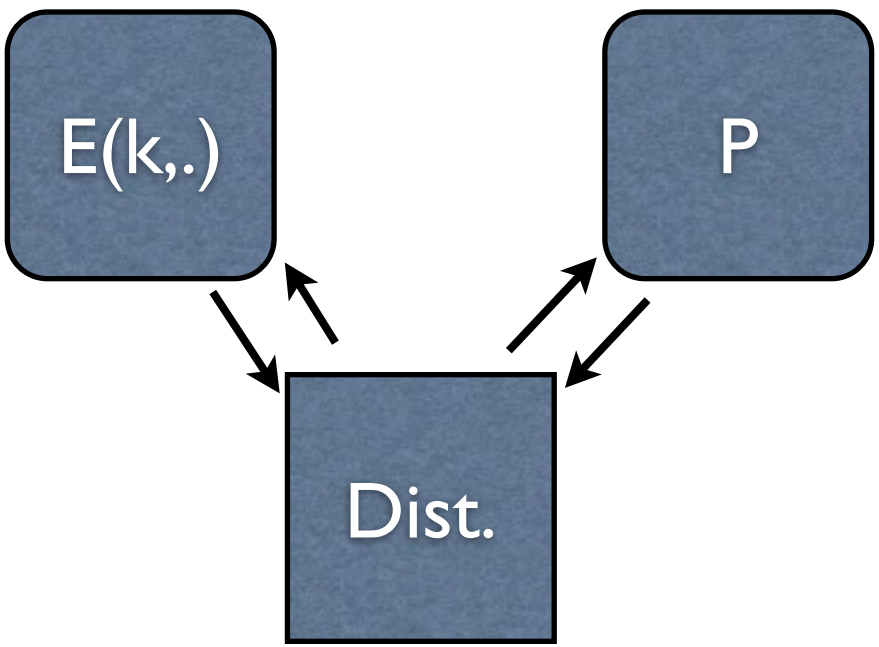


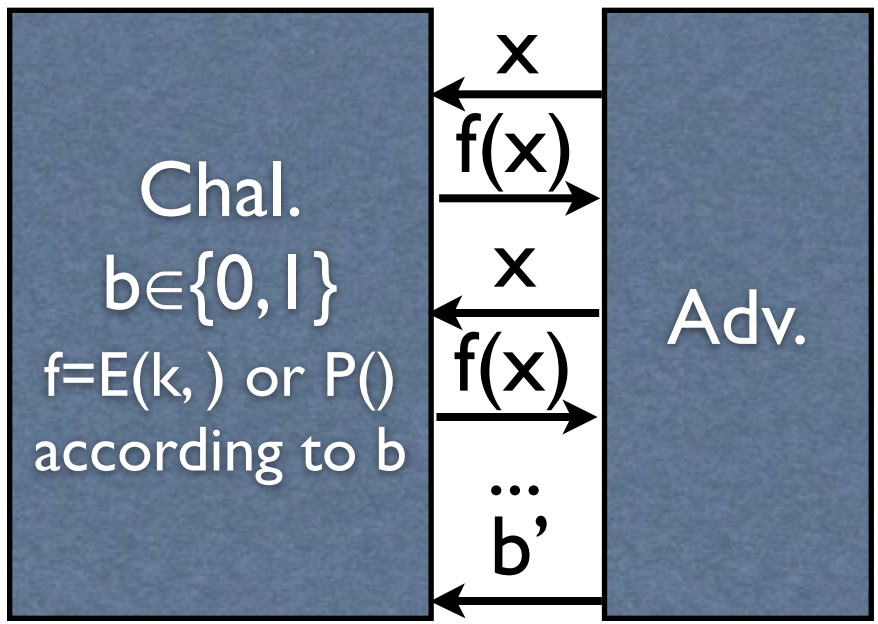
Main drawback of DES

- Exhaustive key search in 2^{56} (3DES)
- Block size (collision for 2^{32} blocks)
- Differential / Linear Cryptanalysis
- DES: well-designed and withstands successfully 30 years of cryptanalysis

Security game

- Block cipher must be indistinguishable from a random permutation
  - for all k, E(k,x) is a permutation which looks random provided the key is not known





Adv(A)=|Pr[b=b']-1/2|

Birthday Paradox

- Randomy and independently chose k balls among N balls, whenever $k \approx \sqrt{N}$, Pr[coll]> ½
- If N=365, the probability that two people same birthday is ½ when $k \approx 23$
- Pr(no coll with k balls)= (1-1/N)(1-2/N)...(1-(k-1)/N)<exp($\sum i$ i/N)=exp(k(k-1)/2N)
- if $k \approx \sqrt{N}$, Pr(coll)>½
- Two sets N and M of random elements in a set D: Number of expected collisions is |N|×|M|/|D| (Birthday paradox with boys and girls)

2DES → 3DES

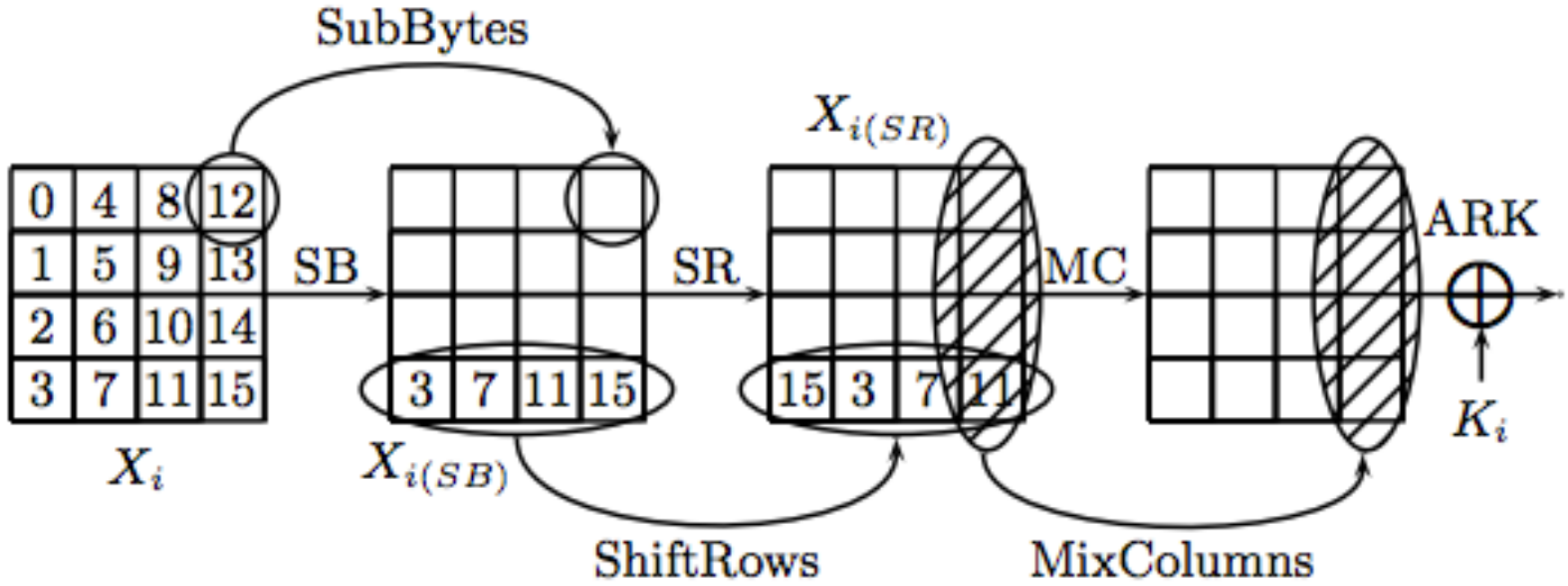
Differential Attack

- Consider an Even-Mansour Scheme

Advanced Encryption Standard

- Substitution / Permutation Network
- Key Length: 128 / 192 / 256 bits
- Round numbers: 10 / 12 / 14 (last round w/o MixColumns)
- Block Length: 128 bits
- Designed by Daemen and Rijmen
- Standardized by NIST in 2000

AES



Diffusion: 2 tours

Attaque sur 6 tours en 2^{48}

Attaque sur 7 tours en 2^{100}

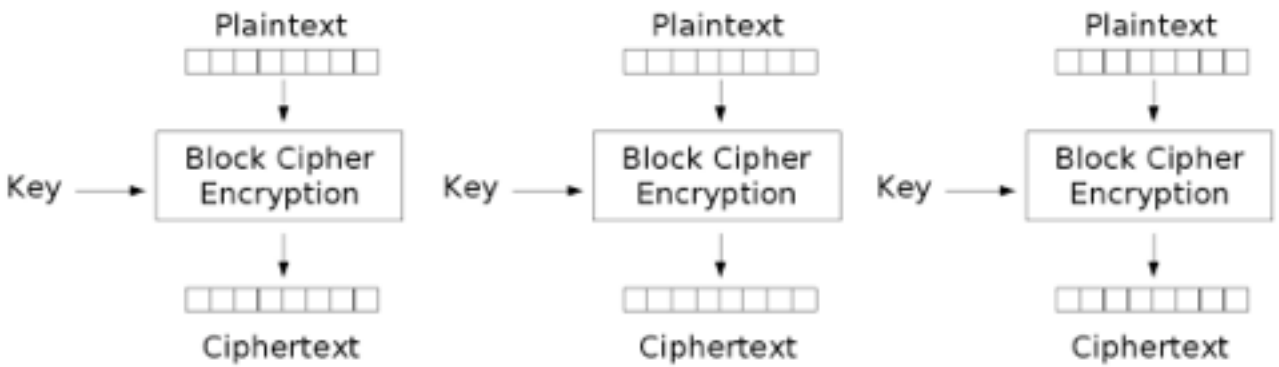
Pas d'attaque au-delà mais en attaque par canaux auxiliaires

Security

- MDS Property of the MixColumn
- Diffusion: In 2 rounds, any difference affect the whole cipher
- Security against Differential / Linear Cryptanalysis: good properties of the SBox
- Square Attack
- Side-channel Attack (timing, Power Analysis) are the most efficient attacks against AES

Modes of operation

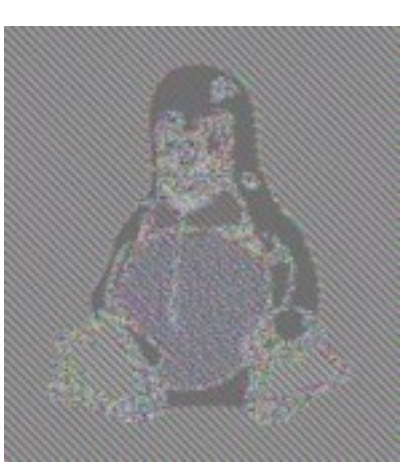
- How to encipher larger messages ?
  - ECB, CBC, CTR, OFB, CFB

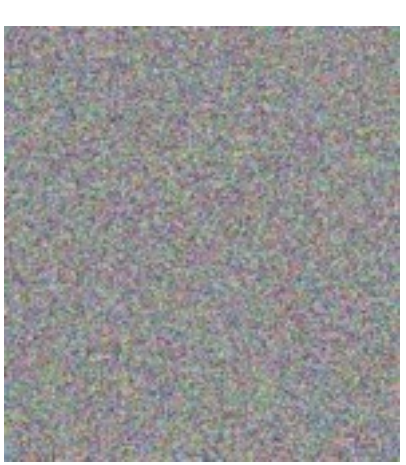


Electronic Codebook (ECB) mode encryption

Drawbacks:
- deterministic

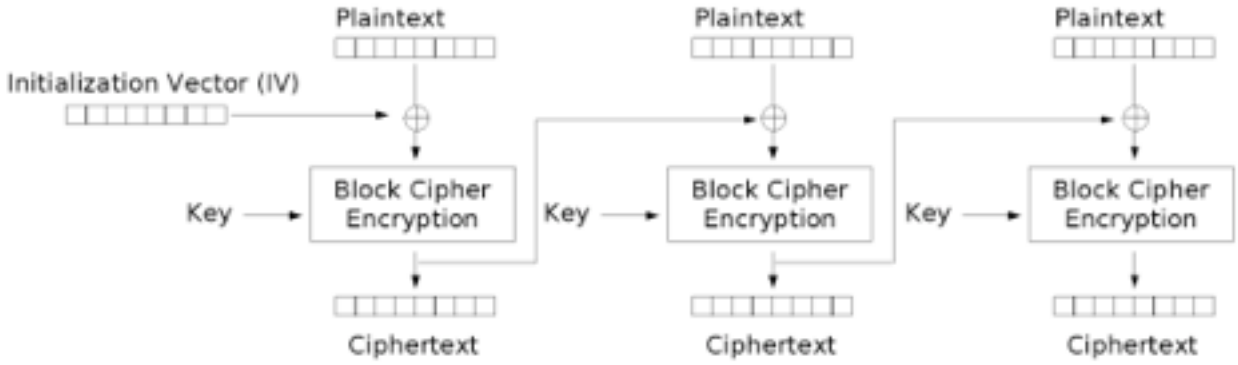
Advantages:
- parallelisable





Ciphertext Block Chaining (CBC)

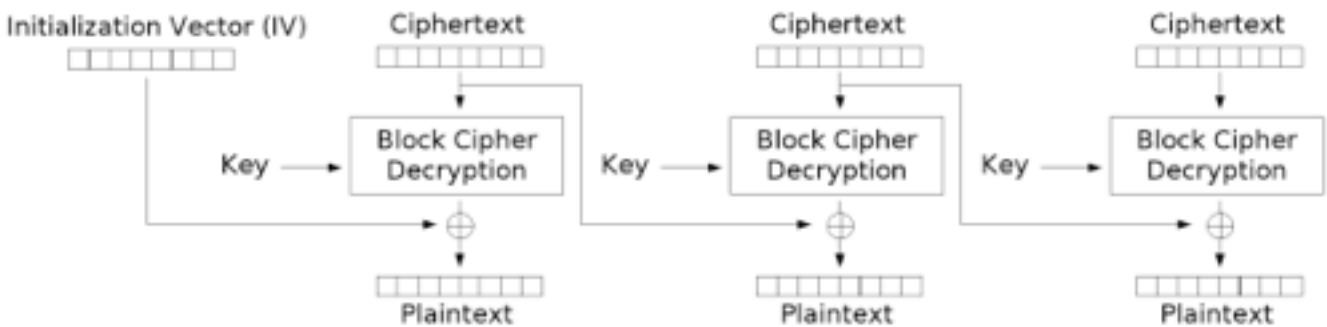
- Encrypting: $C_0=IV, ..., C_i=E(k,C_{i-1} \oplus M_i)$
- Decrypting: $M_i=D(k,C_i) \oplus C_{i-1}$



Cipher Block Chaining (CBC) mode encryption

Drawbacks:
- sequential

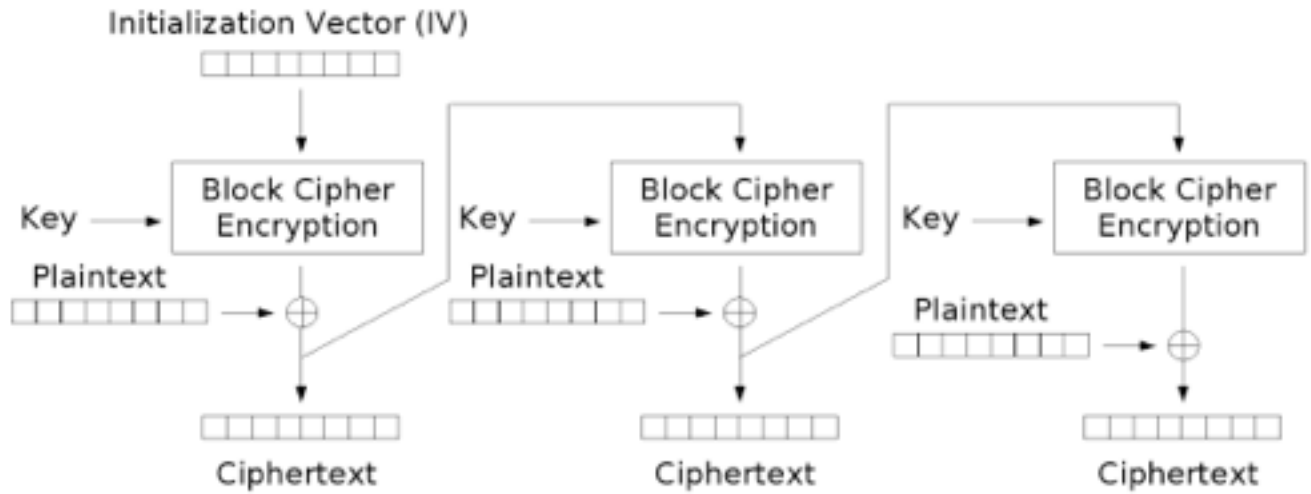
Advantages:
- randomized
- propagation of error in decryption



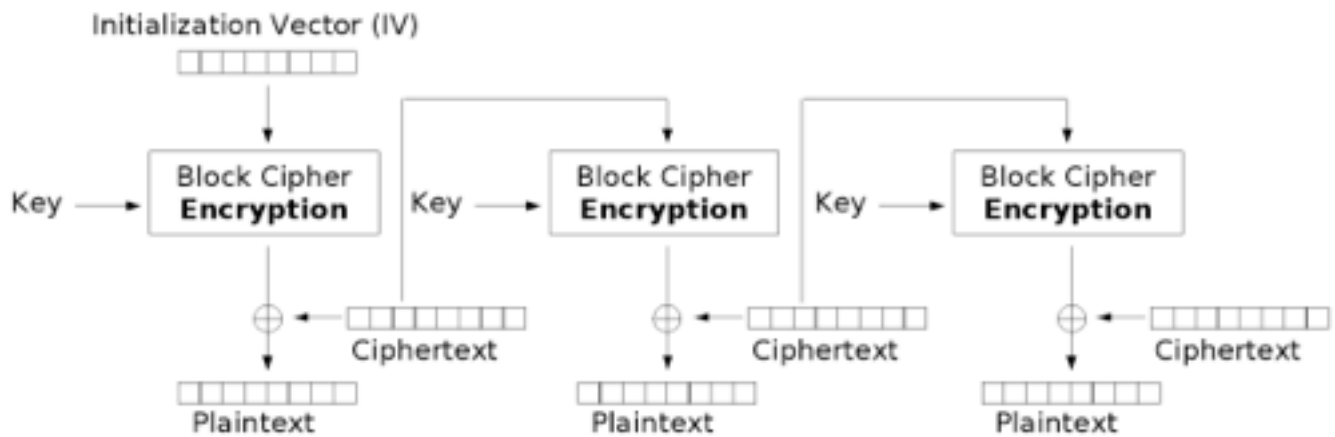
Cipher Block Chaining (CBC) mode decryption

Ciphertext FeedBack (CFB)

- How to use a block cipher as a stream cipher ?



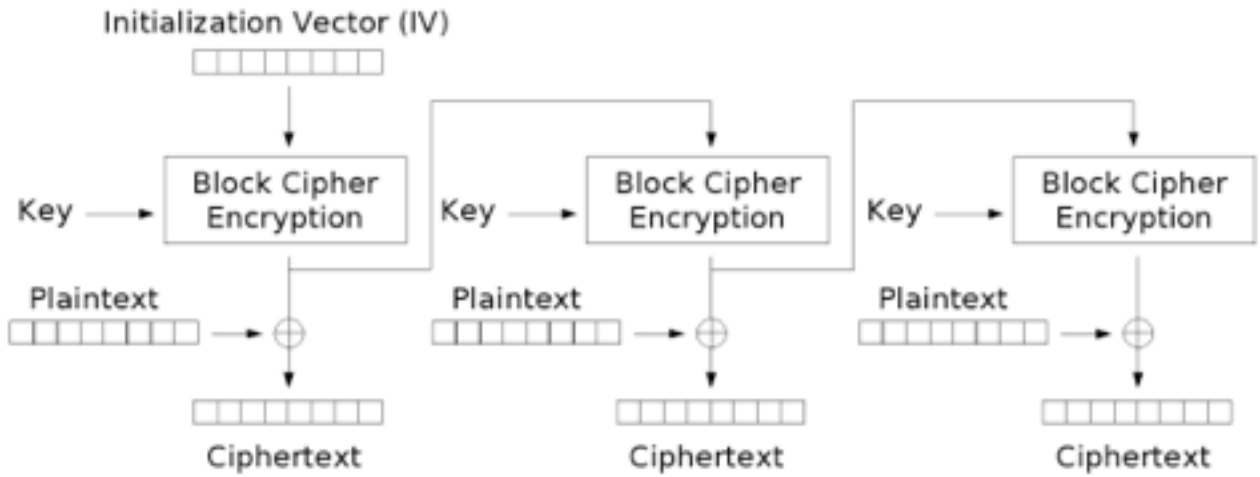
Cipher Feedback (CFB) mode encryption



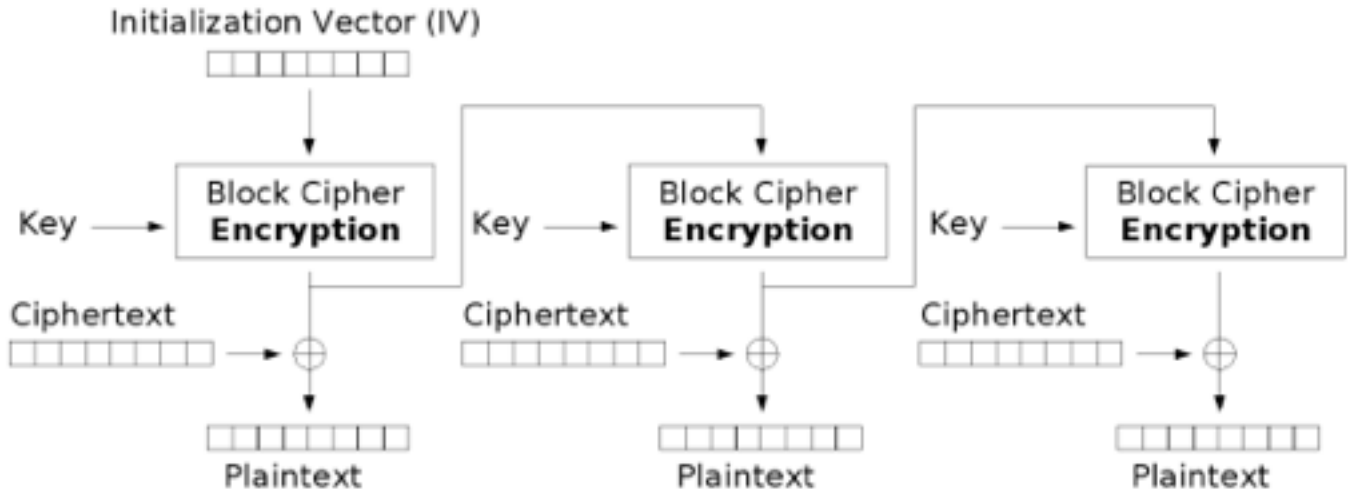
Cipher Feedback (CFB) mode decryption

Output FeedBack (OFB)

- How to use a block cipher as a stream cipher ?



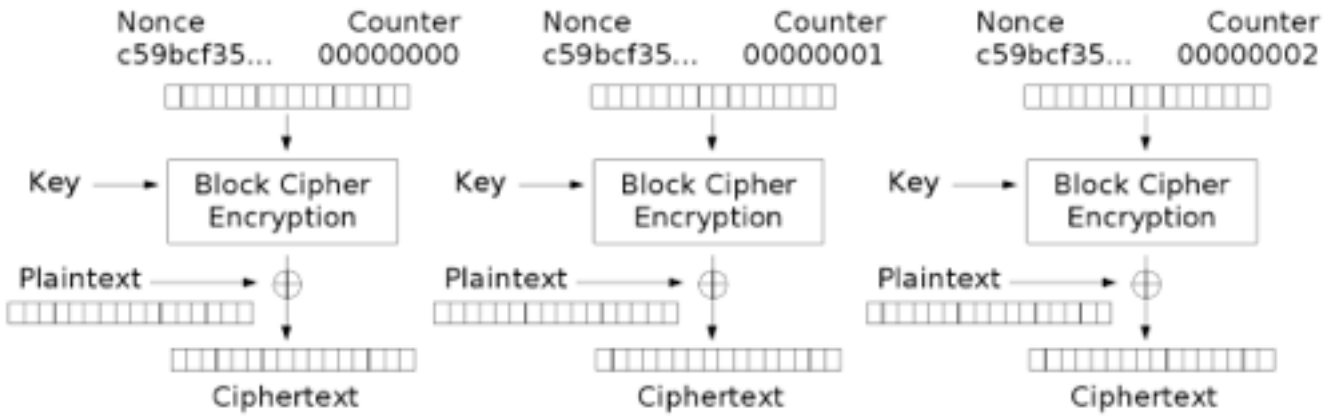
Output Feedback (OFB) mode encryption



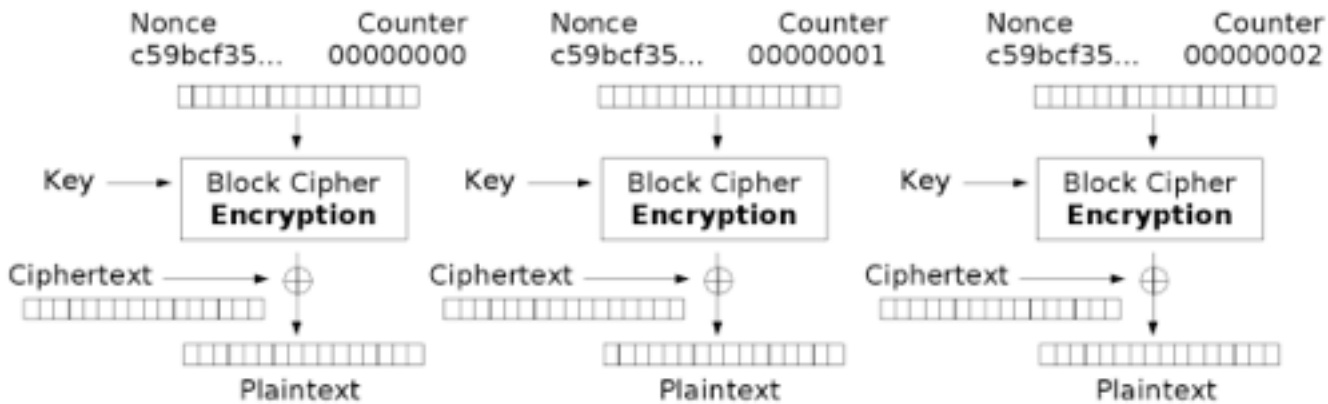
Output Feedback (OFB) mode decryption

Counter Mode (CTR)

- Better solution



Counter (CTR) mode encryption



Counter (CTR) mode decryption

Security

- Confidentiality is ensure by the mode of operation
- Integrity: first block of CBC ?
- Main idea: the ciphertext must be indistinguishable from random for polynomial-time adversaries
- Security Game:

- Example on CBC: