TOPIC: 6.857

DATE: 2/25/19

FILE UNDER:

PAGE: L06.1

**Admin:** Pset #1 due tonight; pset #2 out tonight.

Projects: post one-pager (to find team)

**Today:** Block ciphers

- DES (Data Encryption Standard)
- AES (Advanced Encryption Standard)
- Modes of operation (ECB, CTR, ...)

**Readings:**

- Katz-Lindell Chapter 5
- Aumasson Chapter 4
- Wikipedia

TOPIC:

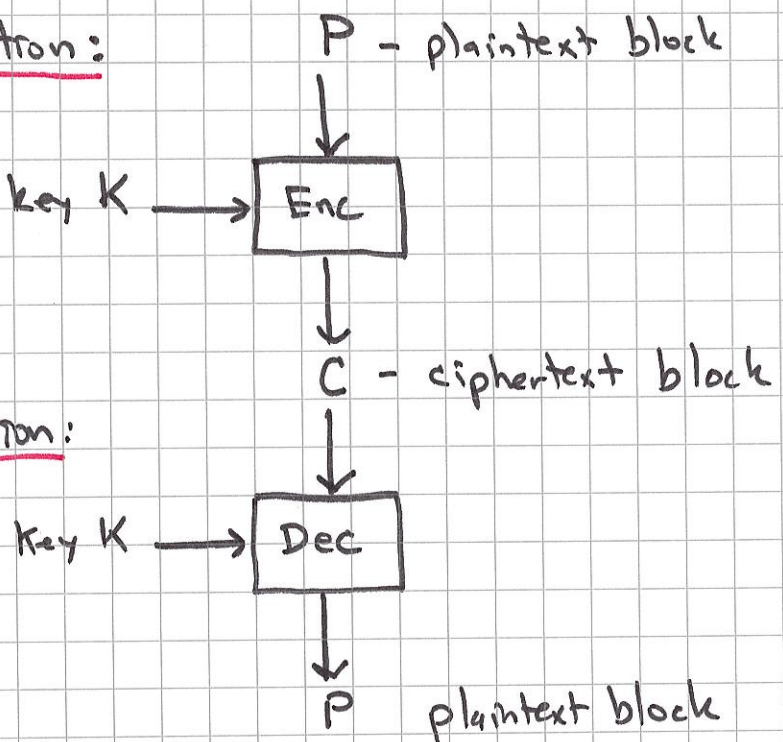
DATE:

FILE UNDER:

PAGE L6.1.5

# Block ciphers

## Encryption:




## Decryption:

Fixed length P, C, K

DES: |P| = |C| = 64 bits  |K| = 56 bits.

AES: |P| = |C| = 128 bits  |K| = 128 bits
192
256

- Use a "mode of operation" to handle arbitrary length input.

Block size:

- Should not be too large for efficiency purposes.
  - Large block ≡ large ciphertext - even if encrypting very short msg ⇒ large overhead.
  - Large block ⇒ large memory footprint.

- Should not be too small for security.
  (o.w. can be broken by brute force; a.k.a. "Codebook Attack")

Security Goal:

Intuitively: as long as key K is secret (and random) Enc(K, P) should look random for any given P.

That is, E(K, ·) should look like a random permutation.

E(K, ·) ... pseudorandom permutation

## Constructions:

Block ciphers used in practice is not a gigantic alg, but rather consists of many repetitions of a "simple" round.

Each round is weak on its own, but strong in number.

## Two main techniques:

- Feistel schemes (as in DES)
- Substitution-permutation schemes (as in AES)

## Feistel Schemes

Designed in 1970's by IBM engineer Horst Feistel.

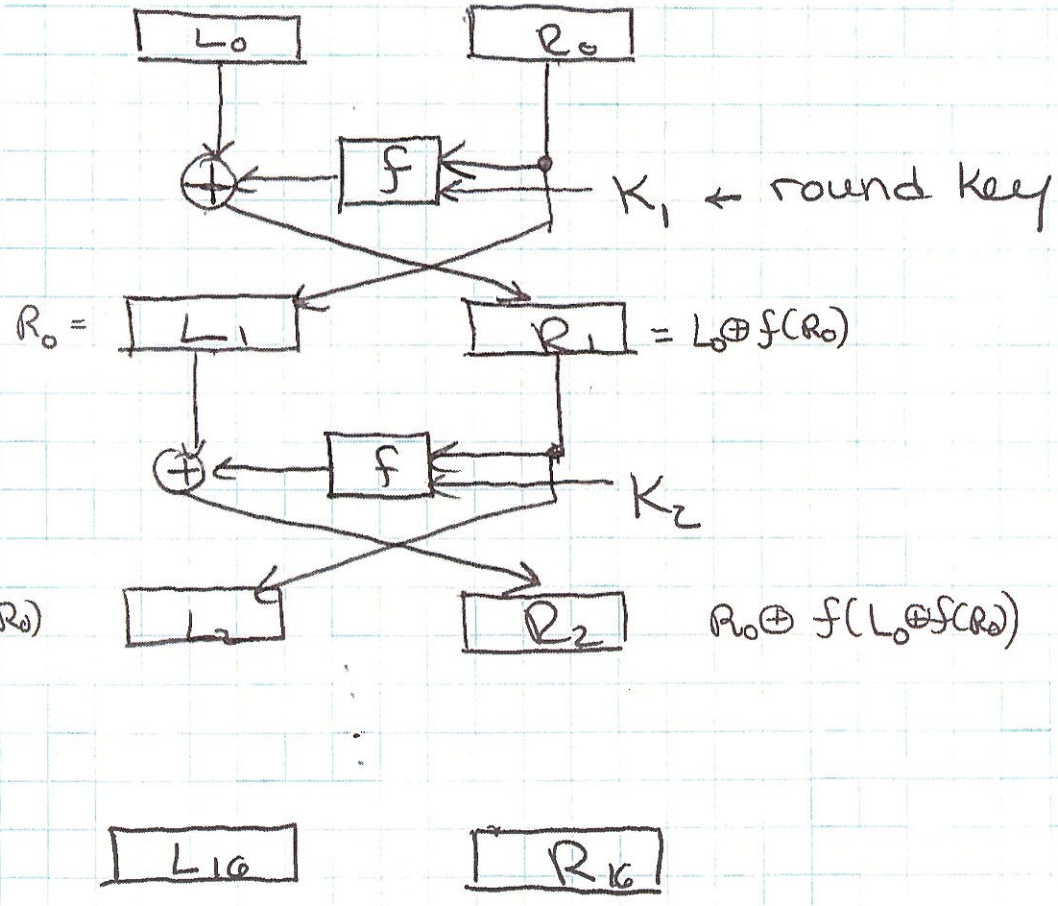
DES (Data Encryption Standard), adopted as a federal standard, in 1976, is based on Feistel scheme.

In 2000, NIST (National Institute of Standards & Technology) selected a successor to DES, called AES (Advanced Encryption Standard).

During the Cold War both US & Soviets used Feistel block cipher (DES & GOST).

Feistel scheme:

- Split 64-bit block into two 32-bit halves $L_0, R_0$




- Note f takes a round key $K_1, \ldots, K_{16}$.
  Round keys are derived from the main key K using an alg' called a "Key schedule Alg".
  Round keys should be different in each round.

In DES main key consists of 56 bits, and each round key consists of 48 bits.

Note: A Feistel scheme is invertible for any $f$ and any key schedule.

* Feistel scheme useful not only for block ciphers [eg., it is used for "Optimal Asymmetric Encryption Padding" (OAEP)]

What is $f$, and in general how many rounds are needed?

$f$ should be non-linear & "cryptographically strong".

DES performs 16 rounds

GOST " 32 rounds.

If $F$ is "as strong as possible" (i.e., modelled as a random oracle) then in theory 3 rounds is enough to get security against chosen plaintext attacks, and 4 rounds are known to be enough against chosen plaintext & chosen ciphertext attacks

[Luby-Rackoff 88]

# Constructing f

[Shannon]: Confusion-diffusion paradigm

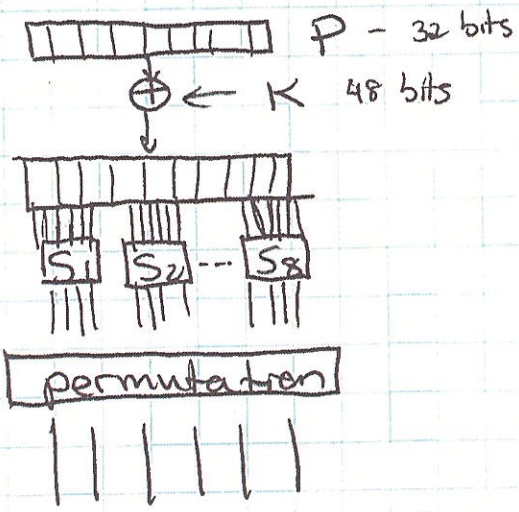
Paradigm for constructing concise random looking functions.

Confusion: Partition the block to many small blocks of 4-8 bits each (6 bits in DES), and apply a random looking function on each small block seperately. This function is called a substitution box (or S-box), and is a lookup table.

S-boxes should be "random"; i.e. non-linear & without statistical bias. [In DES S-box takes 6 bits to 4 bits

Diffusion: The bits of the output are permuted, or "mixed

$f_K$ :




(SPN)

especially when done over many rounds ↓

This is also called substitution-permutation networ

History:

In 1976, after consultation w. the NSA (National Security Agency), the NBS selected Feistel's alg' w. slight modifications, and became the "Data Encryption Standard".

The modifications: weakened key length, changed S-boxes. People were worried that NSA inserted a "backdoor", and shortened key size to their advantage.

~~The Alg. Senate~~

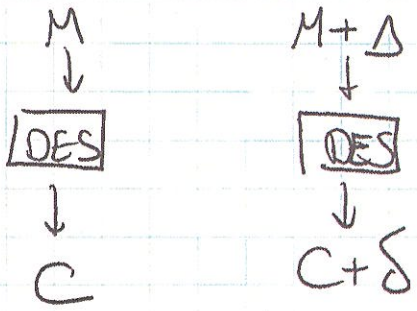
A committee was selected to review the design choices, and claimed that NSA did not tamper w. the alg' design, and that IBM was involved in all decisions.

In contrast, a declassified NSA document claimed that NSA began working on their own alg's, and discovered that Walter Tuchman from IBM was working on modified version. So NSA gave Tuchman clearance and brought him in to work jointly w. the NSA.

Later, (in late 80's) when Biham & Shamir published the differential cryptanalysis method, it was realized that the new S-boxes are more resistant to such attacks, which explains the change to the S-box design.

Differential Attacks:

Requires $2^{47}$ chosen plaintexts. (on DES).




Linear Cryptanalysis [Matsui 90's]

Requires $2^{43}$ chosen plaintexts

Eg. $m_3 \oplus m_{17} \oplus c_1 \oplus k_{12} = 0$

w.p. $\frac{1}{2} + \varepsilon$.

56-bits of security is insuffient!

Today, easily breakable by brute force attack.

AES (Advanced Encryption Standard)

Replaces DES.

Invented by two Belgian cryptographers Rijmen & Daemen

# AES

Used worldwide, the most-used cipher in the universe.

NIST standardized AES in 2000 as a replacement for DES.

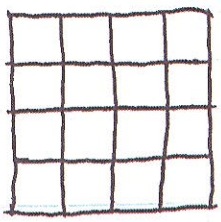
NSA approved it for protecting top-secret information.

Block length = 128 bits w. secret key of 128, 192 or 256 bits, with the 128 bit key being the most common.

It contains 10, 12 or 14 rounds (depending on key length).

AES has byte-oriented design, and does operation in Galois field $GF(2^8)$.

View 128 bit input as 4×4 matrix where each element is in $GF(2^8)$.



$(4 \times 4 \times 8 = 128)$

AES w. 128 bit key uses an SPN structure with 10 rounds. (12 rounds for 192 bit key and 14 rounds for 256 bit key)

In each round:

① xor round-key.

substitution → ② Substitute bytes (using S-box lookup table)

Each $a_{ij} \longrightarrow S(a_{ij})$

] in AES S-boxes need to be invertib

permutation [

③ Rotate rows (row i is shifted by i locations)

④ Mix each column: Applies the same linear transformation* to each of the four columns.

There are very fast implementations.

Intel put supporting HW into its CPU's.

Security: Good, For practical purposes, can treat AES as an ideal block cipher:

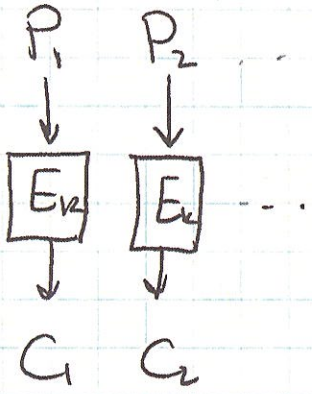
Enc(K, ·) is a random permutation.

# Modes of Operation

How to encrypt variable length msg using a block cipher (such as AES) ?

## Straightforward insecure solution:

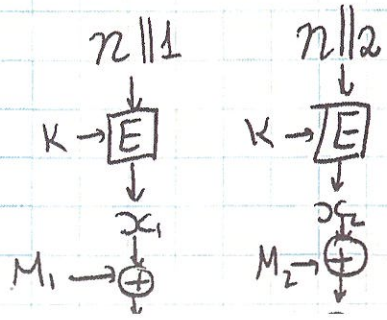
### ECB (Electronic Codebook) Mode:




ECB only good for encrypting random data.

Repeated msg blocks ⟹ Repeated ciphertext blocks.

### CTR (Counter) Mode:




$n$ random nonce
should not be reused
$(x_1, x_2 \ldots)$ "pad"
like OTP

To handle data that is not a multiple of b (=block length) bits in length:

- Use padding method:
  - Alway append 1 to each msg
  - Append enough 0 bits (after the 1) to make the length a multiple of b bits.

Pad before the encryption,

Unpad after decryption.

Important: This padding operation is invertible (1-to-1).

- Use ciphertext stealing method

  [Read about it in wiki or Serious Cryptography].