

- Admin:
- PSet #2 is out, due March 12
 - Also, March ²³: Project descriptions are due. (with team members, bibliography, etc.).
 - By end of this week, post at least one idea on Piazza.

Today: Block ciphers:

DES : "Data Encryption Standard"

AES : "Advanced" "

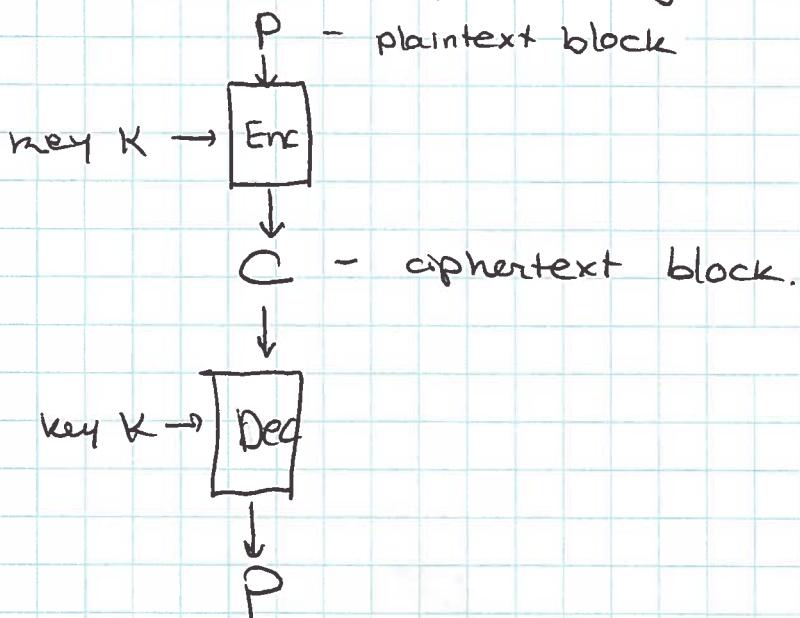
Modes of operation. (ECB, CTR)

Readings:

Chapter 4 of Serious Cryptography.
Chapter 5 of Katz-Lindell
Wikipedia.

Block ciphers: Consist of an encryption alg and a

decryption alg.



Fixed length : P, C, K

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

AES : $|P| = |C| = 128$ bits $|K| = 128$ bits
 $\begin{matrix} 192 \\ 256 \end{matrix}$

- 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 \Rightarrow large overhead.
 - ↳ Large block \Rightarrow large memory footprint.
- Should not be too small for security.
 (Law. can be broken by brute force ; a.k.a. "Codebook Attack")

Security Goal :

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

That is, $E(K, \cdot)$ should look like a random permutation.

$E(K, \cdot)$ is a 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.

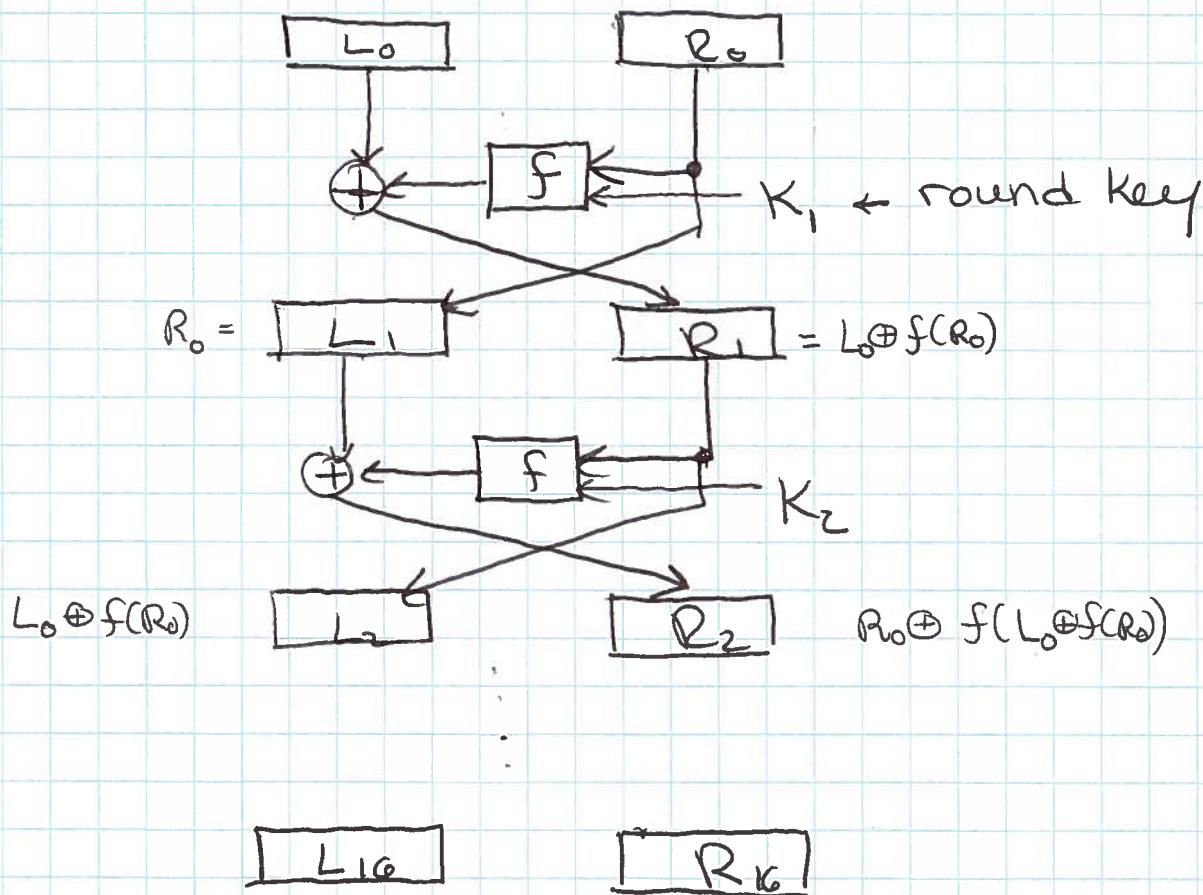
DES (Data Encryption Standard), adopted as a federal standard, in 1976, is based on Feistel scheme.

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, \dots, 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 for security.

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

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

[e.g., it is used for "Optimal Asymmetric Encryption Padding (OAEP)"]

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 attack , and 4 rounds are known to be enough against chosen plaintext & chosen ciphertext attacks

[Luby - Rackoff 86]

Constructing f

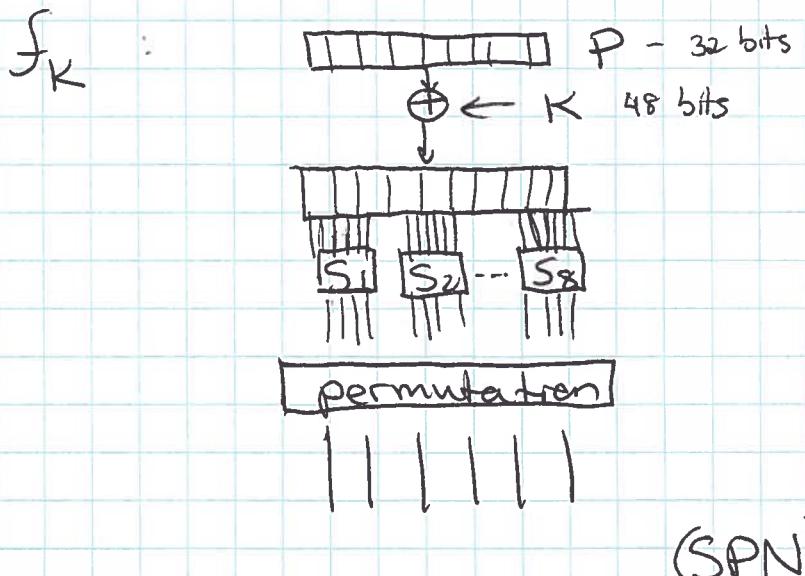
[Shannon]: Confusion-diffusion paradigm

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 separately. 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"



especially when
done over many
rounds. ↓

This is also called

substitution-permutation network

History:

L7.7

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.

~~NSA Senate~~

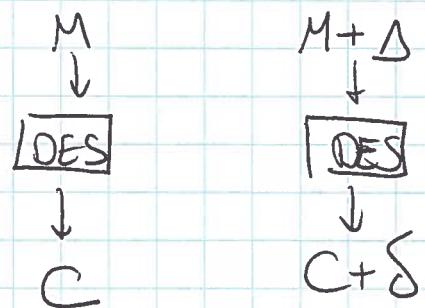
A committee was selected to review the design choices, and claimed that NSA did not tamper w. the alg' design, and that IBM was involved in all decisions.

In contrast, a declassified NSA document claimed that NSA began working on their own alg', 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.

$$\text{Eg. } M_3 \oplus M_{17} \oplus C_1 \oplus K_{12} = 0 \\ \text{w.p. } \frac{1}{2} + \epsilon.$$

56-bits of security is insufficient!
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.

AES It contains 10, 12 or 14 rounds

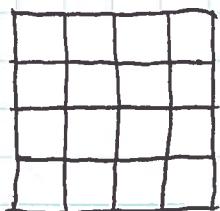
(depending on key length).

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 $GF(2^8)$.

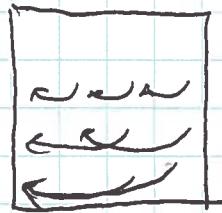
$$(4 \times 4 \times 8 = 128)$$



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.
 - ② Substitute bytes (using lookup table)
 - Each $a_{ij} \rightarrow S(a_{ij})$*
 - S-box*
 - ③ Rotate rows (row i is shifted by i locations)
 - permutation*
 - ④ Mix each column: Applies the same linear transformation to each of the four columns.
-] in AES
S-boxes need to be invertible



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:

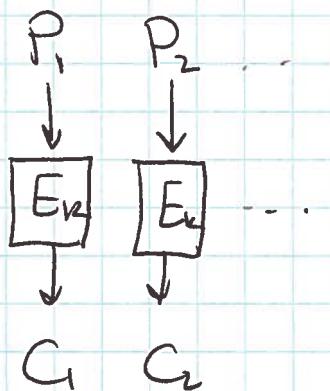
$\text{Enc}(K, \cdot)$ is a random permutation.

Modes of Operation

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

Straightforward insecure solution :

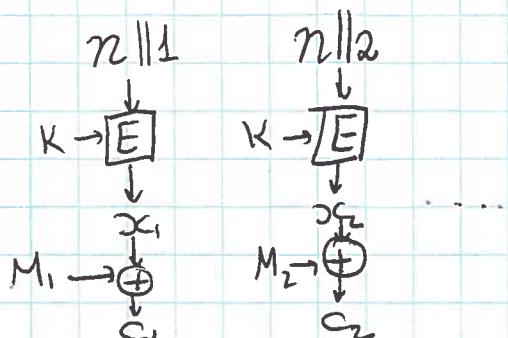
ECB (Electronic Codebook) Mode :



ECB only good for encrypting random data.

Repeated msg blocks \Rightarrow Repeated ciphertext blocks.

CTR (Counter) Mode :



n random nonce
should not be reused

(x_1, x_2, \dots) "pad"
like OTP.

$$CT = (n, c_1, c_2, \dots)$$

To handle data that is not a multiple of b ($= \text{block length}$) bits in length:

- Use padding method:

- Always 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].