Class 3

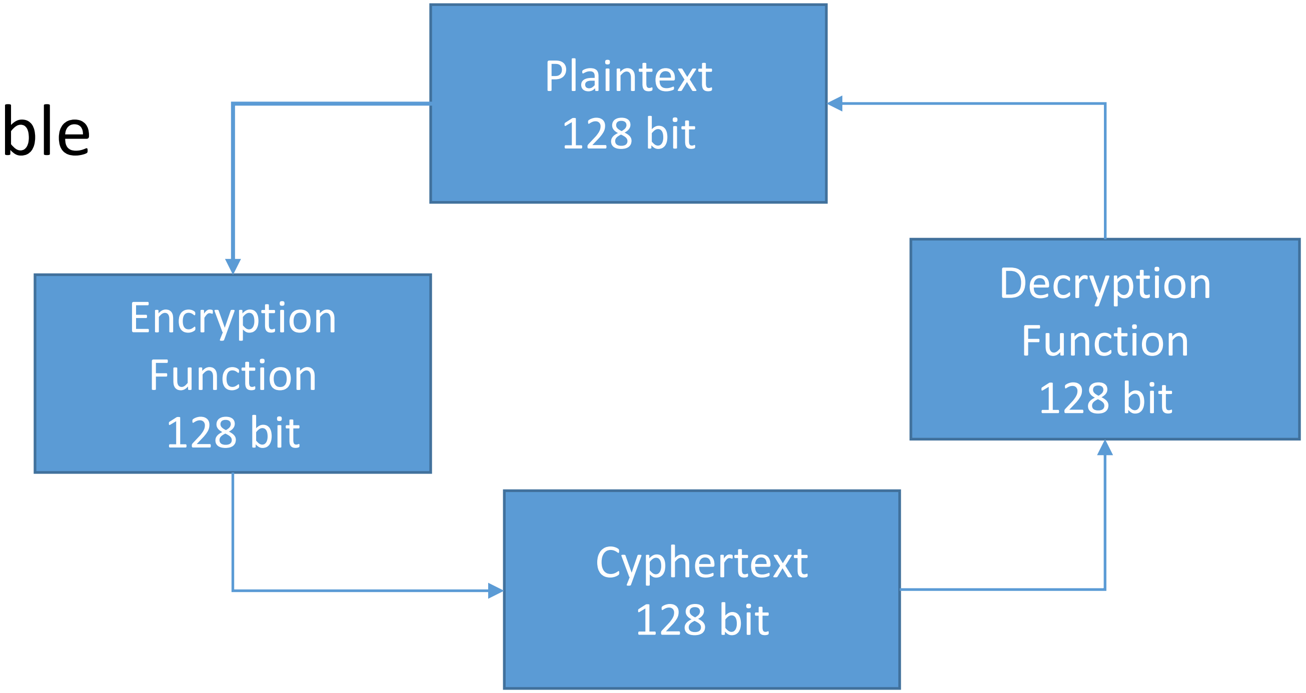
Block Ciphers

Block Cipher

Is an encryption function for fixed size block of data

Is considered as a building blocks of the cryptographic systems

Reversible



Plaintext
128 bit

Encryption
Function
128 bit

Cyphertext
128 bit

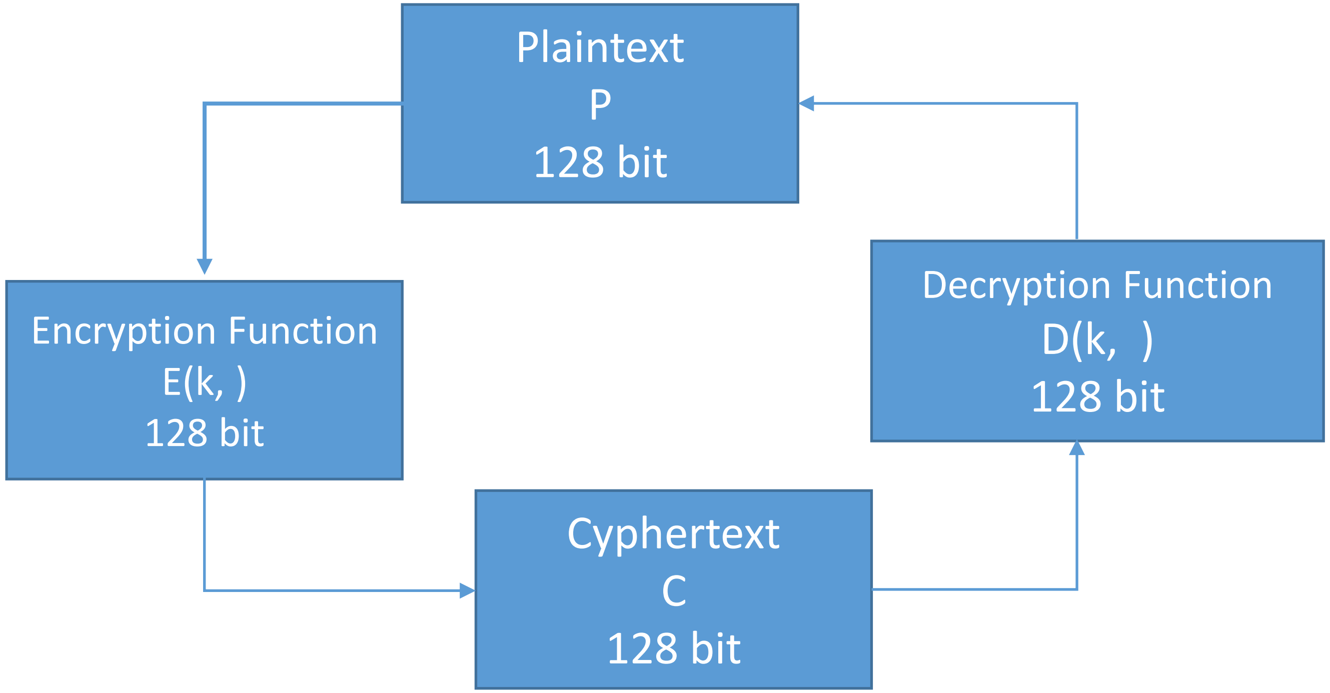
Decryption
Function
128 bit

Block Cipher

A secret key ***K*** is used to encrypt with a block cipher.

Key is a collection of bits. Common sizes are 128 and 256 bits.

Block ciphers are used to encrypt information among others.



Block Cipher

Seen as a lookup up table for a key K, if

m_{11} → C_{11} ……. m_{1n} → C_{1n}

m_{m1} →C_{m1} ……….. m_{mn} → C_{mn}

or,

$$\begin{pmatrix} c_{11} & \cdots & c_{1n} \\ \vdots & \ddots & \vdots \\ c_{m1} & \cdots & c_{mn} \end{pmatrix}$$

A block cipher with a block size of k bits specifies a permutation on k-bit values for each of the key values where $mn=2^k$

A block cipher takes all 2^k *k* bit inputs and maps it into a unique *k* bit output.

For a 32 bit block size the table would be 16GB
For a 64 bit block size the table would be 150 Million TB

Types of Attacks

Ciphertext-only attacks: attacker sees only the ciphertext of a message (rare)
Chosen-plaintext type:

Related-key attacks: assumes that the attacker has access to several encryption functions and knows the relationship between their unknown keys.

Chosen-key attacks: attacker specifies part of the key and then performs a related-key attack.

The Ideal Block Cipher

Can be understood as a random permutation; for each key value the block cipher is a random permutation

The ideal block cipher can be seen as a uniform probability distribution over the set of all possible block ciphers.

The ideal block cipher is a concept that permits discuss security, it does not really exist.

Block Cipher Security

An informal definition

Definition 1

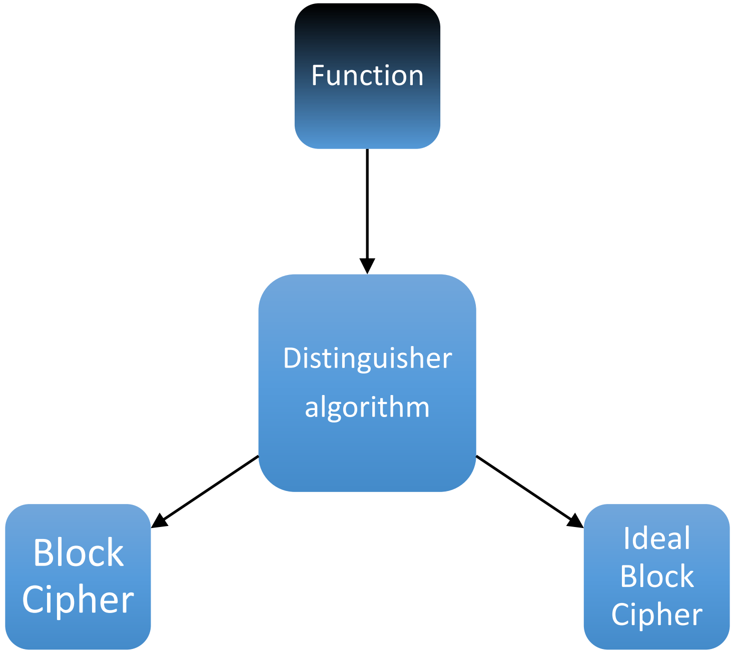
A secure block cipher is one for which no attack exists.

Definition 2

An attack on a block cipher is a non-generic method of distinguishing the block cipher from an ideal block cipher.

Block Cipher Security

The distinguisher algorithm can use any Key for decryption or encryption



A distinguisher is generic if a similar distinguisher is found for almost any block cipher.

If the block cipher has an explicit security level of n bits, then a successful distinguisher should be more efficient than an exhaustive search on n-bit.

Parity and Permutation

Consider a lookup table example for
a single key / block cipher generation

$$\begin{pmatrix} c_{11} & \cdots & c_{1n} \\ \vdots & \ddots & \vdots \\ c_{m1} & \cdots & c_{mn} \end{pmatrix}$$

Two type of permutations:

even (half)

odd (half)

Parity and Permutation

Modern block ciphers work on 128 bit size. However, they operate in words of 32 bits.

32 bits operations builds an encryption function, efficient mechanism but generate only even permutations.

Parity attack a distinguisher that can be used in almost any block cipher.

Definition 3
An ideal block cipher implements an independently chosen random even permutation for each of the key.

Real Block Ciphers

Several block ciphers proposed during past years.

Difficult creation or production of new block cipher. Includes creation its own correctness and implementation (efficiency) for different applications.

Peer review essential for a possible implementation in a production system.

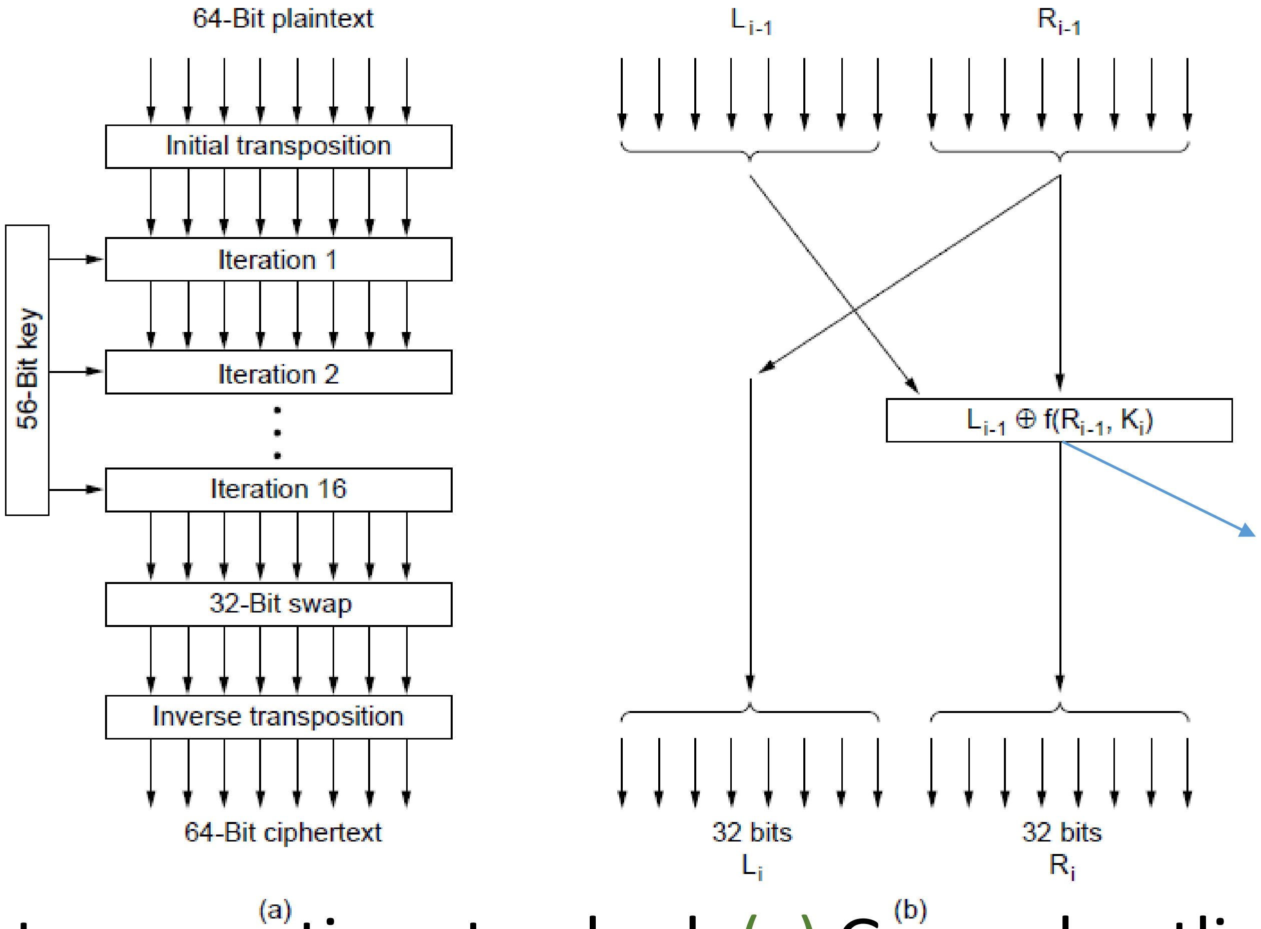
Real Block Ciphers

A Round can be understood as the generation of different repetitions of a week block cipher that in turn generated a “strong” block cipher.

Attacks aims blocks ciphers with low number of rounds.

Real Block Ciphers: Data Encryption System (DES)

Adopted by the US Government in 1977

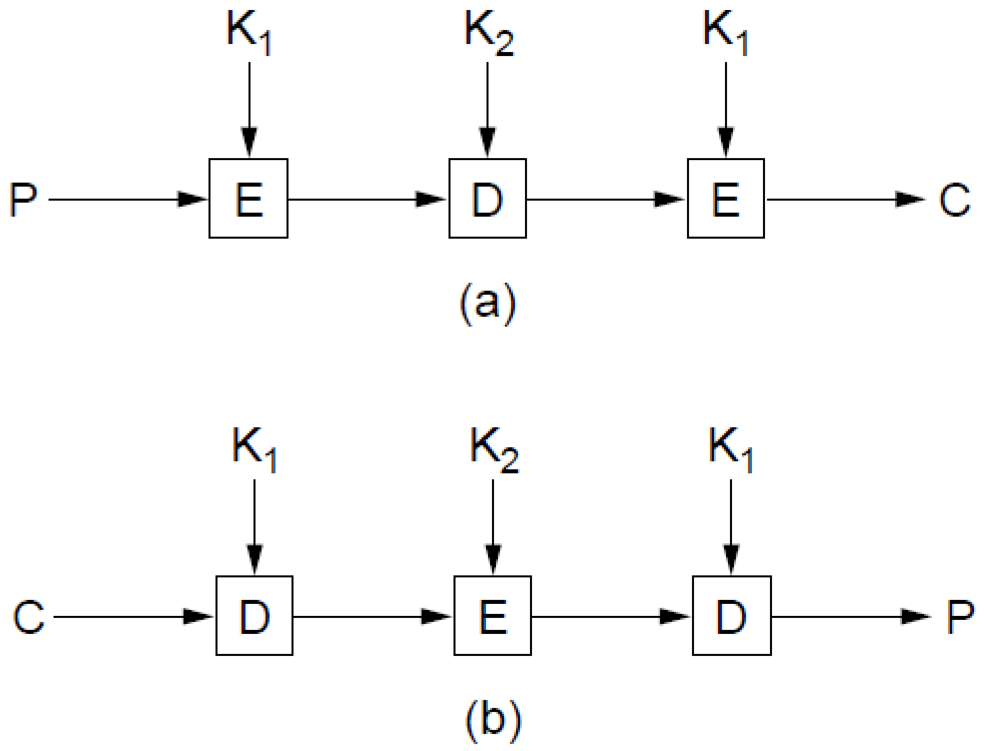


Feistel function

The data encryption standard. (a) General outline. (b) Detail of one iteration. The circled + means exclusive OR.

Computer Networks, Fifth Edition by Andrew Tanenbaum and David Wetherall, Pearson Education-Prentice Hall, 2011

Data Encryption Standard (2)



(a) Triple encryption using DES. (b) Decryption

Computer Networks, Fifth Edition by Andrew Tanenbaum and David Wetherall, Pearson Education-Prentice Hall, 2011

Real Block Ciphers: Advance Encryption System (AES)

Used to replace DES in the US.

The U.S. National Institute of Standards and Technology (NIST) call for proposals to replace DES.
Requirement:

Both software and hardware implementations must be possible.

The algorithm must be public or licensed on nondiscriminatory terms.
The algorithm must be a symmetric block cipher.
The full design must be public.

Key lengths of 128, 192, and 256 bits must be supported.

Real Block Ciphers: Advance Encryption System (AES)

5 ciphers selected out of 15 proposals submitted.

Rijndael was selected to become AES, 2001.

Rijndael (from Joan Daemen and Vincent Rijmen, 86 votes).

Serpent (from Ross Anderson, Eli Biham, and Lars Knudsen, 59 votes).

Twofish (from a team headed by Bruce Schneier, 31 votes).

RC6 (from RSA Laboratories, 23 votes).

MARS (from IBM, 13 votes).

Real Block Ciphers: Advance Encryption System (AES)

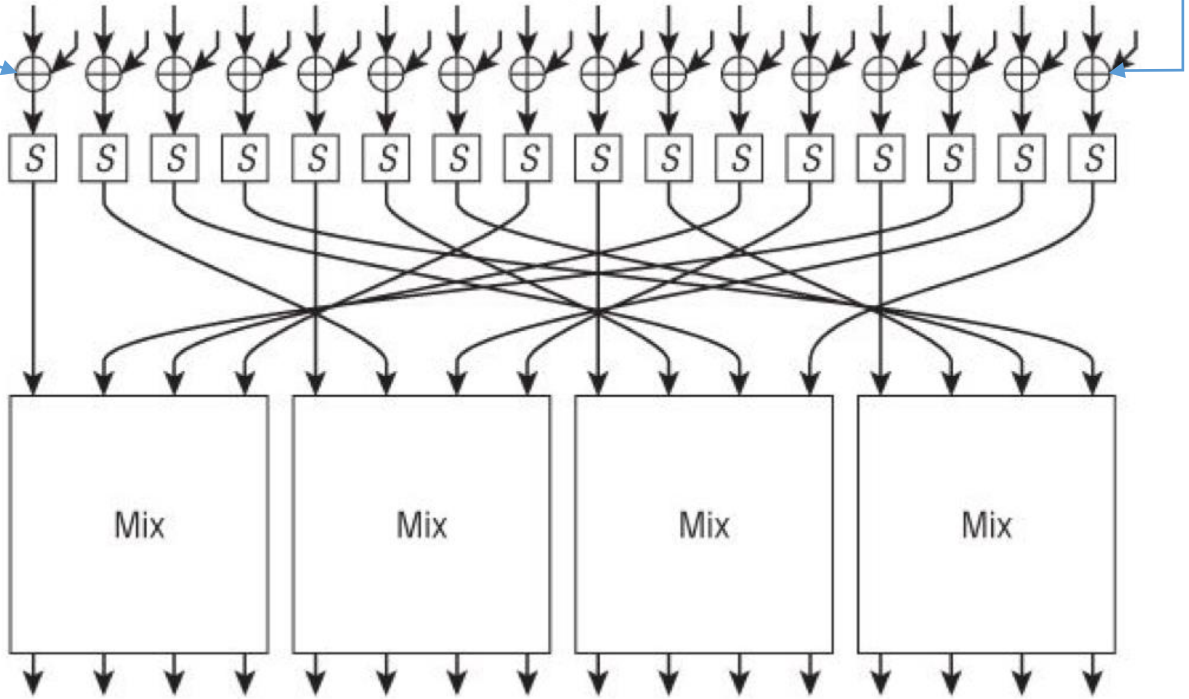
First XOR the plaintext using a 16 bytes round key

The plaintext is organized as 16 bytes (128 bits)

16 bytes are is used as an index

S-box table that maps 8-bit inputs to 8-bit outputs.

Linear mixing function



Single round, full encryption has 10-14 rounds.

Real Block Ciphers: Advance Encryption System (AES)

Single round, full encryption has 10-14 rounds.

Key size	Round
128	10
192	12
256	14

Advantages

Parallel operation to perform encryption

Clean design, separating task/functions for each part of the cipher.

Disadvantages

Due to way the decryption is done; inverse lookup table S-box and the inverse mixing operation.

Real Block Ciphers: Advance Encryption System (AES)

Attacking the cipher 3 to 4 round security margin

Key size	Round	Attacks Round
128	10	6 to 7
192	12	8
256	14	9

“Selection of Rijndael as AES relied on the assumption that future attacks would not give large improvement”

Selecting a Block Cipher

AES is recommended despite that there are know theoretical attack, not practical.

Cryptography libraries support AES.

Consideration double encryption (i.e. AES and Serpent) using two independent keys.

Using AES with 128 bit keys 16 round, 192 bit key and 20 rounds and for 256 bit keys 28 round.

Selecting a key

A suitable value is 128 bits. If so what about the collision attacks?

For a security level of *n* bits every cryptographic value should be a least *2n* bits long.

So how about a Key of 256 bits?

So design strength is 128 bits.

Bibliography

Ferguson, Niels; Schneier, Bruce; Kohno, Tadayoshi (2011-02-02). Cryptography Engineering: Design Principles and Practical Applications (p. 46). Wiley. Kindle Edition.