4 Block ciphers

■ 4.1 Definition of block cipher

Block cipher is a name for symmetric key algorithms, where the message is divided into fixed length blocks and these blocks are encrypted one at the time.

Usually the ciphertext of a block works as one input of the encryption of the following block. This is called chaining.

Block length is 64 bits (8 bytes) or nowadays more often 128 bits (16 bytes).
The key length is nowadays 128 or 256 bits depending on the algorithm.

Operation scheme of a block cipher

What is inside block ciphers ?

In his paper 1949 Claude Shannon introduced the idea of substitution - permutation networks. This idea is the basis of modern block ciphers.

Block ciphers are made of two basic operation: substitutions and permutations.
For permutations it containes Pboxes and for substitutions Sboxes.

Permutations re-order the bits.
For n bits there are n! permutations

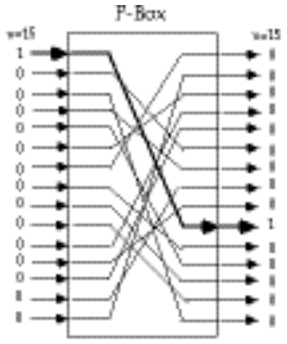


Fig 2.2 - Permutation or Transposition Function

Substitutions are defined by substitution tables called Sboxes

1) the bits are decoded to integers.
2) Integers are subsituted according to the table with other integers.
3) Finally integers are encoded back to bits.

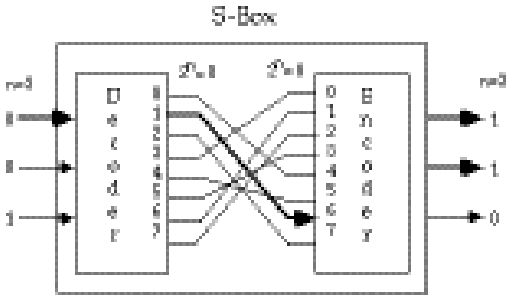


Fig 2.1 Substitution Operation

■ 4.2 History of block ciphers

1970 IBM started a project of developing a fast and secure cipher algorithm for growing needs of US administration and business. Project was led by IBM's engineer *Feistel*. The working name was *Lucifer*.

DES

At the end of Lucifer - project US National Security Agency *NSA* joined the project and they proposed and implemented some changes . The new name was *DES (Digital Encryption Standard)* .

DES has both hardware and software implementations. DES encrypts messages in 64 bit block using 64 bit (in effeect 56 bit key). The speed is more than 200 Mbs which is enough to quarantee fast banking and business applications.

DES was broken 1998. *NIST* (US institute of standards) started to look a successor for DES already at late 1980's. Nothing comparable was available, so *NIST* gave *DES* twice additional time as a US standard.

AES

NIST had DES as an official standard from 1976 to 2001, when NIST announced the winner of a competition for a new standard. Winner was *RijnDael* made by two Belgian cryptographers *Rijmen* and *Daemen*. It was given a title *AES (Advanced Encryption Standard)*

IDEA, RC5 ...

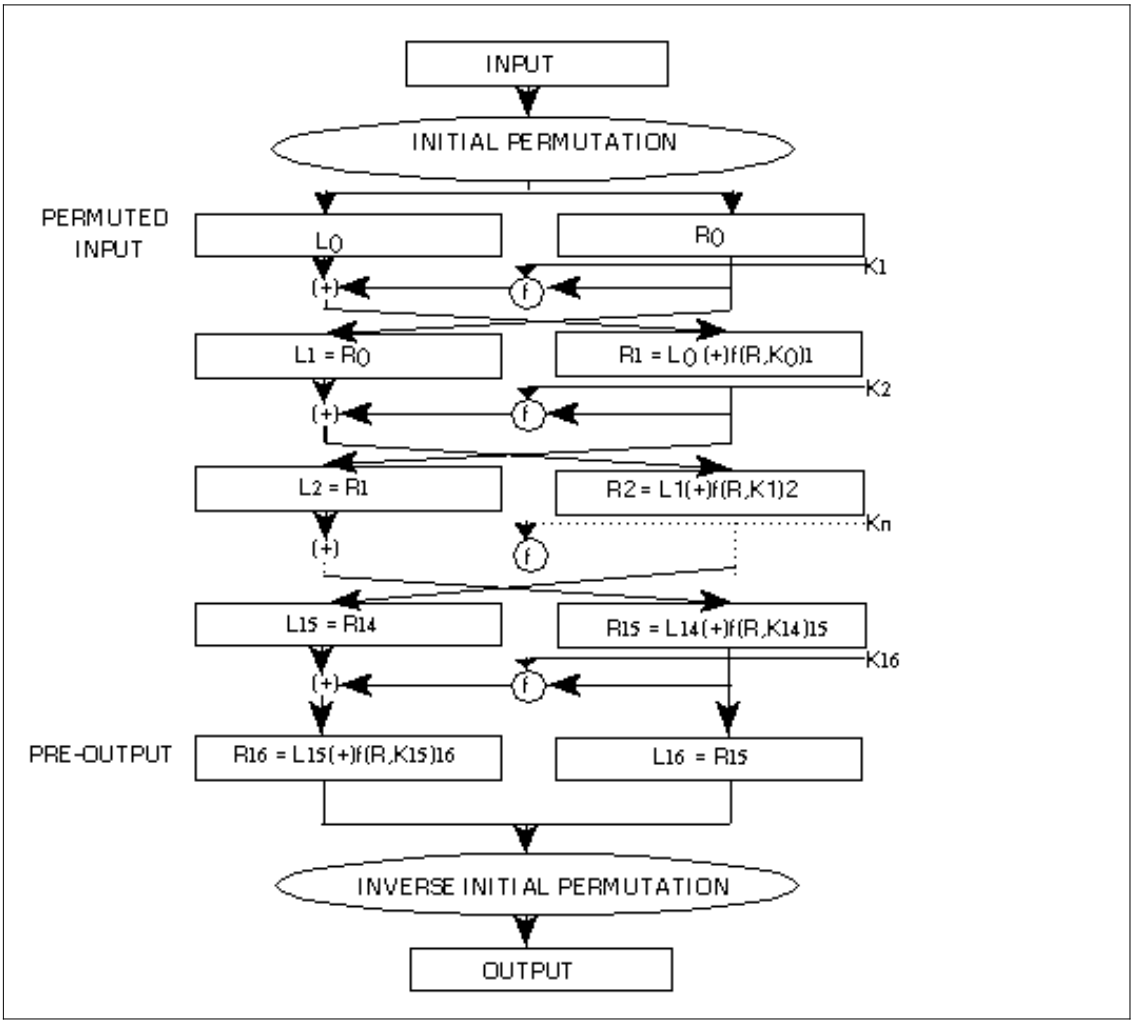
Among AES - finalists there were other good candidates: f.e IDEA and RC5. That is why RijnDaelilla has not so strong monopole position than DES had. In modern secure protocols there exists several possible cryptoalgorithms to choose. It is a choice of users for which algorithm they configure the system.

■ 4.3 DES

DES developers were engineers, not mathematicians. This is seen in the algorithm.

It is based on known, fast techniques of microchips, *permutations*, *shifting of bit registers* , and *Lookup tables called Sboxes.*

DES operation chart



DES in steps

1. Subkey generations
Each user has an 64 bit (effectively 56 bit) key, which DES uses for generation of 16 subkeys using permutations and rotations of bits .

2. **Input** is 64 bit block.
Message is divided into 64 bit blocks, which are encrypted DES one at a time using chaining.

3. **Encryption**
A) First an **initial permutation** IP is performed
B) The follows so called **Feistels structure:**
The block is divided into two halfs.
Then follows 16 rounds, in which the right half is moved to the left and the nwe right half is calculated using Feistel's function f from the prvious left half and the subkey of the round. The f function uses Lookup tables called S -boxes.
C) At the end **inverse permutation of IP** ***is performed***

DES algorithm's detailed description is found at http://www.aci.net/kalliste/des.htm

DES was never ment to be public, but it leaked out like later did GSM cipher A5. This leak gave valuable information for cryptanalysts and helped the cryptanalysis to develop new attack methods.

The *Kerckhoff principle was forgotten*
"Cryptosystem should be secure even if all except the key is public".

(Auguste Kerckhoff 1835 - 1903 , Dutch linquistic and cryptographer)

■ 4.4 Modes of Operation

DES as also other ciphers, can be used in four different modes of operation :

1) ECB Electronic Codebook
The blocks are encrypted independently. If the same block is repeated, the cipher is same.
This mode of operation is not safe.

2) CBC Cipher Block Chaining
The ciphertext of the previous block is part of the input of encryption of the next block.
Every block influences the ciphers of the following blocks. So two identical blocks have different ciphertexts in different parts of the message.

3) CFB Cipher FeedBack
The cipher of a block influences the following ciphers, but in slightly different way than in CBC . This mode can be regarded as a stream cipher mode.

4) OFB Output FeedBack
Can also be regarded as stream cipher mode, a version of Vernam cipher.

■ 4.5 DES security

1. It is said that the short effective key size, 56 bits, is due to NSA. The reason for reserving 8 bits from original 64 for parity check has been doubted. The real motive for 56 bit is said to be a need to listen telecommunication.
(In 2005 only 80 bits quarantees safety against Brute Force)

2. The f - functions include S-boxes, in which bytes (8 bit blocks) are replaced with other bits. Bilham and Shamir developed differential analysis for cryptanalysis of DES. They tested a lot of ciphertexts and examined how one bit changes in the message effected the output.
They came into conclusion that S -boxes did not work in the best possible way. Outputs were not random enough. The effective key space was really only 2^{47}. Some writers claim that the original IBM S-boxes were changed to weaker ones according to NSA:s wishes.

3. As mentioned S-boxes were intentended to be kept secret . Now one can read descriptions of them in Internet and people (including hackers) can write their own DES code. Everyone has posiibility to look for weaknesses in DES.

Bruce Schneier writes:
"Off the record, NSA has characterized DES as one of their biggest mistakes. If they knew the details would be released so that people could write software, they would never have agreed to it. DES did more to galvanize the field of cryptanalysis than anything else. Now there was an algorithm to study: one that the NSA said was secure."

4. Another method - linear cryptoanalysis was developed in 1992 *by Matsui*. In this method the encryyption function is approximated with an *affine function*.

5. DES has four weak keys, which make the cipher easy to break. The weak key produces identical subkeys.

- **Triple DES (3DES)**

DES key space is 2^{56} , which cannot resist Brute Force - attack. In late 1990's one could break DES using 10000$ equipment.
In lack of a good successor DES was given more time. Using three DES chips (Tripple DES) with different keys, one could increase the key space to resist Brute Force. 3DES was published 1999 by IBM. Algorithm can be presented as

$$c = DES_{k3}(DES^{-1}{}_{k2}\ (DES_{k1}\ (m))) \qquad \text{(EDE -mode)}$$

This means that first a DES - encryption with key k1 is performed, then DES - decryption with key k2 and finally DES -encryption with key k3.
3DES can also be used in EEE -mode, where also the second operation is DES -encryption.

3DES security:
Key size k = 3 * 56 = 168 bits . Theoretically this means a keyspace of 2^{168} , but there exists attacks against 3DES , which reduce the effective keys space to 2^{112} , even 2^{90} . However this is enough to resist Brute Force.

3DES is too slow in 32 -bit operation systems. It was not the solution.

- **4.6 AES**

NIST wanted in the late 1990's to find a successor for DES as an US standard. It declared an open competition in 1997 for a new standards. From more that ten candidates in 2001 NIST chose the winner: *Rijndael*. It was developed by two Belgians: Daemen and Rijmen. NIST gave the winner the name AES (Advanced Encryption Standard).

AES is a network of substitutions and permutations. Like DES it has several phases and rounds. **SubBytes** - phase uses S-boxes to replace 8 bit blocks with other 8 bit blocks. In **Shift-Row**-phase rotations of bits are made to the bit sequences. In **MixColumns**- phase two way linear transformations are done to the columns of bits. In this the theory of Finite Fields is applied. Algorithm has several rounds which use subkeys like in DES.
(See http://en.wikipedia.org/wiki/AES)

AES is fast in hardware and software implementations. It is easy to implement and requires only little memory. In 2005 transition from DES to AES is almost in the end. AES has no royalty payments - so it is free.

■ 4.7 AES security

No successfull attacks against AES has been developed. 3 key lengths can be chosen: 128 , 196 and 256 bits. According to NIST up to SECRET - level all key lengths are sage, TOP SECRET documents require 196 bit key.

Some cryptographres doubt AES. An attack was made, in which 200 million chosen messages were encrypted with AES in laboratory conditions. AES was broken, but this has nothing to do with real life security.

■ 4.8 Other block ciphers

The ministry of finance in Finland recommends following block ciphers to be used in Finland: IDEA, Blowfish, Twofish, RC5.

IDEA is chosen as the block cipher of PGP (Pretty Good Privacy), which is a popular freeware cryptosystem. Latest versions of PGP however contained a variety of block ciphers to choose.

Link: http://www.aci.net/kalliste/des.htm

■ 4.9 Other uses of block ciphers

UNIX password files

In UNIX operation system the passwords are encrypted with DES. The user password acts as the encryption key and the message block is the same for all users. The output of DES is the encrypted password, which is stored to the file /ect/passwd.

Random number generation

DES output fulfills quite well the statistical requirements for pseudorandomness. It can be used to produce random bit sequences.