SNS COLLEGE OF ENGINEERING

Kurumbapalayam (Po), Coimbatore – 641 107

An Autonomous Institution

Accredited by NAAC – UGC with 'A' Grade

Approved by AICTE, New Delhi & Affiliated to Anna University, Chennai

19CS503

CRYPTOGRAPHY AND NETWORK SECURITY

Block cipher design principles, Block cipher mode of operation

By

M.Kanchana

Assistant Professor/CSE

Block cipher design principles

There are three critical aspects of block cipher design:

1. Number of rounds,
2. Design of the function F
3. Key scheduling.

Block cipher design principles

Number of Rounds

- When the greater the number of rounds, the more difficult it is to perform cryptanalysis, even for a relatively weak F.
- The number of rounds is chosen so that known cryptanalytic efforts require greater effort than a simple brute-force key search attack
- When round DES S= 16, a differential cryptanalysis attack is slightly less efficient than brute force, the differential cryptanalysis attack requires 255 operations.
- It makes it easy to judge the strength of an algorithm and to compare different algorithms.

1.

Block cipher design principles

Design of Function F

Criteria needed for F,

- It must be difficult to “unscramble” the substitution performed by F.
- The function should satisfy strict avalanche criterion (SAC) which states that any output bit j of an S-box should change with probability 1/2 when any single input bit i is inverted for all i, j.
- The function should satisfy bit independence criterion(BIC), which states that output bits j and k should change independently when any single input bit i is inverted for all i, j, and k.

Block cipher design principles

Key Schedule Algorithm

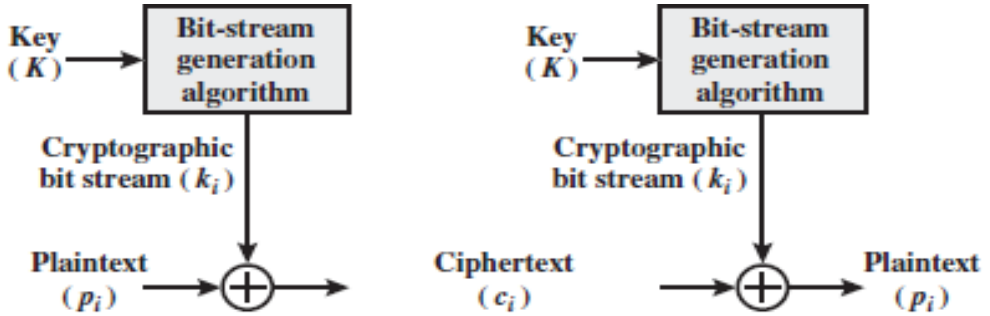
The key is used to generate one sub key for each round.The sub keys to maximize the difficulty of deducing individual sub keys and the difficulty of working back to the main key.

Block cipher design principles

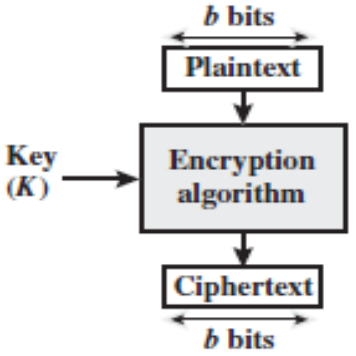
Stream Cipher and Block Cipher

A stream cipher is one that encrypts a digital data stream one bit or one byte at a time. E.g, vigenere cipher.
A block cipher is one in which a block of plaintext is treated as a whole and used to produce a cipher text block of equal length. Typically, a block size of 64 or 128 bits is used.

Block cipher design principles



(a) Stream cipher using algorithmic bit-stream generator

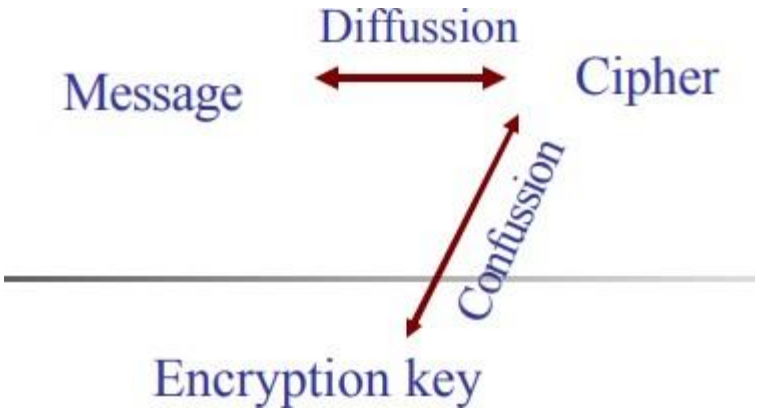


(b) Block cipher

Block cipher design principles

Two methods for frustrating statistical cryptanalysis are:

- Diffusion – Each plaintext digit affects many ciphertext digits, or each ciphertext digit is affected by many plaintext digits.
- Confusion – Make the statistical relationship between a plaintext and the corresponding ciphertext as complex as possible in order to thread attempts to deduce the key



BLOCK CIPHER MODES OF OPERATION

- Block Cipher is the basic building block to provide data security.
- To apply the block cipher to various applications, NIST has proposed 4 modes of operation. The block cipher is used to enhance the security of the encryption algorithm

Multiple Encryption and Triple DES

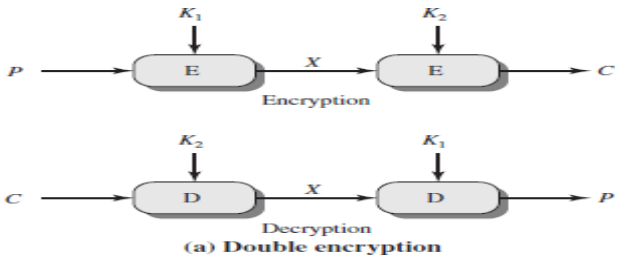
The vulnerability of DES to a brute-force attack has been detected by using two approaches

1. One approach is to design a completely new algorithm, of which AES is a prime example
2. Another alternative, which would preserve the existing investment in software and equipment, is to use multiple encryptions with DES and multiple keys.

BLOCK CIPHER MODES OF OPERATION

Double DES

The simplest form of multiple encryptions has two encryption stages and two keys. Given a plaintext P and two encryption keys K1 and K2, cipher text C is generated as



(a) Double encryption

$$C = \mathrm{E}(K_2, \mathrm{E}(K_1, P))$$

$$P = \mathrm{D}(K_1, \mathrm{D}(K_2, C))$$

$$\mathrm{E}(K_2, \mathrm{E}(K_1, P)) = \mathrm{E}(K_3, P)$$

$$C = \mathrm{E}(K_2, \mathrm{E}(K_1, P))$$

$$X = \mathrm{E}(K_1, P) = \mathrm{D}(K_2, C)$$


SNS COLLEGE OF ENGINEERING
COIMBATORE-107


sns
INSTITUTIONS

Thank You