[CS304] Introduction to Cryptography and Network Security

Course Instructor: Dr. Dibyendu Roy
Scribed by: Dipean Dasgupta (202151188)

Winter 2023-2024
Lecture (Week 2)

1 Hill Cipher

Block ciphers, such as the Hill cipher, are traditional symmetric-key cryptography algorithms. The Hill cipher uses matrix multiplication to convert blocks of plaintext letters into ciphertext. The Hill cipher's primary characteristic is its encryption and decryption methods, which rely on linear algebraic methods.
The secret key is a square matrix which is represented by $K = (a_{ij})_{n\times n}$; invertible matrix.
Let m be a positive integer, and define $P = C = \mathbb{Z}_{26}$. The idea is to take m linear combinations of the m alphabetic characters in one plaintext element, thus producing the m alphabetic characters in one ciphertext element.

$$\text{M= } m_1 m_2 \dots m_n \rightarrow \text{plaintext}$$

ENCRYPTION:

Algo: C= A.M; A=secret key, M=Plaintext, C=CipherText

$$C_{ik} = \sum_{j=1}^{n} a_{i,j} m_{j,k}$$

DECRYPTION:

$$M = K^{-1} \cdot C$$

Some other types of symmetric cipher include:

- **Block Cipher**
- **Stream Cipher**

2 Block Cipher

A block cipher is a type of symmetric key cryptography technique that uses a single key to individually alter each fixed-size block of data. Block ciphers process one block of data at a time, as opposed to stream ciphers, which encrypt data bit by bit. One essential feature of a block cipher is its block size, which is usually expressed in bits.
Let C be CipherText and M be the plaintext. so,

$$M = M_o||M_1||M_2||\dots M_n$$

So, the Encryption function becomes:
$ENC = M.K$
ENCRYPTION:

$$C = ENC(M_o, K)||ENC(M_1, K)||ENC(M_2, K)||\dots ENC(M_n, K)$$
$$C = C_o||C_1||C_2||\dots C_n$$
$$C_i = (m_i, K)$$

DECRYPTION:

$$M = DEC(C_o, K)||DEC(C_1, K)||DEC(C_2, K)||\dots DEC(C_n, K)$$

3 Product Cipher:

A product cipher is a cryptographic construction that builds a more reliable and secure encryption system by combining several cryptographic algorithms or components in a certain way. The purpose of combining various cryptographic primitives is to increase security.

There are 2 main types of product cipher which are:

- **Substitution-Permutation Networks (SPN)**
- **Fiestel Network**

Substitution-Permutation Networks:
A popular product cipher structure called SPN combines permutation and substitution operations throughout several rounds. Modern block ciphers such as the Advanced Encryption Standard (AES) frequently use it. An SPN structure uses a series of rounds of substitution and permutation operations on the plaintext, employing distinct subkeys that are obtained from the primary key in each round.

Let l and m be positive integers. A plaintext(PT) and ciphertext(CT) will both be binary vectors of length lm (i.e., lm is the block length of the cipher). An SPN is built from two components, which are denoted π_s and π_p.

$$\pi_s : \{0,1\}^l \to \{0,1\}^l$$
$$\pi_p : \{1,\dots,lm\} \to \{1,\dots,lm\}$$

π_s=permutation of the 2^l bitstrings of length l
π_p=permutation of integers $1,\dots,lm$.
π_s is also known as an S-box.It is used to replace l bits with a different set of l bits.
π_p, is to permute lm bits through changing their order.

Given an lm-bit binary string, say $x = (x_1,\dots,x_{lm})$, we can regard x as the concatenation of m l-bit substrings, which we denote $x,\dots,x^{<m>}$. Thus

$$x = x||\dots||x^{<m>}.$$

Fiestel Network:
Another kind of product cipher structure is the Feistel network, which is most famously employed in the Data Encryption Standard (DES). The input block of a Feistel network is split in half, and one half is subjected to a function operation, which usually involves substitution and permutation. Before proceeding on to the next round, the outcome is combined with the other half.

Let the Plaintext is of 2n bits. so it is divided into 2parts of n. Let, F be the round function and

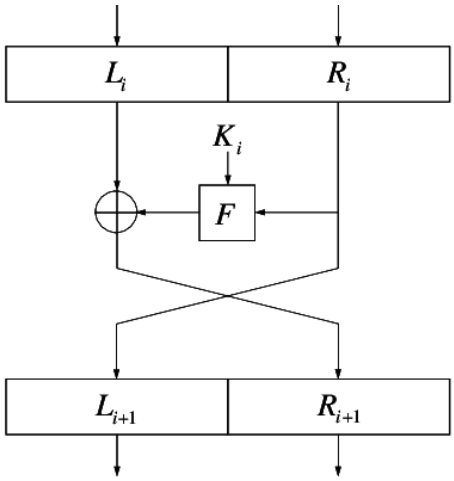

Figure: Single Round Fiestel Network
Source:ResearchGate

two equal parts are L_o and R_o; C be the Ciphertext

ENCRYPTION:

$$\text{For each round } i = 0, 1, \ldots, n \text{ compute}$$
$$L_{i+1} = R_i$$
$$R_{i+1} = L_i \oplus F(R_i, K_i)$$
$$C = (R_{n+1}, L_{n+1})$$

DECRYPTION:

$$\text{for } i = n, n-1, \ldots, 0.$$
$$R_i = L_{i+1},$$
$$L_i = R_{i+1} \oplus F(L_{i+1}, K_i)$$
$$P = (R_0, L_o)$$

4 Iterated Block Cipher:

A particular kind of block cipher design known as an iterated block cipher comprises encrypting data using several rounds of the same basic encryption operation. Using a round key that is obtained from the primary encryption key, each round involves performing a set of transformation functions on the input data, which is usually referred to as the plaintext or the intermediate ciphertext. Each round's outcome feeds into the next one, and the process continues a certain number of

times.

Let F be the round function and K be set of keys $K_1, K_2 \dots K_n$, Plaintext P and Ciphertext C. So now lets generate ciphertext using 2 round Iterated Block Cipher(IBC).
For two rounds, $G(K) = K_1, K_2$
ENCRYPTION:

$$C_1 = F(K_1, P)$$
$$C = F(K_2, C_1)$$

DECRYPTION:

$$C_1 = F^{-1}(C, K_2)$$
$$P = F^{-1}(C_1, K_1)$$

Data Encryption Standard:
A symmetric-key block cipher developed by IBM, the Data Encryption Standard (DES) was extensively used to protect electronic data until the National Institute of Standards and Technology (NIST) formally deprecated it in 2005 because of its tiny key size. DES was a key contributor to the creation of contemporary encryption standards and is still regarded as a significant historical cryptographic algorithm even though it has been deprecated.

Block Size: **64-bit** fixed-size data blocks for operation.
Key Size: **56 bits + 8 parity bits**. total 64.
Network Structure: The network structure of DES is Feistel.A function including key mixing, substitution (S-boxes), permutation (P-boxes), and XOR operations is applied alternately to the two halves of 32 bits.
Rounds: Total **16** rounds for both encryption and decryption.

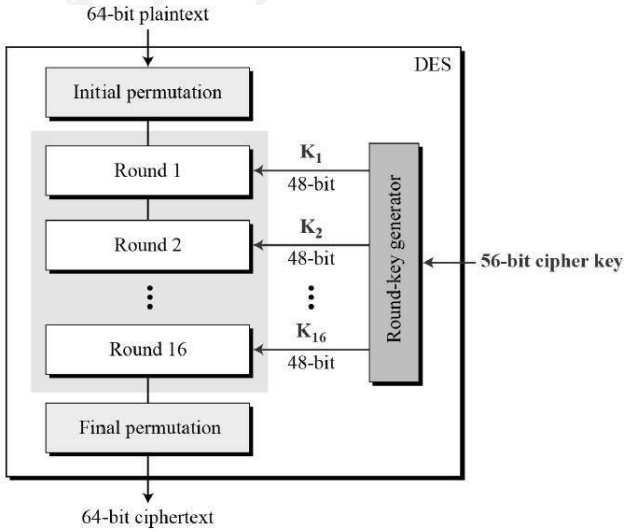

Figure:DES Encryption
Source:TutorialsPoint

The Internal Permutation is mapped= $IP : \{0,1\}^{64} \rightarrow \{0,1\}^{64}$
In the 1st Round: $f : \{0,1\}^{32} * \{0,1\}^{48} \rightarrow \{0,1\}^{32}$
Swapping and IP is done in 1st round.
In the last round, Non-swapping and IP^{-1} are executed.