[CS304] Introduction to Cryptography and Network Security

Course Instructor: Dr. Dibyendu Roy — Winter 2023-2024

Scribed by: Archit Verma (202151192) — Lecture (Week 2)

Hill Cipher

The Hill Cipher is a polygraphic substitution cipher based on linear algebra. It uses a key matrix A to encrypt blocks of plaintext M. The encryption C is calculated by $C = A \cdot M$, and decryption involves using the inverse of the key matrix.

Encryption Process

To encrypt a block of plaintext $M = \begin{bmatrix} m_1 \\ m_2 \\ \vdots \\ m_n \end{bmatrix}$ using the Hill Cipher with key matrix $A = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{bmatrix}$, the...

$$C = A \cdot M = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{bmatrix} \cdot \begin{bmatrix} m_1 \\ m_2 \\ \vdots \\ m_n \end{bmatrix} = \begin{bmatrix} c_1 \\ c_2 \\ \vdots \\ c_n \end{bmatrix}$$

Decryption Process

The decryption of the ciphertext C involves multiplying it by the inverse of the key matrix A^{-1}. The original plaintext M' is obtained as follows:

$$M' = A^{-1} \cdot C = \begin{bmatrix} a_{11}^{-1} & a_{12}^{-1} & \cdots & a_{1n}^{-1} \\ a_{21}^{-1} & a_{22}^{-1} & \cdots & a_{2n}^{-1} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1}^{-1} & a_{n2}^{-1} & \cdots & a_{nn}^{-1} \end{bmatrix} \cdot \begin{bmatrix} c_1 \\ c_2 \\ \vdots \\ c_n \end{bmatrix} = \begin{bmatrix} m'_1 \\ m'_2 \\ \vdots \\ m'_n \end{bmatrix}$$

Block Cipher

In block ciphers, plaintext is divided into fixed-size blocks. The encryption of each block M_i with a key k results in a ciphertext block C_i. The overall ciphertext C is the concatenation of individual ciphertext blocks.

Encryption Process

Let $M = m_0 \| m_1 \| \ldots \| m_n$ be the plaintext divided into blocks. The encryption process is given by:

$$C = \mathrm{Enc}(m_0, k) \| \mathrm{Enc}(m_1, k) \| \ldots \| \mathrm{Enc}(m_n, k)$$

Decryption Process

Similarly, decryption involves decrypting each block individually:

$$M = \text{Dec}(\text{Enc}(m_0, k), k) \| \text{Dec}(\text{Enc}(m_1, k), k) \| \ldots \| \text{Dec}(\text{Enc}(m_n, k), k)$$

ECB Mode of Operation

The Electronic Codebook (ECB) mode is the simplest mode of operation for a block cipher. Each block of plaintext is independently encrypted.

Encryption Process

For ECB mode, each plaintext block M_i is independently encrypted:

$$C_i = \text{Enc}(M_i, k) \quad \text{for each } i$$

Decryption Process

Similarly, decryption involves decrypting each ciphertext block independently:

$$M_i = \text{Dec}(C_i, k) \quad \text{for each } i$$

Product Cipher

A product cipher combines multiple simple ciphers to create a more secure encryption. It involves using different encryption techniques in a sequence or parallel.

Encryption Process

Let $S : \{0,1\}^n \to \{0,1\}^n$ be a substitution cipher. The product cipher is obtained by combining multiple encryption techniques:

$$C = S(E_1(S^{-1}(E_2(S(E_3(\ldots M) \ldots)))))$$

Feistel Cipher

A Feistel Cipher is a symmetric structure used in block cipher design. It operates on blocks of data with repeated rounds.

Encryption Process

In a Feistel Cipher, a block M is divided into two halves L and R. The encryption process is repeated for several rounds:

$$L_{i+1} = R_i$$
$$R_{i+1} = L_i \oplus F(R_i, K_i)$$

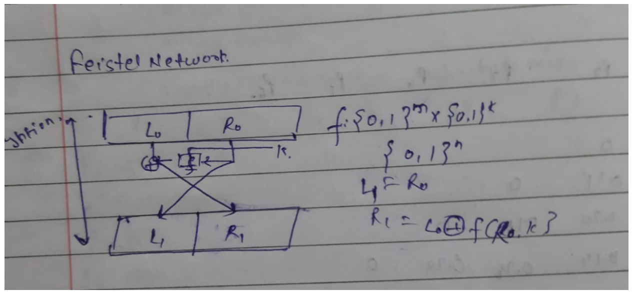

Figure 1: feistel

Iterated Block Cipher

An iterated block cipher involves sequential repetition of an internal function, typically called the round function. It has parameters such as the number of rounds r, block size n, and key size k.

Encryption Process

The encryption process involves iterating the round function r times:

$$C = \text{Round}_r(\ldots \text{Round}_2(\text{Round}_1(M, K_1), K_2) \ldots, K_r)$$

Decryption Process

The decryption process is the reverse of the encryption process:

$$M = \text{Round}_1^{-1}(\ldots \text{Round}_2^{-1}(\text{Round}_r^{-1}(C, K_r), K_{r-1}) \ldots, K_1)$$

Data Encryption Standard (DES)

The Data Encryption Standard (DES) is a symmetric key algorithm designed by IBM. It uses a 64-bit secret key and operates on 64-bit blocks of plaintext.

Key Scheduling Algorithm

DES involves a key scheduling algorithm to generate subkeys for each round.

Encryption Process

The DES encryption process involves 16 rounds of permutation, substitution, and key mixing.

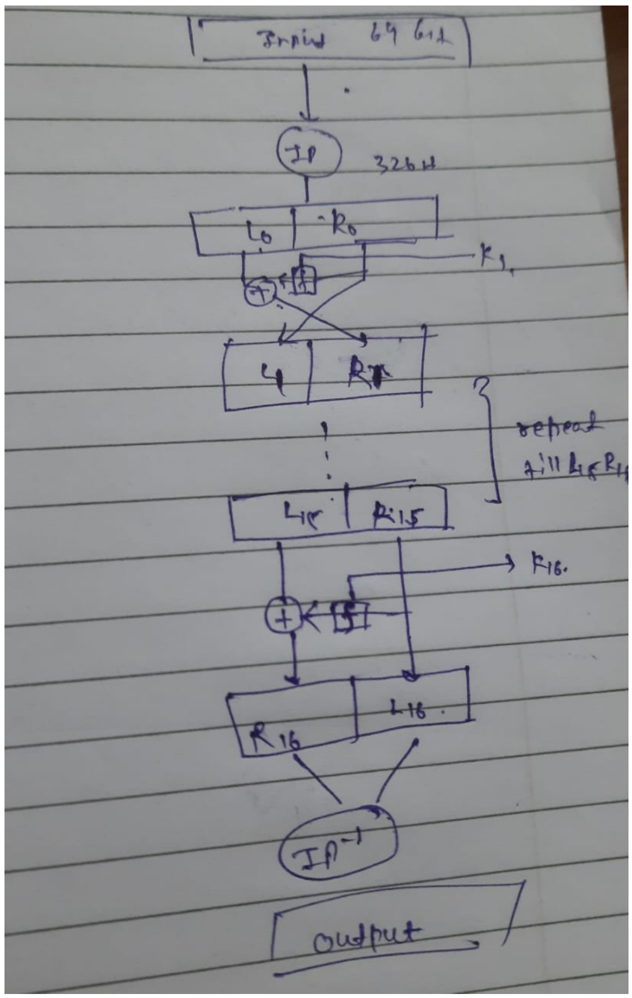

Figure 2: DES