[CS304] Introduction to Cryptography and Network Security

Course Instructor: Dr. Dibyendu Roy
Scribed by: Aniruddh Modi (202151022)

Winter 2023-2024
Lecture 3 (Week 2)

1 Lecture 3

1.1 Hill Cipher

It is a substitution based cipher which involves use of linear algebra for cryptographic operations. For encryption, we divide our message in blocks and use an invertible matrix as a key.

1.1.1 Encryption

$$E(P, K) = (P \times K) \mod 26$$

where P is plain text vector and K is the key matrix.

1.1.2 Decryption

$$D(C, K) = (C \times K^{-1}) \mod 26$$

where C is cipher text vector and K is the key matrix.

1.2 Block Cipher

It comes under a class of symmetric key cryptography which involved breaking down the plain text into blocks consisting of multiple characters. Common block sizes include 64 bits, 128 bits and 256 bits.

$$M = M_0||M_1||...||M_n$$

here length of M_i is m. If suppose l is the length of M, then

$$l = m \times n$$

If this is not satisfied, we add a padding after our text M, which (if not predfined) is usually r 0s or r 1s for optimal division of the blocks.

$$(l + r) \mod n = 0$$

1.2.1 Encryption

$$E(M_i, K) = C_i$$

Then,

$$C = C_0||C_1||...||C_n$$

1.2.2 Decryption

$$D(C_i, K) = M_i$$

Then,

$$M = M_0||M_1||...||M_n$$

1.3 Product Cipher

It combines 2 or more transformations in a manner that the resulting cipher is more secure. Under it comes the following Ciphers :

1.3.1 Substitution Permutation Network

It is a type of block cipher which applies combination of substitution and permutation ciphers on the text to enhance the security of the system.

$$S : \{0,1\}^n \rightarrow \{0,1\}^m$$

$$P : \{0,1\}^{m \times r} \rightarrow \{0,1\}^{m \times r}$$

It will take r block of the plain text and apply S on each of the r blocks.
Later, it will take the resultant $m \times r$ blocks and apply P on it.
The resultant cipher text is of length $m \times r$ after the first round of encryption.

1.3.2 Feistel Network

It is also a type of block cipher in which the plain text is divided into two equal halves. This means that the length must be even. In the case of odd length, we add a zero0 at last to make the length even. For both encryption and decryption, we use the following function :

$$F : \{0,1\}^n \times \{0,1\}^m \rightarrow \{0,1\}^n$$

where m and n are length of key and text respectively.

1.3.2.1 Encryption To encrypt the two halves, we perform following opeartions :

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

1.3.2.2 Decryption To decrypt the two halves, we perform following opeartions :

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

1.4 Iterated Block Cipher

It involves the sequential repetition of a round function. The function takes as parameters the result of previous round and the current round key.

1.4.1 Encryption

First multiple keys K_is are generated from the initial key K. Using these keys, we define result of i_{th} round as

$$C_i = F(C_{i-1}, K_i)$$

and $C_0 = P$.

1.4.2 Decryption

For decryption, we use the following algorithm.

$$C_i = F^{-1}(K_i, C_{i+1})$$

1.5 Data Encryption Standard

It's the most widely used block cipher globally, accepted by NBS (now NIST) in 1977. This cipher protects 64 bits of data using a 56-bit key and follows a Feistel cipher design with 16 processing rounds. The key is 56 bits, with 8 parity check bits, one bit inserted after every 7 bits. The 64-bit key, including parity check bits, is divided into 16 sub-keys

1.5.1 Encryption

1. We take a 64-bit plaintext block and perform a permutation on it using the Initial Permutation Function.
2. Divide the result in two halves (Left and Right).
3. Perform 16 rounds of encryption on both the halves separately.
4. Join both the halves and perform the Final Permutation Function on the combined block.

1.5.2 Decryption

1. We take a 64-bit plaintext block and perform the inverse of final permutation on it.
2. Divide the result in two halves (Left and Right).
3. Perform 16 rounds of decryption on both the halves separately.
4. Join both the halves and perform the inverse of the initial permutation Function on the combined block.

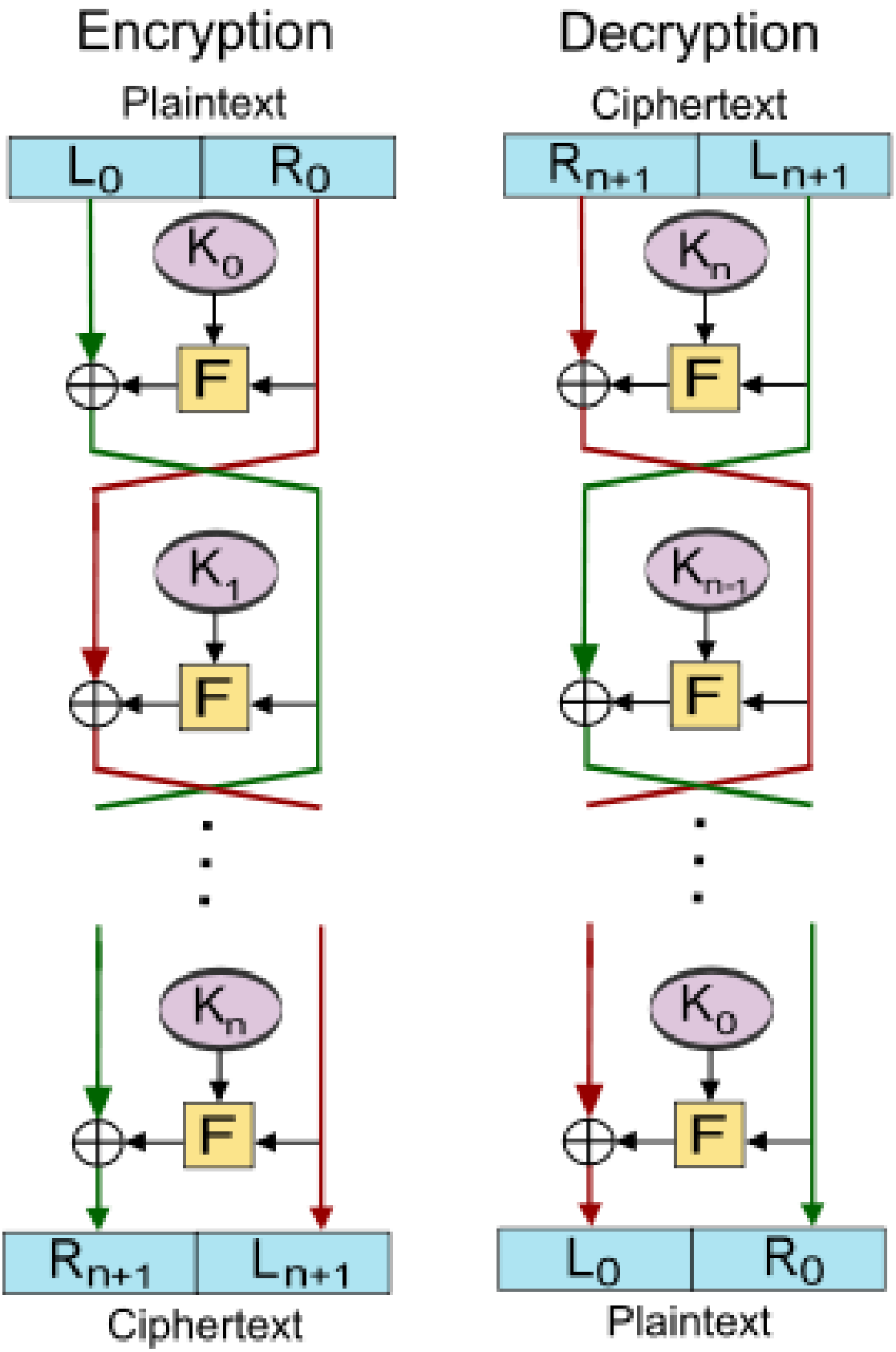

Figure 1: Feistel Network

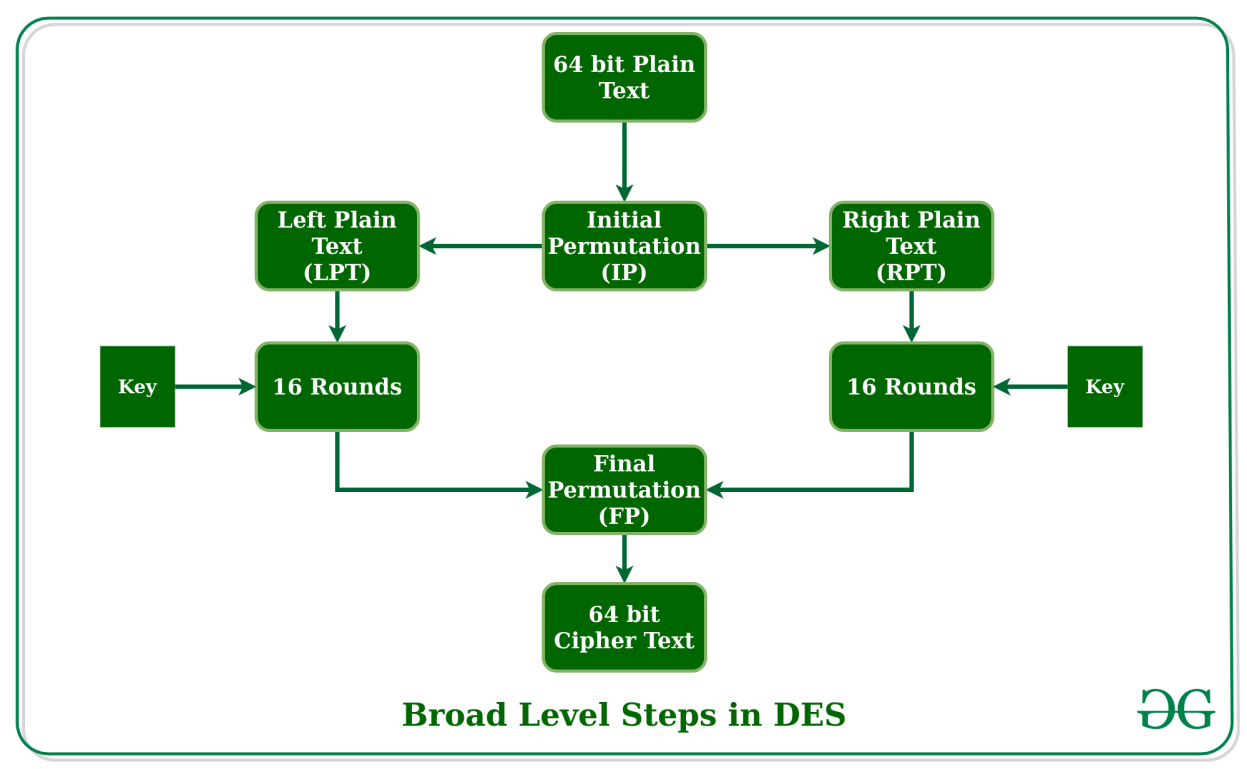
64 bit Plain Text
Left Plain Text (LPT)
Initial Permutation (IP)
Right Plain Text (RPT)
Key
16 Rounds
16 Rounds
Key
Final Permutation (FP)
64 bit Cipher Text
Broad Level Steps in DES

Figure 2: DES