Unit 2

Symmetric Ciphers

(10 Hours)

2.4. Feistel Cipher Structure, Substitution Permutation Network (SPN)

2.5. Data Encryption Standards (DES), Double DES, Triple DES

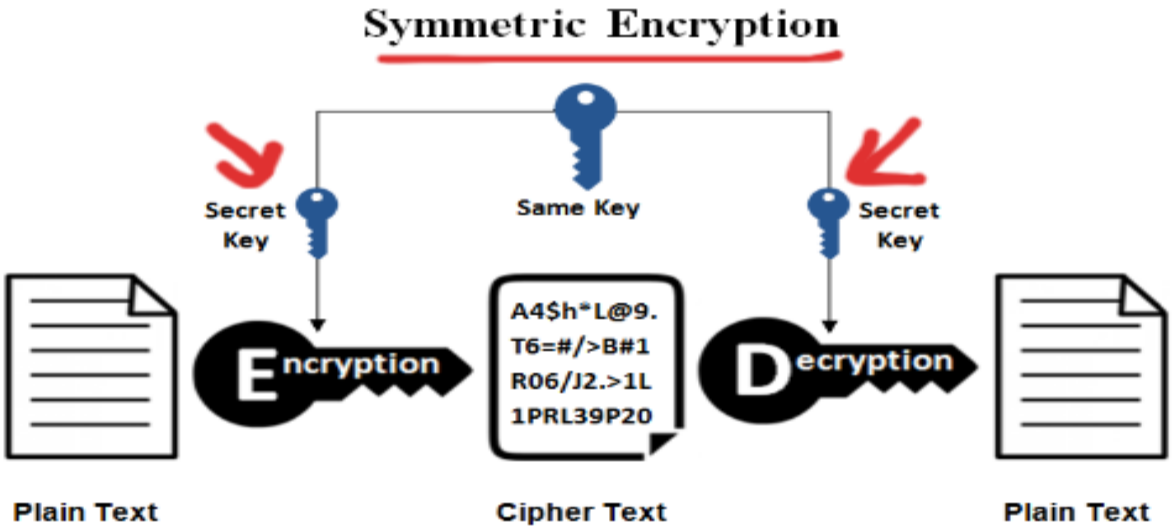
2.6. Finite Fields: Groups Rings, Fields, Modular Arithmetic, Euclidean Algorithm, Galois Fields (GF(p) & GF(2n)), Polynomial Arithmetic

2.7. International Data Encryption Standard (IDEA)

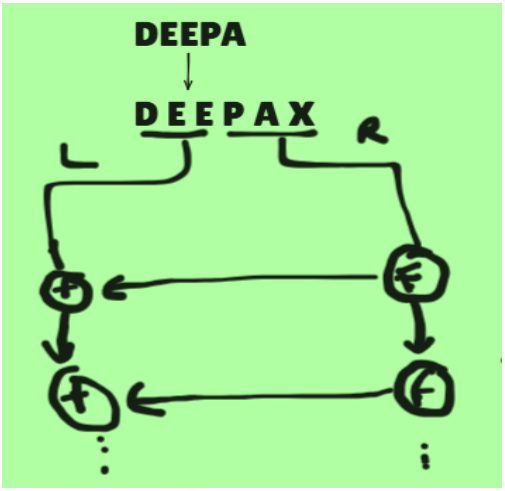
2.8. Advanced Encryption Standards (AES) Cipher

2.9. Modes of Block Cipher Encryptions (Electronic Code Book, Cipher Block Chaining, Cipher Feedback Mode, Output Feedback Mode, Counter Mode)

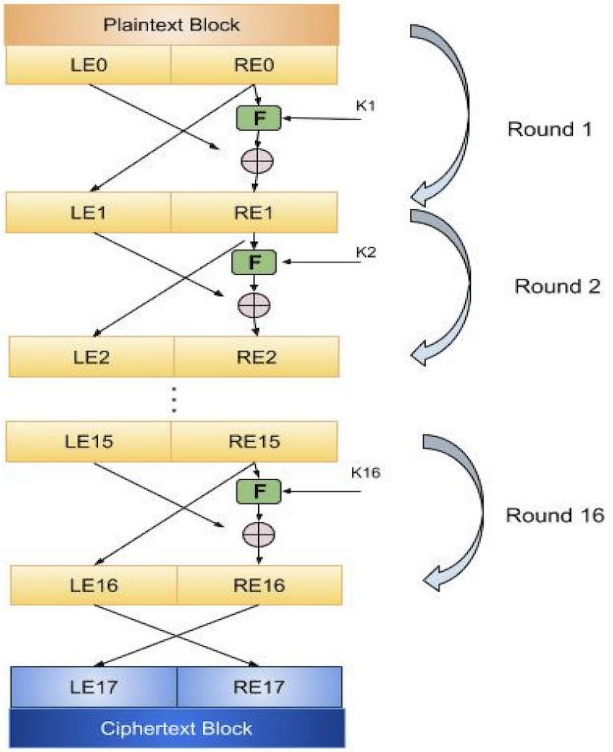
Sanjeev Thapa, Er. DevOps, SRE, CKA, RHCSA, RHCE, RHCSA-Openstack, MTCNA, MTCTCE, UBSRS, HEv6, Research Evangelist



Feistel Cipher Structure



- Feistel Cipher is not a specific scheme of block cipher. It is a design model from which many different block ciphers are derived. DES is just one example of a Feistel Cipher.
- A cryptographic system based on Feistel cipher structure uses the same algorithm for both encryption and decryption.
- Encryption Process
  - The encryption process uses the Feistel structure consisting multiple rounds of processing of the plaintext, each round consisting of a substitution step followed by a permutation step.



- The input block to each round is divided into two halves that can be denoted as L and R for the left half and the right half.
- In each round, the right half of the block, R, goes through unchanged. But the left half, L, goes through an operation that depends on R and the encryption key. First, we apply an encrypting function f that takes two input − the key K and R. The function produces the output f(R,K). Then, we XOR the output of the mathematical function with L.

- In real implementation of the Feistel Cipher, such as DES, instead of using the whole encryption key during each round, a round-dependent key (a subkey) is derived from the encryption key. This means that each round uses a different key, although all these subkeys are related to the original key.
- The permutation step at the end of each round swaps the modified L and unmodified R. Therefore, the L for the next round would be R of the current round. And R for the next round be the output L of the current round.
- Above substitution and permutation steps form a round. The number of rounds are specified by the algorithm design.
- Once the last round is completed then the two sub blocks, R and L are concatenated in this order to form the ciphertext block.

The difficult part of designing a Feistel Cipher is selection of round function f. In order to be unbreakable scheme, this function needs to have several important properties that are beyond the scope of our discussion.

➢ **Decryption Process**

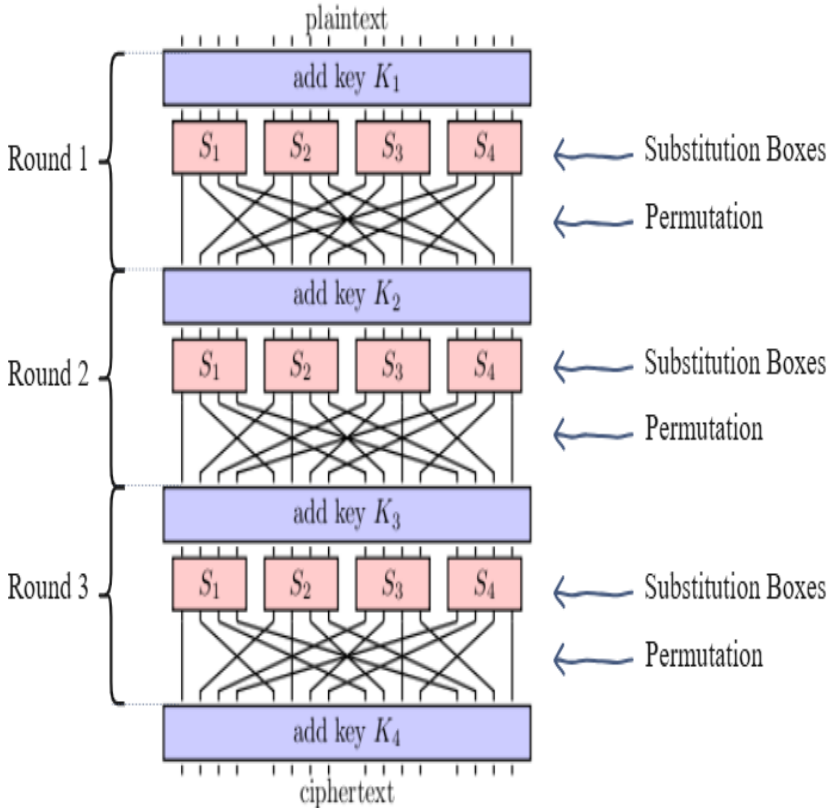
- The process of decryption in Feistel cipher is almost similar. Instead of starting with a block of plaintext, the ciphertext block is fed into the start of the Feistel structure and then the process thereafter is exactly the same as described in the given illustration.
- The process is said to be almost similar and not exactly same. In the case of decryption, the only difference is that the subkeys used in encryption are used in the reverse order.
- The final swapping of L and R in last step of the Feistel Cipher is essential. If these are not swapped then the resulting ciphertext could not be decrypted using the same algorithm.

➢ **Number of Rounds**

- The number of rounds used in a Feistel Cipher depends on desired security from the system. More number of rounds provide more secure system. But at the same time, more rounds mean the inefficient slow encryption and decryption processes. Number of rounds in the systems thus depend upon efficiencysecurity tradeoff.

Substitution Permutation Network (SPN)

A **Substitution-Permutation network** or an **SP network** is a class of block ciphers that consist of rounds of a repeated series of mathematical operations. SP networks form the basis of the infamous AES algorithm.



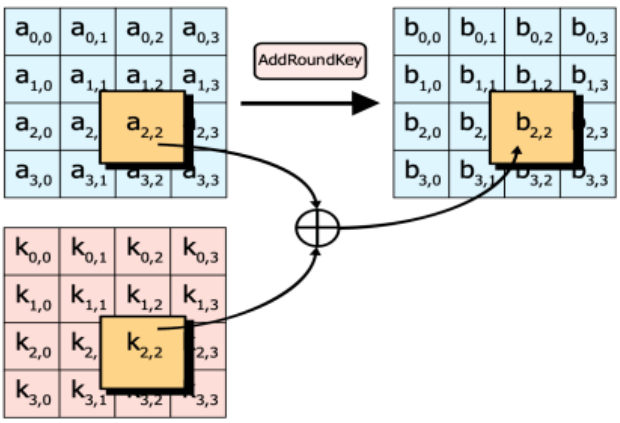
Operations in an SP network

As the figure above shows, the plaintext is passed to an SP network to produce a ciphertext. This is done through rounds, each of which consists of three main operations:

1. **Addition of the round key**
2. **Substitution of bits**
3. **Permutation of bits**

Addition of the round key

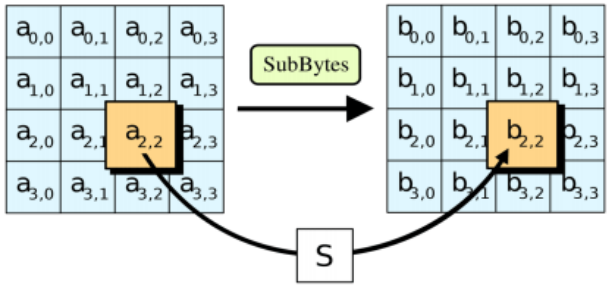
Each round in an SP network has a round key. **Round keys** are retrieved from the expansion of one secret key passed to the network at the start. At the start of each round, the text is XORed with the respective round key. This ensures that the ciphertext can only be decrypted by someone who has the round keys.



Sanjeev Thapa, Er. DevOps, SRE, CKA, RHCSA, RHCE, RHCSA-Openstack, MTCNA, MTCTCE, UBSRS, HEv6, Research Evangelist

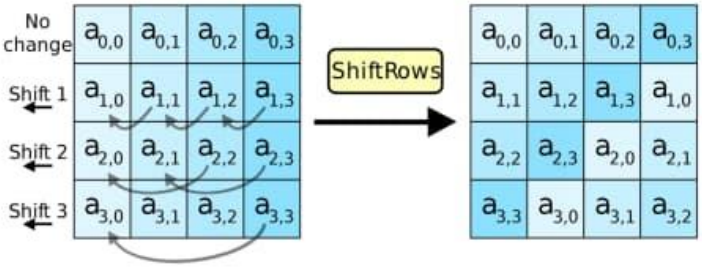
Substitution of bits

Next, the bits of the text are substituted among themselves. Since SP networks are used in block ciphers, the text is arranged as blocks. The block text bytes are substituted based on rules dictated by predefined S-boxes.



Permutation of bits

Finally, comes the permutation step. In this step, bits in the block text are mixed around. One example of such mixing is in AES, where all rows except the first are shifted by one. This is shown below:



Note: The substitution and permutation boxes are not kept hidden in SP networks. Only the round keys are kept secret for security.

Data Encryption Standards (DES)

Double DES and Triple DES

Advanced Encryption Standards (AES) Cipher

International Data Encryption Standard (IDEA)

Sanjeev Thapa, Er. DevOps, SRE, CKA, RHCSA, RHCE, RHCSA-Openstack, MTCNA, MTCTCE, UBSRS, HEv6, Research Evangelist

Finite Fields: Groups Rings, Fields, Modular Arithmetic, Euclidean Algorithm, Galois Fields (GF(p) & GF(2n)), Polynomial Arithmetic

Sdsds

Sdsds