جامعة المستقبل
AL MUSTAQBAL UNIVERSITY

كلية العلوم

قسم علوم الامن السيبراني

Cyber Security Department

Subject: Symmetric Cipher
Class: 2nd
Lecturer: Asst.Lect. Mustafa Ameer Awadh

Lecture: (1)

Study Year: 2024-2025

Historically: cryptography arose to enable parties to maintain privacy of the information they send to each other, even in the presence of an adversary with access to the communication channel. While providing privacy there remains a central goal, the field has expanded to encompass many others, including not just other goals of communication security, such as guaranteeing, integrity and authenticity of communications, but many more sophisticated and fascinating goals, Cryptography is a discipline of mathematics and computer science concerned with information security and related issues, particularly encryption, authentication, and such applications as access Control. Cryptography, as an interdisciplinary subject, draws on several fields. Prior to the early 20th century, cryptography was chiefly concerned with Linguistic patterns. Since then, the emphasis has shifted, and Cryptography now makes extensive use of mathematics, including topics from information theory, computational complexity, statistics, combinatory, and especially number theory. Security has many facets. For a system to be secure, many factors must combine. For example, it should not be possible for hackers to exploit bugs, break into a system, and use an account. They shouldn't be able to buy off your system administrator. They shouldn't be able to steal your back-up tapes. These things lie in the realm of system security. The cryptographic protocol is just one piece of the puzzle. If it is poorly designed, the attacker will exploit that. For example, suppose the protocol transmits a password in the clear (that is, in a way that anyone watching can understand what it is), that is a protocol problem, not a system problem. In addition, it will certainly be exploited. The security of the system is only as strong as its weakest link. This is a big part of the difficulty of building a secure system. To get security we need to address all the problems: how do we secure our machines against intruders? how do we administer machines to maintain security? how do we design good protocols? and so on. All these problems are important, but we will not address all of these problems here. We usually have to assume that the rest of the system is competent at doing its job. We make this assumption because it provides a natural abstraction boundary in dealing with the enormous task of providing security. Information system security is a domain of a different nature, requiring different tools and expertise.

Symmetric Cipher Model

A symmetric encryption scheme has five ingredients:

- Plaintext: This is the original intelligible message or data that is fed into the algorithm as input.
- Encryption algorithm: The encryption algorithm performs various substitutions and
- transformations on the plaintext.
- Secret key: The secret key is also input to the encryption algorithm. The key is a value independent of the plaintext and of the algorithm. The algorithm will produce a different output depending on the specific key being used at the time. The exact substitutions and transformations performed by the algorithm depend on the key.
- Ciphertext: This is the scrambled message produced as output. It depends on the plaintext and the secret key. For a given message, two different keys will produce two different ciphertexts. The ciphertext is an apparently random stream of data and, as it stands, is unintelligible.
- Decryption algorithm: This is essentially the encryption algorithm run in reverse. It takes the ciphertext and the secret key and produces the original plaintext.

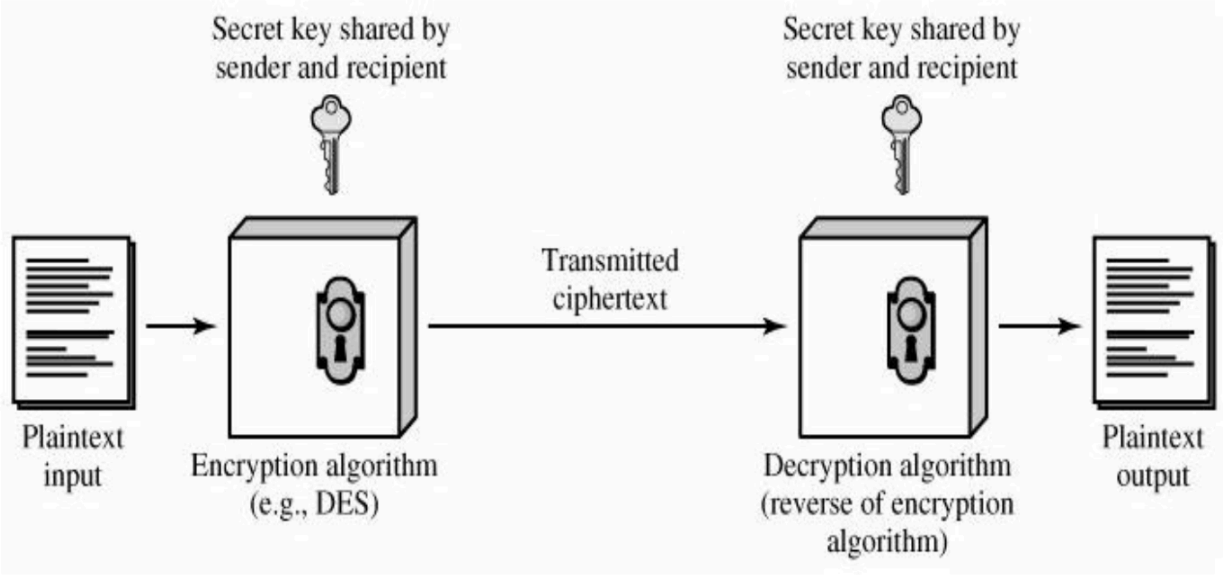


Fig.1 Symmetric algorithm process.

There are two requirements for secure use of conventional encryption:

1- **We need a strong encryption algorithm**. At a minimum, we would like the algorithm to be such that an opponent who knows the algorithm and has access to one or more cipher texts would be unable to decipher the ciphertext or figure out the key. This requirement is usually stated in a stronger form: The opponent should be unable to decrypt ciphertext or discover the key even if he or she is in possession of a number of ciphertexts together with the plaintext that produced each ciphertext.
2- **Sender and receiver must have obtained copies of the secret key** in a secure fashion and must keep the key secure. If someone can discover the key and knows the algorithm, all communication using this key is readable.

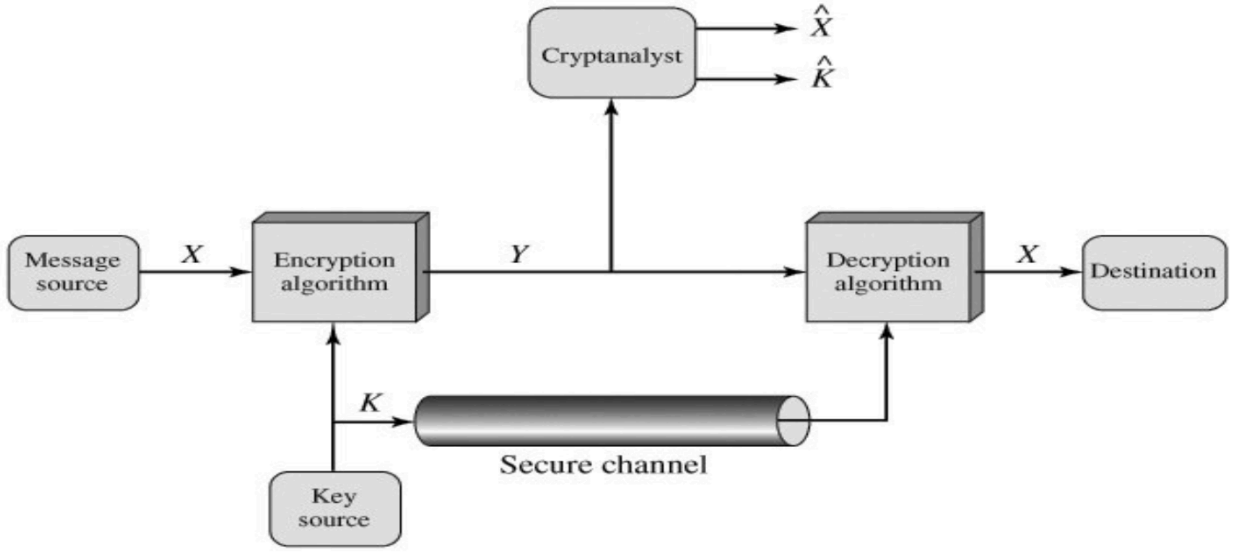


Fig.2 Encryption process between sender and receiver.

NOTE: They are IDEA (1992), RC5 (1995), RC6 (1996), DES (1977) and AES (2001). The Advanced Encryption Standard (AES) specifies a FIPS-approved symmetric block cipher which will soon come to be used in lieu of Triple DES or RC6.

Feistel Mode

In cryptography, a Feistel cipher is a symmetric structure used in the construction of block ciphers, named after the German IBM cryptographer Horst Feistel; it is also commonly known as a Feistel network. A large proportion of block ciphers use the scheme, including the Data Encryption Standard (DES). The Feistel structure has the advantage that encryption and decryption operations are very similar, even identical in some cases, requiring only a reversal of the key schedule. Therefore, the size of the code or circuitry required to implement such a cipher is nearly halved. Feistel networks and similar constructions are product ciphers, and so combine multiple rounds of repeated operations, such as:

- Bit-shuffling (often called permutation boxes or P-boxes)
- Simple non-linear functions (often called substitution boxes or S-boxes)
- Linear mixing (in the sense of modular algebra) using XOR to produce a function with large amounts of what Claude Shannon described as "confusion and diffusion". Bit shuffling creates the diffusion effect, while substitution is used for confusion.

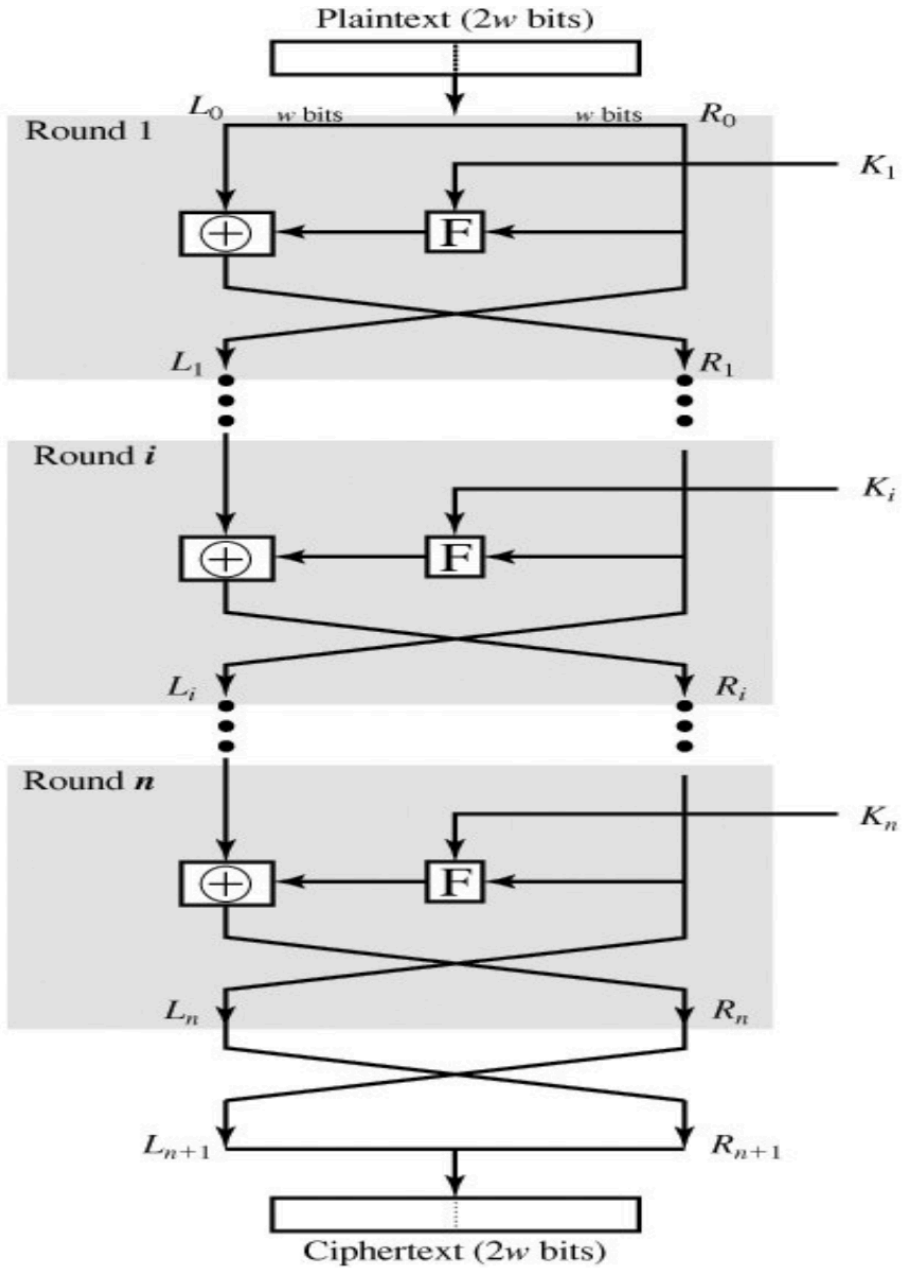
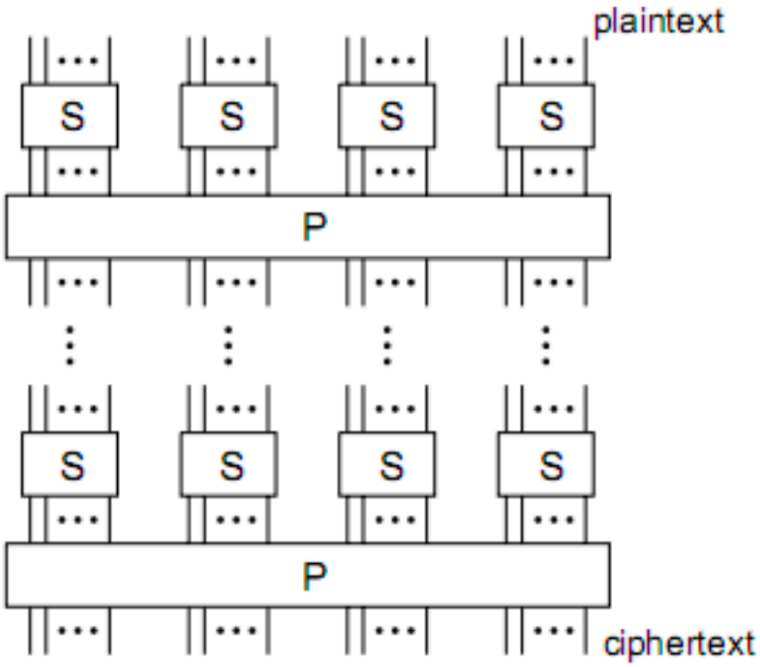


Fig.3 Feistel mode.

Confusion and Diffusion

Successful block cipher designs often integrate the concepts of *confusion* and *diffusion*. These ideas were introduced by Shannon. *Confusion* is a measure of the statistical properties of the input with relation to the output. Essentially, looking at the output should give little or no information about the input; in short, the transformation should complicate the input such that the output bears little statistical relationship with the input. *Diffusion*, on the other hand, attempts to extend the influence of the input symbols over a wide range of output symbols in order to disguise the tendencies of the input. It must be noted that is not mandatory for both characteristics to be utilized to achieve secrecy. Indeed, the Vernam stream cipher achieves perfect secrecy with confusion alone. Since each plaintext symbol is combined with completely random data, there is no need to mix adjacent symbols of plaintext to achieve additional randomness. Unlike stream ciphers, block cipher principles of confusion and diffusion. Since the symbol length of a typical block cipher (64 bits) is often longer than the corresponding symbol in a stream cipher (8 or 32 bits), there are more possible bits positions, which necessitate and assist diffusion. A successful diffusion is one in which each plaintext bit and each key bit affects each ciphertext bit (in the case of encryption). This diffusion can be applied using a permutation which exchanges individual bit locations or sequential algebraic functions which combine and spread the influence of the inputs. A well diffused cipher will satisfy the strict avalanche criteria whereby if a single bit changes in the input, then half of the output bits will change in a random manner.

Definition: A product cipher combines two more transformations in manner intending that the resulting cipher is more secure than the individual components.
Definition: A substitution-permutation (SP) network is a product cipher composed of a number of stages each involving substitutions and permutations.



Substitution Operation a binary word is replaced by some other binary word the whole substitution function forms the key if use n bit words, the key is 2^(n)! bits, grows rapidly

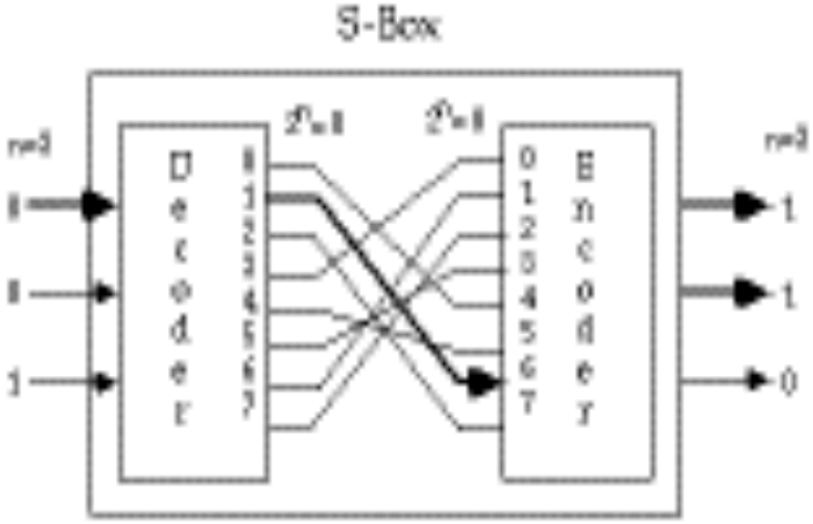


Fig.4 Substitution operation

can also think of this as a large lookup table, with n address lines (hence 2^(n) addresses), each n bits wide being the output value will call them S-boxes

Permutation Operation a binary word has its bits reordered (permuted) the re-ordering forms the key if use n bit words, the key is n! bits, which grows more slowly, and hence is less secure than substitution

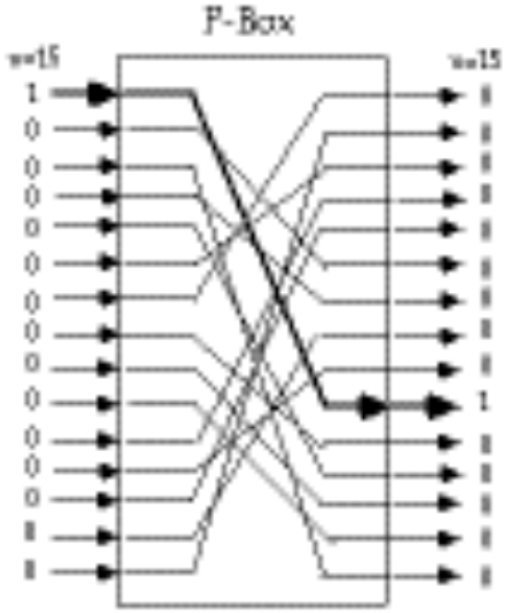


Fig.5 Permutation process

this is equivalent to a wire-crossing in practise (though is much harder to do in software) will call these P-boxes

Substitution-Permutation Network transformations Shannon combined these two primitives he called these mixing

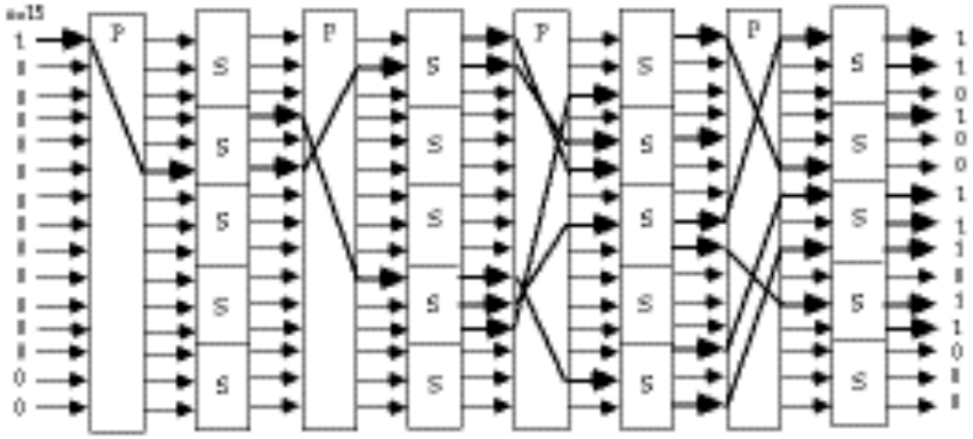


Fig.6 Substitution-Permutation Network

Shannon's mixing transformations are a special form of product ciphers where:

S-Boxes
provide confusion of input bits

P-Boxes
provide diffusion across S-box inputs in general these provide the following results.