NETWORK SECURITY

Confusion and Diffusion

Dr. Faheem Masoodi
masoodifahim@uok.edu.in

Confusion and Diffusion

According to the famous information theorist Claude Shannon, there are two primitive operations with which strong encryption algorithms can be built: **confusion** and **diffusion** are two properties of the operation of a secure cipher identified in 1945 classified report *A Mathematical Theory of Cryptography*. These properties, when present, work to thwart the application of statistics and other methods of cryptanalysis. These concepts are also important in the design of robust hash functions and pseudorandom number generators where decorrelation of the generated values is of paramount importance.

1. **Confusion** is an encryption operation where the relationship between key and ciphertext is obscured. Today, a common element for achieving confusion is substitution, which is found in both DES and AES.

Confusion means that each binary digit (bit) of the ciphertext should depend on several parts of the key, obscuring the connections between the two. The property of confusion hides the relationship between the ciphertext and the key. This property makes it difficult to find the key from the ciphertext and if a single bit in a key is changed, the calculation of the values of most or all of the bits in the ciphertext will be affected. Confusion increases the ambiguity of ciphertext and it is used by both block and stream ciphers.

2. **Diffusion** is an encryption operation where the influence of one plaintext symbol is spread over many ciphertext symbols with the goal of hiding statistical properties of the plaintext. A simple diffusion element is the bit permutation, which is used frequently within DES. AES uses the more advanced Mix-column operation. Ciphers which only perform confusion, such as the Shift Cipher or the World War II encryption machine Enigma, are not secure. Neither are ciphers which only perform diffusion. However, through the concatenation of such operations, a strong cipher can be built. The idea of concatenating several encryption operation was also proposed by Shannon. Such ciphers are known as *product ciphers*. Or we can simplify the concept and say:

Diffusion means that if we change a single bit of the plaintext, then (statistically) half of the bits in the ciphertext should change, and similarly, if we change one bit of the ciphertext, then approximately one half of the plaintext bits should change.[2] Since a bit can have only two states, when they are all re-evaluated and changed from one seemingly random position to another, half of the bits will have changed state. The idea of diffusion is to hide the relationship between the ciphertext and the plain text. This will make it hard for an attacker who tries to find out the plain text and it increases the redundancy of plain text by spreading it across the rows and columns; it is achieved through transposition of algorithm and it is used by block ciphers only.

All of today's block ciphers are product ciphers as they consist of rounds which are applied repeatedly to the data

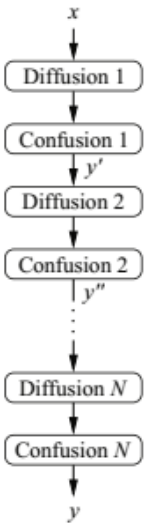

Fig. 1 Principle of an *N* round product cipher, where each round performs a confusion and diffusion operation

Modern block ciphers possess excellent diffusion properties. On a cipher level this means that changing of one bit of plaintext results on average in the change of half the output bits, i.e., the second ciphertext looks statistically independent of the first one. This is an important property to keep in mind when dealing with block ciphers. We demonstrate this behavior with the following simple example.

Example 1. Let's assume a small block cipher with a block length of 8 bits. Encryption of two plaintexts x1 and x2, which differ only by one bit, should roughly result in something as shown in Fig. 2

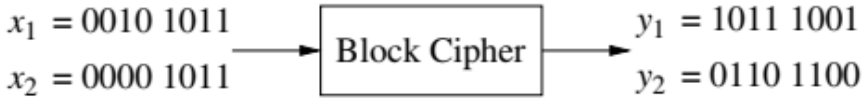

Fig. 2 Principle of diffusion of a block cipher

Note that modern block ciphers have block lengths of 64 or 128 bit but they show exactly the same behavior if one input bit is flipped.

S.NO	CONFUSION	DIFFUSION
1.	Confusion is a cryptographic technique which is used to create faint cipher texts.	While diffusion is used to create cryptic plain texts.
2.	This technique is possible through substitution algorithm.	While it is possible through transportation algorithm.
3.	In confusion, if one bit within the secret's modified, most or all bits within the cipher text also will be modified.	While in diffusion, if one image within the plain text is modified, many or all image within the cipher text also will be modified
4.	In confusion, vagueness is increased in resultant.	While in diffusion, redundancy is increased in resultant.
5.	Both stream cipher and block cipher uses confusion.	Only block cipher uses diffusion.
6.	The relation between the cipher text and the key is masked by confusion.	While The relation between the cipher text and the plain text is masked by diffusion.