In cryptography, **confusion** and **diffusion** are two properties of the operation of a secure cipher which were identified by Claude Shannon in his paper *Communication Theory of Secrecy Systems*, published in 1949.

In Shannon's original definitions, *confusion* refers to making the relationship between the key and the ciphertext as complex and involved as possible; *diffusion* refers to the property that the redundancy in the statistics of the plaintext is "dissipated" in the statistics of the ciphertext. In other words, the non-uniformity in the distribution of the individual letters (and pairs of neighboring letters) in the plaintext should be redistributed into the non-uniformity in the distribution of much larger structures of the ciphertext, which is much harder to detect.

Diffusion means that the output bits should depend on the input bits in a very complex way. In a cipher with good diffusion, if one bit of the plaintext is changed, then the ciphertext should change completely, in an unpredictable or pseudorandom manner. In particular, for a randomly chosen input, if one flips the *i*-th bit, then the probability that the *j*-th output bit will change should be one half, for any *i* and *j* — this is termed the strict avalanche criterion. More generally, one may require that flipping a fixed set of bits should change each output bit with probability one half.

One aim of confusion is to make it very hard to find the key even if one has a large number of plaintext-ciphertext pairs produced with the same key. Therefore, each bit of the ciphertext should depend on the entire key, and in different ways on different bits of the key. In particular, changing one bit of the key should change the ciphertext completely.

The simplest way to achieve both diffusion and confusion is a substitution-permutation network. In these systems, the plaintext and the key often have a very similar role in producing the output, hence it is the same mechanism that ensures both diffusion and confusion.