Confusion and Diffusion

Ref: William Stallings,
Cryptography and Network Security,
3rd Edition, Prentice Hall, 2003

Statistics and Plaintext

- Suppose the frequency distribution of plaintext in a human-readable message in some language is known.
- Or suppose there are known words or phrases that are used in the plaintext message.
- A cryptanalysisist can use this information to break a cryptographic algorithm.

Changing Statistics

- Claude Shannon suggested that to complicate statistical attacks, the cryptographer could dissipate the statistical structure of the plaintext in the long range statistics of the ciphertext.
- Shannon called this process **diffusion**.

Changing Statistics (p.2)

- Diffusion can be accomplished by having many plaintext characters affect each ciphertext character.
- An example of diffusion is the encryption of a message $M=m_1,m_2,...$ using a an averaging: $y_n= \sum_{i=1,k} m_{n+i}$(mod26).

Changing Statistics (p.3)

- In binary block ciphers, such as the Data Encryption Standard (DES), diffusion can be accomplished using **permutations** on data, and then applying a function to the permutation to produce ciphertext.

Complex Use of a Key

- Diffusion complicates the statistics of the ciphertext, and makes it difficult to discover the key of the encryption process.
- The process of **confusion**, makes the use of the key so complex, that even when an attacker knows the statistics, it is still difficult to deduce the key.

Complex Use of a Key(p.2)

- **Confusion** can be accomplished by using a complex substitution algorithm.
- Block ciphers, such as the Data Encryption Standard, makes use of substitution operations.