5.1.4 Product Ciphers

Shannon introduced the concept of a product cipher. A product cipher is a complex cipher combining substitution, permutation, and other components discussed in previous sections.

5.1.4 Continued

Diffusion

The idea of diffusion is to hide the relationship between the ciphertext and the plaintext.

Note

Diffusion hides the relationship between the ciphertext and the plaintext.

5.1.4 Continued

Confusion

The idea of confusion is to hide the relationship between the ciphertext and the key.

Note

Confusion hides the relationship between the ciphertext and the key.

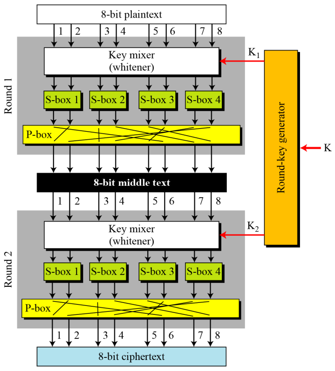
5.1.4 Continued

Rounds

Diffusion and confusion can be achieved using iterated product ciphers where each iteration is a combination of S-boxes, P-boxes, and other components.

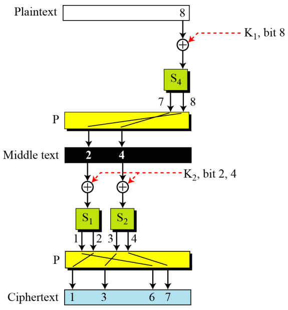
5.1.4 Continued

Figure 5.13 ***A product cipher made of two rounds***



5.1.4 Continued

Figure 5.14 ***Diffusion and confusion in a block cipher***


Plaintext
8
K1, bit 8
S4
7
8
P
Middle text
2
4
K2, bit 2, 4
S1
S2
1
2
3
4
P
Ciphertext
1
3
6
7