DES Encryption

Motivation for the Fiestel Cipher Structure

The encryption algorithm should be reversible so that the same algorithm can be used for decryption.

Possible solution

- A block cipher that operates on a plaintext block of *n* bits produces a ciphertext block of *n* bits.
- There are 2^n possible different plaintext blocks. So, for the encryption to be reversible, each must produce a unique ciphertext block.
- So, if we limit ourselves to reversible mappings, the number of different transformations is $2^n!$.

Problems with this solution

1. If a small block size (e.g. $n = 4$) is used, then the system is equivalent to a classical substitution cipher. Such systems are vulnerable to a statistical analysis of the plaintext.
2. An arbitrary reversible substitution cipher for a large block size is not practical, however, from an implementation point of view. For such a transformation, the mapping itself constitutes the key. And, hence, for an *n*-bit block cipher, the length of the key is $n \times 2^n$.

Possible solution: Diffusion and Confusion

Every block cipher involves a transformation of a block of plaintext into a block of ciphertext, where the transformation depends on the key.

The mechanism of diffusion seeks to make the relationship between the plaintext and ciphertext as complex as possible in order to thwart attempts to deduce the key.

On the other hand, confusion seeks to make the relationship between the statistics of the ciphertext and the value of the encryption key as complex as possible, again to thwart attempts to discover the key. This is achieved by the use of a complex substitution algorithm.

In DES, the S-boxes provide confusion; and the P-box as well as the E-expansion provide diffusion.

AES Encryption

Drawbacks of DES

1. DES key length (56 bits) is too small.
2. The original DES was designed for mid-1970s hardware implementation and does not produce efficient software code.
3. 3DES increased key size, but tripled number of rounds, hence correspondingly slower.
4. Both DES and 3DES use a 64-bit block size. For reasons of both efficiency and security, a larger block size is desirable.

Goals of the Algorithm

1. We need such a design that has
    a. a low correlation between input bits and output bits
    b. the property that the output cannot be described as a simple mathematical function of the input

    so that the algorithm can be resistant to known cryptographic attacks.

    AES Implementation:

    An invertible S-box is used, i.e., IS-box[S-box(a)] = a. However, the S-box is not self-inverse, i.e. S-box(a) ≠ IS-box(a).

2. However, we also need a design where the output bits somewhat depends on the input bits.

    AES Implementation:

    The shift-rows transformation ensures that the 4 bytes of one column are spread out to four different columns.

    The mix-columns transformation ensures that each byte of a column is mapped into a new value that is a function of all four bytes in that column.

    The mix-column transformation combined with the shift-rows transformation ensures that after a few rounds, all output bits depend on all input bits.

3. To increase security, we can
    a. Have multiple rounds with each round consisting of all the previous operations.
    b. Expand the key in such a way so that each expansion of the key can be applied to XOR with the bytes in each round.