SECRET KEY ENCRYPTION PROTOCOLS

Secret-key encryption protocols, sometimes known as symmetric encryption, or single-key encryption protocols, are conventional encryption models. They typically consist of an encryption algorithm, a key, and a decryption algorithm. At the end point, the encrypted message is called ciphertext. Several standard mechanisms can be used to implement a secret-key encryption algorithm. Here, we focus on two protocols: Data Encryption Standard (DES) and Advanced Encryption Standard (AES).

In these algorithms, a shared secret key between a transmitter and a receiver is assigned at the transmitter and receiver points. The encryption algorithm produces a different key at any time for a specific transmission. Changing the key changes the output of the algorithm. At the receiving end, the encrypted information can be transformed back to the original data by using a decryption algorithm and the same key that was used for encryption. The security of conventional encryption depends on the secrecy of the key, not on the secrecy of the encryption algorithm. Consequently, the algorithm need not be kept secret; only the key has to be secret.

Data Encryption Standard (DES)

With the Data Encryption Standard (DES), plaintext messages are converted into 64-bit blocks, each encrypted using a key. The key length is 64 bits but contains only 56 usable bits; thus, the last bit of each 8 byte in the key is a parity bit for the corresponding byte. DES consists of 16 identical rounds of an operation, as shown in Figure 5.15. The details of the algorithm on each 64-bit block of message at each round i of operation are as follows.

Begin DES Algorithm

1. Initialize. Before round 1 begins, all 64 bits of an incoming message and all 56 bits of the secret key are separately permuted (shuffled).
2. Each incoming 64-bit message is broken into two 32-bit halves denoted by L_i and R_i, respectively.
3. The 56 bits of the key are also broken into two 28-bit halves, and each half is rotated one or two bit positions, depending on the round.
4. All 56 bits of the key are permuted, producing version k_i of the key on round i.
5. In this step, $\oplus$is a logic Exclusive-OR, and the description of function F() appears next. Then, L_i and R_i are determined by

Equation 10.2

$$L_i = R_{i-1}$$

and

Equation 10.3

$$R_i = L_{i-1} \oplus F(R_{i-1}, k_i).$$

6. All 64 bits of a message are permuted.

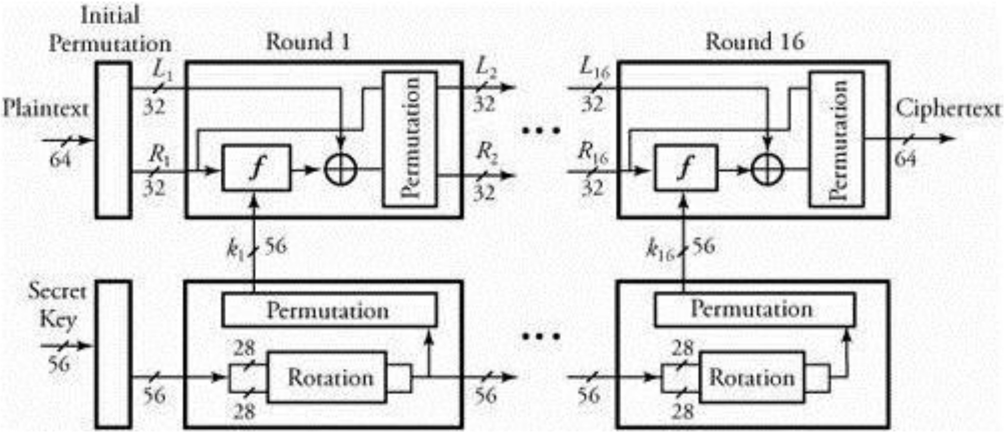

Figure 5.3. The Data Encryption Standard (DES)

The operation of function F() at any round i of DES is as follows.

1. Out of 52 bits of k_i, function F() chooses 48 bits.
2. The 32-bit R_{i-1} is expanded from 32 bits to 48 bits so that it can be combined with 48-bit k_i. The expansion of R_{i-1} is carried out by first breaking R_{i-1} into eight 4-bit chunks and then expanding each chunk by copying the leftmost bit and the rightmost bit from left and right adjacent chunks, respectively.
3. Function F() also partitions the 48 bits of k_i into eight 6-bit chunks.
4. The corresponding eight chunks of R_{i-1} and eight chunks of k_i are combined as follows:

   Equation 10.4

   $$R_{i-1} = R_{i-1} \oplus k_i .$$

At the receiver, the same steps and the same key are used to reverse the encryption. It is now apparent that the 56-bit key length may not be sufficient to provide full security. This argument is still controversial. Triple DES provides a solution for this controversy: three keys are used, for a total of 168 bits. It should also be mentioned that DES can be implemented more efficiently in hardware than in software.

Source : http://elearningatria.files.wordpress.com/2013/10/cse-vi-computer-networks-ii-10cs64-notes.pdf