SAKA AYOBAMI RAHAEL

15/ENG02/045

COMPUTER ENGINEERING

COE 522

ASSIGNMENT 1

Write short note on data encryption standards

SOLUTION

The Data Encryption Standard is a symmetric-key block Cipher based on Feistel structure. It uses 16 rounds of Feistel Structure. It was developed in the early 1970s and was approved as a federal standard in November 1976. It was reaffirmed as a standard in 1983, 1988 and again in 1999. It was only in 2002 when AES ( Advanced Encryption Standard ) was finally adopted following a public competition.

**The DES encryption Algorithm**

DES is a block Cipher, which means that it takes a fixed-length string of plaintext bits and transforms it through a series of complicated operations. This fixed-length of plaintext is of 64-bits, and the key which is the same for both encryption and decryption is also of 64-bits.

Let’s start with the Feistel structure; it is a design model from which various block Ciphers are derived. DES is one such block Cipher. A cryptographic system based on a Feistel model uses the same algorithm for both encryption and decryption. The Feistel model takes 64 bits of plaintext and divides it into halves, L and R of 32 bits each. R₂ is calculated as L⊕ƒ(R, Key) and L₂ is the same as R. This model is shown in the below figure.



The Feistel Structure

In an encryption algorithm, this procedure of transforming the plaintext can be used for any number of times. The output of one round is taken as the input for the next round. This scheme is shown below.



N-round Cryptosystem model using Feistel structure

In standard DES the number of rounds is 16. The 64-bits key is used to generate 16 keys each of 48 bits for each round using a key-scheduling algorithm which will be discussed later and the function ƒ is as described below:



**Description of the ƒ function**

The ƒ function takes input R (32 bits) and Key (48 bits). E is an expansion function which expands 32 bits to 48 bits. These 48 bits are XORed with the Key to get the input for S. S consists of 8 S-boxes which takes 6-bit input and gives 4-bit output. This is the only non-linear operation in DES. After the S operation, we will again get 32-bits which are permuted in a defined way by the P-box, and the output of P-box is XORed with L to get the output of **ƒ**function.