Michael Esposito

Cryptography

Professor Nelson

Homework 2

1. (10 points) Determine the initial 56-bit key K from K’ by computing PC-1(K), which removes parity in every 8th bit position.

1101 0101 1001 0110 1011 1010 1110 0101 0101 0111 0101 0110 1101 1010

2. (5 points) Determine the values for C0 and D0.

|  |  |  |
| --- | --- | --- |
| Round i |  |  |
| 0 |  |  |
| 1 |  |  |
| 2 |  |  |
| 3 |  |  |
| 4 |  |  |

3. (20 points) Use the standard key schedule algorithm to generate the first four 48-bit subkeys K1, K2, K3, and K4 .

0101 0001 1111 1111 0001 1011 0001 1011 1101 1001 1101 1101

0110 0101 1011 1101 1110 0011 0000 0011 1101 0101 1011 0101

4. (5 points) Construct X0 by applying the initial permutation IP to x to get X0 = IP(X).

X0 = 0101 0110 0100 1011 1101 1011 1010 1101 0011 0110 0101 1011 1101 0110 1100 1011

5. (5 points) Determine the values for L0 and R0.

L0 = 0101 0110 0100 1011 1101 1011 1010 1101

R0 = 0011 0110 0101 1011 1101 0110 1100 1011

6. (50 points) Using the standard round function, compute Li and Ri for 𝟏 ≤ 𝒊 ≤ 𝟒.

|  |  |  |
| --- | --- | --- |
| Round i |  |  |
| 0 | 0101 0110 0100 1011 1101 1011 1010 1101 | 0011 0110 0101 1011 1101 0110 1100 1011 |
| 1 | 0011 0110 0101 1011 1101 0110 1100 1011 | 1110 1000 1111 1001 0000 1000 1111 0000 |
| 2 | 1110 1000 1111 1001 0000 1000 1111 0000 | 0000 0110 1000 1111 0101 1001 0011 0110 |
| 3 | 0000 0110 1000 1111 0101 1001 0011 0110 | 0011 1011 1010 0101 1010 0101 1000 0111 |
| 4 | 0011 1011 1010 0101 1010 0101 1000 0111 |  |

7. (5 points) Concatenate L4 and R4 in reverse order and apply IP-1 to R4L4 to get final result.