*****Instituto Politécnico Nacional***

***Escuela Superior de Cómputo***

*Criptography*

***Ejercicios Capítulo II***

***Nombre:*** *Sampayo Hernández Mauro*

***Grupo:*** *3CV17*

***Profesor:*** *Víctor Manuel Silva García*

**Ejercicios**

1. **Utilizando el patrón de la tabla 2.1.1, construya una permutación de un arreglo de 96 elementos, 1 – 96. Además, genere su inversa.**

Permutación :

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 86 | 74 | 62 | 50 | 38 | 26 | 14 | 2 |
| 88 | 76 | 64 | 52 | 40 | 28 | 16 | 4 |
| 90 | 78 | 66 | 54 | 42 | 30 | 18 | 6 |
| 92 | 80 | 68 | 56 | 44 | 32 | 20 | 8 |
| 94 | 82 | 70 | 58 | 46 | 34 | 22 | 10 |
| 96 | 84 | 72 | 60 | 48 | 36 | 24 | 12 |
| 85 | 73 | 61 | 49 | 37 | 25 | 13 | 1 |
| 87 | 75 | 63 | 51 | 39 | 27 | 15 | 3 |
| 89 | 77 | 65 | 53 | 41 | 29 | 17 | 5 |
| 91 | 79 | 67 | 55 | 43 | 31 | 19 | 7 |
| 93 | 81 | 69 | 57 | 45 | 33 | 21 | 9 |
| 95 | 83 | 71 | 59 | 47 | 35 | 23 | 11 |

Permutación :

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 60 | 12 | 72 | 24 | 84 | 36 | 96 | 48 |
| 59 | 11 | 71 | 23 | 83 | 35 | 95 | 47 |
| 58 | 10 | 70 | 22 | 82 | 34 | 94 | 46 |
| 57 | 9 | 69 | 21 | 81 | 33 | 93 | 45 |
| 56 | 8 | 68 | 20 | 80 | 32 | 92 | 44 |
| 55 | 7 | 67 | 19 | 79 | 31 | 91 | 43 |
| 54 | 6 | 66 | 18 | 78 | 30 | 90 | 42 |
| 53 | 5 | 65 | 17 | 77 | 29 | 89 | 41 |
| 52 | 4 | 64 | 16 | 76 | 28 | 88 | 40 |
| 51 | 3 | 63 | 15 | 75 | 27 | 87 | 39 |
| 50 | 2 | 62 | 14 | 74 | 26 | 86 | 38 |
| 49 | 1 | 61 | 13 | 73 | 25 | 85 | 37 |

1. **Construya una tabla de expansión diferente de E.**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 1 | 32 | 31 | 30 | 29 | 28 |
| 29 | 28 | 27 | 26 | 25 | 24 |
| 25 | 24 | 23 | 22 | 21 | 20 |
| 21 | 20 | 19 | 18 | 17 | 16 |
| 17 | 16 | 15 | 14 | 13 | 12 |
| 13 | 12 | 11 | 10 | 9 | 8 |
| 9 | 8 | 7 | 6 | 5 | 4 |
| 5 | 4 | 3 | 2 | 1 | 32 |

1. **Construya una tabla de substitución siguiendo los patrones de las tablas .**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Row No.** | **0** | **1** | **2** | **3** | **4** | **5** | **6** | **7** | **8** | **9** | **10** | **11** | **12** | **13** | **14** | **15** |
| 0 | 1 | 7 | 4 | 15 | 8 | 10 | 0 | 3 | 11 | 12 | 5 | 14 | 9 | 13 | 2 | 6 |
| 1 | 6 | 8 | 2 | 12 | 11 | 13 | 15 | 9 | 7 | 1 | 0 | 4 | 3 | 10 | 5 | 14 |
| 2 | 5 | 2 | 15 | 3 | 7 | 9 | 8 | 6 | 1 | 0 | 11 | 14 | 13 | 4 | 12 | 10 |
| 3 | 11 | 14 | 1 | 6 | 8 | 0 | 7 | 3 | 15 | 10 | 2 | 5 | 12 | 9 | 4 | 13 |

1. **Encuentre la primera llave del programa de llaves,, del criptosistema DES, cuando la llave = a10f4708c621be73.**

Se realiza la conversión de la llave k de hexadecimal a binario:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **a** | **1** | **0** | **f** | **4** | **7** | **0** | **8** | **c** | **6** | **2** | **1** | **b** | **e** | **7** | **3** |
| 1010 | 0001 | 0000 | 1111 | 0100 | 0111 | 0000 | 1000 | 1100 | 0110 | 0010 | 0001 | 1011 | 1110 | 0111 | 0011 |

Se aplica la permutación PC -1:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 0 | 1 | 0 | 1 | 0 | 0 | 0 |
| 1 | 1 | 0 | 0 | 1 | 0 | 1 |
| 0 | 0 | 1 | 1 | 1 | 0 | 0 |
| 0 | 0 | 1 | 1 | 1 | 0 | 0 |
| 1 | 1 | 0 | 1 | 0 | 1 | 1 |
| 0 | 0 | 1 | 0 | 1 | 0 | 1 |
| 1 | 0 | 0 | 1 | 0 | 0 | 1 |
| 0 | 1 | 0 | 0 | 0 | 0 | 0 |

Obteniendo :

|  |  |
| --- | --- |
|  |  |
| 01010 00 1100101 0011100 00 11100 | 11010 11 0010101 1001001 01 00000 |

Realizando un corrimiento a la izquierda, se tiene:

|  |  |
| --- | --- |
|  |  |
| 1010001 1001010 0111000 0111000 | 1010110 0101011 0010010 1000001 |

Se aplica la permutación PC -2:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 0 | 1 | 1 | 1 | 1 | 0 |
| 1 | 0 | 0 | 0 | 0 | 0 |
| 1 | 0 | 0 | 0 | 0 | 1 |
| 1 | 1 | 0 | 0 | 1 | 0 |
| 1 | 0 | 1 | 1 | 0 | 0 |
| 0 | 0 | 0 | 1 | 1 | 1 |
| 0 | 0 | 1 | 1 | 1 | 0 |
| 0 | 1 | 1 | 0 | 1 | 0 |

De esta manera se tiene que la llave es:

1. **Realice la operación {7 c} ● {0 3} mod. . Donde .**

Reescribiendo los operandos como cadenas de 8 bits, se tiene:

Se realiza el producto p(x) X q(x).

Para el primer producto, la cadena 00000001 es la identidad, por lo tanto, el producto es:

01111100 x 00000001 = 01111100.

Se realiza la siguiente multiplicación, misma que es equivalente a multiplicar por x, que a su vez es similar a realizar un corrimiento a la izquierda de una posición en la cadena p(x).

01111100 x 00000010 = 11111000.

Considerando así, los resultados de las multiplicaciones, se tiene:

Finalmente, se expresa el resultado en el sistema hexadecimal usando la notación de la norma:

1. **Proponga un polinomio irreductible de grado ocho. Considerando que los coeficientes pueden ser 0 o 1.**
2. **Dados los valores ac, 3f, 5a y bd; lleve a cabo la operación de substitución usando las cajas 2.3.2.1 y 2.4.1. Compare resultados.**

Se realiza la conversión de hexadecimal a binario:

|  |  |  |  |
| --- | --- | --- | --- |
| **ac** | **3f** | **5a** | **bd** |
| 10101100 | 00111111 | 01011011 | 10111101 |

Aplicando la operación de substitución con las cajas 2.3.2.1 y 2.4.1, se tiene:

|  |  |  |
| --- | --- | --- |
| **Valor inicial** | **Resultado Caja 2.3.2.1** | **Resultado Caja 2.4.1** |
| **ac** | 91 | 96 |
| **3f** | 75 | ac |
| **5a** | be | c9 |
| **bd** | 7a | 68 |

1. **Proponga un sistema de cifrado “Substitution Permutation Network”.**
2. **Encuentre la segunda llave ronda del criptosistema AES, , cuando la llave de 128 bits es la siguiente: 491f7a65de283be0bfe8462ca40ce63b.**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **i** | **temp** | **After**  **RotWord()** | **After**  **SubWord()** | **Rcon**  **[i/Nk]** | **After ⊕**  **With Rcon** | **W[i/Nk]** | **W[i]=temp**  **⊕W[i/Nk]** |
| 4 | a40ce63b | 0ce63ba4 | fe8ee249 | 0100000 | ff8ee249 | 491f7a65 | b691982c |
| 5 | b691982c |  |  |  |  | de283be0 | 68b9a3cc |
| 6 | 68b9a3cc |  |  |  |  | bfe8462c | d751e5e0 |
| 7 | d751e5e0 |  |  |  |  | a40ce63b | 735d03db |

**Operaciones realizadas:**

|  |  |  |
| --- | --- | --- |
| **After ⊕ With Rcon** | ff8ee249 | 1111 1111 1000 1110 1110 0010 0100 1001 |
| **W[i/Nk]** | 491f7a65 | 0100 1001 0001 1111 0111 1010 0110 0101 |
| **W[i]=temp⊕W[i/Nk]** | b691982c | 1011 0110 0001 0001 1001 1001 0010 1100 |

|  |  |  |
| --- | --- | --- |
| **After ⊕ With Rcon** | b691982c | 1011 0110 1001 0001 1001 1000 0010 1100 |
| **W[i/Nk]** | de283be0 | 1101 1110 0010 1000 0011 1011 1110 0000 |
| **W[i]=temp⊕W[i/Nk]** | 68b9a3cc | 0110 1000 1011 1001 1010 0011 1100 1100 |

|  |  |  |
| --- | --- | --- |
| **After ⊕ With Rcon** | 68b9a3cc | 0110 1000 1011 1001 1010 0011 1100 1100 |
| **W[i/Nk]** | bfe8462c | 1011 1111 1110 1000 0100 0110 0010 1100 |
| **W[i]=temp⊕W[i/Nk]** | d751e5e0 | 1101 0111 0101 0001 1110 0101 1110 0000 |

|  |  |  |
| --- | --- | --- |
| **After ⊕ With Rcon** | d751e5e0 | 1101 0111 0101 0001 1110 0101 1110 0000 |
| **W[i/Nk]** | a40ce63b | 1010 0100 0000 1100 1110 0110 0011 1011 |
| **W[i]=temp⊕W[i/Nk]** | 735d03db | 0111 0011 0101 1101 0000 0011 1101 1011 |

La llave es:

|  |  |  |  |
| --- | --- | --- | --- |
| b6 | 68 | d7 | 73 |
| 91 | b9 | 51 | 5d |
| 98 | a3 | e5 | 03 |
| 2c | cc | e0 | db |