1. Given the plaintext to AES {0405060708090A0B000102030C0D0E0F}

Do the following:

1. Show the original contents of state, displayed as 4x4 matrix.
2. Show the value of state after ShiftRows.
3. Show the value of state after MixColumn, Using the following matrix:

02 03 01 01

01 02 03 01

01 01 02 03

03 01 01 02

Solutions:

a.

|  |  |  |  |
| --- | --- | --- | --- |
| 04 | 08 | 00 | 0C |
| 05 | 09 | 01 | 0D |
| 06 | 0A | 02 | 0E |
| 07 | 0B | 03 | 0F |

b.

|  |  |  |  |
| --- | --- | --- | --- |
| 04 | 08 | 00 | 0C |
| 09 | 01 | 0D | 05 |
| 02 | 0E | 06 | 0A |
| 0F | 07 | 0B | 03 |

c.

|  |  |  |  |
| --- | --- | --- | --- |
| 02 | 03 | 01 | 01 |
| 01 | 02 | 03 | 01 |
| 01 | 01 | 02 | 03 |
| 03 | 01 | 01 | 02 |

|  |  |  |  |
| --- | --- | --- | --- |
| 04 | 08 | 00 | 0C |
| 05 | 09 | 01 | 0D |
| 06 | 0A | 02 | 0E |
| 07 | 0B | 03 | 0F |

First row

1. 02 \* 04 ⊕ 03 \* 05 ⊕ 01 \* 06 ⊕ 01 \* 07
2. 02 \* 08 ⊕ 03 \* 09 ⊕ 01 \* 0A⊕ 01 \* 0B
3. 02 \* 00 ⊕ 03 \* 01 ⊕ 01 \* 02 ⊕ 01 \* 03
4. 02 \* 0C ⊕ 03 \* 0D ⊕ 01 \* 0E ⊕ 01 \* 0F

Convert to binary form

1. 0000 0100 \* 10 ⊕ (0000 0101 \* 10 ⊕ 0000 0101 \* 01)⊕ 0000 0110 \* 01 ⊕ 0000 0111 \* 01
2. 0000 1000 \* 10 ⊕ (0000 1001 \* 10 ⊕ 0000 1001 \* 01)⊕ 0000 1010 \* 01 ⊕ 0000 1011 \* 01
3. 0000 0000 \* 10 ⊕ (0000 0001 \* 10 ⊕ 0000 0001 \* 01) ⊕ 0000 0010 \* 01 ⊕ 0000 0011 \* 01
4. 0000 1100 \* 10 ⊕ (0000 1101 \* 10 ⊕ 0000 1101 \* 01) ⊕ 0000 1110 \* 01 ⊕ 0000 1111 \* 01

Shift and XOR

1. 0000 1000 ⊕ 0000 1111 ⊕ 0000 0110 ⊕ 0000 0111 = 0000 0110 = 06 =6
2. 0001 0000 ⊕ 0001 1011 ⊕ 0000 1010 ⊕ 0000 1011 = 0000 1010 = 0A =10
3. 0000 0000 ⊕ 0000 0011 ⊕ 0000 0010 ⊕ 0000 0011 = 0000 0010 = 02 = 2
4. 0001 1000 ⊕ 0001 0111 ⊕ 0000 1110 ⊕ 0000 1111 = 0000 1110 = 0E =14

2.

a. How many bytes in **State** are affected by ShiftRows operation?

1. Explain the three security properties of Hash Functions (with diagrams).

1. Decrypt the cipher C= 87 using RSA with the following parameters:

e = 1127, n = 41 X 37.

1. Apply an attack to send a valid signature to Alice pretending you are Bob, provided, you know that Bob and Alice are using RSA digital signature, Public Key of Bob is 11, and the public Modula n=221.

Show that your attack is successful.

1. Convert the superincreasing knapsack (1, 4, 9, 17, 38, 79) to a general one. Then encrypt the message (101011010100011).