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

**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).