Tutorial-XI (AES)

1. Find the SubByte transformation for the input byte "13" using GF (2^8).

2. Assuming that the 128-bit cipher key agreed upon by Alice and Bob is (24 75 A2 B3 34 75 56 88 31 E2 12 00 13 AA 54 87)$_{16}$ and fourth word of round 2 is i.e. $w_{7=}$ 9F68A5C1 Find the value of T_2 used for key expansion.

3. Find the value of RC_9 using GF (2^8)

Note: Assume irreducible polynomial ($x^8 + x^4 + x^3 + x + 1$) in GF (2^8)