Abdel Rahman Adel
1701296

Assignment 2

Theoritical Questions

(1) 1- first we fill each cell with the byte obtained by joining together its row index & column index

2- Replace the value in each cell by its multiplicative inverse in $GF(2^8)$ based on the irreducible polynomial $x^8 + x^4 + x^3 + x + 1$.
0x00 → itself since no inverse

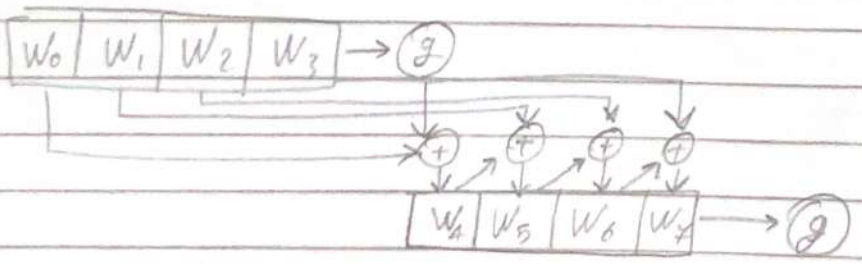
3- Represent each byte as $b_7 b_6 b_5 b_4 b_3 b_2 b_1 b_0$, b_7 = MSB & b_0 = LSB

4- Bit scramble using the following transformation for each bit b_i.

$$b_i' = b_i \otimes b_{(i+4) \bmod 8} \otimes b_{(i+5) \bmod 8} \otimes b_{(i+6) \bmod 8} \otimes b_{(i+7) \bmod 8} \otimes c_i$$

c_i = the ith bit of specific designated byte C of value 0x63

(2) We obtain them like so



i = 0

→ $W_{i+5} = W_{i+4} \otimes W_{i+1}$
→ $W_{i+6} = W_{i+5} \otimes W_{i+2}$
→ $W_{i+7} = W_{i+6} \otimes W_{i+3}$

→ $W_{i+4} = W_i \otimes g(W_{i+3})$

PAGE
DATE

(3) The function g() consists of the following steps:

1- Perform a one byte left circular rotation on the argument 4-byte word

2- Perform a byte substitution for each byte of the word returned by the previous step by using the same 16 x 16 table as used in SubBytes step in encryption round

3- XOR the bytes obtained from the previous step with what is known as a round constant. The constant is a word of whose 3 rightmost bytes are alway zero.

2