Quiz 4

Q1. Define a monoalphabetic substitution cipher and encrypt the following text: “SUSPICIOUS”
Substitution table:

S	U	P	I	C	O	
X	M	A	E	L	Q	

Ciphertext: __XMXAELEQMX_

Q2.
1. Encrypt the following plaintext bitstring using the one time pad provided with XOR operation:

plaintext	1	1	0	0	1	0	1	1	0	1
pad	0	1	1	1	0	1	0	1	1	1
ciphertext	1	0	1	1	1	1	1	0	1	0

2. How do you decrypt the ciphertext to restore the original plaintext? Show how the first (0th) bit will be decrypted

You would decrypt the ciphertext by performing the XOR operation using the same pad as the plaintext for example, the first bit would be 1 XOR 0 = 1 which is the same as the plaintext. And you would continue for the bits.

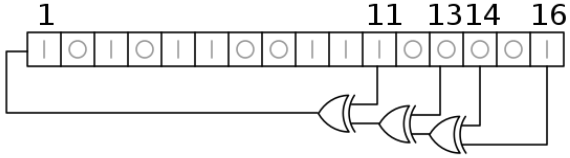
Q3. Encrypt bit string **1011010111** with Key **101 Vigenère cipher** based on the **XOR** operation

plaintext	1	0	1	1	0	1	0	1	1	1
pad	1	0	1	1	0	1	1	0	1	1
ciphertext	0	0	0	0	0	0	1	1	0	0

Q4. Give three requirements for one-time pad that must be fulfilled to make OPT encryption truly secure.

1. Key must never be reused
2. The pad must be truly random for each bit
3. The key must be the same length as the message

Q5. Below demonstrated a Linear Feedback Shift Register's state (shifts to the right) on cycle 0. What will be the state of bits 1th, 13th and 16th (output bit) on the **cycle 1 and cycle 5**?



Cycle 1: Bit 1: ____0_____ Bit 13: ____0_____ Bit 16th: _____0_____
Cycle 5: Bit 1: ____0_____ Bit 13: ____0_____ Bit 16th: _____1_____