1. We have the following cypher text DIJOOITITDGQJQBJXDCDQBTGHFXOSJQBCGJQRCTTYHGODXOTQHOOSTYJ TGJDQXYGJQBOSTGTXSDIIHNCGDFBSOXJQOHEJLDOTOSTUGDJQDQCCGJQ RJQBIDGBTIVXHUTGXFXDBDJQ and the following substitution rule c = (a * p + b) mod 26
    a. Given that cz corresponds to LM and that we know the substitution rule. We get the following two equations

       11 = (2 * a + b) mod 26
       12 = (25 * a + b) mod 26.

       We can then subtract the two to give us:

       1 = 23a mod 26

       Therefore, we need to solve the equation 1 ≡ 23a mod 26, to do this, we need to find the modulo inverse of the above equation (i.e find a s.t. 23 * a would give us a remainder of 1 if we divide by 26).

       To do this, we first check if the gcd of 23 and 26 is 1. As the gcd of 23 and 26 is 1, we know there is a modulo inverse. So now we just need to find it.

       By looping through all values in the range 0 to 25, we find that 17 *23 mod 26≡ 1

       Therefore a = 17
       Now that we know a = 17 we can substitute it back into the following equation

       11 = (2 * a + b) mod 26

       11 = (34 + b) mod 26

       -23 = b mod 26

       Therefore b = 3

$a = 17, b = 3$

b. Given our encryption equation of $c = 17\ p + 3 \bmod 26$, we need to inverse this to get our decryption equation, so we do the following below:

$c = 17p + 3 \bmod 26$

$c - 3 = 17p \bmod 26$

Here we need to multiply by the mod inverse (which we know from above is 23)

$p = 23c – 69 \bmod 26$

Let's test if the decryption is right given that we know to values

$P = 23 * 11 - 69 \bmod 26$

$P = 184 \bmod 26$

$= 2$

$P = 23 * 12 - 69 \bmod 26$

$P = 184 \bmod 26$

$= 25$

Therefore, our decryption equation is right. Now we apply it to the cipher text above to get:

alittlelearningisadangerousthingdrinkdeeportastenotthepierianspringthereshallowdraughtsintoxicatethebrainanddrinkinglargelysobersusagain

c) and d) are questions 2 & 3 under exercise 1.

c. For a key to be valid in the encryption space, we need to have an encryption function that can be invertible which is only possible with the odd numbers (except 13) in the range of 0 to 25. Thus, we have only 12 possible values for a. and since we can use any of the values for b (26 different values). This gives us 12*26 possible keys which is 312 different keys.

d. It would be weaker than a Caeser Cipher. This is because when we set b to 0, we have an even smaller key space than the above calculated. In this case we would only have 12 different keys as opposed to the Caeser ciphers' 26 possible different keys

2. Consider a Feistel cipher with four rounds. The plaintext is denoted as $P = (L_0, R_0)$ and the corresponding ciphertext is $C = (L_4, R_4)$. Obtain the ciphertext C, in terms of L_0, R_0 and the round subkeys K_i, where $i \in \{1, 2, 3, 4\}$, for each of the following round functions

Recall that the encrypt pseudocode is as follows:

For each round 1→n:

$L_i = R_{i-1}$

$R_i = L_{i-1} \oplus F(R_{i-1}, K_i)$

a. Since our round function is 0, $R_i = L_{i-1} \oplus F(R_{i-1}, K_i)$ will become $R_i = L_{i-1}$

Leading to the following

	L_i	R_i
i = 1	$L_1 = R_0$	$R_0 = L_0$
i = 2	$L_2 = R_1$ $= L_0$	$R_2 = L_1$ $= R_0$
i = 3	$L_3 = R_2$ $= R_0$	$R_3 = L_2$ $= L_0$
i = 4	$L_4 = R_3$ $= L_0$	$R_4 = L_3$ $= R_0$

Therefore, $L_4, R_4 = L_0, R_0$

b. Since our round function is R_{i-1}, $R_i = L_{i-1} \oplus F(R_{i-1}, K_i)$ will become $R_i = L_{i-1} \oplus R_{i-1}$ leading to the following

	L_i	R_i
i = 1	$L_1 = R_0$	$R_1 = L_0 \oplus R_0$

i = 2	$L_2=R_1$ $= L_0 \oplus R_0$	$R_2 = L_1 \oplus R_1$ $= R_0 \oplus L_0 \oplus R_0$ $= L_0$
i =3	$L_3 = R_2$ $= L_0$	$R_3 = L_2 \oplus R_2$ $= L_0 \oplus R_0 \oplus L_0$ $= R_0$
i = 4	$L_4 = R_3$ $= R_0$	$R_4 = L_3 \oplus R_3$ $= L_0 \oplus R_0$ $= R_0$

Therefore, $L_4, R_4 = R_0, L_0 \oplus R_0$

c. Since our round function is K_i, $R_i = L_{i-1} \oplus F(R_{i-1}, K_i)$ will become $R_i = L_{i-1} \oplus K_i$ leading to the following

	L_i	R_i
i = 1	$L_1 = R_0$	$R_1 = L_0 \oplus K_1$
i = 2	$L_2=R_1$ $= L_0 \oplus K_1$	$R_2 = L_1 \oplus K_2$ $= R_0 \oplus K_2$
i =3	$L_3 = R_2$ $= R_0 \oplus K_2$	$R_3 = L_2 \oplus K_3$ $= L_0 \oplus K_1 \oplus K_3$
i = 4	$L_4 = R_3$ $= L_0 \oplus K_1 \oplus K_3$	$R_4 = L_3 \oplus R_3$ $= R_0 \oplus K_2 \oplus K_4$

Therefore, $L_4, R_4 = (L_0 \oplus K_1 \oplus K_3, R_0 \oplus K_2 \oplus K_4)$

d. Since our round function is $R_{i-1} \oplus K_i$, $R_i = L_{i-1} \oplus F(R_{i-1}, K_i)$ will become $R_i = L_{i-1} R_{i-1} \oplus K_i$ leading to the following

	L_i	R_i
i = 1	$L_1 = R_0$	$R_1 = L_0 \oplus R_0 \oplus K_1$

i = 2	$L_2 = R_1$ $= L_0 \oplus R_0 \oplus K_1$	$R_2 = L_1 \oplus R_1 \oplus K_2$ $= R_0 \oplus L_0 \oplus R_0 \oplus K_1 \oplus K_2$ $= L_0 \oplus K_1 \oplus K_2$
i =3	$L_3 = R_2$ $= L_0 \oplus K_1 \oplus K_2$	$R_3 = L_2 \oplus R_2 \oplus K_3$ $= L_0 \oplus R_0 \oplus K_1 \oplus L_0 \oplus K_1 \oplus K_2 \oplus K_3$ $= R_0 \oplus K_2 \oplus K_3$
i = 4	$L_4 = R_3$ $= R_0 \oplus K_2 \oplus K_3$	$R_4 = L_3 \oplus R_3$ $= (L_0 \oplus K_1 \oplus K_2) \oplus (R_0 \oplus K_2 \oplus K_3) \oplus K_4$ $= L_0 \oplus R_0 \oplus K_1 \oplus K_3 \oplus K_4$

Therefore, $L_4, R_4 = (R_0 \oplus K_2 \oplus K_3, L_0 \oplus R_0 \oplus K_1 \oplus K_3 \oplus K_4)$

3.

a. As the IV is randomly chosen by Alice and is sent to Bob along with the MAC and message, Mallet can exploit this, even though it doesn't know the key. Recall that for the first block, $C_0 = E(IV \oplus P_0, K)$. C_0 is important as not only does it rely on the sent IV, but it will also be used to calculate the other blocks which is crucial for MAC calculation. Knowing this, the only way to change the first block without detection is if $C'_0 = C_0$. For this to happen, Mallet will create a new IV (IV') such that $IV' = IV \oplus P_0 \oplus P'_0$ while Mallet will also change P_0 into P'_0. That way when Bob uses the new IV and message to try get C_0 using the original formula $E(IV \oplus P_0, K)$, it will now become $C'_0 = E(IV' \oplus P'_0, K)$ and IV', as written above, is $IV \oplus P_0 \oplus P'_0$. Therefore, the calculated C'_0 becomes $C'_0 = E(IV \oplus P_0 \oplus P'_0 \oplus P'_0, K) = E(IV \oplus P_0, K) = C_0$. Despite using P'_0, we got the same cipher block and thus, the MAC will be the same and Bob wouldn't be able to tell something has changed.

b. Given that Mallet knows the K and the CBC-MAC value X for a Message M, Mallet can construct a new message which still has the same MAC value. This is because CBC-MAC is chained, meaning that all blocks are dependent on the previous one. As the MAC is C_{n-1} for a message and since Mallet knows what this value is (as it is X) and the key, Mallet can append a new block of his choice. Let this new block be P'_n such that $C'_n = E(C'_{n-1} \oplus P'_n, K)$ and since Mallet now knows one block of the message, they can add as many blocks as they want as long as the final encryption block is equal to X