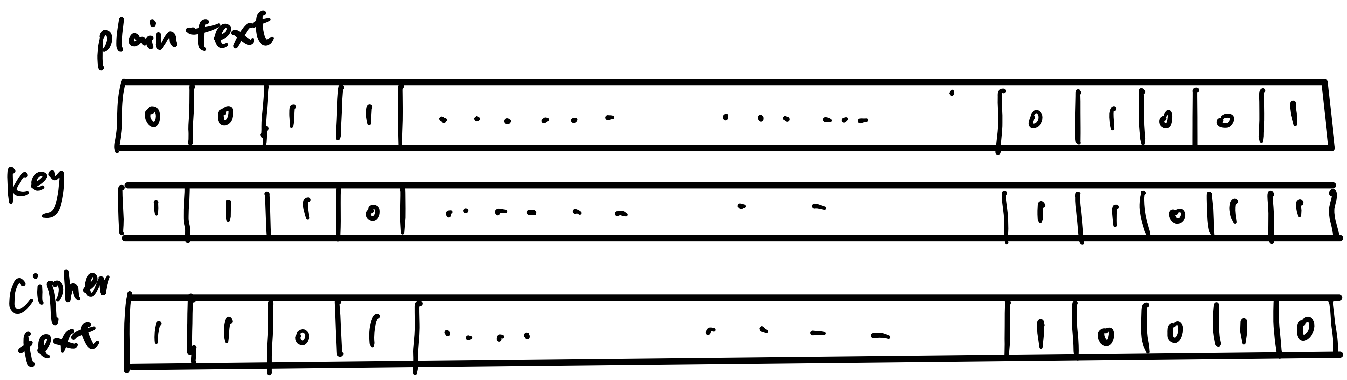
1. The value of bit 20 is 2 ^ 20 = 1,048,576Kr. To receive more than 1 million next month, one of solutions is he can let last bit be 1.



To let last five bits in decrypted message be 1, he can calculate in this way.

He knows that his own salary is less than 1 million, so the last bit of plaintext must be 0. No matter what the last bit is in ciphertext, he can just flip this bit. The procedure is shown below.

1. plaintext[20] xor k[20] = ciphertext[20] (encryption)
2. changed_ciphertext[20] xor k[20] = changed_plaintext[20] (decryption)
3. we know plaintext[20] = 0, which means 0 xor k[20] = ciphertext[20], and to let changed_plaintext[20] be 1, is to let changed_ciphertext[20] xor k[20] = 1
4. so we want to let k[20] = - changed_ciphertext and given that k[20] = ciphertext[20]
5. we need let ciphertext[20] = - changed_ciphertext[20], so just flip last bit in ciphertext.

2. Both. He knows his salary range, which is some information towards plaintext(plaintext[20] = 0), and he can intercept the traffic. So, he can actually derive the key[20], which is not mean to be known by others. so confidentiality has been broken. He can modify bits on traffic and the receiver cannot detect this, which means authenticity has been broken.

3. Because he knows his own salary(or at least the range of his own salary), which means he knows (part of) plaintext.

4. Proof:

1. plaintext[i] xor k[i] = ciphertext[i] (encryption)
2. changed_ciphertext[i] xor k[i] = changed_plaintext[i] (decryption)
3. we want to let changed plaintext be 0, which lead to changed_ciphertext xor k[i] = 0
4. so k[i] = changed_ciphertext[i],
5. so plaintext[i] xor changed_ciphertext[i] = ciphertext[i]
6. plaintext[i] = changed_ciphertext[i] xor ciphertext[i]

if $p > 1-p$, we prefer to believe that plaintext[i] = 1, in this way, attacker can filp the ciphertext[i]. and success probability is p.

if $p < 1-p$, we believe that plaintext[i] = 0, attack can keep ciphertext[i] the same. And success probability is 1-p.

So, the adversary can make the receiver obtain a 0-bit in position i with probability max(p, 1 – p).