HW1

Problem 2

a) - If the key is indeed shared, then r will in fact equal y.
- Through eavesdropping, an attacker can gather what both x and y are, since those are the messages that are transmitted through the network
- we know from step 3), that $y = k_b \oplus X$
- By using math, XORing y and X would be equivalent to X XOR$(X \oplus K_b)$
- That would leave us with the key

$$X \oplus Y = X \oplus (K_B \oplus X) = (X \oplus X) \oplus K_B = K_B$$

Example) - Let's assume that the key is 1 0 1 0
- Alice generates r as 1 0 1 1
- Therefore, X is calculated as 0 0 0 1
- Calculating y with the same key and x would result in 1 0 1 1
- The hacker can then XOR x and y to return 1 0 1 0
- ☆ The hacker got the key correct, therefore proving that it is all too possible to gain possession of the shared key.

b) - If a hacker was able to modify any of the messages, it would be incredibly easy to make Alice and Bob believe they don't share the same key.
- By XORing either X or y with $2^n - 1$, where n is the amount of bits, the message's 0s and 1s would be inverted,
- Therefore, that would be how the attacker could fool Alice and Bob into believing they do not share the same key.