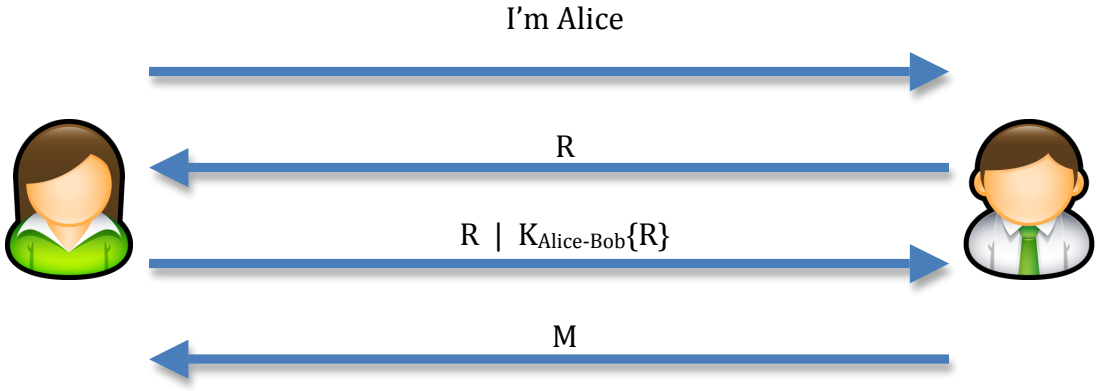
Assignment 2

Question 1 (3 points)

As a defense against a man-in-the-middle (MITM) attack for Diffie-Hellman, Alice can for example encrypt her Ta value with Bob's public key. Why does this preserves the confidentiality of the communication between Alice and Bob, given that anybody, including Eve, can encrypt whatever they want with Bob's public key and send it to Bob?

Question 2 (3 points)

Consider the following authentication protocol between Alice and one of Bob's servers. Notice that R is a nonce, $K_{Alice\text{-}Bob}$ is a secret key shared by Alice and Bob, and M is a plaintext message.

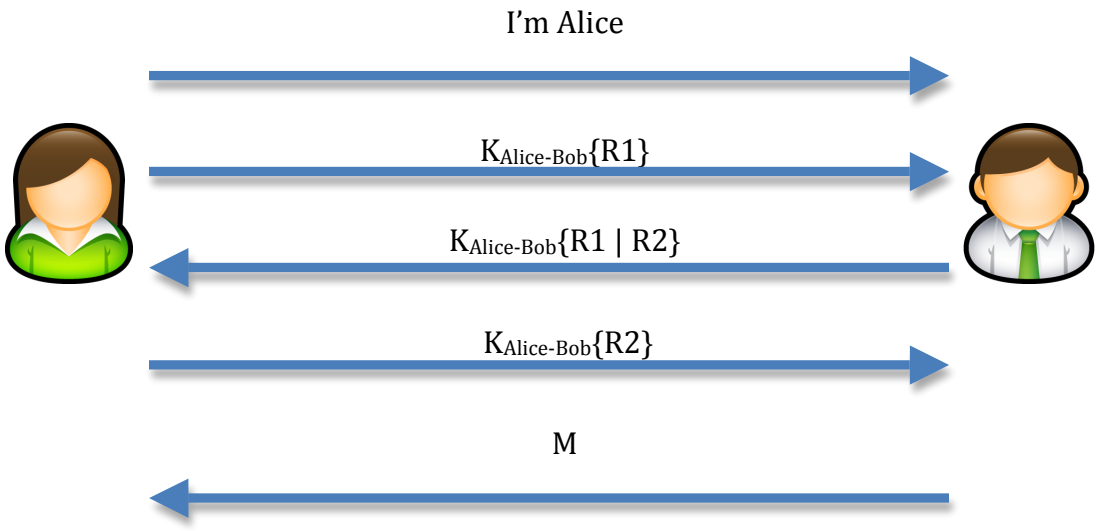


Assume the attacker, Eve, is not "in the middle" between Alice and Bob's server, and also has no way of eavesdropping their conversations. However, Eve may convince Alice that she is one of Bob's servers.

Does the above protocol provide mutual authentication? Under the threat model outlined above, can Eve successfully send a message to Alice pretending to be Bob? If so, why and how? Discuss a possible attack.

Question 3 (4 points)

Consider the modified protocol below. Assume Eve makes Alice believe that she is one of Bob's servers, and that Eve can also talk to Bob (perhaps pretending to be Alice). Is an attack still possible? Why or why not? Propose a simple fix (if needed)


I’m Alice
$K_{Alice-Bob}\{R1\}$
$K_{Alice-Bob}\{R1 \mid R2\}$
$K_{Alice-Bob}\{R2\}$
M