Flipped Classroom Session 7: Security Protocols

CS-E3130 Information Security, 3.10.2023

1. Types of attack

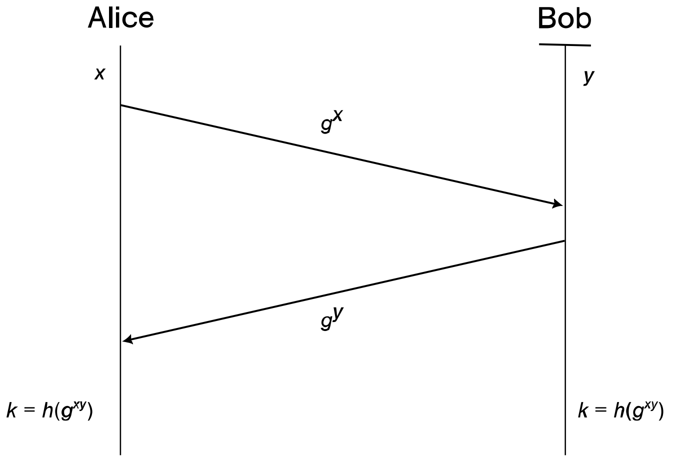
a. Name two defences against replay attacks. What assumptions do you need to make for each defence to be useful?

b. Why would a delay attack be useful to an attacker, if the message hasn't been changed from what the sender originally sent? Explain with the aid of an example, and state any assumptions that you make.

c. Why would a self-reflection attack be useful to an attacker, even though the message hasn't been changed from what the sender originally sent? Explain with the aid of an example, and state any assumptions that you make.

2. Diffie-Hellman Protocol

a. Consider the unauthenticated Diffie-Hellman protocol, drawn below.



Draw a new protocol diagram showing a man-in-the-middle attack on the unauthenticated Diffie-Hellman protocol (put a third vertical line in the middle to represent the attacker).

b. Next consider the authenticated Diffie-Hellman protocol, as shown in slides 21–27 of the lecture.

1. Draw a protocol diagram for the Authenticated Diffie-Hellman protocol.
2. Why doesn't your attack from (a) work against Authenticated Diffie-Hellman?
3. Suppose you have a function $\mathrm{Forge}(\mathrm{pk}, m)$ that can forge a signature $\sigma = \mathrm{Forge}(\mathrm{pk}, m)$ for message m that will validate with public key pk. Can you perform a man-in-the-middle attack against Authenticated Diffie-Hellman? If so, illustrate with a protocol diagram, and if not, why not?