

Tutorial 5

Computer Security
School of Informatics
University of Edinburgh

In the fifth tutorial for the Introduction to Computer Security course we cover Cryptographic Protocols. The tutorial consists of questions from past years exams.

You are free to discuss these questions and their solutions with fellow students also taking the course, and also to discuss in the course forum. Bear in mind that if other people simply tell you the answers directly, you may not learn as much as you would by solving the problems for yourself; also, it may be harder for you to assess your progress with the course material.

1 Encryption

One-time pads Inspired by the one-time pad, Alice decides to design her own protocol to confidentially send messages to Bob. Alice's protocol works as follows:

- When Alice is ready to send her message $M \in \{0, 1\}^\ell$, she randomly selects $K_A \in \{0, 1\}^\ell$, and sends to Bob the message $M_1 = M \oplus K_A$.
- Bob then randomly selects $K_B \in \{0, 1\}^\ell$ and sends to Alice the message $M_2 = M_1 \oplus K_B$.
- Next, Alice computes $M_3 = M_2 \oplus K_A$ and sends it to Bob.
- Bob may now retrieve the message M .

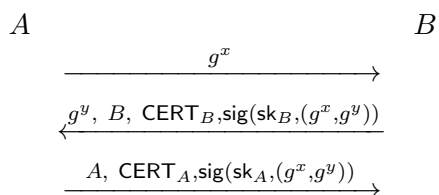
1. Show that $M = M_3 \oplus K_B$.
2. This protocol is insecure. Show that Eve can retrieve any message intended for Bob.

ElGamal

3. Recall the details of the ElGamal encryption scheme seen in class.
4. Assume you are given an ElGamal public key pk , but not the corresponding private key. Assume you are also given the ciphertexts $(e_a, c_a) = E(pk, m_a)$ and $(e_b, c_b) = E(pk, m_b)$ corresponding to the encryption using ElGamal of messages m_a and m_b under pk respectively. You are not given m_a nor m_b though. Show that you can construct a ciphertext which is a valid ElGamal encryption under the key pk of the message $m_a \cdot m_b \pmod{p}$.
5. Assume you are given an ElGamal public key pk (but not the corresponding private key) and a ciphertext $(e, c) = E(pk, m)$ which is the ElGamal encryption of some unknown message m under pk . You are also given access to an oracle that will decrypt any ciphertext other than c . ElGamal is said to be vulnerable to a chosen ciphertext attack if you can retrieve m . Show that ElGamal is indeed vulnerable to a chosen ciphertext attack.

2 The Diffie-Hellman protocol

In class, we saw the Diffie-Hellman protocol, which is a two-party key establishment protocol, secure against passive attackers. However, as we saw, the Diffie-Hellman protocol is insecure against active attackers. Indeed, a malicious agent can mount a man-in-the-middle attack to learn a key not intended for her. This attack is possible because there is no mechanism to authenticate the two parties to one another. We consider the following extension of the Diffie-Hellman protocol to thwart this attack. We assume that the parties A and B have a private signing key sk_A and sk_B respectively, and a certificate on the corresponding public key $CERT_A$ and $CERT_B$ respectively signed by a common Trusted Third Party.



The result is a shared secret $K_{AB} = g^{xy}$ from which the parties derive a session-key.

1. Briefly explain the purpose of the signatures in the protocol above. How does it defend against the attack discussed in class?
2. Show that an active man-in-the-middle, Eve, can cause:
 - A to think that she is communicating securely with B (as required),
 - but B to think he is communicating securely with Eve.

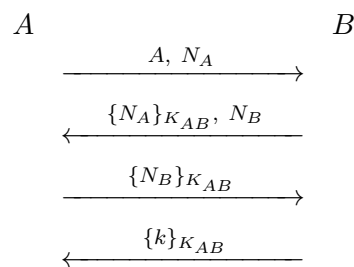
In other words, B is fooled into thinking that the subsequent encrypted messages he is receiving (from A) are coming from Eve. Note that Eve cannot eavesdrop on the resulting encrypted channel.

3. Describe how Eve can use this attack to steal money from A . For example, suppose A gives expert advice in a private chat room run by B , and that she gets paid for that.
4. Propose a way to fix the protocol to defend against this attack. Explain why your fix prevents the attack from Question 2.

3 Authentication and key-agreement protocol

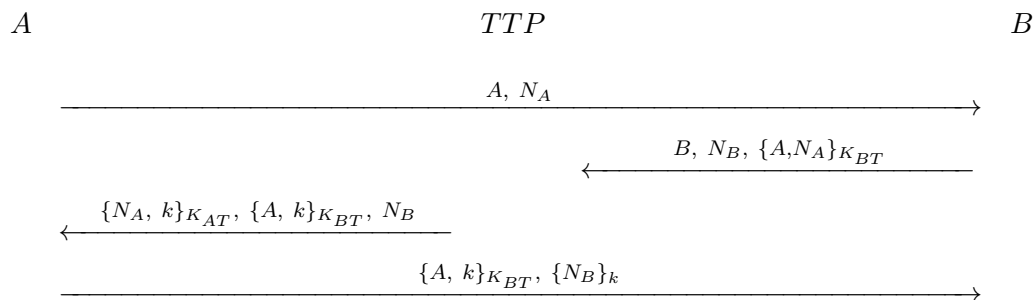
Consider the following two-party authentication and key agreement protocol. Alice and Bob want to establish a session key using a long-term symmetric key K_{AB} . First Alice generates a nonce N_A and sends it along with her identity to Bob. Bob generates his own nonce N_B and sends it together with the encryption of Alice's nonce under the long-term key K_{AB} . Alice acknowledges receipt of this message by sending the encryption of Bob's nonce under the long-

term key. Finally Bob generates the session key k and sends it to Alice encrypted under K_{AB} .



1. This protocol is flawed. Show how Eve could learn a session key that Alice thinks she has securely established with Bob. (Assume that nonces and keys have the same length.)
2. Propose a way to fix the protocol to defend against this attack. Explain why your fix prevents this attack.

If Alice and Bob do not share a long-term symmetric key they could use the following three-party authentication and key agreement protocol that relies on a trusted third party (TTP). Alice and Bob both share a long-term symmetric key K_{AT} and K_{BT} respectively with the TTP.



3. This protocol is flawed. Show how Eve could learn a session key that Alice thinks she has securely established with Bob. (Assume that nonces and keys have the same length.)
4. Propose a way to fix the protocol to defend against this attack. Explain why your fix prevents this attack.