Tutorial 2

Computer Security
School of Informatics
University of Edinburgh

In this second tutorial for the Introduction to Computer Security course we cover Cryptography and 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 Hash functions

Let $\mathcal{M} = \{0,1\}^*$ and $\mathcal{T} = \{0,1\}^n$ for some integer n.

1. Explain what does it mean for a hash function $h : \mathcal{M} \rightarrow \mathcal{T}$ to be one-way.

2. Explain what does it mean for a hash function $h : \mathcal{M} \rightarrow \mathcal{T}$ to be collision resistant.

3. Suppose $h : \mathcal{M} \rightarrow \mathcal{T}$ is collision resistant. Is h also one-way? If so, explain why. If not, give an example of a collision resistant function that is not one-way.

4. Suppose $h : \mathcal{M} \rightarrow \mathcal{T}$ is one-way. Is H also collision resistant? If so, explain why. If not, give an example of a one-way function that is not collision resistant.

5. Let p be a prime number and g a generator of $\mathbb{Z}_p^*$. Consider the function $h : \mathbb{Z} \rightarrow \mathbb{Z}_p^*$ where $h(m) = g^m \bmod p$.

   (a) Is h collision resistant? Explain your answer.

   (b) If we assume the difficulty of the discrete logarithm problem in $\mathbb{Z}_p^*$, can you explain why this function is one way?

6. Bob is on an under cover mission for a week and wants to prove to Alice that he is alive each day of that week. He has chosen a secret random number, s, which he told to no one (not even Alice). But he did tell her the value $H = h(h(h(h(h(h(h(s)))))))$, where h is a cryptographic hash function. During that week Bob will have access to a broadcast channel, so he knows any message he sends to Alice will be received by Alice. Unfortunately Bob knows that Eve was able to intercept message H. Explain how Bob can broadcast a single message everyday that will prove to Alice that he is still alive. Note that your solution should not allow anyone (and in particular Eve) to replay any previous message from Bob as a (false) proof that he still is alive.

2 Symmetric encryption

Let $(\mathcal{E}_{32}, \mathcal{D}_{32})$ be a secure (deterministic) block cipher with 32-bits key size and 32-bits message size. We want to use this cipher to build a new (deterministic) block cipher $(\mathcal{E}_{64}, \mathcal{D}_{64})$ that will encrypt 64-bits messages under 64-bits keys. We consider the following encryption algorithm. To encrypt a message M under a key K, we split M into two parts M_1 and M_2, and we also split K into two parts K_1 and K_2. The ciphertext C is then computed as $\mathcal{E}_{32}(K_1, M_1)||\mathcal{E}_{32}(K_2, M_2)$. In other words we concatenate the encryption of M_1 under K_1 using $\mathcal{E}_{32}$, with the encryption of M_2 under K_2 using $\mathcal{E}_{32}$.

1. What is the corresponding decryption algorithm? To justify your answer prove that the consistency property is satisfied.

2. Consider the following game.

   - In a first phase, the attacker choses a few plaintext messages M_1, …, M_n and gets back the corresponding ciphertexts C_1, …, C_n under some key K that he does not know. The attacker gets to know that C_1 is the ciphertext corresponding to M_1, …, C_n is the ciphertext corresponding to M_1.
   - In a second phase the attacker builds two messages M and M' and gets back C which is the encryption under K either of M or M'. But now, the attacker doesn't know if the plaintext underlying C is M or M' and has to guess it.

   Informally, a symmetric cipher is said to be subject to a chosen plaintext attack if the attacker can guess (with high probability) which of M or M' is the plaintext corresponding to C. Show that the new cipher $(\mathcal{E}_{64}, \mathcal{D}_{64})$ is subject to a chosen plaintext attack even though $(\mathcal{E}_{32}, \mathcal{D}_{32})$ is not.

3. A symmetric cipher is said to be vulnerable to a know plaintext attack if given a plaintext message M and its corresponding ciphertext C under some key K not known to the attacker, the attacker can recover the key K in a reasonable amount of time (that is significantly less than by a brute force-attack). Show that $(\mathcal{E}_{64}, \mathcal{D}_{64})$ is subject to a known plaintext attack.

3 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 protocols 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 $c_a = E(pk, m_a)$ and $c_b = E(pk, m_b)$ corresponding to the encryption using ElGamal of messages m_a and m_b under pk respectively. But you are not given m_a nor m_b. Show that how 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 $c = E(pk, m)$ which is the ElGamal encryption of some unknown message m under pk. You are furthermore 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.

4 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 him. This attack is possible because their 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.

$$\begin{array}{ccc} A & & B \\ & \xrightarrow{\qquad\qquad g^x \qquad\qquad} & \\ & \xleftarrow{g^y,\ B,\ \mathsf{CERT}_B,\mathsf{sig}(\mathsf{sk}_B,(g^x,g^y))} & \\ & \xrightarrow{A,\ \mathsf{CERT}_A,\mathsf{sig}(\mathsf{sk}_A,(g^x,g^y))} & \end{array}$$

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.

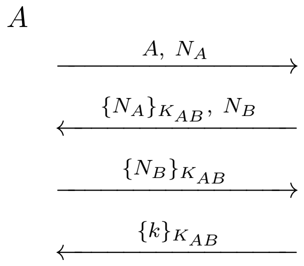
    In other words, B is fooled into thinking that the subsequent encrypted messages he is receiving (from A) are coming from Eve. Note that Eve cannot eavesdrop on the resulting encrypted channel.
    Hint: Eve can also take part in some runs of the protocol, so you may assume that Eve also has a certificate, CERT_E, on her public signature verification key sk_E.

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.

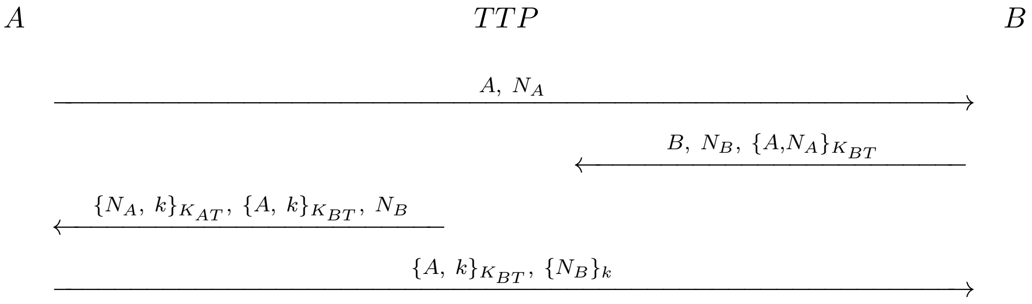
5 Authentication and key-agreement protocol

Consider the following two-party authentication and key agreement protocol. Alice (A) and Bob (B) 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 acknowledge 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. (You will 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.


A
TTP
B
$A,\ N_A$
$B,\ N_B,\ \{A,N_A\}_{K_{BT}}$
$\{N_A,\ k\}_{K_{AT}},\ \{A,\ k\}_{K_{BT}},\ N_B$
$\{A,\ k\}_{K_{BT}},\ \{N_B\}_k$

3. This protocol is flawed. Show how Eve could learn a session key that Alice thinks she has securely established with Bob. (You will 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.