Brandenburg University of Technology
Cottbus-Senftenberg
Chair of IT Security

Exercise Class
"Introduction into Cyber Security"
Winter Term 2018/2019

Introduction into Cyber Security
– 3rd Exercise Sheet –

Discussion on: 28th November 2018

Topics

This exercise deals with integrity protection and the asymmetric encryption algorithm RSA, as well as the Diffie-Hellman Key Exchange protocol.

Instructions

The exercise sheets are to be worked on by you in self-study. In the exercise classes, usually only the control / discussion of the solutions takes place. The following preparation is therefore obligatory:

1. Read the exercise sheet with the tasks carefully. In case you have questions, please resolve them in advance with the tutor or your fellow students.

2. Use the lecture slides to repeat the content of the current subject and check your knowledge.

Careful preparation and processing of the exercise sheets (in addition to attending the lecture) is an essential prerequisite for success in the final exam.

Task 1: RSA Signatures (cont.)

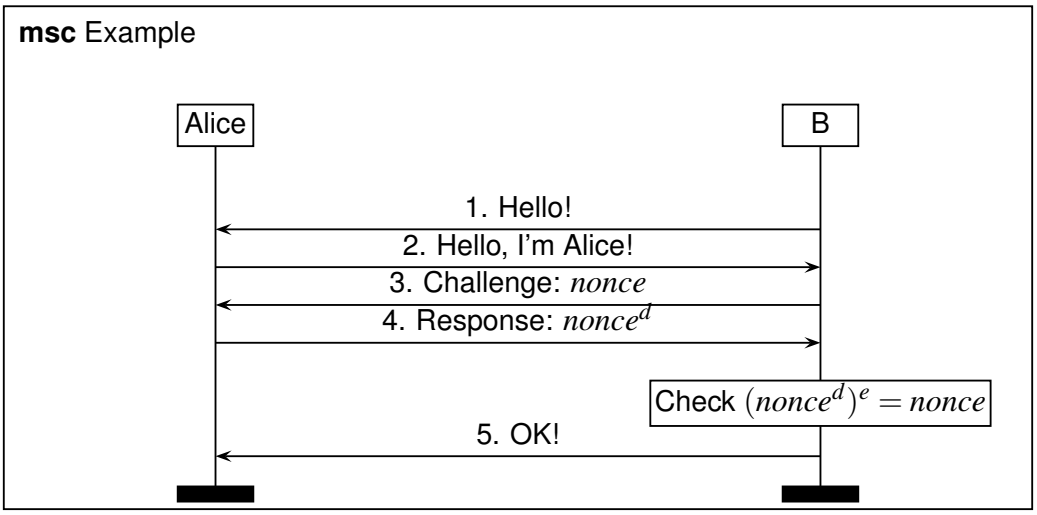

Figure 1: authentication protocol

Assume there is an authentication mechanism between Alice and an arbitrary party B as illustrated in Figure 1. Furthermore (n,e) is a RSA public key and d is the corresponding private key. Alice is the owner of the private key d.

1. What type of authentication is illustrated in Figure 1?

2. Next, Bob sends an encrypted message $E_e(m)$ to Alice. What problems occur if the same key is used for encryption and signature verification? Think of an attacker Malory who eavesdrops the communicated messages between Alice and Bob and is able to use the authentication mechanism provided by Alice.

Task 2: Efficient Modular Exponentiation

The Integer $k \in \mathbb{Z}$ is given by its binary expansion

$$k = \sum_{i=0}^{r-1} k_i 2^i, \qquad k_i \in \{0,1\}.$$

Proof by simple calculation that the modular Exponentiation of an integer z to the power of k is given by the formula

$$z^k = \prod_{i=0}^{r-1} z^{k_i 2^i}.$$

How could this idea help to calculate the Modular Exponentiation more efficient. Apply this idea to calculate $3^{27} \mod 5$ efficiently. Compare the obtained results with a direct computation.

Task 3: Diffie-Hellman Key Exchange

a) Outline the process of the Diffie-Hellman procedure. Use a graphical depiction to illustrate your description.

b) How does a man-in-the-middle attack on the Diffie-Hellman key exchange work?

c) How can such an attack be prevented or detected?

d) The Diffie-Hellman process uses modular potentiation: $a^x \mod m$. The problem inverse to modular potentiation is the calculation of the discrete logarithm of a number, i. e. the calculation of x with $a^x \mod m = (b \mod m)$, with given a, $(b \mod m)$ and m. Determine x for $3^x \mod 17 = (15 \mod 17)$.