Brandenburg University of Technology
Cottbus-Senftenberg
IT Security Group

Exercise Class
“Introduction into Cyber Security”
Winter Term 2018/2019

Introduction into Cyber Security
– 2nd Exercise Sheet –

Discussion on: 22nd November 2018

Topics

This exercise deals with integrity protection and the asymmetric encryption algorithm RSA.

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: Hash Functions

Please answer the questions below regarding the following function: $h(M) = M \mod n$

1. Is h a hash function?
2. Is h pre-image resistant?
3. Is h second pre-image resistant?
4. Is h collision resistant?
5. Assume a message authentication code is defined by $MAC_k(m) = h(k)||m$, where k is the secret key and m is a message. Is this MAC computation resistant?

Task 2: RSA

Let n be a RSA-Modulus and $\phi(n)$ known. Then n can be factorized efficiently.
Assume $n = 4757$ is an RSA-Modulus. In addition, $\phi(4757) = 4620$.

1. Factorize n.
2. Use 13 as exponent e for encryption and compute an exponent d for decryption. What conditions are satisfied by e and d?
3. Encrypt plaintext $m = 4$ and decrypt ciphertext $c' = 20$.
4. What problems occur if you have chosen a small exponent e?
5. Suppose we want to encrypt messages in our class. Therefore we use the same modulus n and each member of the class gets a valid key pair (e_i, d_i) for encrypting and decrypting messages. Is this a good idea for encryption in a fixed domain?

Task 3: RSA Signatures

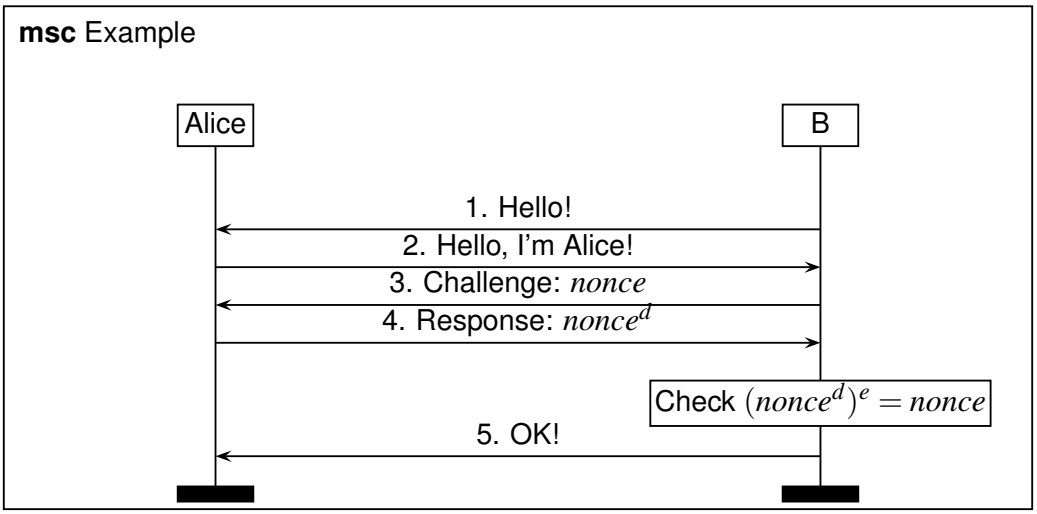

Figure 1: authentication protocol

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.