Brandenburg University of Technology
Cottbus-Senftenberg
Chair of IT Security

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

Introduction into Cyber Security
– 10th Exercise Sheet –

Discussion on: 30th January 2019

Topics

This exercise serves as an repetition of the topics learned in this term. We deal with some basics about asymmetric key cryptography especially elliptic curves, as well as the general topic of asymmetric key cryptography.

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: Repetition on Elliptic Curve Cryptography (cont.)

We consider the following simple ECC Cryptoscheme, where a message m should be send as a point P_m: (x, y) on the curve. It is the point P_m that will be encrypted.

1. Repeat the basics of elliptic curves (Definition, Addition operation, Geometrical interpretation).

2. Why we can not simply encode the message m as the x, y coordinates of P_m?

3. Have you an idea how one could encode the message m for the usage of elliptic curve cryptography?

Lets assume that the algorithm works in the following way:

For an given elliptic curve $E : y^2 = x^3 + \alpha x + \beta$ over $\mathbb{F}_q$, q prime, and an given point $G \in E$ each user selects an private key n_{user} and generates a public key $P_{\text{user}} = n_{\text{user}} \times G$. To encrypt and send a message P_m to an user B, the user A chooses a random positive integer k and calculates the cypher-text C_m as the set of two points $C_m = \{kG, P_m + kP_B\}$. To decrypt the cypher-text, B multiplies the first point, kG, by its private key n_B and subtracts the result from the second point. The user B obtains $P_m + kP_B - n_B(kG)$.

1. Proof that the encrypted message from B equals P_m.

2. Which knowledge and possibilities has an possible attacker?

Task 2: RSA and Public Key Codes

1. In connection with asymmetric encryption methods, typically “one-way functions” and “trap door functions” are being used. Explain what is meant by these terms and how them are used to accomplish the security of asymmetric key cryptography

2. Repeat the basic idea of the RSA algorithm. Which mathematical problem is used?

3. Alice and Bob wants to communicate in a secure way using RSA encryption. Therefore Alice chooses the primes $p = 5$, $q = 11$. Compute the RSA-Modul and the Euler’s totient function. Alice wants to choose $e = 3$ as her public key. Is this an valid choice? What is the corresponding private key? Now Bob wants to send the message $m = 4$ to Alice. Describe the further process of there communication.

4. What happens in the case that the message m is greater than the RSA-Modul N? How

could this problem be prevented?

5. Why is it possible to use RSA for signing as well?

Task 3: S/MIME

What is S/MIME? What is the basic difference between S/MIME and PGP (see 4th exercise sheet) in terms of key hierarchies and key trust and how does this make S/MIME more suitable in practice in a enterprise context?