Brandenburg University of Technology
Cottbus-Senftenberg
Chair of IT Security

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

Introduction into Cyber Security
– 4th Exercise Sheet –

Discussion on: 5th December 2018

Topics

This exercise deals with elliptic curve cryptography, signatures and the management of public keys.

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: Elliptic Curve Cryptography in Diffie-Hellman and El Gamal

We consider the function

$$y^2(x) = x^3 + x\,.$$

1. Is the given function an elliptic curve? Justify your answer.

2. Assume that the given function is defined on the reel numbers $\mathbb{R}$, and sketch the graph of the function in the x, y-plane.

3. Now we assume the case of the finite field $\mathbb{F}_{17} = \mathbb{Z}/17\mathbb{Z}$ with the elements $\{0, 1, \ldots, 16\}$. Calculate all points of the curve and depict them in a table.

4. We introduce an operation $*$ such that the elliptic curve over the field $\mathbb{F}$ becomes an abelian group. The point at infinity I is defined as the identity element, e.g, $P * I = I * P = P$ for any point P on the curve. The inverse of a point $P = (x, y)$ is $P^{-1} = (x, -y)$. Geometrically speaking, P^{-1} is the reflection of P in the x-axis.

   a) Clarify that for any P on the curve, the inverse P^{-1} lies on the curve as well.

   b) Name the self-inverse points (points that satisfy $P * P = I$; $P^{-1} = P$) on the curve.

5. In general, geometrically on $\mathbb{R}$, the operation $*$ could be defined, in the case of $P \neq Q$, by

   $$P * Q = S \text{ if and only if the points } P, Q \text{ and } S^{-1} \text{ are co-linear}$$

   and, in the case of $P = Q$, by

   $$P * Q = S \text{ if and only if the line between } P, S^{-1} \text{ is tangential on the curve in } P$$

   Depict the definition of the operation $*$ and interpret it geometrically.

6. For the general elliptic curve $y^2 = x^3 + \alpha x + \beta$ the result S of $P_1 * P_2$ is determined by the following rule:

   a) If $x_1 = x_2$ and $y_1 = -y_2$ then $S = I$;

   b) Else the coordinates (x_S, y_S) of S are determined by

   $$x_S = \lambda^2 - x_1 - x_2, \quad y_S = \lambda\,(x_1 - x_S) - y_1$$

with

$$\lambda = \begin{cases} (y_2 - y_1)(x_2 - x_1)^{-1} & \text{if } x_1 \neq x_2 \\ (3x_1^2 + \alpha)(2y_1)^{-1} & \text{if } x_1 = x_2, y_1 = y_2 \end{cases}.$$

Use these rules to calculate the product of $P_1 = (1,6)$ and $P_2 = (11,4)$ as well as the square $(P_1)^2$. Compare your results with the solutions obtained by the geometrical approach discussed previously.

Task 2: Signatures and Existential Forgery

1. What is 'Existential Forgery'?

2. We consider the RSA algorithm as discussed in the 2nd task sheet task 2. I.e. the parameters are given by $n = 4757$, $\Phi(4757) = 4620$, $e = 13$, $d = 1777$. Assume that this algorithm is used for signature purposes. Calculate a pair of valid message and signature, i.e. (m,s).

Task 3: Public Key Management in the case of PGP

1. What does the term "Public Key Infrastructure" describe.

2. Name the instances a PKI consist of, and describe there task shortly.

3. Beside the classical PKI's design there are decentralized approaches like the so called "Web of Trust". One widely used application of this design is used in the signing and en-/decryption process of emails by PGP. Inform yourself about PGP and the principle of "Web of Trust".

   a) What characterizes the idea of the Web of Trust? Discuss why paths in the Web of Trust should be as short and disjoint as possible.

   b) Describe examples of how a certificate is created and managed by the Web of Trust.

   c) Which types of trust does PGP distinguish?

4. *Optional:* Repeat your theoretical knowledge by the setup and usage of PGP on your own computer. Therefore solve/follow the following sub-tasks:

   a) Install PGP on your own machine and setup your email-client for the usage of PGP, i.e. create a pair of private and public key.

b) Share your public key by email with one of your colleges and import his/her public key to your own keyring.

c) Write at least one encrypted email and one unencrypted email, which is just signed with your private key.