**Understanding Cryptography**

**Homework No.5** **Due Date: 1400.03.10**

# Chapter 9

**1.**

Consider the following elliptic curve:

$$y^2 = x^3 + 2x + 2 \mod 17$$

**1.1**. Show that the condition $4a^3 + 27b^2 \neq 0 \mod p$ is fulfilled for this curve.

**1.2.** Calculate $(2,7) + (5,2)$ with only a packet calculator.

**1.3.** Verify Hasse's theorem for this curve.

**1.4.** Describe why all elements are primitive elements?

**2.**

Consider the following elliptic curve:

$$y^2 = x^3 + x + 6 \mod 11$$

Consider a $DHKE$ protocol based on this elliptic curve with Alice's private key $a = 6$. Alice receives Bob's public key $B = (5,9)$. Calculate the session key for this protocol using the ***double and add*** algorithm.

# Chapter 10

**3.** Consider an Elgamal signature scheme with $p = 31$, $\alpha = 3$ and $\beta = 6$. You receive the message $x = 10$ twice with two signatures $(17,5)$ and $(13,5)$.

**3.1.** Which one of these signatures is valid?

**3.2.** How many valid signatures are there for each message $x$ and the specific parameters chosen above?

**4.** Given an RSA signature scheme with the public key $(n = 9797, e = 131)$, show how Oscar can perform an existential forgery attack by providing an example of such for the parameters of the RSA digital signature scheme.

## 5.
## CrypTool

1. Answer the following questions with respect to the Digital Signature Algorithm;
   i. Generate a 2048bit DSA key pair using CrypTool key generation tool, with your own first name, last name, and student id (as your PIN).
   ii. Use this key to sign a text of your choice. What does the resulting file consist of?
   iii. Verify your previous signature using the same key.
   iv. Make a slight change to the signature and repeat the previous part. Explain what happens.

2. Answer the following questions about the elliptic curve cryptosystem;
   i. Create a key pair with a 256-bit prime, using your first name, last name, and student ID (as your PIN).
   ii. Use this key with ECC-AES hybrid encryption algorithm to encrypt an arbitrary document. Why are asymmetric ciphers usually used in tandem with symmetric ones to encrypt files, and why don't we use asymmetric-only encryption?
   iii. Decrypt the resulting cipher text in the previous part with the same key and algorithm.

## Programming

Do the following exercise by writing codes in your favorite programming language. Please be noted that you may use available codes on the internet only to draw inspiration but not to copy. Also, please provide brief reports on your codes in which you include your sample inputs and pictures of your program's output to them.

1. Write a program that solves the Elliptic Curve Discrete Logarithm Problem (ECDLP) using Shanks' Baby-Step Giant-Step algorithm; your program should:
   i. Take two coefficients *a* and *b*, a prime number *p*, and coordinates of two points P and Q as input.
   ii. The first three inputs construct an elliptic curve with the following formula:
   $$y^2 \equiv x^3 + a.x + b \bmod p$$
   iii. The points P and Q lie on this curve.
   iv. Use the mentioned algorithm to compute the coefficient x such that Q = x.P