Fundamentals of Cryptography

Homework 4

Dr. Mohammad Dakhilalian

Fall 2023

Theory Part

Question 1

In the DHKE protocol, the private keys are chosen from the set $\{2, ..., p-2\}$. Why are the values 1 and $p-1$ excluded? Describe the weakness of these two values.

Question 2

Find the primitive root (generator) for each of the numbers below.

1. $n = 11$
2. $n = 11^2$
3. $n = 2 * 11^2$
4. $n = 11^{100}$

Question 3

Bob wants to encrypt the plaintext $m = 10101$ using the Elgamal algorithm with parameters $p = 44927$, $a = 7$, and $d = 22105$. Find the public key, ciphertext, and ciphertext decryption.

Question 4

Consider the following elliptic curve:

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

1. Show that the condition $4a^3 + 27b^2 \neq 0 \ mod \ p$ is fulfilled for the curve.
2. Perform the additions $(2, 7) + (5, 2)$ in the group of the curve.
3. Verify Hasse's theorem for this curve. $(\#E = 19)$
4. Why are all points primitive elements?

Question 5

Let E be an elliptic curve defined over $\mathbb{Z}_7$:

$$E : y^2 = x^3 + 3x + 2$$

1. Compute all points on E over $\mathbb{Z}_7$.
2. What is the order of the group?
3. Given the element $\alpha = (0, 3)$, determine the order of α. Is α a primitive element?

Question 6

Your task is to compute a session key in a DHKE protocol based on elliptic curves. Your private key is $a = 6$. You receive Bob's public key $B = (5, 9)$. The elliptic curve being used is defined by

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

CrypTool Part

Question 7

Use the Diffie-Hellman visualization tool to see its key exchange procedure.
(Hint: go to Indiv. Procedures → Protocols → Diffie-Hellman Demonstration)

Question 8

Use the CrypTool Point addition tool (on elliptic curves) on the curve $y^2 = x^3 + 2x + 2$. For each part, explain the approach adopted by the tool to solve the problems;
(Hint: go to Indiv. Procedures → Number Theory – Interactive → Point Addition on Elliptic Curves)

1. Mark an arbitrary point P on the curve, and compute $5 * P$.
2. Mark two other points P and Q, and compute $P + Q$.