Understanding Cryptography

Homework No.5

1.

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.

2.

Consider the following elliptic curve:

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

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

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

2.3. VerifyHasse's theorem for this curve.

2.4. Describe why all elements are primitive elements?

3.1. What is the zero point of an elliptic curve?
3.2. What is the sum of three points on an elliptic curve that lie on a straight line?

4.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$(13, 5)$.

4.1. Which one of these signatures is valid?

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

5.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.

6.
CrypTool

1. Answer the following questions using 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)
   a. Mark an arbitrary point P on the curve, and compute 4*P.
   b. Mark two other points P and Q, and compute P+Q.

2. Answer the following questions with respect to the digital signature algorithm;
   a. Generate a 2048bit DSA key pair using CrypTool key generation tool, with your own first name, last name, and student id (as your PIN).
   b. Use this key to sign a document of your choice. What does the resulting file consist of?
   c. Verify your previous signature using the same key.
   d. Make a slight change to the signature and repeat the previous part. Explain what happens.

visit this link: https://www.iana.org/assignments/tls-parameters/tls-parameters.xhtml#tls-parameters-8
If you're interested to learn more about X.509 Public Key Infrastructure Certificate visit this link: https://tools.ietf.org/html/rfc5280