Understanding Cryptography

Homework No.6 **Due Date: 99.03.15**

Chapter 9

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. Verify Hasse's theorem for this curve.

2.4. Describe why all elements are primitive elements?

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 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.

3. Answer the following questions about the elliptic curve cryptosystem;
   a. Create a key pair with a 256bit prime, using your own first name, last name, and student id (as your PIN).
   b. 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?
   c. Decrypt the resulting ciphertext in the previous part with the same key and algorithm.

OpenSSL:

1. Do the following exercises about DSA;
   a. Generate a 2048bit DSA key and save it in a file named "dsa.key".
   b. The pkeyutl command can be used to perform public key operations using any supported algorithm. Use this command to sign an arbitrary text file with your previously generated key. save the signature in a file named "sign.txt".
   c. Again with the help of pkeyutl command verify your signature.
   d. Create a certificate, valid for 30 days, in X.509 standard using your DSA key. Save it in a file named "dsa.crt", and display the contents of your certificate.

2. Do the following exercises regarding the ECDH cryptosystem;

a. Generate two EC key pairs, using one of the IANA's recommended named curves. Save them in files named "ec_client.key" and "ec_server.key" respectively.
b. Extract the public keys corresponding to the previously generated keys, and save them in files named "client_pub.key" and "server_pub.key".
c. Derive the shared secret value using the pkeyutl command, along with the client's private key, and the server's public key, and name it "secret1".
d. Repeat the previous step but, this time, with the server's private key, and the client's public key, and name the driven file "secret2".
e. How are "secret1" and "secret2" related to each other and why?

Deliverables:

Put the answer to each of the questions in your answer sheet. For CrypTool and OpenSSL exercises, put the outputs generated in every step in your answer file, as well, and explain or show the steps and commands used if necessary.

To access the list of named curves you might need to 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