Understanding Cryptography

Homework No.5 **Due Date: 99.02.26**

Chapter 7

Fermats little theorem

1. Let p be a prime. then prove for every positive integer a:

$$a^p \equiv a \pmod{p}$$

$$(x+y)^p \equiv x^p + y^p \pmod{p}$$

Chinese remainder theorem

2. Let m_1 and m_2 be two positive integers that are relatively prime. Given any two integers a and b, there exists an integers x such that

$$x \equiv a \pmod{m_1}$$
$$x \equiv b \pmod{m_2}$$

Prove any two solutions of these equations are congruent to each other modulo $m_1 m_2$.

Chapter 8

Diffie- Hellman Key Exchange

3.In the DHKE protocol, the private keys are chosen from the set $\{2, \dots, p-1\}$. Why are the values 1 and $p-1$ are not considered?

NOTE*: *Describe the weakness of those two values.

4.1. Compute the two public keys and the common key for the DHKE scheme with the parameters $p = 467$, $\alpha = 2$, $a = 228$, $b = 57$ **.**

4.2. We now design another DHKE scheme with the same prime $p = 467$ as in problem 4.1. this time, we use the element $\alpha = 4$. The element 4 has order 233 and generates a subgroup with 233 elements. Compute k_{AB} for :

$$a = 400\ ,\ b = 134$$
$$a = 167\ ,\ b = 134$$

4.3. Why are the session keys identical?

5. Explain Attack Man-in-the-middle to Diffie –Hellman Key Exchange.

Primitive Roots

6.1. Find a primitive root module 11.
6.2. Find a primitive root modulo 11^2 , modulo $2 . 11^2$, and modulo 11^{100} .

ElGamal Encryption System

7. If Bob uses ELGamal with $p = 44927, a = 7, d = 22105$, find Bob's public key, encode the message $m = 10101$, and then decode the associated ciphertext.

Optional Question

8. Proof the problems of decrypting arbitrary ElGamal ciphertext mod p and breaking arbitrary Diffie-Hellman mod p are equivalent.

9.

- **CrypTool:**
  1. 1963497163 is the product of two prime numbers, use tools within the CrypTool to find these two prime numbers.
  2. Choose three large prime numbers, three Carmichael numbers, and three regular composite numbers, and use CrypTool primality test tools to do the following exercises;
     i. Test the primality of your chosen numbers using Fermat test.
     ii. Test their primality using Miller-Rabin test.
  3. Generate an asymmetric key pair using RSA algorithm, your own last name, first name and student number (as your PIN). Show the generated key pair. (Hint: go to Digital Signatures/PKI :: PKI :: Generate/Import Keys)
  4. Use the key pair generated in the previous question and a text of your choice to do the following exercises;
     i. Encrypt the text using RSA encryption.
     ii. Decrypt the ciphertext in the previous part using the same algorithm.
  5. Use Diffie-Hellman visualization tool to see its key exchange procedure. (Hint: go to Indiv. Procedures :: Protocols :: Diffie-Hellman Demonstration)

- **OpenSSL:**

Do the following exercises with the help of the useful OpenSSL toolkit.

1. Do the following exercises regarding RSA algorithm. For each part mention the command(s) you used.
    i. Generate a 2048bit RSA key, and save it in file named “private.key”.
    ii. Extract the public key out of the previously generated key and save it into a file named “public.key”.
    iii. Extract all parts that contribute to the construction of the respective private key, including prime factors, private and public exponents, and so on. Save the results in a file named “structure.txt”.
2. In OpenSSL 1.0.2 and newer, when you connect to a server, the s_client command prints the strength of the ephemeral Diffie-Hellman key if one is used. Thus, to determine the strength of some server’s DH parameters, all you need to do is connect to it while offering only suites that use the DH key exchange (For this exercise you can use “www.feistyduck.com:443” as your test website).
    i. Use the mentioned command to verify the strength of your favorite server’s DH parameters, and explain the results.

- **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.