Understanding Cryptography

Homework No.4 **Due Date: 1400.02.23**

Chapter 7

Chinese remainder theorem

1. 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 $m_1 m_2$.

Fermats little theorem

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

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

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

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 :

$$\boldsymbol{a = 400\ ,\ b = 134}$$

4.3. Why are the session keys identical?

Primitive Roots

5. Find a primitive root module 11, modulo 11^2 , modulo $2 \cdot 11^2$, and modulo 11^{100}.

ElGamal Encryption System

6. 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.

7.

- **CrypTool:**

1. 131070868929131071 is the product of two prime numbers, use tools within the CrypTool to find these 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.

- **Programming**

Do the following exercises 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 don't forget to provide brief reports on your codes.

1. Write a program that Generates large prime numbers; your program should:
   i. Take the desired number of bits (n) and a security parameter (s) as input.
   ii. Generate a number that holds n bits.
   iii. Test the primality of the previous number using Miller-Rabin algorithm with the given security parameter (s).

iv. Keep doing the previous steps until a prime number is found and print that number as output.

2. Write a program that solves discrete logarithm problem using Shanks' Baby-Step Giant-Step algorithm; your program should:

i. Take a base (g), an integer (h), and a prime number (p) as input.
ii. Use the mentioned algorithm to compute the exponent (exp), as output, such that $h = g^{exp} \bmod p$.

- **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.

Optional Question

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