Understanding Cryptography

Homework No.4 **Due Date: 01.02.04**

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

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

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

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

2.2. We now design another DHKE scheme with the same prime $p = 467$as in problem 2.1. 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 :

$$\boldsymbol{a = 400, b = 134}$$
$$\boldsymbol{a = 167\ , b = 134}$$

2.3. Why are the session keys identical?

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

4.1. What is a primitive root of a number?
4.2. Find all primitive root module 25.
4.3. Find a primitive root modulo 11^2 , modulo$2\ .\ 11^2$

5. If Alice uses ELGamal with $p = 467, g(primitive\ root) = 2, a(private\ key) = 153$,find Alice's public key, encode the message $m = 331, with\ k = 197$ and then decode the associated ciphertext.

Optional Question

6.Proof the problems of decrypting arbitrary ElGamalciphertext mod p and breaking arbitrary Diffie-Hellman mod p are equivalent.

7.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.

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

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

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

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)