COMP 417 INTRODUCTION TO CRYPTOGRAPHY

HOMEWORK 2 (6 Questions, Total=100 points)

Deadline: 26.11.2023 23:59

Read the questions and rules carefully. They are clear and well defined.

Rules:

1. No Cheating: You are not allowed to collaborate with your friends and use any kind of websites or AI. If your homework gives a sign of any of them, **directly it will be graded as zero**.

2. Goal: Please do your homework alone. Our main aim is to **learn** whatever we cover so far.

3. Submission: Submit your homework in a **single pdf. No other file types will be accepted. No multiple pdf files will be accepted. In these cases, your points will be deducted by 30%.**

QUESTIONS

1. a. Explain the man-in-the-middle attack for Diffie Hellman Key exchange protocol.

b. How can we prevent the man-in-the-middle attack for Diffie Hellman Key exchange protocol? **(5*2=10pt)**

2. a. Explain the malleability problem with the textbook RSA encryption algorithm.

b. How can malleability problem be prevented for textbook RSA encryption algorithm? **(5*2=10pt)**

3. a. Explain the malleability problem with the textbook ElGamal encryption algorithm.

b. How can the malleability problem be prevented for textbook ElGamal encryption algorithm? **(5*2=10pt)**

4. Alice and Bob want to communicate each other by using textbook RSA. They agree on p = 13 and q = 11.

a. Calculate n and totient n.

b. Create public key for Bob. Create private key for Bob.

c. Alice will send a message to Bob where m=2. Encrypt the message m=2 and send to Bob.

d. Show how Bob decrypts this message. Show the steps. **(5*4=20pt)**

5. Alice and Bob want to communicate each other by using Diffie-Hellman Key exchange protocol. They agree on q = 29 and primitive root a= 5. If Alice's secret key is 3 and Bob's secret key is 2,

a. What is public key of Alice? What is public key of Bob?

b. Show both sides how Alice and Bob construct the shared key. What is the secret key they exchanged?

c. After they exchange the keys, how can they communicate each other? Offer one cryptographic method.

d. Which hardness assumption does Diffie-Hellman Key exchange protocol depend? Explain why.

(5*4=20pt)

6. Alice and Bob want to communicate each other by using textbook ElGamal. They agree on p = 17 and generator g = 2.

a. Create a private key for Bob. Create a public key for Bob.

b. Alice will send a message to Bob where m=3. Encrypt the message m=3 and send to Bob.

c. Show how Bob decrypts this message. Show the steps.

d. Which hardness assumption does textbook ElGamal's security depend? Explain why.

(5*4=20pt)

7. a. What is the difference between RSA and ElGamal encryption systems?

b. Compare them in terms of efficiency and usability. **(5*2=10pt)**