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.

The man-in-the-middle attack is possible for Diffie Hellman Key exchange protocol since there is no authentication during key exchange. So, there can be a man in the middle to modify the message and a person who plays as the receiver to the sender and as the sender to receiver. With this way, sender will think that s/he sent the message to the receiver while sending the message to bad guy. The adversary can read the message or modify it and to receiver. Thus, while receiver thinks that s/he got the message from the sender.

b. How can we prevent the man-in-the-middle attack for Diffie Hellman Key exchange protocol?

We can prevent the man-in-the-middle attack for Diffie Hellman Key exchange protocol by adding authentication to the process. In other words, there is a need for checking who is sending the message. So, we can choose different ways to solve this issue. Firstly, we can prefer publishing a public key for receiver and sender. With this way, receiver can check the message with the sender's public key to see whether the sender is real person not the adversary. Secondly, if we have sender's RSA Public key, sender can sign the key for Diffie Hellman protocol and receiver can control it.

(5*2=10pt)

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

The malleability problem refers to the ability to modify the ciphertext into something else. In other words, the adversary can transform the ciphertext into something different for example:

Sender sends C = m^e modn → s^e x C will be new after adversary's intentions → Receiver gets C x s^e which is not original message.

In this problem, the problem does not necessarily know the decryption key, s/he can just modify the message and resends it to receiver as sender.

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

We can prevent the malleability problem for textbook RSA encryption algorithm by other security measures like padding schemes. One of the ways can be Optimal asymmetric encryption padding (OAEP) which is used by public key cryptography standard (PKCS). This scheme introduces randomness and complexity while padding the message with random values. Another way could be adding padding schemes to RSA, in this way we add random values to message. With these two ways, we add random values to message, so that we can solve the malleability.

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

The malleability problem with the textbook ElGamal encryption algorithm refers to the vulnerability in the ciphertexts. In other words, the adversary can transform the ciphertexts into something else without the need of decryption key. For example, if the ciphertext C is sent to receiver by the sender, the adversary can modify the ciphertext by doing certain math operations like multiplication (C x a where multiplication is done by adversary) or exponentiation (C^a where attacker does power operation.)

b. How can the malleability problem be prevented for textbook ElGamal encryption algorithm?

We can prevent this problem by adding other techniques in order to resist against math operations/ manipulations. Firstly, we can try to add digital signatures, if the sender signs the original message, the receiver can check if the message is really sent by the sender, or it is modified or not. As another way, we can hash the message, with this way modifying the message without knowing the related discrete algorithm would be almost impossible. Since randomness and complexity are introduced in the method. To sum up, adding authentication and digital signatures to the scheme would overcome the issue.

(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.
n = p x q = 13 x 11 = 143
ϕ(n) = (p-1) (q-1) = (13 -1) (11-1) = 12x10 = 120

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

Choose e such that 1 <e< ϕ(n) and e and ϕ(n) are coprime. This can be 1 < e < 120 so our values can be {7, 11, 13, 17}. Let's choose 7 as e.

So, Bob's public key would be (e,n) => (7, 143).

Now, let's find a d value such that exd mod ϕ(n) = 1. This can be 7 x d mod 120.

d value will be 103. Since 103 x 7 = 721 and 721 mod 120 = 1.

So, Bob's private key would be (d, n) => (103, 143).

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

The encryption of message m = 2:

c = m^e modn = 2^7 mod143 = 128 since 128<143.

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

m = c^d modn = 128^103 mod143 = 2^(7 * 103) mod 143 = 2^721 mod 143 = 2 ^(721 mod ϕ(143)) mod 143 = 2^1 mod 143 since mod ϕ(143) = (13-1) (11-1) = 120 and 721 mod 120 = 1.

So, we would have 2 mod 143 which is equal to the message.

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?
5^3 mod 29 = 9 for Alice's public key 5^2 mod 29 = 25 for Bob's public key.

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

9^2mod29 = 25^3 mod29 = 23

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

After changing the keys, they can use one of the symmetric encryption schemes this can be Ceaser when k = 23 which leads to C = m + 23 mod 26.

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

It depends on the difficulty of discrete logarithm since even though we know q and g, it would be still hard to determine the a from g^a mod q or g^(ab) from g^a mod q and g^b mod q for very large q value.

(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.

Choose random value for private key from {1…p-1}. So, assume x = 5 for Bob's private key.
Calculate y = g^x mod p = 2^5 mod 17 = 15. So, Bob's public key will be y = 15.

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

Let's choose a random k value as 3.

Calculate a = g^k mod p = 2^3 mod 17 = 8

Now, calculate b = m * y ^k mod p = 3 * 15 ^ 3 mod 17 = 10

So Alice will do operations for Enc(m) = (a,b) = (8,10) and (8,10) will be sent to Bob.

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

s = a^x mod p = 8 ^ 5 mod 17 = 9

now calculate s ^ -1 → s * s^-1 mod p = 1 → s ^-1 will be 2 since 9 * 2 mod 17 = 1

then, b * s^-1 mod p should be equal to m.

10 * 2 mod 17 = 3 which is the message sent.

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

ElGamal's security depends on the difficulty of the discrete logarithm problem. Similarly, it is based on the Diffie – Hellman exchange protocol.

(5*4=20pt)

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

Key generation:

In RSA we have p and q which are large prime numbers, then we calculate n as pxq. Then, we have e and d as exd mod $\phi(n)$ = 1. However, in ElGamal we have p as a large prime and g as generator, x as private key and y as public key from g^x mod p.

Use:

We use RSA for encryption and digital signatures however ElGamal is used for encryption mostly.

Security:

RSA depends on the difficulty of factoring large numbers while ElGamal depends on the difficulty of discrete logarithmic problems.

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

Efficiency:

Both RSA and ElGamal include modular exponentiations, for RSA this operation can be hard to compute when the key size increases and it is slower for symmetric key algorithms. Additionally, ElGamal involves multiplications besides modular exponentiation. Even though it is more challenging in terms of computations than symmetric key algorithms, ElGamal is more efficient compared to RSA for exchanging keys in some ways. So, we can say that even RSA is versatile (digital signatures, authentication), ElGamal is used for key exchanging and confidentiality.

Usability:

We have simplicity in key management for RSA however computing can be costly for limited resources. On the other hand, ElGamal is preferred for secure key exchange and confidentiality, but we need to combine it with other encryption schemes.