Assignment

Cryptography

Exercice 1 RSA Key Generation

I. User A chooses the prime parameters p= 11 and q= 23.

Find the public and the private keys of the RSA cryptosystem.

II. Knowing that the plaintext is M= 165, compute the corresponding ciphertext.

Exercice2

The RSA cryptogram *c*=10 has been intercepted. Given that the corresponding public key (*e*,*n*) equals (5,35). What would be the corresponding plaintext?

Exercice3

Alice and Bob use the Diffie-Hellman key exchange protocol with the parameters p and g equal 2 and 3, respectively..

Alice chooses a secret number equal to 6 while Bob chooses his secret equal to 15.

Compute the common key K.

Exercice4

We use the Diffie-Hellman key exchange protocol with the following conditions:

My private key and my public key are denoted by X and Y = a^X mod p, respectively, where p=29 and a=2. My public key equals 15.

(i) Choose your private key X and calculate the corresponding public key Y.

(ii) Calculate the shared key K.

Exercice5

Alice and Bob have designed the following protocol for sending a message securely from A to B. The protocol is based on the idea of the one-time pad, but without a common, shared secret. Instead, for each message, both A and B generate a random nonce and execute the following protocol to send message M from A to B

1. A ->B : M1 = M xor N_A

2. B →A : M2 = M1 xor N_B

3. A →B : M2 xor N_A

Here, in 3 rounds only the messages M1, M2 and M2 xor NA in the right hand side are sent.

1- Show that B can recover M.
2- Is the system secure? Motivate your answer?

Exercice6

A password-based protocol used by a server to authenticate clients consists of the following steps:

a. A password *P* is securely shared with every client server.
b. The client sends *x*=*h*(*P*) to the server, where *h* is a hash function.
c. The server computes *x'*=*h*(*P*) from its local copy of *P* and matches *x* and *x'*. Access is granted if *x*=*x'*.

1- Explain how an attacker can gain access to the server by capturing the traffic between the server and a specific client.
2- Improve the protocol, without modifying the number of steps, to prevent the aforementioned attack.