IT University Of Copenhagen

October 2, 2021

Security

Mandatory exercise set I

Name: Vivian Luisa Machindano Seerup

Email: vise@itu.dk

Notations:

SK: Secrete key

PK: Public Key

Implementation details

The program is written in Java

Main class name: Elgamal

Folder Content:

Report pdf

Elgamal.java : The implementation code

output.txt : The program output saved in file

Assignment report

The assignment requested an implementation of Elgamal where:

- Alice sends message to Bob,
- Eve the attacker intercepts Alice's message and reads it by finding Bob's secret key
- And finally Mallory which has a constrained devise, unable to read the message changes it without reading.

Alice

First I made it public the g, p, and Bob's PK.

After that I created "Alice Encrypt" method where by choosing a random SK she calculates her PK. With the random SK and Bob's PK she computes the shared key. After that she call's "cipher" method and encrypts the message saying "2000".

Next step she uses an array as transportation method to send her PK and the "cipher-text" to Bob.

Eve

By definition everybody can see Alice's PK and the "cipher-text" being transported but they can't read the message , because they don't have the shared key. To be able to see the message, Eve brute force Bob's SK by running a loop. In others cases this would have been hard and almost impossible but because we are using small numbers she finds Bob's SK.

After that she calculates the shared key by computing Bob's SK with Alice's PK that was seen in the transportation Array(response[]).

Mallory

Elgamal garanties confidentiality however it can't ensure integrity and authenticity.

Because Mallory doesn't have the same computation power as Eve he can't brute force the key and read the message, however he changes Alice's message by triplicating the value.

Bob

Finally Bob uses BobDecrypte method, get the data from the transportation array (response[]) calculates the shared key using is SK and Alice's PK, After that to get the message he divided "cipher-text" to the shared key. Normally Bob would know his own SK because is something that he chooses randomly himself but for this implementation I brute force to find Bob SK using a loop inside the bobDecrypte() method. So kindly ignore this as is not part of the Elgamal definition.

For the output, first I show Alice's sending a message to Bob saying 2000 as requested in the exercise1, but because the message is confidential I do not print the content value of the message.

After that I show Eve reading the message, so it prints 2000.

Next I call MalloryAdversary() method where he changes the value of the message.

And Finally I call BobDecrypte method where he reads a corrupted data saying 6000.