Mandatory exercise set I

September 20, 2023

Deadline: Thursday 03. October 2023.

Assignment

1. Alice wants to send 2000 kr. to Bob through a confidential message. She decides to use the ElGamal public key method.

   The public keying material that should be used to send the message to Bob is as follows:

   - The public shared base g=666
   - The public shared prime p=6661
   - Bob's public key $PK = g^x \ mod \ p$ =2227

   Write code that allows Alice to **build an encrypted message containing '2000'**.

2. You are now Eve, who can intercept encrypted messages, including Alice's one. Write code that allows Eve to **find Bob's private key** and **reconstruct Alice's message**. NOTE: Recall that Eve has access to the public terms g, p, and PK.

3. Finally, assume that you are now Weave, who can intercept encrypted messages but runs on a constrained device. So, Weave is unable to find Bob's private key. Write code that allows Weave to **modify Alice's encrypted message** so that when Bob decrypts it, he will get the double amount originally sent from Alice (i.e., Alice's original encrypted message is '2000', thus Bob decrypts '4000'). NOTE: Recall that you don't have Bob's private key and don't have to encrypt a message containing '4000'.

Hand-in

Write a short report that summarises your approach and results. You are expected to write your **original** code in a programming language of your choice to solve the problems **individually**.

You are expected to upload individually to LearnIt the following files

1. The exercise report as a .pdf
2. Source code files archive as .zip