Mandatory exercise set I

September 18, 2024

Deadline: October 1, 2024

Assignment

1. You are Alice and want to send 2000 kr. to Bob through a confidential message. You decide to use the ElGamal public key method.

   The keying material you should use to send the message to Bob is as follows:

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

   Send the message '2000' to Bob.

2. You are now Eve and intercept Alice's encrypted message. Find Bob's private key and reconstruct Alice's message.

3. You are now Mallory and intercept Alice's encrypted message. However, you run on a constrained device and are unable to find Bob's private key. Modify Alice's encrypted message so that when Bob decrypts it, he will get the message '6000'.

Hand-in

Write a short report that summarises your results and your methodology. You are expected to write code to solve the problems. Upload the .pdf and a .zip file containing your files to Learnit. You submit individually.