Mandatory exercise set I

February 24, 2021

Deadline: Sunday 8. March 2020.

Assignment

1. El-gamal

   (a) 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

   Build an encrypted message containing '2000'.

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

   (c) Assume that 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 double amount originally sent for Alice (so, if Alice sends '2000', then Bob would decrypt '4000'). Note that you don't have to encrypt a message containing '4000'.

2. Hash competition

   (a) Download the file provided on LearnIT (hashed.lst). The file contains hashed passwords. The file uses SHA224. Your task is to crack as many of these hashes as possible. Submit one file containing as many of the original passwords as possible, though no fewer than **624**.
   You may want to use a tool such as John the Ripper or hashcat.

Hand-in

- ElGamal: Write a short report that summarises your results and your methodology. You are expected to write code to solve the problems.

- Hash Competition: Create a text file called {your_itu_initials}.txt, containing a list of the passwords that you cracked, in the format {hash}:{password}. An example of the layout is seen below.

rosg.txt

```
b13eaa5bcb49d6c7ff9106b61ea5dcc24a75835ae11183f4ab203929:go
4c1f6281dd8c5f40d66df48604af1f6eb6b42f44eb509388ff15e459:quebec
```

You are expected to upload individually to LearnIt the following files

1. The ElGamal exercise report as a .pdf
2. The Hash competition text file as .txt
3. Any source code files archive as .zip