Mandatory exercise set I

Poppy Jones (esjo)

Exercise 1

The following python script generates a private key for Alice and encrypts the message to Bob. For the prupose of the exercise all keys are printed, even the private keys. The message Alice sends to Bob would include her public key and the cipher text.

```
import random

g   = 666
p   = 6661
bPk = 2227
y   = random.randint(1,g)

print("1: Alice's private key (y) = " + str(y))

aBk = (g ** y) % p
print("2: Alice's public key      = " + str(aBk))

privKey = (bPk ** y) % p
print("3: Shared private key      = " + str(privKey))

c = privKey * 2000
print("4: Cipher-text             = " + str(c))
```

Exercise 2

Since Eve knows the shared prime (p) she can simply brute force her way to Bob's private key (x). After that she can obtain the shared private key and use it to decrypt the cipher-text (c). The following script allows to Eve to enter Alice's public key and the cipher text to decrypt.

```
g   = 666
p   = 6661
bPk = 2227

print("Enter Alice's public key")
aPk = int(input())
print("Enter cipher text")
c = int(input())

x = 0
for i in range(p):
    if( (g ** i ) % p == bPk):
            x = i
```

```
            break
m = int (c / ((aPk ** x) % p))

print("message: " + str(m))
```

Exercise 3

Mallory knows the message `m`, so once Mallory has intercepted the message it is a matter of multiplying the cipher text correctly. Bob has no way of knowing that Mallory has tampered with the message since ElGamal encryption does not have any way to ensure authenticity.

```
m = 2000
goal = 6000

print("Please enter cipher text from Alice")
c = int(input())

print("The modified message is: " + str(int( goal * c / m )))
```