

# SEC MH1

lakt

September 2022

## 1 Report for MH1

### 1.1 Assignment 1

To send the message '2000' to Bob, we make use of the encryption formular from El Gamal with regard to our group  $Z_{6661}^*$

$$c_1 = g^r \bmod p$$

$$c_2 = m \cdot (pk^r \bmod p)$$

where:

$r$  is the secret key of the sender.

$pk$  is the public key of the recipient. In this case it is  $666^x \bmod p = 2227$

$g$  is the shared base = 666

$p$  is the shared prime = 6661

I am Alice, and I pick a random  $r = 5125$ . Now I just make use of the encryption formular, and send the  $c$  to Bob. This can be seen in **main.py**, and copied below:

```
# Shared base g
g = 666

# Shared prime p
p = 6661

# Bob's public key PK = g^sk mod p
bobPK = 2227

# Select random r as Alice's SK
r = 5125

def encryption(m, pk):
    c1 = (g**r) % p
    c2 = m * ((pk**r) % p)
    return (c1, c2)
```

```
# Alice encrypting the message to Bob
c = encryption(2000, bobPK)

print("==== Assignment 1 ====\nAlice's encrypted message to Bob: ",
      c)
```

And thus the result is:

```
==== Assignment 1 ====
Alice's encrypted message to Bob: (2695, 6992000)
```

## 1.2 Assignment 2

To find Bob's private key we make use of a brute force attack. This can be seen in **main.py**, but also copied below:

```
# brute force find Bob's SK
bobSK = 0
for i in range(6661):
    r = (g ** i) % p
    if (r == 2227):
        bobSK = i
```

Once we have Bob's secret key, we can make use of the decryption formular.

$$m = \frac{c_2}{c_1^{sk} \bmod p}$$

Where  $sk$  is the secret key of the recipient of the message, in this case Bob.

Now we can reconstruct Bob's message. This can be found in **main.py**, or copied below:

```
def decryption(c, sk):
    c1, c2 = c
    m = c2 / ((c1 ** sk) % p)
    return m

# Decrypting the message using Bob's SK
m = decryption(c, bobSK)

print("\n==== Assignment 2 ==== \nBob's secret key found using brute
      force: ", bobSK, "\nBob's
      decrypted message, as seen as Eve
      : ", m)
```

And thus the result is:

```
==== Assignment 2 ====
Bob's secret key found using brute force: 66
Bob's decrypted message, as seen as Eve: 2000.0
```

### 1.3 Assignment 3

We are Mallory, and intercepts Alice's encrypted message  $c$ . We know that the message in plain text is '2000'. Thus, to modify the message to decrypt as '6000' we can simply multiply  $c_2$  with 3, since  $\frac{6000}{2000} = 3$ .

This can be seen in **main.py**, or copied below:

```
# Mallory intercepting Alice's message, and modifying it to decrypt
#                                     to 6000
c1, c2 = c
c2 *= 3
c = (c1, c2)

# Bob decrypting the message
m = decryption(c, bobSK)
print("\n==== Assignment 3 ==== \nBob decrypting the modified
      message from Mallory and
      receiving: ", m)
```

And thus the result is:

==== Assignment 3 =====

Bob decrypting the modified message from Mallory and receiving:  
6000.0