Assignment 5

Konstantinos Filippou
ics23044

Exercise 1

Determine the order of all elements of the multiplicative groups $\mathbb{Z}_5^*$, $\mathbb{Z}_{13}^*$ and $\mathbb{Z}_{17}^*$.

$\mathbb{Z}_5^* = \{1, 2, 3, 4\}$

We compute:

$$1^1 \equiv 1 \pmod 5 \Rightarrow \text{ord}(1) = 1$$

$$2^1 \equiv 2, \quad 2^2 \equiv 4, \quad 2^3 \equiv 3, \quad 2^4 \equiv 1 \pmod 5$$
$$\Rightarrow \text{ord}(2) = 4$$

$$3^1 \equiv 3, \quad 3^2 \equiv 4, \quad 3^3 \equiv 2, \quad 3^4 \equiv 1 \pmod 5$$
$$\Rightarrow \text{ord}(3) = 4$$

$$4^1 \equiv 4, \quad 4^2 \equiv 1 \pmod 5$$
$$\Rightarrow \text{ord}(4) = 2$$

a	ord(a)
1	1
2	4
3	4
4	2

$\mathbb{Z}_{13}^*$

a	$\text{ord}(a)$
1	1
2	12
3	3
4	6
5	4
6	12
7	12
8	4
9	3
10	6
11	12
12	2

$\mathbb{Z}_{17}^*$

a	$\text{ord}(a)$
1	1
2	8
3	16
4	4
5	16
6	16
7	16
8	8
9	8
10	16
11	16
12	16
13	4
14	16
15	8
16	2

```
p = 13
Zp = [a for a in range(1, p)]

print("a\tord(a)")
for a in Zp:
    order = Mod(a, p).multiplicative_order()
    print(f"{a}\t{order}")
```

```
a       ord(a)
1       1
2       12
3       3
4       6
5       4
6       12
7       12
8       4
9       3
10      6
11      12
12      2
```

Figure 1: Enter Caption

```
p = 17
Zp = [a for a in range(1, p)]

print("a\tord(a)")
for a in Zp:
    order = Mod(a, p).multiplicative_order()
    print(f"{a}\t{order}")
```

```
a       ord(a)
1       1
2       8
3       16
4       4
5       16
6       16
7       16
8       8
9       8
10      16
11      16
12      16
13      4
14      16
15      8
16      2
```

Figure 2: Enter Caption

Exercise 2

Diffie–Hellman Key Exchange with:

$$p = 467, \quad g = 2$$

Case 1: $a = 3$, $b = 5$

$$A = 2^3 \bmod 467 = 8$$
$$B = 2^5 \bmod 467 = 32$$
$$K = 8^5 \bmod 467 = 78$$
$$K = 32^3 \bmod 467 = 78$$

Case 2: $a = 400$, $b = 134$

$$A = 2^{400} \bmod 467 = 137$$
$$B = 2^{134} \bmod 467 = 84$$
$$K = 137^{134} \bmod 467 = 90$$
$$K = 84^{400} \bmod 467 = 90$$

Case 3: $a = 228$, $b = 57$

$$A = 2^{228} \bmod 467 = 394$$
$$B = 2^{57} \bmod 467 = 313$$
$$K = 394^{57} \bmod 467 = 206$$
$$K = 313^{228} \bmod 467 = 206$$

Exercise 3

Coding functions

[64]:
```
def generate_parameters(bits):
    p=1
    while not is_prime(p):
        q = next_prime(ZZ.random_element(2^bits))
        p = 2*q + 1
    F = GF(p)
    while True:
        g = F.random_element()
        if g != 1 and g^2 != 1 and g^q != 1:
            break
    return (p,q,g,F)
```

[65]:
```
def public_private_pair(p,q,g,F):
    x = F(randint(2,p-2))
    X = g^x
    return(X,x)
```

[66]:
```
def generate_secret(X,y):
    Y = X^y
    return(Y)
```

[70]:
```
p, q, g, F = generate_parameters(100)
print(p, q)
print(g, F)

# Alice computes secret and public value
A, a = public_private_pair(p,q,g,F)
# Bob computes secret and public value
B, b = public_private_pair(p,q,g,F)
# Alice generates shared secret
generate_secret(A,b)
# Bob generates shared secret
generate_secret(B,a)
```

Figure 3: Enter Caption

Exercise 4

ElGamal with $p = 467$, $g = 2$.

First Encryption

$$B = 2^{105} \bmod 467 = 444$$
$$k_s = 444^{213} \bmod 467 = 292$$
$$c = 292 \cdot 33 \bmod 467 = 296$$

Decryption

$$292^{-1} \equiv 8 \pmod{467}$$
$$m = 8 \cdot 296 \bmod 467 = 33$$

Exercise 5

Given:

$$p = 83, \quad g = 2, \quad A = 57$$

First plaintext:

$$m_1 = 7$$

$$76 = 7k_s \pmod{83}$$

$$7^{-1} \equiv 12 \pmod{83}$$

$$k_s = 76 \cdot 12 \equiv 82 \pmod{83}$$

Since $82 \equiv -1 \pmod{83}$:

$$60 = m_2 \cdot 82 \pmod{83}$$

$$m_2 = 60 \cdot 82 \pmod{83}$$

$$\boxed{m_2 = 23}$$