

Diffie-Hellman

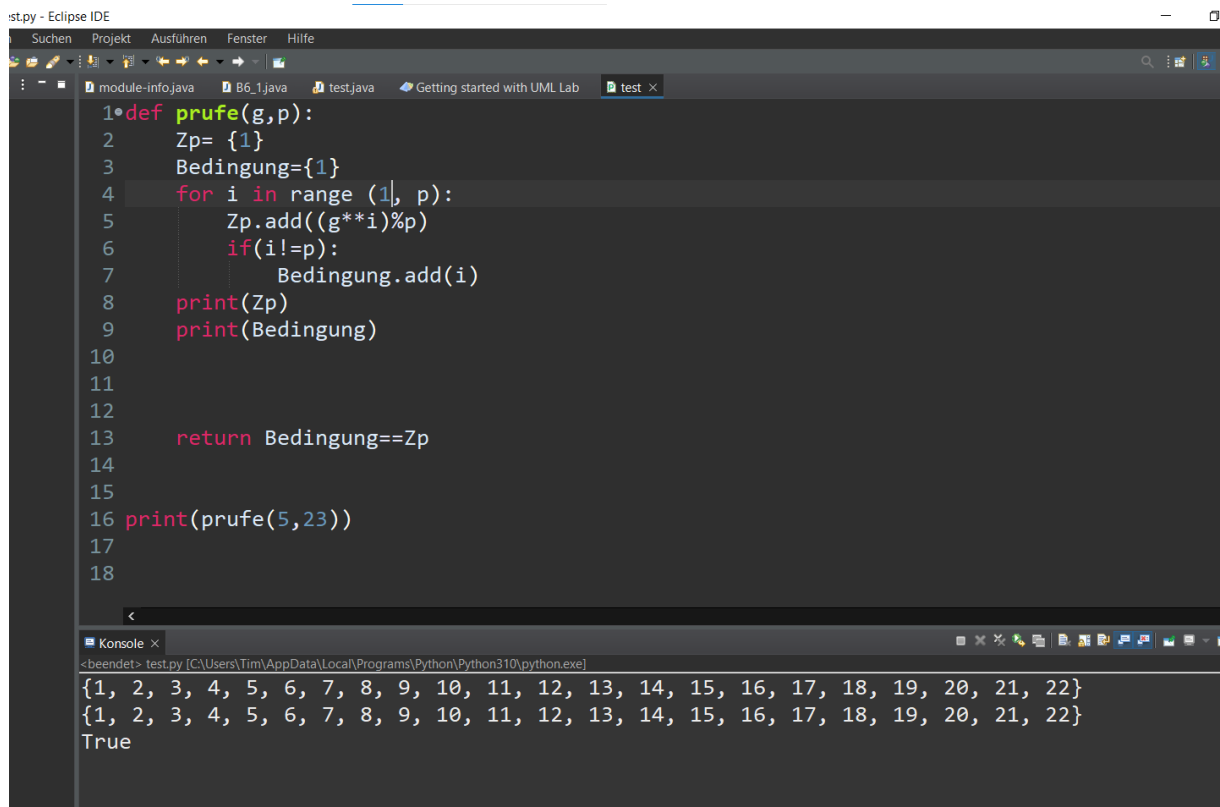
7. Aufgabe: Diffie-Hellman (1)

Alice und Bob verwenden die gemeinsame Primzahl $p=23$ und den Generator $g=5$. Alice wählt $a=7$ und Bob wählt $b=20$.

- Zeigen Sie, dass g eine Primitivwurzel von p ist.
- Welche Werte verschicken Alice und Bob? Was ist der gemeinsame Schlüssel?
- Der Angreifer Malory führt einen Man-in-the-Middle-Angriff durch. Gegenüber Alice verwendet der $m_A=6$, gegenüber Bob verwendet er $m_B=4$. Welche Werte verschickt Malory, welchen Schlüssel verwendet Malory bei einem erfolgreichen Angriff mit Alice und welchen mit Bob? Visualisieren Sie den Angriff.

Tipp zur Berechnung großer Potenzen: Sie können den Satz von Euler oder das „Wiederholte Quadrieren“ anwenden.

a) Nach meiner Funktion ist g eine Primitivwurzel



```
1 def prufe(g,p):
2     Zp= {1}
3     Bedingung={1}
4     for i in range(1, p):
5         Zp.add((g**i)%p)
6         if(i!=p):
7             Bedingung.add(i)
8     print(Zp)
9     print(Bedingung)
10
11
12
13     return Bedingung==Zp
14
15
16 print(prufe(5,23))
17
18
```

Konsole x

```
<beendet> test.py [C:\Users\Tim\AppData\Local\Programs\Python\Python310\python.exe]
{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22}
{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22}
True
```

b)

$$g^a \bmod p = 5^7 \bmod 23$$

$$7 \text{ binär} = 111$$

$$5^0 = 1$$

$$5^1 = 1 * 1 * 5 = 5$$

$$5^{10} = 5 * 5 = 25 \bmod 23 = 2$$

$$5^{11} = 2 * 5 = 10$$

$$5^{110} = 10 * 10 = 100 \bmod 23 = 8$$

$$5^{111} = 8 * 5 = 40 \bmod 23 = 17$$

Alice verschickt 17

$$B = 20$$

$$G^a \bmod p)^b \bmod p = g^{ab} \bmod p = K$$

$$5^{(20*7)} \bmod 23 = 5^{140} \bmod 23$$

Satz von Euler

$$\Phi(23) = 22$$

$$5^{140} = 5^{22} * 5^{22} * 5^{22} * 5^{22} * 5^{22} * 5^{22} * 5^8 = 5^8 \bmod 23$$

$$8 = 1000$$

$$5^0 = 1$$

$$5^1 = 5$$

$$5^{10} = 5 * 5 = 25 \bmod 23 = 2$$

$$5^{100} = 2 * 2 = 4$$

$$5^{1000} = 4 * 4 = 16 \bmod 23$$

$$K = 16$$

$$5^{20} \bmod 23$$

$$20 = 10100$$

$$5^1 = 5$$

$$5^{10} = 25 \bmod 23 = 2$$

$$5^{101} = 2 \cdot 2 \cdot 5 = 20$$

$$5^{1010} = 400 \bmod 23 = 9$$

$$5^{10100} = 9 \cdot 9 = 81 \bmod 23 = 81 - 69 = 12$$

Bob sendet 12

c)

$$mA = 6$$

$$5^6 \bmod 23$$

$$5^{110} \bmod 23$$

$$5^1 = 5$$

$$5^{10} = 5 \cdot 5 \bmod 23 = 2$$

$$5^{11} = 10$$

$$5^{110} = 100 \bmod 23 = 8$$

An Alice 8

$$mB = 4$$

$$5^4 \bmod 23$$

$$4 = 100$$

$$5^1 = 5$$

$$5^{10} = 25 \bmod 23 = 2$$

$$5^{100} = 4$$

An Bob 4

Alice

$$K_{am} = g^{am} \bmod p$$

$$= 5^{7 \cdot 6} \bmod 23 = 5^{42} \bmod 23$$

$$42 = 101010$$

$$5^1 = 5$$

$$5^{10} = 2$$

$$5^{100} = 4$$

$$5^{101} = 20$$

$$5^{1010} = 400 = 9$$

$$5^{10100} = 81 \bmod 23 = 81 - 69 = 12$$

$$5^{10101} = 60 \bmod 23 = 14$$

$$5^{101010} = 196 \bmod 23 = 8$$

$$K_{am} = 8$$

$$K_{bm} = g^{bm} \bmod p = 5^{20 \cdot 4} \bmod 23$$

$$5^{80} \bmod 23 = 5^{22} \cdot 5^{22} \cdot 5^{22} \cdot 5^{14} \bmod 23 = 5^{14} \bmod 23$$

$$14 = 1110$$

$$5^1 = 5$$

$$5^{11} = 5 \cdot 5 \cdot 5 = 10$$

$$5^{110} = 100 \bmod 23 = 8$$

$$5^{111} = 8 \cdot 5 = 40 \bmod 23 = 17$$

$$5^{1110} = 17 \cdot 5 = 50 + 35 = 85 \bmod 23 = 13$$

$$K_{bm} = 13$$

