IT-Security Cryptography and Secure Communications

Exercise: **Public Key Cryptography**
Lecturer: *Prof. Dr. Michael Eichberg*
Version: 2024-02-03

1. Execute the Square-and-Multiply algorithm for 3^17 mod 23.

Solution

```
k = 0001 0001b

i = 4; f =   3 =>
i = 3; f =   9 =>
i = 2; f =  81 mod 23 = 12 =>
i = 1; f = 144 mod 23 = 6 =>
i = 0; f = (((6 * 6) mod 23) * 3) mod 23 = 16
```