IT-Security Cryptography and Secure Communications

Exercise: **Public Key Cryptography**
Lecturer: *Prof. Dr. Michael Eichberg*
Version: 2023-10-19

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
```

2. Perform an encryption of a message using RSA.

   I.e., choose 2 small prime numbers, compute e,d,n. Then encrypt the message (i.e., a (rather) small value) using the public key of a fellow student and send him the encrypted message. Let her/him decrypt your message. Afterwards validate that the encryption is successful.

Solution

Let's assume that $p = 7$ and $q = 11$.

$n = p \times q = 77$

$\phi(n) = (p - 1)(q - 1) = 6 \times 10 = 60;$

Hence the message has to be "less than" 60.

Compute e such that $gcd(\phi(n), e) = 1$.

In this case, 2 to 6 are not possible because they all divide 60. We will select $e = 7$

Compute d; i.e., $ed \; mod \; \phi(n) = 1$. $d = 43$; $(43 \times 7) \; mod \; \phi(60)$

Now: PU = {7,77}, PR = {43,77}.

Let the message M be "13": $C = 13^7 \; mod \; 77 = 62$.

To get the plaintext compute $P = 62^{43} \; mod \; 77$.

3. Can you think of a scenario in which fault-based attacks may be practical?

Solution

It is always practical when you have physical access to a device for a reasonable time to execute the attack. E.g., in IT-forensics.