

IT-Security Cryptography and Secure Communications

Excercise: Public Key Cryptography

Lecturer: Prof. Dr. Michael Eichberg

Version: 2023-10-12

1. Execute the Square-and-Multiply algorithm for $3^{17} \bmod 23$.
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.
3. Can you think of a scenario in which fault-based attacks may be practical?