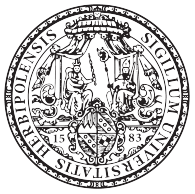

Introduction to Informatics
WiSe 2024/2025

Prof. Dr. Ingo Scholtes
Chair of Informatics XV
University of Würzburg

Exercise Sheet 05

Published: November 27, 2024
Due: December 9, 2024

Please upload your solutions to WueCampus as a scanned document (image format or pdf), a typesetted PDF document, and/or as a `jupyter` notebook.

1. **Caesar Cipher**
   (a) Use the shift key 5 to encrypt the following message with the Caesar cipher:
   `The quick brown fox jumps over the lazy dog.`
   (b) The following messages are encrypted with the Caesar cipher with unknown shift keys (from 0 to 25). Find the shift keys and decrypt the messages.
   (*Hint: You can use the functions in the attached Jupyter notebook for help.*)
      (i) `krz grhv d frpsxwhu jhw guxqn?`
      (ii) `kv vcmgu uetggpujqvu!`

2. **Vignère Cipher**
   (a) Use the Vignère cipher to encrypt the following message with the key `'SECRET'`:
   `Meet me at the park.`
   (b) The following word is encrypted with the Vignère cipher with the key `'KEY'`. Decrypt the word:
   `RIJVS`

3. **RSA key exchange**
   RSA is a widely-used encryption system that allows secure communication between two parties. It works by creating a pair of keys: a public key, which anyone can use to encrypt a message, and a private key, which is kept secret and used to decrypt it. The system is based on the difficulty of breaking large numbers into their prime factors, making it highly secure. This method enables Anna and Bob to exchange information safely, even if others can see the public key.
   Use the prime numbers $p = 3$ and $q = 7$ to perform all steps of the RSA algorithm. Follow the procedure in the columns below to generate keys, encrypt a message $M = 2$, and decrypt it.

1. Chooses two (large) prime numbers p and q.
2. Computes:

$$n = p \cdot q, \quad \phi(n) = (p-1)(q-1)$$

3. Selects a **public key** e such that:

$$1 < e < \phi(n) \quad \text{and} \quad \gcd(e, \phi(n)) = 1$$

4. Computes the **private key** d such that:

$$d \cdot e \equiv 1 \mod \phi(n)$$

5. Publishes (e, n) as the public key.

6. Receives Bob's public key (e, n).
7. Chooses a plaintext message M to send.
8. Encrypts the message:

$$C = M^e \mod n$$

9. Sends the ciphertext C to Bob.

10. Receives the ciphertext C from Anna.
11. Decrypts C using the private key d:

$$M = C^d \mod n$$

12. Recovers the original plaintext message M.

Here $\gcd(a, b)$ is the greatest common divisor of a and b
$M^e \mod n$ is the remainder when M^e is divided by n.
$d \cdot e \equiv 1 \mod \phi(n)$ is equivalent to $d \cdot e \mod \phi(n) = 1$.