# Laboratory work 12

Author: Dávid Kromka

**Algorithm Description - Task 1: Factorization**

Function **factorize(n)**:

1. **Input:**
   * **n**: Integer to be factorized.
2. **Algorithm:**
   * Iterate from **i = 2** to the square root of **n**.
   * If **n** is divisible by **i**, return the factors **(i, n//i)**.

Obrázok, na ktorom je hodiny, písmo, číslo, digitálne hodiny

Automaticky generovaný popis

**Algorithm Description - Task 2: RSA Encryption and Decryption**

Given Parameters:

* **p**, **q**: Prime numbers.
* **n**: Modulus (**n = p \* q**).
* **e**: Public exponent.
* **d**: Private exponent.
* **m**: Message to be encrypted.

Steps:

1. **Calculate Public Key:**
   * Given **n** and **e**, calculate the public key **(n, e)**.
2. **Encryption:**
   * Convert the message **m** to an integer (**m\_int**).
   * Encrypt the message using the RSA encryption formula: **C ≡ m^e (mod n)**.
3. **Decryption:**
   * Decrypt the cryptogram **C** using the private key **(n, d)**: **m\_decrypted ≡ C^d (mod n)**.
4. **Print Results:**
   * Print the public key, cryptogram **C**, and the decrypted message.

Obrázok, na ktorom je písmo, text, snímka obrazovky, typografia

Automaticky generovaný popis

**Algorithm Description - Task 3: Substitution Cipher Decryption**

Function **decrypt(ciphergram, key)**:

1. **Inputs:**
   * **ciphergram**: Encrypted text (string of digits).
   * **key**: Key for decryption.
2. **Algorithm:**
   * Split the **ciphergram** into pairs of digits.
   * For each pair, convert it to an integer and apply the decryption formula.
   * Convert the result to a character and append it to the decrypted text.

Function **brute\_force\_decrypt(ciphergram)**:

1. **Input:**
   * **ciphergram**: Encrypted text (string of digits).
2. **Algorithm:**
   * Iterate through all possible keys (1 to 26) and decrypt the text using the **decrypt** function.
   * Print the decrypted text for each key.
3. **Example Usage:**
   * Given **ciphergram = "202412"**, perform a brute-force decryption.
   * Print the decrypted text for each possible key.
   * Found algorithm is **AES** with key **19**

Obrázok, na ktorom je text, snímka obrazovky, dizajn

Automaticky generovaný popis