# Laboratory work 9

Dávid Kromka

**Task 1, 2, 3, and 4: RSA Encryption and Decryption**

Task 1: RSA Encryption and Decryption with Different Keys

1. **Algorithm Overview:**
   * **Input:**
     + **plaintext**: The text to be encrypted or decrypted.
     + **e** and **d**: The public and private exponents, respectively.
     + **n**: The modulus for both encryption and decryption.
   * **Output:**
     + For encryption: A list of integers representing the encrypted ciphertext.
     + For decryption: The decrypted plaintext as a string.
2. **RSA Encryption (rsa\_encrypt) Algorithm:**
   * Initialize an empty list **ciphertext\_integers** to store the encrypted integers.
   * For each character in the plaintext:
     + Compute the modular exponentiation of **(ord(char) - 64)** with exponent **e** and modulus **n**.
     + Append the result to **ciphertext\_integers**.
   * Return **ciphertext\_integers**.
3. **RSA Decryption (rsa\_decrypt) Algorithm:**
   * Initialize an empty list **plaintext\_integers** to store the decrypted integers.
   * For each integer in the ciphertext:
     + Compute the modular exponentiation of the integer with exponent **d** and modulus **n**.
     + Add 64 to the result and append it to **plaintext\_integers**.
   * Convert the decrypted integers to characters and concatenate them to form the plaintext.
   * Return the plaintext.

Obrázok, na ktorom je text, písmo, snímka obrazovky

Automaticky generovaný popis

Task 2: RSA Encryption and Decryption with Swapped Keys

1. **Algorithm Overview:**
   * Perform RSA encryption and decryption using swapped public and private keys.
2. **Task 2 Execution:**
   * Set up the parameters for RSA with different prime numbers (**p** and **q**).
   * Choose a public key **e** such that **gcd(e, phi) = 1**.
   * Calculate the modular inverse of **e** modulo **phi** to get the private key **d**.
   * Encrypt the plaintext using the private key (**d**) and decrypt it using the public key (**e**).
   * Display the encrypted and decrypted text.

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

Automaticky generovaný popis

Task 3: Generating Possible Public Keys

1. **Algorithm Overview:**
   * Generate possible public keys given two prime numbers **p** and **q**.
   * Public keys are pairs **(e, n)** where **e** is coprime with **(p-1)(q-1)**.
2. **Generate Keys (generate\_keys) Algorithm:**
   * Calculate **n = p \* q** and **(p-1)(q-1)**.
   * Iterate over potential values of **e** from 2 to **(p-1)(q-1)** (exclusive).
   * If **e** and **(p-1)(q-1)** are coprime (gcd is 1), add **(e, n)** to the list of public keys.
   * Return the list of public keys.

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

Automaticky generovaný popis

Obrázok, na ktorom je text, snímka obrazovky

Automaticky generovaný popis

Obrázok, na ktorom je hodiny, písmo, číslo, snímka obrazovky

Automaticky generovaný popis

Task 4: RSA Encryption and Decryption with the Same Keys

1. **Algorithm Overview:**
   * Perform RSA encryption and decryption using the same keys as in Task 1.
2. **Task 4 Execution:**
   * Encrypt the plaintext using the public key (**e**).
   * Decrypt the ciphertext using the private key (**d**).
   * Display the encrypted and decrypted text.

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

Automaticky generovaný popis