# Laboratory work 4

Author: Dávid Kromka

**Task 1: Modulo operations**

2 mod 4 = 2

78 mod 33 = 12

51 mod 7 = 2

27 mod 47 = 27

7-1 mod 47 = 27

19-1 mod 47 = 5

4-1 mod 7 = 2

4-1 mod 15 = 4

3-1 mod 7 = 5

4-1 mod 17 = 13

9-1 mod 17 = 2

2-1 mod 6 -> 2 is not invertible mod 6

**Algorithm Description - Task 2: Vector of Residuals**

Vector of Residuals for Modulus Operation:

1. **Inputs:**
   * **number**: Integer to calculate residuals.
   * **modulus**: Modulus for the operation.
2. **Algorithm:**
   * Calculate the vector of residuals for the given **number** and **modulus**.
   * Store the result in a list (**residuals**).

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

Automaticky generovaný popis

**Algorithm Description - Task 3: Common Secret Key Calculation**

Common Secret Key for Asymmetric Encryption:

1. **Inputs:**
   * For each scenario:
     + **base**: Base value for the power operation.
     + **modulus**: Modulus for the operation.
     + **transmitter\_key**: Exponent for the transmitter.
     + **receiver\_key**: Exponent for the receiver.
2. **Algorithm:**
   * Calculate the common secret key using the formula **(base^transmitter\_key) mod modulus**.
   * Print the result for each scenario.

Modular Inverse Check:

1. **Algorithm:**
   * Attempt to calculate the modular inverse using the function **pow(base, -1, modulus)**.
   * If successful, print the result.
   * If an exception occurs (indicating that the modular inverse does not exist), catch the exception and print an error message.

Obrázok, na ktorom je text, snímka obrazovky, písmo

Automaticky generovaný popis