

Ministry of Education, Culture and Research of the Republic of Moldova

Technical University of Moldova

Department of Software and Automation Engineering

**REPORT**

Laboratory work No. 3

**Discipline**: Cryptography and Security

Elaborated: FAF-221, Cusnir Grigorii

Checked: asist. univ., Dumitru Nirca

Chișinău 2023

**Introduction**

The Vigenère cipher is a method of encrypting alphabetic text by using a simple form of polyalphabetic substitution. It uses a keyword to encrypt and decrypt the text. The letters of the text are shifted based on the corresponding letters of the keyword. This implementation is designed for Russian text, with 33 letters in the alphabet, and works on uppercase Russian characters.

The task here is to implement the Vigenère cipher for messages in Russian (with 33 letters: А, Б, В, Г, Д, Е, Ё, Ж, З, И, Й, К, Л, М, Н, О, П, Р, С, Т, У, Ф, Х, Ц, Ч, Ш, Щ, Ъ, Ы, Ь, Э, Ю, Я). The cipher will work by mapping each letter to a number between 0 and 32, using the key to apply a shifting cipher on the message.

**Functional Description**

**The program performs the following operations:**

* Encrypting messages using the Vigenère cipher.
* Decrypting messages using the inverse of the Vigenère cipher.
* The user can choose between encrypting or decrypting a message, and they are required to input a valid key and message.

**Key requirements:**

* The key must be at least 7 characters long.
* The key must only contain uppercase Russian alphabet letters.

**The message:**

* Will be converted to uppercase.
* Will have spaces removed before processing.
* Must only contain valid Russian alphabet letters (A-Я).

**Code Walkthrough**

**Input Handling:**

* The program prompts the user to choose an operation: encrypt, decrypt, or exit.
* The user is asked to provide a key and a message (text to be encrypted or decrypted).
* The key and message are validated to ensure they consist only of uppercase Russian letters and meet the length requirements.

**Encryption Method (encrypt):**

* The function iterates through each letter of the message and finds its index in the alphabet.
* For each letter, the corresponding key letter is also mapped to its index in the alphabet.
* The ciphertext index is calculated by adding the plaintext letter index and key letter index, then taking the modulus of 33.
* The result is appended to the encrypted message.

**Decryption Method (decrypt):**

Similar to encryption, but instead of adding the key index to the plaintext index, the key index is subtracted from the ciphertext index, and the modulus is taken to ensure the result is within bounds.

**User Interaction:**

The user can encrypt or decrypt messages by entering the appropriate choice. The program ensures that the inputs are valid and handles errors (e.g., invalid characters, too short keys).

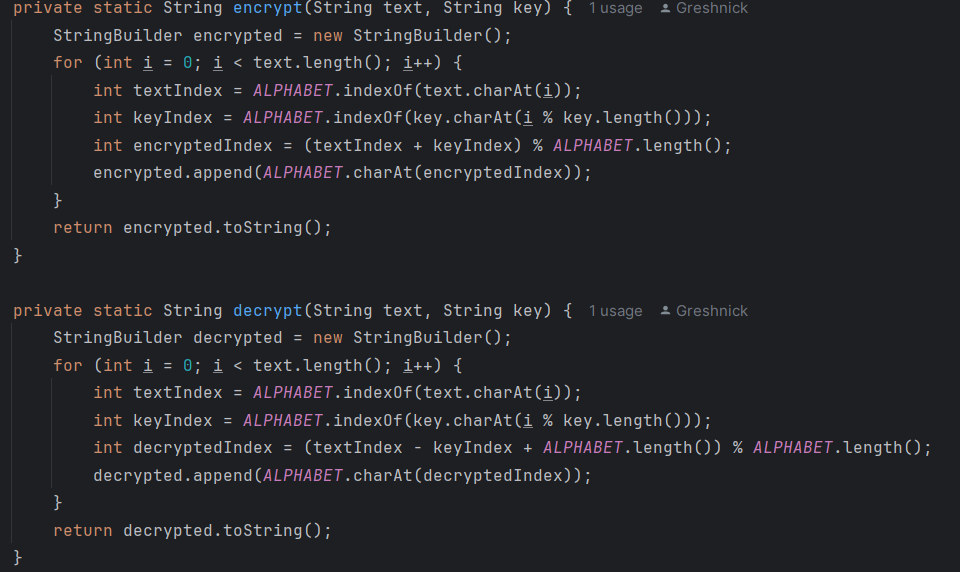
**Key Constraints:**

* Minimum Key Length: 7 characters.
* Character Set: Only uppercase Russian letters (А-Я) are allowed.
* Message Processing: All input messages will be stripped of spaces and converted to uppercase before encryption or decryption.

**Error Handling:**

* If an invalid key (e.g., less than 7 characters or containing non-Russian alphabet letters) is entered, the program prompts the user to re-enter it.
* If a message contains invalid characters (e.g., non-Russian letters), the program displays an error and requests a valid input.

**Code:**

****

**Conclusion:**

This implementation of the Vigenère cipher in Java for the Russian alphabet provides a secure method of encrypting and decrypting messages. The program ensures that user inputs are valid and performs both encryption and decryption efficiently. By following the Vigenère cipher's encryption and decryption formulas, it supports secure text transformations, and the use of a key ensures variability and complexity in the cipher output.