Neamtu Alexandra
group 935

Public Key Cryptography - Lab 1
Documentation

The **Bellaso (Vigenère) Cipher** consists of several Caesar ciphers in sequence with different shift values. In a Caesar Cipher, each letter of the alphabet is shifted along some number of places; for example, in a Caesar cipher of shift 3, `A` would become `D`, `B` would become `E`, `Y` would become `B` and so on. We use the Bellaso Cipher in order to encrypt an decrypt a given text.

To **encrypt** a message text using this cipher, you will need the following:

- a **message** you want to encrypt (plain text); this message should only contain english alphabet letters and white spaces
- a **keyword** (encryption key) after which the app will encrypt the text; the keyword should only contain english alphabet letters and white spaces

When the user press the *"Encrypt message" button, a*fter the app gets the data, it validates it. If both the text and the keyword are correct, the encrypted message will be displayed in uppercase letters, otherwise an error message will be displayed such that the user can find out what were the mistakes.

To **decrypt** a message text using this cipher, you will need the following:

- a **message** you want to decrypt (cipher text); this message should only contain capital english alphabet letters and white spaces
- a **keyword** (encryption key) which should be the same as the one used to encrypt the initial text; the keyword should only contain english alphabet letters and white spaces

When the user press the *"Decrypt message" button, a*fter the app gets the data, it validates it. If both the text and the keyword are correct, the decrypted message will be displayed in lowercase letters, otherwise an error message will be displayed such that the user can find out what were the mistakes.