Министерство образования Республики Беларусь
Учреждение образования
БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ИНФОРМАТИКИ И РАДИОЭЛЕКТРОНИКИ

КАФЕДРА ИНФОРМАТИКИ

Лабораторная работа № 1

Шифр Цезаря

Выполнил студент гр. 953501
Кременевский В.С.

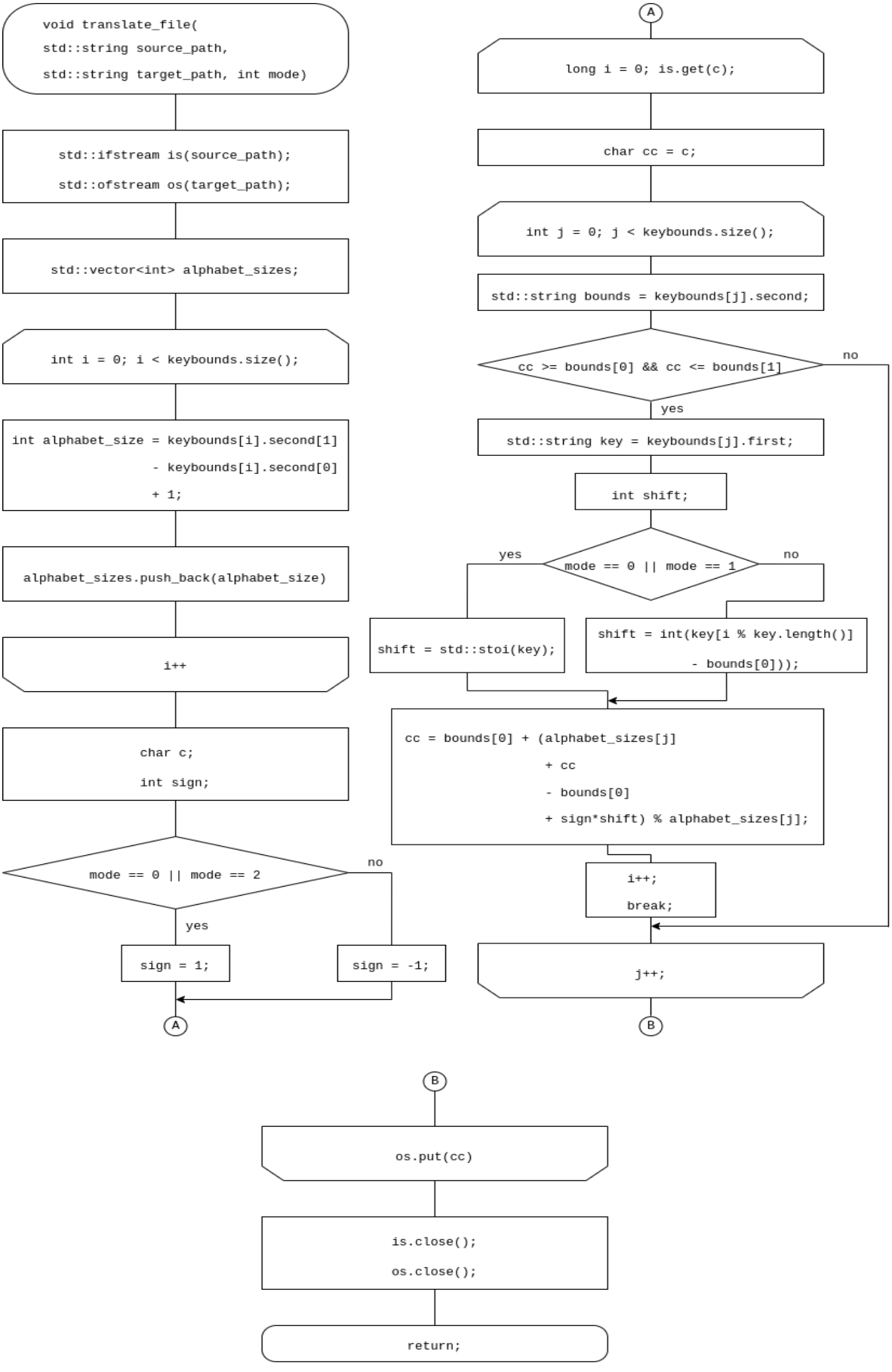
Проверил
Протько М.И.

Минск 2022

1. Введение

Цель данной лабораторной работы – реализовать программные средства шифрования и дешифрования текстовых файлов при помощи шифра Цезаря, (шифра сдвига, кода Цезаря) и шифра Виженера.

2. Блок-схемы алгоритмов



3. Результаты выполнения программы

```
Caesar encryption:
word:  DUBAI
key 5
encrypted: IZGFN
decrypted:  DUBAI

Vigenere encryption:
word:  ATACKATDAWN
key LEMON
encrypted: LXMQXLXPOJY
decrypted:  ATACKATDAWN
```

```
Caesar encryption:
word:  SomeStaff
key 9
encrypted: BxvnBcjoo
decrypted:  SomeStaff

Vigenere encryption:
word:  enctyptmeplease
key imkey
encrypted: mzmxwxfwintqkwc
decrypted:  enctyptmeplease
```

```
Caesar encryption:
word:  ONEmoreEXAMPLE
key 99
encrypted: JIZhjmzZSVHKGZ
decrypted:  ONEmoreEXAMPLE

Vigenere encryption:
word:  GOODmorning
key one
encrypted: AHYXzsfambt
decrypted:  GOODmorning
```

4. Код программы

Шифр цезаря:

```python
def caesar_encrypt(word, shift):
    n_alphabet = 26
    small_a = 97
    big_A = 65
    encrypted = ''
    for ch in word:
        base = big_A
        if ord(ch) > 96:
            base = small_a
        encrypted += chr(((ord(ch) - base + shift) % n_alphabet) + base)
    return encrypted


def caesar_decrypt(encrypted, shift):
    n_alphabet = 26
    small_a = 97
    big_A = 65
    decrypted = ''
    for ch in encrypted:
        base = big_A
        if ord(ch) > 96:
            base = small_a
        decrypted += chr((ord(ch) - base - shift + n_alphabet) % n_alphabet + base)
    return decrypted
```

Шифр Виженера:

```python
def vigenere_encrypt(word, key):
    n_alphabet = 26
    small_a = 97
    big_A = 65

    n_word = len(word)
    new_key = ''
    encrypted = ''

    i = 0
    while len(new_key) != len(word):
        new_key += key[i]
        i += 1
        if i == (len(key)):
            i = 0
    for i in range(len(word)):
        ch = word[i]
        k = new_key[i]
        base = big_A
        if ord(ch) > 96:
            base = small_a
        smallest = ch if ord(ch) < ord(k) else k
        diff = abs(ord(ch) - ord(k))
        encrypted += chr(((ord(smallest) + (ord(smallest) - base) - base + diff) % n_alphabet) + base)
    return encrypted
```

```python
def vigenere_decrypt(encrypted, key):
    n_alphabet = 26
    small_a = 97
    big_A = 65

    n_word = len(encrypted)
    new_key = ''
    decrypted = ''

    i = 0
    while len(new_key) != len(encrypted):
        new_key += key[i]
        i += 1
        if i == (len(key)):
            i = 0
    for i in range(len(encrypted)):
        ch = encrypted[i]
        k = new_key[i]
        base = big_A
        if ord(ch) > 96:
            base = small_a
        decrypted += chr(((ord(ch) - base) - (ord(k) - base)) % n_alphabet + base)
    return decrypted
```

5. Выводы

В ходе данной лабораторной работы были реализованы программные средства шифрования и дешифрования текстовых файлов при помощи шифра Цезаря, (шифра сдвига, кода Цезаря) и шифра Виженера.

Данные алгоритмы шифрования не обеспечивают большую надежность, однако легко реализуемы и, поэтому, представляют некоторый интерес, как алгоритмы для демонстрации процессов шифрования и дешифрования в целом.