Криптографические системы
Лабораторная работа №1
Основы шифрования данных

ФИО студента: Готовко Алексей Владимирович
Вариант: 3
Учебная группа: P34101

1 Цель работы

Изучение основных принципов шифрования информации, знакомство с широко известными алгоритмами шифрования, приобретение навыков их программной реализации.

2 Вариант задания

Реализовать шифрование и дешифрацию файла с использованием метода биграмм. Ключевое слово вводится.

3 Исходный код класса-шифратора

BigramEncryptor.py

```python
from utils import factors_except_one

MAX_KEY_VALUE = 1_000_000


class BigramEncryptor:
    _alphabet = ("АБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯабвгдеёжзийклмнопрстуфхцчшщъыьэюя"
                 "ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz"
                 "0123456789.,?!:;\'\"--()@#%*&№+= ")
    _alph_len = len(_alphabet)
    _alph_len_factors = factors_except_one(_alph_len)
    _char_to_numeric_map = {}

    def __init__(self, key_1: int, key_2: int):
        if key_1 <= 0 or key_2 <= 0:
            raise ValueError("Keys must be positive")
        if key_1 > MAX_KEY_VALUE or key_2 > MAX_KEY_VALUE:
            raise ValueError(f'Keys must be less or equal to {MAX_KEY_VALUE}')
        if (len(factors_except_one(key_1).intersection(self._alph_len_factors)) != 0
                or len(factors_except_one(key_2).intersection(self._alph_len_factors)) != 0):
            raise ValueError(f'Keys must not have dividers from set: {self._alph_len_factors}')

        self._key_1 = key_1
        self._key_2 = key_2
        for i, e in enumerate(self._alphabet):
            self._char_to_numeric_map[e] = i

    def _char_to_numeric(self, char: str) -> int:
        try:
            return self._char_to_numeric_map[char]
        except KeyError:
            raise ValueError(f'Character {repr(char)} is not supported')

    def encrypt(self, text) -> str:
        if len(text) % 2 != 0:
            text += ' '

        encrypted = ""
        for i in range(0, len(text) - 1, 2):
            p = self._char_to_numeric(text[i]) * self._alph_len + self._char_to_numeric(text[i + 1])
            c = (p * self._key_1 + self._key_2) % (self._alph_len ** 2)
```

```
42
43              result_num_1 = c // self._alph_len
44              result_num_2 = c % self._alph_len
45              encrypted += self._alphabet[result_num_1] + self._alphabet[result_num_2]
46
47          return encrypted
48
49      def decrypt(self, text) -> str:
50          decrypted = ""
51          for i in range(0, len(text) - 1, 2):
52              result_num_1 = self._char_to_numeric(text[i])
53              result_num_2 = self._char_to_numeric(text[i + 1])
54              c = result_num_1 * self._alph_len + result_num_2
55
56              p = 0
57              while (self._key_1 * p + self._key_2) % (self._alph_len ** 2) != c:
58                  p += 1
59
60              num_1 = p // self._alph_len
61              num_2 = p % self._alph_len
62              decrypted += self._alphabet[num_1] + self._alphabet[num_2]
63
64          return decrypted
```

4 Результат работы программы

4.1 stdout программы

```
Provide first encryption key: 32414
Provide second encryption key: 5111
Provide file name: test_text.txt
Successfully encrypted data. Saved to: out/bigram_encrypted.txt
Successfully decrypted data. Saved to: out/bigram_decrypted.txt

Process finished with exit code 0
```

4.2 Исходный текст

```
xgodness@xgodness-pc:~/itmo/4-year/information-security$ cat test_text.txt
Ребята, не стоит вскрывать эту тему. Вы молодые, шутливые, вам всё легко. Это не то.
Это не микросервисы на спринге и даже не аннотации Балакшина.
Сюда лучше не лезть. Серьёзно, любой из вас будет жалеть.
Лучше закройте тему и забудьте, что тут писалось.
Я вполне понимаю, что данным сообщением вызову дополнительный интерес,
но хочу сразу предостеречь пытливых - стоп. Остальные просто не найдут.
```

4.3 Зашифрованный текст

```
xgodness@xgodness-pc:~/itmo/4-year/information-security$ cat out/bigram_encrypted.txt
#*ZdjгяVe*ХДUщ+TzпЬaEDягГБhQ!PYTЖм-:YшEvнщхщъDбюф6*TBУнDбюzппмzп;JчwA?бщ;vCTъve*YTЭ:
CTъve*8млаНщю*КпМДEv*гХД,Gj9з*БУпьТЖ&ve*,гщ9гТ(тчУФ8,wыаЛУ*г;v
CHMгчwёйв*л9&vШ*яТ3:&M:G?JУ9hючwgzOjБУХvягEvHP4*UvЦгШ*ГБ;v
УР;6&vmгXGOjЖ*YTЖмCvФvmгHP,БЖ*ячУТъv!PUvЫУУгхщFБ;v
nv0@Гwe*a@@9амZHячУТъvMгщ9QмХДъщ9цJ9О*нvнDXщdPпь.@ГwOУЖ*ЯБ7Dkvj9Ж*:*кю
.щ=ЭРйCv%GДWCv,G"ьzДЖ*:*sБа@мТВУнDЮvzv?T.@;v8ДjгЯБ7D&v,GzДUщл9&v*rЬь*T;v
```

4.4 Расшифрованный текст

```
xgodness@xgodness-pc:~/itmo/4-year/information-security$ cat out/bigram_decrypted.txt
Ребята, не стоит вскрывать эту тему. Вы молодые, шутливые, вам всё легко. Это не то.
Это не микросервисы на спринге и даже не аннотации Балакшина.
Сюда лучше не лезть. Серьёзно, любой из вас будет жалеть.
Лучше закройте тему и забудьте, что тут писалось.
Я вполне понимаю, что данным сообщением вызову дополнительный интерес,
но хочу сразу предостеречь пытливых - стоп. Остальные просто не найдут.
```