Министерство образования Республики Беларусь

Учреждение образования

“Белорусский государственный университет

информатики и радиоэлектроники”

ЛАБОРАТОРНАЯ РАБОТА 2

по дисциплине

«Средства и методы защиты информации в интеллектуальных системах»

Выполнил: Мулярчик Д. С., студент гр. 121703

Проверил: Сальников Д. А.

Минск 2023

Задание:

Реализовать в виде программы шифр (зашифрование и расшифрование) шифр перестановки, использующий простые (прямоугольные) таблицы.

Реализация:

Класс для шифровки и расшифровки (зная ключ).

```
class Cod:

    def __init__(self, text, key):
        self.text = text
        self.key = key
        self.encrypted_text = self.encrypt()
        self.decrypt_text = self.decrypt()
```

Код функции, реализующая зашифровку текста по ключу.

```
def encrypt(self):
    self.text = ''.join(filter(str.isalpha, self.text)).upper()

    rows = len(self.key)
    cols = len(self.text) // rows + (1 if len(self.text) % rows > 0 else 0)

    table = [[' ' for _ in range(cols)] for _ in range(rows)]
    k = 0
    for j in range(cols):
        for i in range(rows):
            if k < len(self.text):
                table[i][j] = self.text[k]
                k += 1

    cipher_text = ''
    for i in self.key:
        for j in range(cols):
            cipher_text += table[i - 1][j]

    return cipher_text
```

Код функции, реализующая расшифровку текста, зная ключ.

```
def decrypt(self):
    rows = len(self.key)
    cols = len(self.encrypted_text) // rows + (1 if len(self.encrypted_text) % rows > 0 else 0)

    table = [[' ' for _ in range(cols)] for _ in range(rows)]
    k = 0
    for i in self.key:
        for j in range(cols):
            table[i - 1][j] = self.encrypted_text[k]
            k += 1

    plain_text = ''
    for j in range(cols):
        for i in range(rows):
            plain_text += table[i][j]

    return plain_text
```

Пример выполнения зашифровки и расшифровки (зная ключ)

```
['H', 'O', 'L']
['E', 'W', 'D']
['L', 'O', ' ']
['L', 'R', ' ']
LR HOLEWDLO
HELLOWORLD
['M', 'O']
['Y', 'M']
['H', 'E']
HEMOYM
MYHOME
```

Класс для расшифровки (если ключ не известен)

```
class Descript:

    def __init__(self, text, max_len):
        self.encrypt_text = text
        self.max_len = max_len
```

```
def decrypt_with_key(self, key):
    cols = len(key)
    rows = len(self.encrypt_text) // cols

    table = [[' ' for _ in range(cols)] for _ in range(rows)]
    k = 0
    for j in range(cols):
        for i in range(rows):
            table[i][j] = self.encrypt_text[k]
            k += 1

    col_order = {key[i]: i for i in range(cols)}

    sorted_table = [[' ' for _ in range(cols)] for _ in range(rows)]
    for i in range(rows):
        for j in range(cols):
            sorted_table[i][j] = table[i][col_order[j + 1]]

    decrypted_text = ''
    for i in range(rows):
        decrypted_text += ''.join(sorted_table[i])

    return decrypted_text
```

```
def break_permutation_cipher(self):
    for key_length in range(1, self.max_len + 1):
        print(f"\nПопытка взлома с ключом длины {key_length}:")

        permutations = itertools.permutations(range(1, key_length + 1))

        for permutation in permutations:
            decrypted_text = self.decrypt_with_key(permutation)
            print(f"Перестановка {permutation}: {decrypted_text}")
```

Пример расшифровки:

```
Попытка взлома с ключом длины 1:
Перестановка (1,): LIAKSRAVTBLMCEE

Попытка взлома с ключом длины 2:
Перестановка (1, 2): LVITABKLSMRCAE
Перестановка (2, 1): VLTIBALKMSCREA

Попытка взлома с ключом длины 3:
Перестановка (1, 2, 3): LRLIAMAVCKTESBE
Перестановка (1, 3, 2): LLRIMAACVKETSEB
Перестановка (2, 1, 3): RLLAIMVACTKEBSE
Перестановка (2, 3, 1): LLRMIACAVEKTESB
Перестановка (3, 1, 2): RLLAMIVCATEKBES
Перестановка (3, 2, 1): LRLMAICVAETKEBS
```

```
Попытка взлома с ключом длины 4:
Перестановка (1, 2, 3, 4): LKABISVLARTM
Перестановка (1, 2, 4, 3): LKBAISLVARMT
Перестановка (1, 3, 2, 4): LAKBIVSLATRM
Перестановка (1, 3, 4, 2): LBKAILSVAMRT
Перестановка (1, 4, 2, 3): LABKIVLSATMR
Перестановка (1, 4, 3, 2): LBAKILVSAMTR
Перестановка (2, 1, 3, 4): KLABSIVLRATM
Перестановка (2, 1, 4, 3): KLBASILVRAMT
Перестановка (2, 3, 1, 4): ALKBVISLTARM
Перестановка (2, 3, 4, 1): BLKALISVMART
Перестановка (2, 4, 1, 3): ALBKVILSTAMR
Перестановка (2, 4, 3, 1): BLAKLIVSMATR
Перестановка (3, 1, 2, 4): KALBSVILRTAM
Перестановка (3, 1, 4, 2): KBLASLIVRMAT
Перестановка (3, 2, 1, 4): AKLBVSILTRAM
Перестановка (3, 2, 4, 1): BKLALSIVMRAT
Перестановка (3, 4, 1, 2): ABLKVLISTMAR
Перестановка (3, 4, 2, 1): BALKLVISMTAR
Перестановка (4, 1, 2, 3): KABLSVLIRTMA
Перестановка (4, 1, 3, 2): KBALSLVIRMTA
Перестановка (4, 2, 1, 3): AKBLVSLITRMA
Перестановка (4, 2, 3, 1): BKALLSVIMRTA
Перестановка (4, 3, 1, 2): ABKLVLSITMRA
Перестановка (4, 3, 2, 1): BAKLLVSIMTRA
```

```
Попытка взлома с ключом длины 5:
Перестановка (1, 2, 3, 4, 5): LKABCISVLEARTME
Перестановка (1, 2, 3, 5, 4): LKACBISVELARTEM
Перестановка (1, 2, 4, 3, 5): LKBACISLVEARMTE
Перестановка (1, 2, 4, 5, 3): LKCABISEVLARETM
Перестановка (1, 2, 5, 3, 4): LKBCAISLEVARMET
Перестановка (1, 2, 5, 4, 3): LKCBAISELVAREMT
Перестановка (1, 3, 2, 4, 5): LAKBCIVSLEATRME
Перестановка (1, 3, 2, 5, 4): LAKCBIVSELATREM
Перестановка (1, 3, 4, 2, 5): LBKACILSVEAMRTE
Перестановка (1, 3, 4, 5, 2): LCKABIESVLAERTM
Перестановка (1, 3, 5, 2, 4): LBKCAILSEVAMRET
Перестановка (1, 3, 5, 4, 2): LCKBAIESLVAERMT
Перестановка (1, 4, 2, 3, 5): LABKCIVLSEATMRE
Перестановка (1, 4, 2, 5, 3): LACKBIVESLATERM
Перестановка (1, 4, 3, 2, 5): LBAKCILVSEAMTRE
Перестановка (1, 4, 3, 5, 2): LCAKBIEVSLAETRM
Перестановка (1, 4, 5, 2, 3): LBCKAILESVAMERT
Перестановка (1, 4, 5, 3, 2): LCBKAIELSVAEMRT
Перестановка (1, 5, 2, 3, 4): LABCKIVLESATMER
Перестановка (1, 5, 2, 4, 3): LACBKIVELSATEMR
Перестановка (1, 5, 3, 2, 4): LBACKILVESAMTER
Перестановка (1, 5, 3, 4, 2): LCABKIEVLSAETMR
Перестановка (1, 5, 4, 2, 3): LBCAKILEVSAMETR
Перестановка (1, 5, 4, 3, 2): LCBAKIELVSAEMTR
Перестановка (2, 1, 3, 4, 5): KLABCSIVLERATME
Перестановка (2, 1, 3, 5, 4): KLACBSIVELRATEM
Перестановка (2, 1, 4, 3, 5): KLBACSILVERAMTE
Перестановка (2, 1, 4, 5, 3): KLCABSIEVLRAETM
Перестановка (2, 1, 5, 3, 4): KLBCASILEVRAMET
```

```
Перестановка (2, 3, 1, 4, 5): ALKBCVISLETARME
Перестановка (2, 3, 1, 5, 4): ALKCBVISELTAREM
Перестановка (2, 3, 4, 1, 5): BLKACLISVEMARTE
Перестановка (2, 3, 4, 5, 1): CLKABEISVLEARTM
Перестановка (2, 3, 5, 1, 4): BLKCALISEVMARET
Перестановка (2, 3, 5, 4, 1): CLKBAEISLVEARMT
Перестановка (2, 4, 1, 3, 5): ALBKCVILSETAMRE
Перестановка (2, 4, 1, 5, 3): ALCKBVIESLTAERM
Перестановка (2, 4, 3, 1, 5): BLAKCLIVSEMATRE
Перестановка (2, 4, 3, 5, 1): CLAKBEIVSLEATRM
Перестановка (2, 4, 5, 1, 3): BLCKALIESVMAERT
Перестановка (2, 4, 5, 3, 1): CLBKAEILSVEAMRT
Перестановка (2, 5, 1, 3, 4): ALBCKVILESTAMER
Перестановка (2, 5, 1, 4, 3): ALCBKVIELSTAEMR
Перестановка (2, 5, 3, 1, 4): BLACKLIVESMATER
Перестановка (2, 5, 3, 4, 1): CLABKEIVLSEATMR
Перестановка (2, 5, 4, 1, 3): BLCAKLIEVSMAETR
Перестановка (2, 5, 4, 3, 1): CLBAKEILVSEAMTR
Перестановка (3, 1, 2, 4, 5): KALBCSVILERTAME
Перестановка (3, 1, 2, 5, 4): KALCBSVIELRTAEM
Перестановка (3, 1, 4, 2, 5): KBLACSLIVERMATE
Перестановка (3, 1, 4, 5, 2): KCLABSEIVLREATM
Перестановка (3, 1, 5, 2, 4): KBLCASLIEVRMAET
Перестановка (3, 1, 5, 4, 2): KCLBASEILVREAMT
Перестановка (3, 2, 1, 4, 5): AKLBCVSILETRAME
Перестановка (3, 2, 1, 5, 4): AKLCBVSIELTRAEM
Перестановка (3, 2, 4, 1, 5): BKLACLSIVEMRATE
Перестановка (3, 2, 4, 5, 1): CKLABESIVLERATM
Перестановка (3, 2, 5, 1, 4): BKLCALSIEVMRAET
Перестановка (3, 2, 5, 4, 1): CKLBAESILVERAMT
```

Улучшение алгоритма шифрования:

1) Использовать шифр простых таблиц совместно с другим, например, шифром Цезаря или сопоставить символы уже зашифрованного сообщения с символами другого алфавита. Таким образом, придётся взламывать два шифра.

2) Можно разбить сообщение на части. И для каждой части использовать свой ключ.

3) Можно вместо того, чтобы записывать открытый текст в таблицу построчно, записывать его иным способом, например, по диагонали.