Презентация №3

Шифр гаммирования

Эттеев Сулейман

1 Цель работы

Изучение алгоритма шифрования гаммированиемработы

Реализация шифратора и дешифратора Python

```
def main(text, gamma):
    dict = {"а" :1, "б" :2 , "в" :3 ,"г" :4 ,"д" :5 ,"е" :6 ,"ё" :7 ,"ж": 8, "з"
: 9, "и": 10, "й": 11, "к": 12, "л": 13,
            "м": 14, "н": 15, "о": 16, "п": 17,
            "р": 18, "с": 19, "т": 20, "у": 21, "ф": 22, "х": 23, "ц": 24, "ч":
25, "ш": 26, "щ": 27, "ъ": 28,
            "ы": 29, "ь": 30, "э": 31, "ю": 32, "я": 32
            }
    dict2 = {v: k for k, v in dict.items()}
    digits_text = list()
    digits_gamma = list()

    for i in text:
        digits_text.append(dict[i])
    print("Числа текста: ", digits_text)

    for i in gamma:
        digits_gamma.append(dict[i])
    print("Числа гаммы: ", digits_gamma)

    digits_res = list()
    ch = 0
    for i in text:
        try:
            a = dict[i] + digits_gamma[ch]
        except:
            ch = 0
            a = dict[i] + digits_gamma[ch]
        if a>=33:
            a = a%33
        ch += 1
        digits_res.append(a)
    print("Числа шифровки: ", digits_res)

    text_enc = ""
    for i in digits_text:
        text_enc += dict2[i]
```

```
print("Шифровка: ", text_enc)

digits = list()
for i in text_enc:
    digits.append(dict[i])
ch = 0
digits1 = list()
for i in digits:
    a = i - digits_gamma[ch]
    if a < 1:
        a = 33 + a
    digits1.append(a)
    ch += 1
text_dec = ""
for i in digits1:
    text_dec += dict2[i]
print("Рассшифровка: ", text_dec)
```

3.2 Контрольный пример

```
In [8]:
1 text = "ялюблюрудн"
2 len(text)

Out[8]: 10

In [9]:
1 gamma = "физматфизм"
2 len(gamma)

Out[9]: 10

In [10]:
1 main(text, gamma)

Числа текста:  [33, 13, 32, 2, 13, 32, 18, 21, 5, 15]
Числа гаммы:  [22, 10, 9, 14, 1, 20, 22, 10, 9, 14]
Числа шифровки:  [22, 23, 8, 16, 14, 19, 7, 31, 14, 29]
Расшифровка:  ялюблюрудн
шифровка:  йвхуккыйыа
```

Figure 1: Работа алгоритма гаммирования

4 Выводы

Изучили алгоритмы шифрования на основе гаммирования

Список литературы

1. Шифрование методом гаммирования
2. Режим гаммирования в блочном алгоритме шифрования