Лабораторная работа № 7

Сулицкий Богдан Романовичч

2023, Москва

Цель работы

Целью данной лабораторной работы является освоение на практике применения режима однократного гаммирования.

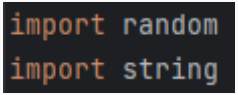

Рис. 1: Добавление библиотек

```python
class VernamCipher:
    def __init__(self, t, key=None):
        self.P = t
        self.len = len(t)
        self.alf = "абвгдеёжзийклмнопрстуфхцчшщъыьэюя" + string.ascii_lowercase + string.digits
        if key is None:
            self.K = self.key_create()
        else:
            self.K = key
        self.C = self.coder(self.P, self.K)
```

Рис. 2: Класс и конструктор

```
def key_create(self):
    return "".join(random.choice(self.alf) for i in range(self.len))
```

Рис. 3: Метод генерации ключа шифрования

```
def coder(self, line, key):
    return "".join(chr(ord(c) ^ ord(k)) for c, k in zip(line, key))
```

Рис. 4: Метод шифровки/дешифровки текста

```
def find_plaintext(self, fragment):
    keyLen = len(fragment)
    possible_keys = []
    for i in range(len(self.C) - keyLen + 1):
        key = [chr(ord(c) ^ ord(k)) for c, k in zip(self.C[i:i + keyLen], fragment)]
        intact_plaintext = "".join(chr(ord(c) ^ ord(k)) for c, k in zip(self.C, key))
        if fragment in intact_plaintext:
            possible_keys.append(''.join(key))
    return possible_keys
```

Рис. 5: Метод определения ключа

```
if __name__ == "__main__":
    text = VernamCipher(input("Введите открытый текст: "))
    print("Текст:", text.P,
          "\nКлюч:", text.K,
          "\nШифротекст:", text.C)
    print("Декодированный текст:", text.coder(text.K, text.C))
    print("\nВозможные ключи: ", text.find_plaintext(input("Введите фрагмент открытого текста: ")))
```

Рис. 6: Инициализация класса и вывод

```
Введите открытый текст: С Новым Годом, друзья!
Текст: С Новым Годом, друзья!
Ключ: y4чosюoffёпуфutzpwxjn2
Шифротекст: bᵇᶜᵈZёсᵉᶠᵍʰFvoᵛⁱчхYТюадяЦСᵇᶜᵈ
Декодированный текст: С Новым Годом, друзья!
Введите фрагмент открытого текста: С Новым Годом

Возможные ключи:  ['y4чosюoffёпуф']
```

Рис. 7: Результат работы программы

Вывод

В ходе проделанной лабораторной работы я освоил на практике применение режима однократного гаммирования.