Лабораторная работа № 7

Элементы криптографии. Однократное гаммирование

Беличева Д. М.

Российский университет дружбы народов, Москва, Россия

Информация

Докладчик

- Беличева Дарья Михайловна
- студентка
- Российский университет дружбы народов
- 1032216453@pfur.ru
- https://dmbelicheva.github.io/ru/

Цель работы

Освоить на практике применение режима однократного гаммирования.

```python
import random

def key_gen(text):
    cirillic = [chr(i) for i in range(1040,1104)]
    symbols = [chr(i) for i in range(32,65)]
    all_characters = cirillic + symbols
    return ''.join([random.choice(all_characters) for i in range(len(text))])
```

```
def xor(text,key):
    return ''.join(chr(ord(a)^ord(b)) for a,b in zip(text,key))
```

```
def part_key_gen(fragment, encrypted_text):
    start_key = xor(fragment,encrypted_text[:len(fragment)])
    remaining_length = len(encrypted_text) - len(fragment)
    key_rest = key_gen(' ' * remaining_length)
    return start_key + key_rest
```

Выполнение лабораторной работы

```
text = 'С Новым годом, друзья!'
key = key_gen(text)
encrypted_text = xor(text,key)
fragment = 'С Новым'
partial_key = part_key_gen(fragment, encrypted_text)
decrypted_guess_text = xor(encrypted_text,partial_key)
```

```
print("Ключ:")
key
```

```
Ключ:
'0a"T%+дЩШ0тд ЯыьаСНГФХ'
```

```
print("Шифротекст:")
encrypted_text
```

```
Шифротекст:
'БАп\x1c3Ѡ\x08Љ\x1bЎv\nMЃ‰xpЬ*_kЄ'
```

```
print("Частично расшифрованный текст:")
decrypted_guess_text
```

```
Частично расшифрованный текст:
'С Новым$"EVPQ=ї6ƹZЪѠoI'
```

Рис. 1: Результат работы программы

Выводы

В результате выполнения данной лабораторной работы я освоила на практике применение режима однократного гаммирования.

Список литературы

1. Гаммирование [Электронный ресурс]. 2023. URL: https://ru.wikipedia.org/wiki/Гаммирование.