Лабораторная работа №8

Основы информационной безопасности

Иванов Сергей Владимирович, НПИбд-01-23

15 мая 2025

Российский университет дружбы народов, Москва, Россия

Цель работы

Освоить на практике применение режима однократного гаммирования на примере кодирования различных исходных текстов одним ключом

Задание

Два текста кодируются одним ключом (однократное гаммирование). Требуется не зная ключа и не стремясь его определить, прочитать оба текста. Необходимо разработать приложение, позволяющее шифровать и дешифровать тексты P_1 и P_2 в режиме однократного гаммирования. Приложение должно определить вид шифротекстов C_1 и C_2 обоих текстов P_1 и P2 при известном ключе; Необходимо определить и выразить аналитически способ, при котором злоумышленник может прочитать оба текста, не зная ключа и не стремясь его определить.

Выполнение работы

Выполнение работы

Я выполнял работу на языке программирования Python, используя функции, реализованные в лабораторной работе №7. (рис. 1)

```
text1 = 'С новым годом, друзья!'
text2 = 'Сегодня 15 мая 2025 г.'

key = generate_key(text1)
en_crypt = en_de_crypt(text1, key)
de_crypt = en_de_crypt(en_crypt, key)

en_crypt_text2 = en_de_crypt(text2, key)
de_crypt_text2 = en_de_crypt(en_crypt_text2, key)

print("Открытый текст:", text1, "\nКлюч:", key, "\nШифротекст:", en_crypt, "\nИсходный текст:", de_crypt, "\n")
print("Открытый текст:", text2, "\nКлюч:", key, "\nШифротекст:", en_crypt_text2, "\nИсходный текст:", de_crypt_text2, "\n")

r = en_de_crypt(en_crypt_text2, en_crypt)
print('Расшифровать второй текст, зная первый: ', en_de_crypt(text1, r))
print('Расшифровать первый текст, зная второй: ', en_de_crypt(text2, r))
```

Рис. 1: Шифровка текстов

Функция шифрования и дешифрования

Расшифровываю оба текста сначала с помощью одного ключа, затем предполагаю, что мне неизвестен ключ, но извествен один из текстов и уже расшифровываю второй, зная шифротексты и первый текст. (рис. 2).

```
Открытый текст: С новым годом, друзья!
Ключ: NNLmwv5OFqLUjsTnBJceFB
Шифротекст: ᛝnψŕxнЉovЯϘӿi_tћЂЉєЩЉc
Исходный текст: С новым годом, друзья!

Открытый текст: Сегодня 15 мая 2025 г.
Ключ: NNLmwv5OFqLUjsTnBJceFB
Шифротекст: ᛝфϖŕуыФowDlѩњмt\rxVEvl
Исходный текст: Сегодня 15 мая 2025 г.

Расшифровать второй текст, зная первый:  Сегодня 15 мая 2025 г.
Расшифровать первый текст, зная второй:  С новым годом, друзья!
```

Рис. 2: Расшифровка

Вывод

Вывод

В ходе лабораторной работы были освоины на практике навыки применения режима однократного гаммирования на примере кодирования различных исходных текстов одним ключом.