

Лабораторная работа №8

Элементы криптографии. Шифрование (кодирование) различных исходных текстов одним ключом

Дорофеева А.Т.

25 октября 2023

Российский университет дружбы народов им. Патриса Лумумбы, Москва, Россия

Информация

- Дорофеева Алёна Тимофеевна
- студент группы НПИбд-01-20
- Российский университет дружбы народов им. Патриса Лумумбы
- 1032201392@pfur.ru
- https://github.com/DorofeevaAT/study_2022-2023_infosec

Вводная часть

- Криптография – это важнейший инструмент кибербезопасности, она обеспечивает дополнительный уровень защиты, позволяет сохранить конфиденциальность данных и предотвращает их перехват киберпреступниками

- Принцип одногратного гаммирования

1. Изучить принцип однократного гаммирования для кодирования двух исходных текстов одним ключом
2. Разработать приложение, позволяющее шифровать и дешифровать тексты P1 и P2 в режиме однократного гаммирования

- Однократное гаммирование

Гаммирование – это наложение (снятие) на открытые (зашифрованные) данные криптографической гаммы, т.е. последовательности элементов данных, вырабатываемых с помощью некоторого криптографического алгоритма, для получения зашифрованных (открытых) данных.

Шифротексты обеих телеграмм можно получить по формулам режима однократного гаммирования:

$$C_1 = P_1 \oplus K$$

$$C_2 = P_2 \oplus K$$

Открытый текст можно найти, зная шифротекст двух телеграмм, зашифрованных одним ключом. Для это оба равенства складываются по модулю 2. Тогда с учётом свойства операции XOR получаем:


$$C_1 \oplus C_2 = P_1 \oplus K \oplus P_2 \oplus K = P_1 \oplus P_2$$

Предположим, что одна из телеграмм является шаблоном — т.е. имеет текст фиксированный формат, в который вписываются значения полей. Допустим, что злоумышленнику этот формат известен. Тогда он получает достаточно много пар $C_1 \oplus C_2$ (известен вид обеих шифровок). Тогда зная P_1 имеем:

$$C_1 \oplus C_2 \oplus P_1 = P_1 \oplus P_2 \oplus P_1 = P_2$$


Пример работы программы

```
vzлом(P1, P2)
```



```
['а', 'б', 'в', 'г', 'д', 'е', 'ж', 'з', 'и', 'й', 'к', 'л', 'м', 'н', 'о', 'п', 'р', 'с', 'т', 'у', 'ф', 'х', 'ц',  
['ю', 'в', 'к', 'о', 'б', 'ч', 'в', 'д', 'л', 'у']  
ЮвкОбЧвДлу
```

Рис. 1: Работа алгоритма взлома ключа



```
Введите гамму: ЮвкОбЧвДлу  
Числа текста [65, 2, 6, 18, 21, 49, 1, 21, 9, 21]  
числа гаммы [64, 3, 12, 75, 71, 57, 3, 37, 13, 21]  
54  
18  
17  
31  
Числа зашифрованного текста [54, 5, 18, 18, 17, 31, 4, 58, 22, 42]  
Зашифрованный текст: ФдррпэгШфи
```

Выводы

В ходе выполнения лабораторной работы было разработано приложение, позволяющее шифровать тексты в режиме однократного гаммирования.