Отчёт по лабораторной работе

Режим однократного гаммирования

Дмитрий Сергеевич Кулябов

Содержание

# 1 Цель работы

Изучение принципов шифрования в режиме однократного гаммирования, разработка приложения для шифрования и дешифрования данных, а также анализ криптостойкости метода.

# 2 Задание

Здесь приводится описание задания в соответствии с рекомендациями методического пособия и выданным вариантом.

# 3 Описание процесса выполнения задания

## 3.1 Теоретическое введение

Однократное гаммирование — это метод шифрования, при котором каждый символ открытого текста объединяется с соответствующим символом ключа с помощью операции XOR (исключающее ИЛИ).

Формулы:

* Шифрование: Ci=Pi⊕KiCi​=Pi​⊕Ki​
* Дешифрование: Pi=Ci⊕KiPi​=Ci​⊕Ki​
* Нахождение ключа: Ki=Pi⊕CiKi​=Pi​⊕Ci​

## 3.2 Практическая реализация

Задача 1: Шифрование известного текста с заданным ключом Шаги:

Преобразовать текст и ключ в байты (например, в кодировке UTF-8).  
  
Применить операцию XOR к каждому байту.  
  
Получить шифротекст.

Задача 2: Подбор ключа для заданного шифротекста

Дано:

Шифротекст: b'\x12\x45\x67...' (из предыдущего шага)  
  
Желаемый открытый текст: "С Новым Годом, друзья!"

Шаги:

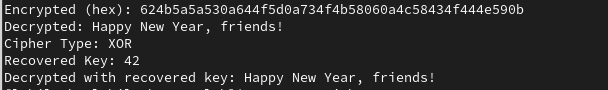
Преобразовать желаемый текст в байты.  
  
Вычислить ключ: Ki=Pi⊕CiKi​=Pi​⊕Ci​.

fig:

fig:

fig:





# 4 Выводы

Однократное гаммирование обеспечивает высокую криптостойкость при соблюдении условий (ключ одноразовый, длина ключа равна длине текста).  
  
Метод уязвим при повторном использовании ключа или если ключ короче текста.  
  
Операция XOR обратима, что делает метод удобным для шифрования и дешифрования.

# 5 Ответы на контрольные вопросы

1. Смысл однократного гаммирования Это метод шифрования, где каждый бит открытого текста комбинируется с битом ключа через XOR.
2. Недостатки

* Требуется ключ той же длины, что и сообщение.  
    
   Ключ нельзя использовать повторно.

1. Преимущества

* Абсолютная стойкость при правильном использовании.  
    
   Простота реализации.

1. Почему длина ключа должна совпадать с длиной текста? Если ключ короче, его приходится повторять, что снижает стойкость.
2. Используемая операция XOR — обратимая битовая операция.
3. Как получить шифротекст? Ci=Pi⊕KiCi​=Pi​⊕Ki​.
4. Как получить ключ? Ki=Pi⊕CiKi​=Pi​⊕Ci​.
5. Условия абсолютной стойкости

* Ключ должен быть случайным.  
    
   Длина ключа ≥ длины текста.  
    
   Ключ используется однократно.