Лабораторная работа №3

Мохаммад хоссейн фарзанфар

4 2, 2025, Москва, Россия

Российский Университет Дружбы
Народов

Цели и задачи

Цель лабораторной работы

Изучение алгоритма шифрования гаммированием

Выполнение лабораторной работы

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.

Гаммирование

Наложение (или снятие) гаммы на блок сообщения в рассматриваемом нами стандарте реализуется с помощью операции побитного сложения по модулю 2 (XOR). То есть при шифровании сообщений каждый блок открытого сообщения ксорится с блоком криптографической гаммы, длина которого должна соответствовать длине блоков открытого сообщения. При этом, если размер блока исходного текста меньше, чем размер блока гаммы, блок гаммы обрезается до размера блока исходного текста (выполняется процедура усечения гаммы).

Алгоритм

```
Выберите операцию:
1. Зашифровать текст с помощью XOR
2. Расшифровать текст с помощью XOR
3. Сгенерировать ключ с помощью линейного конгруэнтного генератора (LCG)
4. Выйти
1
Введите текст для шифрования:
Привет
Введите ключ (должен быть не короче текста):
ключ123
Зашифрованный текст: %{vuЄΨ
```

Рис. 1: Шифрование

Формула

В аддитивных шифрах символы исходного сообщения заменяются числами, которые складываются по модулю с числами гаммы. Ключом шифра является гамма, символы которой последовательно повторяются. Перед шифрованием символы сообщения и гаммы заменяются их номерами в алфавите и само кодирование выполняется по формуле

$$Ci = (Ti + Gi) mod N$$

Пример работы алгоритма

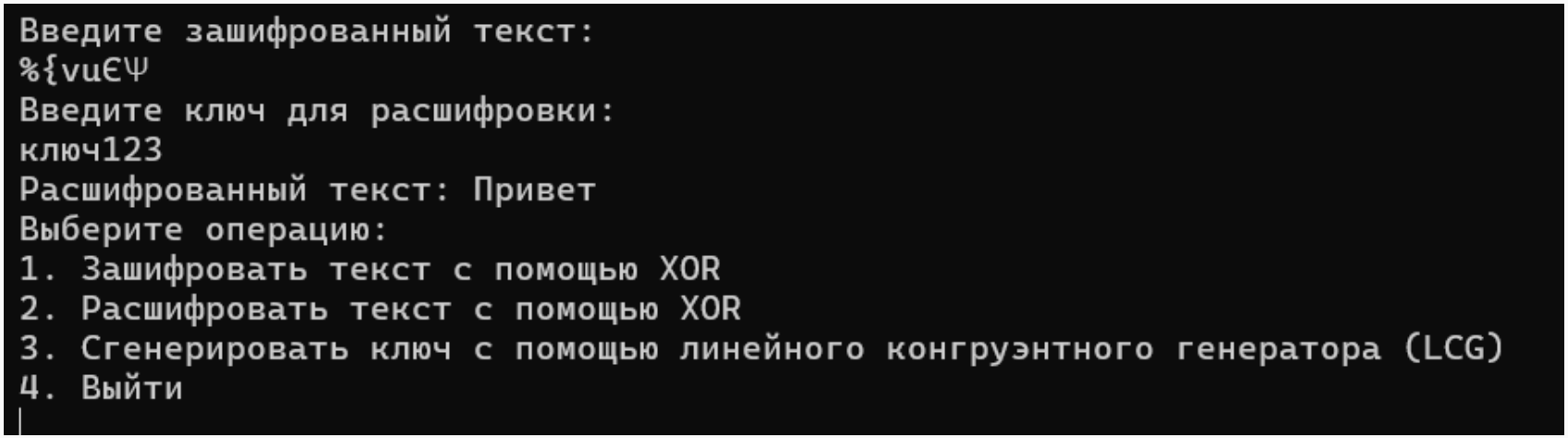

Рис. 2: Работа алгоритма гаммирования

Пример работы программы

```
Выберите операцию:
1. Зашифровать текст с помощью XOR
2. Расшифровать текст с помощью XOR
3. Сгенерировать ключ с помощью линейного конгруэнтного генератора (LCG)
4. Выйти
3
Введите параметры LCG:
Введите значение для a:
5
Введите значение для b:
3
Введите значение для m:
16
Введите начальное значение (seed):
7
Введите длину ключа:
6
Сгенерированная последовательность ключей: [6, 1, 8, 11, 10, 5]
```

Рис. 3: Работа алгоритма гаммирования

Выводы

Результаты выполнения лабораторной работы