Шифр гаммирования

Алгайли Абдулазиз Мохаммед

12 Октябрь, 2024, 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

```
Choose an operation:
1. Encrypt text using XOR
2. Decrypt text using XOR
3. Generate key using Linear Congruential Generator (LCG)
4. Exit
1
Enter the plaintext to encrypt:
Привет
Enter the key (should be as long as or longer than the text):
Ключик
xncrypted text: {vu
```

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

```
Choose an operation:
1. Encrypt text using XOR
2. Decrypt text using XOR
3. Generate key using Linear Congruential Generator (LCG)
4. Exit
1
Enter the plaintext to encrypt:
Привет
Enter the key (should be as long as or longer than the text):
Ключик
xncrypted text: {vu
Choose an operation:
1. Encrypt text using XOR
2. Decrypt text using XOR
3. Generate key using Linear Congruential Generator (LCG)
4. Exit
2
Enter the encrypted text:
{vu
Enter the key used for decryption:
Ключик
Decrypted text: wэл
Choose an operation:
1. Encrypt text using XOR
2. Decrypt text using XOR
3. Generate key using Linear Congruential Generator (LCG)
4. Exit
```

Пример работы программы

```
Choose an operation:
1. Encrypt text using XOR
2. Decrypt text using XOR
3. Generate key using Linear Congruential Generator (LCG)
4. Exit
3
Enter LCG parameters:
Enter value for a:
5
Enter value for b:
3
Enter value for m:
16
Enter the seed (initial value):
7
Enter the length of the key:
6
Generated key sequence: [6, 1, 8, 11, 10, 5]
```

Рис. 3: Работа алгоритма гаммирования

Выводы

Результаты выполнения лабораторной работы

Изучили алгоритм шифрования с помощью гаммирования