Шифр гаммирования

Дабван Луаи Мохаммед Али

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

```
=== Select an Option ===
1. Encryption
2. Decryption
3. Key Generation using LCG
4. Exit
Please enter your choice (1, 2, 3, or 4):
1

=== Encryption ===
Enter the plaintext (original text):
QWE
Enter the key (must be at least as long as the plaintext):
QWER
Encrypted text (base64 encoded): AAAA
```

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

```
=== Encryption ===
Enter the plaintext (original text):
QWE
Enter the key (must be at least as long as the plaintext):
QWER
Encrypted text (base64 encoded): AAAA

=== Select an Option ===
1. Encryption
2. Decryption
3. Key Generation using LCG
4. Exit
Please enter your choice (1, 2, 3, or 4):
2

=== Decryption ===
Enter the encrypted text (base64 encoded):
AAAA
Enter the key (must be the same as the key used for encryption):
QWER
Decrypted text: QWE
```

Работа алгоритма гаммирования

Пример работы программы

```
1. Encryption
2. Decryption
3. Key Generation using LCG
4. Exit
Please enter your choice (1, 2, 3, or 4):
3

=== Key Generation using LCG ===
Enter the first LCG parameter (a):
6
Enter the second LCG parameter (b):
4
Enter the third LCG parameter (m):
16
Enter the seed value:
3
Enter the length of the sequence:
5
Generated key sequence: [6, 8, 4, 12, 12]
```

Работа алгоритма гаммирования

Выводы

Результаты выполнения лабораторной работы

Изучили алгоритм шифрования с помощью гаммирования