Лабораторная работа №7

Автор: Юхнин Илья Андреевич

Группа: НКНбд-01-19

Цель выполнения лабораторной работы

- Изучение алгоритма шифрования гаммированием

Теория

- 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.
- 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).

Выполнение лабораторной работы

Пример работы алгоритма

```
1 shifr("СНовымГодомДрузья")
```

```
Введите гамму(Только символы из dict): яьзурДмодГывНС
Числа текста [51, 47, 16, 3, 29, 14, 36, 16, 5, 16, 14, 37, 18, 21, 9, 30, 32]
числа гаммы [32, 30, 9, 21, 18, 37, 14, 16, 5, 36, 29, 3, 47, 51]
8
2
Числа зашифрованного текста [8, 2, 25, 24, 47, 51, 50, 32, 10, 52, 43, 40, 65, 72, 41, 60, 41]
Зашифрованный текст:  жбчцНСРяиТЙЖЯ7ЗЪЗ
Расшифрованный текст СНовымГодомДрузья
```

Выводы лабораторной работы

- Изучил алгоритм шифрования с помощью гаммирования

Спасибо за внимание!