А. С. Богатко, Д. Д. Курмашев, Н. А. Жиляк
(БГТУ, Минск)

РАБОТА КРИПТОГРАФИЧЕСКОЙ ПРОГРАММЫ CRIPT

Шифрование является основным методом защиты и наиболее широко используемым криптографическим методом сохранения конфиденциальности информации, он защищает данные от несанкционированного ознакомления с ними.

Шифрование информации – это преобразование открытой информации в зашифрованную (которая чаще всего называется шифртекстом или криптограммой), и наоборот. Первая часть этого процесса называется шифрованием, вторая – расшифрованием.

Алгоритм нашего шифратора «CRIPT» состоит из нескольких этапов:

1) Создание базового алфавита для использования.

Базовый алфавит состоит из букв русско-английского алфавита разного регистра и символов (всего 156 символов).

2) Создание протоколов для выбранного алфавита, позволяющие использовать различные комбинации.

Для создания новых алфавитов используются протоколы, позволяющие разнообразить базовый алфавит.

3) Создание функции, которая наиболее оптимальна для шифрации текста.

Алгоритм шифрования состоит из нескольких этапов:

– случайный выбор протокола шифрования;
– использование функции шифрования.

Алгоритм программы построен таким образом, что шифртекст получается в четыре раза больше исходного.

4) Генерация ключа, в зависимости от пунктов 2 и 3.

Генерация ключа. Понятие *ключ* определено следующим образом: «Конкретное секретное состояние некоторых параметров алгоритма криптографического преобразования, обеспечивающее выбор одного преобразования из совокупности всевозможных для данного алгоритма преобразований».

Генерация ключа состоит из двух этапов:

– генерация расширенного ключа;
– создание оптимизированного ключа.

Оптимизированный ключ, убирает недостаток расширенного ключа, а именно: размерность расширенного ключа больше на 1 символ чем, введенный текст. Оптимизированный ключ сокращает эту запись, если это возможно.

Так как в алгоритме, указанным в пункте 3, всего 3 варианта действий, которые обозначаются соответствующими цифрами 1, 2, 3, то можно оптимизировать запись ключа, заменив определенные комбинации, состоящие из 3 символов 1 (Буквы английского алфавита разного регистра).

5) Работа с файлом.

Далее ведется работа с файлами, шифр и код загружается в текстовый документ, который можно будет считать дешифратором.

Таким образом, данный шифратор эффективно зашифровывает текст, что позволяет защитить свои данные от посторонних лиц.