Лабораторная работа № 4

Шифры сложной замены.

Система шифрования Вижинера.

по курсу «Защита информации»

Рабочее задание.

1. Подготовить программные модули для определения числовых эквивалентов букв шифруемого (plaintext0) текста ("прилетаюдевятогомарта") и букв ключевого (key) слова - "почта".
2. Загрузить базовую таблицу шифра Вижинера (distributions\Таблица шифра Вижинера базовая).
3. Разработать модуль шифрования по таблице Вижинера и зашифровать plaintext0 на ключе п.1.
4. Провести шифрование plaintext0 на основе следующей реализации шифра Вижинера: *yi* = (*xi* + *key*(*i* mod *r*)) mod *m*, где *yi* – символ шифртекста, *xi* – символ открытого текста, *key*(*i* mod *r*) – символ ключа, *r* – длина ключа, *m* – длина алфавита.
5. Зашифровать plaintext0 на ключе п.1 с помощью программы alfavit12.exe (distributions).
6. Разработать модуль дешифрования по таблице Вижинера и расшифровать тексты, полученные в п.3, 4, 5. Результаты шифрования и дешифрования отразить в сводной таблице.
7. Модифицировать базовую таблицу шифра Вижинера путем перестановки строк: установить генератор случайных чисел в начальное состояние, соответствующее номеру по списку в группе (SeedRandom[N]), получить таблицу замен строк - RandomSample[Range[1,32]] и переставить строки базовой таблицы.
8. Провести шифрование на ключе п.1 и сравнить с результатами п.3,4,5.
9. Расшифровать текст с номером 20 + Nmod12  из папки CrypttextVG, в которой каждый текст зашифрован на базовой таблице и пароле:

|  |  |  |  |
| --- | --- | --- | --- |
| N | Пароль | N | Пароль |
| 1 | аутентификация | 7 | сообщение |
| 2 | источник | 8 | идентификатор |
| 3 | коммуникации | 9 | конструкция |
| 4 | верификация | 10 | пользователь |
| 5 | целостность | 11 | протокол |
| 6 | теледоступ | 12 | параметр |