Лабораторная работа № 2

Криптосистема Хилла

по курсу «Защита информации»

Рабочее задание.

1. Сформировать матрицу преобразования для реализации криптосистемы Хилла размером 2х2: {{3,3},{2,5}}.
2. Рассчитать детерминант матрицы (Det[]) и проверить, являются ли делители (Divisors[]) числа 32 (длина русского алфавита) и значение детерминанта взаимно простыми числами (GCD[]).
3. Найти матрицу обратного преобразования: Inverse[\*,Modulus->32] и выполнить проверку, перемножив (Dot[]) прямую и обратную матрицы по модулю 32.
4. Подготовить текст «прилетаювосьмого» для шифрования: заменить каждую букву на её числовой эквивалент и разбить полученный список на биграммы.
5. Провести шифрование первой биграммы: перемножить матрицу прямого преобразования на вектор (в данном случае первую биграмму) по модулю 32 со смещением 1 ( Mod[\*,32,1] ).
6. Зашифровать весь текст и преобразовать его из числовых эквивалентов в строку.
7. Шифртекст, полученный в п.6 подготовить к дешифрованию: заменить каждую букву на её числовой эквивалент и разбить полученный список на биграммы.
8. Провести дешифрование первой биграммы: перемножить матрицу обратного преобразования на вектор (в данном случае первую биграмму) по модулю 32 со смещением 1 ( Mod[\*,32,1] ).
9. Расшифровать весь текст и преобразовать его из числовых эквивалентов в строку.
10. Задать начальное состояние генератора случайных чисел равное номеру по списку в группе, получить 16 случайных целых чисел из интервала [1,32] и сформировать матрицу размером 4х4.
11. Выполнить п. 2 и п.3, и если проверки не выполняются - сформировать новый набор случайных чисел.
12. Подготовить открытый текст для шифрования: импортировать файл соответствующий номеру 50 - N и содержащий открытый тест (папка Plaintext; distributives\ импорт открытого текста.nb ), удалить пробелы, привести размер текста к величине кратной 4.
13. Провести шифрование открытого текста 4-граммами и определить число совпадений 4-грамм в зашифрованном тексте.
14. Расшифровать текст с номером 15+N (Лаб. 4 Crypttext Hill), который был зашифрован в рамках криптосистемы Хилла с ключом: . 