Лабораторная работа № 3

Шифры перестановки

по курсу «Защита информации»

Рабочее задание.

1. Подготовить открытый текст для шифрования : импортировать файл соответствующий номеру N по списку в группе и содержащий открытый тест (папка Plaintext; . distributions\ импорт открытого текста.nb ), привести размер текста к величине кратной 10, удалить пробелы.
2. Определить следующие характеристики текста: энтропию позначной модели, энтропию биграммной модели, частоты чередования гласных и согласных букв (см. distributions\ анализ текста на чередование букв.nb).
3. Сформировать матрицу, содержащую 10 столбцов.
4. Провести операцию шифрования методом простой маршрутной перестановки: заполнить таблицу открытым текстом последовательно по строкам, а затем считать текст последовательно по столбцам. Определить характеристики зашифрованного текста согласно п.2.
5. Расшифровать текст соответствующий номеру N (папка Crypttext; . distributions\ импорт зашифрованного текста.nb), который зашифрован методом перестановки столбцов (шифр вертикальной перестановки) с ключом, приведенном в таблице:

|  |  |  |  |
| --- | --- | --- | --- |
| N | Ключ | N | Ключ |
| 1 | барокамера | 7 | кавалерист |
| 2 | ватерлиния | 8 | легкоатлет |
| 3 | галантерея | 9 | магнитофон |
| 4 | двухтомник | 10 | нормировка |
| 5 | жилплощадь | 11 | радиолампа |
| 6 | заповедник | 12 | стекловата |

Определить характеристики зашифрованного текста согласно п.2.

1. Провести процедуру шифрования открытого текста (п. 1) с применением шифра перестановки степени *n* , где *n* – это длина текста. Для чего сформировать случайную неповторяющуюся последовательность целых чисел из интервала [1,n] c помощью функции RandomSample[], ключом является начальное состояние генератора случайных чисел, определяемое N. Провести перестановку символов в списке и получить зашифрованный текст. Определить характеристики зашифрованного текста согласно п.2. Провести расшифрование зашифрованного текста.
2. Построить таблицу результатов экспериментов :

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | Энтропия  позначная | Энтропия  биграмм | Частота  ГГ | Частота  ГС | Частота  СГ | Частота  СС |
| Открытый  текст |  |  |  |  |  |  |
| Простая маршрутная  перестановка |  |  |  |  |  |  |
| Шифртекст перестановки по столбцам (п.5) |  |  |  |  |  |  |
| Решетка  Кардано |  |  |  |  |  |  |
| Перестановка степени *n* |  |  |  |  |  |  |

1. Зашифровать открытый текст (п. 1) с применением решетки Кардано: сформировать решетку состоящую из 10 столбцов, число строк (должно быть четным) определяется размером шифруемого текста, выбор варианта решетки определяется N (см. distributions\ формирование решетки Кардано.nb); полностью заполнить матрицу символами открытого текста (1 - позиция размещения символа), выполняя поворот решетки вокруг горизонтальной и вертикальной осей симметрии. Провести считывание последовательно по столбцам. Определить характеристики зашифрованного текста согласно п.2.