Лабораторная работа № 5

Система шифрования Вернама

по курсу «Защита информации»

Рабочее задание.

1. Сформировать таблицу кодирования букв русского алфавита двоичным пятиразрядным кодом. Выравнивание осуществлять с помощью команды PadLeft[].
2. Преобразовать строку открытого текста plainText="прилетаюдвадцатьтретьегомарта" в двоичный список. Определить длину полученного списка.
3. Установить начальное состояние генератора случайных чисел равным номеру по списку в группе и получить ключ в виде двоичного списка, с помощью команды RandomInteger[]. Длина ключевой последовательности должна быть равна длине двоичного списка открытого текста.
4. Зашифровать plainText (путем сложения по mod2 двоичных последовательностей), а затем расшифровать на ключе, сформированном в п. 3.
5. Разработать модуль шифрования по методу Вернама – входные параметры: строка текста и строка ключевой последовательности; выход: строка шифртекста.
6. Разработать модуль дешифрования по методу Вернама – входные параметры: строка шифртекста и строка ключевой последовательности; выход: строка расшифрованного текста.
7. Подготовить программный модуль, реализующий генератор BBS c параметрами, приведенными в work task \ tableBBS\_W.xls, N – номер по списку в группе. Получить ключевую последовательность длиной m.
8. Зашифровать, а затем расшифровать Plaintext \Text-N.txt на ключе п. 7.
9. Получить ключевую последовательность от генератора BBS длиной 50m (см. п.7).
10. Провести анализ качества ключевой последовательности с помощью частотного теста в подпоследовательностях (Frequency Test Within a Block): articles\ Методы оценки качества ПСП\стр. 165.