Задание №1.4

Реализовать алгоритм шифрования данных «Шифрующие таблицы Трисемуса».

Описание алгоритма

В 1508 г. аббат из Германии Иоганн Трисемус написал печатную работу по криптологии под названием "Полиграфия". В этой книге он впервые систематически описал применение шифрующих таблиц, заполненных алфавитом в случайном порядке. Для получения такого шифра замены обычно использовались таблица для записи букв алфавита и ключевое слово. В таблицу сначала вписывалось по строкам ключевое слово, причем повторяющиеся буквы отбрасывались. Затем эта таблица дополнялась не вошедшими в нее буквами алфавита по порядку.

При шифровании находят в этой таблице очередную букву открытого текста и записывают в шифртекст букву, расположенную ниже ее, в том же столбце. Если буква текста оказывается в нижней строке таблицы, тогда для шифртекста берут самую верхнюю букву из того же столбца.

Пример. Для русского алфавита шифрующая таблица может иметь размер 4x8. Выберем в качестве ключа слово БАНДЕРОЛЬ. Шифрующая таблица примет вид:

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Б | А | Н | Д | Е | Р | О | Л |
| Ь | В | Г | Ж | 3 | И | И | К |
| М | П | С | Т | У | Ф | X | Ц |
| Ч | Ш | Щ | Ы | Ъ | Э | Ю | Я |

Таблица 9 - Пример использования Шифрующей таблицы Трисемуса

При шифровании с помощью этой таблицы:

сообщения В Ы Л Е Т А Е М П Я Т О Г О

получаем шифртекст П Д К З Ы В З Ч Ш Л Ы Й С Й

Примеры работы шифрования и расшифрования

НГТУ



ФИО

