ЛАБОРАТОРНАЯ РАБОТА 3

РЕАЛИЗАЦИЯ АЛГОРИТМА ШИФРОВАНИЯ ПЛЕЙФЕЙРА

Цель работы: формирование умений шифрования с использованием алгоритма шифрования Плейфейра.

Содержание задания

Зашифруйте сообщение, используя алгоритм Плейфейра согласно своему варианту (табл. 3.1). Размер шифрующей таблицы 4 × 8.

Таблица 1

|  |  |  |
| --- | --- | --- |
| Вариант | Сообщение | Ключевое слово |
| 17 | Тот, кто смотрит на дело с обеих сторон, обычно не видит ни одной из них | ЖИЗНЬ |

Для начала сделаем таблицу Трисемуса для ключевого слова

Таблица 2

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

Далее разбиваем сообщение для шифра на биграммы

ЙЦЙ, УЙЦ ЕХЦЙШДЪ ЙЛ ИЙМЦ Е ВМЗДЦ ТЙЦДЦЙ, ВЮЬЖЪВ ЙЗ ОДРРН ЬЗ ГЕЙВН ДН ЬРБ

Теперь можно зашифровать сообщение следуя алгоритму

Получаем: А УЗТЧКЗГР ГЧЖЖСЕСЖСЕМ ЪЖХСЛЕДЗОЪ ЖШЧЯПУСЩЛЕДЗОЪ ЗЧСЫАЧФКОЬЪЦЧЩ ОДЩСОГЦИН ЕОЬ ЕЖФВИЖГКЧКОЬ

Контрольные вопросы

1. Как формируется шифрующая таблица для реализации алгоритма Плейфейра?

Для формирования шифрующей таблицы в алгоритме Плейфейра используется ключевое слово или фраза, которые преобразуются в битовую строку. Затем эта битовая строка разбивается на две равные части, которые записываются вертикально друг под другом. После этого над битами верхней и нижней строки проводятся операции XOR (исключающее ИЛИ). В результате получается квадратная матрица, где каждый элемент является результатом операции XOR между соответствующими битами верхней и нижней строк. Эта матрица и является шифрующей таблицей, которая используется в алгоритме Плейфейра для шифрования текста.

1. Какие ограничения накладываются на шифруемый текст?

Шифруемый текст должен иметь четное количество букв, и в нем не должно быть биграмм, содержащих двеодинаковые буквы.

1. Что такое биграмма?

Биграмма — это последовательность из двух символов

1. В чем заключается процедура шифрования с помощью алгоритма Плейфейра?

Для шифрования текста с помощью алгоритма Плейфейра необходимо выполнить следующие шаги:

1. Выбрать ключевое слово или фразу, которая будет использоваться для формирования шифрующей таблицы.
2. Преобразовать выбранное ключевое слово или фразу в битовую строку, разбив каждый символ на его двоичное представление.
3. Разделить полученную битовую строку на две равные части и записать их вертикально друг под другом.
4. Выполнить операцию XOR над битами каждой пары соответствующих э. лементов верхней и нижней строк, получив в результате квадратную матрицу.
5. Зашифровать текст, разбивая его на биграммы и выполняя над каждой биграммой операцию XOR с соответствующим элементом шифрующей таблицы. Результат операции XOR также записывается в виде битовой строки.
6. Повторить шаги 5 и 6 для всех биграмм текста, объединив полученные битовые строки в зашифрованный текст.