**Лабораторная работа №3**

Тема: “Реализация алгоритма шифрования Плейфера”

Цель работы:

Формирование умений шифрования с использованиемалгоритма шифрования Плейфера.

Ход работы:

Задание 1. Зашифруйте сообщение, используя алгоритм Плейфейра со- гласно своему варианту (рис. 1). Размер шифрующей таблицы 4 × 8.

Рисунок 1 – Фрагмент таблицы.

Таблица 1 – Алгоритм Плейфера.

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

ПР ИО БМ ЕН ЕД АН НЫ МИ ПО СЕ ТЯ МВ ОЗ НИ КА ЕТ ПР ОБ ЛЕ МА УС ТА НО ВЛ ЕН ИЯ ПО ДЛ ИН НО СТ ИА ВТ ОР ОВ .

РСИ УМЧЦРВ ЖЦХСШЙГ ВУ ТРБЫБ ДТИГУАБТО РСКЦАЖБЛ УФОБ- ЦУАДЦРМЬ ВУЖМГУЦУЗЫО ЛЕОЕУЕА.

Контрольные вопросы:

1. Формирование шифрующей таблицы для алгоритма Плейфейра:

* Выберите ключевое слово или фразу;
* запишите ключевое слово в таблицу 5x5 (для латинского алфавита) или 4x8 (для кириллического алфавита), исключая повторяющиеся буквы;
* заполните оставшиеся ячейки таблицы буквами алфавита, которые не входят в ключевое слово, по порядку;

1. ограничения на шифруемый текст:

* Текст должен содержать четное количество символов. Если количество символов нечетное, в конец текста добавляется дополнительный символ (например, “X”);
* в тексте не должно быть пар одинаковых символов. Если такие пары встречаются, между ними вставляется разделительный символ (например, “X”);

1. биграмма — это пара символов, рассматриваемая как единое целое при шифровании. В алгоритме Плейфейра текст разбивается на биграммы, каждая из которых шифруется отдельно;
2. процедура шифрования с помощью алгоритма Плейфейра:

* Разбейте текст на биграммы;
* для каждой биграммы найдите соответствующие символы в шифрующей таблице:
* если символы биграммы находятся в одной строке таблицы, замените их символами, стоящими справа (с циклическим переходом);
* если символы биграммы находятся в одном столбце таблицы, замените их символами, стоящими ниже (с циклическим переходом);
* если символы биграммы находятся в разных строках и столбцах, замените их символами, находящимися на пересечении строки одного символа и столбца другого.