

**МИНОБРНАУКИ РОССИИ**

Федеральное государственное бюджетное образовательное учреждение высшего образования

**«МИРЭА – Российский технологический университет»**

|  |
| --- |
| **РТУ МИРЭА** |
|  |
| **Институт кибербезопасности и цифровых технологий (ИКБ)** |
|  |
| КБ-2 «Информационно-аналитические системы кибербезопасности» |

**ОТЧЕТ О ВЫПОЛНЕНИ ЛАБОРАТОРНОЙ РАБОТЫ №3**

**В РАМКАХ ДИСЦИПЛИНЫ «МЕТОДЫ И СРЕДСТВА КРИПТОРГАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ»**

Выполнил:

Студент 3-ого курса

Учебной группы БИСО-02-22

Зубарев В.С.

Берем ту таблицу, которая приложена в файле  
сделать друг другу зашифрованное письмо, с помощью построения дерева решений найти ключ. Длинна ключа 4-5 символов  
Для шифрования при помощи шифра Плейфера необходимо создать квадрат Плейфера.



Рисунок 1 - Квадрат Плейфера

Далее нужно разбить открытый текст на биграммы.Если биграмма содержит две одинаковые буквы, добавляем между ними "x". Если длина текста нечетная, добавляем "x" в конец.

Зашифруем слово night

Полученное разбиение: "ni", "gt", "tx"n", "ig", "ht".

**Шифрование биграмм**

Правила шифрования:

1. Если буквы биграммы находятся в одной строке, заменяем их на буквы справа (циклически).
2. Если буквы находятся в одном столбце, заменяем их на буквы снизу (циклически).
3. Если буквы образуют прямоугольник, заменяем их на буквы в противоположных углах прямоугольника (по строке).

Применим эти правила к каждой биграмме:

1. **"ni"**:
   * "n" и "i" находятся в разных строках и столбцах. Образуют прямоугольник.
   * Координаты:
     + "n" → (4, 1)
     + "i" → (3, 2)
   * Заменяем на противоположные углы: "0" (4, 2) и "h" (3, 1).
   * Шифр: "oh".
2. **"gh"**:
   * "g" и "h" образуют прямоугольник.
   * Координаты:
     + "g" → (2, 5)
     + "t" → (1, 2)
   * Заменяем на буквы справа: "a" (2, 1) и "i" (1, 5).
   * Шифр: "db".
3. **"hx"**:
   * "h" и "x" образуют прямоугольник.
   * Координаты:
     + "h" → (2, 3)
     + "x" → (5, 4)
   * Заменяем на буквы снизу: "l” (3, 4) и "u" (5, 1).
   * Шифр: "lu".

Таким образом зашифрованный текст получается OHDBLU

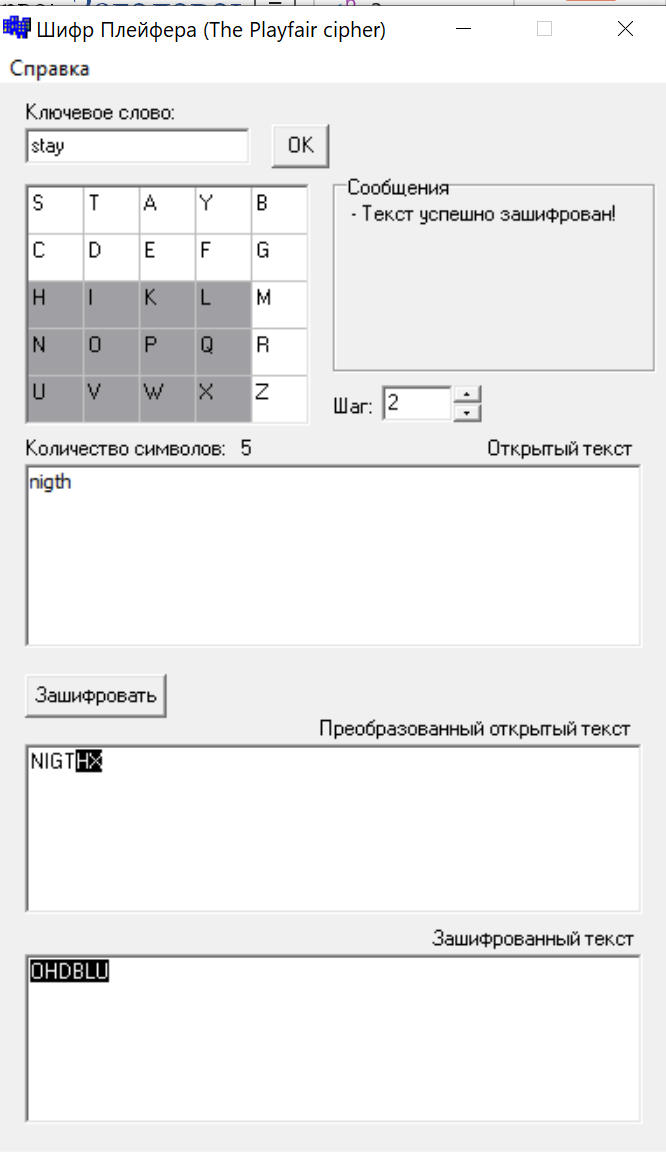


Рисунок 2 -Шифрование методом Плейфера