##### **СРСП 2.** Биграммные замены. Шифр Плейфера и криптоанализ шифра. Шифр «двойной квадрат».

**Форма и содержание отчета**

Отчет должен содержать:

1. Титульный лист установленного образца.
2. Описание комплексного поиск возможных методов доступа.
3. Сравнительный анализ рассмотренных терминалов защищенной информационной системы.
4. Перечень использованных информационных источников.

Отчет выполняется на листах формата А4 рукописным или печатным способом. При рукописном оформлении отчета текст следует излагать четким почерком чернилами черного цвета.

**Бигра́ммный шифр** — это [криптографический](https://ru.wikipedia.org/wiki/%D0%9A%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D0%B8%D1%8F) [алгоритм](https://ru.wikipedia.org/wiki/%D0%90%D0%BB%D0%B3%D0%BE%D1%80%D0%B8%D1%82%D0%BC), который предназначен для [шифрования](https://ru.wikipedia.org/wiki/%D0%A8%D0%B8%D1%84%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D0%B5) групп из двух [букв](https://ru.wikipedia.org/wiki/%D0%91%D1%83%D0%BA%D0%B2%D0%B0) (биграмм).

**Шифр Плейфера** - ручная симметричная техника шифрования, в которой впервые использована замена биграмм. Изобретена в 1854 году Чарльзом Уитстоном. Шифр предусматривает шифрование пар символов (биграмм), вместо одиночных символов, как в шифре подстановки и в более сложных системах шифрования Виженера. Таким образом, шифр Плейфера более устойчив к взлому по сравнению с шифром простой замены, так как затрудняется частотный анализ. Он может быть проведен, но не для 26 возможных символов (латинский алфавит), а для 26х26=676 возможных биграмм. Анализ частоты биграмм возможен, но является значительно более трудным и требует намного большего объема зашифрованного текста.

#### **Шифрование**

Шифр Плейфера использует матрицу 5х5 (для латинского алфавита, для русского алфавита необходимо увеличить размер матрицы до 6х6), содержащую ключевое слово или фразу. Для создания матрицы и использования шифра достаточно запомнить ключевое слово и четыре простых правила. Чтобы составить ключевую матрицу, в первую очередь нужно заполнить пустые ячейки матрицы буквами ключевого слова (не записывая повторяющиеся символы), потом заполнить оставшиеся ячейки матрицы символами алфавита, не встречающимися в ключевом слове, по порядку (в английских текстах обычно опускается символ "Q", чтобы уменьшить алфавит, в других версиях "I" и "J" объединяются в одну ячейку). Ключевое слово может быть записано в верхней строке матрицы слева направо, либо по спирали из левого верхнего угла к центру. Ключевое слово, дополненное алфавитом составляет матрицу 5х5 и является ключом шифра.

Для того, чтобы зашифровать сообщение необходимо разбить его на биграммы ( группы из двух символов), например « Hello World» становится «HE LL OW OR LD», и отыскать эти биграммы в таблице. Два символа биграммы соответствуют углам прямоугольника в ключевой матрице. Определяем положения углов этого прямоугольника относительно друг друга. Затем руководствуясь следующими 4 правилами зашифровываем пары символов исходного текста:

* Если два символа биграммы совпадают, добавляем после первого символа «Х», зашифровываем новую пару символов и продолжаем. В некоторых вариантах шифра Плейфера вместо «Х» используется «Q».
* Если символы биграммы исходного текста встречаются в одной строке, то эти символы замещаются на символы, расположенные в ближайших столбцах справа от соответствующих символов. Если символ является последним в строке, то он заменяется на первый символ этой же строки.
* Если символы биграммы исходного текста встречаются в одном столбце, то они преобразуются в символы того же столбца, находящимися непосредственно под ними. Если символ является нижним в столбце, то он заменяется на первый символ этого же столбца.
* Если символы биграммы исходного текста находятся в разных столбцах и разных строках, то они заменяются на символы, находящиеся в тех же строках, но соответствующие другим углам прямоугольника.

Для расшифровки необходимо использовать инверсию этих четырёх правил, откидывая символы «Х» (или «Q») , если они не несут смысла в исходном сообщении.

#### **Пример**

Используем ключ «Playfair example», тогда матрица примет вид:



Зашифруем сообщение «Hide the gold in the tree stump» HI DE TH EG OL DI NT HE TR EX ES TU MP
1. Биграмма HI формирует прямоугольник, заменяем её на BM.
2. Биграмма DE расположена в одном столбце, заменяем её на ND.
3. Биграмма TH формирует прямоугольник, заменяем её на ZB.
4. Биграмма EG формирует прямоугольник, заменяем её на XD.
5. Биграмма OL формирует прямоугольник, заменяем её на KY.
6. Биграмма DI формирует прямоугольник, заменяем её на BE.
7. Биграмма NT формирует прямоугольник, заменяем её на JV.
8. Биграмма HE формирует прямоугольник, заменяем её на DM.
9. Биграмма TR формирует прямоугольник, заменяем её на UI.
10. Биграмма EX находится в одной строке, заменяем её на XM.
11. Биграмма ES формирует прямоугольник, заменяем её на MN.
12. Биграмма TU находится в одной строке, заменяем её на UV.
13. Биграмма MP формирует прямоугольник, заменяем её на IF.
Получаем зашифрованный текст «BM ND ZB XD KY BE JV DM UI XM MN UV IF» Таким образом сообщение «Hide the gold in the tree stump» преобразуется в «BMNDZBXDKYBEJVDMUIXMMNUVIF»

#### Иллюстрации в примерах

Предположим, что необходимо зашифровать биграмму OR. Рассмотрим 4 случая:



OR заменяется на YZ



OR заменяется на BY



OR заменяется на ZX



OR заменяется на ZY

**Криптоанализ алгоритма.**

Суть алгоритма сводится к следующим действиям:

1. Выбирается случайная последовательность букв — основной-ключ. Шифртекст расшифровывается с помощью основного ключа. Для получившегося текста вычисляется коэффициент, характеризующий вероятность принадлежности к естественному языку.
2. Основной ключ подвергается небольшим изменениям (перестановка двух произвольно выбранных букв, перестановка столбцов или строк). Производится расшифровка и вычисляется коэффициент полученного текста.
3. Если коэффициент выше сохраненного значения, то основной ключ заменяется на модифицированный вариант.
4. В противном случае замена основного ключа на модифицированный происходит с вероятностью, напрямую зависящей от разницы коэффициентов основного и модифицированного ключей.
5. Шаги 2-4 повторяются около 50 000 раз.

 Алгоритм периодически замещает основной ключ, ключом с худшими характеристиками. При этом вероятность замены зависит от разницы характеристик, что не позволяет алгоритму принимать плохие варианты слишком часто.
 Для расчета коэффициентов, определяющих принадлежность текста к естественному языку лучше всего использовать частоты появления триграмм.

**Шифрование биграммами с двойным квадратом**

В 1854 году англичанин Чарльз Уитстон разработал новую шифровку биграммами, которую называют двойной квадрат. Шифрование здесь происходит аналогично шифру Playfair, но биграммы шифруются по двум таблицам, случайным образом заполненных алфавитами. Для пары символов из исходного сообщения строится прямоугольник в двух таблицах по правилу – первая буква в левой таблице является одним углом, вторая в правой - другим. Буквы биграммы шифра берутся из двух оставшихся вершин прямоугольника. Если обе буквы лежат в одних и тех же строках, то буквы шифра берут из той же строки, но в следующем столбце таблицы (для последнего столбца – из первого столбца). Пример шифрования методом биграмм с двойным квадратом приведен на рисунке.

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

открытый текст: МЕТОД БИГРАММ.

шифротекст: ФВЪФХ-ХКБ,ЖУЗ-

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

 Криптостойкость биграммных методом существенно выше, чем у методов простой замены (метод биграмм с двойным квадратом использовался военными еще во времена Второй мировой войны). Частотный анализ здесь можно применить только для оценки частоты встречаемости тех или иных буквосочетаний. И хотя анализ показывает, что какие-то биграммы встречаются в текстах на заданном языке чаще других, большое количество биграмм (а их насчитывается 1089 только для букв русского языка) не позволяет выявить соответствие биграмм открытого и закрытого текста.