Полиграммные шифры подстановки

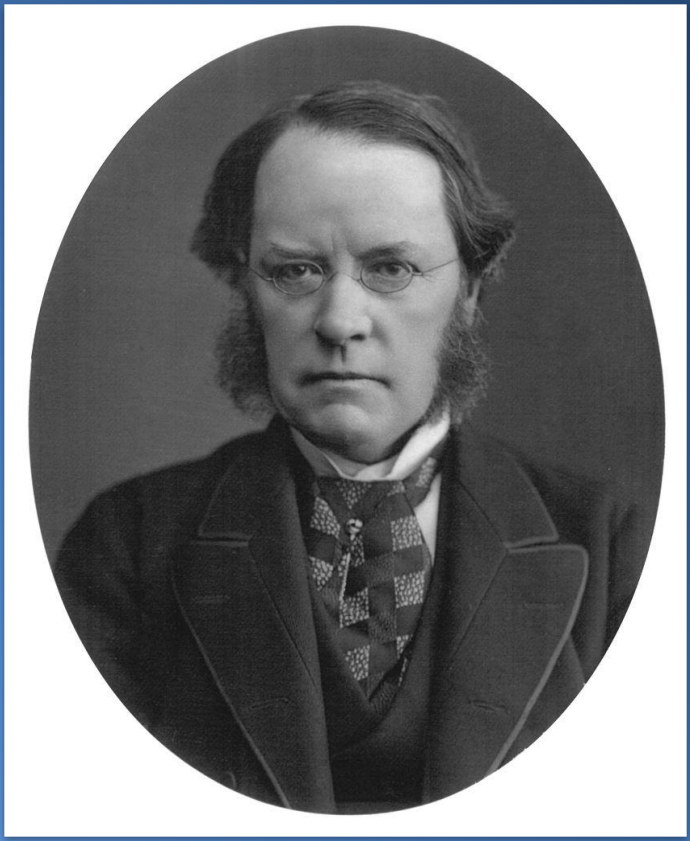
Шифр подстановки

Шифр подстановки - метод шифрования, в котором элементы исходного открытого текста заменяются зашифрованным текстом в соответствии с некоторым

Полиграммные шифры подстановки

В полиграммных шифрах подстановки буквы открытого текста заменяются не по одной, а группами. Первое преимущество такого способа заключается в том, что распределение частот групп букв значительно более равномерное чем отдельных символов. Во-вторых для продуктивного частотного анализа требуется больший размер зашифрованного текста, так число различных групп букв значительно больше, чем просто алфавит.

Шифр Плейфера



Шифр Плейфера – ручная симметричная техника шифрования, в которой впервые использована замена биграмм. Изобретена в 1854 году Чарльзом Уитстоном, но названа именем Лорда Лайона Плейфера, который внедрил данный шифр в государственные службы Великобритании.

Шифр Плейфера

Шифр Плейфера использует матрицу 5x5, содержащую ключевое слово или фразу. Для создания матрицы и использования шифра достаточно запомнить ключевое слово и четыре простых правила. Чтобы составить ключевую матрицу, нужно заполнить пустые ячейки матрицы буквами ключевого слова, потом заполнить оставшееся ячейки матрицы символами алфавита, не встречающимися в ключевом слове, по порядку. Ключевое слово, дополненное алфавитом, составляет матрицу 5x5 и является ключом шифра.

Шифр Плейфера

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 символом.

Правила шифра Плейфера

1.Если два символа биграммы совпадают (или остался один символ), добавляем после первого символа «Х», зашифровываем новую пару символом и продолжаем.

2.Если символы биграммы исходного текста встречаются в одной строчке, 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.

3. Если символы биграммы исходного текста встречаются в одном столбце, то они преобразуются в символы того же столбца, находящиеся непосредственно под ними. Если символ является нижним в столбце, то он заменяется на первый символ этого же столбца.

4. 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.

Шифр Хилла

Шифр Хилла, изобретенный в 1928 году Лестером Хиллом, является полиграммным шифром, который может использовать большие группы с помощью линейной алгебры. Каждой букве сперва сопоставляется число. Для латинского алфавита часто используется простейшая схема: A=0, B=1,…,Z=25. Блок из n букв рассматривается как мерный вектор и умножается на n x n по модулю 26. Компоненты матрицы являются ключом, и должны быть случайными при условии что матрица обратима, чтобы была возможна операция расшифрования.

Спасибо за просмотр!