**МИНИСТЕРСТВО ОБРАЗОВАНИЯ МОСКОВСКОЙ ОБЛАСТИ**

**Государственное бюджетное профессиональное образовательное учреждение Московской области «Люберецкий техникум имени Героя Советского Союза, летчика-космонавта Ю.А.Гагарина»**

**КУРСОВАЯ РАБОТА**

**Ефремова Егора Михайловича**

**ОП. 03 Основы алгоритмизации и программирования**

**по теме:Шифрование сообщения в Python**

**Выполнил студент \_\_\_\_\_\_\_\_\_\_\_\_\_ Ефремов Егор Михайлович**

**(подпись) (ФИО полностью)**

**Руководитель Тарджиманян Лия Николаевна**

**(подпись) (ФИО полностью)**

**Оценка \_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Дзержинский 2022**

**Содержание**

**ВВЕДЕНИЕ**…………………………………………………...…………………..4

**Глава 1**.**КРИПТОГРАФИЧЕСКИЕ СВЕДЕНИЯ**……………...……………..7

1.1**Шифр цезаря**…………………………………………………..…….....7

1.2**Шифр Виженера**………………………………………………….........8

1.3**Дешифрование**………………………………………..……..…………9

**Глава 2.Пример работы Шифра Виженера**……………..……………..…….13

**ЗАКЛЮЧЕНИЕ**………………………………….…….………..………..…….15

**Список источников**………………………...…………………………………..16

**ВВЕДЕНИЕ**

Наверное, нет ни одного человека, не знакомого с понятием "шифрование". Каждому пользователю компьютера приходилось защищать свои файлы от "чужого глаза" и шифрование в этом помогает как нельзя лучше. Но намного чаще возникает желание передать защищенные файлы по каналам связи. Особенно актуально задача защищенной передачи данных и подтверждение их подлинности встает сейчас, после принятия Закона об ЭЦП.

Какие же проблемы могут возникнуть у вас при попытке передать какие-либо данные в зашифрованном виде? Если вы выбираете какой-либо симметричный алгоритм шифрования (например, DES или ГОСТ 28147-89), то один и тот же ключ используется и для зашифрования и расшифрования данных. Т.е. ваш оппонент должен иметь ключ, используемый для шифрования. Передать этот ключ по обычным каналам связи в открытом виде не представляется возможным - любой получивший доступ к этому ключу сможет расшифровать ваши данные. Одним из решений этой проблемы является использование фельдъегерской службы, но это очень дорого и не всегда применимо на практике.

Вторым решением, которое получило широкое распространение в коммерческих и государственных структурах, является применением криптографии с открытыми ключами (например, RSA), смысл которой заключается в следующем. Вместо одного секретного ключа используется два - закрытый (или секретный) и открытый (или публичный). Исходя из названия последнего, можно сделать вывод, что он распространяется без ограничений, и именно он используется при зашифровании информации для владельца этого ключа. Т.к. открытый и закрытый ключи связаны между собой особыми математическими преобразованиями, то расшифровать полученные данные можно только с помощью секретного ключа, входящего в пару "открытый/закрытый ключи".

На первый взгляд проблема с передачей зашифрованных сообщений решена, но… это только на первый взгляд. Как пользователь, получивший открытый ключ своего оппонента сможет удостовериться, что ключ получен именно от него, а не от злоумышленника, решившего проникнуть в чужие тайны? Вторая проблема, как владелец открытого ключа сможет убедиться в том, что он послал свой ключ своему оппоненту, а не маскирующемуся злоумышленнику?

При небольшом числе участников защищенного обмена, к тому же проживающих в одном городе, эта проблема решается элементарно - достаточно встретиться вместе и обменяться на дискете открытыми ключами. Но что делать, если участники находятся в разных городах (а зачастую и странах) и таких участников слишком много - сотни тысяч и даже миллионы? И вот тут на сцену выходит PKI (Public Key Infrastructure).

На свете множество неразгаданных шифров, непонятных языков, загадочных тайнопись и не расшифрованных карт, но мы остановимся лишь на 2 из них:

- Шифр Цезаря, также известный как шифр сдвига, код Цезаря или сдвиг Цезаря;

- Шифр Виженера (фр. *Chiffre de Vigenère*).

Шифр Цезаря называют в честь Гая Юлия Цезаря, который согласно «Жизни двенадцати царей» Светония использовал его со сдвигом 3, чтобы защищать военные сообщения. Цезарь был первым зафиксированным человеком, использующим эту схему, но еще и до него были зафиксированы случаи использования других, похожих шифров подстановки.

Шифр Виженера, названный в честь Блеза Вижинера, объединил подходы Тритемия, Беллозо, Порта к шифрованию открытых текстов, по существу, не внеся в них ничего оригинального. Дэвид Кан в своей книге «Взломщики кодов» (см. прил. 1) отозвался об этом осуждающе, написав, что история «проигнорировала важный факт и назвала шифр именем Виженера, несмотря на то что он ничего не сделал для его создания».

Шифр Виженера имел репутацию исключительно стойкого к «ручному» взлому. Известный писатель и математик Чарльз Лютвидж Доджсон назвал шифр Виженера невзламываемым в своей статье «Алфавитный шифр» англ. «*The Alphabet Cipher»*, опубликованной в детском журнале в 1868 году. В 1917 году Scientific American также отозвался о шифре Виженера как о не поддающемся взлому. Это представление было опровергнуто после того, как Фридрих Касиски полностью взломал шифр в XIX веке, хотя известны случаи взлома этого шифра некоторыми опытными криптоаналитиками ещё в XVI веке.

*Актуальность:*

Несмотря на современную криптоаналитическую нестойкость, шифры Цезаря и Виженера являются яркими примерами двух значимых периодов в истории криптографии и криптоанализа. Они являются отправной точкой для дальнейшего углубленного изучения шифров для любого новичка, решившего познакомиться с ними.

Изучив основу их работы, а также самостоятельно воссоздав её своими руками можно понять основы криптографии, необходимые для более трудных шифров. Более того, рассмотрев их криптоаналитические аспекты и принципы их взлома, а также алгоритмизировать их в виде компьютерного кода можно использовать аналогичные методы на шифрах более высокого порядка. Изучение первых шифров поможет лучше понять, зачем нужна та или иная операция в современных алгоритмах шифрования.

Именно поэтому нужно знать и уметь реализовывать шифрование и дешифрование этих важных исторических шифров.

**Глава 1. КРИПТОГРАФИЧЕСКИЕ СВЕДЕНИЯ**

**1.1 Шифр цезаря**

Шифр Цезаря — это вид шифра подстановки, в котором каждый символ в открытом тексте заменяется символом, находящимся на некотором постоянном числе позиций левее или правее него в алфавите. Например, в шифре со сдвигом вправо на 3, “А” была бы заменена на “Г”, “Б” станет “Д”, и так далее (см. прил. 4-5).

Этот шифр, известный также как шифр сдвига, код Цезаря или сдвиг Цезаря, является одним из самых простых и наиболее широко известных методов шифрования.

Шаг шифрования, выполняемый шифром Цезаря, часто включается как часть более сложных схем, таких как шифр Виженера, и всё ещё имеет современное приложение в системе ROT13. Как и все моноалфавитные шифры, шифр Цезаря легко взламывается и не имеет почти никакого применения на практике. Тем не менее, он является одним из самых ярких и важных примеров в развитии шифров, в том числе и моноалфавитных.

Многократное шифрование никак не улучшает стойкость, так как применение шифров со сдвигом a и b эквивалентно применению шифра со сдвигом a + b. В математических терминах шифрование с различными ключами образует группу.

Математическая модель

Если сопоставить каждому символу алфавита его порядковый номер (нумеруя с 0), то шифрование можно выразить формулами модульной арифметики:

y=(x+k) mod n, x=(y+k) mod n,

где x — символ исходного текста, y — символ шифрованного текста, n — мощность алфавита, k — ключ.

С точки зрения математики шифр Цезаря является частным случаем аффинного шифра.

**1.2 Шифр Виженера**

*Шифр Виженера* (фр. *Chiffre de Vigenère*) — метод полиалфавитного шифрования буквенного текста с использованием ключевого слова. Этот метод является простой формой многоалфавитной замены, то есть, по сути, усложненной формой метода шифра Цезаря.

*Шифр Виженера* изобретался многократно. Впервые этот метод описал Джованни Баттиста Белласо (итал. *Giovanni Battista Bellaso*) в книге «La cifra del. Sig. Giovan Battista Bellas» в 1553 году, однако в XIX веке получил имя Блеза Вижинера, французского дипломата. Метод прост для понимания и реализации, он является недоступным для простых методов криптоанализа. Многие люди пытались реализовать схемы шифрования, которые по сути являлись шифрами Виженера.

Хотя шифр легко понять и реализовать, на протяжении трех столетий он противостоял всем попыткам его сломать; чем и заработал название “le chiffre indéchiffrable” (с французского “неразгаданный шифр”).

*Описание*

В шифре Цезаря каждая буква алфавита сдвигается на несколько позиций; например, в шифре Цезаря при сдвиге +3, A стало бы Г, Б стало бы Д и так далее. Шифр Виженера состоит из последовательности нескольких шифров Цезаря с различными значениями сдвига. Для зашифровывания может использоваться таблица алфавитов, называемая “tabula recta” или квадрат (таблица) Виженера (см. прил. 7-8).

Применительно к русскому алфавиту таблица Виженера составляется из строк по 33 символов (26 для латинского), причём каждая следующая строка сдвигается на несколько позиций. Таким образом, в таблице получается 33 (26) различных шифров Цезаря. Иногда также выделяют версию с русским алфавитом без буквы “ё”, что значительно упрощает некоторые процессы шифрования и дешифрования, а также реализацию шифра в виде компьютерной программы.

В общем, на каждом этапе шифрования используются различные алфавиты, выбираемые в зависимости от символа ключевого слова.

*Математическая модель*

Расшифровывание производится следующим образом: находим в таблице Виженера строку, соответствующую первому символу ключевого слова; в данной строке находим первый символ зашифрованного текста. Столбец, в котором находится данный символ, соответствует первому символу исходного текста. Следующие символы зашифрованного текста расшифровываются подобным образом. Шифрование можно представить как:

cj=(mj+kj) mod n, mj=(cj+n-kj) mod n,

где n — количество букв в алфавите, mj — буквы исходного текста, kj — буквы ключа

**1.3 Дешифрование**

*Дешифрование шифра Цезаря*

Несмотря на то, что при дешифровании в эксперименте мы будем отталкиваться от того, что пользователь знает всё, кроме ключа, полезно рассмотреть и другой случай, когда пользователь знает всё, кроме использованного шифра.

*Взлом без знания шифра*

Итак, взломщик знает (или предполагает), что использовался простой шифр подстановки (исходя из того, что ключ является некоторым целым числом, что сразу отсекает почти все не подстановочные шифры), но не знает, что это — схема Цезаря.

Тогда шифр может быть взломан, используя те же самые методы что и для простого шифра подстановки, такие как частотный анализ. Используя эти методы, взломщик, вероятно, быстро заметит регулярность в решении и поймёт, что используемый шифр — это шифр Цезаря.

*Взлом без знания ключа*

Это наш основной рассматриваемый случай.

Мы знаем, что взломщик знает, что использовался шифр Цезаря, но не знает значение сдвига. В таком случае взлом шифра является даже более простым.

Действительно, дешифровать шифротекст можно простым полным перебором, ведь существует всего 33 значения сдвига для русского языка (26 для английского языка), так что метода грубой силы вполне достаточно.

Можно пойти и другим путём для взлома, если, например, процесс необходимо автоматизировать (избавиться от необходимости присутствия человека) — использовать частотный анализ и проверить частоты встречаемости букв. Изобразив диаграммой частоты встречания букв в зашифрованном тексте, и зная ожидаемое распределение букв для обычного текста на рассматриваемом языке, можно легко определить сдвиг, взглянув на смещение некоторых характерных черт на диаграмме.

Однако, стоит учитывать, что этот метод (как и любой другой метод дешифрования) работает тем лучше, чем больше длина шифротекста, и наоборот. То есть, чем короче данный для анализа текст, тем больше вероятность того, что частотный анализ выдаст ошибку.

*Дешифрование шифра Виженера*

Криптоанализ шифра Виженера процесс очень трудный, затратный по времени и силам, особенно если проводить его вручную, без использования техники. В целом, его можно разбить на 2 этапа:

- Сначала пытаются определить длину ключа. Длина ключа задаёт количество используемых алфавитов и период шифрования этими алфавитами. Поэтому на этом этапе исследуется периодичность шифротекста;

- После того, как найдена длина, приступают к поиску конкретного вида ключа. Для этого вычисляют относительные сдвиги используемых алфавитов, а затем подбирают ключ перебором.

*Алгоритм нахождения длины ключа*

Разобьем текст *x1x2…xn* на столбцы размера *t*:

Если *t* кратно длине ключа, то каждые два элемента текста, отстоящие друг от друга на позиций, *a* ∈ *N*, зашифрованы одним и тем же алфавитом. А это означает, что каждая строка в выписанной выше таблице получена из открытого текста перестановкой. Если же *t* не кратно длине ключа, то строки являются полиалфавитным шифром.

Ранее было показано, что индекс совпадений для перестановки открытого текста и для полиалфавитного шифра заметно отличается. Таким образом, перебирая различные значения *t* и вычисляя для каждого из них индекс совпадений, мы можем выделить те *t*, которые кратны длине ключа. Определить длину ключа по этим данным не составляет труда.

*Алгоритм нахождения ключа*

Предположим, мы определили длину ключа *t*. Найдем теперь сам ключ.

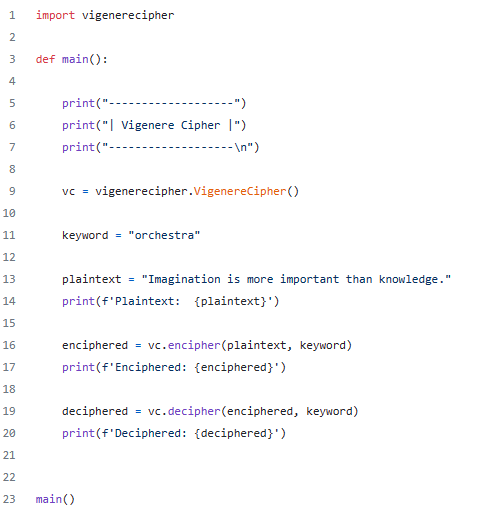
Вновь выпишем текст в столбцы размера *t*.

Рассмотрим две строки этой таблицы. Сдвинем алфавит одной из строк на *s* символов и вычислим взаимный индекс совпадений полученных строк. Т.к. каждая из этих двух строк получена сдвигом алфавита открытого текста, то максимум взаимного индекса совпадений будет наблюдаться при нулевом конечном относительном сдвиге.

Поэтому применяется следующий алгоритм: вычисляется взаимный индекс совпадений для различных *s*, ищется значение *s*, при котором взаимный индекс совпадений максимален. Тогда начальный относительный сдвиг строк будет равен *m-s* (*m* — размер алфавита). Вычисляются относительные сдвиги между всеми парами строк. Т.к. сдвиги строк таблицы соответствуют сдвигам букв ключа, то остаётся перебрать *m* возможных ключей и выбрать из них наиболее правдоподобный.

**Глава 2. Пример работы шифра Виженера**

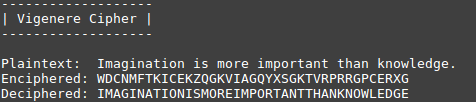
*Код на Python для шифра Виженера:*

****

**Рисунок 1**

На рисунке 1 представлен код шифра Виженера (main.py в папке)

*Выход:*

****

**Рисунок 2**

На рисунке 2 представлен результат работы кода шифра Виженера

*Функция vigenere cipher* принимает два аргумента: message - сообщение, которое нужно зашифровать, и key - ключевое слово, используемое для шифрования.  
Сначала функция создает таблицу Полибия, где каждая строка и столбец представляют собой буквы алфавита от A до Z. Затем ключевое слово преобразуется в числовой массив, где каждая буква заменяется на соответствующее число от 0 до 25.  
Далее происходит шифрование сообщения. Каждая буква сообщения заменяется на букву из таблицы Полибия, используя текущую букву ключа. Если текущий символ сообщения не является буквой алфавита, он остается без изменений. Индекс ключа увеличивается на 1 после каждого зашифрованного символа, и если индекс достигает конца ключа, он переходит обратно к началу.

В результате функция возвращает зашифрованное сообщение.

**ЗАКЛЮЧЕНИЕ**

В процессе работы были выполнены следующие задачи:

* описан принцип работы шифра Цезаря
* описан принцип шифрования предложенный Виженером;
* разработан код в Pacharm, демонстрирующей шифрование Виженера

В работе были рассмотрены и изучены принципы работы двух способов шифрования текста(сообщений),также был представлен пример работы шифра Виженера, что позволило перейти от теории к практическому применению данного метода шифрования.

**Список использованных источников**

**1.** [**https://ru.wikipedia.org/wiki/Шифр\_Виженера**](https://ru.wikipedia.org/wiki/%D0%A8%D0%B8%D1%84%D1%80_%D0%92%D0%B8%D0%B6%D0%B5%D0%BD%D0%B5%D1%80%D0%B0)

**2.** [**https://ru.wikipedia.org/wiki/Шифр\_Цезаря**](https://ru.wikipedia.org/wiki/%D0%A8%D0%B8%D1%84%D1%80_%D0%A6%D0%B5%D0%B7%D0%B0%D1%80%D1%8F)

**3. https://ru.wikipedia.org/wiki/Криптография**