**МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ**

**БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ**

**Факультет прикладной математики и информатики**

**Ястребова Вероника**

**Классические криптосистемы**Отчет по лабораторной работе №2

Вариант 20

(«Криптография»)

студентки 2 курса 13 группы

**Преподаватель**

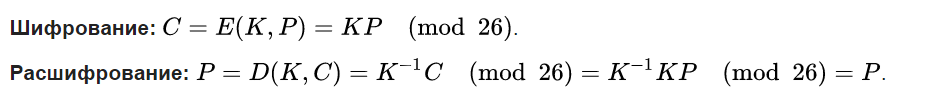
**Ярошеня Ю.В**

**Минск 2018**

**1. Шифр Хилла**

Шифр Хилла является полиграммным шифром, который может использовать большие блоки с помощью линейной алгебры. Каждой букве алфавита сопоставляется число по модулю 26. Для латинского алфавита часто используется простейшая схема: A = 0, B = 1, …, Z = 25. Блок из *n* букв рассматривается как *n*-мерный вектор и умножается по модулю 26 на матрицу размера *n* × *n*. Элементы матрицы являются ключом. Матрица должна быть обратима в {\displaystyle \mathbb {Z} \_{26}^{n}}чтобы была возможна операция расшифрования.

Для того, чтобы ***расшифровать*** сообщение, требуется получить обратную матрицу ключа {\displaystyle K^{-1}}К-1. Не все матрицы имеют обратную. Матрица будет иметь обратную в том и только в том случае, когда её детерминант не равен нулю и не имеет общих делителей с основанием модуля. Если детерминант матрицы равен нулю или имеет общие делители с основанием модуля, то такая матрица не может использоваться в шифре Хилла, и должна быть выбрана другая матрица (в противном случае шифротекст будет невозможно расшифровать).



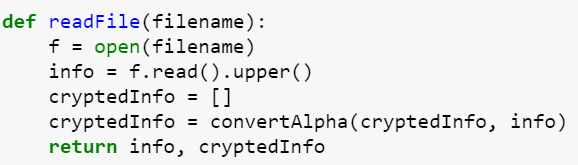
Р – открытый текст

С – закрытый текст

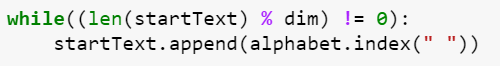
К – ключ шифрования

Процесс ***шифрования***:

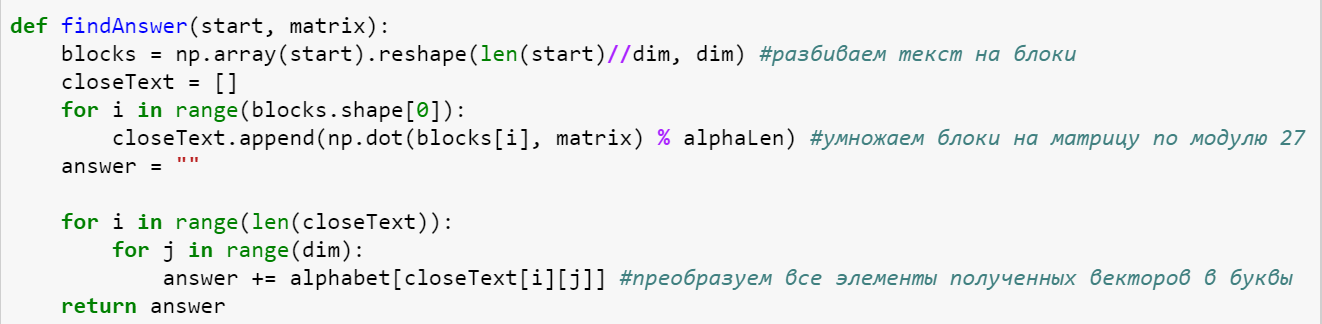
1. Разбиваем открытый текст на блоки по 2 элемента. Если в конце остается один символ, то дополняем текст пробелом.





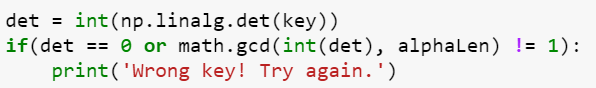


2. Преобразуем блоки текста в вектора и умножаем их на матрицу ключа по модулю 27. Заменяем в полученной числовой последовательности числа на буквы в соответствии с нашей схемой.



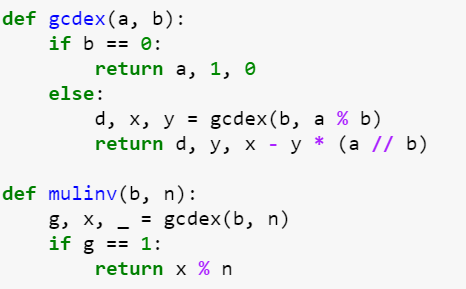
Процесс ***дешифрования*** :

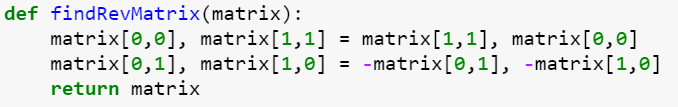
1. Находим определитель матрицы ключа. Если он равен 0 или не является взаимно простым с длиной алфавита, то матрица ключа не имеет обратной и расшифровать сообщение мы не сможем.



2. Находим обратный к определителю элемент по модулю 27 с помощью расширенного алгоритма Евклида





3. Находим матрицу алгебраических дополнений для матрицы ключа

4. Получаем обратную матрицу по модулю 27 для матрицы ключа:



5. Разбиваем закрытый текст на блоки и, используя обратную по модулю матрицу, расшифровываем закрытый текст

***Криптостойкость***

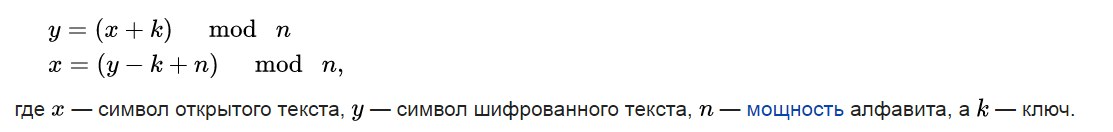
Стандартный шифр Хилла уязвим к атаке по выбранному открытому тексту, потому что в нем используются линейные операции. Криптоаналитик, который перехватит n2 пар символ сообщения/символ шифртекста сможет составить систему линейных уравнений, которую обычно несложно решить.

Полный перебор – не самая эффективная атака на шифр Хилла

**2. 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.

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

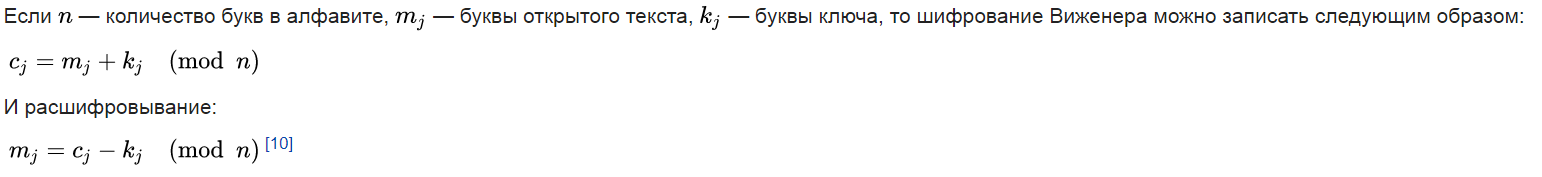


***Криптостойкость***

Шифр Цезаря очень легко взламывается и не имеет почти никакого применения на практике. Достаточно всего лишь перебрать 26 вариантов сдвига и будет легко найти осмысленный текст.

**3. Шифр Виженера**

Шифр Виженера — метод полиалфавитного ***шифрования*** буквенного текста с использованием ключевого слова. 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. Применительно к латинскому алфавиту таблица Виженера составляется из строк по 26 символов, причём каждая следующая строка сдвигается на несколько позиций. Таким образом, в таблице получается 26 различных шифров Цезаря. На каждом этапе шифрования используются различные алфавиты, выбираемые в зависимости от символа ключевого слова.

***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. 

***Криптостойкость***

Шифр Виженера «размывает» характеристики частот появления символов в тексте, но некоторые особенности появления символов в тексте остаются. Главный недостаток шифра Виженера состоит в том, что его ключ повторяется. Поэтому простой криптоанализ шифра может быть построен в два этапа:

1. Поиск длины ключа. Можно анализировать распределение частот в зашифрованном тексте с различным прореживанием. То есть брать текст, включающий каждую 2-ю букву зашифрованного текста, потом каждую 3-ю и т. д. Как только распределение частот букв будет сильно отличаться от равномерного, то можно говорить о найденной длине ключа.
2. Криптоанализ. Совокупность *l* шифров Цезаря (где *l* — найденная длина ключа), которые по отдельности легко взламываются.

Определить длину ключа можно с помощью тестов Фридмана и Касиски.

Листинг:

