КРИПТОГРАФИЯ

ВЫПОЛНИЛА: НИЧУТИНА ЕКАТЕРИНА,
УЧЕНИЦА 8 КЛАССА,
МКОУ №9 С.КОМИССАРОВО.

Цели:

- Познакомиться с основными понятиями криптографии и некоторыми шифрами прошедших веков.
- Узнать, каким образом происходит шифрование с помощью этих шифров.
- Научиться дешифровать сообщения, зашифрованные такими шифрами.

Защищая свою информацию, мы стремимся сохранить в тайне имеющийся у нас запас знаний, а рассекречивая чужую — увеличить этот запас за счет конкурентов. В документах древних цивилизаций - Индии, Египта, Месопотамии - есть сведения о системах и способах составления шифрованных писем

Криптография – наука о методах шифрования информации с целью её защиты от незаконных пользователей.

Шифр – метод преобразования информации с целью её защиты.

Шифрование – процесс преобразования защищаемой информации в шифрованное сообщение с помощью определённых правил, содержащихся в шифре.

История

Коды появились в глубокой древности в виде криптограмм (по-гречески - тайнопись). Порой священные иудейские тексты шифровались методом замены. Вместо первой буквы алфавита писалась последняя буква, вместо второй - предпоследняя и так далее. Этот древний метод шифрования назывался атбаш. Известно, что шифровалась переписка Юлия Цезаря (100 - 44 гг. до н. э.) с Цицероном (106 - 43 г.г. до н. э.). Шифр Цезаря реализуется заменой каждой буквы в сообщении другой буквой этого же алфавита, отстоящей от нее в алфавите на фиксированное число букв. В своих шифровках Цезарь заменял букву исходного открытого текста буквой, отстоящей от исходной буквы впереди на три позиции.

С начала эпохи Возрождения (конец XIV столетия) начала возрождаться и криптография. Наряду с традиционными применениями криптографии в политике, дипломатии и военном деле появляются и другие задачи - защита интеллектуальной собственности от преследований инквизиции или заимствований злоумышленников. В разработанных шифрах перестановки того времени применяются шифрующие таблицы, которые в сущности задают правила перестановки букв в сообщении.

В качестве ключа в шифрующих таблицах используются: a) размер таблицы; b) слово или фраза, задающие перестановку; c) особенности структуры таблицы.

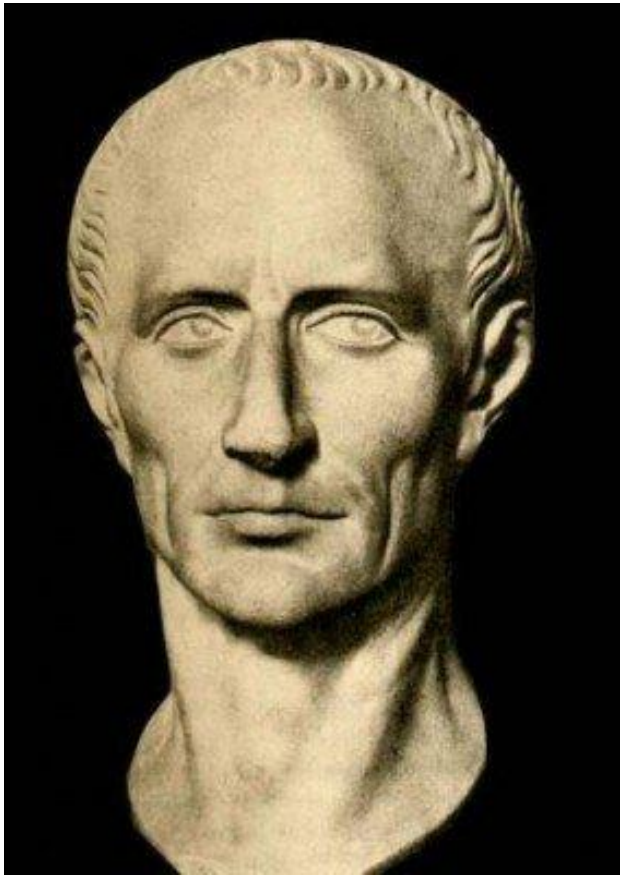
Скитала

Первые сведения об использовании шифров в военном деле связаны с именем спартанского полководца Лисандра. Он использовал шифр “Скитала”. Этот шифр известен со времен войны Спарты против Афин в V веке до н.э.

Квадрат Полибия

В Древней Греции во II в. до н.э. был известен шифр, называемый “квадрат Полибия”.

Шифр Цезаря



Примером наиболее простого шифра,

относящегося к группе шифров простой подстановки, является шифр Цезаря.

Математическая модель

Шифрование и дешифрование шифра Цезаря можно выразить следующими формулами:

$$y = x + k \qquad\qquad x = y - k$$

где x — символ открытого текста, y — символ шифрованного текста, а k — ключ.

Виды криптограмм:

- 1)Простая перестановка
- 2)Одиночная перестановка
- 3)Двойная перестановка

1)Простая перестановка

(Один из самых простых табличных шифров перестановки, для которой ключом служит размер таблицы. Естественно, отправитель и получатель сообщения должны заранее условиться об общем ключе в виде размера таблицы.

З	А	Н	Т
А	Т	А	О
Н	Е	Я	Р
И	Л	И	И
М	Ь	С	Я

2)Одиночная перестановка

Несколько большей стойкостью к раскрытию обладает метод шифрования, называемый одиночной перестановкой по ключу. Этот метод отличается от предыдущего тем, что столбцы таблицы переставляются по ключевому слову, фразе или набору чисел длиной в строку таблицы.

М	О	С	К	В	А
4	5	6	3	2	1
С	Д	К	Е	З	Ё
Т	Ё	И	Б	А	Ж
О	Ж	В	Е	С	Е
О	Е	С	З	Т	К

А	В	К	М	О	С
1	2	3	4	5	6
Ё	З	Е	С	Д	К
Ж	А	Б	Т	Ё	И
Е	С	Е	О	Ж	В
К	Т	З	О	Е	С

3)Двойная перестановка

Для обеспечения дополнительной скрытности можно повторно зашифровать сообщение, которое уже прошло шифрование. Такой метод шифрования называется *двойной перестановкой*. В случае двойной перестановки столбцов и строк таблицы перестановки определяются отдельно для столбцов и отдельно для строк. Сначала в таблицу записывается текст сообщения, а потом поочередно переставляются столбцы, а затем строки

	4	1	3	2
3	П	Р	И	Л
1	Е	Т	А	Ю
4	В	О	С	Ь
2	М	О	Г	О

Исходная таблица

	1	2	3	4
3	Р	Л	И	П
1	Т	Ю	А	Е
4	О	Ь	С	В
2	О	О	Г	М

Перестановка столбцов

	1	2	3	4
1	Т	Ю	А	Е
2	О	О	Г	М
3	Р	Л	И	П
4	О	Ь	С	В

Перестановка строк

Заключение

- *Познакомилась с основными понятиями криптографии: шифр, шифрование,ключ и некоторыми шифрами прошедших веков: шифр «Скитала», «квадрат Полибия», шифр Цезаря, шифры перестановок.*
- *Узнала, каким образом происходит шифрование с помощью этих шифров.*
- *Научилась дешифровать сообщения, зашифрованные такими шифрами*

Спасибо за внимание