Математика и криптография

Выполнила: Павлова Ольга Владимировна, учитель математики МБОУ СОШ № 36 г. Волжского Волгоградской области

Проблема защиты информации от прочтения посторонним лицом волновала человеческий ум с давних времен.

Цель работы: изучить способы засекречивания информации и выявить необходимость криптографии в современном обществе.

Задачи:

- Собрать научную информацию о разных способах засекречивания информации;
- Выявить в ходе экспериментов наиболее простые и эффективные способы шифрования;
- Разработать собственный шифр;
- Собрать рецепты симпатических (невидимых) чернил.

Гипотеза: криптография необходима в современном мире.
Заниматься шифрами увлекательно и полезно.
Знание и использование шифра помогает засекретить информацию, не предназначенную для посторонних

Методы исследования работы:

Теоретический

Изучить литературу по данной теме

Практические

Анкетирование, эксперим

Что такое шифр и криптография?

Шифр *(от арабского "цифра")* - это система условных знаков для секретного письма, читаемого с помощью ключа.

Криптография *(от греч. cryptos - тайный, сокрытый, и grapho - пишу, черчу, рисую)* — слово греческое, в переводе означает тайное, скрытое (крипто) письмо (графия), или тайнопись.

Немного из истории…

Наукой не установлен точный исторический период, когда появилась криптография, каковы были ее первоначальные формы и кто был ее создателем.

Американский криптограф Л. Д. Смит подчеркивает, что криптография по возрасту старше египетских пирамид.

Использовалась тайнопись и в рукописных памятниках Древнего Египта. Здесь шифровались религиозные тексты и медицинские рецепты.

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.

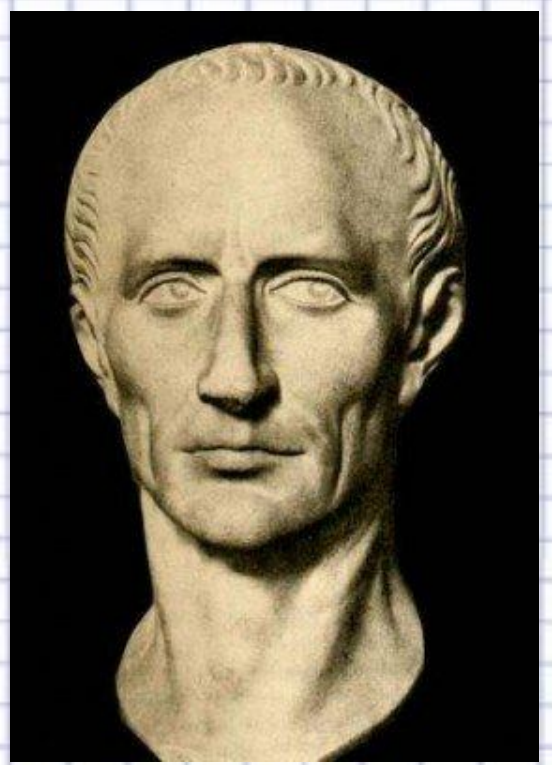
Методы защиты информации:

шифрование по принципу замены (шифр Юлия Цезаря, шифровальный диск);

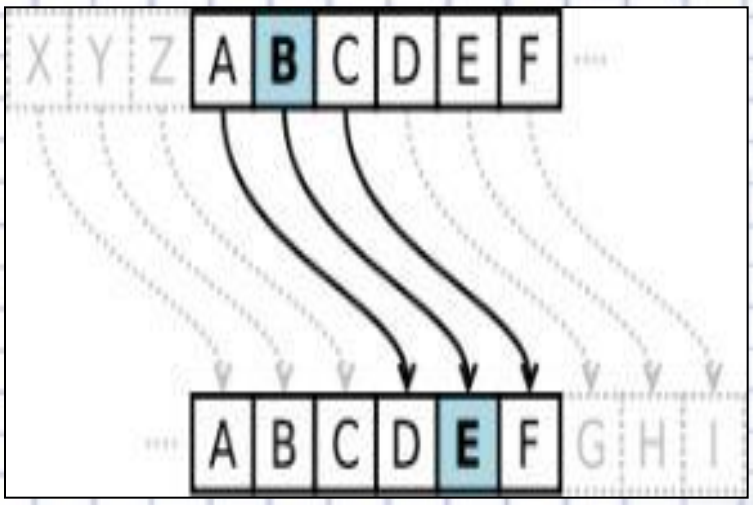
физическая защита информации (физическое ограничение доступа к информации путем хранения ее в надежном сейфе или строго охраняемом помещении, «запрятывание» секретных сообщений, использование симпатических чернил.)

шифрование по принципу перестановки (шифровальный прибор скитала)

Шифр Юлия Цезаря



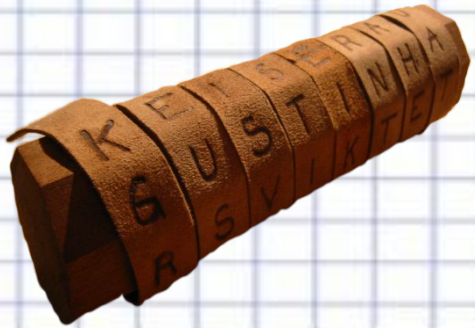
Примером наиболее простого шифра, относящегося к группе шифров простой подстановки, является шифр Цезаря.



Достоинства - простота шифрования и дешифрования.

Недостатки - легко взламывается и, поэтому не имеет практически никакого применения

Шифровальный прибор "Скитала"

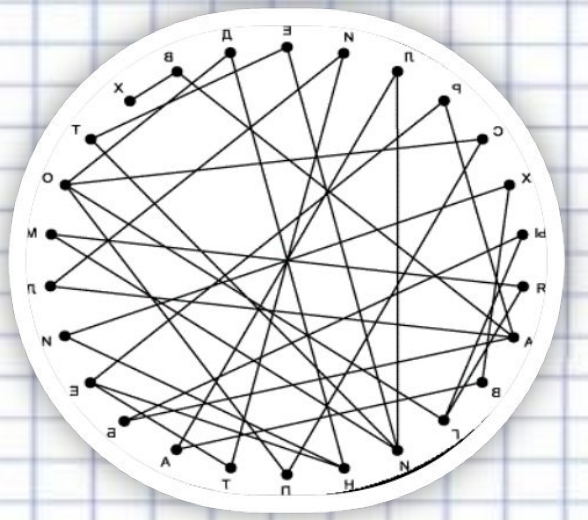


Первые сведения об использовании шифров в военном деле связаны с именем спартанского полководца Лисандра. Он использовал шифр “Скитала”. Этот шифр известен со времен войны Спарты против Афин в V веке до н.э.

Достоинства - простота и отсутствие ошибок

Недостатки - легко взламывается

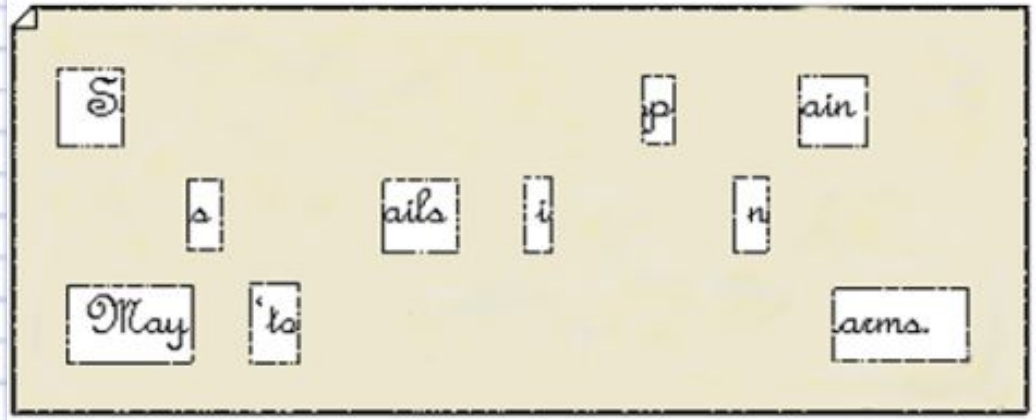
Диск Энея:



Небольшой диск с просверленными вдоль его края отверстиями.
Для того, чтобы зашифровать текст, - нить вдевали в эти отверстия так, чтобы нить свободно выходила.
Если гонца захватывали – он быстро выдёргивал нить, чтобы никто не догадался, что там было зашифровано.

Шифр Ришелье

Sir John regards you well and spekes again that
all as rightly 'vails him is yours now and ever.
May he 'tone for past d'lays with many charms.



Достоинства - легок в применении, расшифровка для злоумышленника — задача практически невыполнимая, зашифрованный текст не попадает под подозрение.

Недостатки - метод является медленным и требует наличия литературных навыков. Любой шифровальный аппарат может быть утерян, украден или конфискован.

Симпатические (невидимые) чер

Письмо, написанное симпатическими чернилами, не оставляет следов на бумаге. Чтобы прочитать такое послание, нужны нехитрые манипуляции (нагрев, освещение, химический проявитель и т. д.). В качестве чернил можно использовать молоко, яблочный и луковый соки, стиральный порошок, крахмал и т.д

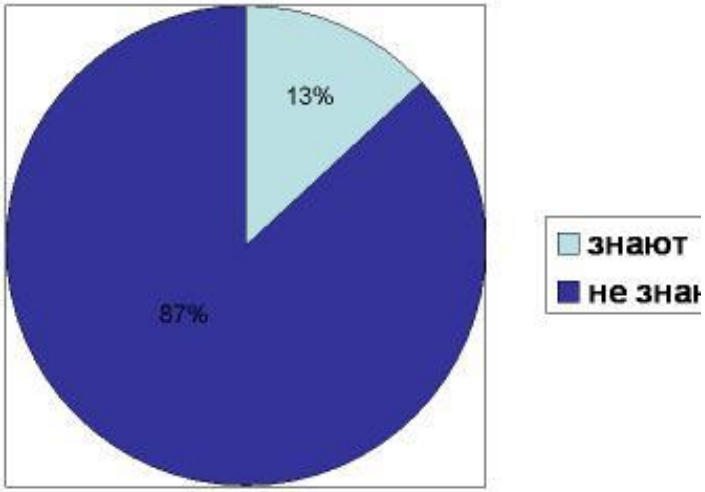
Исследовательская рабо

Метод исследования: анкетирование одноклассников.

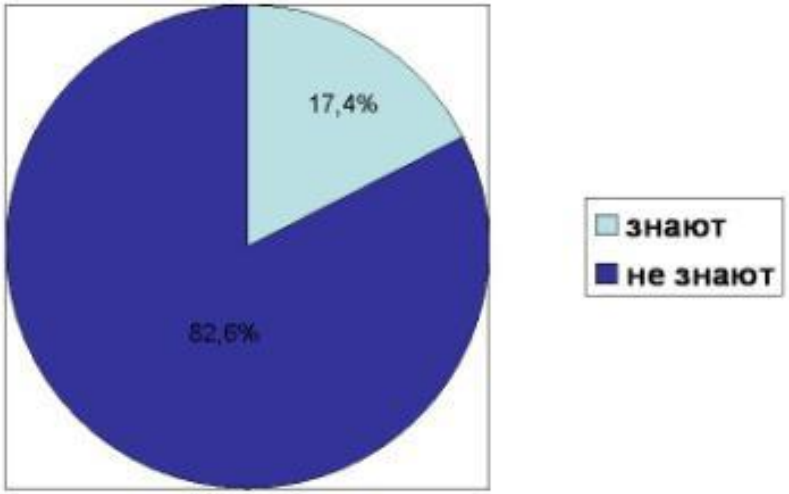
Участники анкетирования: учащиеся 6а класса МБОУ СОШ № 36 в количестве 25 человек.

Результаты опроса одноклассников:

Вопрос 1: Знаете ли вы, что такое шифр?

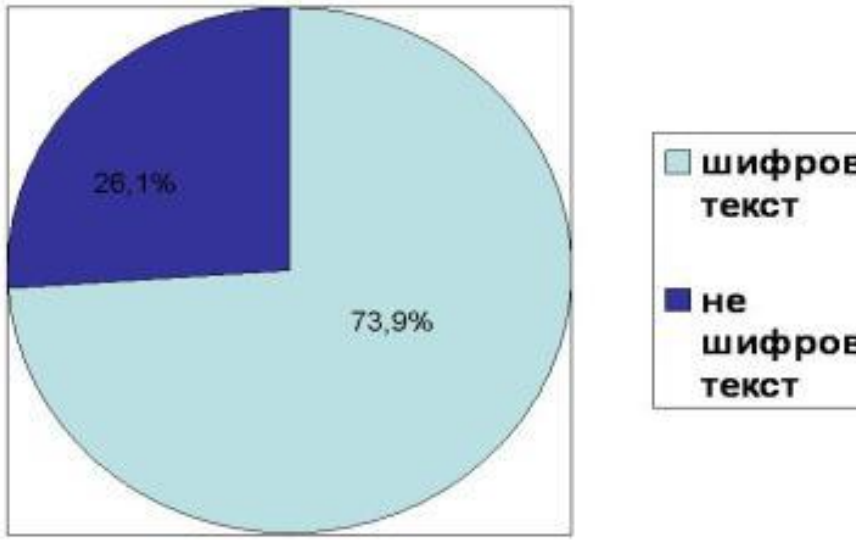


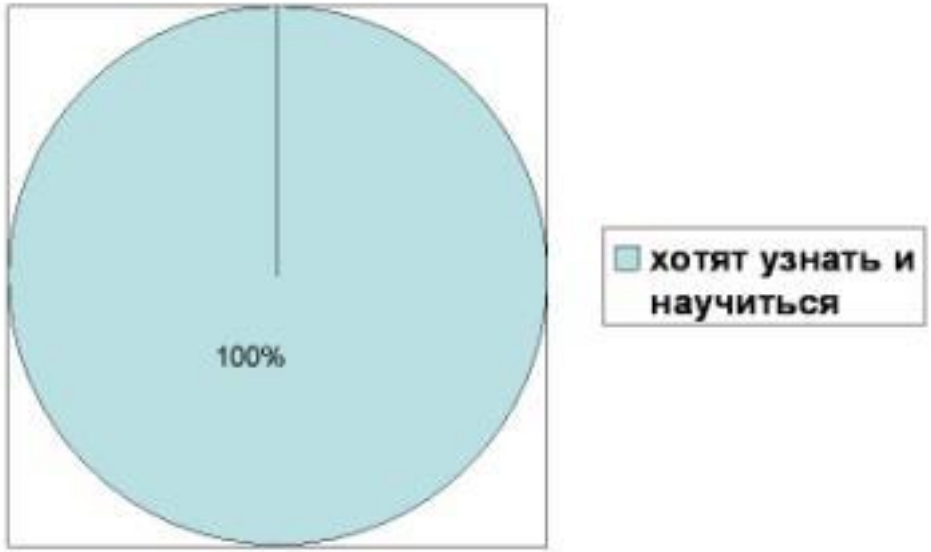
Вопрос 2: Знаете ли вы, что такое криптография?



Вопрос 3: Пробовали ли вы когда-нибудь зашифровать текст?

Вопросы 4 и 5: Хотелось ли узнать о разных методах шифрования и

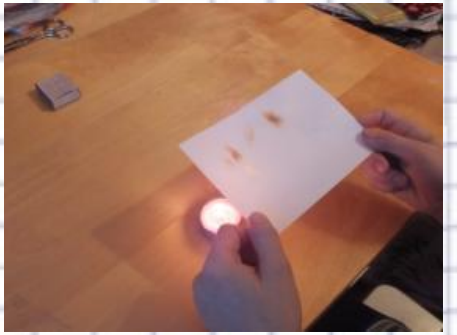




Результаты проведённых экспериментов:

Эксперимент № 1.

Цель: доказать, что написание секретного письма молоком и луковым соком **возможно**



Вывод: с помощью симпатических чернил (молока, лукового сока) можно написать секретное письмо и защитить важную информацию.

Эксперимент № 2.

Цель: зашифровать текст методом перестановки с помощью изготовленной сциталы и представить друзьям и родным ленту с зашифрованным текстом.

Вывод: данный метод перестановки прост в использовании и без специального прибора текст не прочитывается.

Эксперимент № 3.

Цель: зашифровать текст с помощью решетки Ришелье, представить его друзьям и родным.

Вывод: данный метод прост в использовании, но более медленный и без специальной шифр-решетки текст не прочитывается.

Эксперимент № 4.

Цель: разработать собственный шифр замены букв картинками.

Вывод: разработанный шифр прост и легко расшифровывается

Вывод:

Главным выводом всей моей работы стало то, что

С усложнением информационных технологий в человеческом обществе возникают новые задачи по защите информации, что требует развития новых методов в криптографии.

Спасибо за внимание!

Используемая литература:

1. «Мир математики», сборник

2. Интернет – ресурсы.