От древних способов шифрования до шифрования в современном мире

Выполнил: ученик 6 «А» класса
МБОУ СШ №74
Волков Артём
Преподаватель:
Третьякова Е.А

Цели и задачи:

- **Цель проекта:** изучить историю становления науки криптографии и ее практическую значимость.

- **Задачи проекта:**
- Изучить научную, учебную литературу по исследуемому предмету.
- Рассмотреть различные способы шифрования текстов.
- Показать практическую значимость криптографии от Древнего мира до настоящего времени.

Новизна

В ходе выполнения проекта пополнены свои знания о науке криптографии

Актуальность

Актуальностью проблем шифрования заключается в том, что всё больше и больше данных по всему миру хранятся на цифровых носителях. Кодирование используется и в повседневной жизни, и в специальных отраслях. Для реализации мер безопасности используются различные способы шифрования (криптографии).

ПИФАГОР

О числах первый начал рассуждать Пифагор.

Пифагор и его ученики сократили все числа до цифр от 1 до 9, так как считали их исходными, из которых могут быть получены все другие числа.

Учение Пифагора оказало огромное влияние не только на древнегреческую, но и всю европейскую культуру. Его исследование ПРОСТОГО ЧИСЛА, предвосхитило современную цифровизацию и появление искусственного интеллекта.

Простые числа

Простое число - это натуральное число,

у которого нет других делителей, кроме 1 и самого себя.

Среди натуральных чисел есть множество простых, остальные числа называются составными.

2	3	5	7	11	13	17	19
23	29	31	37	41	43	47	53
59	61	67	71	73	79	83	89
97	101	103	107	109	113	127	131
137	139	149	151	157	163	167	173
179	181	191	193	197	199	211	223
227	229	233	239	241	251	257	263
269	271	277	281	283	293	307	311
313	317	331	337	347	349	353	359
367	373	379	383	389	397	401	409
419	421	431	433	439	443	449	457
461	463	467	479	487	491	499	503
509	521	523	541	547	557	563	569
571	577	587	593	599	601	607	613
617	619	631	641	643	647	653	659
661	673	677	683	691	701	709	719
727	733	739	743	751	757	761	769
773	787	797	809	811	821	823	827
829	839	853	857	859	863	877	881
883	887	907	911	919	929	937	941
947	953	967	971	977	983	991	997

Простые числа в шифровании

А	М	И	Р	Г	Ф	Л	Ч	Е	Т	С	О	П	Н
29	2	3	5	41	83	31	37	19	17	13	11	7	23

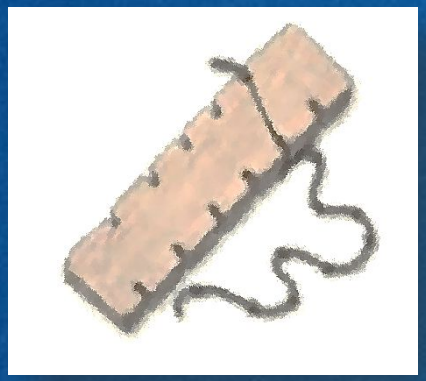
***Криптография** – это наука о способах преобразования (шифрования) информации с целью ее защиты.

***Шифрование** - преобразование информации в целях её защиты от неавторизованных лиц.

* **Кодирование** информации - процесс преобразования сигнала из формы, удобной для непосредственного использования информации, в форму, удобную для передачи, хранения или автоматической переработки.

***Кодировка –** это таблица, в которой описывается соответствие определённого символа и числа.

Древние способы шифрования



«Линейка Энея»

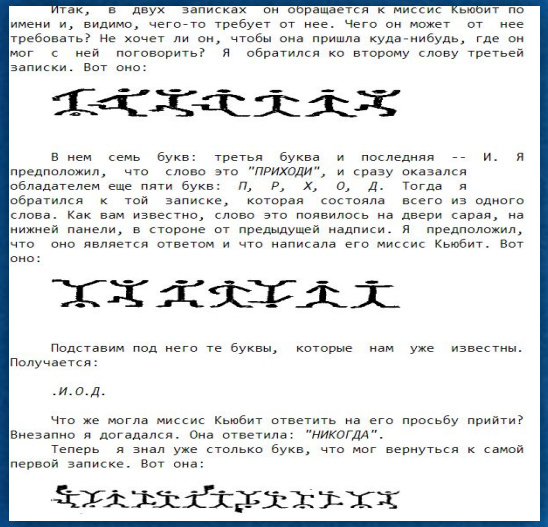
»Скитала»

«Узелковое письмо»

«Клинопись»

«Послание на голове»

Шифрование в книге Артура Конан Дойла



Итак, в двух записках он обращается к миссис Кьюбит по имени и, видимо, чего-то требует от нее. Чего он может от нее требовать? Не хочет ли он, чтобы она пришла куда-нибудь, где он мог с ней поговорить? Я обратился ко второму слову третьей записки. Вот оно:

В нем семь букв: третья буква и последняя -- И. Я предположил, что слово это *"ПРИХОДИ"*, и сразу оказался обладателем еще пяти букв: *П, Р, Х, О, Д*. Тогда я обратился к той записке, которая состояла всего из одного слова. Как вам известно, слово это появилось на двери сарая, на нижней панели, в стороне от предыдущей надписи. Я предположил, что оно является ответом и что написала его миссис Кьюбит. Вот оно:

Подставим под него те буквы, которые нам уже известны. Получается:

.И.О.Д.

Что же могла миссис Кьюбит ответить на его просьбу прийти? Внезапно я догадался. Она ответила: *"НИКОГДА"*.

Теперь я знал уже столько букв, что мог вернуться к самой первой записке. Вот она:

«Пляшущие человечки»

«Пляшущие человечки» — один из 56 рассказов английского писателя ***Артура Конан Дойла.***

В рассказе великий сыщик Шерлок Холмс разоблачает загадку таинственного шифра, состоящего из изображений пляшущих человечков.

Шифрование в Отечественную войну

«Энигма»

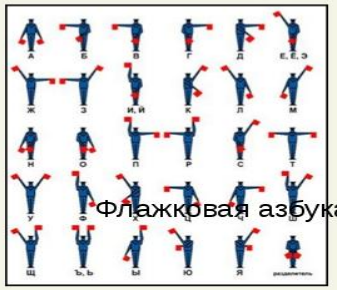
«М-209»

Во время Войны криптографией уже активно пользовались все страны-участницы. Однако самыми известными случаями применения являются американская шифровальная машина М-209 и семейство немецких электромеханических шифровальных машин «Энигма».

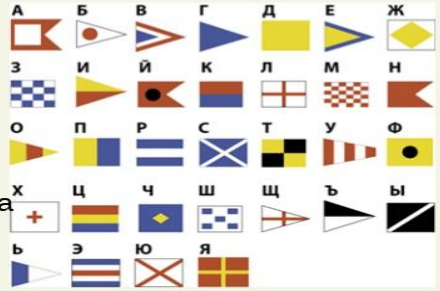
Кодировки в Военно-морском флоте

Разнообразие кодов

А а	.–	Р р	.–.
Б б	–...	С с	...
В в	.––	Т т	–
Г г	––.	У у	..–
Д д	–..	Ф ф	..–.
Е е	.	Х х	....
Ё ё	.	Ц ц	–.–.
Ж ж	...–	Ч ч	–––.
З з	––..	Ш ш	––––
И и	..	Щ щ	––.–
Й й	.–––	Ъ ъ	–..–
К к	–.–	Ы ы	–.––
Л л	.–..	Ь ь	–..–
М м	––	Э э	..–..
Н н	–.	Ю ю	..––
О о	–––	Я я	.–.–
П п	.––.		



Флажковая азбука



Азбука Морзе | Семафорная азбука | Флажковая азбука

В зависимости от среды распространения сигнала и принципов устройств аппаратуры, в ВМФ используются различные рода связи.

Средства и методы шифрования в ФНПЦ АО «МАРС»

В ФНПЦ АО «МАРС» применяются различные средства и методы шифрования в целях:
- преобразования информации ограниченного доступа для передачи её по каналам связи.

-разработки генераторов(датчиков) псевдослучайных чисел для формирования устойчивых паролей пользователей.

- применения хеш-функций для хранения в АС информации ограниченного доступа.

ФНПЦ АО «НПО «МАРС»

Шифрование в современном мире

В современном мире криптография находит множество различных применений. Кроме очевидных — собственно, для передачи информации, она используется в сотовой связи, платном цифровом телевидении при подключении к Wi-Fi и на транспорте для защиты билетов от подделок, и в банковских операциях, и даже для защиты электронной почты от спама.

ЗАКЛЮЧЕНИЕ

В процессе работы мои знания пополнены историей развития криптографии множеством различных способов шифрования информации.

Шифрование информации – это то, без чего не может жить большинство современных людей, хотя и многие не знают об этом. Данная тема не только крайне интересна для изучения, но и актуальна в современном мире.

Приложения

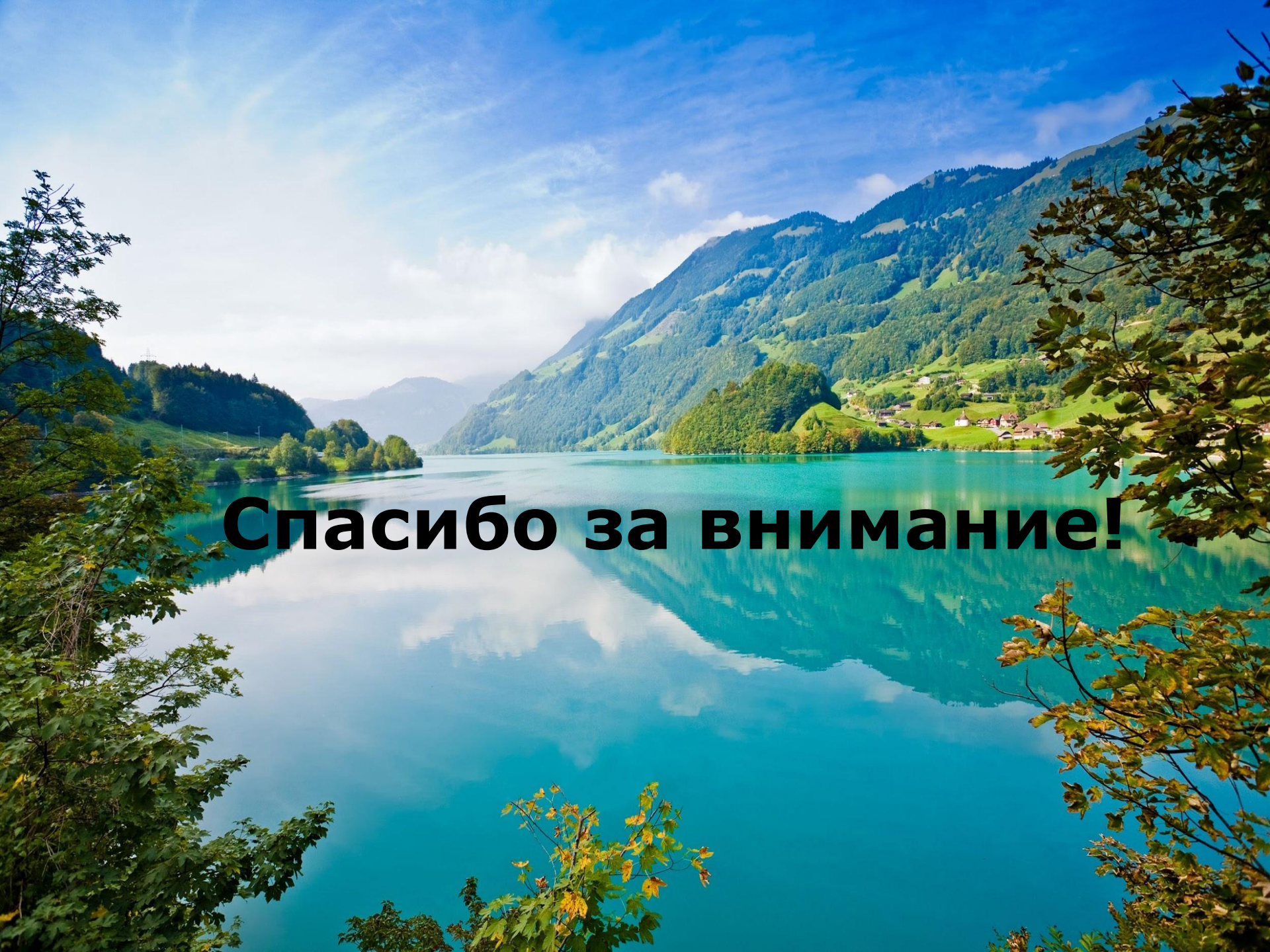
Список используемых сайтов:

1.https://yandex.ru/images/search?text=шифр&noreask=1&lr=240

2.https://www.yandex.ru/search/?text=криптограмма%20что%20это%20такое&lr=240&clid=9582

3.https://ru.wikipedia.org/wiki/Шифр

4.https://yandex.ru/images/search?text=что%20такое%20криптограмма&noreask=1&lr=240


Спасибо за внимание!