Тайные знаки

Наши цели:

- **Основополагающий вопрос**
- *Зачем человеку нужны тайны?*
- **Проблемные вопросы учебной темы**
- 1. Когда нужно защищать информацию?
- 2. Зачем нужно защищать информацию?
- 3. Возможен ли абсолютно стойкий шифр?

Гипотеза:

- Без тайн не может быть не только государства, но даже малой общности людей - без них нельзя выиграть сражение или выгодно продать товар, одолеть своих политических противников в жесткой борьбе за власть или сохранить первенство в технологии.

Мы предполагали

- В ходе эволюции человек учился защищаться от холода, голода, диких зверей и капризов погоды. На каком-то из этапов своего развития он понял важность своевременного получения достоверной и правильно отобранной информации. И, наконец, осознал необходимость информацию эту защищать.
- Защищая свою информацию, мы стремимся сохранить в тайне имеющийся у нас запас знаний

Что мы делали:

- рассмотреть основные понятия криптографии;
- показать некоторые связи между математикой и криптографией;
- поделиться полученными в процессе исследования знаниями с учащимися школы;
- оформить результаты своих исследований с помощью ИКТ (презентация, буклет, вики-статья)

Информация, которая нуждается в защите, возникает в самых разных жизненных ситуациях. Обычно в таких случаях говорят, что информация содержит тайну или является защищаемой, приватной, конфиденциальной, секретной. Для наиболее типичных, часто встречающихся ситуаций такого типа введены даже специальные понятия:

- государственная тайна;
- военная тайна;
- коммерческая тайна;
- юридическая тайна;
- врачебная тайна и т.д.

Когда же надо защищать информацию?

- В тех случаях, когда есть опасения, что информация станет доступной посторонним, которые могут обратить её во вред законному пользователю.
- Чтобы предотвратить возможный вред от её разглашения.

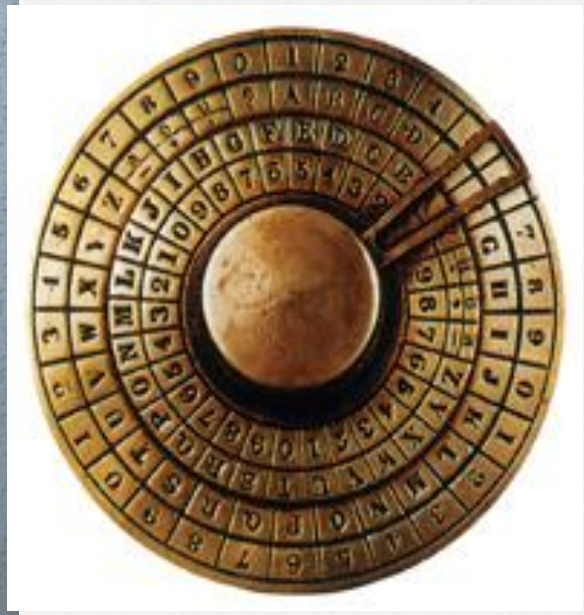
Тайнопись

- О важности сохранения информации в тайне знали уже в древние времена, когда с появлением письменности появилась и опасность прочтения ее нежелательными лицами.
- Криптография - слово греческое и в переводе означает "тайнопись". По утверждению ряда специалистов криптография по возрасту - ровесник египетских пирамид. В документах древних цивилизаций - Индии, Египта, Месопотамии - есть сведения о системах и способах составления шифрованных писем.

Криптограмма – тайный код

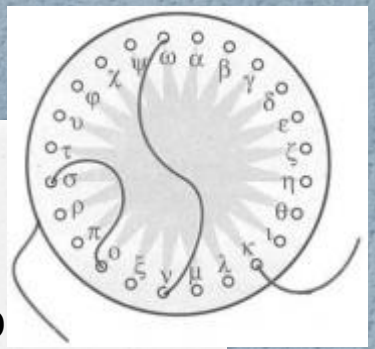
- Основные понятия криптографии - шифр (от арабского "цифра"; арабы первыми стали заменять буквы на цифры с целью защиты исходного текста). Секретный элемент шифра, недоступный посторонним, называется ключом шифра. Как правило, в древние времена использовались так называемые шифры замены и шифры перестановки.

Шифр Цезаря



Историческим примером шифра замены является шифр Цезаря (1 век до н.э.), описанный историком Древнего Рима Светонием. Гай Юлий Цезарь использовал в своей переписке шифр собственного изобретения. Применительно к современному русскому языку он состоял в следующем. Выписывался алфавит: А, Б, В, Г, Д, Е,...,; затем под ним выписывался тот же алфавит, но со сдвигом на 3 буквы влево.

Диск Энея



- Древнегреческий полководец Эней Тактика в IV веке до н.э предложил устройство, названное впоследствии "диском Энея".
- На диске диаметром 10-15 см и толщиной 1-2 см высверливались отверстия по числу букв алфавита. В центре диска помещалась "катушка" с намотанной на ней ниткой достаточной длины.
- При зашифровании нитка "вытягивалась" с катушки и последовательно протягивалась через отверстия, в соответствии с буквами шифруемого текста. Диск и являлся посланием. Получатель послания последовательно вытягивал нитку из отверстий, что позволяло ему получать передаваемое сообщение, но в обратном порядке следования букв. При перехвате диска недоброжелатель имел возможность прочитать сообщение тем же образом, что и получатель. Но Эней предусмотрел возможность легкого уничтожения передаваемого сообщения при угрозе захвата диска. Для этого было достаточно выдернуть "катушку" с закрепленным на ней концом нити до полного выхода всей нити из всех отверстий диска.

Сцитала

- Одним из первых приборов, реализующих шифр перестановки, является так называемый прибор СЦИТАЛЛА (или скитала). Он был изобретен в древней "варварской" Спарте во времена Ликурга; Рим быстро воспользовался этим прибором. Для зашифрования текста использовался цилиндр заранее обусловленного диаметра. На цилиндр наматывался тонкий ремень из пергамента, и текст выписывался построчно по образующей цилиндра (вдоль его оси). Затем ремень сматывался и отправлялся - получателю сообщения. Последний наматывал его на цилиндр того же диаметра и читал текст по оси цилиндра. В этом примере ключом такого шифра являлся диаметр цилиндра и его длина, которые, по существу, порождают двухстрочную запись, указанную выше.
- Античные греки и спартанцы в частности, использовали этот шифр для связи во время военных кампаний.

Шифр Полибия

- Еще одно изобретение древних греков - так называемый квадрат Полибия. Применительно к современному латинскому алфавиту из 26 букв шифрование по этому квадрату заключалось в следующем. В квадрат размером 5x6 клеток выписываются все буквы алфавита, при этом буквы I,J не различаются (J отождествляется с буквой I);
- Шифруемая буква заменялась на координаты квадрата, в котором она записана. Так, B заменялась на AB, F на BA, R на DB и т.д. При расшифровании каждая такая пара определяла соответствующую букву сообщения. Ключом такого шифра являлось расположение букв в таблице 5x5.

A	B	C	D	E	
A	A	B	C	D	E
D	F	G	H	I	K
C	L	M	N	O	P
D	Q	R	S	T	U
E	V	W	X	Y	Z

«Узелковое письмо»

«Узелковое письмо" получило распространение у индейцев Центральной Америки. Свои сообщения они передавали в виде нитки, на которой завязывались разноцветные узелки, определявшие содержание сообщения.

«Узелковое письмо»

- Узелковое письмо— разновидность письменности, использующая в качестве носителя информации нити (шнуры), а для её кодирования — узлы, а также цвета нитей.
- Кипу— «узел», «завязывать узлы», «счёт — древняя мнемоническая и счётная система инков и их предшественников в Андах, своеобразная письменность: представляет собой сложные верёвочные сплетения и узелки, изготовленные из шерсти южноамериканских верблюдовых (альпаки и ламы) либо из хлопка. В кипу может быть от нескольких свисающих нитей до 2000. Она использовалась для передачи сообщений посыльными часки по специально проложенным имперским дорогам, а также в самых разных аспектах общественной жизни (в качестве календаря, топографической системы, для фиксации налогов и законов, и др.). Один из испанских хронистов (Хосе де Акоста) — писал, что «вся империя инков управлялась посредством кипу»[5] и никто не мог избежать тех, кто проводил подсчёты с помощью узлов[6].

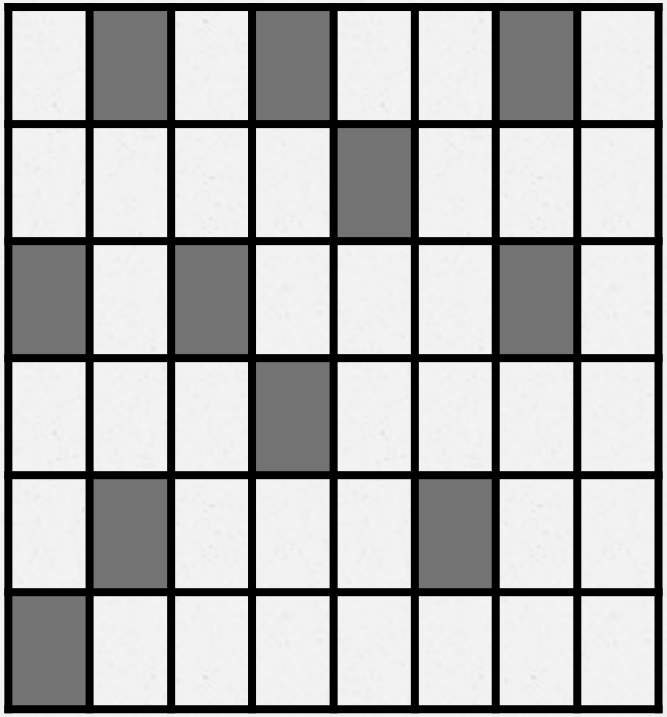
"Тайна головы раба"

- Известно, например, что в Древней Греции голову раба брили, писали на его голове, ждали, когда волосы вновь вырастут, после чего отправляли с поручением к адресату. Что и говорить, время было такое — расстояния большие, скорости малые, плюс-минус два месяца роли не играли.
- Знатокам поэзии хорошо известен такой довольно широко используемый в то время прием тайнописи, как акростих, в котором скрываемое сообщение образуют начальные буквы стихотворных строк

Способ «решётки»

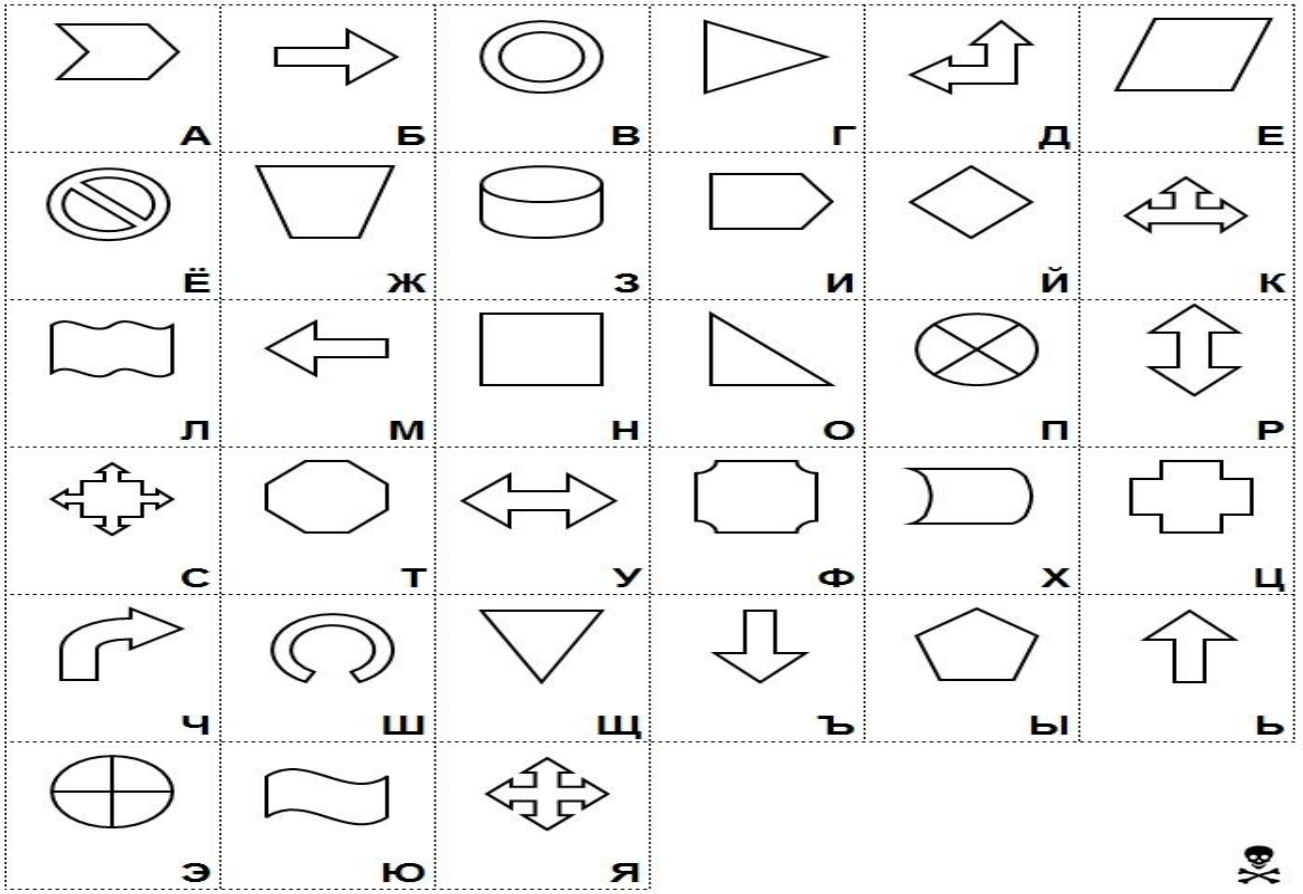
- Одним из способов ведения секретной переписки является, так называемый способ «решётки». Его придумал Джироламо Кардано, известный римский математик.
- Желающие вести тайную переписку по этому способу готовят решётку, то есть бумажный квадрат с прорезанными окошечками. Окошечки размещены не произвольно, а в определенном порядке. Адресат наложит свою решётку на текст, сможет в этих окошках прочитать текст.

Шифр Кардано



у	л	д	ё	я	о	д	н
ы	г	б	в	т	р	о	а
р	т	о	у	ч	ь	н	з
п	к	и	у	а	а	т	р
х	л	а	а	е	с	д	б
я	а	в	о	к	п	г	е

Тайнопись пиратов



Шифры в литературе

В художественной литературе классическим примером шифра замены является известный шифр "Пляшущие человечки" (К. Дойля). В нем буквы текста заменялись на символические фигурки людей. Ключом такого шифра являлись позы человечков, заменяющих буквы...

Самые важные составляющие любого шифра :

- общее правило, по которому преобразуется исходный текст (алгоритм шифра);
- конкретная особенность именно этой серии шифрованных сообщений (так называемый ключ).

Теперь мы знаем:

- ТАЙНОПИСЬ или КРИПТОГРАФИЯ - специальная система изменения обычного письма, понятная только узкому кругу посвященных лиц.
- Криптография обеспечивает сокрытие смысла сообщения с помощью шифрования и открытие его дешифрованием, которые выполняются по специальным криптографическим алгоритмам с помощью ключей у отправителя и получателя.
- **Когда же надо защищать информацию?** В тех случаях, когда есть опасения, что информация станет доступной посторонним, которые могут обратить её во вред законному пользователю.
- **Зачем необходима защита информации?** Чтобы предотвратить возможный вред от её разглашения.

Источники которые мы использовали:

- Зелинский Ф. Сказочная древность Эллады. М., 1993.
- Жельников В. Криптография от папируса до компьютера. М., 1996.
- Горбовский А. Загадки древнейшей истории М., 1971.
- Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В. Основы криптографии. Учебное пособие. М., Гелиос АРВ, 2005, 327 с.
- Бабаш А.В., Шанкин Г.П. История криптографии. Часть I. М.: Гелиос, 2002, 239 с..
- Молдовян Н.А., Советов Б.Я.. Криптография. М., Лань, 2001, 329 с.
- http://ru.wikipedia.org/wiki/Древнерусские_тайнописи
- http://potomy.ru/school/2775.html

Спасибо за внимание!