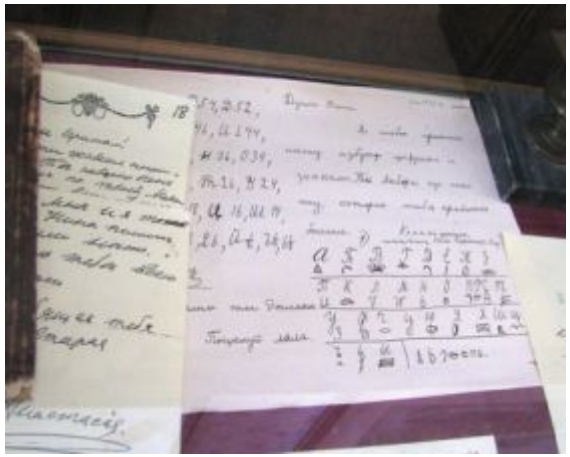
БОЛЬШОЙ СЕКРЕТ ДЛЯ МАЛЕНЬКОЙ КОМПАНИИ

В НАЧАЛЕ БЫЛО СЛОВО…

В начале было Слово… Потом появилось много слов. И очень скоро человек понял, что слова надо прятать. Так началось зарождение криптографии. В переводе с древнегреческого «криптография» означает «тайнопись».



5 мая 1921 года постановлением Совета народных комиссаров РСФСР была создана Криптографическая служба, которая должна была обеспечивать защиту информации. Этим она занимается и по сей день, причем не просто в информационно-телекоммуникационных системах и системах специальной связи в России и в зарубежных учреждениях РФ, но и в системах, которые используют современные информационные технологии.

КАКИЕ СЕКРЕТЫ И ТАЙНЫ ЗАЩИЩАЕТ ЧЕЛОВЕЧЕСТВО?

Не стоит думать, что шифровки возникли только тогда, когда возникла письменность.

Что такое запутывание следов животным, как не методика шифровки? Так что первые шифровки появились на свет вместе с человечеством. А вот расцветать искусство шифрования начало с появлением политики, науки и особенно – племенных, а впоследствии государственных границ.

Шифровалось все: рецепты лекарей, сообщения разведслужб, технические и научные достижения, письма влюбленных, деловая переписка, бухгалтерские книги… Нет той области человеческой деятельности, которую не затронуло бы шифрование.

КАКИЕ СЕКРЕТЫ И ТАЙНЫ ЗАЩИЩАЕТ ЧЕЛОВЕЧЕСТВО?

- Об искусстве шифровки и дешифровки написаны тома. Шифрованием и дешифрованием занимаются талантливые программисты и математики, люди, обладающие широчайшим кругозором – ведь никогда заранее не известно, что именно будет использовано в шифре, какой ключ поможет его взломать (иногда может оказаться, что это – редкая порода кошек, а в иных случаях поможет только знание классической литературы).

ВИДЫ ШИФРОВ

Лозунговый шифр

В данном шифре запоминание ключа основано на лозунге – легко запоминающемся слове или фразе. Например, лозунг – слово «заявление». Заполняем вторую строку таблицы по следующему правилу: сначала вписывается слово-лозунг, причем повторяющиеся буквы отбрасываются, затем эта таблица дополняется не вошедшими в нее буквами алфавита.

Ключ будет иметь вид:

А	Б	В	Г	Д	Е	Ж	З	И	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я
З	А	Я	В	Л	Е	Н	И	Б	Г	Д	Ж	К	М	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	

ВИДЫ ШИФРОВ

Магический квадрат

Магическими квадратами называются квадратные таблицы со вписанными в их клетки последовательными натуральными числами от 1, которые дают в сумме по каждому столбцу, каждой строке и каждой диагонали одно и то же число. Подобные квадраты широко применялись для вписывания шифруемого текста по приведенной в них нумерации.

Считалось, что созданные с их помощью шифровки охраняет не только ключ, но и магическая сила.

16	3	2	13
5	10	11	8
9	6	7	12
4	15	14	1

О	И	Р	М
Е	О	С	Ю
В	Т	А	Ь
Л	Г	О	П

ОИРМЕОСЮВТАЬЛГОП

Шифрованный текст: ПРИЛЕТАЮ ВОСЬМОГО

ВИДЫ ШИФРОВ

Шифр Атбаш

Некоторые фрагменты библейских текстов зашифрованы с помощью шифра, который назывался Атбаш. Правило зашифрования состояло в замене i-й буквы алфавита буквой с номером n – i + 1, где **n** - число букв в алфавите (значит, первая буква заменяется последней, вторая – предпоследней и т.д.)

Тарабарская грамота

Способ шифровки следующий. Все согласные буквы русской азбуки записываются в две строки; одна половина букв вверху, другая половина - внизу, причем в обратном порядке (одна буква под другой).

Б В Г Д Ж З К Л М Н

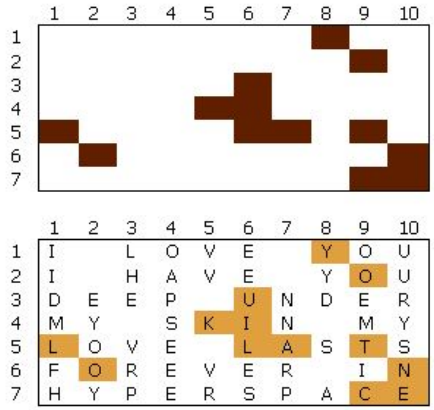
Щ Ш Ч Ц Х Ф Т С Р П

При зашифровке слов согласные взаимно заменяются, а остальные буквы и символы остаются на своих местах без изменения.

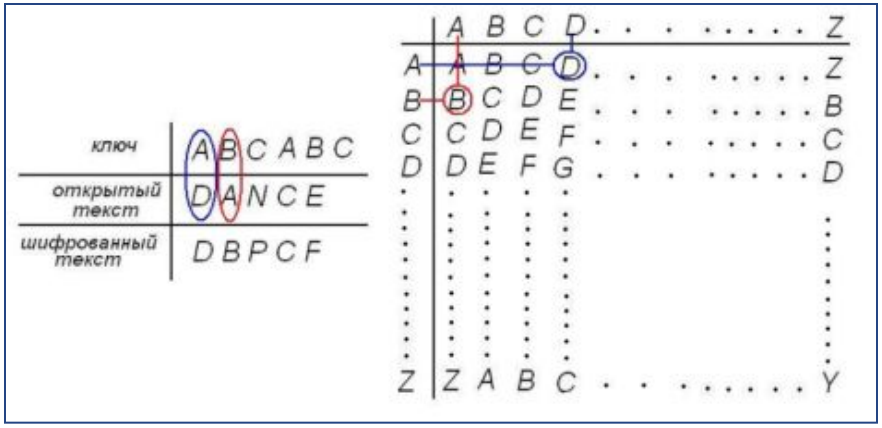
ВИДЫ ШИФРОВ

Хотите разобраться в классификации шифров, их применении и истории создания?

Выбирайте проект «Виды шифров»



	1	2	3	4	5	6	7	8	9	10
1	I		L	O	V	E		Y	O	U
2	I		H	A	V	E		Y	O	U
3	D	E	E	P		U	N	D	E	R
4	M	Y		S	K	I	N		M	Y
5	L	O	V	E		L	A	S	T	S
6	F	O	R	E	V	E	R		I	N
7	H	Y	P	E	R	S	P	A	C	E



КАК СОХРАНИТЬ И ЗАЩИТИТЬ ИНФОРМАЦИЮ?

Разработкой мер защиты информации занимаются КРИПТОГРАФИЯ И СТЕГАНОГРАФИЯ.

В ближайшем будущем криптография станет "третьей грамотностью" наравне со "второй грамотностью" - владением компьютером и информационными технологиями.

Какую сторону защиты информации изучает каждая из этих наук?
Какова история их развития?
Заинтересовались? Тогда предлагаю проект «Криптография от папируса до компьютера»

ЗНАМЕНИТЫЕ ЛИЧНОСТИ И КРИПТОГРАФИЯ

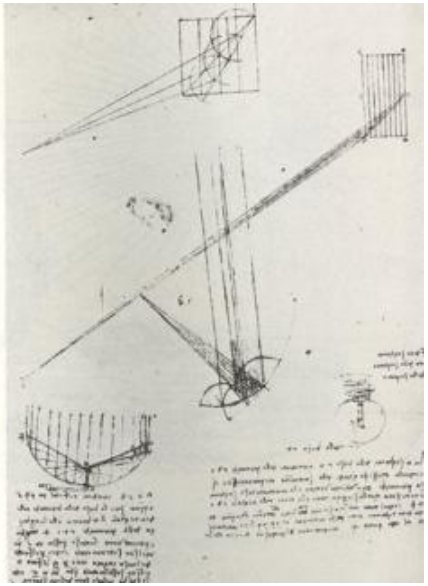
Свой след в истории криптографии оставили многие хорошо известные исторические личности, в том числе кардинал Ришелье, Леонардо да Винчи, король Генрих IV, Петр I, Наполеон, А.С.Пушкин. Зашифровывать свои мысли Пушкин начал давно, но наиболее преуспел в этом деле, когда стремился скрыть информацию о декабристском движении. Какими только приемами он при этом не пользовался! Это могли быть буквы и точки, даты, рисунки, изменение порядка в размещении строк стихотворения… Но оказывается, все это было так, пробой пера, накоплением опыта в построении такой системы шифра, которая отвечала бы его целям:

- Донести до потомков информацию о декабристском движении, которая не была известна Следственной комиссии.
- Не навредить современникам.
- Не дать им (современникам) навредить его собственным идеям.

Этот замысел ему удался. Созданная им шифрограмма оставалась неразгаданной 163 года… Речь идет о романе "Дубровский".

ЗНАМЕНИТЫЕ ЛИЧНОСТИ И КРИПТОГРАФИЯ

Леонардо да Винчи многое шифровал, чтобы его идеи раскрывались постепенно, по мере того, как человечество до них "дозреет". Изобретатель писал левой рукой и невероятно мелкими буковками, да еще и справа налево. Но и этого мало - он все буквы переворачивал в зеркальном изображении.



Он говорил загадками, сыпал метафорическими пророчествами, обожал составлять ребусы. Леонардо не подписывал своих произведений, но на них есть опознавательные знаки. Например, если вглядываться в картины, можно обнаружить символическую взлетающую птицу. Таких знаков, видимо, немало, поэтому те или иные его детища вдруг обнаруживаются через века.

ЗНАМЕНИТЫЕ ЛИЧНОСТИ И КРИПТОГРАФИЯ

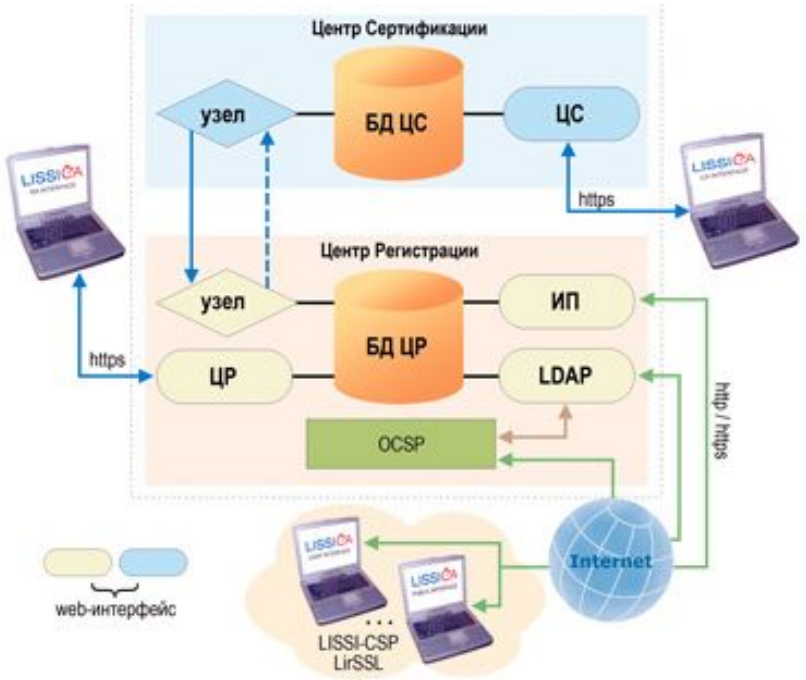
Если вы хотите раскрыть тайну шифра исторических личностей и знаменитых людей, вам нужно работать над темой ***«Знаменитые личности и криптография»***

ЭЛЕКТРОННАЯ ЦИФРОВАЯ ПОДПИСЬ, ИЛИ АЛГОРИТМ ЭЛЬ-ГАМАЛЯ

В настоящее время, редкая организация не использует компьютер при работе с документами. Информационные технологии активно применяются при организации делопроизводства, почти все документы подготавливаются в электронном виде. Электронный документ тоже требует защиты. Для подтверждения авторства и неизменности информации того или иного электронного документа применяется **электронная цифровая подпись**.

ЭЛЕКТРОННАЯ ЦИФРОВАЯ ПОДПИСЬ, ИЛИ АЛГОРИТМ ЭЛЬ-ГАМАЛЯ

Если вы хотите узнать, какой шифр лежит в основе стандартов электронной цифровой подписи в США и России, то вам следует выбрать проект «*Электронная цифровая подпись, или алгоритм Эль-Гамаля*»



РАЗГАДАННАЯ "ЗАГАДКА", ИЛИ ШИФРЫ И КОДЫ ВТОРОЙ МИРОВОЙ ВОЙНЫ

- Наша героиня впервые явила миру свои лик в Германии в 1923 году. О чем идет речь? О *шифровально-дешифровальной машине «Энигма»*. Первоначально "Загадку" (а именно так переводится слово "Энигма") использовали в коммерческих целях, для сохранения тайны деловой переписки, однако позднее ею заинтересовалось германское командование и ее усовершенствованные модели поступили в войска.

РАЗГАДАННАЯ "ЗАГАДКА", ИЛИ ШИФРЫ И КОДЫ ВТОРОЙ МИРОВОЙ ВОЙНЫ

Как технически осуществлялся процесс шифровки-дешифровки информации с помощью Энигмы? Кому удалось разгадать ее загадку?

Разведки всего мира очень неохотно раскрывают свои тайны, даже если они относятся к давно прошедшим временам. Данные факты относятся к периоду второй мировой войны, но вплоть до 70-х годов их покрывала завеса тайны, а многие подробности стали известны лишь спустя полвека после окончания войны. Эти события - одна из ярчайших страниц в истории вычислительной техники.

Если вас заинтересовала эта тема, предлагаю вам проект «Разгаданная «Загадка», или шифры и коды II мировой войны»

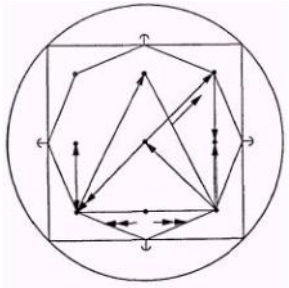
СУЩЕСТВУЕТ ЛИ БИБЛЕЙСКИЙ КОД?

- Даже в Библии можно найти примеры шифровок, хотя мало кто это замечает. Исаак Ньютон видел в Библии шифровку, и поиски кода, который позволил бы ее прочесть, считал более важной работой, чем создание своей теории Вселенной. Он изучил древнееврейский язык и полжизни потратил на поиски ключа к библейскому шифру.

Великий физик был уверен: в Библии скрыты пророчества о человеческой истории. Ньютон верил, что Библия наравне с устройством Вселенной есть "криптограмма Всевышнего", и он хотел разгадать Его загадку и узнать предопределенное.

Так ли это? Если желаете разобраться, выбирайте проект «Существует ли библейский код?»

МАГИЯ ЧИСЕЛ



- Среди множества тайн мироздания умы людей с давних времен занимает **магия чисел** и их влияние на судьбу человека. **Числа** сопровождают человека с момента рождения и до самой смерти. Существуют ли **магические числа** , которые определяют судьбу каждого человека? И вообще, какую роль играет **магия чисел в нашей жизни** ?

- Люди издавна боятся и преклоняются перед магическими числами.

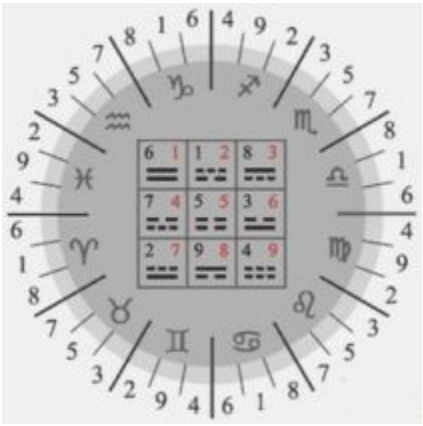
  Например, **число** 12 – олицетворяет божественную гармонию, а в противовес ему – **число** 13 или «чертова дюжина», вызывает суеверный ужас и трепет. **Магия** связывает **число** 666 с дьяволом, а 7 – с везением и удачей.

НУМЕРОЛОГИЧЕСКИЙ КОД

- Разгадать **магию чисел** человечество стремилось с давних времен. Еще в древнем мире наука о **числах** – нумерология, являлась достоянием «просвещенных»: магов и жрецов. В Древней Греции изучением значения **чисел** в судьбе человека занимался Пифагор. Согласно его теории человеческая душа - бессмертна, и проходит череду последовательных перевоплощений. А все окружающие нас предметы по существу - **числа**.
- Одним из **магических чисел**, определяющих основные черты характера человека и предопределяющих его дальнейшую судьбу, является **число** даты рождения.

- Нумерология также позволяет найти магическую связь между **именем человека** и его числом. Определив, какое число соответствует имени человека, можно узнать о его сокровенных интересах, движущих мотивах его поведения, тайных желаниях и устремлениях.
- Есть ли связь между событиями и их датами?

НУМЕРОЛОГИЧЕСКИЙ КОД



Заинтересовались?

Тогда включайтесь в разработку проекта

«Нумерологический код»

ТЕМЫ ПРОЕКТОВ

- *Криптография от папируса до компьютера*
- *Виды шифров*
- *Знаменитые личности и криптография*
- *Электронная цифровая подпись, или алгоритм Эль-Гамаля*
- *Разгаданная «Загадка», или шифры и коды II мировой войны*
- *Существует ли библейский код?*
- *Нумерологический код*