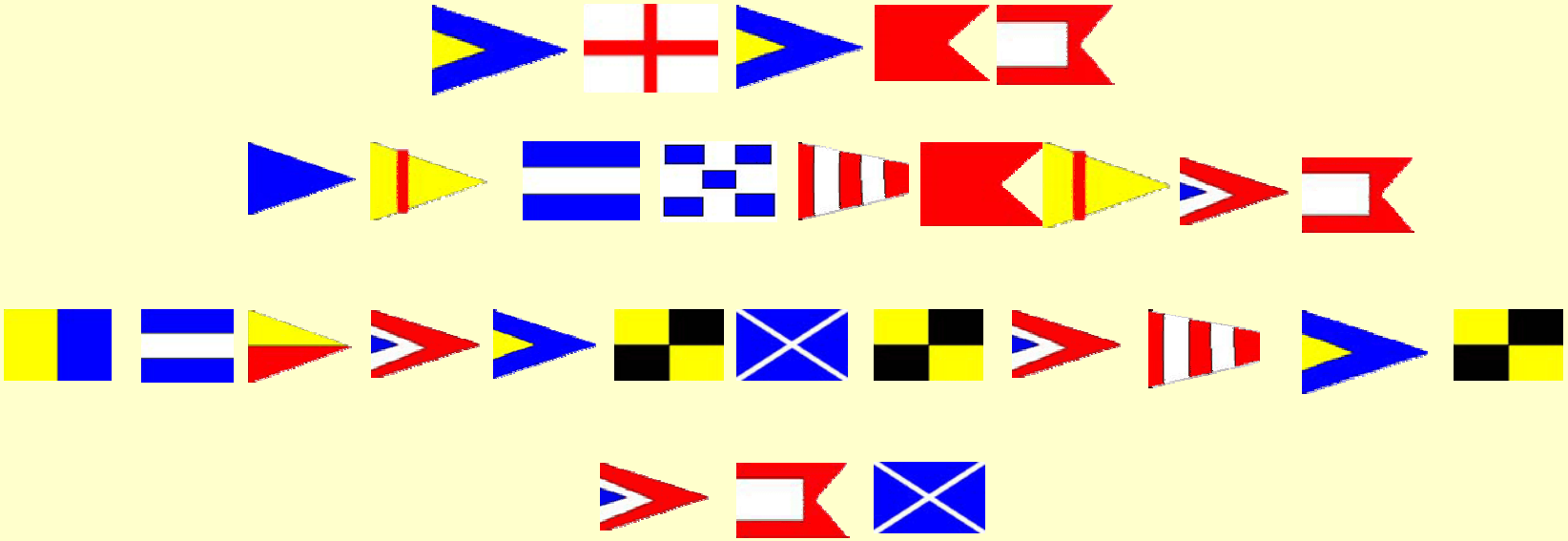
Проектная работа
по теме:

Шифры и криптография

Автор: **Горшунова Елена** ученица 7А класса
ГОУ СОШ № 1000 ЗОУО ДО г. Москвы
Руководитель: **Полункина Светлана Николаевна**
учитель математики



ЕЛЕНА ГОРШУНОВА ПРИВЕТСТВУЕТ ВАС

Содержание

Введение. План работы
Криптография: что такое и зачем
История криптографии. Из глубины веков до наших дней
Криптография древнего мира
Средневековый прорыв криптографической науки
Криптология нового времени
Та самая «Энигма»
Сегодняшний день. Что дальше?
Использование частотного анализа для взлома шифров
Мои шифры

Введение

- Человек много тысячелетий живет в обществе себе подобных. Одной из важнейших его способностей является умение общаться с другими людьми - передавать им сведения о том, что происходит в окружающем их мире и о фактах реальности. С зарождением человеческой цивилизации возникло умение сообщать информацию одним людям так, чтобы она не становилась известной другим.
- В своей работе я ставлю цель изучить различные тайные способы передачи информации, а также разработать свой собственный способ передачи информации, т.е. шифр.

План работы

1. Изучить литературу по теме: «История развития криптографии».

2. Привести примеры известных шифров.

3. Разработать свой шифр. Показать его использование.

Криптография: что такое и зачем

В переводе с греческого «**криптография**» означает «**тайнопись**». Если коротко, то криптография - раздел математики, изучающий способы шифрования сообщений, то есть преобразования осмысленного текста в бессмысленный набор символов (криптограмму). Указанное преобразование осуществляется по специальному алгоритму с использованием некоторого ключа. Для того, чтобы расшифровать криптограмму, надо знать этот ключ. Способы расшифровки криптограмм без знания ключа (взлома шифра) изучает **криптоанализ.**

Зачем нужна криптография? Испокон веков не было ценности большей, чем информация. А ценности надо беречь и не допускать попадания их в руки злоумышленников. Поэтому с распространением компьютеров в деловой сфере, с развитием систем передачи данных и Интернета очень актуальной становится проблема защиты информации от несанкционированного доступа (НСД). Испытанным же методом защиты информации от НСД является ее шифрование.

Кому нужна криптография? Во-первых, людям. Мы обычно рады получить письмо от знакомых, но бываем не в восторге заметив, что с его содержимым кто-то ознакомился. Во-вторых, государству. Военным необходимо тайно сообщать о своих маневрах, ученым – сохранять данные исследований, банкирам – для защиты от финансовых махинаций, правительству – для сохранности стратегически важной для страны информации.

История криптографии. Из глубины веков до наших дней

Способы защиты информации

О важности сохранения информации в тайне знали уже в древние времена, когда с появлением письменности появилась и опасность прочтения ее нежелательными лицами. Существовали три основных способа защиты информации:

- **Один** из них предполагал защиту ее чисто силовыми методами: секретный документ охранялся физическими лицами, а для его передачи использовали специальных курьеров.
- **Второй** способ получил название **«стеганография»** (латино-греческое сочетание слов, означающих, в совокупности, «тайнопись»). Он заключался в сокрытии самого факта наличия информации. При использовании так называемых симпатических чернил текст становился видимым после соответствующего «проявления» бумаги. Пример сокрытия информации приведен в трудах древнегреческого историка Геродота. На голове раба, которая брилась наголо, записывалось нужное сообщение. И когда волосы его достаточно отрастали, раба отправляли к адресату, который снова брил его голову и считывал полученное сообщение.

- **Третий** способ защиты информации был криптографическим. Криптография - ровесница египетских пирамид. В документах древних цивилизаций - Индии, Египта, Месопотамии - есть сведения о способах составления шифрованных писем. Один из самых старых шифрованных текстов из Месопотамии представляет собой табличку, написанную клинописью и содержащую рецепт изготовления глазури для гончарных изделий. Для написания его были использованы редко употребляемые клинописные знаки, игнорировались некоторые гласные и согласные и употреблялись числа вместо имен. Шифрованные тексты Древнего Египта - это чаще всего религиозные тексты и медицинские рецепты. Совершенно отсутствуют сведения об использовании шифров в Древнем Китае, что объясняется, по-видимому, сложностью самих иероглифов. Наиболее полные и достоверные сведения о шифрах относятся к Древней Греции.

Основное понятие криптографии - **шифр** - происходит от арабского «цифра». Арабы первыми стали заменять буквы на цифры с целью защиты исходного текста. **Шифрование** является преобразованием сообщения по определенным правилам, что делает его бессмысленным набором знаков для непосвященного в тайну шифра человека.

Скрытые сообщения. Тайнопись

Данные о первых способах тайнописи весьма обрывочны. Предполагается, что она была известна в древнем Египте и Вавилоне. До нашего времени дошли указания на то, что искусство секретного письма использовалось в древней Греции.

Опишем кратко сообщения симпатические или скрытые. Они могут быть сделаны специальными техническими средствами, как передача остронаправленным лучом, или надпись бесцветными чернилами, проявляющаяся лишь после специального физического или химического воздействия. **Именно скрытые сообщения принято называть тайнописью, но не шифры.**

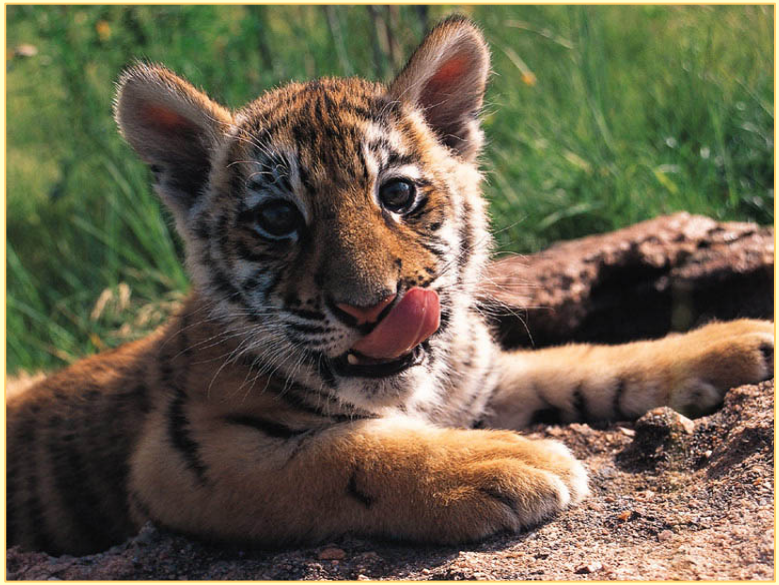
Популярные исторические книжки сообщали, что российские революционеры в тюрьмах использовали в качестве симпатических чернил обычное молоко - и это правда. При нагревании на огне или горячим утюгом такие записи становились отчетливо видны. Переписка химией состоит в следующем. Пишут на шероховатой, не глянцевой бумаге. Пишут сначала обыкновенными чернилами какой-нибудь безразличный текст, то есть что-либо совершенно безобидное, ни слова о делах. Когда это письмо написано, то берут совершенно чистое мягкое перо и пишут между строками уже то, что хотят сказать о конспиративных делах. Это конспиративное письмо пишут химическими чернилами, то есть раствором какой – нибудь кислоты, например, молочной.

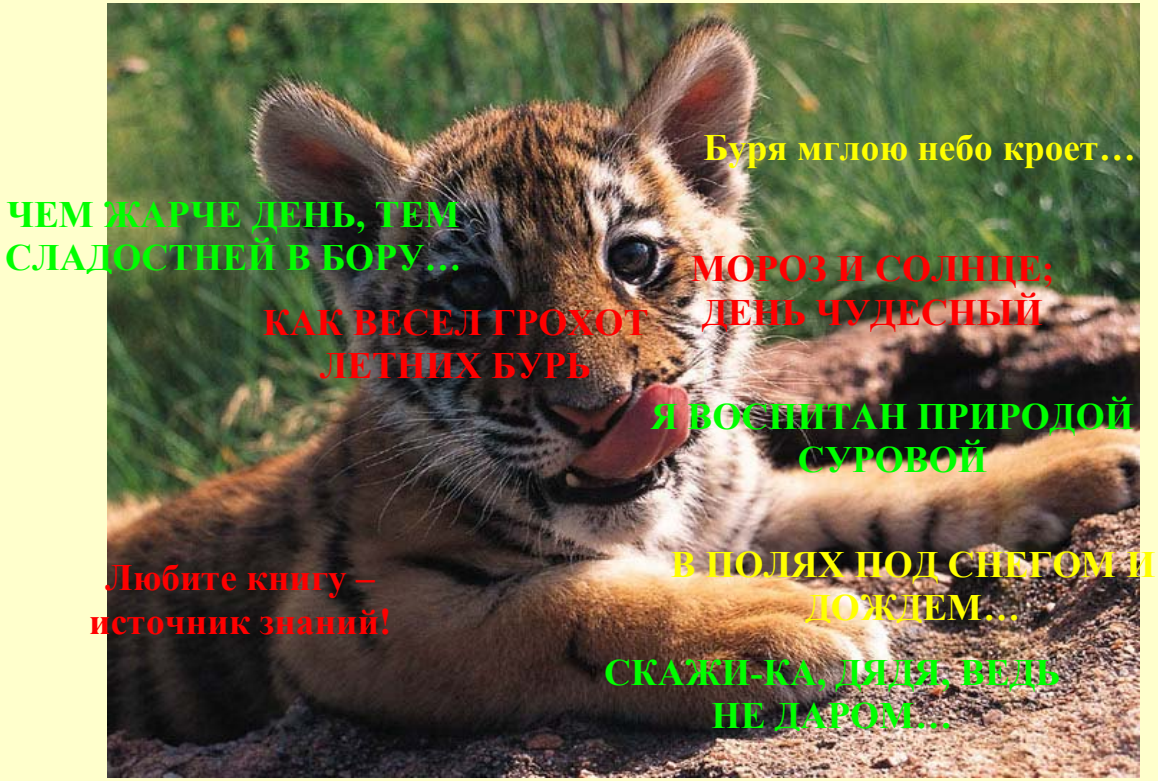
Выявить и прочесть тайнопись не составляет большой сложности, ведь были разработаны и развиты способы чтения скрытых и стертых текстов с помощью фотографии, подбора освещения и явления люминесценции. **Трудность прочтения «молочной» тайнописи всего лишь легенда.**

После Второй мировой войны распространились сверхминиатюрные фотографии, называемые микроточками. Одна **микроточка** размером с обычную точку текста могла содержать сотни страниц документов и найти ее в книге среднего формата было много сложнее, чем иголку в стоге сена. Сейчас нет технических проблем записать текст так мелко, что его вообще нельзя будет прочесть оптическими средствами, а придется рассматривать в электронный микроскоп.

Пример современной тайнописи - цифровой снимок.

Цифровая фотография содержит несколько мегабайт информации, и умело произведенное сокрытие в нем мегабайта шифровки практически не ухудшит качества изображения.





Прятать шифровки очень просто потому, что они ничем не отличимы от обычного шума или помех в каналах связи. Если обычная тайнопись легко читается, то тайнопись шифрованного сообщения, замаскированного под шум или сбои, найти невозможно.

Прибегая к симпатическим сообщениям, невольно приходится вступать в бесконечное **состязание меча и щита**, которому нет конца - **на каждый щит найдется и поражающий его меч**. Любой способ создания симпатического текста будет вскоре разрушен, и к этому нужно быть готовым. А что это за секретность без гарантий стойкости?

Коды

Коды как и тайнопись к шифрам не относятся. Коды – это системы условных обозначений или названий, применяемых при передаче информации в дипломатии, коммерции и военном деле. Кодирование часто применяется для повышения качества передачи. Хорошо известны и широко используются коды, исправляющие ошибки при передаче сообщений по каналам связи или хранении данных в памяти ЭВМ. Другой многочисленный класс кодов представлен средствами сжатия данных. Употребление этих кодов вызвано не секретностью, а стремлением сэкономить на стоимости передачи или хранения сообщения.

Сейчас аналогичных кодов тьма-тьмущая и все они представляют собой замену отдельных слов или фраз группами цифр или букв.

«**Ж**ивете **Д**обро **У**хо **Б**уки **О**н **Р**цы **И**же **С**лово»

«**Ж**еня **Д**митрий **У**льяна
Борис **О**льга **Р**оберт
Игорь **С**вета»

«**J**uliet **D**elta **U**niform **B**ravo **O**scar **R**omeo **I**ndia **S**ierra»

Такое кодирование называется
акрокодом
(«Akro» - по-гречески край,
первые буквы слов или строк.)

«**Ж**елезная **д**орога **у**ведомлена.
Буду **о**бмер **р**абот **и**сполнять **с**ам»

Специальные знаки и сигналы

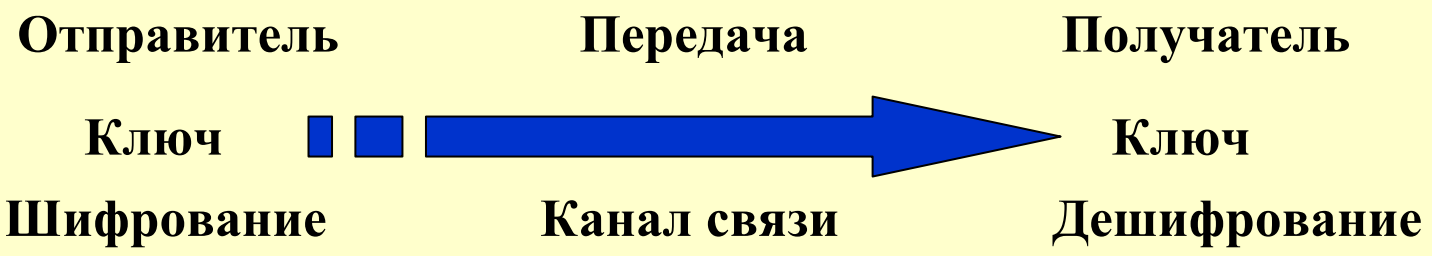
На флоте до сих пор используется семафорная азбука, сигнал флаги и спец флаги, которые в особых случаях расцвечивают суда флота. Сигнальными флагами написано «ЕЛЕНА ГОРШУНОВА ПРИВЕТСТВУЕТ ВАС» в начале работы. Специальным сигналом мог быть костер на холме, оповещающий древних воинов о приближении неприятеля, могут быть даже цветы купленные у цветочника-связника или горшок с цветком на подоконнике явочной квартиры.

«Петр Великий»
на рейде Североморска
в день ВМФ расцвечен
сигнальными флагами

Криптографический (третий) метод защиты информации

Дипломатические, военные и промышленные секреты обычно передаются или хранятся не в исходном виде, а после шифрования. В отличие от тайнописи, которая прячет сам факт наличия сообщения, шифровки передаются открыто, а прячется только смысл. ***Криптография обеспечивает сокрытие смысла сообщения с помощью шифрования и открытие его расшифровыванием, которые выполняются по специальным криптографическим алгоритмам с помощью ключей у отправителя и получателя.***

Классическая схема передачи секретных сообщений криптографическим преобразованием, где указаны этапы и участники этого процесса выглядит так:



Шифрование и расшифровывание, выполняемые криптографами, а также разработка и вскрытие шифров криптоаналитиками составляют **предмет науки криптологии** (от греческих слов «криптос» - тайный и «логос» - мысль). В этой науке преобразование шифровки в открытый текст (сообщение на оригинальном языке, порой называемое ***«клер»***) может быть выполнено в зависимости от того, известен или нет **ключ**. Условно ее можно разделить на криптографию и криптоанализ.

Криптография связана с шифрованием и расшифровыванием конфиденциальных данных в каналах коммуникаций. Она также применяется для того, чтобы исключить возможность искажения информации или подтвердить ее происхождение.

Криптоанализ занимается в основном вскрытием шифровок без знания ключа и, порой, примененной системы шифрования. Эта процедура еще называется взломкой шифра.

Итак, криптографы стремятся обеспечить секретность, а криптоаналитики ее сломать.

Криптография древнего мира

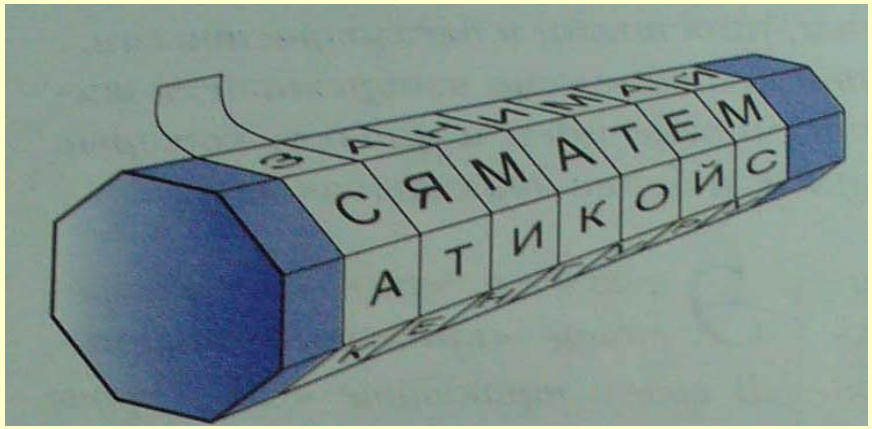
Ряд систем шифрования дошел до нас из глубокой древности. Появились они одновременно с письменностью в 4-м тысячелетии до нашей эры. Методы секретной переписки были изобретены независимо во многих древних обществах, таких как Египет, Шумер и Китай...

Коды, появившиеся вместе со словарями, были хорошо известны в Вавилоне и Ассирии, а древние египтяне применяли по меньшей мере 3 системы шифрования. Упрощение письма стимулировало развитие криптографии.

Принципиально иной шифр, более древний, связан с перестановкой букв сообщения по определенному, известному отправителю и получателю правилу.

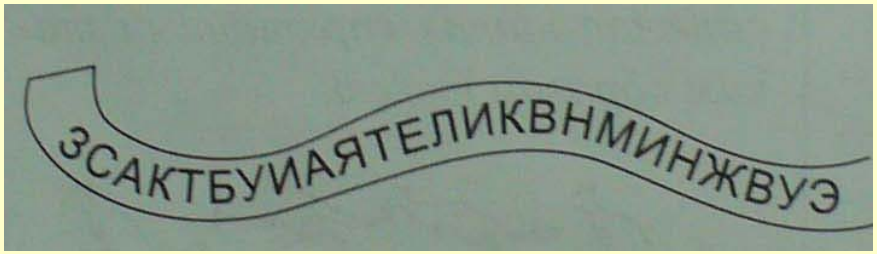
Даже в Библии можно найти примеры шифровок. В книге пророка Иеремии (25, 26) применен древний метод шифрования **атбаш** - шифровка простой заменой (вместо первой буквы алфавита писалась последняя, вместо второй - предпоследняя и так далее): «...а царь Сессаха выпьет после них». Читая по «**атбашу**» слово СЕССАХ, на языке оригинала получаем слово ВАВИЛОН.

Спартанская хитрость

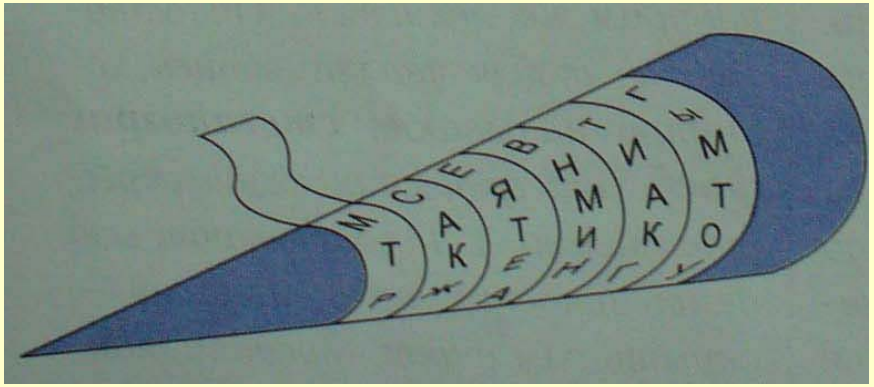


Одним из первых приборов, реализующих шифр перестановки, была **СЦИТАЛЛА.**

Какой-то хитрец из спартанцев обнаружил, что если полоску пергамента намотать спиралью на палочку и написать на нем вдоль палочки текст сообщения, то, после снятия полоски буквы на ней расположатся хаотично. Это то же самое будет если буквы писать не подряд, а через условленное число знаков по кольцу до тех пор, пока весь текст не будет исчерпан.

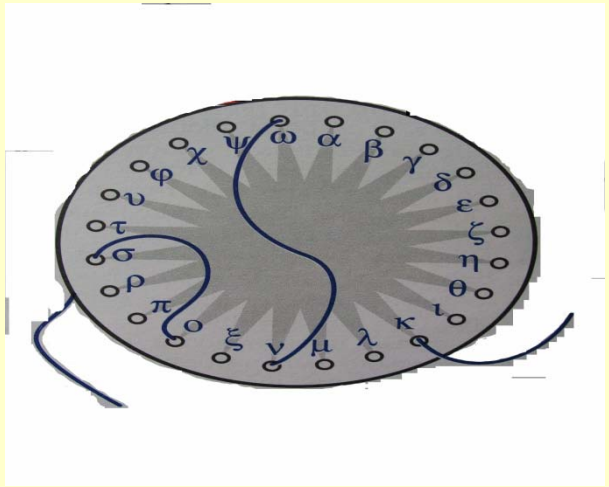


Текст записанный на ремне из пергамента.



Цилиндр известного диаметра-ключ шифра **АНТИСЦИТАЛЛА.**

Диск Энея



κ ϖ ν ο δ

Один из первых изобретателей шифров, известный нам по имени, греческий полководец **Эней Тактика**. Он создал простое, но очень удобное устройство - **«диск Энея»** - небольшой диск, с просверленными вдоль его края отверстиями соответствующими буквам алфавита. Для того, чтобы зашифровать текст «шишка», нить вдевали в отверстия так, чтобы по ходу нити последовательность отверстий была такой же, как у соответствующих букв в тексте.

Получатель сообщения, вытягивая эту нить, мог прочитать все буквы, правда, в обратном порядке. Послание «шишка» означало условный сигнал. Если сообщение было перехвачено, гонец легко мог его уничтожить, выдернув нить.

Еще Эней придумал **шифровальную линейку**
и предложил **«книжный шифр».**

Квадрат Полибия

	1	2	3	4	5
1	a	b	c	d	e
2	f	g	h	i	k
3	l	m	n	o	p
4	q	r	s	t	u
5	v	w	x	y	z

51 = V; 15 = e; 33 = n; 24 = i и.т.д.

<u>51</u>1533245124142451241324

- Veni, vidi, vici.

- Пришел, увидел, победил.

В древнем Риме придумали немало своих способов шифрования. Например, **квадрат Полибия**, изобретённый во II веке до н.э., не вышел из употребления до сих пор. Устроен он так: все (или почти все) буквы алфавита располагают в квадрате или прямоугольнике соответствующего размера: (5 на 4 для латинского, 5 на 6 для русского алфавита). После этого каждая буква кодируется двумя числами - номером строки и номером столбца, в которых она расположена. Конечно, буквы можно (и нужно) располагать не по порядку: - тогда шифр становится гораздо сложнее.

Шифр Цезаря

А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	...	Ь	Ъ	Э	Ю	Я
Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х		Ю	Я	А	Б	В

3

Первые достоверные сведения с описанием метода шифрования относятся к периоду смены старой и новой эры и описывают **шифр Цезаря** - способ, которым Юлий Цезарь прятал свои записи от излишне любопытных глаз. Шифр Цезаря предельно прост: в нем каждая буква сообщения заменялась на следующую за ней по алфавиту. Однако для того времени, когда умение читать и писать было редким исключением, его криптостойкости вполне хватало. В переписке с Цицероном (106 - 43 гг. до н.э.) он использовал шифр собственного изобретения. Применительно к современному русскому языку он состоял в следующем. Выписывался алфавит: А, Б, В, Г, Д, Е, ..., Э, Ю, Я; затем под ним выписывался тот же алфавит, но со сдвигом на 3 буквы влево.

Ключом в шифре Цезаря является число 3 - величина сдвига нижней части алфавита (сообщение УЛП означает РИМ). Цезарь Август использовал тот же шифр, но с ключом, равным 4. Слово РИМ шифруется как ФМР.

Шифры - перестановки

В шифрах перестановки для получения нечитабельной криптограммы изменяется порядок чередования символов исходного текста. Рассмотрим простой пример. Выберем целое положительное число, скажем 5. Расположим числа от 1 до 5 в двух строчной записи. Зашифруем фразу «ВСТРЕЧА СОСТОИТСЯ ЗАВТРА». В этой фразе 22 буквы. Допишем в конце ее несколько букв «Ъ» (это редко встречающаяся буква) так, чтобы общее количество букв стало кратным 5, то есть 25. Выпишем эту дополненную фразу без пропусков, одновременно разбив ее на пятизначные группы: ВСТРЕ ЧАСОС ТОИТС ЯЗАВТ РАЪЪЪ.

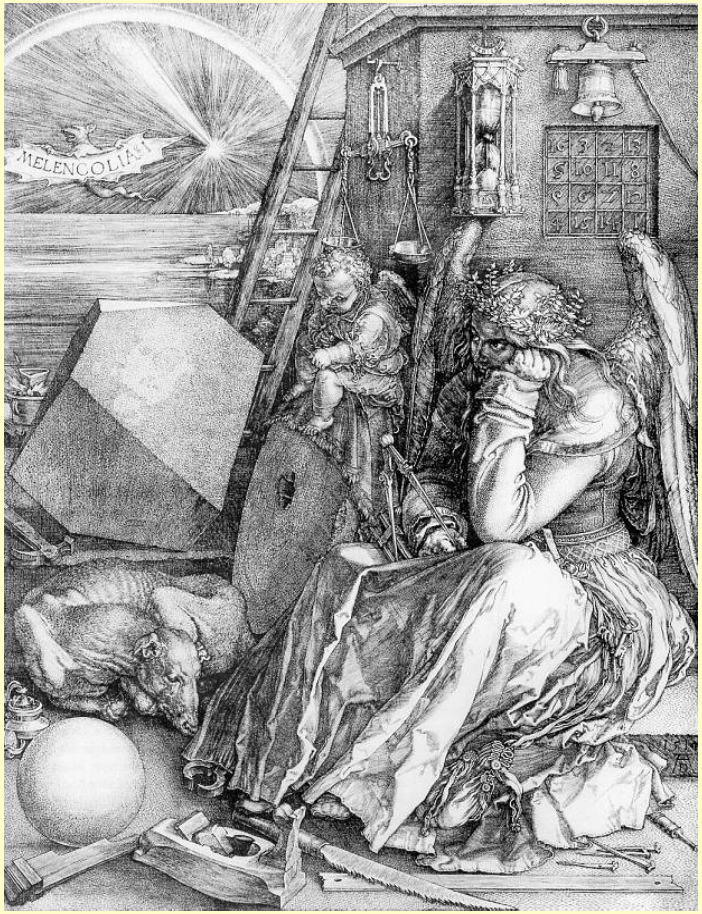
1	2	3	4	5
3	2	5	1	4

Буквы каждой группы переставим в соответствии с указанной двухстрочной записью по следующему правилу: первая буква встает на третье место, вторая - на второе, третья - на пятое, четвертая - на первое и пятая - на четвертое. Преобразованные группы соединим без пропусков и получим криптограмму: РСВЕТОАЧССТОТСИВЗЯТАЪАРЪЪ.

При расшифровании криптограмма разбивается на группы по 5 букв и эти буквы переставляются в обратном порядке: 1 на 4 место, 2 на 2, 3 на 1, 4 на 5 и 5 на 3. Ключом шифра является выбранное число 5 и порядок расположения чисел в нижнем ряду двухстрочной записи.

Шифры перестановки чрезвычайно коварны в том смысле, что могут дать несколько вариантов осмысленного прочтения, если не знать точного значения ключа.

Средневековый прорыв криптографической науки



На гравюре А. Дюрера «Меланхолия» позади грустящего ангела изображен магический квадрат, заполненный цифрами.

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. Если потом выписать содержимое таблицы по строкам, то получалась **шифровка перестановкой букв.**

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

Магический квадрат из-за спины грустного ангела:

16 03 02 13
05 10 11 08
09 06 07 12
04 15 14 01

Шифровка этого магического квадрата:

О И Р Т
З Ш Е Ю
Ж А С
Е Г О П

Полученная шифровка из
ПРИЕЗЖАЮ ШЕСТОГО,
ОИРТЗШЕЮ ЖАСЕГОП
представляется основательной. На первый взгляд кажется, будто магических квадратов очень мало. Тем не менее их число очень быстро возрастает с увеличением размера квадрата.

Так, существует лишь один магический квадрат размером 3 х 3, если не принимать во внимание его повороты. Магических квадратов 4 х 4 насчитывается уже 880, а число магических квадратов размером 5 х 5 около 250000. Поэтому магические квадраты больших размеров могли быть хорошей основой для надежной системы шифрования того времени, потому что ручной перебор всех вариантов ключа для этого шифра был немыслим.

Аббат из Германии Иоганн Трисемус – «второй отец» криптологии

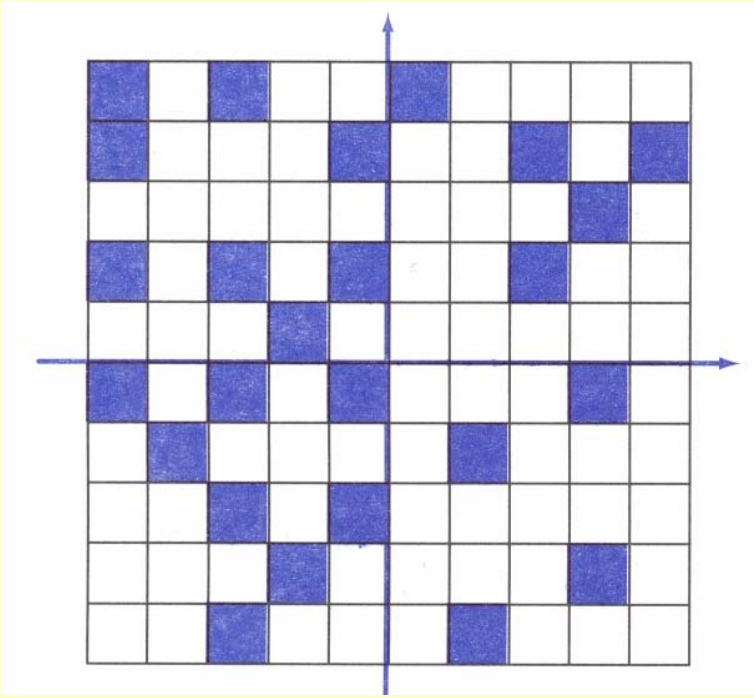
В 1508 году Трисемус написал **«Полиграфию»**, первую печатную работу по криптологии. В ней он первым описал применение шифрующих таблиц, заполненных алфавитом в случайном порядке. Для получения такого шифра обычно использовались ключевое слово или фраза и таблица, которая для русского языка может иметь размер 5 х 6. Ключевое слово вписывалось в таблицу по строкам, а повторяющиеся буквы отбрасывались. Таблица дозаполнялась не вошедшими в нее буквами алфавита по порядку. Поскольку ключевое слово легко хранить в памяти, то такой подход упрощал процессы шифрования и дешифрования. Такие табличные шифры называются монограммными, так как шифрование ведется по одной букве. Трисемус первым заметил, что можно шифровать по две буквы за раз. Такие шифры были названы биграммными.

При всем при том, что «Полиграфия» была довольно доступной печатной книгой, описанные в ней идеи получили признание лишь тремя веками позже. Скорее всего это вызвано плохой известностью среди криптографов Трисемуса, который слыл богословом, библиофилом и основателем архивного дела.

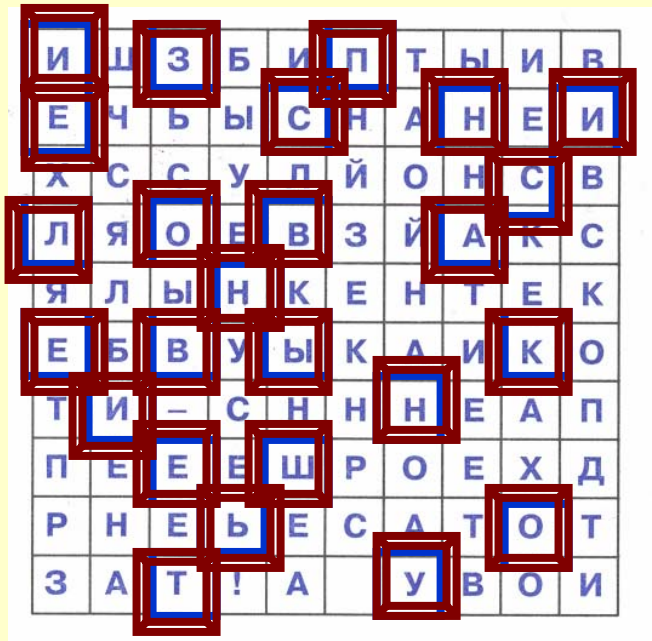
Среди шифров средневековья встречается много курьезов. **Леонардо да Винчи** шифровал большинство своих личных записей. Самый простой вид шифра которым он пользовался, это обратное написание текста так, что прочесть его можно лишь в отражении зеркала. Однако Леонардо иногда использовал шифры и посерьезнее, поэтому далеко не все его заметки и записи расшифрованы и изучены. Люди, умеющие писать левой рукой справа налево зеркальный текст, нередки. Изумительно, но встречаются люди, которые умеют даже произносить фразы "наоборот" и понимать их на слух. Поистине, человеческим способностям нет предела. В средние века появляются профессиональные и даже потомственные криптографы, вроде семейства **Арджентн**, служившего у папы Римского.

Выдающийся итальянский математик **Джероламо Кардано**, имя которого дошло до нас благодаря изобретенному им шарнирному механизму. Увлечение теорией магических квадратов привело Кардано к открытию нового класса шифров перестановок, названных **решетками или трафаретами**. Они представляют собой квадратные таблицы, где четверть ячеек прорезана так, что при четырех поворотах они покрывают весь квадрат. Вписывание в прорезанные ячейки текста и повороты решетки продолжаются до тех пор, пока весь квадрат не будет заполнен …

Зашифрованные пословицы шифром Кардано

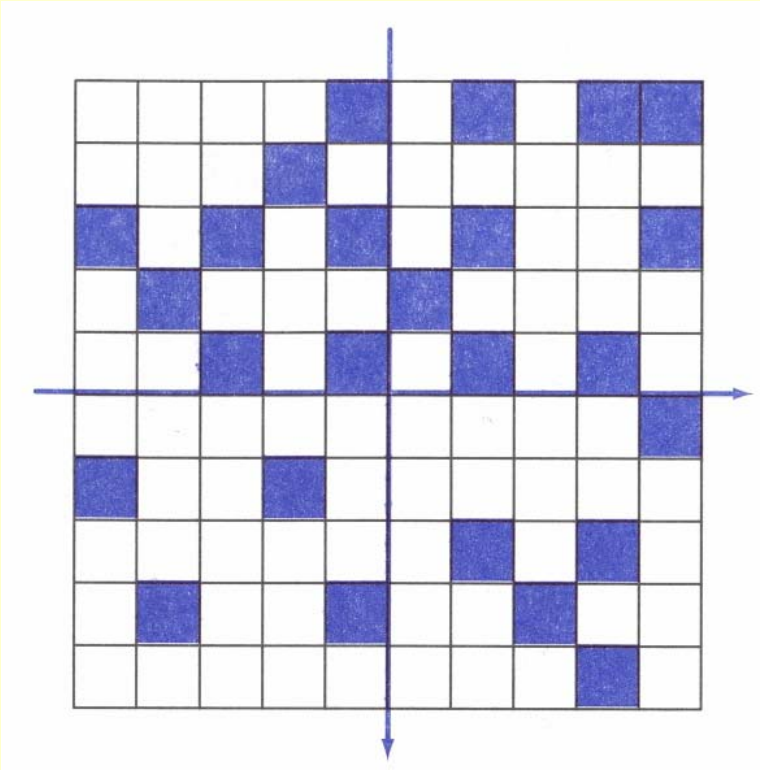


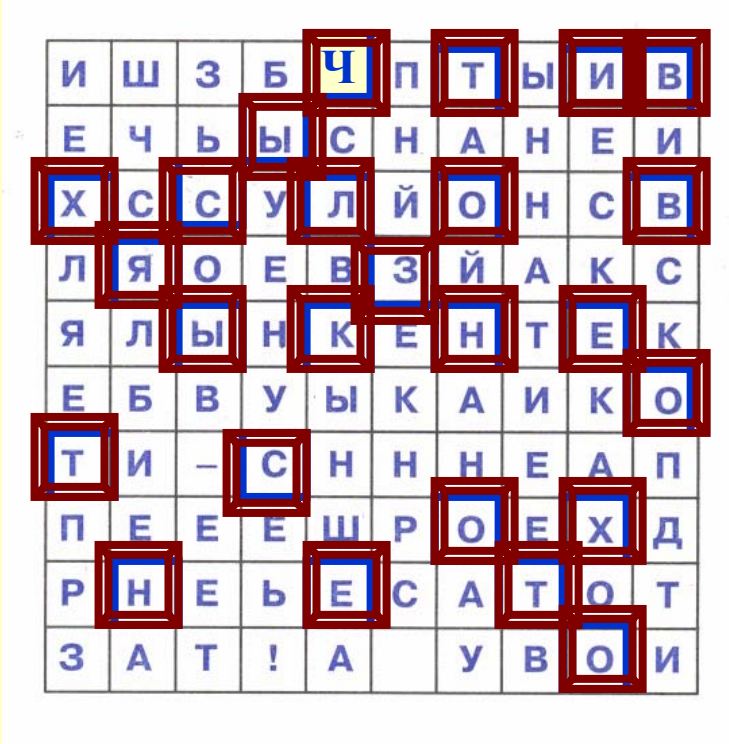
Шаблон - квадрат
с отверстиями



Рамкой выделены буквы после
первого приложения шаблона

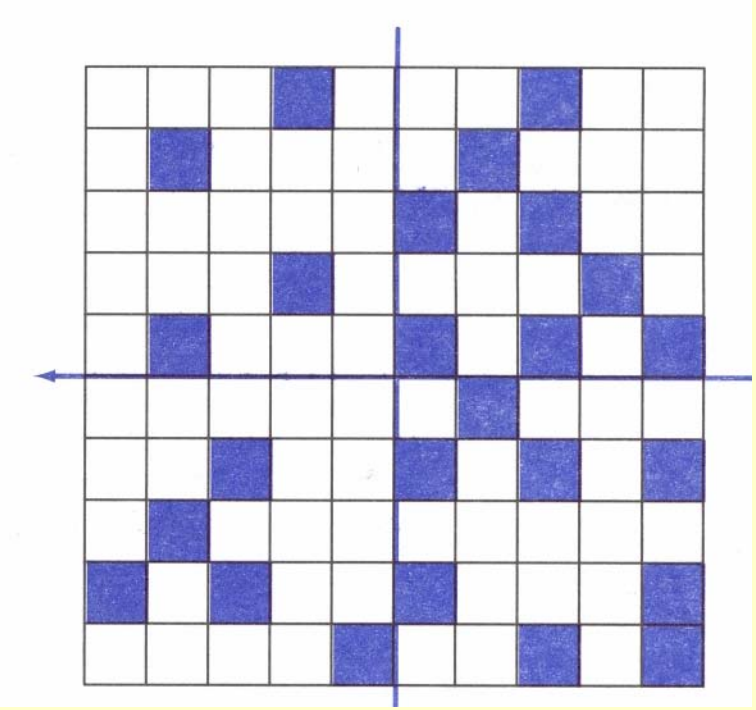
- 0 град.: - ИЗПЕСНИСЛОВАНЕВЫКИНЕШЬ…ОТУ
  - **= ИЗ ПЕСНИ СЛОВА НЕ ВЫКИНЕШЬ**





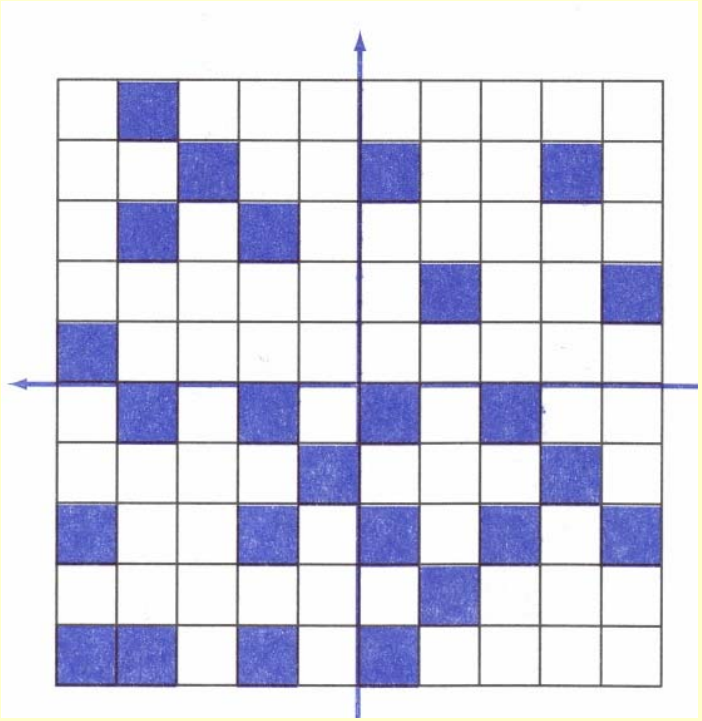
Поворачиваем шаблон на 90 градусов.
Рамкой выделены буквы после второго приложения шаблона

- ОТУ…90град.: - ЧТИВЫХСЛОВЯЗЫКНЕОТСОХНЕТ…О
- **=ОТ УЧТИВЫХ СЛОВ ЯЗЫК НЕ ОТСОХНЕТ**



Поворачиваем шаблон еще на 90 градусов.
Рамкой выделены буквы после третьего приложения шаблона

- О…180град.: БЫЧАЙНЕКЛЕТКА-НЕПЕРЕСТАВИ….
- **=ОБЫЧАЙ НЕ КЛЕТКА - НЕ ПЕРЕСТАВИШЬ**



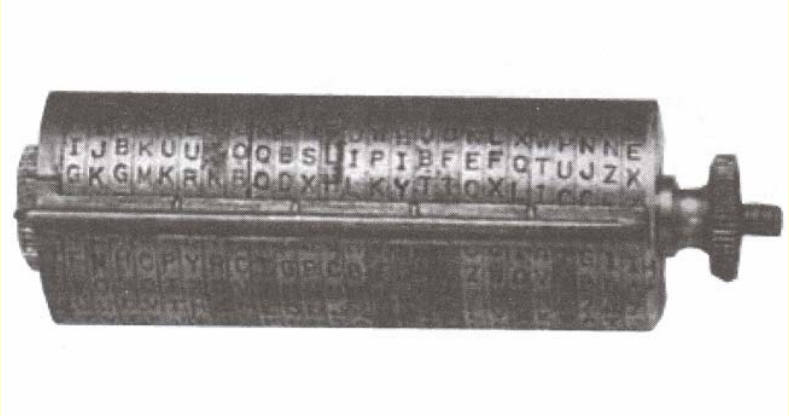
- 270 град. ШЬ……НЕСУЙСЯБУКИНАПЕРЕДАЗА!
- **=НЕ СУЙСЯ БУКИ НА ПЕРЕД АЗА!**

Таким образом, к XVIII веку криптография окончательно сложилась в виде самостоятельной науки. Однако несмотря на наличие профессиональных криптологов, находящихся на государственной службе, и постоянного использования шифров в дипломатии и военном деле, **криптология еще не вышла из младенческого возраста и ею могли заниматься лишь избранные, одаренные одиночки.**

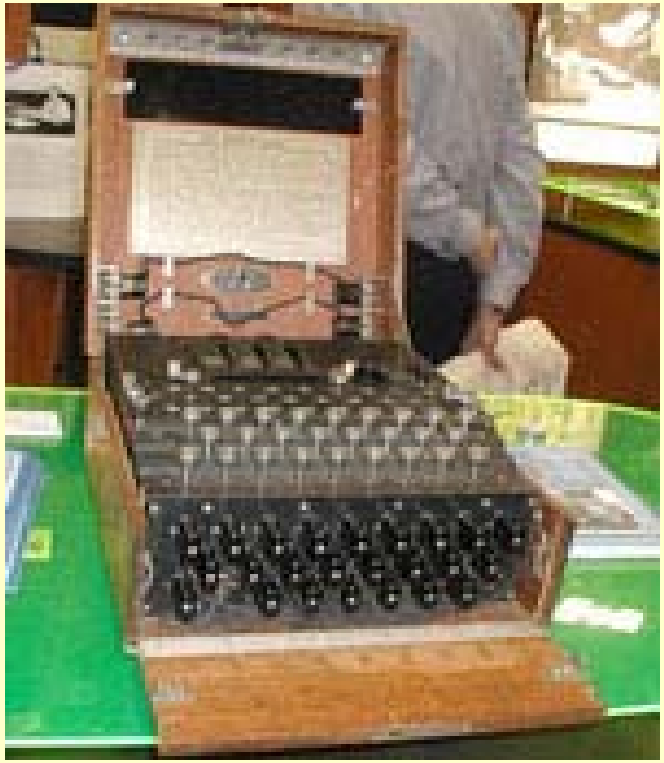
Криптология нового времени

Во второй половине XIX века появляется множество работ по вскрытию сложных шифров замены для конкретных условий, при использовании повторяющегося короткого ключа, при шифровке нескольких сообщений одним ключом. Тогда же в Англии и США стали выходить периодические издания, посвященные вопросам криптоанализа, где профессионалы и любители, обмениваясь опытом, предлагали новые типы шифров и анализировали их стойкость ко взлому. Криптография впервые серьезно заявила о своей исключительно большой значимости в современном мире.

XIX век с расширением связных коммуникаций занялся автоматизацией процесса шифрования. Появился телеграф, нужно шифровать и его. Любопытно, что **цифровое шифрующее колесо** было изобретено госсекретарем **Томасом Джефферсоном.**



Принцип работы таких машин заключается в многоалфавитной замене текста сообщения по длинному ключу. Длина периода ключа определялась наименьшим общим кратным периодов оборотов шифрующих колес. При 4 колесах и периодах их оборотов 13, 15, 17 и 19 получалась большая длина периода ключа 62985, очень затрудняющая расшифровку коротких сообщений. Перед началом шифрования диски помешались на общую ось в порядке, определяемым ключом.

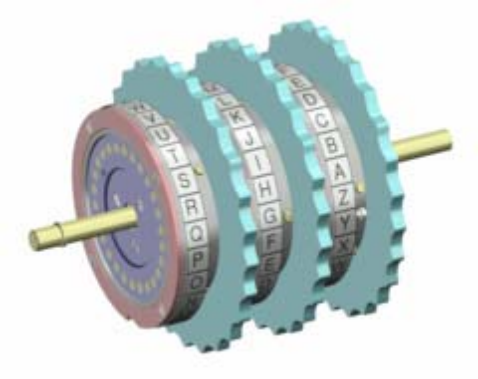


Та самая «Энигма»

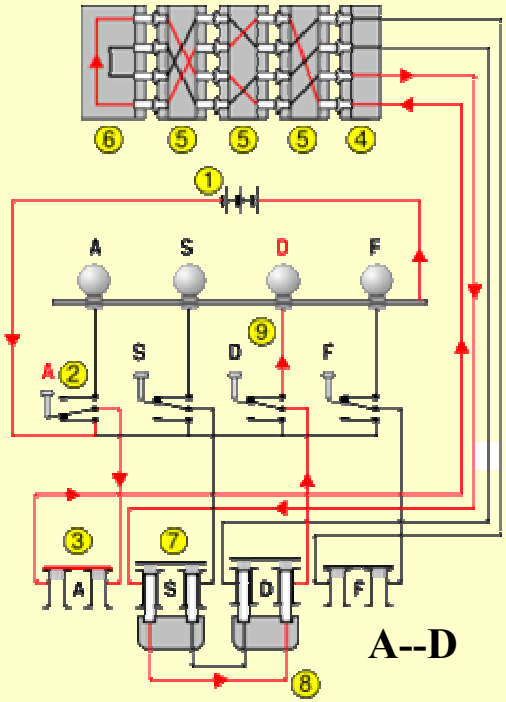
Предшественница современных криптографических машин была роторная машина, изобретенная **Эдвардом Хеберном** в 1917 году и названная впоследствии **Энигмой** (Слово enigma переводится как **загадка**. Промышленные образцы этой машины изготовляла фирма Siemens.). Она представляла собой 4 вращающихся на одной оси барабана, обеспечивающих более миллиона вариантов шифра простой замены, определяемого текущим положением барабанов.

На каждой стороне барабана по окружности располагалось 25 электрических контактов, столько же, сколько букв в алфавите. Контакты с обеих сторон барабана соединялись попарно случайным образом 25 проводами, формировавшими замену символов. Колеса складывались вместе и их контакты, касаясь друг друга, обеспечивали прохождение электрических импульсов сквозь весь пакет колес. Перед началом работы барабаны поворачивались так, чтобы устанавливалось заданное кодовое слово - ключ, а при нажатии клавиши и кодировании очередного символа правый барабан поворачивался на один шаг.

После того, как он делал оборот, на один шаг поворачивался следующий барабан - будто бы в счетчике электроэнергии. Таким образом, получался ключ заведомо гораздо более длинный, чем текст сообщения. Например, в первом правом барабане провод от контакта, соответствующего букве U, присоединен к контакту буквы F на другой его стороне. Если же барабан поворачивался на один шаг, то этот же провод соответствовал замене следующей за U буквы V на следующую за F букву G. Так как барабаны соприкасались контактами, то электрический импульс от нажатой клавиши с буквой исходного текста прежде чем достигал выхода претерпевал 4 замены: по одной в каждом барабане.



Три последовательно соединенных ротора - сердце «Энигмы»



Для затруднения расшифровывания барабаны день ото дня переставлялись местами или менялись. Дальнейшее усовершенствование этой машины сделало движение барабанов хаотичным, а число их увеличилось сначала до 5, а потом до 6. Все устройство могло поместиться в портфеле и было так просто, что обслуживалось обычными связистами.

Сегодняшний день. Что дальше?

В наши дни, когда существуют достаточно мощные персональные компьютеры, специалисты - криптологи решились на штурм секретов «Энигмы». Для этого в январе 2006 года был создан так называемый проект **M4**. Стартовал он 9 января, и всего за два месяца удалось прочитать одно из трех сообщений. Все очень просто: каждый человек, чей компьютер подключен к Интернету, может, как сказано на сайте, поделиться своим временем и мощностью компьютера для общего дела.

Установленный на компьютере специальный программный продукт соединяется с сервером и, таким образом, становится рабочим модулем. А дальше - все эти рабочие модули начинают, используя так называемый «метод перебора», просматривать варианты шифрограмм числом 2 X 10 в 145-й степени.

Содержание радиосигнала 1851/19/252: "F T 1132/19: ***Вынужден к погружению атакой. Глубина допустимая. Последняя позиция противника 0830h AJ 9863, (курс]) 220 градусов, (скорость) 8 узлов. Преследую. (Барометр) упал до 14 миллибар, (ветер) северо-северо-восточный, (сила) 4, видимость 10 (морских миль)".***

Все нынешние системы кодировки находятся под угрозой, поскольку внедрение все более мощных суперкомпьютеров в принципе позволяет расколоть любой шифр путем быстрой проверки всех возможных комбинаций.

Новый способ криптографии – **квантовая криптография** - основанный на исходной непредсказуемости поведения квантовой системы или принципе неопределенности Гейзенберга, открытого еще в 1927 году, сегодня стал давать практические результаты.

Информация в таких системах кодируется с помощью квантовых частиц (например, фотонов), меняющих свое состояние при малейшей попытке их перехватить и измерить. При этом оказывается невозможным одновременно получить координаты и импульс частицы. Как утверждается, это делает расшифровку в принципе невозможной. Кроме того, сама попытка расшифровать секретную информацию становится известна адресату, поскольку он получает видоизмененные параметры частиц.

Алиса и Боб пытаются сохранить от Евы тайну шифровального ключа, передавая его в виде поляризованных фотонов по схеме, изобретенной в 1980-х гг. Чарльзом Беннеттом из IBM и Жилем Брассаром из Монреальского университета.

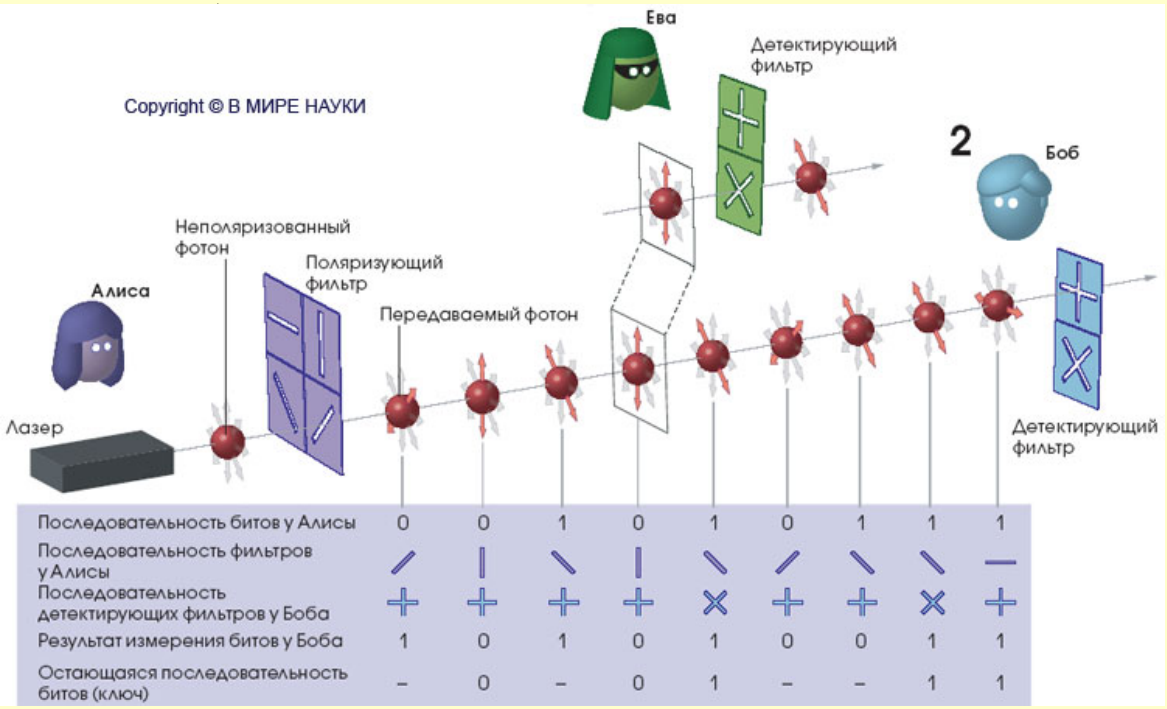
1. Для создания ключа Алиса посылает фотоны через прямой или диагональный поляризующий фильтр и записывает направление плоскости поляризации.

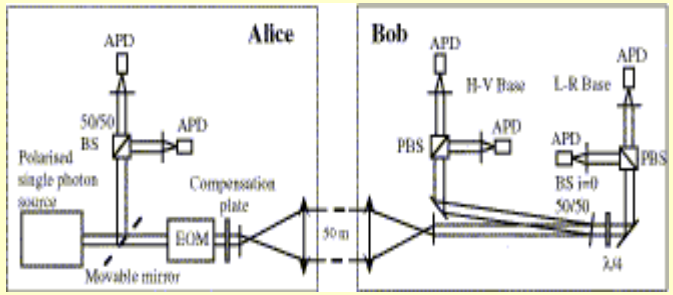
2. Для каждого поступающего бита Боб случайным образом выбирает фильтр для обнаружения и записывает поляризацию и значение бита.

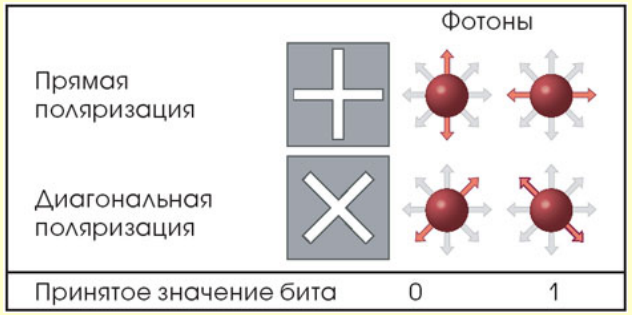
3. Когда злоумышленник (Ева) пробует отследить последовательность фотонов, принципы квантовой механики не позволяют ему использовать оба типа фильтров для выяснения направления поляризации одного фотона. Если Ева выбирает непра-вильный фильтр, то возникают ошибки, обусловленные изменением поляризации.

4. Получив все фотоны, Боб по открытому каналу сообщает Алисе последователь-ность фильтров, которые он использовал для поступающих фотонов. О считанных значениях битов он ничего не сообщает.

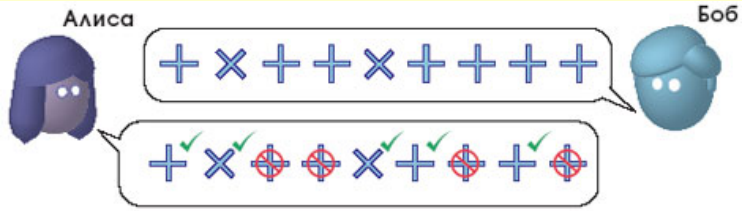
5. Алиса говорит Бобу, какие фильтры он выбрал правильно. Измеренные с их помощью биты будут использоваться при формировании ключа для шифрования







После передачи Боб связывается с Алисой по обычному (несекретному) каналу, чтобы сообщить ей, каким из двух способов он пользовался при приеме каждого фотона, но не указывает, какое значение - 0 или 1 - он получил в результате измерения. Затем Алиса сообщает Бобу, какие из фотонов были считаны правильно. Неверно измеренными фотонами пренебрегают. Верно принятые фотоны образуют ключ, который используется для шифрования или расшифровки секретных сообщений. Согласно принципу Гейзенберга злоумышленница Ева, пытающаяся перехватить поток фотонов, не сможет произвести измерения каждого фотона обоими способами. Если Ева проведет измерение неправильным способом, то неизбежно внесет ошибки, даже если потом перешлет измеренные биты Бобу. Алиса и Боб смогут обнаружить присутствие нарушителя, сверяя отобранные биты.



Криптоанализ очень интересная и сложная проблема, которую я не готова рассмотреть в данной работе. Для успешной ломки шифрограмм необходимы глубокие знания математики, языка… Но прикоснуться к таинству криптографического процесса можно с помощью подручных средств, что я и сделала, и о чем расскажу в следующих разделах моей работы.

Использование частотного анализа для взлома шифров

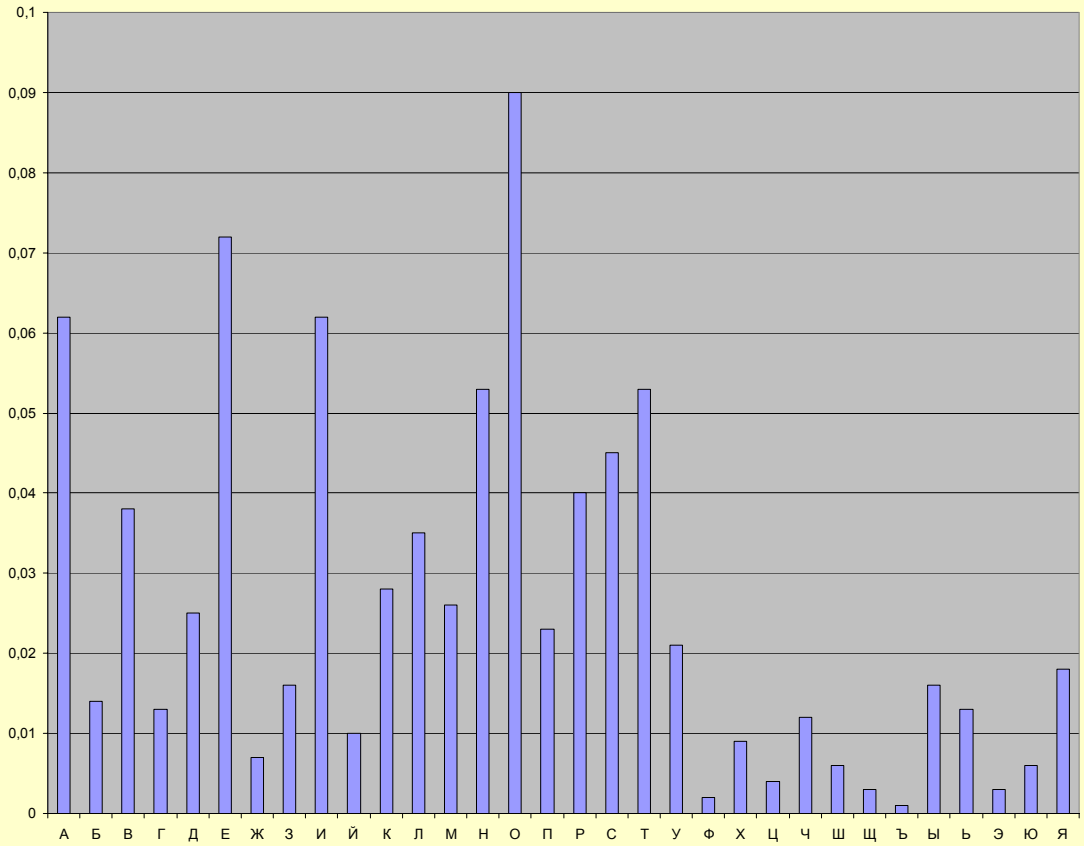
«М ТВНШ ЪН ЬТЭТЧШНСЪИВ ХФ ЯХБШХЮН, ПЮМ ЬЫЧШНУНЩЫТЦ ЯТШТУЧХ ЮЫЮЯЫМШН ХФ ЫСЪЫРЫ ЪТОЫШЙЕЫРЫ ДТЩЫСНЪН, ЧЫЯЫЭИЦ СЫ ЬЫШЫПХЪИ ОИШ ЪНОХЯ ЬАЯТПИЩХ ФНЩТЯЧНЩХ Ы РЭАФХХ. ОЫШЙЕНМ ДНЮЯЙ ХФ ЪХВ, Ч ЮДНЮЯХЛ СШМ ПНЮ, ЬЫЯТЭМЪН, Н ДТЩЫСНЪ Ю ЫЮЯНШПЪИЩХ ПТЖНЩХ, Ч ДНЮЯХЛ СШМ ЩТЬМ, ЫЮЯНШЮМ ГТШ».

Перед нами зашифрованный текст. Все что мы о нем знаем – это то, что для его шифровки был использован код Цезаря.

Ключ кода Цезаря - смещение букв алфавита на несколько символов - ищем с помощью метода частотного анализа шифрованного текста.

При этом нам известна таблица частот букв русского алфавита.

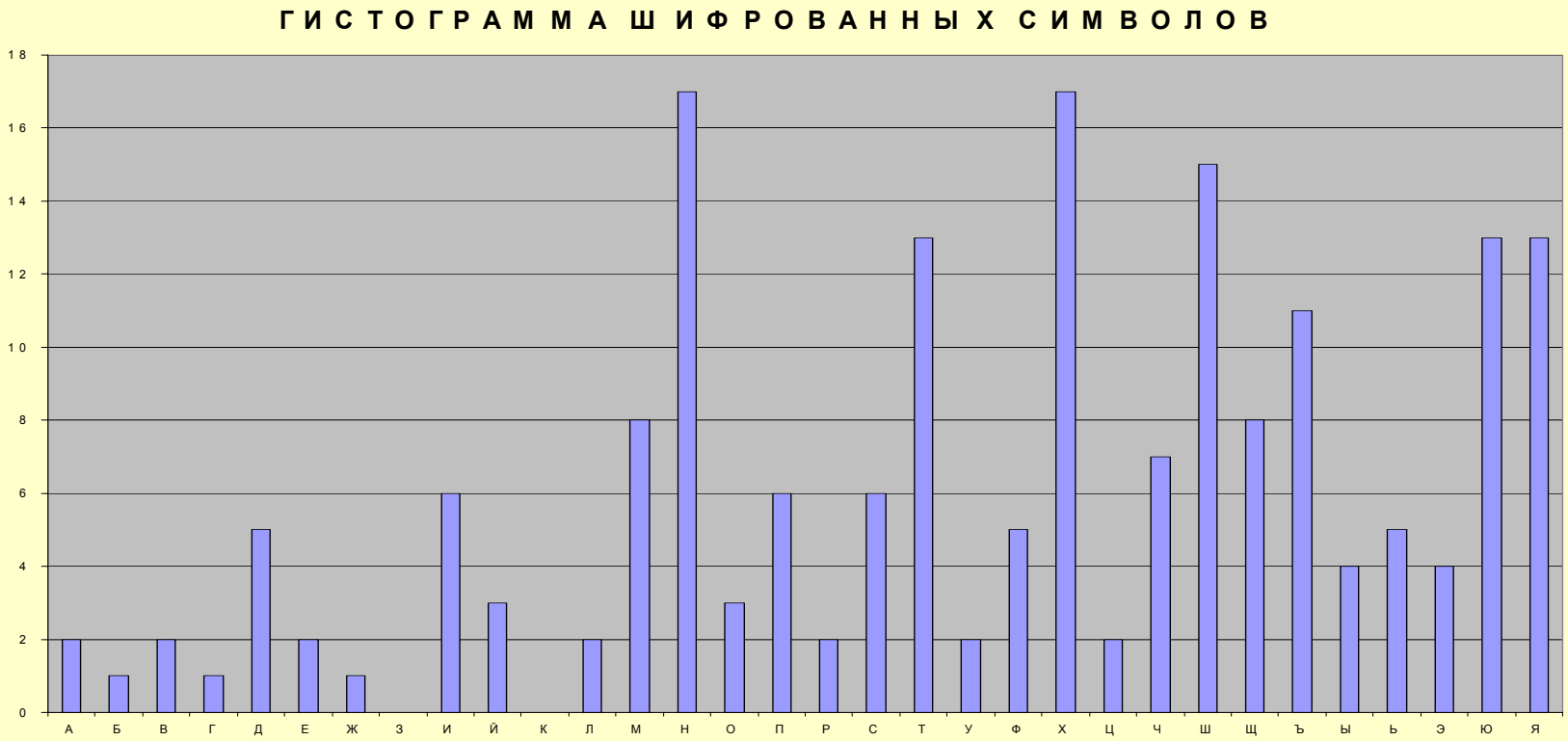
ГИСТОГРАММА ЧАСТОТ БУКВ РУССКОГО АЛФАВИТА



Посчитаем частоту символов:

Буква алфавита	Количество в тексте	Частота в русском языке
А	2	0,062
Б	1	0,014
В	2	0,038
Г	1	0,013
Д	5	0,025
Е	2	0,072
Ж	1	0,007
З	0	0,016
И	6	0,062
Й	3	0,010
К	0	0,028
Л	2	0,035
М	8	0,026
Н	17	0,053
О	3	0,090

Буква алфавита	Количество в тексте	Частота в русском языке
П	6	0,023
Р	2	0,040
С	6	0,045
Т	13	0,053
У	2	0,021
Ф	5	0,002
Х	17	0,009
Ц	2	0,004
Ч	7	0,012
Ш	15	0,006
Щ	8	0,003
Ъ	11	0,001
Ы	21	0,016
Ь	5	0,013
Э	4	0,003
Ю	13	0,006
Я	13	0,018



Сравнивая гистограммы частот букв русского языка и шифрованных символов получим возможные варианты замены символов:

А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	13
Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	
О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	
П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	15

Читаем зашифрованный тест:

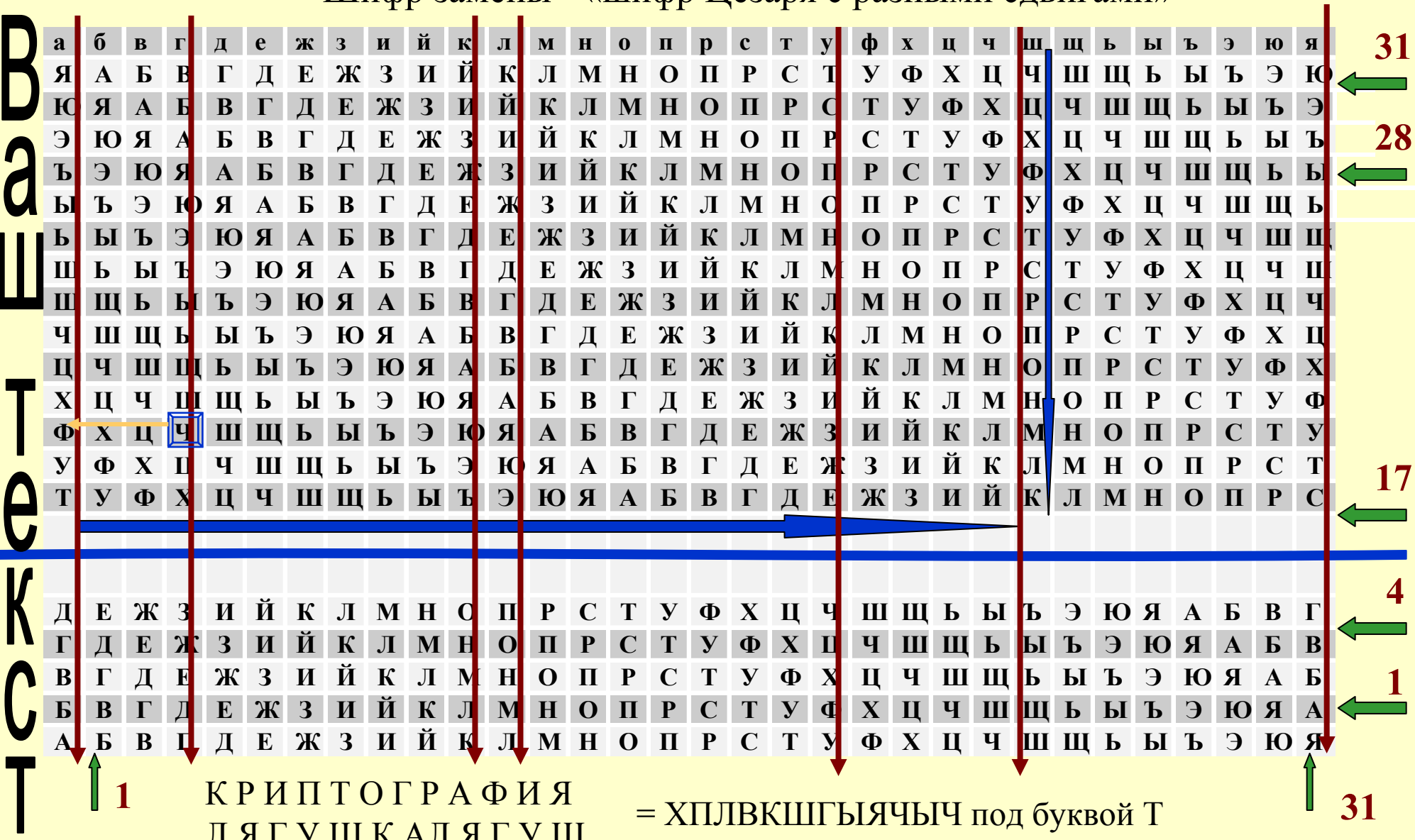
1	2	3	4	5	6	7	8	9	10	1	2	3	4	5	6	7	8	9	20	1	2	3	4	5	6	7	8	9	30	1	2	3
М	Т	В	Н	Ш	Ъ	Н	Ь	Т	Э	Т	Ч	Ш	Н	С	Ъ	И	В	Х	В	Я	Х	Б	Ш	Х	Ю	Н	П	Ю	М			
Я	Е	Х	А	Л	Н	А	П	Е	Р	Е	К	Л	А	Д	Н	Ы	Х	И	З	Т	И	Ф	Л	И	С	А	В	С	Я			
Ь	Ы	Ч	Ш	Н	У	Н	Щ	Ы	Т	Ц	Я	Т	Ш	Т	У	Ч	Х	Ю	Ы	Ю	Я	Ы	М	Ш	Н	Х	Ф	Ы	С	Ъ	Ы	Р
П	О	К	Л	А	Ж	А	М	О	Е	Й	Т	Е	Л	Е	Ж	К	И	С	О	С	Т	О	Я	Л	А	И	З	О	Д	Н	О	Г
Ы	Ъ	Т	О	Ы	Ш	Й	Е	Ы	Р	Ы	Д	Т	Щ	Ы	С	Н	Ъ	Н	Ч	Ы	Я	Ы	Э	И	Ц	С	Ы	Ь	Ы	Ш	Ы	П
О	Н	Е	Б	О	Л	Ь	Ш	О	Г	О	Ч	Е	М	О	Д	А	Н	А	К	О	Т	О	Р	Ы	Й	Д	О	П	О	Л	О	В
Х	Ъ	И	О	И	Ш	Ъ	Н	О	Х	Я	Ь	А	Я	Т	П	И	Щ	Х	Ф	Н	Щ	Т	Я	Ч	Н	Щ	Х	Ы	Р	Э	А	Ф
И	Н	Ы	Б	Ы	Л	Н	А	Б	И	Т	П	У	Т	Е	В	Ы	М	И	З	А	М	Е	Т	К	А	М	И	О	Г	Р	У	З
Х	Х	О	Ы	Ш	Й	Е	Н	М	Д	Н	Ю	Я	П	Х	Ф	Ъ	Х	В	Ч	Ю	Д	Н	Ю	Я	Х	Л	С	Ш	М	Д	Н	Ю
И	И	Б	О	Л	Ь	Ш	А	Я	Ч	А	С	Т	Ь	И	З	Н	И	Х	К	С	Ч	А	С	Т	И	Ю	Д	Л	Я	В	А	С
Ь	Ы	Я	Т	Э	М	Ъ	Н	Н	Д	Т	Щ	Ы	С	Н	Ъ	Ю	Ы	Ю	Я	Н	Ш	Й	Ь	И	Щ	Х	П	Т	Ж	Н	Щ	Х
П	О	Т	Е	Р	Я	Н	А	А	Ч	Е	М	О	Д	А	Н	С	О	С	Т	А	Л	Ь	Н	Ы	М	И	В	Е	Щ	А	М	И
Ч	Ю	Д	Н	Ю	Я	Х	Л	С	Ш	М	Щ	Т	Ъ	М	Ы	Ю	Я	Н	Ш	Ю	М	Г	Т	Ш								
К	С	Ч	А	С	Т	И	Ю	Д	Л	Я	М	Е	Н	Я	О	С	Т	А	Л	С	Я	Ц	Е	Л								
1	2	3	4	5	6	7	8	9	10	1	2	3	4	5	6	7	8	9	20	1	2	3	4	5	6	7	8	9	30	1	2	3

«Я ехал на перекладных из Тифлиса. Вся поклажа моей тележки состояла из одного небольшого чемодана, который до половины был набит путевыми заметками о Грузии. Большая часть из них, к счастию для вас, потеряна. А чемодан с остальными вещами, к счастию для меня, остался цел.»

А.С. Пушкин «Путешествие в Арзрум»

ТАБЛИЦА ВИЖИНЕРА. КЛЮЧЕВОЕ СЛОВО - ЛЯГУШКА

Шифр замены - «шифр Цезаря с разными сдвигами»



К Р И П Т О Г Р А Ф И Я

Л Я Г У Ш К А Л Я Г У Ш

= ХПЛВКШГЫЯЧЫЧ под буквой Т стоит Ш, а пишем из таблицы К

Зашифруем пушкинскую прозу с помощью таблицы Вижинера, используя ключевое слово лягушка.

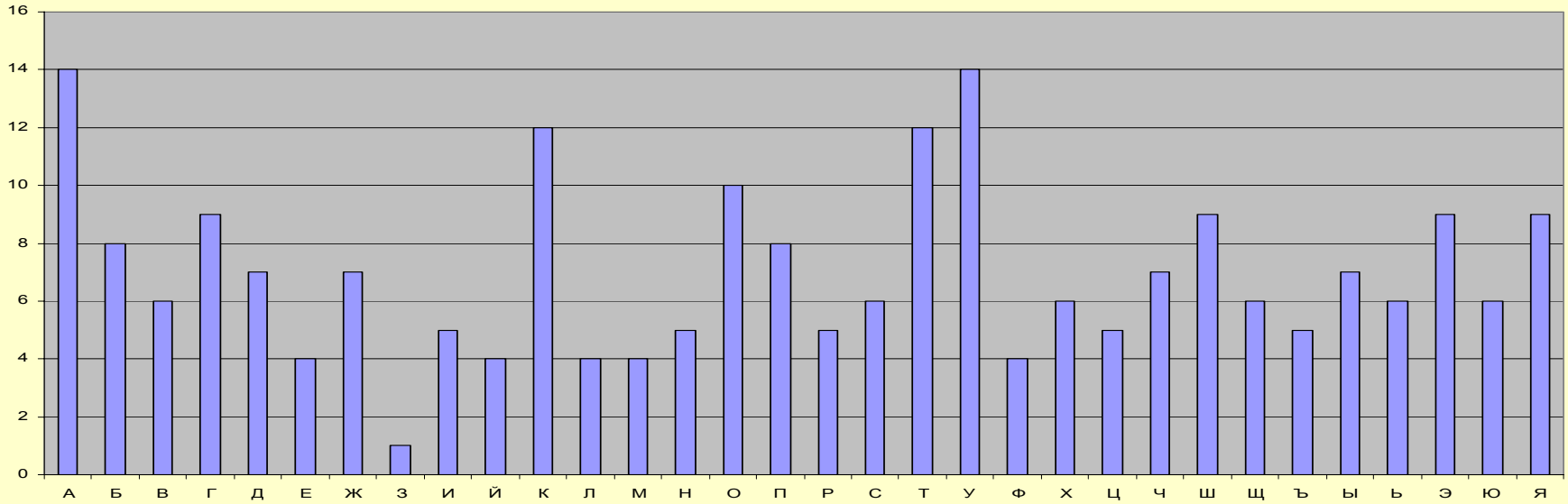
1	2	3	4	5	6	7	8	9	10	1	2	3	4	5	6	7	8	9	20	1	2	3	4	5	6	7	8	9	30	1	2	3
Л	Я	Г	У	Ш	К	А	Л	Я	Г	У	Ш	К	А	Л	Я	Г	У	Ш	К	А	Л	Я	Г	У	Ш	К	А	Л	Я			
Я	Е	Х	А	Л	Н	А	П	Е	Р	Е	К	Л	А	Д	Н	Ы	Х	И	З	Т	И	Ф	Л	И	С	А	В	С	Я			
К	Д	Ш	У	Г	Ч	А	Ь	Д	У	Ш	В	Х	А	П	М	Ю	И	А	С	Т	У	У	О	Ы	Й	К	В	Ъ	Ю			
Г	У	Ш	К	А	Л	Я	Г	У	Ш	К	А	Л	Я	Г	У	Ш	К	А	Л	Я	Г	У	Ш	К	А	Л	Я	Г	У	Ш	К	А
П	О	К	Л	А	Ж	А	М	О	Е	Й	Т	Е	Л	Е	Ж	К	И	С	О	С	Т	О	Я	Л	А	И	З	О	Д	Н	О	Г
Т	Б	В	Х	А	Р	Я	П	Б	Э	У	Т	Р	К	И	Щ	В	Т	С	Щ	Р	Х	Б	Ч	Х	А	У	Ж	С	Ч	Е	Ш	Г
Л	Я	Г	У	Ш	К	А	Л	Я	Г	У	Ш	К	А	Л	Я	Г	У	Ш	К	А	Л	Я	Г	У	Ш	К	А	Л	Я	Г	У	Ш
О	Н	Е	Б	О	Л	Ь	Ш	О	Г	О	Ч	Е	М	О	Д	А	Н	А	К	О	Т	О	Р	Ы	Й	Д	О	П	О	Л	О	В
Щ	М	И	Ф	Ж	Х	Ь	Г	Н	Ж	Б	П	П	М	Щ	Г	Г	А	Ш	Ф	О	Э	Н	У	О	Б	О	О	Ь	Н	О	Б	Ь
К	А	Л	Я	Г	У	Ш	К	А	Л	Я	Г	У	Ш	К	А	Л	Я	Г	У	Ш	К	А	Л	Я	Г	У	Ш	К	А	Л	Я	Г
И	Н	Ы	Б	Ы	Л	Н	А	Б	И	Т	П	У	Т	Е	В	Ы	М	И	З	А	М	Е	Т	К	А	М	И	О	Г	Р	У	З
Т	Н	Ж	А	Ю	Ю	Е	К	Ф	У	С	Т	Ж	К	П	В	Ж	Л	Л	Ь	Ш	Ц	Е	Э	Й	Г	Я	А	Ш	Г	Ы	Т	К
У	Ш	К	А	Л	Я	Г	У	Ш	К	А	Л	Я	Г	У	Ш	К	А	Л	Я	Г	У	Ш	К	А	Л	Я	Г	У	Ш	К	А	Л
И	И	Б	О	Л	Ь	Ш	А	Я	Ч	А	С	Т	Ь	И	З	Н	И	Х	К	С	Ч	А	С	Т	И	Ю	Д	Л	Я	В	А	С
Ы	А	Л	О	Ц	Щ	Ы	У	Ч	Б	А	Ъ	С	Э	А	Я	Ч	И	А	Й	Ф	К	Ш	Ы	Т	У	Э	З	Ю	Ч	М	А	Ъ
Я	Г	У	Ш	К	А	Л	Я	Г	У	Ш	К	А	Л	Я	Г	У	Ш	К	А	Л	Я	Г	У	Ш	К	А	Л	Я	Г	У	Ш	К
П	О	Т	Е	Р	Я	Н	А	А	Ч	Е	М	О	Д	А	Н	С	О	С	Т	А	Л	Ь	Н	Ы	М	И	В	Е	Щ	А	М	И
О	С	Е	Э	Ь	Я	Ш	Я	Г	К	Э	Ц	О	П	Я	Р	Д	Ж	Ы	Т	Л	К	Э	А	У	Ц	И	Н	Д	Ъ	У	Д	Т
А	Л	Я	Г	У	Ш	К	А	Л	Я	Г	У	Ш	К	А	Л	Я	Г	У	Ш	К	А	Л	Я	Г	У	Ш	К	А				
К	С	Ч	А	С	Т	И	Ю	Д	Л	Я	М	Е	Н	Я	О	С	Т	А	Л	С	Я	Ц	Е	Л	А	С	П	П				
К	Ъ	Ц	Г	Д	К	Т	Ю	П	К	В	Я	Э	Ч	Я	Щ	Р	Х	У	Г	Ы	Я	Б	Д	О	У	Й	Ш	П				
1	2	3	4	5	6	7	8	9	10	1	2	3	4	5	6	7	8	9	20	1	2	3	4	5	6	7	8	9	30	1	2	3

Шифровка отрывка из «Путешествия в Арзрум»

КДШУГДА ЬДУШВХА ПМЮЧАСТ УУОЫЙКВ ЪЮТБВХА РЯПБЭУТ
РКИЩВТС ЩРХБЧХА УЖСЧЕШТ ЩМИФЖХЬ ГНЖБППМ ЩГГАШФО
ЭНУОБОО ЬНОБЬТН ЖАЮЮЕКФ УСТЖКПВ ЖЛЛЬШЦЕ ЭЙГЯАШГ
ЫТКЫАЛО ЦЩЫУЧБА ЪСЭАЯЧИ АЙФКШЫТ УЭЗЮЧМА ЪОСЕЭЬЯ
ШЯГКЭЦО ПЯРДЖЫТ ЛКЭАУЦИ НДЪУДТК ЪЦГДКТЮ ПКВЯЭЧЯ
ЩРХУГЫЯ БДОУЙШП «Лягушка»

Усложненный шифр Цезаря: - шифрование текста с различными сдвигами букв алфавита, с использованием ключевого слова «лягушка», приводит к сглаживанию гистограммы. Поэтому так просто, как при одиночном сдвиге букв алфавита, это послание не расшифровать.

Частотная гистограмма шифросимволов Пушкинской прозы



Мои шифры

<u>1. Шифровальная таблица</u> выполнена мной на основе «квадрата Полибия»: - «Моя недостроенная пирамида». Сообщения шифруются числом, у которого первая цифра определяет столбец таблицы, а вторая – номер строки. На пересечении секретная буква. Например, 33 – c; 73 – u; 41 – o …

5					**e**	**j**				
4				d	i	n	r			
3			c	h	m	q	u	x		
2		b	g	l	p	t	w	z	,	
1	a	f	k	o	s	v	y	.	!	?
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**

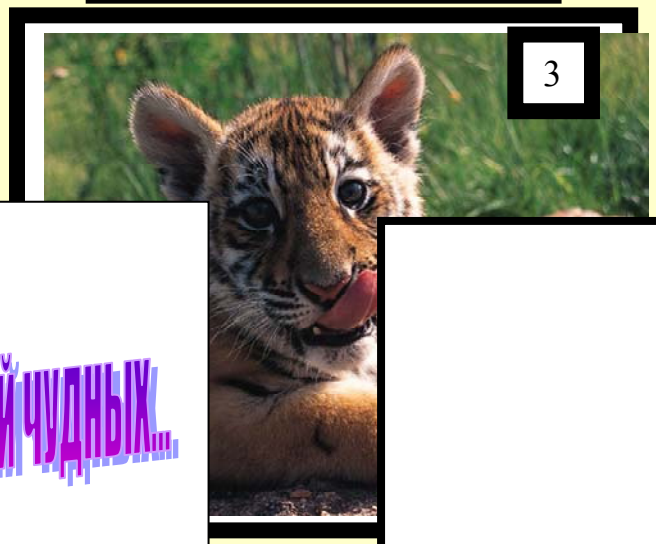
Например, **337341443354624121546292335462415255745462 81**

- Cuod cito fit, cito perit – Что быстро делается, то быстро и погибает.

2. Тайнопись

«Любите книгу - источник знаний!»

Зашифрованный текст спрятан в микроточке под несколькими слоями белой бумаги и посторонней информации.



2

КАК МНОГО НАМ ОТКРЫТИЙ ЧУДНЫХ...

1

3. Шифрование с ключом

Microsoft Excel - Шифратор.xls

R1C1 = ЛЮБЛЮОТЧИЗНУЯНОСТРАННОЮЛЮБОВЬЮ

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33
1	ЛЮБЛЮОТЧИЗНУЯНОСТРАННОЮЛЮБОВЬЮ																																
2	6	12	26	29	1	9	7	3	8	2	4	10	5	13	16	19	11	18	15	14	17	20	30	25	28	21	23	27	22	24			
3	О	У	Б	Ь	Л	И	Т	Б	Ч	Ю	Л	З	Ю	Я	С	А	Н	Р	О	Н	Т	Н	Ю	Ю	В	Н	Ю	О	О	Л			
4																																	
5																																	
6																																	
7																																	
8																																	
9																																	
10																																	
11																																	
12																																	
13																																	
14																																	
15																																	
16																																	
17																																	
18																																	
19																																	
20																																	
21																																	

Лист1 / Лист2 / Лист3

Готово NUM

Пуск | Total Commande... | [2] Total Comma... | Microsoft Power... | Документ2 - Mic... | Microsoft Exce... | RU | 11:32

Microsoft Excel - КЛЮЧ30.xls

Файл Правка Вид Вставка Формат Сервис Данные Окно Справка Adobe PDF

Arial Cyr 10

R4C1 = 1

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36
1	6	12	26	29	1	9	7	3	8	2	4	10	5	13	16	19	11	18	15	14	17	20	30	25	28	21	23	27	22	24						
2	Ю	У	Б	Ь	Л	И	Т	Б	Ч	Ю	Л	З	Ю	Я	С	А	Н	Р	О	Н	Т	Н	Ю	Ю	В	Н	Ю	О	О	Л						
3																																				
4	1	Л																																		
5	2	Ю																																		
6	3	Б																																		
7	4	Л																																		
8	5	Ю																																		
9	6	О																																		
10	7	Т																																		
11	8	Ч																																		
12	9	И																																		
13	10	З																																		
14	11	Н																																		
15	12	У																																		
16	13	Я																																		
17	14	Н																																		
18	15	О																																		
19	16	С																																		
20	17	Т																																		
21	18	Р																																		
22	19	А																																		
23	20	Н																																		
24	21	Н																																		
25	22	О																																		
26	23	Ю																																		
27	24	Л																																		
28	25	Ю																																		
29	26	Б																																		

Лист1 Лист2 Лист3

Готово Цикл: R2C1 Сумма=465 NUM

Пуск [2] Total Commander 6.... Microsoft PowerPoint - [... Документ3 - Microsoft ... Microsoft Excel - КЛ... RU 11:49

Принцип работы «шифрования с ключом»

Шифрованное послание: **ОУБЬЛИТБЧЮЛЗЮЯСАНРОНТНЮЮВНЮООЛ**

Создадим шифр с ключом длиной равной 30. Для этого нам понадобится любой компьютер с установленным на нем MS Excel. Сначала настроим параметры листа Excel. Установим стиль ссылок R1C1. (Для этого выберем в главном меню пункт “Сервис” - “Параметры...” и на вкладке “Общие” выберем “Стиль ссылок” R1C1).

В ячейку R1C1 вводим исходный текст:

ЛЮБЛЮОТЧИЗНУЯНОСТРАННОЮЛЮБОВЬЮ

В ячейки R2C1, ..., R2C30 второй строки вводим в произвольном порядке все целые числа от 1 до 30. Эта случайная перестановка чисел и является ключом.

В ячейку R3C1 вводим формулу =ПСТР(R1C1,R2C,1,1). (Наименование функции “ПСТР” следует набирать русскими буквами). Это функция работы с текстовыми данными – пересортировать.

Вводим ту же формулу и в ячейки R3C2, ..., R3C30. (Это можно сделать одним легким движением мыши: выделив ячейку R3C1, устанавливаем курсор на маленький черный квадрат в углу этой ячейки и тянем вправо до ячейки R3C30.)

Всё! В 3-й строке получим зашифрованный текст (по одной букве в 30 ячейках).

Если в ячейку R1C1 ввести другой исходный текст, то в 3-й строке автоматически появится новый шифрованный текст.

Для того чтобы обмениваться с кем-нибудь секретной информацией, надо скрытно передать этому абоненту выбранный вами секретный ключ. Получатель на своем компьютере должен аналогично настроить параметры листа Excel своего файла и ввести полученный ключ в ячейки R1C1, ..., R1C30.

Расшифровка криптограммы выполняется следующим образом:

Зашифрованный текст вводится посимвольно в ячейки R2C1, ..., R2C30 второй строки непосредственно под ключом.

Выделяется диапазон ячеек, в которых записаны ключ и символы шифротекста.

Выделенный диапазон копируется.

Щелкнув правой кнопкой мыши на ячейке R4C1, выбирается из появившегося контекстного меню команда “Специальная вставка...”.

В появившемся диалоговом окне “Специальная вставка” устанавливается флажок “транспонировать” и нажимается кнопка OK.

Вставленный диапазон ячеек сортируется (для этого надо, не снимая выделения с указанного диапазона ячеек, щелкнуть кнопку “Сортировка по возрастанию” на панели инструментов “Стандартная”).

Во второй колонке сверху вниз (начиная с 4-й строки) можно прочесть расшифрованный текст.

Рассмотренный шифр классифицируется как блочный шифр простой перестановки с длиной блока N=30 и длиной ключа, равной 30.

Если в исходном тексте количество символов больше N, то надо предварительно разбить его на блоки по N символов в каждом и затем шифровать каждый блок в отдельности. То же относится и к расшифровке.

Криптостойкость созданного шифра:

Учитывая, что количество перестановок из 30 символов равно 30!, можно было бы предположить, что полный перебор на таком множестве ключей затруднен. Тем не менее современные методы криптоанализа позволяют вскрыть многие шифры, и не перебирая всех возможных комбинаций. Вообще говоря, очень трудно придумать шифр, который нельзя было бы вскрыть другим более эффективным способом.

Если вы хотите, чтобы ваш шифр очень сложно было взломать, надо:

- чаще менять ключ (желательно, каждый сеанс);
- не допускать перехвата ключа;
- не оставлять на винчестере или дискете копию исходного текста;
- вводить исходный текст без пробелов, в одном регистре (только верхнем или только нижнем);
- (Вскрывать ваши криптограммы будет сложно еще и в том случае, если у вас по орфографии была двойка).

4. Массив шифрованной информации (Ход конем)

Е И А Д Х Л Т А
П Е Л Т К Г И О
Н С Ы И М Х Л Е
Т А Ы О К Л О К
С Ы А Ц Н К В Ц
Ж Е Й А О В А Л
Г К Ы М В А О Е
Т И Д Д Р Н Е К

Зашифрованный текст

	A	B	C	D	E	G	H	F
8	Е	И	А	Д	Х	Л	Т	А
7	П	Е	Л	Т	К	Г	И	О
6	Н	С	Ы	И	М	Х	Л	Е
5	Т	А	Ы	О	К	Л	О	К
4	С	Ы	А	Ц	Н	К	В	С
3	Ж	Е	Й	А	О	В	А	Л
2	Г	К	Ы	М	В	А	О	Е
1	Т	И	Д	Д	Р	Н	Е	К

Подсказка для первого хода **А4**

	A	B	C	D	E	G	H	F
8	3[4]	•	3[4]	•	•	•	•	•
7	•	3[3]	•	3[3,4]	•	•	•	•
6	3[5]	2[4]	•	•	3[3]	•	•	•
5	•	3[2]	2[3]	3[2,4]	•	•	•	•
4	1	•	3[1,4]	•	3[2,3]	•	•	•
3	•	3[3]	2[2]	3[1,3]	•	•	•	•
2	3[2]	2[1]	•	•	3[2]	•	•	•
1	•	3[2]	•	3[1,2]	•	•	•	•

Начальные ходы

Подсказка - строчка зашифрованного текста - ТЫ УКРАШЕНИЕМ БЫЛА?

	A	B	C	D	E	G	H	F
8	17	20	13	34	47	50	11	32
7	14	35	16	19	12	33	46	49
6	21	18	37	62	51	48	31	10
5	36	15	64	57	54	61	52	45
4	1	22	3	38	63	56	9	30
3	4	25	58	55	60	53	44	41
2	23	2	27	6	39	42	29	8
1	26	5	24	59	28	7	40	43

«Ветка» - В13 – ветка, дающая решение задачи

В 1759 году знаменитому математику Леонарду Эйлеру удалось найти замкнутый маршрут обхода всех клеток шахматной доски ходом коня ровно один раз и последним 65-м ходом вернуться в точку начала маршрута. Великий Леонард Эйлер посвятил этой задаче большой труд – «Решение одного любопытного вопроса, который, кажется, не подчиняется никакому исследованию».

Я не знаю с какой точки начал свой исторический обход Эйлер. Но я могу с помощью распространенной компьютерной игрушки «ход конем» - «Путешествия коня» успешно осуществить обход досок различных размеров, делая первый ход из любой клетки. И таким образом наглядно показать сложности раскрытия тайного послания. Конечно, матерый дешифровальщик первым делом произведет частотный анализ символов текста и, возможно, вообще не будет решать шахматную задачу. А ленивый криптоаналитик скорее всего заставит какую - нибудь поисковую систему найти подобное тексту «… ТЫ УКРАШЕНИЕМ БЫЛА?» , а мы посмотрим начало шахматного пути:

шаги	1	2	3а	3б	3в	3г	3д	3е	3ж	
Вар.1	**A4**	**B2**	**D1**	**D3**	**C4**	-	-	-	-	ПОЛЕ
	С	К	Д	А	А					БУКВА
Вар.2	**A4**	**C3**	**A2**	**B1**	**D1**	**E2**	**E4**	**D5**	**B5**	ПОЛЕ
	С	Й	Г	И	Д	В	Н	О	А	БУКВА
Вар.3	**A4**	**C5**	**B3**	**D3**	**E4**	**E6**	**D7**	**B7**	**A6**	ПОЛЕ
	С	Ы	Е	А	Н	М	Т	Е	Н	БУКВА
Вар.4	**A4**	**B6**	**C4**	**D5**	**D7**	**C8**	**A8**	-	-	ПОЛЕ
	С	С	А	О	Т	А	Е			БУКВА

Вариант 1 – три маршрута после второго хода «СКД…», «СКА…» и «СКА..».
Вариант 2 – семь маршрутов после второго хода «СЙГ…», «СЙИ…», «СЙД…», «СЙВ…», «СЙН…», «СЙО…», «СЙА…».
Вариант 3 – семь маршрутов после второго хода «СЫЕ…», «СЫА…», «СЫН…», «СЫМ…», «СЫТ…», «СЫЕ…», «СЫН…».
Вариант 4 – пять маршрутов после второго хода «ССА…», «ССО…», «ССТ…», «ССА…», «ССЕ…».

Видно, что с каждым ходом количество маршрутов и ответвлений будет увеличиваться. Поэтому, сделав начальные ходы (разумные маршруты подчеркнуты), будем запускать программу игры «ход конем», чтобы найти решение задачи и расшифровать послание.

После ходов коня «A4-B2-C4-A3-B1-D2-G1-F2…» программой найдено решение.

Осталось полученное решение занести в таблицу, где вместо координат шахматных полей поставить соответствующие буквы.

В процессе расшифровки были рассмотрены 22 маршрута обхода шахматной доски конем (для перебора вариантов использовалась программа «Путешествие коня»). Среди них 18 некорректных решений - 65-ход не возвращает коня на поле А4 или «улучшенное» решение обрывается на 62 ходу.

B11

	A	B	C	D	E	G	H	F
8	45	40	43	18	47	14	11	16
7	42	19	46	53	62	17	48	13
6	39	44	41	58	51	12	15	10
5	20	59	52	63	54	61	32	49
4	1	38	55	60	57	50	9	34
3	24	21	26	37	64	33	6	31
2	27	2	23	56	29	4	35	8
1	22	25	28	3	36	7	30	5

B44

	A	B	C	D	E	G	H	F
8	•	22	3	26	19	30	33	28
7	4	25	20	61	50	27	18	31
6	21	2	23	48	57	32	29	34
5	24	5	60	51	62	49	58	17
4	1	52	47	56	59	54	35	•
3	6	41	44	53	36	11	16	13
2	43	46	39	8	55	14	37	10
1	40	7	42	45	38	9	12	15

Решения аналогичные B11: - B21, B22, B23, B24, B26, B27, B31, B33, B34, B35, B36, B37, B45.

Решения аналогичные B44: - B41, B42, B43.

Верные решения, кроме «Ветки»(B13): - версии B12, B25, B32.

B12

	A	B	C	D	E	G	H	F
8	31	8	29	26	33	10	13	16
7	28	25	32	9	56	15	34	11
6	7	30	27	54	61	12	17	14
5	24	47	64	57	52	55	62	35
4	1	6	53	60	63	58	51	18
3	46	23	48	3	50	41	36	39
2	5	2	21	44	59	38	19	42
1	22	45	4	49	20	43	40	37

Абракадабра

ШАГИ	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**
ПОЛЕ	A4	B2	D3	C1	A2	B4	A6	B8	D7	G8	F7
БУКВА	**С**	**К**	**А**	**Д**	**Г**	**Ы**	**Н**	**И**	**Т**	**Л**	**О**
ШАГИ	**12**	**13**	**14**	**15**	**16**	**17**	**18**	**19**	**20**	**21**	**22**
ПОЛЕ	G6	H8	F6	G7	F8	H6	F4	H2	E1	C2	A1
БУКВА	**Х**	**Т**	**Е**	**Г**	**А**	**Л**	**С**	**О**	**Р**	**Ы**	**Т**
ШАГИ	**23**	**24**	**25**	**26**	**27**	**28**	**29**	**30**	**31**	**32**	**33**
ПОЛЕ	B3	A5	B7	D8	C6	A7	C8	B6	A8	C7	E8
БУКВА	**Е**	**Т**	**Е**	**Д**	**Ы**	**П**	**А**	**С**	**Е**	**Л**	**Х**
ШАГИ	**34**	**35**	**36**	**37**	**38**	**39**	**40**	**41**	**42**	**43**	**44**
ПОЛЕ	H7	F5	H3	F1	G2	F3	H1	G3	F2	G1	D2
БУКВА	**И**	**К**	**А**	**К**	**А**	**Л**	**Е**	**В**	**Е**	**Н**	**М**
ШАГИ	**45**	**46**	**47**	**48**	**49**	**50**	**51**	**52**	**53**	**54**	**55**
ПОЛЕ	B1	A3	B5	C3	D1	E3	H4	E5	C4	D6	G5
БУКВА	**И**	**Ж**	**А**	**Й**	**Д**	**О**	**Р**	**К**	**А**	**И**	**Л**
ШАГИ	**56**	**57**	**58**	**59**	**60**	**61**	**62**	**63**	**64**	**65**	
ПОЛЕ	E7	D5	G4	E2	D4	E6	H5	E4	C5	A4	
БУКВА	**К**	**О**	**К**	**В**	**Ц**	**М**	**О**	**Н**	**Ы**	*	

B25

	A	B	C	D	E	G	H	F
8	35	14	33	30	37	16	41	20
7	32	29	36	15	52	19	38	17
6	13	34	31	50	63	40	21	42
5	28	49	64	53	60	51	18	39
4	1	12	59	62	3	54	43	22
3	48	27	2	55	58	61	4	7
2	11	56	25	46	9	6	23	44
1	26	47	10	57	24	45	8	5

Абракадабра

ШАГИ	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**
ПОЛЕ	A4	C3	E4	H3	F1	G2	F3	H1	E2	C1	A2
БУКВА	**С**	**Й**	**Н**	**А**	**К**	**А**	**Л**	**Е**	**В**	**Д**	**Г**
ШАГИ	**12**	**13**	**14**	**15**	**16**	**17**	**18**	**19**	**20**	**21**	**22**
ПОЛЕ	B4	A6	B8	D7	G8	F7	H5	G7	F8	H6	F4
БУКВА	**Ы**	**Н**	**И**	**Т**	**Л**	**О**	**О**	**Г**	**А**	**Л**	**С**
ШАГИ	**23**	**24**	**25**	**26**	**27**	**28**	**29**	**30**	**31**	**32**	**33**
ПОЛЕ	H2	E1	C2	A1	B3	A5	B7	D8	C6	A7	C8
БУКВА	**О**	**Р**	**Ы**	**Т**	**Е**	**Т**	**Е**	**Д**	**Ы**	**П**	**А**
ШАГИ	**34**	**35**	**36**	**37**	**38**	**39**	**40**	**41**	**42**	**43**	**44**
ПОЛЕ	B6	A8	C7	E8	H7	F5	G6	H8	F6	H4	F2
БУКВА	**С**	**Е**	**Л**	**Х**	**И**	**К**	**Х**	**Т**	**Е**	**Р**	**Е**
ШАГИ	**45**	**46**	**47**	**48**	**49**	**50**	**51**	**52**	**53**	**54**	**55**
ПОЛЕ	G1	D2	B1	A3	B5	D6	G5	E7	D5	G4	D3
БУКВА	**Н**	**М**	**И**	**Ж**	**А**	**И**	**Л**	**К**	**О**	**К**	**А**
ШАГИ	**56**	**57**	**58**	**59**	**60**	**61**	**62**	**63**	**64**	**65**	
ПОЛЕ	B2	D1	E3	C4	E5	G3	D4	E6	C5	A4	
БУКВА	**К**	**Д**	**К**	**А**	**К**	**В**	**Ц**	**М**	**Ы**	*	

B32

	A	B	C	D	E	G	H	F
8	37	34	15	30	51	40	13	28
7	16	31	36	39	14	29	52	41
6	35	38	33	62	55	50	27	12
5	32	17	2	49	58	61	42	53
4	1	48	59	56	63	54	11	26
3	18	21	64	3	60	57	8	43
2	47	4	23	20	45	6	25	10
1	22	19	46	5	24	9	44	7

Абракадабра

ШАГИ	1	2	3	4	5	6	7	8	9	10	11
ПОЛЕ	A4	C5	D3	B2	D1	G6	F1	H3	G1	F2	H4
БУКВА	**С**	**Ы**	**А**	**К**	**Д**	**Х**	**К**	**А**	**Н**	**Е**	**Р**
ШАГИ	12	13	14	15	16	17	18	19	20	21	22
ПОЛЕ	F6	H8	E7	C8	A7	B5	A3	B1	D2	B3	A1
БУКВА	**Е**	**Т**	**К**	**А**	**П**	**А**	**Ж**	**И**	**М**	**Е**	**Т**
ШАГИ	23	24	25	26	27	28	29	30	31	32	33
ПОЛЕ	C2	E1	H2	F4	H6	F8	G7	D8	B7	A5	C6
БУКВА	**Ы**	**Р**	**О**	**С**	**Л**	**А**	**Г**	**Д**	**Е**	**Т**	**Ы**
ШАГИ	34	35	36	37	38	39	40	41	42	43	44
ПОЛЕ	B8	A6	C7	A8	B6	D7	G8	F7	H5	F3	H1
БУКВА	**И**	**Н**	**Л**	**Е**	**С**	**Т**	**Л**	**О**	**О**	**Л**	**Е**
ШАГИ	45	46	47	48	49	50	51	52	53	54	55
ПОЛЕ	E2	C1	A2	B4	D5	G6	E8	H7	F5	G4	E6
БУКВА	**В**	**Д**	**Г**	**Ы**	**О**	**Х**	**Х**	**И**	**К**	**К**	**М**
ШАГИ	56	57	58	59	60	61	62	63	64	65	
ПОЛЕ	D4	G3	E5	C4	E3	G5	D6	E4	C3	A4	
БУКВА	**Ц**	**В**	**К**	**А**	**О**	**Л**	**И**	**Н**	**Й**	*	

Секретным посланием оказался фрагмент стихотворения М.Ю. Лермонтова «Ветка Палестины»:

	A	B	C	D	E	G	H	F
8	17	20	13	34	47	50	11	32
7	14	35	16	19	12	33	46	49
6	21	18	37	62	51	48	31	10
5	36	15	64	57	54	61	52	45
4	1	22	3	38	63	56	9	30
3	4	25	58	55	60	53	44	41
2	23	2	27	6	39	42	29	8
1	26	5	24	59	28	7	40	43

«Скажи мне, ветка Палестины,
Где ты росла, где ты цвела,
Каких холмов, какой долины
Ты украшением была»

ШАГИ	1	2	3	4	5	6	7	8	9	10	11
ПОЛЕ	A4	B2	C4	A3	B1	D2	G1	F2	H4	F6	H8
БУКВА	**С**	**К**	**А**	**Ж**	**И**	**М**	**Н**	**Е**	**В**	**Е**	**Т**
ШАГИ	12	13	14	15	16	17	18	19	20	21	22
ПОЛЕ	E7	C8	A7	B5	C7	A8	B6	D7	B8	A6	B4
БУКВА	**К**	**А**	**П**	**А**	**Л**	**Е**	**С**	**Т**	**И**	**Н**	**Ы**
ШАГИ	23	24	25	26	27	28	29	30	31	32	33
ПОЛЕ	A2	C1	B3	A1	C2	E1	H2	F4	H6	F8	G7
БУКВА	**Г**	**Д**	**Е**	**Т**	**Ы**	**Р**	**О**	**С**	**Л**	**А**	**Г**
ШАГИ	34	35	36	37	38	39	40	41	42	43	44
ПОЛЕ	D8	B7	A5	C6	D4	E2	H1	F3	G2	F1	H3
БУКВА	**Д**	**Е**	**Т**	**Ы**	**Ц**	**В**	**Е**	**Л**	**А**	**К**	**А**
ШАГИ	45	46	47	48	49	50	51	52	53	54	55
ПОЛЕ	F5	H7	E8	G6	F7	G8	E6	H5	G3	E5	D3
БУКВА	**К**	**И**	**Х**	**Х**	**О**	**Л**	**М**	**О**	**В**	**К**	**А**
ШАГИ	56	57	58	59	60	61	62	63	64	65	
ПОЛЕ	G4	D5	C3	D1	E3	G5	D6	E4	C5	A4	
БУКВА	**К**	**О**	**Й**	**Д**	**О**	**Л**	**И**	**Н**	**Ы**	*	

Спасибо за внимание, помощь и поддержку!

41924454555352741155334211747353 91