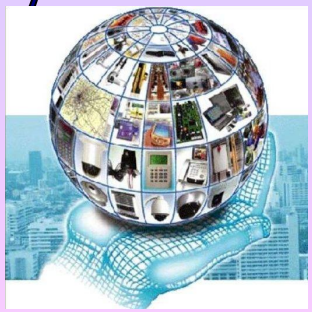
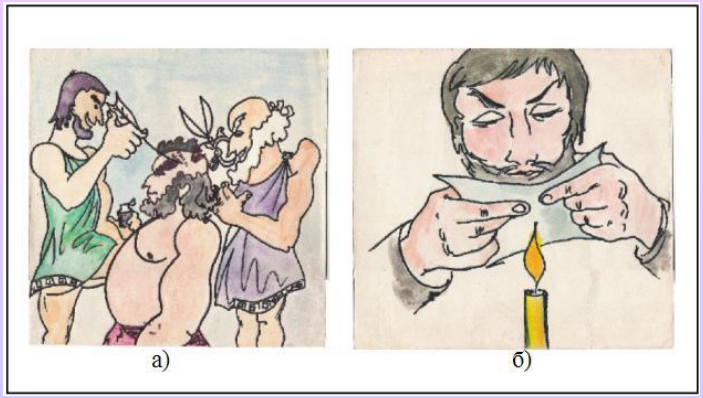
Тайна за семью печатями

Выполнил : Станишевский Данил 9-в класс

Кто владеет информацией, тот владеет миром

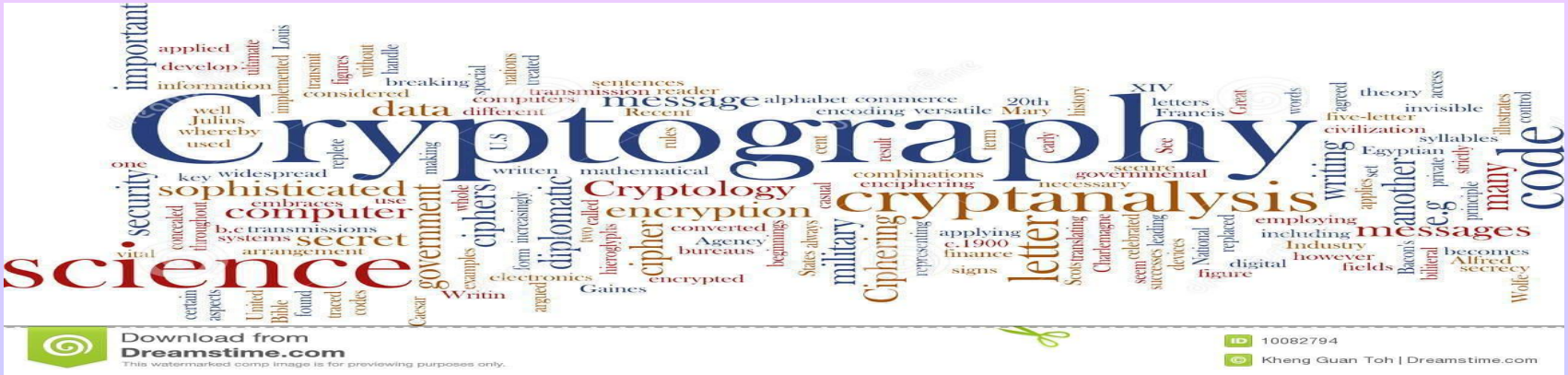
Люди очень давно осознали, что информация имеет ценность. Тысячи лет короли, королевы и полководцы управляли своими странами и командовали своими армиями, опираясь на надежно и эффективно действующую связь. В то же время все они осознавали последствия того, что произойдет, если их сообщения попадут не в те руки, если вражескому государству будут выданы ценные секреты, а жизненно важная информация окажется у противника.





Рассказывают, как один царь обрил голову гонца, написал на ней послание и отослал гонца к союзнику лишь тогда, когда волосы его на голове отросли. Развитие химии дало удобное средство тайнописи: симпатические чернила, записи которыми не видны до тех пор, пока бумагу не нагреют или обработают каким-нибудь химикатом.

Криптография (от греч.)– наука о методах шифрования информации с целью её защиты от незаконных пользователе. 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. Другой американец — Флетчер Пратт в своей книге «История шифров и кодов» дает такое определение криптографии: «Криптография – искусство шифрования — это процесс выражения слов, передающих смысл только немногим лицам, которым известен этот секрет». Из подобного определения следует, что всякое письмо, написанное на неизвестном для того или иного человека языке, является шифрованным письмом, то есть любой алфавит может стать шифром.



Цель проекта: Познакомиться с основными понятиями криптографии и некоторыми шифрами прошедших веков и узнать, каким образом происходит шифрование с помощью этих шифров.

Задачи:

Изучить учебную литературу по данной теме

Рассмотреть различные способы шифрования текстов.

Расширить кругозор сверстников, развить их познавательную активность, познакомив с тайными шифрами.

Показать практическую значимость криптографии

Гипотеза: Без тайн не могут нормально существовать не только государства, но и группы простых людей - без них нельзя выиграть сражение или выгодно продать товар, одолеть своих политических противников в жесткой борьбе за власть или сохранить первенство в технологии.

Методы исследования:

Изучение литературы

Опрос

Основной принцип шифрования в древности

Атбаш

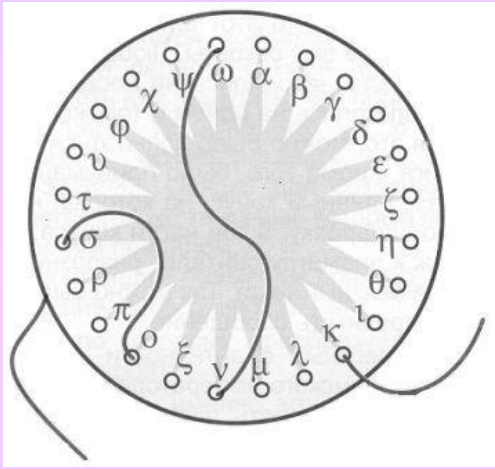
Некоторые фрагменты библейских текстов зашифрованы с помощью шифра, который назывался атбаш. Правило зашифрования состояло в замене i-й буквы алфавита буквой с номером n − i + 1, где n — число букв в алфавите. Происхождение слова атбаш объясняется принципом замены букв. Это слово составлено из букв Алеф, Тае, Бет, Шит, то есть первой и последней, второй и предпоследней букв древнесемитского алфавита.

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

Шифр атбаш

Табличка Энея

На небольшой табличке горизонтально располагался алфавит, а по ее боковым сторонам имелись выемки для наматывания нити. При зашифровании нить закреплялась у одной из сторон таблички и наматывалась на нее. На нити делались отметки (например, узелки) в местах, которые находились напротив букв данного текста. По алфавиту можно было двигаться лишь в одну сторону, то есть делать по одной отметке на каждом витке. После зашифрования нить сматывалась и передавалась адресату. Этот шифр представляет собой шифр замены букв открытого текста знаками, которые означали расстояния между отметками на нити. Ключом являлись геометрические размеры таблички и порядок расположения букв алфавита. Это был довольно надежный шифр, история не сохранила документов, подтверждающих сведения о методах его вскрытия

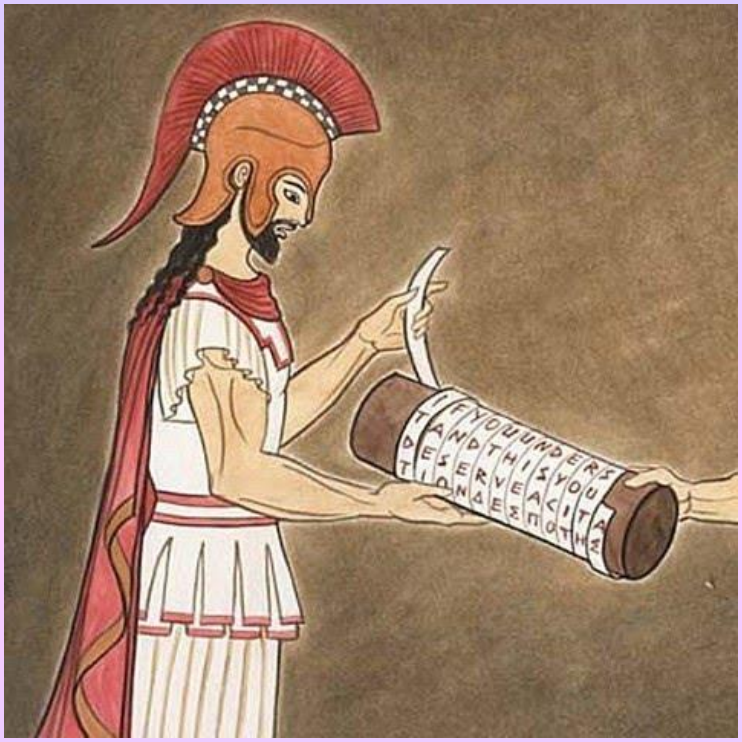


Скитала

"Скитала"(сцитала).

Его способ заменять одну букву другой встречался вплоть до наших времен.

На этот посох наматывалась по спирали полоска пергамента с зашифрованным посланием. Смысл такого «гаджета» был в том, что прочитать эту полоску мог лишь обладатель скиталы аналогичного размера. При правильном размере витка буквы послания совпадали, и получался связный текст. Устройство было очень простым и практичным, хотя особо надежным его назвать никак нельзя.

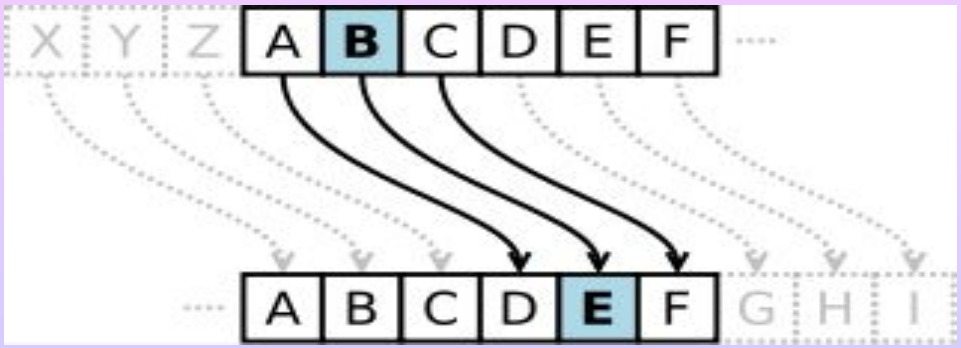


Шифр Цезаря

Шифр Цезаря — один из древнейших шифров. При шифровании каждый символ заменяется другим, отстоящим от него в алфавите на фиксированное число позиций. Шифр Цезаря можно классифицировать как шифр подстановки, при более узкой классификации — шифр простой замены.

Шифр назван в честь римского императора Гая Юлия Цезаря, использовавшего его для секретной переписки.

Например, шифрование с использованием ключа $k = 3$. Буква С «сдвигается» на три буквы вперед и становится буквой «Ф». Твердый знак, перемещённый на три буквы вперед, становится буквой «э», и так далее.

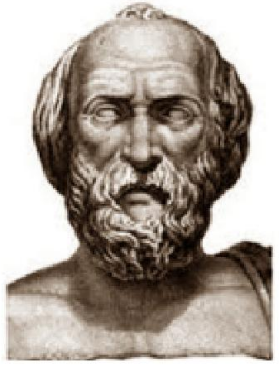


Квадрат Полибия

Греческий писатель Полибий использовал систему сигнализации, которая была широко принята как метод шифрования. Он записывал буквы алфавита в квадратную таблицу и заменял их координатами: парами чисел (i, j), где i — номер строки, j — номер столбца. Применительно к латинскому алфавиту квадрат Полибия имеет следующий вид.

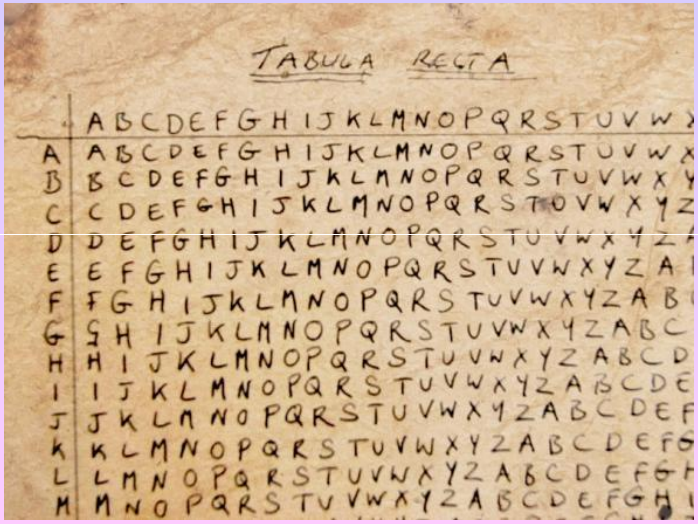
Пары (i, j) передавались с помощью факелов. Например, для передачи буквы O нужно было взять 3 факела в правую руку и 4 факела — в левую.

КВАДРАТ ПОЛИБИЯ



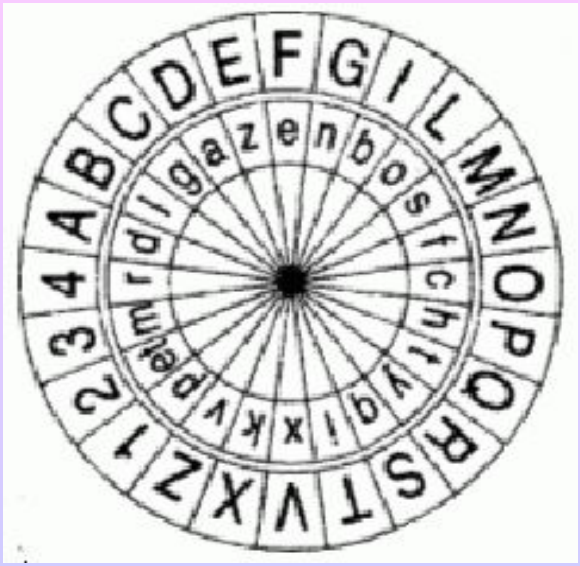
θ	μ	β	φ	ρ
ε	ς	λ	ο	δ
ψ	α	σ	ζ	υ
π		ι	ω	κ
η	ξ	χ	γ	τ

Шифр Виженера

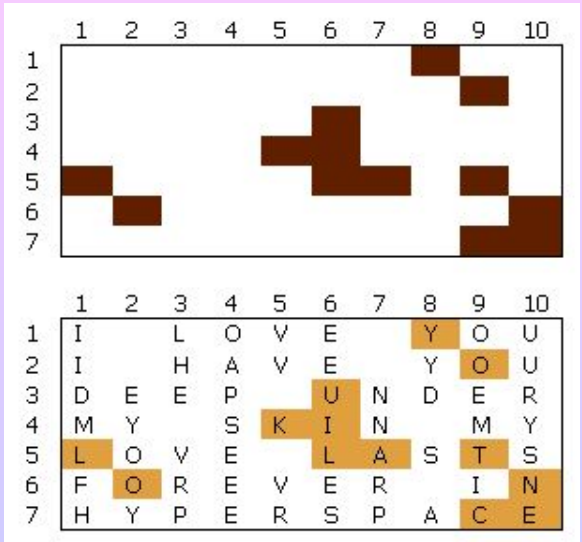


Линейка Сен-Сира

Шифровальный диск



Поворотная решетка



Зарождение русской тайнописи

Появление в России первых специалистов-тайнописцев, находящихся на государственной службе, следует отнести к 1549 г., ко времени образования Посольского приказа, осуществлявшего общее руководство внешней политикой страны. Именно в области дипломатии в России проходило становление криптографии как дела государственной значимости.

Как правило, она составлялась по одному из наиболее примитивных способов зашифровки, получивших название "тарабарской грамоты" либо литореи (от лат. litera - буквенный), в которой все гласные буквы оставались неизменными, а согласные заменялись одна другой по следующей схеме:

б	**в**	**г**	**д**	**ж**	**з**	**к**	**л**	**м**	**н**
щ	**ш**	**ч**	**ц**	**х**	**ф**	**т**	**с**	**р**	**п**

Символ открытого текста ищется в таблице и заменяется на символ шифрованного, который в том же столбце таблицы, но в другой строке. Если символа в таблице нет, то он никак не изменяется.

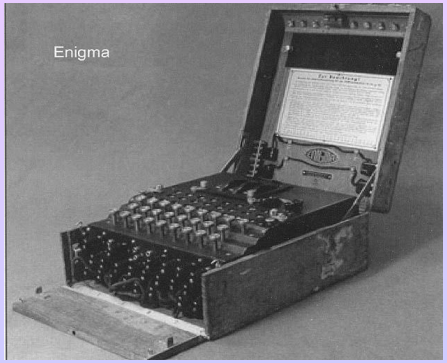
Например, вместо "Тайна покрытая семью печатями" получается "Кайпа нотмыкая лерью негакяри".

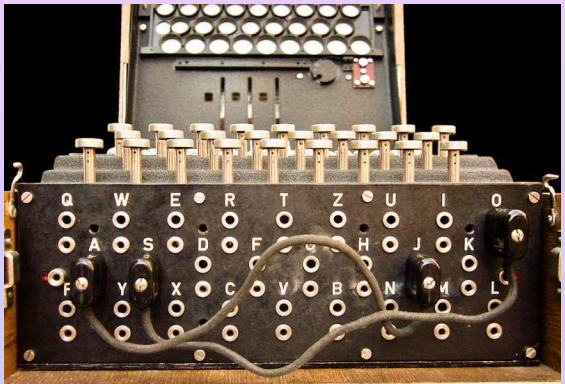
Современная криптография

Начало XX характеризуется внедрением электромеханических машин в работу шифровальщиков, таких, как Энигма.

Энигма состоит из комбинаций механических электрических систем: клавиатуры, набора вращающихся роторов, расположенных вдоль вала и прилегающих к нему, и ступенчатого механизма, двигающего один или более роторов при каждом нажатии клавиши.

На роторах располагаются контакты, соответствующие буквам в алфавите (обычно от A до Z). Сам ротор отвечает очень простому типу шифрования, т.е. элементарному шифру замены. Например, контакт, отвечающий за букву E, мог быть соединен с контактом буквы T на другой стороне ротора. Но при использовании нескольких роторов в связке получается более надёжное шифрование





Тайны до сих пор не раскрытые

Во дворе здания ЦРУ в Лэнгли стоит S-образная медная плита с зашифрованным текстом. Это самый известный элемент скульптуры «Криптос», её авторы — скульптор Джеймс Санборн и Эд Шейдт, отставной глава криптографического отдела ЦРУ. Они придумали шифр, разгадать который трудно, но вполне реально. По крайней мере, им так казалось.

По замыслу авторов, «Криптос» олицетворяет процесс сбора информации. Шифр «Криптоса» — 869 символов, поделённых на четыре части. Создатели предполагали, что на решение первых трёх частей уйдёт около семи месяцев, на решение всей задачи — примерно семь лет.

23 года спустя полной расшифровки всё ещё нет

2. Шифр Дорабеллы

14 июля 1897-го знаменитый английский композитор Эдвард Элгар отправил записку Дорабелле — так он называл свою подругу Дору Пенни. «Мисс Пенни», — гласила надпись на одной стороне карточки. На другой был трехстрочный шифр из 87 символов. Дора не смогла расшифровать послание, и оно пролежало в ящике её стола 40 лет, прежде чем его перепечатали в книге воспоминаний Пенни об Элгаре.

Расшифровывая письмо композитора, одни пытались обойтись простейшим методом замены символов на буквы, другие приходили к выводу, что здесь вообще скрыты не слова, а мелодия. У одних получались сообщения, в которых не понятно абсолютно ничего, у других — предельно лиричные тексты, полные мечтательности и любви. Окончательного решения нет до сих пор; ничем закончился и конкурс по расшифровке, проведённый в 2007-м в честь 150-летия Элгара

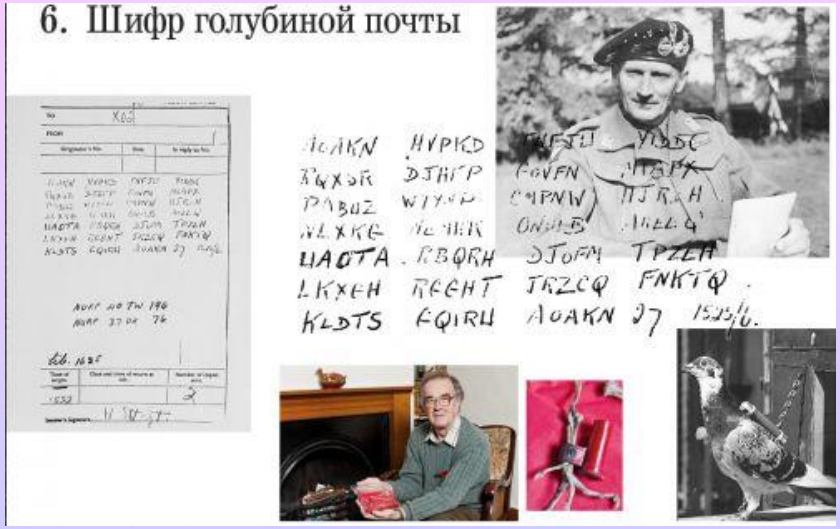
Через несколько дней Зодиак прислал ещё одно письмо, в котором зашифровал свое имя, — оно также осталось неразгаданным. Затем было письмо, в котором убийца угрожал взорвать школьный автобус. К нему он приложил карту и шифр — с их помощью якобы можно было найти бомбу, что планируется использовать для теракта. С этим шифром тоже никто не справился, но и взрыв не произошёл.

Убийца, про которого всё ещё ничего не известно, отправлял в калифорнийские газеты зашифрованные письма, обещая, что в них найдутся ключи к установлению его личности. Первое послание Зодиака (август 1969-го) состояло из трёх частей и 408 символов, быстрее всех его расшифровала обычная калифорнийская семейная пара. Смысл письма сводился к тому, что убивать людей гораздо интереснее, чем животных, ведь человек — самое опасное существо на планете. «Я попаду в рай, где те, кого я убил, станут моими рабами», — гласила записка.

Эта была последняя успешная попытка расшифровать криптограмму Зодиака. Тайной остаётся содержание открытки с кодом из 340 знаков, пришедшей три месяца спустя в редакцию San Francisco Chronicle. «Можете напечатать его на первой странице? Мне ужасно одиноко, когда меня не замечают», — просил убийца в сопутствующем письме.

В годы Второй мировой войны британская армия нередко использовала голубей для передачи зашифрованных посланий.
В 2012 году житель графства Суррей (юг Англии) нашёл в трубе своего дома останки птицы, к лапе которой был прикреплён контейнер с сообщением.

Изучив сообщение, эксперты Британского центра правительственной связи пришли к выводу, что без доступа к книгам кодов, использованных при создании шифра, найти правильное решение практически невозможно. «Подобные сообщения создавались так, чтобы их могли прочитать только отправитель и получатель. Если мы не узнаем хоть что-то о том, кто написал это письмо или кому оно предназначалось, мы не сможем его расшифровать», — заявил анонимный работник Центра правительственной связи в интервью BBC



Разработка собственного шифра

Изучив литературу по криптогафии и, рассмотрев основные правила замены, я захотела придумать собственный способ шифрования.

Он основывается на простом принципе замены, основанным на Шифре Цезаря.

Каждая буква русского алфавита заменяется другой, отстоящей от нее в алфавите на фиксированное число. Это число определяется ежедневно и соответствует числовой дате по календарю.

Например, вчера было 18 февраля, значит каждый символ смещается вперед на 18.

Таким образом, фраза «Тайна за семью печатями» имела вид: ЛЩГЖЩ БЩКУЧ ИЮРЩЛЦЕВ,
а сегодня 19 февраля - МЬДЗЬ ВЬЛФШ ЙЯСЬМЧЁГ

Заключение

Сегодня криптография засекречена не меньше, чем сопутствующие ей службы - военные, дипломатические, разведывательные - поэтому, естественно, многое остается скрытым под плотной завесой государственной тайны.

Считаю, что каждый человек, который пользуется компьютером, должен задумываться о том, что его информация может быть взломана и использована в корыстных целях (от рассылки спама с вашей электронной почты до скачивания паролей вашей банковской карты или другой важной информации). В таком случае, проблема защиты информации в настоящее время всё более и более возрастает в связи с развитием информационных технологий

История тайнописи в России, конечно, повидала на своем веку все, в том числе неудачи и успехи, разочарования и победы. Тем не менее, хотелось бы искренне надеяться, что в нынешнее время и в будущем криптографы России совершат и будут совершать все возможное и невозможное для выполнения перед ними ответственных задач, постоянно приумножая славу нашей страны.


Спасибо
за
внимание!