

Проект по информатике «Искусство шифрования»



Выполнили:

Смирнов Даниил, обучающийся 7б класса

Дзоц Артем, обучающийся 7 б класса

Руководитель:

учитель информатики Виноградов С.М.

Содержание

1.	Введение	3
2.	Криптография в древности	5
3.	Зарождение русской тайнописи	10
4.	Современная криптография	14
5.	Криптоанализ	15
6.	Тайны, которые до сих пор не раскрыты	16
7.	Разработка собственного шифра	19
8.	Заключение	20
9.	Использованные источники информации	21

Кто владеет информацией,

Введение.

Люди очень давно осознали, что информация имеет ценность. Тысячи лет короли, королевые 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.

И именно опасение того, что враги перехватят сообщение, послужило причиной активного развития кодов и шифров — способов скрытия содержания сообщения таким образом, чтобы прочесть его смог только тот, кому оно адресовано. Сначала ими пользовались пираты, отмечая расположение кладов, алхимики, купцы, заговорщики. впоследствии - дипломаты, стремящиеся сохранить тайны переговоров, военачальники, скрывающие от противника отданные распоряжения, разведчики и другие.

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 пользователей. 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.

Актуальность проекта обусловлена тем, что в наши дни информация приобрела коммерческую ценность и стала обычным товаром. Её продают и покупают, производят, хранят, транспортируют и, следовательно, воруют и подделывают. В результате возникла необходимость защиты важной информации. Поэтому криптография в современном мире информационных технологий особенно необходима.

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

Задачи:

1. Изучить учебную литературу по данной теме
2. Рассмотреть различные способы шифрования текстов.
3. Расширить кругозор сверстников, развить их познавательную активность, познакомив с тайными шифрами.
4. 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
-

Тип проекта: информационный

Форма проекта: индивидуальный

Криптография в Древности

Появление письменности стало одним из переломных моментов в истории человечества, дало мощный импульс к развитию знаний в самых разных областях. Но как

только человек понял, что может передавать свои мысли в виде графических символов, он тут же начал искать способы делать это тайно, чтобы лишь избранные могли прочесть написанное. Родились первые алгоритмы шифрования, а вместе с ними стали появляться и диковинные приспособления, которые служили ключом к пониманию зашифрованного текста.

Сама история криптографии насчитывает около 4-х тысяч лет.

Уже в исторических документах древних цивилизаций — Индии, Египта, Месопотамии — имеются сведения о системах и способах составления шифрованного письма.

В древнеиндийских рукописях приводится более 60 способов письма. Среди них есть и такие, которые можно рассматривать как криптографические, то есть обеспечивающие секретность переписки. Так, встречается описание системы замены гласных букв согласными, и наоборот. В этих рукописях упоминается о тайнописи как об одном из 64 искусств, которым должны овладеть и женщины.

Один из самых старых шифрованных текстов Месопотамии представляет собой табличку, написанную клинописью и содержащую рецепт изготовления глазури для гончарных изделий. Автор этой клинописи, стремясь скрыть содержание написанного, использовал редко употребляемые знаки, игнорировал некоторые гласные и согласные, вместо имен употребил цифры.

Использовалась тайнопись и в рукописных памятниках Древнего Египта. Здесь шифровались религиозные тексты и медицинские рецепты.

Сохранились достоверные сведения о системах шифров, применявшихся в Древней Греции. Там криптография широко использовалась в разных областях деятельности. Так, Плутарх сообщает, что жрецы хранили в форме тайнописи свои прорицания. Однако наиболее широкое применение криптография получила в государственной сфере. Во все времена криптография была одним из основных орудий в межгосударственной борьбе, надежным средством сокрытия политических, дипломатических, экономических и иных секретов государства, с одной стороны, и средством проникновения в секреты государства-противника — с другой.

Основной принцип шифрования в древности – принцип замены. Рассмотрим самые известные.

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.

В древней Спарте в V-IV веках до н.э. существовала тайнопись и шифровальный прибор, получивший название "табличек Энея"

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

А другие греки того времени для шифрования применяли прибор под названием "Скитала" (сцитала). Его способ заменять одну букву другой встречался вплоть до наших времен.

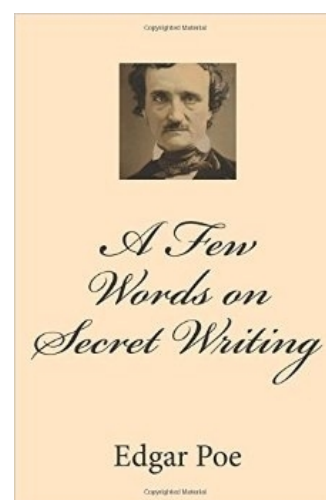


На этот посох наматывалась по спирали полоска пергамента с зашифрованным посланием. Смысл такого «гаджета» был в том, что прочитать эту полоску мог лишь обладатель скиталы аналогичного размера. При правильном размере витка буквы послания совпадали, и получался связный текст. Устройство было очень простым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

его назвать никак нельзя.

Согласно легенде, этот «шифр» сумел разгадать еще Аристотель, а в 1841 году в июльском журнале Graham's Magazine его редактор Эдгар Аллан По опубликовал статью «Несколько слов о тайнописи», в которой рассказал про скиталу и поведал об остроумном методе дешифровки скиталы любого диаметра.

По словам родоначальника детективного жанра, для «взлома» скиталы нужно взять, скажем, шестифутовый конус и намотать на него ленту с текстом, а затем перемещать вдоль длины конуса, пока текст не станет читаемым. Страсть Эдгара По к различным головоломкам и шифрам нашла свое отражение не только в его бессмертных произведениях. Будучи редактором журнала, он вел активное общение с читателями, призывая присылать ему ребусы и зашифрованные послания, которые он старался разгадывать совместно с подписчиками издания, совершенствуя тем самым свои навыки в криптологии.



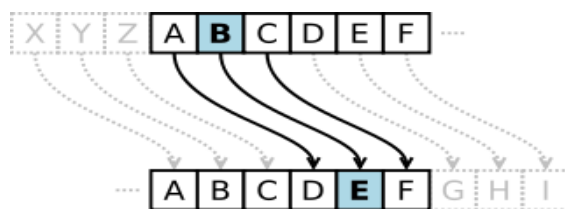
Шифр Цезаря

Криптография сыграла значительную роль в укреплении могущества Римской империи. В частности, особая роль в обеспечении государственной тайны принадлежит новому способу шифрования, изобретенному Юлием Цезарем и изложенному им в «Записках о галльской войне» (I в. до н. э.).

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 О нужно было взять 3 факела в правую руку и 4 факела — в левую.

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I, J	K
3	L	M	N	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z

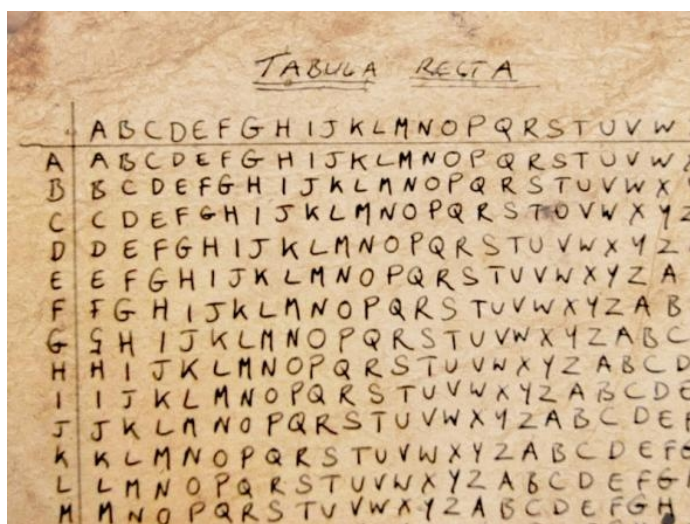
Шифр Виженера

В средневековье над изобретением тайнописи трудились многие выдающиеся люди, поставившие развитие криптографии на высокую ступень совершенства - голландский государственный деятель Гуго Гроций, английский философ Р.Бэкон. В XVII в. простой французский писец Антуан Ровсиньоль опередил свое время, составив шифр, не раскрытый на протяжении двух веков и получивший название "великого шифра". "Великий шифр" включал в себя буквы, слова, слоги, - всего объемом около 600 величин, которым придавалось несколько значений пропорционально повторяемости в тексте.

Обычное замещение текста — слишком слабый способ шифрования, который очень просто разгадывается с помощью банальной логики и статистики употребления тех или иных букв в языке. Помните, как лихо расшифровал подобный шифр сыщик Шерлок Холмс в рассказе «Пляшущие человечки» Артура Конан Дойля? Аналогично можно было бы расшифровать шифр Цезаря. Но с **шифром Виженера** у великого сыщика не вышло бы так просто разгадать загадку, ведь одна и та же буква в кодируемом сообщении могла иметь разные подстановки.

Интересно, что человек, давший имя этому шифру, никакого отношения к нему не имел. На самом деле его автором был итальянский математик Джованни Батиста Беллазо. Его труды и изучил Блез де Виженер во время своей двухлетней дипломатической миссии в Риме. Вникнув в простой, но эффективный принцип шифрования, дипломат сумел преподнести эту идею, показав ее комиссии Генриха III во Франции.

Суть нового принципа шифрования заключалась в том, что величина сдвига для замещения букв была переменной и определялась ключевым словом или фразой. Долгое



время этот метод считался неуязвимым для разгадывания, и даже авторитеты в области математики признавали его надежность. Так, легендарный автор приключений «Алисы в зазеркалье» и «Алисы в стране чудес», писатель-математик Льюис Кэрролл в своей статье «Алфавитный шифр» прямо и категорично называет шифр Виженера «невзламываемым». Эта статья вышла в детском журнале в 1868 году, но даже спустя полвека после статьи Чарльза Латуиджа Доджсона (это настоящее имя автора сказок про

Алису) научно-популярный американский журнал Scientific American продолжал утверждать, что шифр Виженера невозможно взломать.

Для расшифровки шифра Виженера использовалась специальная таблица, которая называлась *tabula recta*.

Линейка Сен-Сира

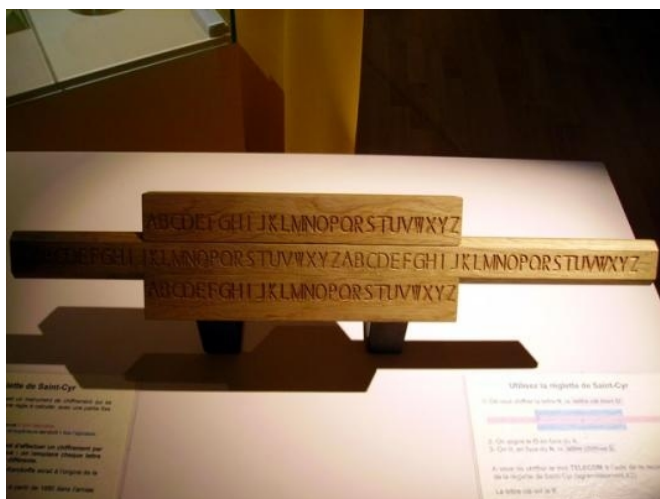


Еще одним примером полиафавитных шифров является **«Линейка Сен-Сира»**. Её название произошло от названия военного училища, которое в свое время организовал Наполеон Бонапарт. Это высшее учебное заведение выпустило немало известных личностей — маршалов и военачальников. В военной академии Сен-Сир придумали простое и оригинальное устройство, состоящее из двух частей — алфавитной линейки и подвижного бегунка с написанным алфавитом и прорезью. Принцип шифрования этой линейкой был очень простым и основывался на замещении букв алфавита. Но, в отличие от шифра Цезаря, где общий сдвиг букв при письме был одним и тем же (например, А — Б, вместо В — Г и так далее), в линейке Сен-Сира был реализован шифр замещения с переменным сдвигом, так называемый шифр Блеза де Виженера, французского дипломата, жившего в шестнадцатом столетии.

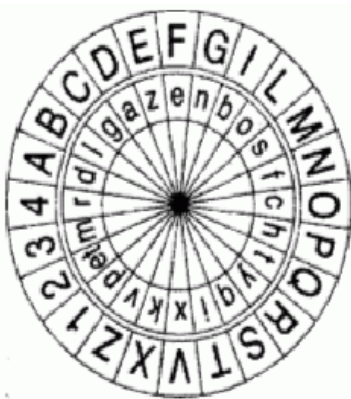
Линейка Сен-Сира — это своего рода механическая таблица Виженера. Пользоваться линейкой Сен-Сира несложно. Предположим, вы хотите закодировать текст MORTALENEMY ключевым словом POST.

Многokrатно пишем это ключевое слово, чтобы получившееся выражение было по длине таким же, как шифруемый текст. Получается так:
MORTALENEMY
POSTPOSTPOS

На линейке подбираем положение бегунка, чтобы начало алфавита совпадало с буквой Р и смотрим, какая буква соответствует первой букве шифруемого текста М. Это — буква В. Аналогичным образом букве О соответствует буква С, R меняется на J и так далее. В результате мы получаем зашифрованное слово: BCJMPZWGTAQ



Шифровальный диск



Еще один значительный шаг вперед криптография сделала благодаря труду Леона Альберти. Известный философ, живописец, архитектор, он в 1466 г. написал труд о шифрах. В этой работе был предложен шифр, основанный на использовании *шифровального диска*. Сам Альберти назвал его шифром, «достойным королей».

Шифровальный диск представлял собой пару соосных дисков разного диаметра (см. рисунок). Большой из них — неподвижный, его окружность разделена на 24 равных сектора, в которые вписаны 20 букв латинского алфавита в их естественном порядке и 4 цифры (от 1 до 4). При этом из 24-буквенного алфавита были удалены 4 буквы, без которых можно было обойтись, подобно тому, как в русском языке обходятся без Ъ, Ё, И. Меньший диск —

подвижный, по его окружности, разбитой также на 24 сектора, были вписаны все буквы смешанного латинского алфавита.

Имея два таких прибора, корреспонденты договаривались о первой индексной букве на подвижном диске. При шифровании сообщения отправитель ставил индексную букву против любой буквы большого диска. Он информировал корреспондента о таком положении диска, записывая эту букву внешнего диска в качестве первой буквы шифртекста. Очередная буква открытого текста отыскивалась на неподвижном диске и стоящая против нее буква меньшего диска являлась результатом ее зашифрования. После того как были зашифрованы несколько букв текста, положение индексной буквы изменялось, о чем также каким-либо образом передавалось корреспонденту.

Такой шифр имел две особенности, которые делают изобретение Альберти событием в истории криптографии. Во-первых, в отличие от шифров простой замены шифровальный диск использовал не один, а несколько алфавитов для зашифрования. Такие шифры получили название многоалфавитных. Во-вторых, шифровальный диск позволял использовать так называемые коды с перешифрованием, которые получили широкое распространение лишь в конце XIX века, то есть спустя четыре столетия после изобретения Альберти.

Для этой цели на внешнем диске имелись цифры. Альберти составил код, состоящий из 336 кодовых групп, занумерованных от 11 до 4444. Каждому кодовому обозначению соответствовала некоторая законченная фраза. Когда такая фраза встречалась в открытом сообщении, она заменялась соответствующим кодовым обозначением, а с помощью диска цифры зашифровывались как обычные знаки открытого текста, превращаясь в буквы.

Поворотная решетка

Кардано принадлежит идея поворотной решетки как средства шифрования. Изначально обычная решетка представляла собой лист из твердого материала, в котором через неправильные интервалы сделаны прямоугольные вырезы высотой для одной строчки и различной длины. Накладывая эту решетку на лист писчей бумаги, можно было записывать в вырезы секретное сообщение. После этого, сняв решетку, нужно было заполнить оставшиеся свободные места на листе бумаги неким текстом, маскирующим секретное сообщение. Подобным стеганографическим методом маскировки сообщения пользовались многие известные исторические лица, например кардинал Ришелье во Франции и русский дипломат и писатель А. Грибоедов. Так, Ришелье использовал прямоугольник размера 7×10. Для длинных сообщений прямоугольник использовался несколько раз. Прорези трафарета размещались в позициях: (1, 8), (2, 9), (3, 6), (4, 5), (4, 6), (5, 1), (5, 6), (5, 7), (5, 9), (6, 2), (6, 10), (7, 9), (7, 10).

Текст выглядит как невинное любовное письмо, однако используя трафарет Ришелье, получит зловещую команду: «YOU KILL AT ONCE».

	1	2	3	4	5	6	7	8	9	10
1										
2										
3										
4										
5										
6										
7										

	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

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.

Подьячие Приказа тайных дел и посольские дьяки, поддерживающие связи с царскими представителями за границей, нередко прибегали к зашифрованной переписке ("затейное письмо"). Ключ к расшифровке этих посланий не записывался, его заучивали наизусть. Существовали различные варианты секретного письма и, как положено по правилам конспирации, никто из подьячих не должен был знать всех вариантов тайнописи.

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



Фрагмент тайнописи Звенигородского колокола.

Символ открытого текста ищется в таблице и заменяется на символ зашифрованного, 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 "Кайпанотмыкая лерью некакяри".

Нередко писцы прибегали к написанию фраз в обратном порядке, составляя своеобразные криптограммы, или не дописывали буквы - подобный шифр назывался "полусловицей".

На рубеже XVII-XVIII веков в России происходят серьезные экономические и политические преобразования. Их олицетворением стало правление Петра I Великого, с именем которого связана большая работа почти во всех областях и сферах деятельности государства Российского. Поэтому не удивительно, что именно Петр I оценил огромное значение тайнописи.

Необходимость в "тарабарской грамоте" являлась более чем насущной задачей, поскольку Петр вел огромную работу во внешнеполитическом и внутривнутреннем направлениях. Рост дипломатических отношений требовал использования шифров в массовом количестве; начавшаяся Северная война привела к росту и дальнейшему совершенствованию видов тайнописи.

Все русские послы при иностранных дворах пользовались специальными шифрами ("цыфирь", "азбука", "ключ") для переписки с руководящими лицами Посольской канцелярии и царем. Именно Посольская канцелярия, ведавшая важнейшей политической перепиской, явилась главным учреждением царя по организации систематического использования тайнописи. Под непосредственным руководством Петра и "начального президента государственной посольской канцелярии" А.Ф.Головина работало "цыфирное отделение".

В 30-е гг. XVIII в. в России появляются совершенно новые системы тайнописи - алфавитные, позже - неалфавитные коды. В алфавитном коде текст и шифрообозначения нумеруются параллельно друг другу. В этом-то и существовало слабое место. Данная

система облегчала дешифровку, избежать которой можно было путем перемешивания шифрообозначений; вводятся в обиход различные уловки.

Необходимость скрыть от чужих глаз тексты секретных донесений послов, разнообразных агентов вело, разумеется, к созданию новейших систем шифров. В связи с этим в середине 50-х г.г. XVII в., возникают новые виды тайнописи. "Цыфирные азбуки" увеличиваются в объеме, включая в себя более тысячи величин. Словарь шифров включает буквы, слоги, географические названия, имена, даты. Шифровальщики отказываются от идеограмм, знаков и целиком и полностью переходят к цифрам; создаются особые знаки, так называемые скрытые пустышки. Другими словами, при их дешифровке отдельные элементы текста могут ничего не значить.

Например, в одной из цифирей зашифрованный знак + означал, что следующее за ним шифрообозначение не несет смысловой нагрузки. Два знака ++ говорили дешифровальщику, что не следует читать два следующих за ним шифрообозначения. Некоторые знаки сообщали о ненужности строк, страниц и даже параграфов текста! Все зависело от фантазии автора шифрованного сообщения. В результате получалось нагромождение цифр, усложнявшее работу вражеских дешифровальщиков, ради чего и создавались данные системы.

Первые успехи в России криптографов в дешифровке иностранных шифров связывались с именем математика Христиана Гольдбаха. Особенно он прославился при раскрытии шифров посла Франции в России Д. Шетарди (которого сыграл М. Боярский в фильме "Гардемарины, вперед!"). В результате тяжелой и кропотливой работы Х.Гольдбах приобрел огромный опыт в дешифровке, что позволяло ему раскрывать чужую "цыфирь" в течение двух недель.

В результате дворцового переворота в 1762 г. на престол России восходит императрица Екатерина II, при которой внешняя и внутренняя политика была отмечена важными законодательными актами, выдающимися военными событиями и значительными территориальными приобретениями; престиж екатерининской России в Европе значительно укрепился.

История тайнописи при Екатерине II была тесно связана с графом Н.И. Паниным. В 60-80-е г.г. XVII в. по его указаниям вводились в обиход разнообразные новые шифры. Не меньше внимания граф уделял дешифровке переписки иностранных посланников в России со своими королями. В этом деле Н.И. Панин весьма преуспел в перлюстрации (тайное вскрытие и копирование корреспонденции) бумаг послов, предпринятой еще в 40-50-х гг. того же века канцлером А.П. Бестужевым-Рюминым, создателем "черных кабинетов" (служба перлюстрации).

Для повышения надежности переписки необходимо было пользоваться разными шифрами. С одной стороны, шифрующий должен был указать своему корреспонденту шифр, которым пользовался сам; с другой стороны, эту информацию требовалось как можно тщательнее скрыть.

В правление Александра I в государственной структуре России происходят важные перемены. В 1802 г. вместо прежних приказов и коллегий впервые появляются министерства. При министерстве иностранных дел (МИД) формируется собственная канцелярия, в которой - помимо других подразделений - образуются три секретных экспедиции (управления): первая - цифирная (шифровальная), вторая - цифирная (дешифровальная) и третья - газетная (служба перлюстрации).

Российская дешифровальная служба еще с середины XVIII в. вела успешную борьбу с королевской Францией, практически без особого труда взломав ее шифры. Подобное состояние дел перекочевало и в XIX в. Русские дешифровальщики и здесь поработали прекрасно: в руках Александра I имелось достаточно сведений о переписке наполеоновских генералов.

Более того, полковник А.И. Чернышев (использовал шифр А.В. Суворова), сотрудник Особенной канцелярии (специального органа русской внешней разведки),

проделавший в Париже огромную и значительную работу по розыску сведений о состоянии Великой армии Наполеона. В результате блестяще проделанной работы А.И. Чернышеву удалось завербовать одного сотрудника военного министерства Франции, благодаря которому документы, имевшие стратегическое значение для Франции, Наполеон получал чуть ли не одновременно с Александром I.

Как ни странно, но гений Наполеона остался равнодушным к тайнам криптографии, хотя, конечно, император использовал тайнопись. Не чурался "тарабарской грамоты" и наполеоновский генералитет, применявший, например, т.н. книжный шифр. Для его использования у двух корреспондентов имелась одна и та же книга, по которой они шифровали донесения, нумеруя, как правило, слова, буквы, указывая номер страницы, строчки и т.д.

Вторая половина XIX в. - это рост внешних и внутренних связей, развитие экономики, ведущей к появлению разнообразнейших шифров в каждом ведомстве - МИДе, армии, флоте, полиции, в том числе и у революционеров. Развитие научно-технического прогресса повлияло и на систему криптографии. Появляются сложные по структуре биграмные, биграмно-буквенные, биклавные шифры, основанные на многозначной замене.

Получают большое распространение кодовые таблицы, возникшие в конце XVIII в. Объем кодов состоял от 300 до 10 тысяч словарных величин. До 70-х гг. XIX в. в России в основном использовались коды объемом 300, 600, 900 и 1.200 величин. К концу XIX - началу XX вв. появились коды объемом более 10 тысяч словарных величин. К 1917 г. наибольшее распространение имели коды именно такого объема.

Перед Первой мировой войной и во время нее дешифровальщики цифирного комитета МИДа провели большую и успешную работу по раскрытию шифров и кодов многих государств, в первую очередь стран, находившихся в состоянии войны с Россией. Так, в период с 1913 по 1916 г.г. было дешифровано 1.157 австрийских, 852 болгарских, 512 итальянских, 406 турецких, 231 германская телеграмм. Уже из перечисления сухих цифр можно сделать вывод о качестве шифров за границей - самым труднораскрываемыми оказались германские.

Первая мировая война 1914-1918 г.г. явилась невиданной для мира катастрофой, превратившей всю Европу в огромный театр военных действий. Для нашей страны она стала войной, принесшей ей неимоверные разрушения, распад и возникновение нового государства - Советской России.

Как писал впоследствии немецкий полковник Макс Хоффман, благодаря радиоперехвату "мы знали все о планах русских". Слово во время штабных игр русские оказались в кольце противника, который был в курсе каждого их шага.

Подобное поражение стало закономерным из-за неразберихи в шифровальной службе. Штабы 1-й и 2-й армий общались посредством шифров, передаваемых по радио. В армии П.К. Ренненкампа новый получили быстрее, чем в армии А.В. Самсонова, поэтому в 1-й армии старый шифр уничтожили, и штабы не могли понять сообщения друг друга. Оказавшись в экстремальной ситуации, армии перешли на открытый текст в эфире, что повлекло за собой сокрушительное поражение.

Россия вступила в войну отсталой страной с точки зрения технической оснащенности, что явилось первой причиной проигрыша в "шифровальной войне". Коды и шифры, которыми пользовались военные, оказались несостоятельными и легкораскрываемыми. Поэтому, русскую шифропереписку читали как державы Центрального союза (Германия, Австро-Венгрия), так и союзники России по Антанте (например, Великобритания). Немцы и австрийцы дешифровали код, использующийся в русских армиях, в результате чего противник смог свободно читать донесения и приказы наших штабов.

Конечно, и русские дешифровальщики действовали удачно. Так, в конце 1914 г. им удалось раскрыть несколько немецких шифров, что оказало некоторое положительное

влияние на дальнейшую "шифровальную войну". К сожалению, русских дешифровальщиков сопровождали многочисленные неудачи.

Когда криптография не требовала серьезной материально-технической и финансовой базы на разработку шифров, Россия могла очень успешно соревноваться с Западом. Но когда мир вступил в век серьезных научно-технических открытий и изобретений, криптография оказалась в одном ряду с наукоемкими производствами, и Россия в начале XX в. начинает терпеть поражения.

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 А до Z). Сам ротор отвечает очень простому типу шифрования, т.е. элементарному шифру замены. Например, контакт, отвечающий за букву Е, мог быть соединен с контактом буквы Т на другой стороне ротора. Но при использовании нескольких роторов в связке получается более надёжное шифрование.

С середины XX века до 1970-х гг. математика серьёзно внедряется в процесс шифрования. Обязательным этапом становится изучение уязвимостей шифра. Однако до 1975 года криптография оставалась классической (криптографией с секретным ключом).

С 1970-х годов наступает современный этап развития криптографии.

Симметричные шифрование - это способ шифрования, в котором для шифрования и расшифровывания используют один и тот же ключ.

Ключ шифрования должен быть известен обеим сторонам...и должен оставаться в секрете для посторонних.

Итак, первый метод симметричного шифрования - это метод простой перестановки:

1. Простая перестановка:

Из названия видно, что данный способ является самым простым.... Итак, кодируемое сообщение записывается в таблицу по столбцам. После этого для образования шифра текст считывается по строкам. Отправителю и получателю сообщения обязательно нужно договориться об общем виде размера таблицы. При расшифровывании действия выполняются в обратном порядке.

2. Одиночная перестановка по ключу.

Обладает несколько большей стойкостью к раскрытию....Этот способ отличается от предыдущего тем, что столбцы таблицы переставляются по ключевому слову, фразе или набору чисел длиной в строку таблицы. Например, по слову пеликан.

В верхней строке левой таблицы записан ключ, а номера под буквами ключа определены в соответствии порядка их следования в алфавите....В правой таблице столбцы упорядочены по числам. Далее сообщение также считывается по строкам, как в предыдущем примере.

3. Двойная перестановка.

Суть этого способа заключается в шифровании сообщения, которое уже было зашифровано. Итак, сначала в таблицу записывается текст сообщения, а потом поочерёдно переставляются столбцы, а затем строки. Число вариантов двойной перестановки увеличивается, если увеличивается размер самой таблицы.

4. Перестановка «магический квадрат».

Этот способ применялся ещё в средние века. Магическим квадратом называют таблицу с вписанными в них натуральными числами, которые дают в сумме по каждому столбцу, каждой строке и каждой диагонали одно и то же число.

В магический квадрат вписывали шифруемое сообщение в соответствии с нумерацией символов. Далее сообщение выписывается по строкам, как и в предыдущих примерах. В те времена считалось, что криптограмма, полученная с помощью магического квадрата, являлась более стойкой к расшифровке.

Существует более десятка современных алгоритмов симметричных шифров, параметрами которого являются стойкость, длина ключа, сложность преобразования.

Криптоанализ

Говоря о шифровании, мы должны рассматривать две области - криптографию и криптоанализ. Криптография шифрует сообщение, а криптоанализ взламывает зашифрованные сообщения.

Основная цель криптоанализа с течением времени не изменилась. Криптоаналитики по-прежнему пытаются подобрать ключ, чтобы расшифровать шифр. Но методы криптоанализа сильно изменились. В наши дни используются специализированные криптоаналитические компьютеры для взлома шифра. Раньше криптоаналитиками являлись по большей части лингвисты, а сейчас это удел чистых математиков.

Некоторые методы взлома криптограмм были изобретены десятки веков назад. Первым известным письменным упоминанием о криптоанализе является «Манускрипт о дешифровке криптографических сообщений», написанный арабским учёным Ал-Кинди ещё в IX веке. В этом труде содержится описание частотного анализа.

Сутью частотного анализа является мысль о том, что частота появления заданной буквы алфавита в достаточно длинных текстах одна и та же для разных текстов одного языка.

Утверждается, что в каждом языке есть свои закономерности употребления различных комбинаций букв. Например, пара стоящих рядом букв «ся» в русском языке более вероятна, чем пара «цы», а «оь» вообще не встречается. Именно на этом строится метод частотного анализа.

Например, полиалфавитный шифр Виженера, о котором я уже упоминал, до 1863 года являлся самым устойчивым, пока Фридрих Касиски не предложил свою методику взлома этого шифра.

Следующий этап развития связан с изобретением роторных шифровальных машин, таких как Энигма.

Благодаря математике криптография достигла такого развития, что количество математических операций по шифрованию и, следовательно, по взлому достигло астрономических значений.

Современная криптография стала гораздо более устойчивой к криптоанализу, в то время как раньше для взлома достаточно было ручки и листа бумаги. Тем не менее, криптоанализ рано списывать со счетов, поскольку неизвестно, насколько эффективными являются методы, применяемые спецслужбами для взлома шифра, а также сколько было проведено атак на различные распространенные сложные шифры. Таким образом, криптоанализ по-прежнему играет важную роль в обширной области защиты информации.

Главной задачей всех методов криптоанализа является поиск шифра, по которому производилось шифрование. Методы применяются в зависимости от того, какая информация содержится на руках у криптоаналитика. Если криптоаналитик обладает только шифром, то он будет пытаться найти ключ атакой на основе шифротекста и т.д.

Следует отметить, что подробного рассмотрения этих шифров, а также примеров их использования не содержится в открытой литературе. Информация, связанная с методами криптоанализа, является закрытой и предусмотрена только для служебного пользования.

Стоит также помнить, что в соответствии с Уголовным Кодексом РФ взлом чужой информации является уголовно наказуемым деянием.



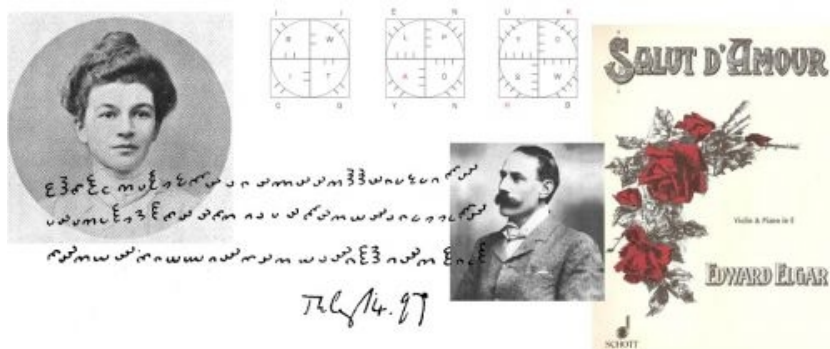
Во дворе здания ЦРУ в Лэнгли стоит S-образная медная плита с зашифрованным текстом. Это самый известный элемент скульптуры «Криптос», её авторы — скульптор Джеймс Санборн и Эд Шейдт, отставной глава криптографического отдела ЦРУ. Они придумали шифр, разгадать который

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. «Криптосом» занимаются любители (с 2003 года на Yahoo! существует группа из примерно 1500 человек) и профессионалы (из ЦРУ и АНБ) — их задачу осложняют намеренные ошибки, допущенные Санборном и Шейдтом (частично чтобы запутать людей, частично из эстетических соображений).

Считается, что Санборн — единственный человек на планете, знающий разгадку «Криптоса». Скульптор рассказывает, что люди, помешанные на созданном им шифре, звонят и говорят ужасные вещи: «Они называют меня прислужником дьявола, ведь у меня есть секрет, которым я ни с кем не делюсь». Санборн говорит, что в случае его смерти ответ обязательно перейдет к кому-то другому, но добавляет, что не совершенно не расстроится, если правильное решение навсегда останется тайной.

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.

3. Письма Зодиака



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. Именно этот шифр изображён на постере фильма Дэвида Финчера «Зодиак».

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.

Попытки разгадать коды Зодиака продолжаются. В 2011-м криптограф-любитель Кори Старлипер заявил, что расшифровал сообщение из 340 символов, и нашёл в нём признание Артура Ли Аллена, когда-то проходившего главным подозреваемым по делу Зодиака, но отпущенного за неимением доказательств. Про Старлипера написали многие газеты, но быстро выяснилось, что его метод не выдерживает никакой критики.

4. Шифр Д'Агапеева

75628 28591 62916 48164 91748 58664 74748 28483 81638 18174
74826 28475 83828 49170 74658 37575 75936 36565 81638 17585
75756 46282 32857 46382 75748 38165 81848 56485 64858 56382
72628 36281 81728 16483 75828 16483 63828 58163 63620 47481
81918 46385 84656 48565 62946 26285 91859 17491 72756 46579
71658 36264 74818 28462 82649 18193 65626 48484 91828 57491
81657 27483 83858 28364 62726 26566 31657 16648 32847 52747
82858 47582 81837 28462 82837 58163 63620 47481 72756 46579

MYSTERIOUS CYPHER IS
PUZZLE TO EVERYBODY



В первом издании книги Codes and Ciphers («Коды и шифры») английского картографа и криптографа русского происхождения Александра Д'Агапеева был напечатан шифр, до сих пор остающийся неразгаданным.

Уже после выхода книги автор признался, что забыл правильный ответ. В следующих изданиях «Кодов и шифров» криптограммы не

Разработка собственного шифра

Изучив литературу по криптографии и, рассмотрев основные правила замены, я захотел 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, сегодня 26 февраля, значит каждый символ смещается вперед на 26. Таким образом, фраза «Тайна за семью печатями» будет иметь вид: ЛЩГЖЩ БЩКУЧ ИЮРЩЛЦЕВ, а 27 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.

Источники

1. <http://proxy.coollib.net/b/233545/read>
2. <http://russify.ru/print:page,1,1144-tarabarskaja-gramota.html>
3. <http://magspace.ru/blog/intresting/278061.html>