История криптографии

Знаете ли вы что такое «криптография»?

Криптография возникла именно как практическая дисциплина, изучающая и разрабатывающая способы шифрования сообщений, то есть при передаче сообщений – не скрывать сам факт передачи, а сделать сообщение недоступным посторонним. Для этого сообщение должно быть записано так, чтобы с его содержимым не мог ознакомиться никто за исключением самих корреспондентов.

Арсенал криптографии (тайнописи) чрезвычайно богат. Человечество изобрело большое число способов секретного письма, например, симпатические чернила, которые исчезают вскоре после написания ими текста или невидимы с самого начала, «растворение» нужной информации в сообщении большего размера с совершенно «посторонним» смыслом, подготовка текста при помощи непонятных знаков.

Точных дат и бесспорных сведений о секретном письме в древности сохранилось очень мало. Однако вместе с шифрами были, само собой разумеется, и попытки сокрытия текста. В древней Греции для этого однажды обрили раба, написали на его голове, и, когда волосы отросли, отправили с поручением к адресату. Отзвук этой истории можно встретить в "Гиперболоиде инженера Гарина" Алексея Толстого, где текст нанесли на спину мальчика.

Криптография (от *крипто…* и *графия*) тайнопись, система изменения письма с целью сделать текст непонятным для непосвященных лиц. В наши дни общепринято полагать, что область применения криптографии, шифров и кодов ограничена военной и дипломатической сферой, компьютерными технологиями и банковским делом. Между тем, еще несколько веков назад криптограммы играли важную роль в литературе и философии.

Древний период

Полибий (212 или 205 г. до н.э. - 130 или 123 г. до н.э.)

Полибий — известный историк, сын Ликорты, уроженец Мегалополя. Род. между 212 и 205 г.. ум. между 130 и 123 г. до Р. Хр.

В Древней Греции (II в. до н.э.) был известен шифр, называемый "квадрат Полибия". Шифровальная таблица представляла собой квадрат с пятью столбцами и пятью строками, которые нумеровались цифрами от 1 до 5. В каждую клетку такого квадрата записывалась одна буква. В результате каждой букве соответствовала пара чисел, и шифрование сводилось к замене буквы парой чисел. Идею квадрата Полибия проиллюстрируем таблицей с русскими буквами. Число букв в русском алфавите отличается от числа букв в греческом алфавите, поэтому и размер таблицы выбран иным (не квадрат 5x5, а прямоугольник 8x4).

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

Зашифруем фразу: КРИПТОГРАФИЯ: 23 31 21 28 33 27 14 31 11 35 21 48

Из примера видно, что в шифрограмме первым указывается номер строки, а вторым - номер столбца.

Гай Юлий Цезарь (102 или 100 -44 до н.э.)

ЦЕЗАРЬ (Caesar) Гай Юлий (100-44 до н. э.), римский диктатор в 49, 48-46, 45, с 44 до н. э. — пожизненно. Полководец. Начал политическую деятельность как сторонник республиканской группировки, занимая должности военного трибуна в 73 до н. э., эдила в 65 до н. э., претора в 62 до н. э. Добиваясь консулата, в 60 до н. э. вступил в союз с Г. Помпеем и Крассом (1-й триумвират). Консул в 59 до н. э., затем наместник Галлии; в 58-51 до н. э. подчинил Риму всю заальпийскую Галлию. В 49 до н. э., опираясь на армию, начал борьбу за единовластие. Разгромив Помпея и его сторонников в 49-45 до н. э. (Красс умер в 53 до н. э.), оказался во главе государства. Сосредоточив в своих руках ряд важнейших республиканских должностей (диктатора, консула и т. п.), стал фактически монархом. Убит в результате заговора республиканцев.

Автор «Записок о галльской войне» и «Записок о гражданских войнах»; провел реформу календаря (Юлианский календарь).

Примером наиболее простого шифра, относящегося к группе шифров простой подстановки, является шифр Цезаря. По свидетельству древнеримского историка, Гай Юлий Цезарь (102 или 100-44 до н.э.) использовал его для тайной переписки. В шифре Цезаря каждая буква исходного сообщения сдвигается в алфавите на фиксированное число позиций вперед, при необходимости переходя циклически на начало алфавита. Сам Цезарь использовал сдвиг на три позиции. В этом случае сообщение

ВОЗВРАЩАЙТЕСЬ В РИМ

шифруется так: ЕСКЕУГЪГМХИФЯ Е УЛП

здесь буква В шифруется буквой Е, отстоящей от буквы В на три позиции, буква О- буквой С и так далее (считается, что буквы Ё в алфавите нет). Последняя буква алфавита Я шифровалась бы при этом методе как В. Для расшифровки сообщения нужно сделать сдвиг на три позиции назад. Шифр Цезаря определяется величиной сдвига. Поскольку число различных сдвигов на единицу меньше, чем число букв алфавита, разгадывание шифра Цезаря не представляет особого труда. Достаточно перебрать всевозможные величины сдвига- от 1 до 31 в случае русского алфавита. Сообщение будет расшифровано, как только получится осмысленный текст.

Блез де Виженер - шифр Виженера

Блезом де Виженером, придворным короля Франции Генриха III, в конце XVI в. был предложен весьма изящный метод шифрования. Иногда этот шифр называют также шифрам с перекрытием текста. Для шифрования используется секретное слово или фраза. Нужно писать это секретное слово над исходным текстом, повторяя его, пока не кончится сообщение. Каждая буква исходного текста заменяется на отстоящую от неё в алфавите на несколько позиций. Величина сдвига задаётся буквой ключевого (секретного) слова, стоящей над данной буквой исходного текста. Для буквы А сдвиг вообще отсутствует, буква Б соответствует сдвигу на одну позицию вперёд, буква В — сдвигу на две позиции и так далее. Последняя буква—Я — соответствует сдвигу на 31 позицию, поскольку в русском алфавите 32 буквы. То есть размер сдвига определяется порядковым номером буквы в алфавите, из которого вычтена единица.

В примере в качестве ключевого используется слово ХОЛМС. Пусть надо зашифровать сообщение

ПРИХОДИ НЕМЕДЛЕННО

Для этого пишется ключевое слово над шифруемой фразой:

Х	О	Л	М	С	Х	О		Л	М	С	Х	О	Л	М	С	Х	О
П	Р	И	Х	О	Д	И		Н	Е	М	Е	Д	Л	Е	Н	Н	О

Теперь каждую букву сообщения надо сдвинуть вперёд по алфавиту в соответствии с буквой ключевого слова, стоящей над ней. Например, буква Х является двадцать второй буквой алфавита и задаёт сдвиг на двадцать одну позицию вперёд. Вместо буквы П исходного текста получится буква Д зашифрованного сообщения. Вторая буква —Р— исходного сообщения сдвигается в соответствии с буквой О ключевого слова на 14 позиций вперёд и заменяется на букву Ю. И так далее:

ДЮУБЯЩЦ ШСЭЪТЦСЮВЬ

Эту мысль повторил позднее **Блез Паскаль** и в наше время **Норберт Винер**. Предложение Виженера во многом развивает идею Кардано о применении открытого или шифрованного текста в качестве ключа

Криптография в литературе

Явление тайнописи привлекает внимание исследователей, представляющих различные области знания. Издавна и по настоящее время оно предстает неотъемлемой частью человеческого бытия. Скрытыми смыслами наделяется вселенная и составляющие ее объекты, природные процессы. Ими наполнены как сфера сакрального, божественного, так и земного, «видимого» пространства. Тайнопись обладает особой притягательной силой, поскольку содержит в себе компонент загадочного. Человеку присуще стремление к постижению неизвестного, приоткрытою смысловых глубин мироздания.

Шифровальные системы, способствующие развитию фантазии, творческого потенциала, используются и в явлениях культуры. Тайным значением наделены библейские, каббалистические и другие древние тексты, литературные памятники. Скрытые сообщения содержатся в авторских сочинениях разных эпох. Они встречаются в творчестве многих писателей и поэтов, к примеру, А. Данте, Ф. Петрарки, В. Шекспира, Э. По, Д. Джойса, У. Эко, Т. Манна, В. Набокова, Д. Хармса, В. Хлебникова.

Чаще всего это шифры простой подстановки и использованы они в основном в детективах и исторических романах. Однако иногда в произведения писателей можно найти "новоизобретенный" шифр. Примером такого произведения является "Пляшущие человечки" **Артура Конан Дойла**.

Нередко можно встретить и произведения, посвященные криптографии. Особенно много их было написано в годы противостояния официальной власти и революционеров, а также в годы Первой и Второй Мировых войн. Одним из таких произведений является "Легенда о шифре" **Е. Долматовского**.

Артур Конан Дойл (1859 - 1930)

ДОЙЛ (Doyle) Артур Конан (1859-1930), английский писатель. Ввел в детективную литературу образ сыщика-любителя (Шерлок Холмс). Повести «Собака Баскервилей» (1901-02), «Долина ужаса» (1914-15), рассказы отличаются занимательной интригой и простотой

повествования. Исторические и научно-фантастические романы.

В рассказе Артура Конан Дойла «Пляшущие человечки» описано *шифрование простой подстановкой*. При этом шифровании каждая буква исходного сообщения кодируется другим знаком, заданным таблицей кодировки. Верхняя строка таблицы содержит все буквы алфавита. В нижней строке таблицы можно произвести любую перестановку букв алфавита; каждой такой перестановке соответствует определенный шифр. В рассказе каждая буква сообщения изображалась определенной фигуркой пляшущего человечка. «Цель изобретателя этой системы заключалась, очевидно, в том, чтобы скрыть, что эти значки являются письменами, и выдать их за детские рисунки. Но всякий, кто сообразит, что значки соответствуют буквам, без особого труда разгадает их, если воспользуется обычными правилами разгадывания шифров». Какие же правила имел ввиду Шерлок Холмс?

Изобретатели шифра «пляшущих человечков»- чикагские бандиты значительно облегчили задачу разгадывания шифра, снабдив флагами человечков, стоящих в начале и конце слов.

МБОУ СОШ
№32

Чехова 10/2

Телефон: (3462)52-57-75
Факс: (555)555-55-55
Эл. почта: proverka@example.com

Сделал дело - гуляй смело

Организация

«Тарабарская грамота».

В этой системе согласные буквы заменяются по схеме:

Б	В	Г	Д	Ж	З	К	Л	М	Н
Щ	Ш	Ч	Ц	Х	Ф	Т	С	Р	П

«Рыба с головы гниет».

«МЫЩА Л ЧОСОШ ЫСПИЕК»

В шифрах перестановки

изменяется порядок чередования символов исходного текста.

1	2	3	4	5
3	2	5	1	4

Зашифруем фразу «ВСТРЕЧА СОСТОИТСЯ ЗАВТРА».

РСВЕТОАЧССТОТСИВЗЯТАЪАРЪЪ

В заключение ...

В настоящее время, когда компьютерные технологии нашли массовое применение, проблематика криптографии включает многочисленные задачи, которые не связаны непосредственно с засекречиванием информации. Современные проблемы криптографии включают разработку систем электронной цифровой подписи и тайного электронного голосования, протоколов электронной жеребьевки и идентификации удаленных пользователей, методов защиты от навязывания ложных сообщений и т.п. Специфика криптографии состоит в том, что она направлена на разработку методов, обеспечивающих стойкость к любым действиям злоумышленника, в то время как на момент разработки криптосистемы невозможно предусмотреть все способы атаки, которые могут быть изобретены в будущем на основе новых достижений теории и технологического прогресса.