Д.Г. Гаев

Основы прикладной криптографии (часть 1)

Ил. 1

В материале «Электронный концлагерь» («Культура в современном мире», № 4/2013) много говорилось об угрозах частной жизни, исходящих от деятельности разведывательных ведомств (в первую очередь, конечно, американских, а именно печально известное Агентство национальной безопасности США). Могло создаться впечатление, что у простых людей нет никаких серьезных средств для противодействия этим угрозам, но это не соответствует действительности. Защитить свои секреты от чужих глаз и ушей вполне реально: компьютерные и сетевые технологии дают для этого развитой арсенал средств. Современные средства защиты информации в основном используют методы прикладной криптографии, так называемые средства ее шифрования и дешифрования. В этой статье речь пойдет о том, как нужно грамотно применять эти средства.

Криптография и жизнь

Абсолютное большинство про криптографию и шифры знают или, по крайней мере, что-то слышали. Однако многие по привычке думают, что шифры — это атрибуты сурового мира военных и разведывательных служб, не имеющие прямого отношения к жизни обычного человека. Между тем это уже давно не так! Простые люди давно сталкиваются с зашифрованной информацией ничуть не реже, чем штирлицы или джеймсы бонды своего времени, хотя многие и не подозревают об этом.

Например, технологии шифрования — это органичная часть современного Интернета. Чтобы постоянно использовать их, уже не надо быть шпионом. В Web давно реализованы средства шифрования входящего и исходящего траффика. Если вы видите в адресной строке браузера префикс «**https://**» (вместо более привычного «**http://**»), значит, с сервером установлено не простое соединение, а криптографически защищенное. Поскольку подобные соединения более ресурсоемкие, они обычно устанавливаются для передачи самой деликатной информации, например, регистрационных имен и паролей пользователей. Но на сайтах, предъявляющих повышенные требования к конфиденциальности (таких, как платежные и банковские онлайн-порталы), шифрованию обычно подвергается весь процесс

взаимодействия с пользователем от начала до конца. А технология TOR (“The Onion Router”) обеспечивает максимальный уровень защиты секретности: многоуровневое (послойное) шифрование данных на всем пути от сервера до клиента.

К сожалению, основные протоколы работы с электронной почтой не обеспечивают встроенного шифрования данных. Но это компенсируется тем, что давно разработаны отдельные модули шифрования (например, PGP / GPG), которые легко подключаются к любой современной почтовой программе, обеспечивая автоматическое кодирование входящих и исходящих сообщений. Аналогичные средства давно разработаны и для шифрования данных на дисках и т. п. специальные программы (как-то, TrueCrypt) позволяют шифровать информацию как на отдельных файлах, так и на целых логических дисках, доступ к которым будет возможен лишь после ввода пароля, надежно и избирательно. Средства шифрования встроены в том числе и в такие суперпопулярные технологии интернет-телефонии, как Skype.

Шифрование избирательно применяется и в сетях сотовой телефонии, например GSM. Средства шифрования реализованы в большинстве популярных смартфонов, хотя их надежность специалисты оценивают весьма критически. Действительно надежную (и всестороннюю) защиту сотовых переговоров обеспечивают профессиональные сотовые аппараты, так называемые *криптофоны*, которые, как Ancort A-7, весьма недешевы, но все же доступны и обычному абоненту.

Конечно, шифрование контента находит большое применение в коммерческих сетях телевещания — прежде всего, кабельных и спутниковых. Так, большинство провайдеров зарубежных и отечественных спутниковых телеканалов (Viasat, «НТВ-Плюс» или «Триколор ТВ») шифруют свои передачи для защиты от нелицензированного просмотра. Для декодирования передач ресивер требует специальную ключевую карту, которая предоставляется только платным абонентам.

Также активно эти средства внедряются в технологии записи данных на оптические носители разных типов. Если для самых первых CD-ROM подобные средства еще не были разработаны, то к выходу DVD уже была технология CSS (*Content Scrambling System*). Для оптических носителей нового поколения (BluRay, HD DVD) изобрели AACS (*Advanced Access Content System*). Впрочем, чтобы непосредственно столкнуться с CSS, нужен лицензированный DVD: пиратские, конечно, давно уже «взломаны». Вообще, жизнь убедительно доказала, что применение технологий криптозащиты для аудио- и видеоносителей как непопулярно, так и неэффективно. С одной стороны, они могут серьезно усложнить жизнь законопослушным пользователям, потому что диски нередко оказываются несовместимы с некоторыми моделями плееров. С другой стороны, от пиратского

копирования они защищают плохо: как технология CSS, так и AACS на данный момент считаются успешно взломанными (причем все средства для их взлома уже давно и свободно доступны в Интернете). Примерно такое же фиаско ожидало и попытки создать средства криптозащиты для электронных книг. Большинству конечных пользователей они создают неудобства, несмотря на то что профессионалами вполне успешно ломаются (читатели, возможно, помнят историю с арестом российского программиста Дмитрия Склярова, который был арестован в США в 2001 году за разработку системы для взлома электронных документов от фирмы Adobe).

Но вот с необходимостью криптотехнологий в сфере платежно-банковских операций не спорит никто: ни поставщики услуг, ни их конечные пользователи. Представьте себе, с каким риском были бы связаны любые удаленные финансовые операции, если бы информация о них не защищалась надежно на всем пути от пользователя до банка! Ясно, что ее эффективную защиту может обеспечить только очень стойкое шифрование. Поэтому без развитой криптографии не было бы банкоматов и платежных терминалов, невозможно было бы оплачивать банковскими карточками услуги и покупки в магазинах. Вероятно, перестали бы работать даже бесконтактные smart-карты, которые используют турникеты в метро и АСКП в наземном транспорте.

Таким образом, представить себе современный мир без криптографии — так же нереально, как без компьютеров. Да и жить в нем было б крайне неуютно.

Основные понятия криптографии

Предмет науки о шифрах весьма сложен, а современная криптография — это в основном сложнейшая математика. Но здесь мы все-таки дадим лишь самые основные и необходимые термины, которые не требуют каких-то специальных знаний, но важны для обсуждения всего дальнейшего.

— *сообщение* — это именно то, что требует шифрования с целью защиты его тайны. Обычно (но необязательно) это *текст*, объем которого может быть произвольным: от короткой фразы до конфиденциального документа объемом в сотни страниц.

— *шифротекст* (он же *криптограмма*) — это финальный результат шифрования исходного сообщения. Другими словами, это именно то, что передается по незащищенным (или же уязвимым для перехвата) каналам связи адресату.

— *шифрование* и *дешифрование* — метод или набор методов, применяемых для превращения исходного сообщения в шифротекст и для восстановления исходного сообщения. Методы шифрования и дешифрования, взаимно дополняющие друг друга, в совокупности называются *алгоритмом шифрования* (*криптоалгоритмом*).

— *ключ* — это основной параметр криптоалгоритма, обеспечивающий уникальность и воспроизводимость процессов шифрования и дешифрования (т. е. его секретная часть). Обычно (но не обязательно) ключом является строка текста, например, некое слово или кодовая фраза.

— *симметричный криптоалгоритм* — алгоритм шифрования, в котором и для шифровки, и для дешифровки сообщения применяется *один и тот же* ключ. Или (как вариант) ключи шифровки и дешифровки не полностью идентичны — но при этом один из них может быть легко определен (или вычислен), если известен другой. С практической точки зрения, в этой ситуации также можно говорить о наличии одного ключа.

— *асимметричный криптоалгоритм* — алгоритм шифрования, в котором для шифровки сообщения применяется один ключ, а для дешифровки — другой. Более того, между обоими ключами не существует очевидной связи, как и нет простого способа вычислить один из ключей, даже если другой уже известен. Обычно ключ дешифрования называется *закрытым ключом*, а ключ шифрования — *открытым*. Открытый ключ, в отличие от закрытого, обычно нет смысла держать в секрете: он может быть свободно доступен всем интересующимся.

— *криптоатака*, или *взлом*, — это любая попытка прочитать зашифрованное сообщение, не зная его ключа. (Обычно предполагается, что используемый криптоалгоритм при этом в какой-то степени известен.) Криптоатака может осуществляться как непосредственно на сообщение, так и на его ключ.

— *уязвимость* — наличие в криптоалгоритме системных недостатков, потенциально делающих более успешными определенные криптоатаки на него. Иногда фактором уязвимости может быть ключ: некоторые ключи (или целые классы ключей) могут оказаться криптографически «слабее», чем прочие.

— *лобовая атака* (или взлом методом «грубой силы») — это попытка взлома шифра путем последовательного перебора всех возможных ключей. Поскольку для большинства известных криптоалгоритмов число таких ключей конечно, то теоретически подобным способом можно взломать любой шифр. (Образно говоря, это можно сравнить с попыткой открывания сейфа путем перебора всех возможных комбинаций его кодового замка.) Основным *практическим* препятствием обычно является то, что количество возможных ключей в большинстве современных алгоритмов *астрономически велико*, поэтому их перебор требует вычислительных ресурсов, недоступных даже для самых быстродействующих из существующих сегодня вычислительных систем.

Наконец, сама *криптография* — это наука, задачей которой является изучение шифров, равно как и методов их взлома. В рамках криптографии неявно предполагается, что сам факт наличия шифрованного сообщения не секретен. Именно этим она отличается от

стеганографии: последняя дисциплина изучает вопрос, как можно скрыть сам *факт присутствия* закодированного сообщения.

Наш обзор мы начнем с рассмотрения криптографии докомпьютерной эпохи. Исторически было известно два класса шифров: *перестановочные* и *подстановочные*. Первые основаны на изменении порядка букв (или символов) в исходном сообщении регулярным образом. Вторые — на регулярной замене их другими буквами (или символами).

Шифры Цезаря и шифры простой замены

Подобные шифры хорошо известны с самых древних времен. Так, Юлий Цезарь шифровал свои военные сообщения. В своем простейшем варианте — шифрование Цезаря состоит в *циклическом сдвиге* символов сообщения (на несколько позиций вперед или же назад, двигаясь по алфавиту). Например, для русского алфавита, циклический сдвиг на 3 позиции вперед — означает, что буква «**А**» заменяется на «**Г**», «**Б**» — на «**Д**», «**В**» — на «**Е**» и так далее (вплоть до «**Э**» — «**А**», «**Ю**» — «**Б**» и «**Я**» — «**В**»). Для дешифровки, соответственно, нужно циклически «сдвинуть» все символы на столько же позиций назад. Число позиций для сдвига — и является единственным ключом шифра. Но поскольку таких ключей не больше, чем букв в используемом алфавите, вскрыть такой шифр очень просто путем последовательного перебора, поэтому шифр Цезаря не пригоден для сколь-нибудь серьезной криптографии.

Другой вариант подобного шифра — так наз. шифр «*атбаш*», в котором замена символов осуществляется в инверсном порядке (для русского алфавита, «**Я**» — «**А**», «**Ю**» — «**Б**» и т. д.). Он также может использоваться в комбинации с циклическим сдвигом. Наконец, в самом общем варианте подстановочного шифра предлагается использовать произвольно выбранную *таблицу замены*, которая и является ключом шифра. Например, для русского языка можно использовать такую подстановочную таблицу:

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

С ее использованием, исходное сообщение «Секретная миссия успешно выполнена» примет вид: «Вияъигцою тёввёю евшисцу рфшубцицо».

Дешифровка выполняется в обратном порядке: т. е. в нижней строке таблицы ищется каждая буква и заменяется на соответствующую в верхней строке.

Для подобного шифра возможных ключей, конечно, очень много. Для знакомых с элементарной математикой это — факториал от количества букв алфавита (для 33 букв русского алфавита это астрономически большое число). Механическим перебором подобный

шифр взломать невозможно. Кроме того, можно поменять исходные буквы на буквы альтернативного алфавита (например, латинского или греческого), цифры или любые специальные символы. Тем не менее, все подобные шифры ломаются довольно легко, например, методами *частотного анализа*, потому что относительная частота символов в зашифрованном сообщении — всегда та же, что и в исходном, т. е. наиболее распространенные буквы («а» или «е») в криптограмме будут встречаться столь же часто, а редкие («щ» или «ц») также редко. То же самое справедливо и для относительной частоты двухбуквенных последовательностей (*биграмм*): сочетания букв «ба» или «по» будут встречаться намного чаще, чем «щп» или «рц». Часто исходное слово можно сразу угадать по характерным повторам букв. Например, по криптослову «**тёввёю**» сразу видно, что второе слово в сообщении имеет длину в 6 букв, причем в нем совпадают вторая и пятая буквы, первая и четвертая. Таких слов в словаре русского языка не так уж и много, вполне реально найти и проверить все.

Про то, что шифры простой подстановки ломаются достаточно легко, было прекрасно известно очень давно. Здесь уместно вспомнить классический рассказ Эдгара Аллана По «Золотой жук». Как вы помните, главный герой успешно прочитал зашифрованное сообщение капитана Кидда, в котором рассказывалось, где искать пиратский клад. Об используемых им методах герой сам рассказывает так:

«...Как видите, текст криптограммы идет в сплошную строку. Задача была бы намного проще, если б отдельные слова были выделены просветами. Я начал тогда бы с анализа и сличения более коротких слов, и как только нашел слово из одной буквы (например, местоимение «я» или союз «и»), счел бы задачу решенной. Но просветов в строке не было, и я принялся подсчитывать однотипные знаки, чтобы узнать, какие из них чаще, какие реже встречаются в криптограмме. Закончив подсчет, я составил такую таблицу:

знак «8» встречается 34 раза,

знак «;» встречается 27 раз,

знак «4» встречается 19 раз,

знак «)» встречается 16 раз,

знак «#» встречается 15 раз,

знак «» встречается 14 раз,*

знак «5» встречается 12 раз,

знак «6» встречается 11 раз,

знак «+» встречается 8 раз,

знак «1» встречается 7 раз,

знак «0» встречается 6 раз,

знаки «9» и «2» встречаются 5 раз,

знаки «:» и «3» встречаются 4 раза,

знак «?» встречается 3 раза,

знак «||» встречается 2 раза,

знаки «=» и «]» встречаются 1 раз.

В английской письменной речи самая частая буква – e. Далее идут в нисходящем порядке a, o, i, d, h, n, r, s, t, u, y, c, f, g, I, m, w, b, k, p, q, x, z. Буква e, однако, настолько частотна, что трудно построить фразу, в которой она не занимала бы господствующего положения.

Итак, уже сразу у нас в руках путеводная нить. Составленная таблица, вообще говоря, может быть очень полезна, но в данном случае она нам понадобится лишь в начале работы. Поскольку знак 8 встречается в криптограмме чаще других, мы примем его за букву e английского алфавита. Для проверки нашей гипотезы взглянем, встречается ли этот знак дважды подряд, потому что в английском, как вам известно, буква e очень часто удваивается, например в словах meet или fleet, speed или seed, seen, been, agree и так далее. Хотя криптограмма невелика, знак 8 стоит в нем дважды подряд не менее пяти раз...».

Рассказ дальше цитировать не будем, но отметим, что начался он с сообщения:

53‡‡†305))6*;4826)4‡.)4‡);806*;48†8¶
60))85;1‡(;:‡*8†83(88)5*†;46(;88*96*
?;8)*‡(;485);5*†2:*‡(;4956*2(5*—4)8¶
8*;4069285);)6†8)4‡‡;1(‡9;48081;8:8‡
1;48†85;4)485†528806*81(‡9;48;(88;4(
‡?34;48)4‡;161;:188;‡?;

Успешно удалось дешифровать как:

agoodglassinthebishopshostelinthedev
ilsseattwentyonedegreesandthirteenmin
utesnortheastandbynorthmainbranchsev
enthlimbeastsideshootfromthelefteyeo
fthedeathsheadabeelinefromthetreethr
oughtheshotfiftyfeetout

(«A good glass in the Bishops Hostel in the Devils Seat twenty one degrees and thirteen minutes northeast and by north main branch seventh limb east side shoot from the left eye of the deaths head a bee line from the tree through the shot fifty feet out.»)

Можно вспомнить другой известный из литературы пример простого подстановочного

шифра из рассказа А. Конан-Дойля «Пляшущие человечки». Не будем его подробно цитировать (кто не читал его в детстве?). Но отметим один существенный момент: простой шифр «пляшущих человечков» основывался больше на том, что имитировал детские рисунки или каракули (т. е. по своей сути, он был ближе к стеганографии, а не к криптографии в истинном смысле слова). Когда же Шерлок Холмс понял, что имеет дело не с детскими каракулями, а с шифрованными сообщениями, он сумел прочитать их без особого труда, несмотря на довольно скромный объем доступного ему шифроматериала. Рассказ — хорошее свидетельство того, что в XIX веке уже прекрасно понимали серьезную уязвимость простых подстановочных криптоалгоритмов.

В настоящее время взлом простого подстановочного шифра — задача настолько тривиальная, что вполне может быть доверена компьютеру. Частотные таблицы для всех более или менее употребляемых в мире языков (в том числе, конечно, и для русского) давно составлены и опубликованы. С такими таблицами компьютерные программы способны взломать любой «шифр Цезаря» буквально за доли секунды.

Биграммные шифры и шифр Плейфера

Очевидный способ усложнить криптоатаку на простой подстановочный шифр — сделать алгоритм подстановки менее тривиальным. Например, вместо регулярной замены отдельных символов можно использовать замену целых *символьных пар*. Такие криптоалгоритмы называются *биграммными*. Наиболее известный из них и один из самых простых и удобных в использовании — так называемый «шифр Плейфера». Он получил свое имя в честь лорда Лайона Плейфера, активно внедрявшего его в правительственные учреждения Великобритании, хотя изобретен и описан он был Чарльзом Уитстоном.

Ил. 2. Лорд Лайон Плейфер (1818—1898)

Ключом в шифре Уитстона-Плейфера является квадратная или прямоугольная таблица, составленная из букв используемого алфавита. Она должна содержать все (или практически все) буквы, при этом они не должны повторяться. Для английского, как и для большинства европейских языков, в качестве таблицы удобнее всего использовать квадрат 5 строк на 5 столбцов (в нем 25 символов, так что один из них отбрасывается, чаще всего «Q»). Для русского — хорошо подходит таблица 4 строки на 8 столбцов, или наоборот (всего 32 символа, из них отбрасываем один, например твердый знак).

Процесс шифрования состоит в следующем. Исходное сообщение разбивается на идущие подряд пары букв (пробелы и знаки препинания не учитываются). Далее каждая пара букв ищется в ключевой таблице и преобразуется в другую пару по следующим несложным правилам:

- если они находятся *в одной строке*, циклически сдвигаем их *вправо* (то есть берем два символа из следующего столбца или из первого, если этот столбец был крайним справа);
- если они находятся *в одном столбце*, циклически сдвигаем их *вниз* (т. е. берем символы из следующей строки или из первой, если эта строка была крайней снизу);
- если эти два символа находятся в *двух углах прямоугольника*, тогда мы берем вместо них символы, находящиеся *в двух других* его углах.
- если оба символа *совпадают* (две буквы «с» в слове «миссия»), тогда возможны варианты. (Проще всего вообще избегать этой ситуации, сжимая все подряд идущие пары символов в один.)

Дешифровка осуществляется с помощью той же таблицы, но все преобразования и сдвиги выполняются *в противоположном порядке*. Возможны вариации используемого алгоритма: например, необходимо определиться, в каком порядке символы берутся из углов прямоугольника (четыре варианта). Кроме того, когда символы находятся в одной строке (столбце), возможен сдвиг в каком-либо другом направлении или на иное количество строк/столбцом таблицы. Обо всем этом использующие шифр должны договориться заранее.

Приведем пример практического использования шифра Плейфера. Берем такую ключевую таблицу:

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

(Здесь номера строки и столбцов, разумеется, не являются частью ключа, мы привели их исключительно для наглядности.) Если мы зашифруем с помощью этой таблицы сообщение: «Секретная миссия успешна», предварительно разбив его на пары букв СЕ, КР, ЕТ, НА, ЯМ, ИС, СИ, ЯУ, СП, ЕШ, НА, результат шифрования окажется таким:

«ЛСМЮДЬКЮВЁНИИНВФЕЮЯСКЮ»

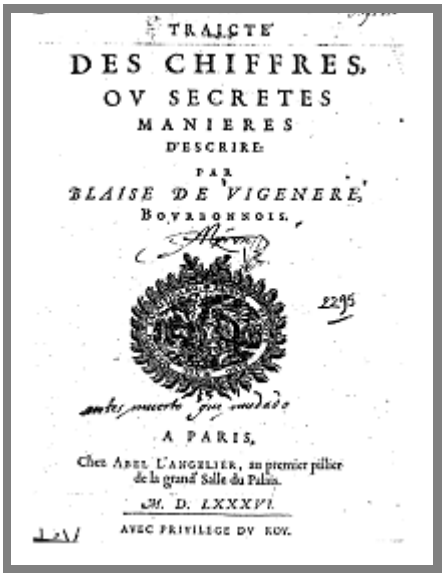
Каждый может легко убедиться, что, имея перед глазами ключевую таблицу, расшифровать эту криптограмму совсем нетрудно. А вот без ее помощи это уже довольно непростая задача.

Конечно, шифр Плейфера тоже не лишен многочисленных недостатков. Например, хотя относительная частота отдельных букв не сохраняется — но вот частота *буквенных пар* уже остается без изменения, что вполне может быть использовано для взлома. Кроме того, инверсия любой буквенной пары всегда преобразуется в другую инверсию (т. е. если «АБ» превращается в «XY», то «БА» превращается в «YX»). Это особенно заметно, когда пары встречаются в одном слове (например, последовательность букв «ИССИ» в слове «миссия» преобразовалась в «НИИН»). Поэтому некоторые устойчивые шаблоны букв при применении шифра сохраняются — что, конечно, является серьезной уязвимостью.

Тем не менее — даже при всех этих недостатках — шифр Плейфера использовался довольно долго. Известно, что он применялся британцами во время Англо-Бурской войны, затем во время Первой мировой, и даже находил определенное применение во время Второй мировой (хотя к этому времени, конечно, уже активно применялись другие, намного более совершенные методы шифрования).

Шифр Виженера

Шифр Виженера получил свое название в честь французского дипломата (и алхимика) XVI века Блеза де Виженера. По-видимому, название не вполне справедливо: хотя Виженер активно интересовался криптографией, но названный в его честь шифр придумал, видимо, не он. Более того, довольно похожий способ шифрования еще в XV веке в Венеции предлагал использовать Леон Батиста Альберти (так называемые диски Альберти). Также на шифр Виженера очень похож шифр Гронсфельда (последний существенно проще, так как ключ в нем состоит исключительно из цифр).


TRAICTE
DES CHIFFRES,
OV SECRETES
MANIERES
D'ESCRIRE
PAR
BLAISE DE VIGENERE,
BOVRBONNOIS.
A PARIS,
Chez ABEL L'ANGELIER, au premier pillier de la grand' Salle du Palais.
M. D. LXXXVI.
AVEC PRIVILEGE DV ROY.

Ил. 3. Титульная страница «Трактата о шифрах» Блеза де Виженера, 1586

Метод Виженера находил широкое практическое применение, например, во время гражданской войны в США, известной, как война между Севером и Югом.

По своей сути шифр Виженера является шифром *мультиподстановки*. А именно к разным буквам исходного сообщения применяются *разные* подстановочные шифры, последовательностью применения которых управляет выбранное *ключевое слово*.

Для применения шифра Виженера есть смысл заранее подготовить *таблицу подстановки*. (В отличие от метода Плейфера, сама эта таблица не является секретной, она употребляется только для удобства шифровки и дешифровки). Для русского языка (без букв «Ё», «Й» и «Ъ») она должна выглядеть примерно так.

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

Как легко заметить, каждая следующая строка этой таблицы представляет собой результат циклического сдвига предыдущей на одну позицию *влево*. Таким образом, таблица симметрична относительно главной диагонали. Процесс шифрования начинается с выбора ключевого слова. Для каждой буквы исходного текста и для каждой (по порядку) буквы ключевого слова выбирается символ, стоящий на пересечении соответствующей строки и столбца таблицы. (В каком порядке берется эта пара букв, несущественно ввиду диагональной симметрии таблицы). Буквы ключевого слова перебираются циклически: дойдя до последней буквы, возвращаемся к первой.

Попробуем зашифровать сообщение «ЗАДАНИЕ УСПЕШНО ВЫПОЛНЕНО», используя ключевое слово «САПФИР». Для начала, запишем под сообщением повторяющийся ключ:

ЗАДАНИЕ УСПЕШНО ВЫПОЛНЕНО
САПФИРС АПФИРСА ПФИРСАПФИ

В результате, получим такую криптограмму: «ШАУФХШЦ УАГОИЮО СПЧЮЬНФБЦ»

Заметим, что здесь, в отличие от шифра Плейфера, вполне можно сохранить разбиение на слова и знаки пунктуации. (Хотя для дополнительной секретности пробелы из криптограммы тоже можно полностью исключить.) Дешифровка криптограммы также выполняется просто, если известно ключевое слово. Выбирая последовательно буквы из ключевого слова, ищем в строке, соответствующей данной букве, очередную по порядку букву из криптограммы. Она указывает столбец, который соответствует очередной букве дешифрованного сообщения. (Ввиду диагональной симметрии таблицы можно, разумеется, делать все наоборот: буквы из криптограммы будут указывать на столбцы, а результат браться из строк.)

Основные проблемы с криптоалгоритмом Виженера состоят в том, что, по своей сути он является результатом множественного применения разных шифров Цезаря (которые, как мы помним, очень просты и крайне неустойчивы к взлому). Шифр также предъявляет жесткие требования к ключевому слову: оно должно быть достаточно длинным и повторения букв в нем крайне нежелательны. Криптоанализ шифра Виженера сильно упрощается, если удается угадать длину используемого ключевого слова. Если известно, что длина слова — N символов, то криптограмма разбивается на N различных последовательностей букв, каждую из которых можно рассматривать, как зашифрованную простым сдвиговым шифром. А тут уже легко можно применять все стандартные методы взлома, например частотный анализ.

Для определения длины ключа изобретены разные метод. Так, метод Фридриха Касицкого основан на частотном анализе биграмм в зашифрованном тексте. Он также легко реализуется на компьютере.

Решетка Кардано

Все шифры, о которых шла речь выше, были *подстановочными*. Рассмотрим теперь и *перестановочные* шифры. Наиболее популярные из них — шифры, ориентированные на использование так называемой *криптографической решетки*.

Ил. 4. Джероламо Кардано (1501—1576)

Традиционно принято связывать изобретение такого метода криптографии с именем *Джероламо Кардано* — великого итальянского мыслителя, математика и механика XVI века (помимо прочего, давшего свое имя карданному валу). Именно ему принадлежит идея использовать для шифрования лист бумаги (или другого материала) с прорезями. Прорези в листе заполняются буквами (или словами) кодируемого сообщения, затем лист убирается, и оставшиеся незаполненными строки заполняются (например) случайным текстом так, чтобы исходное сообщение оказалось скрытым внутри него. Впрочем, такой подход, конечно, крайне примитивен: «секретность» здесь сильно зависит от размера ячеек решетки, «постороннего» текста надо написать довольно много, и т. п. Однако совершенствование этого метода привело к изобретению криптографической решетки.

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

Ил. 5

Крипторешетка должна быть квадратной, хотя размер ее может варьироваться. Мы рассмотрим здесь решетку 8 * 8 как достаточно компактную, но при этом обеспечивающую высокий уровень секретности. Изготовить ее нетрудно с помощью следующего шаблона (ил. 5).

Все 64 ячейки заполнены числами от 1 до 16 (как легко заметить, каждое из них встречается ровно 4 раза — по одному разу в каждом из 4-х квадрантов). Для построения ключевой решетки, нужно произвольно выбрать в ней числа от 1 до 16 (для каждого из которых, очевидно, всего есть 4 варианта выбора). Как на ил. 6.

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

Ил. 6

Теперь осталось только аккуратно вырезать все черные квадратики — и решетка готова!

Использовать ее для шифрования нужно так. Кладем ее на чистый лист бумаги и аккуратно вписываем в отверстия по порядку буквы шифруемого сообщения слева направо и сверху вниз. После того как написаны первые 16 букв, аккуратно переворачиваем решетку на 90 градусов по часовой стрелке, и записываем следующие 16. Повторяем процедуру до тех пор, пока решетка не совершит полный оборот (так будет записано 64 символа исходного текста). После того как мы уберем решетку, мы увидим квадрат 8*8, заполненный буквами исходного сообщения, но при этом перемешанными до полной нечитаемости! Заметим, устройство решетки гарантирует, что при каждом повороте отверстия попадают на чистые, т. е. еще не заполненные места. Если в сообщении больше 64 букв, передвигаем решетку на чистое место, заполняем следующий квадрат и т. д. Для этого метода требуется, чтобы число букв в сообщении строго делилось на 64, поскольку в реальности редко получается так удачно и нужно дополнить исходное сообщение до кратного числа (лучше всего мешаниной из случайных букв). Но ни в коем случае нельзя оставлять в криптограмме незаполненные места (пробелы), так как они «расконспирируют» значительную часть используемой решетки!

Дешифровка сообщения осуществляется практически так же, как и шифровка. Мы прикладываем решетку к криптограмме и выписываем по порядку буквы, попавшие в отверстия. Дешифровав каждый квадрат (т. е. очередные 64 символа), переходим к следующему до тех пор, пока сообщение не будет полностью дешифровано.

Основное неудобство этого метода заключается в том, что ключом здесь является не число или кодовая фраза, а крипторешетка, т. е. (по сути) несложное физическое приспособление. Однако совершенно не требуется передавать адресату саму решетку, т.к. ему достаточно «рецепта» ее изготовления. Фактически единственными важными «параметрами» ключевой решетки являются ее размеры и положение отверстий в ней. Последнее (в большинстве случае) можно закодировать, например, просто перечислив номера квадратов с отверстиями в определенном порядке (например, справа налево и сверху вниз). Для использованной нами решетки такой код будет выглядеть так:

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

Эта последовательность из 16 чисел *однозначно* определяет используемую нами решетку, т. е. по сути она является достаточным ключом к любому сообщению, зашифрованному с ее помощью.

Надежность метода шифрования с помощью крипторешетки обусловлена тем, что таких ключевых решеток очень много. Так, нетрудно подсчитать, что для решетки 8*8 возможно 4^{16} возможных вариантов перфорации — а это больше 4 триллионов! Реально получится, конечно, заметно меньше (например, желательно исключить из использования решетки, в

которых отверстия прямо соседствуют). Но даже с поправкой на это, все равно количество возможных вариантов будет астрономическое! Поэтому взломать этот шифр, не имея ключевой решетки или точной информации о том, как ее изготовить, было практически нереально — во всяком случае, до наступления эры компьютеров.

Шифрование с помощью «решетки Кардано» также нашло свое отражение в художественной литературе. В известном романе Жюля Верна «Матиас Шандор» именно с помощью подобной решетки обменивались секретными сообщениями заговорщики, собиравшиеся поднять антиавстрийское восстание в Венгрии. В этой книге примечательно то, что, даже когда их записки были совершенно случайно перехвачены, полиция сумела их прочитать не методами «честного» криптоанализа, а лишь с помощью предателя, который сумел втереться заговорщикам в доверие и выкрасть ключ. Очевидно, Жюль Верн предполагал, что без явного предательства в сюжете заговор бы раскрыть просто не удалось, хотя заговорщики использовали простую крипторешетку 6*6, и это предположение, в общем, адекватно существовавшим возможностям криптографической науки XIX века. Реальный взлом этого шифра без ключа связан с появлением мощных компьютерных систем.

Ил. 7. Так называемый манускрипт Войнича — это загадочная рукопись предпо-ложительно XV века. В настоящее время хранится в библиотеке Йельского уни-верситета. До сих пор не известен ни язык этой рукописи, ни ее настоящее на-звание, ни ее автор.Не исключено и то, что она написана на каком-нибудь из европейских языков, но тщательно зашифрована.

Кстати, существует предположение, что именно с помощью крипторешетки или какого-то похожего приспособления был зашифрован легендарный манускрипт Войнича. Впрочем, так это или нет, точно сказать невозможно: этот манускрипт *никому* не удалось прочитать...

Загадки «Энигмы»

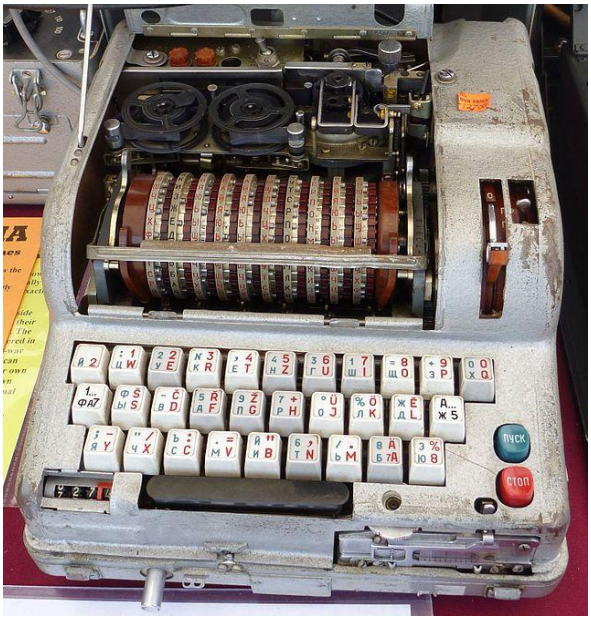
Конечно, любой рассказ о криптотехнологиях будет неполон без упоминания «Энигмы». Легендарная шифровальная машина Третьего рейха сыграла в истории довольно неоднозначную роль. С одной стороны, она долгое время считалась достаточно надежной, чтобы доверять ей самые серьезный военные тайны. С другой — именно необоснованная вера в ее надежность нанесла серьезный удар по секретам вермахта: ведь в конце концов

шифры «Энигмы» союзники тоже научились довольно успешно взламывать.

“Энигма” принадлежит к семейству так называемых *роторных* электромеханических шифровальных машин. Подобные выпускались во многих странах мира: США, Великобритании, Франции, Японии. Существовали и отечественные аналоги: советская шифровальная машина «Фиалка М-125» активно использовалась и после Второй мировой.

Внешне «Энигма» напоминала обыкновенную пишущую машинку, оснащенную стандартной латинской клавиатурой. Однако, в отличие от пишущей машинки, устройством вывода для нее является не лист бумаги, а набор лампочек (каждая из них соответствует одной букве).

Ил. 8. Шифровальная машина «Энигма» (трёхроторная модификация)



Ил. 9. А это советский ответ на «Энигму» - десятиро-торная шифровальная машина «Фиалка М-125». Инте-ресно, что вместо штеккерного коммутатора «Эниг-мы» в «Фиалке» применялись бумажные перфокарты (еще до эры ЭВМ!). Кроме того, «Фиалка» могла выда-вать результат на лист бумаги или на перфоленту.

Сердцем шифромашины является набор *роторов* — дисков, изготовленных из изолирующего материала (чаще бакелита) с электрическими контактами. Этих роторов было несколько (в разных модификациях от трех до четырех), и соединены они были последовательно.

Проходя через все роторные соединения, электрический ток заставлял зажечься одну из лампочек (какую именно — зависело от роторов, их поворота и последовательности их подключения). Каждый ротор по своей функциональности реализует некий алгоритм простой подстановки, заменяя «входящий» символ на «исходящий». Если бы в процессе шифрования все роторы всегда находились в одном положении, это стало бы

эквивалентом той же «простой замены» (взлом которой, как мы помним, несложен). Секрет шифромашины в том, что роторы *вращались*. После кодирования каждой буквы первый ротор перемещается на одну позицию. Таким образом, следующая буква сообщения будет закодирована уже совсем иным подстановочным шифром. После того как первый ротор завершит полный оборот, на одну позицию сдвигается второй, после него — третий и т. п. Получается, что роторы вращаются подобно автомобильному счетчику километража (одометру) с той разницей, что шаг их поворота тоже может меняться. За счет этого практически к каждой букве исходного сообщения применяется свой уникальный метод шифрования. Рано или поздно, конечно, все роторы совершат полный цикл и вернутся к началу, однако для этого кодируемое сообщение должно быть *очень* длинным. Реальные сообщения, разумеется, были намного короче. В дополнение к роторному механизму, в аппарате присутствовал *штеккерный коммутатор,* соединения которого вносили дополнительную сложность в шифр (хотя в отличие от роторов они устанавливались один раз и в процессе шифрования / дешифровки уже не изменялись).

Само устройство «Энигмы», разумеется, не было особым секретом, ведь корпорация «Chiffriermaschinen AG» массово выпускала эти шифровальные машины еще с 1923 года. Подсчитано, что всего было выпущено не менее 100 000 машин разных модификаций. Конечно, у всех заинтересованных сторон, включая разведки стран-союзниц, действующие «Энигмы» имелись. Секретом шифра были только установки шифромашины. Собственно, ключ «Энигмы» определяется тремя наборами параметров: выбором роторов и их относительного расположения (*Walzenlage*), начальными позициями роторов (*Ringstellung*) и выбранными подключениями на штеккерном коммутаторе (*Steckerverbindungen*). Без точного знания всего перечисленного корректная дешифровка сообщения невозможна, ибо для наиболее распространенной военной модификации машины (четырехроторной) общее число возможных ключей измеряется *миллиардами*.

Каким же образом удавалось взламывать шифры «Энигмы»? Одним из факторов успеха было то, что союзники привлекли к дешифровке величайшие математические умы столетия. Прежде всего одного из «отцов кибернетики» Алана Тьюринга. Для борьбы с «Энигмой» впервые были применены электронные дешифровальные машины. Фактически, это были уже предки нынешних компьютеров. Эти машины, получившие прозвище «бомбочки», так как в процессе работы они ритмично «тикали», как часовой механизм бомбы, позволяли автоматически перебирать сотни возможных шифров «Энигмы» за минуты.

Однако даже с их помощью дешифровка была бы невозможна, если бы не некоторые уязвимости самой шифромашины. Одна из них заключалась в том, что «Энигма» *никогда* не шифровала какой-либо символ сам в себя. Как ни странно, именно эта особенность ее работы

оказалось уязвимостью, причем достаточно серьезной (особенно, когда шифротекст был достаточно длинным).

Наконец, взломать «Энигму» помогали ошибки ее пользователей (иногда грубые). Многие закодированные ею сообщения строго соответствовали определенному шаблону. Например, зашифрованные метеосводки (для немецких подводных лодок) часто начинались с одних и тех же позывных, которые дешифровщикам были уже известны. Один из уроков, который можно извлечь из истории «Энигмы», заключается в том, что даже самая надежная шифровальная техника может быть скомпрометирована, если грубо нарушать дисциплину ее использования.

Об «Энигме» и британской команде ее дешифровщиков из Блетчли-парка существует обширная литература, как специальная, так и художественная. Не так давно, в 2001 году, был снят даже полнометражный фильм («Энигма», 2001). Однако самих шифромашин сохранилось не так уж много, в основном в музеях. Кстати, в музее криптографии в Форт-Миде (штаб-квартире АНБ) тоже имеются экземпляры «Энигмы», причем некоторые из них действующие, несмотря на прошедшие десятилетия.

Список литературы:

1. [Электронный ресурс]. – Режим доступа: URL: http://crypto.hut2.ru/ (дата обращения: 20.08.2014).

2. [Электронный ресурс]. – Режим доступа: URL: http://mind-control.wikia.com/wiki/%D0%A8%D0%B8%D1%84%D1%80_Playfair (дата обращения: 20.08.2014).

3. [Электронный ресурс]. – Режим доступа: URL: http://www.cryptomuseum.com/crypto/fialka/ (дата обращения: 20.08.2014).

4. [Электронный ресурс]. – Режим доступа: URL: http://kriptografea.narod.ru/ (дата обращения: 20.08.2014).

5. [Электронный ресурс]. – Режим доступа: URL: http://habrahabr.ru/post/103055/ (дата обращения: 20.08.2014).

6. [Электронный ресурс]. – Режим доступа: URL: http://samlib.ru/m/marchenko_a_m/enigma.shtml (дата обращения: 20.08.2014).

7. [Электронный ресурс]. – Режим доступа: URL: http://www.jproc.ca/crypto/russian_m125_fialka.html (дата обращения: 20.08.2014).

Сведения об использованных иллюстрациях:

Иллюстрация содержания. [Электронный ресурс]. – Режим доступа: URL: http://www.bezpeka.com/ru/news/2010/09/02/Researchers-discover-flaw-in-quantum-cryptography.html (дата обращения: 20.08.2014).

Ил. 1. [Электронный ресурс]. – Режим доступа: URL: http://www.masters.donntu.edu.ua/2013/frt/gryshko/ind/index.htm (дата обращения: 20.08.2014).

Ил. 2. Лорд Лайон Плейфер [Электронный ресурс]. – Режим доступа: URL: http://www.sil.si.edu/digitalcollections/hst/scientific-identity/fullsize/SIL14-P004-04a.jpg (дата обращения: 20.08.2014).

Ил. 3. Титульный лист «Трактата о шифрах...» [Электронный ресурс]. – Режим доступа: URL: http://gallica.bnf.fr/ark:/12148/bpt6k73371g (дата обращения: 20.08.2014).

Ил. 4. Джероламо Кардано [Электронный ресурс]. – Режим доступа: URL: http://www.bdn-steiner.ru/modules/Coppermine/albums/Deyateli/ev-15a-Kardano.jpg (дата обращения: 20.08.2014).

Ил. 7. «Рукопись Войнича» (разворот) [Электронный ресурс]. – Режим доступа: URL: https://ru.wikipedia.org/wiki/%D0%A0%D1%83%D0%BA%D0%BE%D0%BF%D0%B8%D1%81%D1%8C_%D0%92%D0%BE%D0%B9%D0%BD%D0%B8%D1%87%D0%B0#mediaviewer/%D0%A4%D0%B0%D0%B9%D0%BB:68r.jpg (дата обращения: 20.08.2014).

Ил. 8. «Энигма» [Электронный ресурс]. – Режим доступа: URL: http://img.theranking.com/card/51566/image/19420c611b982671cd25bcbb2db003f2/resize_image.jpg (дата обращения: 20.08.2014).

Ил. 9. «Фиалка М-125» [Электронный ресурс]. – Режим доступа: URL: https://upload.wikimedia.org/wikipedia/commons/thumb/0/0f/Fialka_P1010706.jpg/220px-Fialka_P1010706.jpg (дата обращения: 20.08.2014).