Государственное бюджетное общеобразовательное учреждение

гимназия № 73 «Ломоносовская гимназия» Выборгского района Санкт-Петербурга

Развитие полиалфавитных шифров в эпоху Возрождения.

Шифр Виженера

Работу выполнил: Боревич Андрей Алексеевич, 5.3 класс;

Руководители: Трофимова Светлана Николаевна,
Боревич Алексей Альбертович,
Боревич Ирина Сергеевна

Санкт-Петербург 2014 год

Оглавление

Введение

В ходе моей прошлой работы («Криптография в древнем мире») я познакомился с шифрами древности: квадратом Полибия, диском Цезаря, скиталой, диском Энея. В этой работе я решил проследить дальнейшую эволюцию методов шифрования и уделить внимание развитию полиалфавитных шифров в эпоху Ренессанса. Одним из таких шифров является шифр Виженера.

У меня интерес к этой теме возник после прочтения книги Саймона Сингха «Книга шифров: тайная история шифров и их расшифровки». Кроме того, я использовал и другие

Я выбрал именно этот шифр из-за его близости к уже знакомому мне шифру Цезаря. Он также является шифром алфавитной замены, но шифр Цезаря моноалфавитный (то есть основанный на одном алфавите), а шифр Виженера – полиалфавитный. Именно поэтому шифр Виженера на протяжении длительного периода не могли взломать. В то время это был принципиально новый вид шифрования.

В наши дни криптография находит всё больше применений. Ценность информации возрастает, и для защиты личных данных приходится использовать всё более современные методы шифрования. Шифр Виженера – один из взломостойких шифров и хорошо подходит для защиты персональных данных. Однако, взломать этот шифр можно, поэтому в настоящее время он не подходит для защиты им корпоративных и государственных секретов.

Цель работы:

- Изучение шифра Виженера, истории его создания и развития, структуры, для создания прикладной программы, реализующей его алгоритм.

Задачи работы:

- Проследить историю развития шифра Виженера
- Раскрыть его особенности и слабые места
- Проанализировать математический аппарат шифра Виженера
- Создать информационную модель шифра Виженера
- Популяризировать информацию по шифру Виженера

Методы:

- Изучение литературы
- Теоретический анализ программ других авторов
- Написание собственной программы шифрования по методу Виженера

Глава 1. История развития полиалфавитных шифров

Моноалфавитные шифры, которые мы рассматривали в прошлой научной работе, стали устаревать в результате развития в арабских странах, а затем и в Европе, метода частотного криптоанализа.[1]

Теперь любой человек, посылающий зашифрованное сообщение, уже не мог быть уверен, что недоброжелатель не сможет расшифровать его в случае перехвата. Именно так возникла идея полиалфавитных шифров.

В эпоху Возрождения значительные успехи в области криптографии были сделаны благодаря работам первых криптографов, развивавших идею полиалфавитных шифров (Леон Баттиста Альберти, Иоганн Тритемий, Джованни Порта, Блез де Виженер).

В то время непрерывная вражда Итальянских городов-государств, требовала усиленных методов криптографии для защиты дипломатической и коммерческой переписки.

Саймон Сингх приводит в своей работе «Книга шифров» такую историю про возникновение первого полиалфавитного шифра. В 60-е годы XV века выдающийся флорентийский ученый-энциклопедист Леон Баттиста Альберти столкнулся со своим другом Леонардо Дато, который в то время работал секретарем у Папы Римского. Дато завел с Альберти разговор о криптографии и сложностях в ней. Используемые в то время шифры замены требовали отдельного шифралфавита для зашифровывания каждого сообщения! Альберти предложил использовать два или более шифралфавита в одном сообщении, переходя от одного к другому в процессе зашифровывания и сбивая этим с толку возможных криптоаналитиков.

Для переключения между алфавитами Альберти использовал металлический шифровальный диск (1467 год)[2]. Система Альберти

[1] Цыганов А.В., «Криптография и криптоанализ», СПбГУ, 2009, стр.9
[2] См. Приложение 2.

переключает алфавиты после нескольких зашифрованных слов. Несмотря на то, что Альберти совершил самый значительный за более чем тысячу лет переворот в криптографии, он не сумел довести свою идею до целостной системы.

После Альберти разработкой алгоритмов полиалфавитного шифрования занимались Джованни Порта (1535-1615 гг.) и Иоганн Тритемий (1462-1516 гг.). В 1518 году Иоганн Тритемий в своей работе «Полиграфия» изобрел tabula recta – первую таблицу для полиалфавитного шифрования[3].

В tabula recta 24 буквы латинского алфавита располагались в квадрате, содержащем 24 строки (буквы «i» и «j», а также «u» и «v» считались одинаковыми). Таблица получается путём сдвига обычного алфавита в каждой следующей строке на одну позицию влево. При шифровании первая буква послания шифруется с помощью алфавита, расположенного в первой строке таблицы: вторая – с помощью второго и так далее.[4] Из-за использования разных алфавитов в процессе шифрования, зашифрованное послание не поддавалось классическому частотному криптоанализу, поскольку одинаковые буквы в шифртексте обозначались разными символами.

Дальнейшее развитие полиалфавитных шифров учёные связывают с именем Виженера.

Блез де Виженер (1523 – 1595) родился в деревне Сен-Пурсен-сюр-Сиуль (Франция). Служил секретарём в Вормсском рейхстаге, где свёл полезные знакомства в церковных и дипломатических кругах. Благодаря этим знакомствам, он поступил на службу к герцогу Неверскому, в составе дипломатической миссии в 1554 и 1566 годах посещал Рим. В этих поездках он познакомился с книгами о криптографии.

---

[3] См. Приложение 3.

[4] Риксон Ф. Б., «Коды, шифры и тайная передача информации», М: АСТ, 2011, стр.191

В возрасте 47 лет он вышел на пенсию и написал более 20 трудов, в том числе «Трактат о шифрах и тайнописи» (1586 год).

Удивительно, что сам он не придавал большого значения криптологии, считая её «бесполезной тратой времени и ума». [5]

Блез де Виженер предложил использовать в качестве координат букв перемешанные алфавиты, включающие в себя даты и ключевые фразы. Повторяющиеся буквы пропускаются, а оставшиеся буквы алфавита дописываются после фразы.[6] Но впоследствии, в качестве координат стали использовать простой алфавит.

Виженер не сам придумал то, что мы сейчас называем шифром Виженера. Впервые шифр на основе tabula recta Тритемия, с ключом, используемым для переключения между алфавитами шифра не подряд, а в определенном порядке, описал Беллазо в своей работе «Шифр синьора Джованни Батиста Беллазо».

Изобретение шифра было присвоено Блезу де Виженеру, потому что именно он изложил его описание комиссии Генриха III в 1586 году, и шифр стал активно использоваться для обеспечения секретности государственной переписки.

Хотя шифр Виженера считался не взламываемым, над методами его вскрытия трудились видные умы, в их числе Леон Альберти и Джованни Порта. Последний вплотную подошёл к решению этой проблемы: «Поскольку между первыми тремя M и этими же тремя буквами, повторенными в 13-м слове, находится 51 буква, я прихожу к выводу, что ключ повторен три раза и правильно считаю, что он содержит 17 букв». [7] К сожалению, Порта так и не смог сделать практические выводы из этих

[5] Риксон Ф. Б., «Коды, шифры и тайная передача информации», стр.547
[6] Риксон Ф. Б., «Коды, шифры и тайная передача информации», стр.192
[7] Давид Кан «Взломщики кодов», М: Центрполиграф, 2000, стр.14

наблюдений, и шифр Виженера не поддавался взлому вплоть до середины XIX века, хотя иногда и были случаи угадывания ключа.

В 1868 году, в своей статье «Алфавитный шифр» писатель и математик Чарльз Лютвидж Доджсон (Льюис Кэрролл) назвал не взламываемым шифр Виженера.

Однако, Кэрролл ошибался: уже в 1854 году эксцентричный английский гений Чарльз Бэббидж (автор прообраза современного компьютера)[8] нашёл способ взлома шифра Виженера, но нигде не опубликовал его. Он занимался взломом «нового» шифра, «изобретённого» Джоном Твэйтсом. Бэббидж доказал, что шифр Твэйтса на самом деле являлся частным случаем шифра Виженера, и успешно расшифровал предложенный Твэйтсом текст, который оказался поэмой «The Vision of Sin» Альфреда Теннисона, зашифрованной ключевым словом Emily – именем жены поэта.[9]

Почему же Бэббидж не опубликовал свою работу? Саймон Сингх пишет, что «была у него такая привычка – бросать незавершёнными значительные и многообещающие начинания и не сообщать о своих открытиях».[10] Но более вероятной представляется версия, что работа осталась не опубликованной из-за военно-политической обстановки того времени: начиналась Крымская война, и технология взлома полиалфавитных шифров давала преимущество Англии.

Действуя независимо от Бэббиджа, прусский шифровальщик Фридрих Вильгельм Касиски (1805–1885) в 1863 году первым опубликовал успешный алгоритм атаки на шифр Виженера в своей работе «Секретное письмо и

[8] http://ru.wikipedia.org, статья «Бэббидж, Чарльз»
[9] http://ru.wikipedia.org, статья «Шифр Виженера»
[10] Сингх Саймон, «Книга шифров: тайная история шифров и их расшифровки», М: АСТ, 2007, стр.97

искусство дешифрования» (нем. Die Geheimschriften und die Dechiffrierkunst)[11].

Предложенный им способ взлома известен как «метод Касиски» и стал прорывом в криптографии. В следующей главе мы подробнее рассмотрим этот метод.

[11] http://ru.wikipedia.org, статья «Криптоанализ полиалфавитных шифров»

Хронологическая таблица

Автор	**Время**	**Результат**	**Недостатки**
Леон Баттиста Альберти	1467 год	Предложил использовать два или более шифралфавита в одном сообщении.	Не было ключа. Алфавит сменялся через определённое число позиций.
Джованни Порта	1535-1615 гг.	Усовершенствовал систему шифрования при помощи диска Альберти. Вплотную подошёл к идее взлома полиалфавитного шифра.	
Иоганн Тритемий	1518 год	Изобрел tabula recta – первую таблицу для полиалфавитного шифрования.	Алфавиты переключались подряд, а не в определённой последовательности.
Джованни Баттиста Беллазо	1553 год	Ввёл ключ для переключения между алфавитами.	Не смог продвинуть свою идею на государственном уровне.
Блез де Виженер	1586 год	Доработал систему и представил её королю Генриху III, а также изобрел модификации шифра.	

Глава 2. Практика шифрования и взлома шифра Виженера

В данной главе мы рассмотрим основные алгоритмы шифрования и взлома шифра Виженера, а также модификации шифра (бегущий ключ).

Мы выведем математическую формулу, реализующую алгоритм шифра Виженера, и опишем созданную нами прикладную программу, выполняющую зашифровку и расшифровку по методу Виженера.

Хотя Блез де Виженер предлагал использовать в качестве координат букв перемешанные алфавиты, чаще всего, в качестве координат использовали простой алфавит. Именно этот алгоритм мы и рассмотрим.

В отличие от более ранних шифров, шифру Виженера особую стойкость придавало то, что в нём использовался не один, а 26 (33 для русского языка) алфавита, где каждый следующий сдвигался на букву влево относительно предыдущего алфавита[12].

Таким образом, 1-ый ряд представляет собой алфавит шифра Цезаря со сдвигом на 1 позицию, то есть этот шифралфавит может использоваться в качестве алфавита шифра Цезаря. Точно так же 2-ой ряд является алфавитом шифра Цезаря со сдвигом на 2 позиции и т. д.

Над открытым текстом писался многократно повторяющийся ключ, и каждая буква ключа соответствовала букве в верхнем алфавите, а буква открытого текста – букве в левом алфавите. Буква, находящаяся на пересечении столбца и строки, являлась буквой шифртекста.

Поясним на примере. Возьмём в качестве открытого текста начало известного детского стихотворения, а в качестве ключа фамилию автора:

Открытый текст	Е	С	Л	И	В	Ы	П	О	К	О	Р	И	Д	О	Р	У	М	Ч	И	Т	Е	С	Ь
Ключ	О	С	Т	Е	Р	О	С	Т	Е	Р	О	С	Т	Е	Р	О	С	Т	Е	Р	О	С	Т
Шифртекст	У	Г	Ю	Н	Т	Й	Б	Б	П	Я	Я	Ъ	Ц	У	Б	В	Ю	Й	Н	Г	У	Г	О

[12] См. Приложение 4.

Видно, что одинаковые буквы открытого текста шифруются по разному: первая буква «О» шифруется буквой «Б», вторая буква «О» шифруется буквой «Я», третья буква «О» шифруется буквой «У»). Именно из-за этого шифр Виженера так трудно взломать.

Буква шифртекста получается из соответствующей буквы открытого текста сдвигом на столько позиций (по алфавиту), на сколько буква ключа отдалена от первой буквы алфавита. Например, буква ключа «К» (11 позиций от «А») преобразует букву открытого текста «О» в букву «Щ» шифртекста. Буква «О» - 16-ая буква алфавита (сдвинута на 15 позиций от буквы «А»), буква «Щ» - 27-ая буква (сдвинута на 26 позиций от «А»). Та же буква ключа «К» преобразует букву открытого текста «Ц» (сдвиг 23) в букву алфавита со сдвигом 34. В русском алфавите 33 буквы, поэтому вместо буквы со сдвигом 34 мы возьмём букву со сдвигом 1 (34-33=1) – это буква «Б». Для математической записи такого преобразования подходит операция деления с остатком:

$(11+15) \bmod 33 = 26;$

$(11+23) \bmod 33 = 1.$

В общем виде (K – расстояние от текущей буквы ключа до первой буквы алфавита, T – расстояние от текущей буквы открытого текста до первой буквы алфавита, R – расстояние от текущей буквы шифртекста до первой буквы алфавита):

$(K+T) \bmod 33 = R.$ [13]

Бегущий ключ

Виженер придумал модификацию шифра с использованием открытого текста в качестве ключа: бегущий ключ. Здесь в качестве ключа используется

[13] Выведенная мной формула аналогична приведенной в книге: Ященко В.В., ред. «Введение в криптографию», М: МЦНМО, 2000

одна буква (первичный ключ), а каждой следующей буквой ключа становится буква открытого текста.

Например:

(Ж – первичный ключ)

Открытый текст	Е	С	Л	И	В	Ы	П	О	К	О	Р	И	Д	О	Р	У	М	Ч	И	Т	Е	С	Ь
Ключ	Ж	Е	С	Л	И	В	Ы	П	О	К	О	Р	И	Д	О	Р	У	М	Ч	И	Т	Е	С
Шифртекст	Л	Ц	Э	Ф	К	Э	К	Ю	Щ	Щ	Я	Щ	М	Т	Я	Д	А	Д	А	Ы	Ч	Ц	Н

Для расшифровки сообщения адресат, знающий первую букву ключа, находит первую букву открытого текста, которая становится следующей буквой ключа.

Прикладная программа. Описание

Я создал прикладную программу, реализующую алгоритм шифра Виженера. Чтобы познакомить с шифром Виженера больше людей, программа реализована на языке программирования PHP и размещена в интернете на сайте http://andrey.borevich.ru.

Листинг программы приведён в Приложении 5.

Созданная программа подходит для шифрования только на русском языке. Все символы, отличные от русского алфавита, шифруются и дешифруются не корректно.

В программных средах используются различные кодировки для букв русского алфавита. Чтобы избежать проблем с разными кодировками, программа производит замену символов. Символы кириллицы (заглавные буквы от «А» с индексом 0, и до «Я» с индексом 32, и строчные: от «а» с индексом 0, до «я» с индексом 32), находятся и преобразуются в заглавные латинские буквы. Недостающие заглавные латинские символы дополняются строчными (у «A» индекс 0, у «Z» индекс 25, у «a» (латинской) индекс 26, у «b» - 27 и т. д.). Дальше буквы латинского алфавита преобразуются в числа

(индексы букв от 0 до 32), с которыми работать проще. Алгоритм шифрования прост: каждый индекс буквы текста складывается с индексом буквы ключа и нацело делится на количество букв в алфавите. Остаток от деления и будет индексом буквы шифртекста. После использования этого алгоритма для каждой пары букв (буква ключа + буква текста), получаем индексы букв шифртекста. Далее, индексы преобразуются в буквы латиницы, которые преобразуются в заглавные буквы кириллицы. Поэтому при вводе латинских символов, в конце они преобразуются в кириллические эквиваленты. Также программа производит удаление «ненужных» символов (пробелы и знаки пунктуации).

Взлом шифра

На протяжении трёх веков шифр Виженера считался не взламываемым. Первые успешные попытки взлома этого шифра были предприняты в XIX веке. В разное время, в разных странах, независимо друг от друга, два человека изобрели метод взлома шифра Виженера. Это были Чарльз Беббидж и Фредерик Касиски (в некоторых источниках «Касицки, Казиски»).

Этот метод был основан на определении длины ключа (ключевой фразы). Если нам известна длина ключа, то весь зашифрованный текст мы можем разбить на фрагменты, каждый из которых кодируется одинаково, и, используя частотный криптоанализ, расшифровать сообщение.

Но для того, чтобы вскрыть длину ключа, нужно приложить много усилий.

Попробуем проанализировать методом Касиски следующий текст: «УГЮНТЙББПЯЯЪЦУБВЮЙНГУГОТРРЦЮУВЧБЧИХОЯТЖВБВЧЬДРСЯНШРСАТЯШУНЭХЪБТФРЮАХШЬНДОТХАУБХРЁЪФЕЪБЦФПДДЯРЖЫВЖАЙГРЦГИЛШЖБРЯТЪЮБЮЧЬЕУБЫАЪНГУЭЁЬИУУВЕАВБТФРЫРХПЩШААФБЭГЕНГ». Этот зашифрованный текст содержит повторяющиеся биграммы: например, «НГ» (позиции 19, 124 и 154), «ОТ» (позиции 23 и 73) и «РС» (позиции 46 и 51). Биграмма «НГ» повторяется на расстоянии в 105 и

30 позиций, «ОТ» - на расстоянии в 50 позиций, «РС» - на расстоянии в 5 позиций. Скорее всего, длина ключа равна 5. Далее методом частотного криптоанализа можно взломать текст. Это известное детское стихотворение Григория Остера из книги «Вредные советы», а в качестве ключа используется фамилия автора.

Рассматриваемый метод требует некоторого везения, так как в тексте могут возникать «случайные» биграммы. Их вероятность много ниже, чем у «регулярных», но в небольших текстах они могут значительно усложнить расшифровку. Взломать короткие фразы таким методом очень сложно из-за редкого возникновения биграмм.

Есть ещё один метод определения длины ключа, предложенный Вильямом Фридманом в 1920 году[14].

Суть метода в циклическом сдвиге сообщения. Полученные таким образом сообщения записываются под оригинальным шифртекстом и подсчитывается число совпавших букв в верхней и нижней строке. На основе этих чисел вычисляется индекс совпадений, равный отношению количества совпадений к полной длине сообщения. Для русских текстов индекс совпадений равен примерно 6%[15]. В то время как для случайных текстов этот индекс равен 1/32, то есть приблизительно 3%. На этом факте и основан метод Фридмана. Текст записывается со сдвигом в 1, 2, 3 и т. д. позиции, и для каждого сдвига вычисляется индекс совпадений.

[14] ru.wikipedia.org, статья «Фридман, Уильям Фредерик»
[15] ru.wikipedia.org, статья «Индекс совпадений»

Попробуем проанализировать методом Фридмана наш текст. Посмотрим, при каких сдвигах индекс совпадений больше 6%. Циклически сдвигая шифртекст, получаем:

При сдвиге на	Количество совпадений	Индекс совпадений	
13	11	7,1%	
20	10	6,5%	
25	10	6,5%	
37	11	7,1%	
49	11	7,1%	
50	13	8,4%	
55	14	9%	
59	10	6,5%	
75	13	8,4%	
80	13	8,4%	
96	10	6,5%	
100	14	9%	
105	13	8,4%	
106	11	7,1%	
118	11	7,1%	
130	10	6,5%	
135	10	6,5%	
142	11	7,1%	

При сдвиге текста на длину, равную длине ключа, индекс резко возрастает, следовательно, длина ключевого слова, скорее всего, равна 5. Понять, почему индекс резко возрастает, довольно просто. В случае, когда

все символы сдвигаются на одну и ту же позицию, индекс совпадения такой же, как и у исходного текста. В случае, когда мы вычисляем индекс для шифра Виженера, мы во всех случаях (кроме того, где длина сдвига равна длине ключа) сравниваем фактически случайный текст.[16]

[16] Данный метод описан на сайте http://habrahabr.ru/post/103055/

Заключение

В этой работе мы рассмотрели историю создания и взлома полиалфавитных шифров, вершиной которых стал шифр Виженера, создали прикладную программу, шифрующую и дешифрующую сообщения. Теперь мы можем, опираясь на изложенную выше информацию, сделать выводы:

1. Шифр Виженера стоек против «ручного» взлома (быстрого взлома без оборудования и использования программного обеспечения) и хорошо подходит для защиты личных, оперативных данных, которые важны лишь недолгое время, а потом теряют свою ценность, или данных, которые практически невозможно перехватить.

2. Шифр Виженера не может долго противостоять взлому, и, с учётом развития современного криптоанализа, он не подходит для шифрования им важной информации.

3. Шифр Виженера нельзя взломать методом частотного криптоанализа, который опирается на повторение символов, потому что в шифре Виженера одна и та же буква открытого текста может шифроваться по разному.

4. Все методы взлома шифра Виженера основаны на нахождении длины ключа. Эти методы были открыты лишь в XIX веке, что позволило шифру на протяжении трёх веков считаться не взламываемым.

Я создал прикладную программу для шифрования по методу Виженера. Программа помогает шифровать гораздо быстрее и точнее, чем вручную с использованием квадрата Виженера. Все желающие могут использовать её на сайте http://andrey.borevich.ru.

В наше время шифрование информации всё более важно. Необходимо скрывать информацию от всех конкурентов, политических соперников, разведки других стран или прессы. Конечно, шифр Виженера не очень стоек,

и в следующей работе мы сможем рассмотреть более сложные функции шифрования, в том числе признанные невзламываемыми.

Приложения

Приложение 1. Глоссарий

Биграмма – две стоящие рядом буквы

Дешифровка – удаление шифра, скрывающего содержание сообщения. Выполняется адресатом, имеющим верный ключ.

Индекс совпадений – количество (процент) совпадающих символов или групп символов в сообщении (тексте).

Ключ – инструкции, которые управляют ходом шифрования (кодирования) и расшифровки (раскодирования) сообщений.

Код – способ сокрытия информации с использованием слов, чисел или слогов, для замены исходных слов или фраз сообщения. При применении кодов заменяются целые слова, в то время как в кодах заменяются буквы или пары букв.

Криптография – методы сокрытия содержания сообщения с помощью кодов или шифров.

Криптоанализ (взлом) – процесс извлечения открытого текста из зашифрованного сообщения без знания ключа.

Моноалфавитный шифр – шифр, основанный на нахождении буквы в одном алфавите, и заменой её на другой символ (всегда один и тот же), соответствующий ей.

Открытый (исходный) текст – сообщение, передаваемое без шифрования или кодирования, а также сообщение до того, как его зашифруют или после того, как его расшифруют.

Полиалфавитный шифр – шифр, в котором для одной буквы есть несколько эквивалентов, между которыми происходит переключение по определённой схеме.

Шифр (от арабского «сифр» – «никто, пустота») – алгоритм, по которому производится замена букв открытого текста на буквы шифртекста.

Закрытый текст (шифртекст) – результат применения алгоритма шифрования к тексту. Зашифрованный текст является закрытым текстом (шифртекстом).

Шифрование – процесс преобразования открытого текста на основе алгоритма и ключа, в результате которого возникает зашифрованный текст.

Шифралфавит – алфавит, в который преобразуется обычный алфавит.

Приложение 2. Диск Альберти

Recta transpositionis tabula.

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

In hac tabula literarũ canonica siue recta tot ex uno & usuali nostrę latinarum literarum ipsarum per mutationem seu transpositionẽ babet alphabeta, quot in ea per totum sunt monogrammata, uidelicet quater & uigesies quatuor & uiginti, quæ faciunt in numero D.lxxvi. ac per totidẽ multiplicata, paulo efficiunt minus q̃ quatuordecẽ milia.

Приложение 4. Квадрат (таблица) Виженера для русского алфавита

а	**б**	**в**	**г**	**д**	**е**	**ё**	**ж**	**з**	**и**	**й**	**к**	**л**	**м**	**н**	**о**	**п**	**р**	**с**	**т**	**у**	**ф**	**х**	**ц**	**ч**	**ш**	**щ**	**ъ**	**ы**	**ь**	**э**	**ю**	**я**
б	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А
в	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б
г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В
д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г
е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д
ё	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е
ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ё
з	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ё	Ж
и	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ё	Ж	З
й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	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	А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й
л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К
м	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л
н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М
о	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н
п	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О
р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П
с	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П	Р
т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С
у	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т
ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У
х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф
ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х
ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц
ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч
щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш
ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	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	Ё	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ
ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы
э	Ю	Я	А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь
ю	Я	А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э
я	А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю

Приложение 5. Прикладная программа на языке PHP

```
<p>На этой странице вы можете зашифровать или расшифровать текст по методу Вижинера. Для ввода текста и шифрключа необходимо использовать только буквы русского алфавита (в любом регистре). Обратите внимание, что при вводе прочих символов (в том числе букв английского алфавита) преобразования могут выполняться некорректно.</p>
<form method="get">
Введите текст: <input name="text" type="text" autofocus size="60" /><br />
Введите ключ: <input name="code" type="text" size="30" maxlength="256" /><br />
<input name="beginencode" type="submit" value="Зашифровать" />
<input name="begindecode" type="submit" value="Расшифровать" /><br />
</form>
<?php
//--Задаём массив с заглавными буквами алфавита языка сообщения--//
$rusl=array('А','Б','В','Г','Д','Е','Ё','Ж','З','И','Й','К','Л','М','Н','О','П','Р','С','Т','У','Ф','Х','Ц','Ч','Ш','Щ','Ъ','Ы','Ь','Э','Ю','Я');
//--Задаём массив со строчными буквами алфавита языка сообщения--//
$rus2=array('а','б','в','г','д','е','ё','ж','з','и','й','к','л','м','н','о','п','р','с','т','у','ф','х','ц','ч','ш','щ','ъ','ы','ь','э','ю','я');
//--Задаём массив для замещения кирилических символов--//
$eng=array('A','B','C','D','E','F','G','H','I','J','K','L','M','N','O','P','Q','R','S','T','U','V','W','X','Y','Z','a','b','c','d','e','f','g');
//--Задаём массив с ненужными символами--//
$symbl=array(' ',',','.','!','?',':',';','-');
//--Задаём массив для замещения ненужных символов--//
$symb2=array('','','','','','','','');
//--Задаём массив для перевода латинских символов в числа--//
$dictl=array('A'=>0,'B'=>1,'C'=>2,'D'=>3,'E'=>4,'F'=>5,'G'=>6,'H'=>7,'I'=>8,'J'=>9,'K'=>10,'L'=>11,'M'=>12,'N'=>13,'O'=>14,'P'=>15,'Q'=>16,'R'=>17,'S'=>18,'T'=>19,'U'=>20,'V'=>21,'W'=>22,'X'=>23,'Y'=>24,'Z'=>25,'a'=>26,'b'=>27,'c'=>28,'d'=>29,'e'=>30,'f'=>31,'g'=>32);
//--Задаём массив для перевода чисел в латинские символы--//
$dict2=array(0=>'A',1=>'B',2=>'C',3=>'D',4=>'E',5=>'F',6=>'G',7=>'H',8=>'I',9=>'J',10=>'K',11=>'L',12=>'M',13=>'N',14=>'O',15=>'P',16=>'Q',17=>'R',18=>'S',19=>'T',20=>'U',21=>'V',22=>'W',23=>'X',24=>'Y',25=>'Z',26=>'a',27=>'b',28=>'c',29=>'d',30=>'e',31=>'f',32=>'g');
//--Обрабатываем нажатие кнопки "Зашифровать"--//
if(isset($_GET[beginencode]))
                {
//--Получаем данные из полей формы--//
$text=$_GET[text];
$code=$_GET[code];
print '<p style="wrap">Производим зашифровку текста "';
print $text;
print '" с ключом "';
print $code;
print '".</p>';
//--Заменяем кирилицу латиницей--//
$text=str_replace($rusl,$eng,$text);
$code=str_replace($rusl,$eng,$code);
$text=str_replace($rus2,$eng,$text);
$code=str_replace($rus2,$eng,$code);
//--Заменяем ненужные символы пустыми--//
$text=str_replace($symbl,$symb2,$text);
```

```
$code=str_replace($symbl,$symb2,$code);
//--Вводим переменную для растягивания ключа--//
$key=$code;
//--Делаем цикл для преобразования каждой буквы текста--//
for ($i=0; $i<strlen($text); $i++)
    {
        $result.=$dict2[(($dictl[$text[$i]]+$dictl[$key[$i]])%33)];
        $key.=$code;
    }
//--Преобразуем латиницу в кирилицу--//
    $result=str_replace($eng,$rusl,$result);
//--Выводим результат--//
    print '<p style="wrap">Зашифрованный текст: "';
    print $result;
    print '".</p>';
                }
//--Обрабатываем нажатие кнопки "Дешифровать"--//
if(isset($_GET[begindecode]))
                {
//--Получаем данные из полей формы--//
$text=$_GET[text];
$code=$_GET[code];
print '<p style="wrap">Производим расшифровку текста "';
print $text;
print '" с ключом "';
print $code;
print '".</p>';
//--Заменяем кирилицу латиницей--//
$text=str_replace($rusl,$eng,$text);
$code=str_replace($rusl,$eng,$code);
$text=str_replace($rus2,$eng,$text);
$code=str_replace($rus2,$eng,$code);
//--Заменяем ненужные символы пустыми--//
$text=str_replace($symbl,$symb2,$text);
$code=str_replace($symbl,$symb2,$code);
//--Вводим переменную для растягивания ключа--//
$key=$code;
//--Делаем цикл для преобразования каждой буквы текста--//
for ($i=0; $i<strlen($text); $i++)
    {
        $result.=$dict2[(($dictl[$text[$i]]+33-$dictl[$key[$i]])%33)];
        $key.=$code;
    }
//--Преобразуем латиницу в кирилицу--//
    $result=str_replace($eng,$rusl,$result);
//--Выводим результат--//
    print '<p style="wrap">Расшифрованный текст: "';
    print $result;
    print '".</p>';
                }
?>
```

Библиография

Кан, Давид, Взломщики кодов. М: Центрполиграф, 2000

Риксон, Фред Б. Коды, шифры, сигналы и тайная передача информации. М: АСТ, 2011

Сингх, Саймон, Книга шифров: тайная история шифров и их расшифровки. М: АСТ, 2007

Цыганов А.В., Криптография и криптоанализ, СПбГУ 2009

Ященко В.В., ред. Введение в криптографию. М: МЦНМО, 2000

Википедия: http://ru.wikipedia.org