Учёные записки Комсомольского-на-Амуре государственного технического университета № II-1(2) 2010

Котляров В.П., Воробьев А.А.
V.P. Kotlyarov , A.A. Vorobiev

О РЕШЕНИЯХ ПОВЫШЕНИЯ КРИПТОСТОЙКОСТИ ШИФРОВ С ПОМОЩЬЮ КОНТИНУАЛЬНОГО МНОЖЕСТВА

ON SOLUTIONS TO IMPROVE CRYPTOGRAPHIC ENDURANCE OF CIPHERS USING CONTINUUM SET

Котляров Валерий Петрович – кандидат технических наук, профессор кафедры «Информационные системы», декан факультета компьютерных технологий Комсомольского-на-Амуре государственного технического университета. Россия, 681013, г.Комсомольск-на-Амуре, ул. Ленина, д. 27, тел.: +7–(4217)–59–46–59, e–mail: fct@knastu.ru
Mr. Valeriy P.Kotlyarov – Ph.D., Professor of the Department of Information Systems, Dean of the Faculty of Computer Science, Komsomolsk-on-Amur State Technical University», 27, Lenina prospect, 681013 Komsomolsk-on-Amur, Khabarovsky region, Russian Federation, tel: +7–(4217)–59–46–59, e–mail: fct@knastu.ru

Воробьев Антон Александрович – студент пятого курса (специальность 230401 «Прикладная математика») Комсомольского-на-Амуре государственного технического университета. Россия, 681013, г. Комсомольск-на-Амуре, ул. Ленина, д. 27, тел.: 8-909-845-58-72, e–mail: zeromem@acm.org
Mr. Anton A.Vorobiev – last-year student, discipline No. 230401 «Applied Mathematics», Komsomolsk-on-Amur State Technical University», 27, Lenina prospect, 681013 Komsomolsk-on-Amur, Khabarovsky region, Russian Federation, cell.: 8-909-845-58-72, e–mail: zeromem@acm.org

Аннотация: В данной работе рассмотрена проблема, общая для симметричного шифрования, шифрования с открытым ключом, – атака методом «грубая сила». Предложено решение в виде использования континуального множества действительных чисел через взаимно-однозначное отображение дискретных натуральных величин на сферу Римана с возможностью повышения криптостойкости при помощи варьирования запятой.

Summary: The paper considers a problem that is common for symmetric encryption and public key encryption – the so-called "brute force" attack. Proposed is a solution to it in the form of using a continuum set of real numbers via one–to–one mapping of discrete natural values onto the Riemann sphere with a possibility of increasing the cipher endurance by binary point variations.

Ключевые слова: криптография, сфера Римана, варьирование запятой, «грубая сила», защита информации, континуальные множества.

Keywords: cryptography, Riemann sphere, comma variations, brute force, information security, continuum sets.

УДК 003.26, 004.056.5

Симметричное шифрование, шифрование с открытым ключом, предложенные много десятилетий назад [5], имеют кроме преимуществ ряд недостатков. Одним из недостатков

Поступила в редакцию 03.05.2010 г.

является проблема «bruteforce» (англ. грубая сила), то есть атака методом «грубая сила». В качестве преимуществ можно указать простоту основной идеи указанных алгоритмов.

В симметричных алгоритмах атака методом «грубая сила» заключается в переборе всевозможных ключей. В алгоритмах с открытым ключом часто используются в качестве функции с секретом сложные математические задачи, требующие, без знания секрета [4, 5], больших ресурсов для вычислений. Примером таких задач может служить задача о разложении достаточно больших чисел на множители (факторизация) или дискретное логарифмирование.

Известно [4], что указанные выше задачи являются сложными для решения, хотя данное утверждение и не совсем верно, так как не доказано, что они действительно являются сложными, и отсутствие быстрого алгоритма решения не говорит о несуществовании такого.

Показать "тенденцию" к нахождению все более быстрых алгоритмов, а также невозможность предсказания временного периода, в течение которого подобные задачи будут решены, можно на примере задачи разложения на множители.

В 1979 г. Рон Ривест [4] высказал предположение, что еще 40 квадриллионов лет понадобится для разложения на множители числа порядка 10125. А как произошло на самом деле: уже в 1994 г. на множители разложили число порядка 10129, благодаря параллельным вычислениям 1800 компьютеров в течение 8 месяцев.

В то же время с развитием вычислительных мощностей алгоритмы также развиваются: алгоритм квадратной сетки, сетка общего поля чисел, сетка специальных чисел [4]. В 1989 г. никто не говорил бы о практическом применении сетки общего поля чисел, в 1993 сказали бы, что реализация практически возможна, а сегодня они уже есть и работают быстрее алгоритма квадратной сетки.

Известны (см. рис. 1) результаты разложения на множители за период с 1983 по 1994 гг., вследствие которых нелинейность прогресса [4] в данной области очевидна. При этом даже Аржан Лестра – ведущий в мире «раскладыватель» на множители не берется делать предсказания, следовательно, никто не застрахован от компрометации атакой «грубой силой».

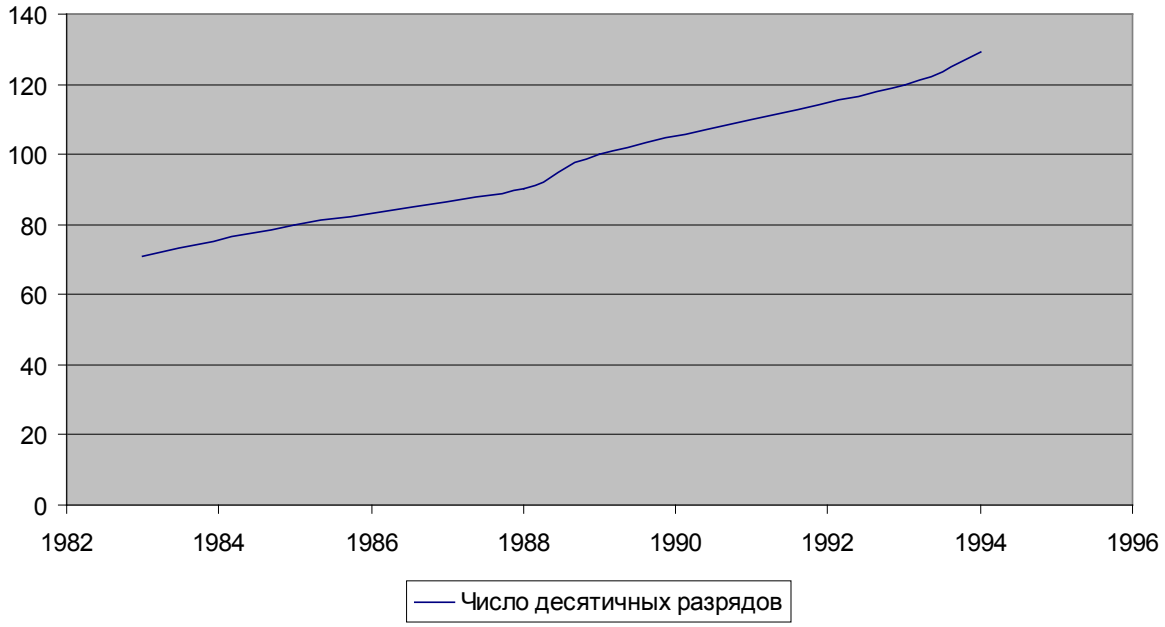

Рис. 1. Диаграмма зависимости числа десятичных разрядов от года

Из такого опасного положения выходят, например, увеличением длины ключа. Но, как и на взлом ключа требуется время, пропорциональное длине, так и на шифрование сообщения необходимо время, также зависящее от размера ключа.

Исходя из текущего положения, логично задать вопрос: можно ли предоставить такой криптографический алгоритм, которой бы совершенно не поддавался данному виду атаки?

Ответ на этот вопрос неоднозначный. Но главная идея состоит в том, чтобы дискретное количество элементов представить элементами континуального множества. Тогда для перебора необходимо будем перебрать весь континуум, что невозможно.

Решение о повышении криптостойкости шифров

Одним из вариантов взаимно-однозначного преобразования дискретных элементов натуральных чисел в совокупность действительных чисел на практике может служить отображение на сферу Римана.

Пусть дано некоторое множество дискретных данных $I = \{a_i\}, i = 1,2,\ldots,n.$. Предполагаем, что каждый элемент a_i является 8-битовым беззнаковым целым числом в диапазоне $[0,255]$.

Сопоставим ему некоторое равномощное множество $K = \{b_i\}$, т.е. другими словами $|I| = |K|$. Из данного сопоставления получим некоторую совокупность упорядоченных пар $C = \{(a_i, b_i)\}, i = 1,2,\ldots,n.$ Назовем шумовой функцией некоторую функцию $n(i)$ генерации элементов $b_i = n(i)$.

Тогда пары (a_i, b_i) можно считать некоторыми точками комплексных чисел z_i на комплексной плоскости Ψ.

Из теории функций комплексной переменной [3] известно, что эти пары могут быть биективно отражены на сферу Римана некоторого радиуса R с выколотой вершиной, так как предполагаем невозможность постановки точки в бесконечности.

В результате такого отображения совокупность упорядоченных пар перейдет в совокупность троек чисел

$$S = \{x(a_i, b_i), y(a_i, b_i), z(a_i, b_i)\} = \{x_i, y_i, z_i\}. \quad (1)$$

Покажем возможность данного отображения.

Пусть дана декартова система координат, причем оси x и y лежат в заданной комплексной плоскости Ψ, и на плоскости имеем заданную точку $a(x_i, y_i)$. Также имеем сферу Римана радиусом R с выколотой верхней вершиной P, которая касается Ψ в начале координат, причем точка P лежит на оси z. Проведем некоторую прямую через данную выколотую вершину сферы $b(0,0,2R)$ и точку на плоскости. Имеем пересечение прямой со сферой в двух местах, – в самой выколотой точке и в некоторой иной точке $\alpha(x, y, z)$ сферы. Поиск данной точки сводится из аналитической геометрии к решению системы:

$$\begin{cases} x^2 + y^2 + (z - R)^2 = R^2, \\ \dfrac{x - x_i}{0 - x_i} = \dfrac{y - y_i}{0 - y_i} = \dfrac{z - 0}{2R - 0}. \end{cases} \quad (2)$$

На самом деле здесь присутствуют четыре уравнения, но нам нужны будут только три из них, причем решение $\begin{cases} x = 0 \\ y = 0 \\ z = 2R \end{cases}$ нас не удовлетворяет по построению.

Второе решение имеет вид:

$$x = \frac{4x_i R^2}{4R^2 + y_i^2 + x_i^2}, y = \frac{4y_i R^2}{4R^2 + y_i^2 + x_i^2}, z = 2R - \frac{8R^3}{4R^2 + y_i^2 + x_i^2}. \quad (3)$$

Покажем биективность данного отображения.

Действительно, по указанной выше схеме мы находили общую точку сферы и прямой. Последняя задана с помощью двух точек C и P – точки плоскости и точки выколотой вершины сферы соответственно (см. рис. 2). Отсюда находим точку Q – точку пересечения прямой со сферой. Обратно, даны две точки P и Q на сфере. Необходимо найти точку на плоскости. Очевидно, что при данных двух точках система (2) и равенства (3) дадут нам ту же самую прямую, которая пересечет комплексную плоскость Ψ в требуемой точке C. Таким образом, комплексная плоскость оказывается вложенной в сферу.

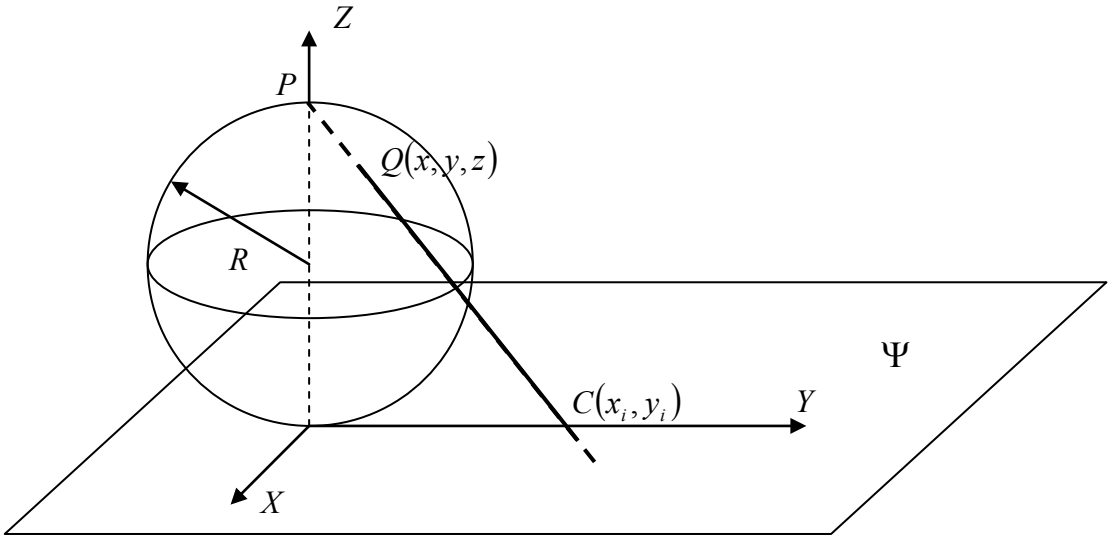

Рис. 2. Отображение комплексной величины C на сферу Римана

При вычислении значений (3) вероятнее всего мы получим числа с плавающей точкой, и, соответственно, потери точности неизбежны. Следовательно, задача состоит в том, чтобы найти и исследовать параметры обратного преобразования для однозначного обращения данных в первоначальное состояние, а также узнать и подобрать такие из них, чтобы выполнялось условие невозможности использования атаки методом «грубая сила».

Основная гипотеза состоит в том, что варьируя бесконечно малые величины заданного порядка $\varepsilon > 0$, действующие по неустойчивой схеме [1] (т.е. небольшое изменение бесконечно малого влечет сильное искажение данных), невозможно будет использовать перебор всего отрезка действительных чисел, так как мощность любого бесконечно малого отрезка на множестве действительных чисел есть континуум.

Кроме того, добавление четвертого параметра к каждой тройке координат точек $Q_i, i = 1,2,\ldots,n.$, а для определенности предположим, что это будет масса точки, можно определить некоторую механическую систему материальных точек, что при некоторых допущениях дает нам аппарат динамики твердого тела, базирующийся на законах Ньютона.

Произведем первичный анализ исходя из полученных формул биективного отображения на сферу.

Каждая точка Q_i в пространстве образована соотношениями (3), причем в общем случае компоненты Q_i принадлежат континуальному множеству. Чтобы получить и произвести оценки погрешностей, рассмотрим различные случаи представления этих отношений. Для

упрощения положим, что мы рассматриваем некоторое соотношение $\frac{x}{y}$, где $x > 0, y > 0$, так как полученные выводы можно легко расширить и для формул (3).

Логично, что при делении одного числа на другое мы можем получить ответ лишь с некоторой долей точности. Из теории погрешностей известно [1], что, зная относительную погрешность числа, можно восстановить некоторое количество значащих цифр. Очевидно, что для однозначного восстановления информации нам необходимо определить, сколько в том или ином случае взять цифр, чтобы обратное преобразование дало ожидаемый результат.

Для соотношения $\frac{x}{y}$ основные варианты использования можно представить в виде

$$\frac{x}{y} = z_{\approx} + \sigma_z z_{\approx}, \tag{4}$$

где $z_{\approx}$ – приближенный результат дроби; σ_z – относительная погрешность результата дроби, $x \in \{N, Q, R\}, y \in \{N, Q, R\}, x > 0, y > 0$

Рассмотрим самый простой первый случай, когда числитель и знаменатель являются числами натуральными, тогда в формуле (3) очевидно, что $x_i \in N, y_i \in N, R \in N$. Так как числа натуральные, значит, операция выполняется на числах без погрешностей. Но результат деления может оказаться как конечной десятичной дробью, так и бесконечной периодической. Отсюда встает вопрос: с какой точностью передать значение (4) удаленной стороне, чтобы имелась возможность однозначно обратить данные в исходное состояние и повысить криптостойкость?

Гипотетически, точность, с которой нужно передавать число, можно определить по количеству значимых цифр. Но для данных рассуждений нам потребуется знать, сколько будет цифр в результате операции, если известно начальное количество знаков в каждом из операндов. Определить для операции сложения количество знаков не составляет труда, поэтому рассмотрим операцию умножения. Для этого сформулируем и докажем теорему.

Теорема 1: Пусть x и y – целые, причем x состоит из $n > 0$ цифр, а y состоит из $m > 0$ цифр. Тогда $z = xy$ не превышает $m + n$ цифр. Числа x и y представлены в десятичной системе.

Доказательство:

Для определенности положим, что $n \le m$.

В десятичной системе записи возможные цифры в числе представляются в виде от 0 до 9. То есть, если мы хотим из k цифр составить целое число, то минимальное такое число будет $1\underbrace{000\ldots0}_{k-1\text{ раз}}$, а максимальное, – $\underbrace{999\ldots9}_{k\text{ раз}}$.

Докажем теорему по методу индукции.

1. Пусть $m = 2$, тогда n может быть либо 1, либо 2. Имеем в максимальном случае: $99 \cdot 9 = 891\,(3\text{ знака})$ и $99 \cdot 99 = 9801\,(4\text{ знака})$. Условие выполняется.

2. Предполагаем, что $m = k, k \in N$, тогда $n \in [1, k]$ и условие также выполняется.

3. Покажем, что условие выполняется и при $n = k + 1$.

Пусть $x = \underbrace{999\ldots9}_{k\text{ раз}}$ и $y = \underbrace{999\ldots9}_{i\text{ раз}}$, где $i = \overline{1,k}$. Данные числа можно представить в виде следующих сумм:

$$x = \underbrace{99\ldots9}_{k} + 9 \cdot 10^k,$$

$y = \underbrace{99\ldots9}_{i-1} + 9 \cdot 10^{i-1}$.

Рассмотрим их произведение.

$xy = \underbrace{99\ldots9}_{k} \cdot \underbrace{99\ldots9}_{i-1} + \underbrace{99\ldots9}_{k} \cdot 9 \cdot 10^{i-1} + \underbrace{99\ldots9}_{i-1} \cdot 9 \cdot 10^{k} + 9 \cdot 9 \cdot 10^{k+i-1}$.

По пунктам 1 и 2 первые три произведения можно свернуть. Тогда имеем:

$xy = \underbrace{99\ldots9}_{k+i-1} + \underbrace{99\ldots9}_{k+1}\underbrace{00\ldots0}_{i-1} + \underbrace{99\ldots9}_{i}\underbrace{00\ldots0}_{k} + 81\underbrace{00\ldots0}_{k+i-1} =$

$\left(\underbrace{99\ldots9}_{k+i-1} + 81\underbrace{00\ldots0}_{k+i-1}\right) + \left(\underbrace{99\ldots9}_{k+1}\underbrace{00\ldots0}_{i-1} + \underbrace{99\ldots9}_{i}\underbrace{00\ldots0}_{k}\right)$

Первая скобка дает число $81\underbrace{99\ldots9}_{k+i-1}$ с $k+i+1$ знаком, вторая скобка аналогично дает число с $k+i+1$ знаком. Отсюда при сложении получаем число максимум с $k+i+2$ знаками.

Так как произведение коммутативно, то теорема будет справедливой и для $n > m$. Таким образом, по методу математической индукции теорема доказана.

Покажем максимальное количество цифр, достаточных для однозначного восстановления информации.

Выберем число $\frac{1}{3}$ с некоторой точностью (обозначим его как $\frac{1}{3_{\approx}}$) и получим из данного числа число $\frac{1}{9}$ с некоторой точностью, далее умножим приближенное значение на 9, тем самым показав, какие условия способствуют его округлению к точному результату 1.

Пусть $\frac{1}{3_{\approx}} = 0.3333$ с погрешностью $\sigma_{\frac{1}{3_{\approx}}} = 0.0001$. Тогда

$\frac{1}{3_{\approx}}\frac{1}{3_{\approx}} = \frac{1}{9_{\approx}} = 0{,}11108889$ с погрешностью $\sigma_{\frac{1}{9_{\approx}}} = 0.0002$.

Но $9 \cdot \frac{1}{9} \approx \left(\frac{1}{3_{\approx}}\frac{1}{3_{\approx}} + \sigma_{\frac{1}{9_{\approx}}}\frac{1}{3_{\approx}}\frac{1}{3_{\approx}}\right) \cdot 9 = \overbrace{0.111111107778}^{k} \cdot 9 = 0.99999970002 \approx 1$.

Из полученного результата видно, что для восстановления исходных данных достаточно взять значащие цифры и операцией округления привести значение к точному результату.

Определим достаточное количество цифр в потоке передачи шифротекста для корректного восстановления данных. В приведенном примере мы могли бы передавать в поток данных $\frac{1}{3_{\approx}}\frac{1}{3_{\approx}}$, но тогда для применения теории погрешностей нам необходимо передавать и относительную погрешность, что неудобно. Потому логично вести передачу результата $\left(\frac{1}{3_{\approx}}\frac{1}{3_{\approx}} + \sigma_{\frac{1}{9_{\approx}}}\frac{1}{3_{\approx}}\frac{1}{3_{\approx}}\right)$. Теория погрешностей [1] утверждает необходимость выбрать минимум столько цифр, сколько имеется значащих цифр. Но, исходя из различных вариаций умножения чисел с определенной точностью, по аналогии с примером выше, гипотетически нет смысла брать более, чем $n+m+1$. Действительно, исходя из теоремы 1, можно легко показать ее справедливость и для чисел вида $\frac{1}{x}, x \in Z$. Произведение $\frac{1}{3_{\approx}}\frac{1}{3_{\approx}}$ не превышает $n+m$

цифр, а слагаемое $\sigma_{\frac{1}{9_{\approx}}} \frac{1}{3_{\approx}} \frac{1}{3_{\approx}}$ дает максимум плюс 1 цифру. Тем самым, если мы будем передавать $\left(\frac{1}{3_{\approx}} \frac{1}{3_{\approx}} + \sigma_{\frac{1}{9_{\approx}}} \frac{1}{3_{\approx}} \frac{1}{3_{\approx}} \right)$ с более чем $n+m+1$ цифрой, это не окажет никакого влияния на значащие цифры конечного результата, а значит, и не играет важной роли в операции восстановления данных.

Покажем, что для повышения криптостойкости можно использовать следующую простую схему. Представим, что данные в потоке передаются числами с плавающей точкой. Причем за 1 такт мы получаем лишь 1 цифру. В каком месте разделение разряда в числе – в потоке данных данная информация отсутствует. Отсюда получается, что для обратных преобразований, требующих достаточной точности числа, неизвестно, в каком месте числа поставить запятую (это особенно важно, когда небольшая погрешность в исходном значении дает сильное отклонение результата). Эту информацию можно представлять дополнительным ключом (назовем его степенным ключом), который и определяет, в каком месте необходимо поставить знак (варьирует запятую). Без необходимых данных о положении запятой вычислительная сложность самого алгоритма перебора возрастет в число различных положений запятой. В случае, когда информация о положении запятой известна, сложность остается прежней. Действительно, пусть вычислительная сложность обратимости некоторого алгоритма шифрования равна q. Дополняя схему отображением на сферу Римана, а следовательно и переходом к числам с плавающей запятой, данная схема позволяет повысить сложность решения задачи обратимости криптоалгоритма в k раз, где k – возможные различные положения запятой. То есть по основной теореме умножения комбинаторики мы имеем максимально возможную сложность алгоритма kq, что и требовалось показать.

Заключение

Из сказанного можно сделать следующие выводы:

1. Переход от дискретных величин не более чем счетных множеств с помощью преобразования со сферой к величинам континуальных множеств сводит на нет возможность атаки методом «грубой силы».
2. Полученные после преобразований числа с плавающей точкой как элементы континуального множества предоставляют возможность применять, например, аппарат динамики твердого тела, базирующийся на законах Ньютона.
3. Введение варьирования запятой в совокупности чисел с плавающей точкой из континуального множества позволяет повысить вычислительную сложность атаки методом «грубой силы» до k раз, где k – возможные различные положения запятой.

ЛИТЕРАТУРА

1. Демидович, Б.П. Численные методы анализа. Приближение функций, дифференциальные и интегральные уравнения. – 3-е изд. / Б.П. Демидович, И.А. Марон, Э.З. Шувалова. – М.: Наука, 1967. – 368 с.
2. Новиков, Ф.А. Дискретная математика для программистов. – 2-е изд. / Ф. А. Новиков. – СПб.: Изд-во Питер, 2006. – 364 с.
3. Свешников, А.Г. Теория функций комплексной переменной. – 5-е изд. / А.Г. Свешников, А.Н. Тихонов. – М.: Физматлит, 2004. – 336 с.
4. Шнайер, Б. Прикладная криптография: Протоколы, алгоритмы, исходные тексты на языке Си / Б. Шнайер. – М.: Изд-во Триумф, 2002. – 816 с.
5. Ященко, В.В. Введение в криптографию. / В.В. Ященко. – М.: МЦНМО, "ЧеРо", 1998. – 271 с.