В представленной работе определенный интеграл $\int e^{-\frac{x^2}{2}} dx$ – вычислен тремя способами:

1. Разложением подынтегральной функции в ряд Макларена.
2. Приближенным методом Симпсона.
3. С помощью таблицы значений функции Лапласа.

1. Значение интеграла вычислялось с точностью до 0,0001

$$e^t = 1 + \frac{t}{1!} + \frac{t^2}{2!} + \frac{t^3}{3!} + \ldots = \sum_{n=0}^{\infty} \frac{t^n}{n!};$$

$$e^{-\frac{x^2}{2}} = 1 + \frac{\frac{1}{2}x^2}{1!} + \frac{\left(\frac{1}{2}x^2\right)^2}{2!} + \frac{\left(\frac{1}{2}x^2\right)^3}{3!} + \frac{\left(\frac{1}{2}x^2\right)^4}{4!} \ldots = \sum_{n=0}^{\infty} \frac{(-1)^n}{2^n n!} x^{2n}.$$

Вычислим интеграл

$$\int_0^{0,2} e^{-\frac{x^2}{2}} dx = \left(x - \frac{1}{2 \cdot 1!} \cdot \frac{x^3}{3} + \frac{1}{4 \cdot 2!} \cdot \frac{x^5}{5} - \frac{1}{8 \cdot 3!} \cdot \frac{x^7}{7} + \ldots \right) \Bigg|_0^{0,2} = 0,2 - 0,00133 + 0,000008 - \ldots.$$

Для знакочередующегося числового ряда остаток оценивается с…

$$\left.\begin{array}{l} |R_n| \le U_n + 1 \\ U_3 \le 0,0001 \end{array}\right\}$$

поэтому

$$\int_0^{0,2} e^{-\frac{x^2}{2}} dx \approx 0,2 - 0,00133 \approx 0,19867.$$

2. $\int_0^{0,2} e^{-\frac{x^2}{2}} dx.$

Разделим промежуток [0; 0,2] на 5 частей и вычислим

$$\int_{x_1}^{x_2} e^{-\frac{x^2}{2}} dx.$$

По формуле

$$\int_{x_1}^{x_2} f(x)dx \approx \frac{x_2 - x_1}{6} \left(f(x_1) + 4f\left(\frac{x_1 + x_2}{2}\right) + f(x_2) \right).$$

Применим формулу Симпсона на каждом шаге:

1) $\int_0^{0,04} e^{-\frac{x^2}{2}} dx = 0,03994;$

2) $\int_{0,04}^{0,08} e^{-\frac{x^2}{2}} dx = 0,03988;$

3) $\int_{0,08}^{0,12} e^{-\frac{x^2}{2}} dx = 0,03975;$

4) $\int_{0,12}^{0,16} e^{-\frac{x^2}{2}} dx = 0,039567;$

5) $\int_{0,16}^{0,2} e^{-\frac{x^2}{2}} dx = 0,039315.$

Сложив пошаговые результаты, получим окончательное значение интеграла:

$$0,03994 + 0,03988 + 0,03975 + 0,039567 + 0,039315 = 0,19845$$

3. С помощью функции Лапласа

$$\Phi(x) = \frac{1}{\sqrt{2\pi}} \int_0^{0,2} e^{-\frac{t^2}{2}} dt \Rightarrow \int_0^{0,2} e^{-\frac{x^2}{2}} dx = \Phi(0,2) = \sqrt{2\pi} \cdot 0,0793 = 0,198776.$$

Сравним все полученные результаты

1) ряд Макларена	0,19867;
2) формула Симпсона	0,19845;
3) функция Лапласа	0,198776.

Список литературы

1. Математическая статистика: учебное пособие / Д.К. Агишева, С.А. Зотова, Т.А. Матвеева, В.Б.Светличная // Успехи современного естествознания. – 2010. – №9. – С. 122-123.

ПРИКЛАДНОЕ ЗНАЧЕНИЕ СРАВНИМОСТИ ЧИСЕЛ В КРИПТОГРАФИИ

Посевкин Р.В., Светличная В.Б.

Волжский политехнический институт, филиал Волгоградский государственного технического университета, Волжский, www.volpi.ru, e-mail: rus_posevkin@mail.ru

Сравнения нашли широкое применение в криптографии и шифровании. Один из наглядных примеров – алгоритмы ассиметричного шифрования. Основная идея асимметричного шифрования заключается в существовании сразу двух ключей для обмена информацией – открытого, известного любому желающему, и закрытого, который известен лишь получателю информации. Очевидно, что открытый и закрытый ключи генерируются одновременно и между ними существует определенная математическая связь. Основная задача проектировщика асимметричного алгоритма заключается в том, чтобы по известному открытому ключу было бы невозможно (очень трудоемко) получить секретный ключ шифрования. Для этого в основу асимметричных алгоритмов закладываются вычислительно трудные задачи факторизации, дискретного логарифмирования, проецирования точек на эллиптической кривой и т.д. Объединяет все эти задачи то, что они используют операцию получения остатка от целочисленного деления (сравнения). Говорят, что два целых числа a и b являются сравнимыми по модулю n, если (a mod n) = (b mod n). Это записывается в виде:

$$a \equiv b \bmod n.$$

В качестве примера алгоритмов симметричного шифрования можно привести первую систему с открытым ключом – метод экспоненциального ключевого обмена Диффи – Хеллмана. Метод предназначен для передачи секретного ключа симметричного шифрования. В обмене задействованы два участника А и Б. Сначала они выбирают большие простые числа n и $g < n$ (эти числа секретными не являются). Затем участник А выбирает большое целое число x, вычисляет $X = g^x \bmod n$ и передает X участнику Б. Б в свою очередь выбирает большое целое число y,

вычисляет $Y = g^y \bmod n$ *и* передает *Y* участнику А. Б вычисляет $K' = X^y \bmod n$, *A* вычисляет $K'' = Y^x \bmod n$. Легко заметить, что $K' = K'' = g^{xy} \bmod n$, *и* это значение оба участника могут использовать в качестве ключа симметричного шифрования. Злоумышленник может узнать такие параметры алгоритма, как *n, g, X, Y,* но вычислить по ним значения *x* или *y* – задача, требующая очень больших вычислительных мощностей и времени.

Примером действительно асимметричного алгоритма шифрования, основанного на проблеме дискретного логарифма, является алгоритм Эль-Гемаля. Последовательность действий при генерации ключей, шифровании и дешифрации представлена на рис. 1.

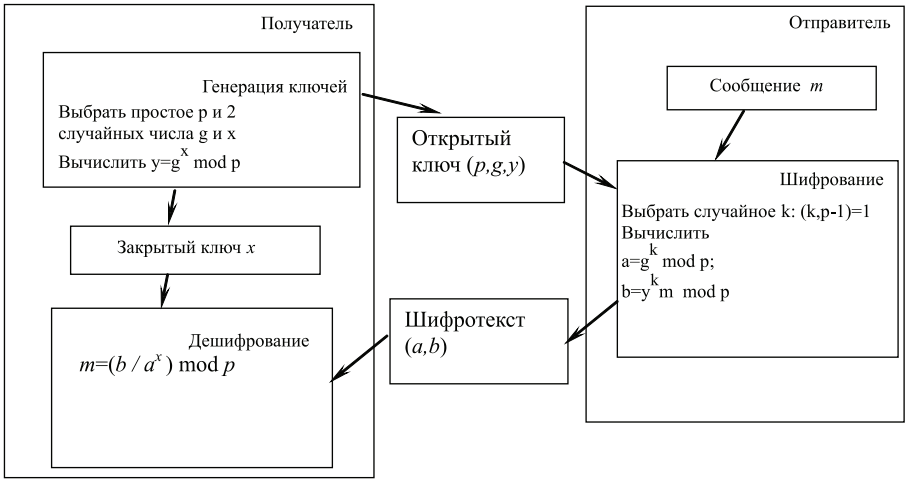

Рис. 1. Схема шифрования алгоритма Эль-Гемаля

Так как $a^x \equiv g^{kx} \bmod p$, то имеем:

$$\frac{b}{a^x} \equiv \frac{y^k m}{a^x} \equiv \frac{g^{xk} m}{g^{kx}} = m \bmod p. \qquad (1)$$

Самым первым, действительно асимметричным алгоритмом стал алгоритм RSA. В основу криптостойкости RSA положена задача факторизации (разложения на множители) больших (более 200 двоичных разрядов) целых чисел.

Процедуры генерации ключей, шифрования и дешифрования для этого алгоритма представлены на рис. 2.

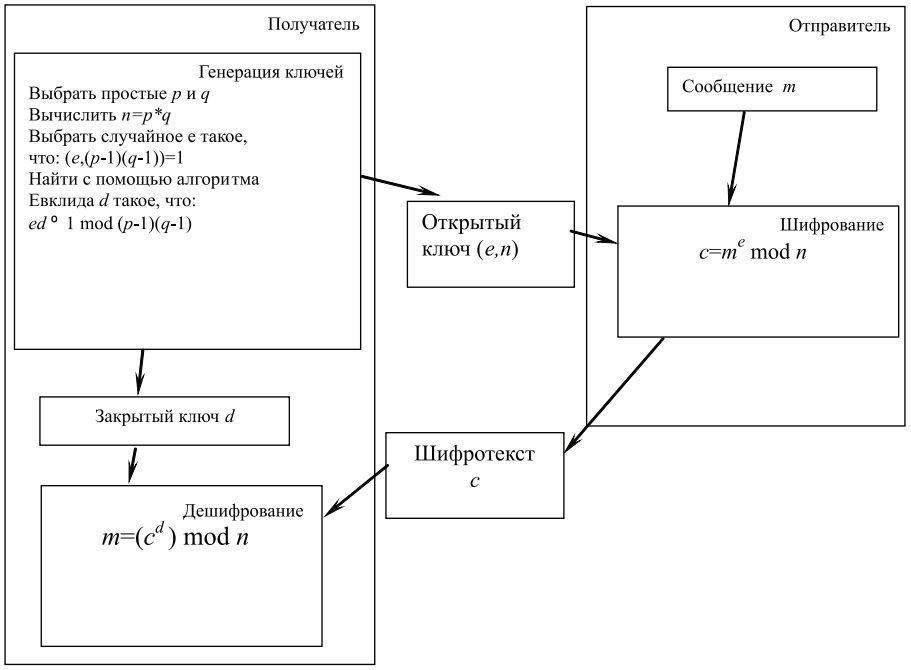

Рис. 2. Схема шифрования алгоритма RSA

На этапе генерации ключей формируется пара ключей: закрытый *d* и открытый *e*. Шифрование данных должно начинаться с его разбиения на блоки *m* размером $k = [\log_2 (n)]$ бит каждое, чтобы блок *m* можно было рассматривать как целое число в диапазоне [0.. *n* – 1]. Обратимость операции шифрования и дешифрования RSA требует доказательства. Из теоремы Эйлера известно, что для двух целых чисел *n и x,* таких, что $(n,x) = 1$, выполняется:

$$x^{\varphi(n)} \equiv 1 \bmod n, \qquad (2)$$

где $\varphi(n)$ – функция Эйлера, значение которой равно количеству чисел меньших *n и* взаимно простых

с ним. Для $n = p \cdot q$ из алгоритма RSA, где p и q – простые числа, можно записать $\varphi(n) = (p-1)(q-1)$.

Тогда (1) можно переписать в виде:

$$x^{(p-1)(q-1)} \equiv 1 \bmod n. \quad (3)$$

Возведем обе части (3) в степень $-y$:

$$x^{(-y)(p-1)(q-1)} \equiv 1^{(-y)} \bmod n \equiv 1 \bmod n. \quad (4)$$

Умножим обе части (4) на x:

$$x^{(-y)(p-1)(q-1)+1} \bmod n = x. \quad (5)$$

Но при генерации ключей мы получили e и d такие, что $ed \equiv 1 \bmod (p-1)(q-1)$, а это означает, что в (5) можно заменить $1 - y(p-1)(q-1)$ на ed:

$$x^{ed} \bmod n = x. \quad (6)$$

Тогда, если мы возведем шифротекста $c = m^e \bmod n$ в степень d по модулю n, как мы это и делаем при дешифровании, то получим:

$$(c^d) \bmod n = (m^e \bmod n)^d \bmod n = m^{ed} \bmod n = m. \quad (7)$$

Очевидно, что основная задача криптоаналитика при взломе этого шифра – узнать закрытый ключ d. Для этого он должен выполнить те же действия, что и получатель при генерации ключа – решить в целых числах уравнение $ed + y(p-1)(q-1) = 1$ относительно d и y. Однако, если получателю известны входящие в уравнение параметры p и q, то криптоаналитик знает только число n – произведение p и q. Следовательно, ему необходимо произвести факторизацию числа n, то есть разложить его на множители. Для решения задачи факторизации к настоящему времени разработано множество алгоритмов: квадратичного решета, обобщенного числового решета, метод эллиптических кривых. Но для чисел большой размерности это очень трудоемкая задача.

Список литературы

1. Методы и средства защиты компьютерной информации: учебное пособие / Д.Н. Лясин, С.Г. Саньков – РПК «Политехник», 2005.

РЕШЕНИЕ ИНТЕГРАЛЬНЫХ УРАВНЕНИЙ ОПЕРАЦИОННЫМ МЕТОДОМ

Трощенко О.Н., Чегурихина Д.Ю., Матвеева Т.А.

Волжский политехнический институт, филиал ФГБОУ ВПО «Волгоградский государственный технический университет», Волжский, www.volpi.ru, e-mail: dianachegurihin@mail.ru

Для одного и тоже дифференциального уравнения метод решения может существенно зависеть от вида граничных условий. Этого можно избежать, если исходную задачу свести к интегральному уравнению, которое будет эквивалентно дифференциальному уравнению вместе с соответствующими краевыми условиями. Нередко самые разнообразные краевые задачи сводятся к одному и тому же интегральному уравнению.

Мы остановимся на рассмотрении одного типа интегральных уравнений – уравнений Вольтерра первого, второго рода:

$$\int_0^t k(t-\tau)x(\tau)\,d\tau = f(t)$$

и

$$x(t) = f(t) + \int_0^t k(t-\tau)\,x(\tau)\,d\tau,$$

где $x(\tau)$ – искомая функция.

Одним из методов решения данных интегральных уравнений – это применение преобразования Лапласа:

$$F(p) = \int_0^{+\infty} e^{-pt} \cdot f(t)\,dt.$$

Сущность операционного исчисления состоит в том, что изучается не сама функция $f(t)$ (оригинал), а ее видоизменение $F(p)$ (изображение).

Рассмотрим применение данного метода к решению следующего интегрального уравнения:

$$x(t) = 1 + \frac{1}{6} \cdot \int_0^t (t-\tau)^3 \cdot x(\tau)\,d\tau.$$

Пусть искомая функция является оригиналом $x(t)$, которая имеет изображение $X(p)$. Тогда данное уравнение можно записать в виде

$$x(t) = 1 + \frac{1}{6} \cdot (t-\tau)^3 \cdot x(t).$$

где $x(t) \cdot k(t) = \int_0^t x(\tau) \cdot k(t-\tau)\,d\tau.$ – свертка оригиналов.

Применив к уравнению преобразование Лапласа, учитывая теорему о свертки

$$x(t) \cdot k(t) \leftrightarrow X(p) \cdot K(p)$$

получаем

$$X(p) = \frac{1}{p} + \frac{6}{p^4} \cdot X(p)$$

или

$$X(p)\left(1 - \frac{1}{p^4}\right) = \frac{1}{p}.$$

Из полученного уравнения находим изображение искомой функции (используем метод неопределенных коэффициентов для разложения дроби на сумму простейших дробей):

$$X(p) = \frac{p^3}{p^4 - 1} = \frac{p^3}{(p-1)(p+1)(p^2+1)} = \frac{1}{4}\left(\frac{1}{p-1} + \frac{1}{p+1} + \frac{2p}{p^2+1}\right).$$

Применяя таблицу и свойство линейности преобразования Лапласа, для изображения $X(p)$ находим выражение искомой функции

$$x(t) = \frac{1}{4}\left(e^t + e^{-t} + 2 \cdot ch(t)\right) = \frac{1}{2}\left(\cos(t) + 2 \cdot ch(t)\right).$$

Операционное исчисление – один из методов математического анализа, позволяющий в ряде случаев посредством простых правил решать сложные математические задачи. Поэтому операционные методы используются там, где классические методы не эффективны. Они применяются в физике, электротехнике, радиотехнике, механике, теории автоматического регулирования и т.д.

Список литературы

1. Лунгу К.Н., Норин В.П., Письменный Д.Т., Шевченко Ю.А. Сборник задач по высшей математике // под ред. С.Н. Федина – М.: Айрис-пресс, 2004. — 592 с.

2. Матвеева Т.А. Некоторые методы обращения преобразования Лапласа и их приложения: автореф. дис … канд. физ-мат. наук. – СПб., 2003. – 16 с.

3. Матвеева Т.А. Специальные главы математики: операционное исчисление: учебное пособие / Т.А. Матвеева, В.Б. Светличная, Д.К. Агишева, С.А. Зотова. – Волгоград, 2010. – 56 с.