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.