при начальных условиях

$$x(0)=0,\quad y(0)=\tau,\quad u(0)=-\tau\ \ (\tau\in\mathbf{R}).$$

Параметрическое решение последней системы имеет вид

$$x=t,\quad y=-t+\tau,\quad u=\frac{\tau-1}{2}e^{2t}+t+\frac{1-3\tau}{2}.$$

Отсюда найдем явное решение исходной задачи Коши

$$u(x;y)=\frac{x+y-1}{2}e^{2x}+\frac{1-x-3y}{2}.$$

Ответ: $u(x;y)=\dfrac{x+y-1}{2}e^{2x}+\dfrac{1-x-3y}{2}.$

Список литературы

1. Тихонов, А. Н. Уравнения математической физики : учеб. пособие / А. Н. Тихонов, А. А. Самарский. – М. : Наука, 1977. – 736 с.
2. Романко, В. К. Курс дифференциальных уравнений и вариационного исчисления / В. К. Романко. – М.: Лаборатория Базовых Знаний, 2000. – 344 с.
3. Берс, Л. Уравнения с частными производными / Л. Берс, Ф. Джон, М. Шехтер. – М. : Мир, 1966. – 352 с.
4. Сборник задач по уравнениям математической физики / В. С. Владимиро [и др.]. – М. : ФИЗМАТЛИТ, 2016. – 520 с.

УДК 004.056.55

ПРИМЕР ПОСТРОЕНИЯ АЛГОРИТМА ШИФРОВАНИЯ

М.А. Протько

Белорусский государственный университет информатики и радиоэлектроники, г. Минск.

Научный руководитель: О.Ф. Борисенко, канд. физ.-мат. наук, доцент

Введение. Что составляет любой базовый криптографический алгоритм? По сути, это два соответствия: базовый/шифрованный текст. Связь между первым и вторым происходит по некой функции F с приблизительно следующими свойствами:

$F(B)=A$ – легко рассчитываемая функция.

$B=F^{-1}(A)$ – не вычисляемая функция доступными средствами.

То есть задача построения алгоритма шифрования будет соответствовать следующей формулировке:

Пусть К – пространство ключей, e и d – ключи шифрования и расшифрования соответственно. E_e – односторонняя функция шифрования для произвольного ключа e ∈ K, такая, что $E_e(t)=c$, c ∈ C, C - пространство шифротекстов, t ∈ T, T – пространство сообщений. D_d – функция расшифрования, такая, что $D_d(c) = t$. Каждая пара (E,D) имеет свойство: зная E_e невозможно найти $E_e(t)=c$.

Учитывая необходимость в вычислительной сложности таковых функций, простой перебор всех возможных значений и применение принципа индукции могут не дать доказательства их верности. Для более качественной оценки полученных алгоритмов необходимо четко обозначить условия, из которых они вытекают, а также те параметры, которым они обязаны удовлетворять.

Условия, удовлетворяемые шифром

1) $T = D(E(T))$ – где T – пространство сообщений. D и E – функции расшифрования и шифрования соответственно.

Иначе: применив функции D или E, мы получим однозначный свзяный текст без потери информации в обоих случаях. Мы можем выполнять эту операцию сколь угодно долго.

2) $H(E) \geq H(T)$ – где $H(E)$ и $H(T)$ – неопределенности зашифрованного и изначального сообщения.

Иными словами, вероятность предсказания следующего символа перехваченного сообщения (нахождения закономерности) значительно уменьшается при шифровании.

3) Удовлетворяет принципу Керкго́ффса

То есть, даже зная процедуру (функцию F), невозможно получить изначальный текст. Необходим ключ, чтобы это стало возможным.

Допущения:

– У злоумышленника нет никаких априорных сведений о зашифрованном сообщении (все исходные варианты равновероятны).

– Отсутствуют специальные символы

Пример работы алгоритма:

Воспользуемся RSA алгоритмом.

Для построения RSA алгоритма нам будет необходимо:

1) Выбрать два случайных простых числа p и q
2) Найти модуль: $n = pq$
3) Найти функцию Эйлера $\varphi(n) = (p-1)(q-1)$
4) Найти простое число e, $1 < e < \varphi(n)$, где e – взаимно простое по отношению к φ(n)
5) Найти d из уравнения $de \equiv 1(\operatorname{mod} \varphi(n))$

В итоге, получим пары (e,n) – открытый ключ, (d,n) – закрытый ключ.

Допустим, у нас есть ряд чисел, которые необходимо зашифровать

T: 2 1 4 3 8 5 6 n = 10 e = 3 d = 3

$$E(m) = m^e \qquad (1)$$

$$c = E(m) \operatorname{mod} n \qquad (2)$$

$$D(c) = c^d \qquad (3)$$

$$m = D(c) \operatorname{mod} n \qquad (4)$$

Воспользовавшись формулами 1-4 получим:

$E(m)$:	8	1	64	27	512	125	216
c:	8	1	4	7	2	5	6
$D(c)$	512	1	64	343	8	125	216
m:	2	1	4	3	8	5	6

Оценка полученного алгоритма

Для качественной оценки алгоритма нам будут необходимы формулы 5-7:

$$H(T) = -\sum_{i=1}^{n} p_i \log_2 p_i \quad 5)$$

где H(T) – мера неопределенности сообщения/шифра. T – множество возможных отправленных сообщений, p_i – вероятность отправки соответствующего сообщения T_i, n – количество битов шифротекста. Физический смысл найденной величины: количество битов информации, которое необходимо в среднем передать, чтобы полностью устранить неопределенность.

После перехвата полученного сообщения получим следующее значение неопределенности (в литературе называемое условным):

$$H(T|T') = -\sum_{i=1}^{n} p_i(T|T')\log_2 p_i(T|T') \quad 6)$$

Где $p(T_i|T')$ – вероятность того, что исходное сообщение есть T_i при условии, что результат шифрования T'.

Отсюда найдем значимую характеристику нашего шифра:

$$I = H(T) - H(T|T') \quad 7)$$

Где I - информация об исходном тексте, которую злоумышленник может извлечь из перехваченного шифротекста. Необходимо обеспечить, чтобы $H(T) \to H(T|T')$ ($I \to 0$).

Т.е, чем меньше I, тем меньше вероятность однозначного дешифрования без знания ключа.

Качественная оценка полученного алгоритма

Для начала предположим, что один бит сообщения T – одна цифра. Передается по порядку следования. Никаких манипуляций, связанных с непоследовательной передачей сообщения, не было. Также не передается «шум» - какие-либо последовательности, не имеющие логического смысла.

Предположим, что злоумышленнику известно, что предаются цифры от 1 до 9.

Посчитаем H(T) из вышеописанных условий:

$p_i = 0,11111$ (1 к 9 , где событие – выбор конкретной цифры.)

Поскольку мы рассматриваем априорный случай, предыдущие сообщения никак не влияют на последующие:

$$H(T) = -\sum_{i=1}^{7} 0,11111\log_2 0,11111 = -2,4654 \quad 8)$$

Если никаких апостериорных сведений не было получено:

$H(T) = H(T|T')$, I=0 – самый лучший исход, возможный только теоретически.

Если предположить, что цифры не повторяются:

$$H(T|T') - \sum_{i=1}^{n} \frac{1}{n-i+1}\log_2\left(\frac{1}{n-i+1}\right) = -3,0518 \quad (9)$$

$$I = -2,4654 - (-3,0518) = 0,5864 \quad (10)$$

Вывод

Из вышеизложенного следует, что для построения шифра с высокими показателями криптографической стойкости необходимо учитывать вычислительную сложность алгоритма шифрования, условия передачи информации и изначальные показатели незашифрованного сообщения, поскольку из знания последних будет возможно найти уязвимость, которая существенно влияет на защиту информации.

Список использованных источников:

1. Липницкий, В. А. Современная прикладная алгебра. Математические основы защиты информации от помех и несанкционированного доступа: учеб.-метод. Пособие / В. А. Липницкий. – Минск: БГУИР, 2006.-87 с.

УДК 378.147:51

МОМЕНТ ИНЕРЦИИ СТЕРЖНЯ ПРИ ЕГО ВРАЩЕНИИ

Н. Н. Сендер, Д. В. Честный

Брестский государственный университет имени А. С. Пушкина, Брест

Рассмотрим так называемый момент инерции. Это понятие появляется при рассмотрении вращательного движения стержня. Пусть стержень вращается вокруг оси, перпендикулярной к плоскости чертежа и проходящей через начало координат. При таком вращении каждая точка стержня описывает окружность, радиус которой равен абсциссе данной точки x в начальном (горизонтальном) положении стержня (рисунок 1). Обозначим ω угловую скорость вращения, выраженную в рад/с. Это значит, что за время dt ось x поворачивается на угол $d\varphi = \omega dt$. Длина дуги, которую проходит произвольно выбранная точка с абсциссой x, равна

$$dl = xd\varphi = x\omega dt;$$

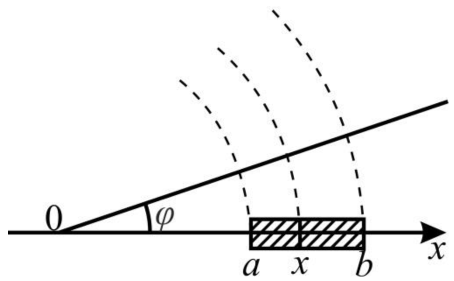

Рисунок 1

следовательно, линейная скорость движения каждой точки окружности равна

$$v(x) = \frac{dl}{dt} = \omega x.$$

Найдем кинетическую энергию вращательного движения всего стержня. Элемент массы dm, находящийся на расстоянии x от начала координат (в отрезке dx от x до $x + dx$), имеет кинетическую энергию

$$\frac{v^2}{2}dm = \frac{\omega^2 x^2}{2}dm = \frac{\omega^2 x^2}{2}\rho(x)dx.$$

Следовательно, кинетическая энергия всего стержня равна

$$E = \frac{\omega^2}{2}\int_a^b x^2 \rho(x)dx.$$