Министерство образования и науки Российской Федерации
Ярославский государственный университет им. П.Г. Демидова
Кафедра компьютерных сетей

Математические методы защиты информации

Методические указания

Ярославль 2004

ББК В 311
М 33
УДК 519.6

Составитель **М.В. Краснов**

Математические методы защиты информации: Метод. указания / Сост. М.В. Краснов; Яросл. гос. ун-т. – Ярославль, 2004. – 27 с.

В работе сформулированы основные идеи алгоритмов с открытым ключом. Наиболее известные из них подробно описаны. Особое внимание уделено электронной цифровой подписи как решению задач, связанных с аутентификацией документов.

Указания предназначены для студентов, обучающихся по направлению 510200 Прикладная математика и информатика (дисциплина "Математические методы защиты информации", блок СД), очной формы обучения.

Рецензент: кафедра компьютерных сетей Ярославского государственного университета им. П.Г. Демидова; д-р физ.-мат. наук Л.С. Казарин.

В настоящее время использование электронной вычислительной техники в различных областях человеческой деятельности все более и более возрастает. Однако чаще всего вычислительная техника используется для хранения и передачи информации. Естественно, возникает задача защиты информации от несанкционированного использования. Среди способов защиты информации одним из наиболее распространенных методов является криптографический метод. Он предусматривает такое преобразование информации, при котором она становится доступной для прочтения лишь обладателю некоторого секретного параметра (ключа).

Опишем задачу защиты информации с помощью криптографического метода. Отправитель хочет послать получателю по каналу, который не является безопасным, текст *T*. Взломщик хочет перехватить передаваемую информацию. Отправителю нужно так послать сообщение, чтобы взломщик не смог прочитать исходный текст *T* из перехваченного сообщения, а получатель мог бы за приемлемое время восстановить исходный текст из полученного сообщения.

Чтобы решить поставленную задачу, отправитель шифрует исходный текст *T* с помощью некоторого преобразования E_k, где *k* – ключ шифрования. Шифр-текст $C = E_k(T)$ передается по каналу связи.

Получатель должен уметь расшифровать шифр-текст – восстановить исходный текст *T* с помощью некоторого преобразования $D_{\tilde{k}}$, где $\tilde{k}$ - ключ расшифрования:

$$T = D_{\tilde{k}}(C).$$

Если отправитель знает ключ *k*, то он может зашифровывать информацию; если получатель знает ключ $\tilde{k}$, то он может расшифровывать сообщение.

Перед взломщиком стоит более сложная задача: он должен найти ключ $\tilde{k}$, или свой способ дешифровки.

Алгоритмы, используемые в современных криптосистемах, можно разделить на два типа:

♦ симметричные, в которых ключ расшифрования легко находится по ключу шифрования;

♦ с открытым ключом, в которых ключ расшифрования трудно найти даже при известном ключе зашифрования.

В представленных методических указаниях основное внимание уделяется алгоритмам с открытым ключом.

Элементы теории чисел

Алгоритм Евклида

Пусть a, b – целые числа, $b \geq 1$, тогда существуют такие однозначно определенные $q, r \in Z$, что

$$a = qb + r, \quad 0 \leq r < b.$$

Величину r (остаток от деления) будем обозначать $r = a \mod b$.

Всякое целое, делящее числа a и b без остатка, называется их общим делителем. Наибольший из общих делителей для чисел a и b называется наибольшим общим делителем и обозначается $НОД(a,b)$.

Утверждение. Для любых $a, b \in Z$ существуют $x, y \in Z$ такие, что

$$ax + by = НОД(a, b).$$

Напомним обобщенный алгоритм Евклида, который находит как наибольший общий делитель $d = НОД(a,b)$ двух целых чисел $a, b \in Z, b \geq 1$, так и числа $x, y \in Z$ из сформулированного утверждения.

Вход алгоритма $a, b \in Z$.

Выход алгоритма $d = НОД(a, b)$, $x, y \in Z$.

Алгоритм

Вводим четыре дополнительных переменных $x_0, x_1, y_0, y_1 \in Z$.

1. [Инициализация] $x_0 := 1; \quad x_1 := 0; \quad y_0 := 0; \quad y_1 := 1.$

2. [Основной цикл] Пока $b > 0$, выполнять следующий цикл{

$$q := \left[\frac{a}{b}\right]; \qquad r := a - qb;$$

$$a := b; \qquad b := r;$$

$$x := x_0 - q^* x_1; \qquad y := y_0 - q^* y_1;$$

$$x_0 := x_1; \quad x_1 := x; \qquad y_0 := y_1; \quad y_1 := y;$$

}

3. [Выход] Вернуть $d := a; \quad x := x_0; \quad y := y_0$

Алгоритм завершен.

Пример. Найти числа *x* и *y* такие, что $d = НОД(342,612) = ax + by$.

Рассмотрим обобщенный алгоритм Евклида.

Итерация	q	a	b	x_0	x_1	y_0	y_1
0	-	342	612	1	0	0	1
1	0	612	342	0	1	1	0
2	1	342	270	1	-1	0	1
3	1	270	72	-1	2	1	-1
4	3	72	54	2	-7	-1	4
5	1	54	18	-7	9	4	-5
6	3	18	0	9	-34	-5	19

Получаем 18=342*9+612*(-5).

Простые числа

Натуральное число $p \geq 2$ называется простым, если оно не имеет других натуральных делителей, кроме 1 и *p*.

Утверждение. Существует бесконечно много простых чисел.

Два целых числа *a* и *b* называются взаимно простыми, если $НОД(a,b) = 1$.

Определение. Функцией Эйлера $\phi(a)$ называется количество целых чисел на отрезке $[1,\ldots,a]$, взаимно простых с *a*.

Утверждения:

1) $\phi(p) = p-1$, если *p* - простое число;

2) если $НОД(a,b) = 1$, то $\phi(ab) = \phi(a)\phi(b)$;

3) если $n = p_1^{e_1} \ldots . p_k^{e_k}$, то $\phi(n) = n\prod_{i=1}^{k}\left(1-\frac{1}{p_i}\right)$;

4) если *p* – простое число, то $\phi(p^k) = p^k - p^{k-1}$, $k \in \mathbb{N}$.

Вычеты

Рассмотрим кольцо $\mathbb{Z}_n$ по модулю *n* (остатков от деления на *n*). Операции сложения и умножения выполняются по $\bmod n$.

Если $НОД(a,n) \neq 1$, то элемент $a \in \mathbb{Z}_n$ не имеет обратного, в противном случае элемент $a \in \mathbb{Z}_n$ имеет обратный, который можно найти, используя обобщенный алгоритм Евклида.