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 $q, r \in \mathbb{Z}$, 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 $a, b \in \mathbb{Z}$ существуют $x, y \in \mathbb{Z}$ такие, что

$$ax + by = НОД(a, b).$$

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

Вход алгоритма $a, b \in \mathbb{Z}$.

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

Алгоритм

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

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.

*Утверждения:*

1) *теорема Эйлера.* Пусть $НОД(a, n) = 1$, тогда $a^{\phi(n)} = 1 \mod n$;

2) *малая теорема Ферма.* Если $p$ - простое число и $a$, не делящееся на $p$ число, тогда справедливо равенство $a^{p-1} = 1 \mod p$.

Обозначим через $Z_n^*$ множество обратимых элементов $Z_n$.

*Определения:*

1) порядком элемента $a$ называется наименьшее целое число $S$ такое, что $a^s = 1 \mod n$;

2) элемент $a \in Z^*_n$ называется примитивным элементом, если порядок $a$ равен $\phi(n)$.

*Утверждения:*

1) группа $Z_n^*$ является циклической, если в ней существует примитивный элемент;

2) пусть $p$ - простое нечетное число. Тогда для группы $Z_n^*$, где $n = p^k$ или $2p^k$, существует примитивный элемент.

Из сформулированного выше утверждения следует, что все элементы группы $Z_n^*$, где $n = p^k$ или $2p^k$, можно записать как $Z_n^* = \{1, g, \ldots, g^{\phi(n)-1}\}$, где $g$ - примитивный элемент группы $Z_n^*$. Для чисел $a$, взаимно простых с $n$, введем понятие дискретного логарифма.

Пусть $a = g^y \mod n$. Число $y$ $(y \geq 0)$ называется дискретным логарифмом числа $a$ по модулю $n$ при основании $g$.

*Утверждение (китайская теорема об остатках).* Пусть задано:

- множество натуральных чисел $\{m_1, m_2, \ldots, m_k\}$, не равных единице, которые являются попарно взаимно простыми, т.е. $НОД(m_i, m_j) = 1$, при $i \neq j$;
- множество натуральных чисел $\{b_1, b_2, \ldots, b_k\}$ таких, что $0 \leq b_i < m_i$.

Тогда система сравнений

$$\begin{cases} x = b_1 \mod m_1 \\ x = b_2 \mod m_2 \\ \quad \dots \\ x = b_k \mod m_k \end{cases}$$

имеет единственное решение $x = x_0 \mod(m_1 m_2 \dots m_k)$; значение $M$ определяется как $x_0 = M_1 M_1' b_1 + M_2 M_2' b_2 + \dots + M_k M_k' b_k$, где числа $M_s$ и $M_s'$ определены из условий

$$m_1 m_2 \dots m_k = M_s m_s, \qquad M_s M_s' = 1 \mod m_s.$$

Пример. *Решим систему.*

$$\begin{cases} x = 1 \mod 4 \\ x = 3 \mod 5 \\ x = 2 \mod 7 \end{cases}$$

Рассматриваемая система удовлетворяет требованиям приведенного выше утверждения. Тогда легко заметить, что $M_1 = 35,\ M_2 = 28,$ $M_1 = 20.$ В свою очередь, не составляет труда вычислить, что $M_1' = 3,\ M_2' = 2,\ M_3' = 6.$

Осталось заметить, что $x_0 = M_1 M_1' b_1 + M_2 M_2' b_2 + \dots + M_k M_k' b_k$, а следовательно,

$$x_0 = 35*3*1 + 28*2*3 + 20*6*2$$

и, значит,

$$x = 105*1 + 56*3 + 120*2 \mod 140$$

$$x = 93 \mod 140.$$

**Проверка простоты нечетного числа**

Рассмотрим теперь задачу проверки на простоту большого числа *n*.

В основе первого теста лежит малая теорема Ферма. Она дает необходимый признак простоты числа *n*.

Выберем некоторое число *a*. Если $НОД(a, n) \neq 1,$ то *n* не является простым. Проверяем, выполняется ли $a^{n-1} = 1 \mod n.$ Если это сравнение нарушается, то *n* не является простым.

Однако выполнение малой теоремы Ферма не является достаточным признаком простоты числа. Оказалось, что теорема, обратная малой теореме Ферма, неверна, а именно существуют составные числа $n$ такие, что для любых $a$ с $НОД(a,n)=1$ имеет место сравнение $a^{n-1}=1 \mod n$. Такие числа называются числами Кармайка. Приведем несколько чисел Кармайка:

$$561=3\times11\times17 \qquad 1729=7\times13\times31$$
$$1105=5\times13\times17 \qquad 2465=5\times17\times29$$

В качестве второго теста проверки числа $n$ на простоту приведем вероятностный тест Миллера - Рабина:

1. Находим нечетное число $r$ и число $S$ такие, что $n-1=2^s r$.

2. Выбираем число $a$. Если $НОД(a,n)\neq1$, то $n$ не является простым.

3. Если $НОД(a,n)=1$, то проверяем выполнение хотя бы одного из условий:

1) $a^r=1 \mod n$;

2) существует $0\le s'<s$ такое, что $a^{2^{s'}r}=-1 \mod n$.

Если ни одно из условий невыполнимо, то $n$ не является простым.

Отметим, что для вероятностных тестов на простоту характерно, что, как правило, со 100-процентной гарантией можно определить, что число $n$ не является простым и только с вероятностью, близкой к 1 (но не равной 1), можно определить, что $n$ - простое число. Так, для теста Миллера - Рабина после нахождения $k$ чисел $a$, для которых тест выполняется, можно заключить, что вероятность того, что $n$ составное, не превосходит $\frac{1}{4^k}$.

В ГОСТ Р 34.10-94 для электронной цифровой подписи предложен следующий тест на простоту числа $n$.

1. Находим нечетное простое число $q$ и четное $p$ такие, что $n=qp+1$.

2. Если также $n<(2q+1)^2$ и выполняются условия:

1) $2^{qp}=1 \mod n$;

2) $2^p \neq 1 \mod n$,

то $n$ - простое.

## Криптосистемы с открытым ключом

Идею, лежащую в основе криптосистем с открытым ключом, высказали в 1975 г. У. Диффи и М. Хеллмэн. Они ввели понятие односторонней функции с секректом. Эта идея состоит в том, что по заданному аргументу $x$ легко вычислить значение функции $f(x)$, тогда как определение $x$ из $f(x)$ без учета дополнительной информации очень трудоемко. Это дало принципиальную возможность разрабатывать криптосистемы с открытым ключом, в которых алгоритм шифрования является общедоступным, и поэтому нет необходимости в секретных каналах связи для предварительного обмена ключами. На практике реализация идеи состоит в том, что используют два ключа: ключ зашифрования (открытый ключ) и ключ расшифрования (секретный ключ). Отметим, что лучшие криптосистемы с открытым ключом основаны на тех математических проблемах, которые решаются уже сотни лет и не решены до сих пор, несмотря на все усилия исследователей.

Рассмотрим несколько криптосистем с открытым ключом.

**Рюкзачный метод шифрования**

Выберем пару $w$, $m$ натуральных взаимно простых чисел и будем считать их секретными. Число $w$ назовем множителем, а $m$ – модулем. Дополнительно выберем секретную последовательность $b = (b_1, \ldots, b_n)$ положительных целых с двумя условиями:

$$b_i > \sum_{j=1}^{i-1} b_j, \text{ для любого } i \geq 1 \qquad \text{и} \qquad m > \sum_{j=1}^{n} b_j.$$

Такую последовательность будем называть сверхрастущей.

Последовательность $a = (a_1, \ldots, a_n)$, где

$$a_i \equiv w b_i \mod m, \qquad i \geq 1,$$

считается несекретной.

Сообщение $X = (x_1, \ldots, x_n)$, являющееся набором нулей и единиц, шифруется по правилу

$$C = \sum_{i=1}^{n} x_i a_i.$$

Для расшифрования полученного сообщения $C$ достаточно, решая уравнение вида $C = \sum_{i=1}^{n} \mu_i a_i$, найти вектор $\mu = (\mu_1, \ldots, \mu_n) \in \{0,1\}^n$. В этом случае вектор $\mu$ совпадает с вектором $x$. Уравнение расшифрования основано на задаче о рюкзаке, которая относится к классу NP-полных задач. Тем не менее следующее утверждение указывает эффективный метод ее решения легальным пользователем для сверхрастущих последовательностей.

*Утверждение.* Если $b = (b_1, \ldots, b_n)$ - сверхрастущая последовательность и $S > 0$, то уравнение $S = \sum_{i=1}^{n} x_i b_i$ имеет не более одного решения $x = (x_1, \ldots, x_n) \in \{0,1\}^n$ с условием $S \le \sum_{i=1}^{n} b_i$.

Метод решения задачи о рюкзаке для сверхрастущих последовательностей можно описать как

$$x_i = \begin{cases} 1, & \textit{если} \quad S \ge b_i + \sum_{j=i+1}^{n} x_j b_j \\ 0, & \textit{если} \quad S < b_i + \sum_{j=i+1}^{n} x_j b_j \end{cases}, \qquad i = 1, \ldots, n.$$

Остается показать, что для легального пользователя функция расшифрования эффективно вычислима. При получении зашифрованного сообщения $C$ пользователь вычисляет $w^{-1}$, для которого выполняется условие $w * w^{-1} = 1 \mod m$, и находит $S = w^{-1} C \mod m$. Для завершения процедуры расшифрования легальному пользователю остается решить «задачу о рюкзаке»: $S = \sum_{i=1}^{n} x_i b_i$. Действительно,

легальный пользователь должен решить уравнение вида $C = \sum_{i=1}^{n} x_i a_i \Rightarrow$

$$w^{-1}C = w^{-1}\sum_{i=1}^{n} x_i w b_i \mod m \Rightarrow w^{-1}C = \sum_{i=1}^{n} x_i b_i \mod m.$$

*Пример.* Построим рюкзачную криптосистему.

Пусть $b = (1,7,13,28,52)$, $m = 111$ и $w = 55$ образуют секретный ключ рюкзачной криптосистемы. Тогда последовательность $a = (55,52,49,97,85)$ образует открытый ключ.

Пусть двоичное представление текста *M* (текст, который надо зашифровать) - это (1,0,0,1,1).

Вычислим число *C*, которое и будет шифр-текстом:

$$C = \sum_{i=1}^{5} x_i a_i = (55 + 97 + 85) = 237.$$

Выполним расшифрование этого шифр-текста. С помощью обобщенного алгоритма Евклида найдем $w^{-1}$ и вычислим вспомогательную переменную *S*, для которой выполняется равенство $S = w^{-1}C$. Следовательно, $w^{-1} = 109$, а $S = 109 * 237 \mod 111$, т.е. $S = 81$. Расшифрование завершается решением «задачи о рюкзаке»: $81 = \sum_{i=1}^{n} x_i b_i$. Легко заметить, что $x = (1,0,0,1,1)$.

Отметим, что стойкость рюкзачной криптосистемы очень низка. Это связано с тем, что для расшифрования не обязательно знать секретный ключ $(w, m)$. Взломщик знает последовательность $a = (a_1, \ldots, a_n)$ и может попытаться успешно найти пару чисел $(\overline{w}, \overline{m})$ таких, что последовательность $\overline{b} = (\overline{b_1}, \ldots, \overline{b_n})$, определяемая условием $\overline{b_i} = a_i w \mod m$, является сверхрастущей и обладает свойством $m > \sum_{j=1}^{n} \overline{b}_j$. Полученную пару $(\overline{w}, \overline{m})$ взломщик использует в качестве секретного ключа.

**Криптосистема RSA**

Метод шифрования RSA предложен в 1977 г. Ривестом, Шамиром и Адлеманом. Опишем процесс шифрования сообщений. Сначала исходный текст должен быть переведен в числовую форму. Будем считать, что метод преобразования текста в числовую форму считается известным. В результате текст представляется в виде одного большого числа. Затем полученное число разбивается на части так, чтобы каждая из них была числом в промежутке от 0 до $n$, где $n$ будет выбрано позже. Процесс шифрования одинаков для каждой части. Поэтому можно считать, что исходный текст представлен числом $x$ таким, что $0 < x < n$.

Параметрами алгоритмов шифрования и расшифрования RSA являются:

1) открытый ключ - числа $n$ и $e$, которые подчинены двум условиям:

1.1) $n = pq$, где $p$ и $q$ – большие простые числа, которые держатся в секрете. Числа $p$ и $q$ обычно выбираются порядком не ниже чем $2^{256}$;

1.2) число $e$ берется взаимно простым с $\phi(n) = (p-1)(q-1)$.

2) секретный ключ образуют уже упомянутые числа $p$ и $q$, а также число $d$ такое, что $1 \le d \le n-1$ и $ed = 1 \mod \phi(n)$.

Шифрование блока $x$ $(0 < x < n)$ происходит по правилу

$$C = x^e \mod n.$$

Расшифрование блока $C$ $(0 < C < n)$ выполняется по правилу

$$x = C^d \mod n.$$

*Утверждение.* Если тройка $(n, e, d)$ образует RSA - криптосистему и известно натуральное $d$ такое, что $ed = 1 \mod \phi(n)$, то существует эффективный вероятностный алгоритм полиномиальной сложности для факторизации $n$.

*Пример.* Построим криптосистему RSA.

Пусть $p = 3$, а $q = 11$, тогда $n = pq = 3*11 = 33$. Вычислим функцию Эйлера $\phi(33)$. Поскольку $\phi(n) = (p-1)(q-1)$, то $\phi(33) = 20$. В качестве открытого ключа возьмем пару $(n, e)$, где $e = 7$. Проверим,

выполняется ли условие взаимной простоты $e$ и $\phi(n)$. Действительно, $НОД(7,20)=1$. В качестве секретного ключа возьмем $d=3$ и проверим, выполняется ли условие $ed=1 \mod \phi(n)$. Действительно, условие $7*3=1 \mod 20$ выполняется. В качестве текста, который надо зашифровать, возьмем $x=14$.

Найдем шифр-текст $C=x^e \mod n \Rightarrow C=(14)^7 \mod 33 \Rightarrow C=20$.

Расшифруем пришедший шифр-текст, пусть $C=20$, тогда

$x=C^d \mod n \Rightarrow x=(20)^3 \mod 33 \Rightarrow x=14$.

*Возможные атаки на криптосистему RSA*

Метод повторного шифрования. Он состоит в следующем. Пусть $e$ - экспонента зашифрования, $C$ - зашифрованное сообщение, для которого выполняется условие $C=x^e \mod n$ для некоторого $x$. Строим последовательность $C_i$ :

$$C_1=C;$$

$$C_i=C_{i-1}^e \mod n.$$

Последовательность строится до тех пор, пока вновь не получим шифр-текст $C$. Пусть $C_N=C$, тогда $C_{N-1}=x$. Аналогичный метод криптоанализа можно построить для любого алгоритма с открытым ключом.

*Пример.* Рассмотрим метод повторного шифрования.

Пусть известно, что $C=5$, $e=3$ и $n=33$. Требуется найти исходный текст $x$, для которого выполняется условие $C=x^e \mod n \Rightarrow 5=x^3 \mod 33$. Строим последовательность:

$$C_1=5;\ C_i=C_{i-1}^3 \mod 33.$$

Получаем $C_1=5; C_2=26; C_3=20; C_4=14; C_5=5$. Следовательно, исходный текст $x=14$.

**Криптосистема Рабина**

Стойкость схемы Рабина основана на трудности решения квадратичных сравнений по большому составному модулю.

Определим параметры криптосистемы:

выбираем два простых числа $p$ и $q$, для которых выполняются условия $p = 3 \mod 4$ и $q = 3 \mod 4$. Эта пара чисел образует секретный ключ криптосистемы Рабина, а их произведения $n = pq$ - открытый ключ.

Для зашифрования сообщения $m$ $(0 < m < n)$ вычисляем

$$c = m^2 \mod n.$$

Расшифрование. Предположим, что получено сообщение $c$, $(0 < c < n)$. Для расшифрования надо:

1) вычислить вспомогательные величины $r$ и $s$

$$r = c^{\frac{p+1}{4}} \mod p,\ s = c^{\frac{p+1}{4}} \mod q;$$

2) найти целые числа $a$ и $b$ такие, что $ap + bq = 1$;

3) исходным текстом $m$ будет одно из четырех значений

$$m_{1,2} = \pm(aps + bqr) \mod n$$

$$m_{3,4} = \pm(aps - bqr) \mod n.$$

Если исходное сообщение является осмысленным текстом, то правильное сообщение $m_i$ выбирается легко. С другой стороны, если сообщение – случайная последовательность цифр, то нет возможности определить корректное сообщение $m_i$. Один из методов, позволяющих облегчить процедуру выбора исходного текста из $m_1, m_2, m_3, m_4$, заключается в добавлении к исходному тексту перед шифрованием известного заголовка.

*Утверждение*. Пусть $n$ - произведение двух нечетных простых, тогда следующие условия эквивалентны:

- существует эффективный алгоритм решения сравнения $x^2 = m \mod n$;
- существует эффективный алгоритм факторизации $n$.

**Криптосистема Эль-Гамаля**

Схема Эль-Гамаля была предложена в 1985 г. Ее безопасность обусловлена сложностью вычисления дискретных логарифмов в конечном поле. Так же, как и в предыдущих криптосистемах, алгоритмы шифрования и расшифрования работают независимо с отдельными блоками, на которые разбит текст. Поэтому будем рассматривать работу криптосистемы только для отдельного блока.

Криптосистема Эль-Гамаля строится следующим образом:

1) сначала выбирается большое простое число $p$;

2) выбирается число $g$, которое является примитивным элементом поля $Z_p$;

3) выбирается случайное число $x$, причем $x < p$;

4) вычисляется число $y = g^x \mod p$.

Числа $p, g, x, y$ определяют параметры криптосистемы, причем тройка чисел $(p, g, y)$ образует открытый ключ, а $x$ - секретный ключ криптосистемы Эль-Гамаля.

Для того чтобы зашифровать сообщение $M$, надо выполнить следующие действия:

1) выбрать случайное целое число $k$, $1 < k < p-1$, такое, что числа $k$ и $p-1$ являются взаимно простыми;

2) вычислить числа $a = g^k \mod p$ и $b = y^k M \mod p$.

Пара чисел $(a, b)$ и есть зашифрованный текст.

Для того чтобы расшифровать полученное сообщение $(a, b)$, вычисляем $M = \dfrac{b}{a^x} \mod p$.

Поскольку $\dfrac{b}{a^x} = \dfrac{y^k M}{a^x} = \dfrac{g^{kx} M}{g^{kx}} = M \mod p$, то соотношение $M = \dfrac{b}{a^x} \mod p$ справедливо.

*Пример.* Построим криптосистему Эль-Гамаля.

Пусть $p = 13$, $g = 2$, секретный ключ $x = 8$. Вычислим $y = g^x \mod p$, следовательно, $y = 2^8 \mod 13 \Rightarrow y = 9$.

Пусть текст $M$, который надо зашифровать, равняется 5. Выберем некоторое случайное число $k = 7$. Убедимся, что $НОД(k, p-1) = 1$. Действительно, $НОД(7,12) = 1$.

Вычисляем пару чисел $(a, b)$.

$a = g^k \mod p$, следовательно, $a = 2^7 \mod 13 \Rightarrow a = 11$.

$b = y^k M \mod p$, следовательно, $b = 9^7 * 5 \mod 13 \Rightarrow b = 6.$

Получили пару чисел $(a,b) = (11,6)$, которая и есть зашифрованный текст.

Выполним расшифрование этого шифр-текста

$M = \frac{b}{a^x} \mod p$, следовательно, $M = \frac{6}{11^8} \mod 13 \Rightarrow$

$M = 6 * 11^{-8} \mod 13 \Rightarrow$ $M = 6 * 9^{-1} \mod 13 \Rightarrow$

$M = 6 * 3 \mod 13 \Rightarrow M = 5.$

## Электронная цифровая подпись (ЭЦП)

При работе с электронными документами в сети встает вопрос об аутентификации автора документа и самого документа, т.е. установления подлинности автора и отсутствия изменений в полученном документе. Цифровая подпись служит для решения задач аутентификации. Она представляет собой относительно небольшое количество дополнительной информации, передаваемой вместе с подлинным текстом. Система ЭЦП включает в себя две процедуры:

- постановка подписи;
- проверка подписи.

Обобщенной моделью ЭЦП можно считать следующую схему.

Пусть A и B - некоторые пользователи, обменивающиеся информацией по открытому каналу связи. Пусть $X$ - совокупность всевозможных сообщений, $Y$ - некоторое множество подписей. Пусть $F_k : Y \to X$ функция, которая зависит от параметра (ключа) $k$, а ключ $k$ состоит из двух частей: открытой $k_e$ и секретной $k_d$. Пусть для любого $x \in X$ существует прообраз $y = F_k^{-1}(x)$ и, кроме того, функция $F$ общеизвестна.

Предположим, что выполняются следующие свойства:

- зная открытый ключ $k_e$, функцию $F_k(y)$ можно вычислить за полиномиальное время;
- зная секретный ключ $k_d$, функцию $F_k^{-1}(x)$ можно вычислить за полиномиальное время;
- зная $k_e$, но не зная $k_d$, функцию $F_k(y)$ сложно инвертировать.

Подписью некоторого сообщения $x$ называется $y = F_k^{-1}(x)$, а пара $(x, y)$ называется подписанным сообщением.

В общем виде алгоритм ЭЦП можно описать следующим образом:

1. Для отправляемого сообщения $x$ отправитель А находит $y = F_k^{-1}(x)$; зная секретный ключ $k_d$, это можно сделать за полиномиальное время.

2. А передает В по каналу связи пару $(x, y)$.

3. Получив подписанное сообщение $(x, y)$, В находит $x' = F_k(y)$, знание открытого ключа позволяет сделать это за полиномиальное время.

4. Получатель В сверяет $x$ и $x'$. Если они совпадают, то полученное сообщение считается подлинным. В противном случае либо сообщение $x$ изменено (фальшивое), либо подпись $y$ неверная (поддельная).

Принципиальным моментом в системе ЭЦП является невозможность подделки ЭЦП пользователя без знания его секретного ключа.

Роль функции $F_k$ может играть некоторая схема шифрования с открытым ключом.

Перед описанием конкретных ЭЦП введем следующее определение.

*Определение*. Функцией хэширования называется отображение $h\colon\ A^* \to A^l$ слов конечной длины в алфавите $A$ в слова длиной $l$. Хэш-значение $Y = h(X)$ используется для контроля целостности $X$. Предполагается, что алгоритм вычисления хэш-значения является эффективным и общедоступным. Хэш-функция должна удовлетворять целому ряду условий:

1) хэш-функция должна быть чувствительной к всевозможным изменениям в тексте;

2) должна обладать свойством необратимости, т.е. задача подбора документа $X'$, который бы обладал требуемым хэш-значением, вычислительно трудная;

3) вероятность того, что хэш-значения двух различных документов совпадут, должна быть очень мала.

Отметим, что обычно электронная цифровая подпись строится не для первоначального текста $X$, а для его вычисленного хэш-значения $m = h(X)$. Это связано с тем, что вычисленное значение хэш-функции $h(X)$ представляет собой один короткий блок информации $m$, характеризующий весь текст $X$ в целом.

Поскольку хэш-функция считается общедоступной, дальнейшее ее обсуждение в настоящих методических указаниях проводиться не будет.

**Схема ЭЦП RSA**

Параметры схемы описываются аналогично рассмотренной выше криптосистеме и состоят из секретного ключа - $(p,q,d)$ и открытого ключа - $(n,e)$.

Формирование подписи $y$ для текста $x$ $(0 < x < n)$ определяется следующим правилом $y = x^d \mod n$.

Соответственно, проверка подписи заключается в вычислении $x' = y^e \mod n$ и в последующем сравнении $x'$ с $x$. Если они совпадают, то сообщение $x$ подлинное.

Атака на цифровую подпись RSA. Цифровая подпись RSA уязвима к так называемой мультипликативной атаке. Иначе говоря, если подписаны два сообщения $y_1 = x_1^d \mod n$ и $y_2 = x_2^d \mod n$, то можно без знания секретного ключа $d$ получить подпись $y = x^d \mod n$ под документом $x = x_1 x_2 \mod n$, так как $y = y_1 y_2 \mod n$.

**Схема ЭЦП Эль-Гамаля**

Параметры схемы совпадают с параметрами криптосистемы Эль-Гамаля, и соответственно тройка $(p,g,y)$ образует открытый ключ, а число $x$ - секретный ключ схемы.

Для того чтобы сформировать подпись для текста $M$, надо выполнить следующие действия:

1) выбрать случайное целое число $k$ $(1 < k < p-1)$ такое, что $k$ и $(p-1)$ являются взаимно простыми;

2) вычислить величину $a = g^k \mod p$ с помощью секретного ключа $x$ – целое число $b$

$$b = (M - xa)k^{-1} \mod (p-1).$$

Подпись – это пара чисел $(a,b)$.

Проверка подписи. После приема подписанного сообщения подпись считается подлинной, если выполняется равенство $y^a a^b = g^M \mod p$.

*Пример.* Построим ЭЦП Эль-Гамаля.

Выберем числа $p = 11,\ g = 2$ и секретный ключ $x = 8$. Вычислим значение открытого ключа $y = g^x \mod p = y = 2^8 \mod 11 \Rightarrow y = 3$.

Вычислим цифровую подпись для сообщения $M = 5$. Сначала выберем случайное целое число $k = 3$. Убедимся, что числа $k$ и $(p-1)$ являются взаимно простыми. Действительно, $НОД(3,10) = 1$. Найдем число $k^{-1}$, для которого выполняется условие $k * k^{-1} = 1 \mod(p-1)$. Легко заметить, что $k^{-1} = 7$. Далее вычисляем элементы $a$ и $b$ подписи:

$a = g^k \mod p = 2^3 \mod 11 = 8$

$b = (M - xa)k^{-1} \mod(p-1) = 7(5 - 8*8) \mod 10 = 7$

Цифровая подпись представляет собой пару чисел: $a = 8,\ b = 7$..

Проверка подписи. Приняв сообщение $M$ и цифровую подпись $(a = 8, b = 7)$, получатель вычисляет два числа:

$y^a a^b \mod p = 3^8 * 8^7 \mod 11 = 10$;

$g^M \mod p = 2^5 \mod 11 = 10$.

Так как эти два целых числа равны, принятое получателем сообщение признается подлинным.

**Схема ЭЦП DSA**

Алгоритм цифровой подписи DSA предложен в 1991 г.

Схема DSA строится следующим образом:

1) сначала выбирается большое простое число $p$ $\left(2^{512} < p < 2^{1024}\right)$;

2) выбирается простое число $q$ $\left(2^{159} < q < 2^{160}\right)$ и делитель числа $(p-1)$;

3) выбирается число $t$ $(0 < t < p)$. Если число $t^{\frac{p-1}{q}} = 1 \mod p$, то выбираем другое число $t$ $(0 < t < p)$; в противном случае $g = t^{\frac{p-1}{q}} \mod p$.

4) выбирается случайное число $x$, причем $1 < x < q$;

5) вычисляется число $y = g^x \mod p$.

Числа $p, g, x, y, q$ определяют параметры криптосистемы, причем числа $(p, g, y, q)$ образуют открытый ключ, а $x$ – секретный ключ схемы ЭЦП DSA.

Формирование подписи для текста $M$ происходит по следующему алгоритму:

1) вычисляется число $m$, которое равняется хэш-значению исходного текста $M$, причем $0 < m < q$;

2) выбирается случайное целое число $k$ $(0 < k < q)$;

3) вычисляется число $k^{-1}$, для которого выполняется условие $k * k^{-1} = 1 \mod q$;

4) находятся два числа $r$ и $s$ по следующему правилу:

$$r = (g^k \mod p) \mod q,$$

$$s = k^{-1}(xr + m) \mod q.$$

Подписью к сообщению $M$ является пара чисел $(r, s)$.

Проверка подписи. После получения сообщения $M'$ и подписи к нему $(r', s')$ надо убедиться, что $M$ совпадает с $M'$. Для этого:

1) если хотя бы одно из условий $0 < r' < q$, $0 < s' < q$ не выполняется, то подпись считается недействительной;

2) вычисляется $v = (s')^{-1} \mod q$;

3) находим

$z_1 = h(M')v \mod q$;

$z_2 = r'v \mod q$;

$u = ((g^{z_1} y^{z_2}) \mod p) \mod q$.

4) проверяем условие $r' = u$. Если оно выполняется, то подпись считается подлинной, а сообщение – неизмененнным.

*Пример*. Схемы DSA

Генерация ключа:

1) выбираем простые числа $p = 23$, $q = 11$ и проверяем, выполняется ли условие, что $q$ делит $(p - 1)$. Действительно, $\frac{(p-1)}{q} = \frac{22}{11} = 2.$;

2) выбираем число $t$ $(0 < t < p)$. Пусть $t = 3$, тогда вычисляем $g = t^{\frac{p-1}{q}} \mod p \Rightarrow g = 3^2 \mod 23 \Rightarrow g = 9$;

3) выбирается случайное число $x$, причем $1 < x < q$, пусть $x = 2$;

4) вычисляем $y = g^x \mod p \Rightarrow y = 9^2 \mod 23 \Rightarrow y = 12$.

Открытый ключ ( $p = 23, q = 11, g = 9, y = 12$), секретный – $x = 2$.

Вычислим цифровую подпись для сообщения $M$.

1) найдем хэш-значение для этого сообщения, пусть $m = h(M) = 3$;

2) выберем произвольное целое число $k$ $(0 < k < q)$, пусть $k = 4$;

3) вычислим значение $k^{-1} \mod q$, легко заметить, что $k^{-1} = 3$;

4) чтобы создать цифровую подпись для сообщения $M$, осталось найти числа $r$ и $s$:

$$r = (g^k \mod p) \mod q \Rightarrow r = (9^4 \mod 23) \mod 11 \Rightarrow r = 6.$$

$$s = k^{-1}(xr + m) \mod q \Rightarrow s = 3(2*6 + 3) \mod 11 \Rightarrow s = 1.$$

Пара чисел (6,1) является цифровой подписью сообщения $M$.

Проверка подписи. Приняв сообщение $M'$ и цифровую подпись $(r' = 6, s' = 1)$, получатель выполняет следующие действия:

1) проверяет неравенства $0 < r' < q$, $0 < s' < q$. Если они не выполняются, то подпись считается недействительной;

2) вычисляет хэш-значение для принятого сообщения, пусть $m' = h(M') = 3$;

3) вычисляет $v = (s')^{-1} \mod q \Rightarrow v = 1^{-1} \mod 11 \Rightarrow v = 1$;

4) находим

$z_1 = h(M')v \mod q \Rightarrow z_1 = 3*1 \mod 11 \Rightarrow z_1 = 3$;

$z_2 = r'v \mod q \Rightarrow z_2 = 6*1 \mod 11 \Rightarrow z_2 = 6$;

$u = ((g^{z_1} y^{z_2}) \mod p) \mod q \Rightarrow$

$u = ((9^3 * 12^6) \mod 23) \mod 11 \Rightarrow u = 6$;

5) проверяем условие $r' = u$. Если оно выполняется, то подпись считается подлинной, а сообщение - неизмененнным.

Сделаем несколько замечаний относительно алгоритма DSA:

• алгоритм DSA медленный. В то время как скорость получения подписи сравнима со скоростью шифрования по схеме RSA, проверка подписи в большом количестве случаев примерно в 100 раз медленнее, чем RSA;

• анализ алгоритма показывает, что в данном случае проблема взлома подписи, вообще говоря, не сводится к проблеме дискретного логарифмирования, поскольку в алгоритме DSA $g$ – не примитивный элемент по модулю $p$, а лишь элемент порядка $q$, что намного меньше $p-1$. Таким образом, вполне возможно, что проблема взлома алгоритма ЭЦП легче общей проблемы дискретного логарифмирования.

**Схема ГОСТ Р 34.10-94**

Алгоритм цифровой подписи, определяемый этим стандартом, концептуально близок к алгоритму DSA. Он задается следующими параметрами:

1) большое простое число $p$, где $\left(2^{509} < p < 2^{512}\right)$ либо $\left(2^{1020} < p < 2^{1024}\right)$;

2) $q$ – простой сомножитель числа $(p-1)$, имеющий длину 254…256 бит;

3) целое число $g$ $(1 < g < p-1)$, такое, что $g^q \bmod p$ равняется 1;

4) целое число $x$, меньшее $q$;

5) целое число $y$, такое, что $y = a^x \mod p$.

Числа $p, g, y, q$ образуют открытый ключ, а $x$ - закрытый ключ схемы ЭЦП ГОСТ Р34.10-94.

Чтобы сформировать подпись для некоторого текста $M$, пользователь должен выполнить следующие действия:

1) вычислить значение вспомогательной переменной $m = h(M)$;

2) сгенерировать случайное число $k$, причем $k < q$;

3) вычислить значение переменных $r$ и $s$

$$r = (g^k \mod p) \mod q;$$

$$s = (xr + km) \mod q.$$

Если $rs = 0$, то выбираем другое значение $k$ и начинаем снова.

Цифровая подпись представляет собой пару чисел:

$$r \mod 2^{256} \text{ и } s \mod 2^{256}.$$

Алгоритм проверки подписи. После получения сообщения $M'$ и подписи к нему $(r', s')$ надо убедиться, что $M$ совпадает с $M'$. Для этого выполняем следующие действия:

1) если $r < 0$ или $r > q - 1$, или $s < 0$, или $s > q - 1$, то подпись недействительна;

2) вычисляем значение вспомогательной переменной $m' = h(M')$;

3) вычисляем $z_0 = (m')^{q-2} \mod q$;

4) вычисляем $z_1 = sz_0 \mod q$;

5) вычисляем $z_2 = ((q - r)z_0) \mod q$;

6) вычисляем $u = ((g^{z_1} * y^{z_2}) \mod p) \mod q$.

Если $u = r$, то подпись считается верной.

*Пример*. Построим схему ЭЦП ГОСТ Р 34.10-94.

Генерация ключа:

1) выбираем простые числа $p = 23$, $q = 11$. Остается проверить, выполняется ли условие: $q$ делит $(p - 1)$. Действительно, $\frac{(p-1)}{q} = \frac{22}{11} = 2$;

2) выбираем целое число $g = 2$ и проверяем, выполняется ли условие ($g^q \mod p$ равняется 1). Действительно, $2^{11} \mod 23$ равняется 1;

3) выбирается случайное число $x$, причем $1 < x < q$, пусть $x = 2$;

4) вычисляем $y = g^x \mod p \Rightarrow y = 2^2 \mod 23 \Rightarrow y = 4$.

Открытый ключ ( $p = 23, q = 11, g = 2, y = 4$), секретный – $x = 2$.

Вычислим цифровую подпись для сообщения $M$.

1) найдем хэш-значение для этого сообщения, пусть $m = h(M) = 3$;

2) выберем произвольное целое число $k$ $(0 < k < q)$, пусть $k = 6$;

3) чтобы создать цифровую подпись для сообщения $M$, осталось найти числа $r$ и $s$.

$$r = (g^k \mod p) \mod q \Rightarrow r = (2^6 \mod 23) \mod 11 \Rightarrow r = 7.$$

$$s = (xr + km) \mod q \Rightarrow s = (2*7 + 6*3) \mod 11 \Rightarrow s = 10.$$

Проверка подписи. Пусть было принято сообщение $M'$ и цифровая подпись $(r'=7, s'=10)$, для проверки подписи получатель выполняет следующие действия:

1) если $r<0$ или $r>q-1$, или $s<0$, или $s>q-1$, то подпись недействительна;

2) вычисляет хэш-значение для принятого сообщения, пусть $m'=h(M')=3$;

3) $z_0=(m')^{q-2} \mod q \Rightarrow z_0=(3)^9 \mod 11 \Rightarrow z_0=4$;

4) $z_1=s'z_0 \mod q \Rightarrow z_1=10*4 \mod 11 \Rightarrow z_1=7$;

5) $z_2=((q-r')z_0) \mod q \Rightarrow z_2=((11-7)*4) \mod 11 \Rightarrow z_2=5$;

6) вычисляем

$u=((g^{z_1}*y^{z_2}) \mod p) \mod q \Rightarrow$

$u=((2^7*4^5) \mod 23) \mod 11 \Rightarrow u=7.$

Поскольку условие $u=r'$ выполняется, то подпись $(r'=7, s'=10)$, считается подлинной, а сообщение $M'$ - неизмененнным.

## Несколько упражнений

**Элементы теории чисел**

1. Применяя обобщенный алгоритм Евклида к паре чисел 217 и 413, найдите числа $a$ и $b$ такие, что $d=НОД(217,413)=217a+413b$.

2. Решить систему сравнений

$$\begin{cases} x=1 \mod 3 \\ x=4 \mod 5 \\ x=2 \mod 7 \\ x=9 \mod 11 \\ x=3 \mod 13 \end{cases}$$

3. Указать общее решение для системы

$$\begin{cases} x=b_1 \mod 13 \\ x=b_2 \mod 17 \end{cases}$$

Пользуясь этим общим решением, далее найти три числа, которые при делении на 13 и 17 давали бы соответственно остатки 1 и 12, 6 и 8, 11 и 4.

4. Найти все примитивные элементы в $Z_7$ и в $Z_{81}$.

5. Докажите, что если $НОД(a,b)=1$, то $\phi(ab)=\phi(a)\phi(b)$.

**Криптосистемы с открытым ключом**

1. Зашифровано сообщение по правилу

$$y = x^k \mod p,$$

где $p$ - большое простое число, $1 \le x \le p-1$, $k$ - целое число $1 \le k \le p-1$. Показать, что если $k$ выбрано взаимно простым с $p-1$, то алгоритм расшифрования

$$d(y) = y^d \mod p$$

является корректным с $d = k^{-1} \mod(p-1)$ и $d(y) = x$.

2. Что случится с криптосистемой в предыдущей задаче, если ошибочно взять целое число $k$, которое не является взаимно простым с $p-1$.

3. Предположим, что пользователь RSA в качестве модуля $n$ по ошибке выбрал большое простое число. Показать, что в этом случае расшифровать текст легко.

4. Рассмотрим RSA систему с модулем $n$. Целое число $x$, $1 \le x \le n-1$, назовем неподвижной точкой, если оно и в зашифрованном виде тоже $x$. Показать, что если $x$ - неподвижная точка, то и $n-x$ также есть неподвижная точка.

5. Построить рюкзачную криптосистему со сверхрастущей последовательностью $b=(1,3,5,11,22,45,100)$ и зашифровать слово «вектор».

6. Построить криптосистему Рабина и зашифровать число 10.

**Электронная цифровая подпись**

1. В системе аутентификации, основанной на схеме RSA, пользователь А выбрал открытый ключ $e=7$ и $n=77$. Если он получит от В число 23, то что А должен ответить, чтобы аутентифицировать себя ?

2. В схеме подписи, основанной на RSA, пользователи А и В имеют открытые ключи $e_A=3$, $n_A=15$; $e_B=7$, $n_B=77$ соответственно. Пользователь А хочет послать сообщение. $M=4$ как подпись к некоторому документу. Какое целое число он посылает?

3. В схеме подписи RSA пользователь А имеет открытый ключ $e=11$, $n=899$. Как он подпишет сообщение 876?

4. В схеме подписи DSA пользователь A имеет открытый ключ (*p=124540019, q=17389, g=10083255, y=119946265*) и закрытый ключ *x=12496*. Как он подпишет сообщение, хэш-значение которого *h(m) = 5246*?

## Литература


1. Акритас А. Основы компьютерной алгебры с приложениями. М., 1994.

2. Виноградов И.М. Основы теории чисел. М., 1965.

3. Романец Ю.В., Тимофеев П.А. Защита информации в компьютерных системах и сетях. М., 2001.

4. Саломаа А. Криптография с открытым ключом. М., 1995.

5. Тимофеев Е.А. Защита информации в распределенных сетях. Ярославль, 2001.

6. Харин Ю.С., Берник В.И. Математические и компьютерные основы криптологии. Минск, 2003.

Учебное издание

# Математические методы защиты информации

Составитель **Краснов** Михаил Владимирович

Редактор, корректор В.Н. Чулкова
Компьютерная верстка И.Н. Ивановой

Подписано в печать 04.10.2004. Формат 60x84/16.
Бумага тип. Усл. печ. л. 1,63. Уч.-изд. л. 1,13. Тираж 70 экз. Заказ

Оригинал-макет подготовлен в редакционно-издательском отделе
Ярославского государственного университета

Отпечатано на ризографе

Ярославский государственный университет
150000 Ярославль, ул. Советская, 14.


# Математические методы защиты информации