9. ПРОБЛЕМА КВАДРАТИЧНОГО ВЫЧЕТА И ПРОБЛЕМА КВАДРАТНОГО КОРНЯ

8.1 Квадратичные вычеты. Символы Лежандра и Якоби

Число $a, a \in Z_n^*$, $1 \le a \le n$ называется *квадратичным вычетом по модулю* n, если существует число x, такое, что, $x^2 \equiv a(\mathrm{mod}\ n)$, иначе оно называется *квадратичным невычетом по модулю* n. При этом число x называется *квадратным корнем* числа a по модулю n. Будем обозначать Q_n и $\bar{Q}_n$ множества квадратичных вычетов и квадратичных невычетов по модулю n соответственно.

Если число $a \equiv x^2(\mathrm{mod}\ p)$, где p – простое число, то число $-x$ также удовлетворяет указанному сравнению, то есть квадратичный вычет a по модулю простого числа p имеет два квадратных корня.

Если p — простое число и α — образующий элемент группы Z_p^*, то $a \in Z_p*$ является квадратичным вычетом тогда и только тогда, когда $a = \alpha^i \bmod p$, где i — чётное. Отсюда следует, что $|Q_p| = |\bar{Q}_p| = (p-1)/2$, то есть половина элементов из Z_p^* является квадратичными вычетами, а вторая половина — квадратичными невычетами. Все квадратичные вычеты по модулю простого числа p можно найти возведением в квадрат по модулю p чисел 1,2,…, (p-1)/2.

Пример Число $\alpha = 6$ является примитивным элементом группы Z_{13}^*. Его степени приведены в таблице

i	0	1	2	3	4	5	6	7	8	9	10	11
$\alpha^i \bmod 13$	1	6	10	8	9	2	12	7	3	5	4	11

Из таблицы видно, что $Q_{13} = \{1, 3, 4, 9, 10, 12\}$ $\bar{Q}_{13} = \{2, 5, 6, 7, 8, 11\}$.

В общем случае для $n = p_1^{e_1} \cdot \ldots \cdot p_k^{e_k}$, где $p_1, \ldots,\ p_k$ — различные нечетные простые числа и $e_i \ge 1,\ i = 1, \ldots, k$, всякий элемент $a \in Q_n$ имеет точно 2^k квадратных корней в Z_n^*.

Пример а) Квадратными корнями числа 12 по модулю 37 являются числа 7 и 30.
б) Число 121 имеет 8 квадратных корней по модулю 315:

$$11, 74, 101, 151, 164, 214, 241\quad 304.$$

Символ Лежандра для целого a и простого p определяется следующим образом:

$$\left(\frac{a}{p}\right) = \begin{cases} 0, & \text{если } p \text{ делит } a, \\ 1, & \text{если } a \mod p - \text{ квадратичный вычет по модулю } p, \\ -1, & \text{если } a \mod p - \text{ квадратичный невычет по модулю } p, \end{cases}$$

Легко показать, что имеет место *критерий Эйлера*:

$$\left(\frac{a}{p}\right) = a^{(p-1)/2} \mathrm{mod}\ p.$$

Символ Якоби является обобщением символа Лежандра (поэтому обозначается так же). Он определяется для целого a и нечетного $n,\ n > 2$. Пусть n разлагается на простые множители:

$$n = p_1^{e_1} \cdots p_k^{e_k}.$$

Тогда символ Якоби определяется как произведение соответствующих символов Лежандра:

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right)^{e_1} \cdots \left(\frac{a}{p_k}\right)^{e_k}.$$

Для некоторых значений a символ Якоби вычисляется следующим образом:

$$\left(\frac{1}{n}\right) = 1,\ \left(\frac{-1}{n}\right) = (-1)^{(n-1)/2},\ \left(\frac{2}{n}\right) = (-1)^{(n^2-1)/8},$$

то есть $\left(\frac{2}{n}\right) = 1$ если $n \equiv 1$ или $7 \pmod 8$, и $\left(\frac{2}{n}\right) = -1$ если $n \equiv 3$ или 5 (mod 8).

Значение символа Якоби для нечетных чисел m и n, больших 2, можно вычислять на основе *закона взаимности*

$$\left(\frac{m}{n}\right) = (-1)^{(n-1)(m-1)/4} \cdot \left(\frac{n}{m}\right).$$

Можно показать, что это свойство эквивалентно следующему:

$$\left(\frac{m}{n}\right) = \left(\frac{n}{m}\right),$$

если только не выполняется $m \equiv n \equiv 3 (\mathrm{mod}\ 4)$.

В последнем случае

$$\left(\frac{m}{n}\right) = -\left(\frac{n}{m}\right).$$

"Числитель"в символе Якоби можно заменять любым сравнимым с ним по модулю "знаменателя"числом, использую следующее свойство символа Якоби: Если $a \equiv b \pmod n$, то $\left(\frac{a}{n}\right) = \left(\frac{b}{n}\right)$

Это позволяет с учетом закона взаимности вычислять символ Якоби по алгоритму, подобному алгоритму Евклида и имеющему ту же сложность.

Полезно использовать также свойство мультипликативности

$$\left(\frac{ab}{n}\right) = \left(\frac{a}{n}\right) \cdot \left(\frac{b}{n}\right).$$

Это свойство влечет

$$\left(\frac{ab^2}{n}\right) = \left(\frac{a}{n}\right).$$

Пример 4.

$$\left(\frac{2001}{2773}\right) = \left(\frac{2773}{2001}\right) = \left(\frac{772}{2001}\right) = \left(\frac{193}{2001}\right) = \left(\frac{2001}{193}\right) = \left(\frac{71}{193}\right) =$$

$$= \left(\frac{193}{71}\right) = \left(\frac{51}{71}\right) = -\left(\frac{71}{51}\right) = -\left(\frac{20}{51}\right) = -\left(\frac{5}{51}\right) =$$
$$= -\left(\frac{51}{5}\right) = -\left(\frac{1}{5}\right) = -1.$$

Используя свойства символа Якоби, при нечётном $n \geq 3$ и $a = 2^e a_1$, где a_1 нечётно, можно заключить, что

$$\left(\frac{a}{n}\right) = \left(\frac{2^e}{n}\right) \cdot \left(\frac{a_1}{n}\right) = \left(\frac{2}{n}\right)^e \cdot \left(\frac{n \bmod a_1}{a_1}\right) (-1)^{(a_1-1)(n-1)/4}.$$

Отсюда можно получить следующий рекурсивный алгоритм для вычисления символа Якоби $\left(\frac{a}{n}\right)$, не требующий факторизации n.

JACOBI(a,n)

ВХОД: нечётное целое $n \geq 3$, и целое $a \in Z_n^*$.

ВЫХОД: символ Якоби (Лежандра, если n – простое число) $\left(\frac{a}{n}\right)$

1. Если $a = 1$, то вернуть 1.

2. Если $2|a$
 если $2|(n^2-1)/8$ вернуть JACOBI $(a/2, n)$,
 иначе вернуть $-$JACOBI $(a/2, n)$;

(*теперь a – нечетное*)

3. Если $2|(a-1)(n-1)/4$ вернуть JACOBI $(n \bmod a, a)$;

4. вернуть – JACOBI $(n \bmod a, a)$.

Сложность алгоритма $O((\log n)^3)$. Символ Лежандра лучше вычислять по этому алгоритму, чем возведением в степень.

Пример Для $a = 158$ и $n = 235$ алгоритм вычисляет символ Якоби $\left(\frac{158}{235}\right)$ следующим образом:

$$\left(\frac{158}{235}\right) = -\left(\frac{79}{235}\right) = \left(\frac{77}{79}\right) = \left(\frac{2}{77}\right) = -\left(\frac{1}{77}\right) = -1.$$

Здесь учтено, что 2 не делит $(235^2-1)/8$, 2 не делит $(78\cdot 234)/4$, $2|(76\cdot 78)/4$, 2 не делит $(77^2-1)/8$). Заметим, что если n – простое число, то символ Якоби, просто вычисляемый описанным способом, указывает, является ли m квадратичным вычетом по модулю n.

8.2 Проблема квадратичного вычета и проблема квадратного корня

Если же n – составное, например, $n = pq$, то m является квадратичным вычетом по модулю n тогда и только тогда, когда $\left(\frac{m}{p}\right) = 1$ и $\left(\frac{m}{q}\right) = 1$. Но эти два условия не следуют из равенства 1 символа Якоби числа m по модулю n, так как $\left(\frac{m}{n}\right) = 1$

и в том случае, когда $\left(\frac{m}{p}\right) = -1$ и $\left(\frac{m}{q}\right) = -1$. (Такие вычеты m называются *псевдоквадратами* по модулю $n = pq$).

Но не известно, как различить эти два случая, не разлагая число n на простые множители. То есть из равенства $\left(\frac{a}{n}\right) = 1$ ещё не следует, что число a является квадратичным вычетом.

Проблема квадратичного вычета в том и состоит, что требуется узнать, является ли число m, символ Якоби по модулю составного числа $n = pq$ которого равен 1, квадратичным вычетом. В настоящее время неизвестен алгоритм ее решения, не предполагающий факторизации числа n.

Пример Множество квадратичных вычетов по модулю $n = 21 : Q_{21} = \{1, 4, 16\}$; множество квадратичных невычетов по модулю $n = 21 : \bar{Q}_{21} = \{2, 5, 8, 10, 11, 13, 17, 19, 20\}$. Последнее включает три псевдоквадрата 5,17 и 20.

Если разложение $n = pq$ известно, то можно извлечь квадратный корень из квадратичного вычета.

Действительно, если $0 < a < n$ – квадратичный вычет по модулю $n = pq$, то $a \mod p$ является квадратичным вычетом по модулю p, и $a \mod q$ является квадратичным вычетом по модулю q. то есть при существовании $x, x^2 \equiv a \pmod{n}$ существуют такие y и z, что

$$(\pm y)^2 \equiv a \pmod{p}, \quad (\pm z)^2 \equiv a \pmod{q}.$$

При известных p и q числа y и z могут быть найдены за полиномиальное время по алгоритму, приведенному ниже.

Тогда из сравнений

$$x \equiv \pm y \pmod{p} \quad x \equiv \pm z \pmod{q}$$

по китайской теореме об остатках[1] можно получить четыре квадратных корня x по модулю n. Обозначим их $\pm s$ и $\pm t$, где $s \not\equiv t (\mod n)$. (Такие s и t называются *различными* квадратными корнями).

При этом $s = cpz + dqy, \ t = cpz + dq(-y)$, где элементы c и d составляют решение диофантова уравнения $cp + dq = 1$.

Пример. Пусть $n = p \cdot q = 5 \cdot 7 = 35, \ a = 4$. Тогда $y = \sqrt{a} \mod 5 = \pm 3; \ z = \sqrt{a} \mod 7 = \pm 5$.

[1] Китайская теорема об остатках. *Если модули m_i взаимно просты, то система сравнений*

$$x \equiv a_i \pmod{m_i}, \quad i = 1, \ \dots, \ t,$$

имеет в интервале $[0, m-1], \ m = m_1 \cdot m_2 \cdot \ldots \cdot m_t$ *единственное решение x вида*

$$x = \Sigma_{i=1}^{t} a_i \cdot N_i \cdot \ M_i \mod m,$$

где $M_i = \frac{m}{m_i}, N_i = (M_i)^{-1} (\mod m_i), i = 1, \ldots, t$.

При $t = 2$ $m = n = pq, \ m_1 = p, \ m_2 = q, \ M_1 = q, \ M_2 = p, \ N_1 = q^{-1} \mod p, \ N_2 = p^{-1} \mod q$. $N_2 p + N_1 q = 1$, то есть N_1 и N_2 можно найти посредством расширенного алгоритма Евклида. После этого вычисляем корни $x = yqN_1 \pm zpN_2$.

Уравнение $cp+dq=1$ имеет вид $c\cdot 5+d\cdot 7=1$, его решение есть $c=3,\ d=-2$.
Отсюда $s=cpz+dqy=3\cdot 5\cdot 5-2\cdot 7\cdot 3 \mod 35=75-42=33.\ -s=2.$
$t=cpz-dqy=3\cdot 5\cdot 5-2\cdot 7\cdot 2 \mod 35=(75-28)\text{mod}35=12\ -\text{t}=23.$

Таким образом, знание разложения $n=pq$ позволяет вычислить различные квадратные корни.

Проблема квадратного корня заключается в том, что требуется найти квадратный корень из квадратичного вычета по модулю составного числа $n=pq$. В настоящее время неизвестен метод решения этой проблемы, не предполагающий факторизации числа n.

Проблема квадратного корня эквивалентна по сложности проблеме факторизации: как показано выше, знание факторизации составного модуля позволяет извлечь квадратный корень из квадратичного вычета; знание различных квадратных корней позволяет разложить $n=pq$ на простые множители за полиномиальное время. Действительно,

$$s^2-t^2=(s+t)(s-t)\equiv 0 \pmod n.$$

Это означает, что n делит $(s+t)(s-t)$.

Но по выбору s и t число n не делит ни $(s+t)$, ни $(s-t)$. Отсюда, число $s+t$ кратно числу p или q, и НОД$(s+t,n)$ есть p или q. Так что применяя алгоритм Евклида, можно разложить n.

8.3 Извлечение квадратного корня по модулю простого числа

Алгоритм 1.

ВХОД: простое число p, целое $a\in Q_n$.

ВЫХОД: квадратный корень a по модулю p.

1. (инициализация) Представить $p-1=2^s t$, где t нечетно; присвоить $b=a^t \pmod p$; $r:=s$, $k:=0$;

2. (первая задача) Найти $f\in \bar{Q}_n$; присвоить $g:=f^t \pmod p$;

3. (вторая задача, поиск экспоненты k);
пока $b\neq 1$
3.1. Найти наименьшее неотрицательное m такое, что $b^{2^m}\equiv 1 \pmod p$;
3.2. Присвоить $b:=bg^{2^{r-m}} \pmod p$; $k:=k+2^{r-m}$; $r:=m$;

4. Вернуть $a^{(t+1)/2}g^{k/2} \pmod p$.

Этот алгоритм можно оптимизировать, не прибегая к явному вычислению константы k.

Алгоритм 2.

ВХОД: нечетное простое p и целое a, $1 \le a \le p-1$.

ВЫХОД: два квадратных корня числа a по модулю p, в предположении, что a есть квадратичный вычет по модулю p.

1. Вычислить символ Лежандра $\left(\frac{a}{p}\right)$. Если $\left(\frac{a}{p}\right) = -1$, то вернуть ($a$ не имеет квадратных корней помодулю p) и завршить.

2. Выбирать случайно целые b, $1 \le b \le p-1$, пока не будет найдено число с символом Лежандра $\left(\frac{b}{p}\right) = -1$. ($b$ есть квадратичный невычет по модулю p.)

3. Многократным делением на 2, получить $p - 1 = 2^s t$, где t нечетно.

4. вычислить $a^{-1} \bmod p$ по расширенному алгоритму Евклида.

5. Принять $c = b^t \bmod p$ и $r = a^{(t+1)/2} \bmod p$.

6. Для i от 1 до $s-1$ выполнить:

   6.1 Вычислить $d = (r^2 \cdot a^{-1})^{2^{s-i-1}} \bmod p$.

   6.2 Если $d = -1 \pmod p$ то принять $r = r \cdot c \bmod p$.

   6.3 Принять $c = c^2 \bmod p$.

7. Вернуть$(r, -r)$.

Этот, как и предыдущий алгоритм вероятностный. Детерминированных алгоритмов вычисления квадратного корня по модулю простого числа не известно.

Временная сложность этого алгоритма $O((\lg p)^4)$ битовых операций.

Это оценка получается с учетом того, что шаг 6 выполняется $s-1$ раз, н на каждой итерации осуществляется возведение в степень, что требует $O((\lg p)3)$ битовых операций. При малых s алгоритм работает быстрее.

8.4 Частные полиномиальные алгоритмы

Если $p \equiv 3$ или $7 \pmod 8$, то квадратный корень по модулю p можно получить по формуле

$$x = \pm a^{(p+1)/4} \bmod p.$$

Действительно, в этом случае $p+1$ кратно 4. Пусть $x = a^{(p+1)/4} \bmod p$. Тогда с учетом того, что $a^{(p-1)/2} \equiv 1 \pmod p$, имеем

$$x^2 \equiv a^{(p+1)/2} \equiv a^{(p-1)/2} a \equiv a \bmod p.$$

Если $p \equiv 5 \bmod 8$, то

$$\text{а)} x = \pm a^{(p+3)/8} \bmod p, \text{ если } d = 1,$$

$$\text{б)} x = \pm (4a)^{(p+3)/8}/2 \bmod p, \text{ если } d = p-1,$$

где $d = a^{(p-1)/4} \bmod p$.

Действительно, в этом случае $p+3$ кратно 8. Поскольку $(p-1)/2$ четно, -1 удовлетворяет критерию Эйлера как квадратичный вычет. Пусть $x = a^{(p+3)/8} \bmod p$, $a \in Q_p$.

Из $a^{(p-1)/2} \equiv 1 \pmod p$, с учетом, что 1 в Z_p^* имеет только два квадратных корня 1 и -1, получаем $a^{(p-1)/4} \equiv \pm 1 \pmod p$.

Следовательно,

$$x^2 \equiv a^{(p+3)/4} \equiv a^{(p-1)/4} \cdot a \equiv \pm a \pmod p.$$

Если знак $+$, то это соответствует случаю а).

Если знак –, то

$$-x^2 \equiv (\sqrt{-1}x)^2 \equiv a \pmod p.$$

Поэтому решением является

$$x = \sqrt{-1}a^{(p+3)/8} \text{mod } p.$$

Задача сведена к вычислению $\sqrt{-1}(\text{mod } p)$.

Пусть b есть квадратичный невычет по модулю p. Тогда по критерию Эйлера

$$(b^{(p-1)/4})^2 \equiv b^{(p-1)/2} \equiv -1 \pmod p,$$

отсюда $b^{(p-1)/4} \pmod p$ можно взять вместо $\sqrt{-1}(\text{mod } p)$:

$$x \equiv (\sqrt{-1}a^{(p+3)/8(}\text{mod}) \; p \equiv b^{(p-1)/4}a^{(p+3)/8}(\text{mod } p).$$

Далее, заметим, что

$$p^2 - 1 = (p+1)(p-1) = (8k+6)(8k+4) = 8(4k+3)(2k+1),$$

и правая часть есть нечетное число, умноженное на 8. Поэтому $2 \in \bar{Q}_p$ (по свойству $\left(\frac{2}{p}\right)$). Таким образом, в этом случае можно использовать $2^{(p-1)/4}$ вместо $\sqrt{-1}$. Таким образом,

$$x \equiv (\sqrt{-1}a^{(p+3)/8} \equiv 2^{(p-1)/4}a^{(p+3)/8} \equiv (4a)^{(p=3)/8}/2 \pmod p.$$

Алгоритм извлечения квадратного корня по модулю p, $p \equiv 3,$ или $7 \pmod 4$ или $p \equiv 5(\text{mod } 8)$.):

ВХОД: простое число p, $p \equiv 3,$ или $7 \pmod 4$ или $p \equiv 5(\text{mod } 8)$, квадратичный вычет a по модулю p.

ВЫХОД: квадратный корень x числа a по модулю p.

1. Если $p \equiv 3$ или $7 \pmod 8$ вернуть $a^{(p+1)/4} \pmod p$;
2. если $a^{(p-1)/4} \equiv 1 \pmod p$вернуть $a^{(p+3)/8} \pmod p$;
3. вернуть $(4a)^{(p+3)/8}/2 \pmod p$.

Сложность этого алгоритма есть $O((\log\ p)^3)$.

Рассмотренные выше алгоритмы могут быть распространены на любые поля F_q нечетного порядка $q = p^m$, p простое, $m \geq 1$. Квадратные корни в полях четного порядка вычисляются в соответствии со следующим фактом:

Каждый элемент $a \in F_{2^m}$ поля четного порядка имеет единственный квадратный корень $a^{2^{m-1}}$.

8.5 Числа Блума

Особое значение в криптографии имеют числа Блума (Blum numbers). Составное число $n = pq$ называется числом Блума, если p и q – простые числа, сравнимые с 3 по модулю 4. Они имеют следующие свойства:

1) $\left(\frac{-1}{p}\right) = \left(\frac{-1}{q}\right) = -1,$ следовательно, $\left(\frac{-1}{n}\right) = 1;$

2)Для $y \in Z_n^*,$ если $\left(\frac{y}{n}\right) = 1,$то либо $y \in Q_n,$ либо $y \in \bar{Q}_n,$

3)каждый вычет $y \in Q_n$ имеет 4 квадратных корня $t, -t, s, -s,$ такие, что

а)$\left(\frac{s}{p}\right) = 1,$ $\left(\frac{s}{q}\right) = 1,$ то есть $s \in Q_n;$

б)$\left(\frac{-s}{p}\right) = -1,$ $\left(\frac{-s}{q}\right) = -1;$

в)$\left(\frac{t}{p}\right) = -1,$ $\left(\frac{t}{q}\right) = 1;$

г)$\left(\frac{-t}{p}\right) = 1,$ $\left(\frac{-t}{q}\right) = -1.$

д) функция $f(x) = x^2 \pmod{n}$ есть перестановка на Q_n;

е) для каждого $y \in Q_n$ точно один квадратный корень из y по модулю n, имеющий символ Якоби 1, меньше, чем n/2;

ж) Z_n^* разбивается на четыре класса эквиваленитности:

мультипликативная группа Q_n и три смежных левых класса:

$(-1)Q_n, \xi(Q_n), (-\xi)Q_n$, где ξ есть квадратный корень из 1 по модулю n с символом Якоби -1.

Примечание. По свойствам 3а), 3в) и 3б), 3г) два различных квадратных корня из квадратичного вычета имеют различные символы Якоби по модулю n.

8.6 BBS-генератор

Криптографическая стойкость Blum-Blum-Shub - генератора (BBS-генератора) базируется на сложности проблемы квадратичного вычета и проблемы извлечения квадратного корня.

BBS-генератор это $(k, l(k)-$генератор, осуществляющий вычисления по следующему алгоритму ($k \in Z^+,$ $l(x)$ есть полином над Z^+, l(k)>k).

ВХОД: k, l
ВЫХОД: псевдослучайное двоичное число $(z_1, z_2, \dots z_l)$ длины l.
Сформировать два секретных и разных простых числа p и q
длиной $k/2$ бит, конгруэнтных 3 по модулю 4.
Вычислить $n = p \cdot q$.
Выбрать случайное число $r \in [1, n-1]$
взаимно простое с числом n (НОД$(r, n) = 1$.
Вычислить "зерно"$s = r^2 \bmod n$ и принять $x_0 = s$
Для $i = \bar{1,} l$ выполнять
  $x_i = x_{i-1}^2 \bmod n$.
  $z_i = x_i \bmod 2$.

Как видим,

$$z_i = (s^{2^i} \bmod n) \bmod 2,\ 1 \le i \le l.$$

В теории криптографически стойких генераторов доказывается, что алгоритм, вычисляющий с неисчезающим предпочтением символ последовательности, предшествующий любому ее известному отрезку ее отрезку можно применить для решения проблемы квадратичного вычета. Рассмотрим пример конкретного BBS-генератора [3] См. на обороте (лист 11).

8.7 Обоснование Алгоритма 1

Пусть p –простое число и $p-1 = 2^s t$, где t – нечетное число, $s \geq 1$. Циклическая группа Z_p^* имеет единственную циклическую подгруппу G порядка 2^s. Квадратичные вычеты по модулю p из G имеют порядки, равные степени 2, поскольку они делят 2^{s-1}. Если $a \in Q_p$, то $a^t \in Q_p$ и $a^t \in G$, последнее – поскольку

$$a^{(p-1)/2} \equiv (a^t)^{2^{s-1}} \equiv 1 \ (\mathrm{mod}\ p.)$$

Следовательно, существует четное $k,\ 1 \leq k \leq 2^s$ такое, что

$$a^t g^k \equiv 1 \ (\mathrm{mod}\ p), \qquad (*)$$

где g – образующий элемент подгруппы G.

Пусть найдены образующий элемент $g \in G$ и четное k. Определим

$$x = a^{(t+1)/2} g^{k/2}. \qquad (**)$$

Легко проверить, что $x^2 \equiv a \ (\mathrm{mod}\ p)$.

Таким образом, задача разбита на две части:
(1) нахождение образующего элемента $g \in G$,
(2) нахождение наименьшего четного k, удовлетворяющего соотношению (*). Приведем алгоритм извлечения квадратного корня по модулю простого числа.

Первая задача решается легко: поскольку t нечетно, любой элемент $f \in \bar{Q}_n$ является нечетной степенью образующего элемента α группы $Z_p^* : f = \alpha^l$, $\mathrm{ord}_p(f) = 2^s \cdot t/l$ и по теореме о порядке степени элемента $\mathrm{ord}_p(f^t) = \mathrm{ord}\ \alpha^l/\text{НОД}\ (\mathrm{ord}\ \alpha^l, t) = 2^s$, поэтому f^t есть образующий элемент подгруппы G. Таким образом, выбирая случайно $f \in Z_n^p$ и проверяя $\left(\frac{f}{p}\right) = -1$, находим f^t – образующий элемент группы G. Вероятность успеха выбора такого элемента f есть $1/2$.

Вторая задача сложнее не на много. Для быстрого поиска k, удовлетворяющего (*), используем тот факт, что порядки не равных единице квадратичных вычетов из G есть степени 2. Так, полагая сначала

$$b = a^t \equiv a^t g^{2^s} \ (\mathrm{mod}\ p), (***)$$

имеем $b \in G$. Теперь можно найти наименьшее $m,\ 0 \leq m < s$ такое, что

$$b^{2^m} \equiv 1 \ (\mathrm{mod}\ p)$$

и затем преобразовать b следующим образом:

$$b := bg^{2^{s-m}} \equiv a^t g^{2^{s-m}} \ (\mathrm{mod}\ p).$$

После этого порядок b уменьшается, но остается степенью 2, b остается квадратичным вычетом из G. При повторном редуцировании m строго уменьшается. Когда m станет равным 0, b будет равно 1 и (***) преобразуется в (*).

Поскольку $s < \log_2\ p$, временная сложность алгоритма есть $Q((\log p)^4)$.

8.8 Специальный алгоритм

Следующий алгоритм извлечения квадратного корня по модулю простого p предпочтительнее предыдущего в случае, когда $p - 1 = 2^s \cdot t$ при большом s, Например, в случае $p =$

79076259159302559746169024888344288715687325104676653725950742075980075688534039141435558249060018496471634647195684070532840151603837158775762029726478655997560696112152198415517106805815588973853636194362645200040249434125776128536340811629524848704378024655888530796689097233146870422627311101523758131239860255062820510282741319901148431534999213215363534121237188194950246284442249548595555781122453612549517085054531233995922889749586673144014476787252150592743022654922687150869291812896325927934503293681102586066710347304382079042809556573966434559044700575973228231117989078950519716287995538203121342643929691810875645314924865979433114835616422571549164410495752130127239756399127685954763999852995652000715806933369288408707753549095114261820007947701632817349789046076530277096838749081825347635066364802515029585174421701561060380414675119918760178110966120396548278013577977522799979878007655471804453493745898233953698239585008558258080513959919617$=$

$= 2^{2690} \cdot 13407807929942597099574019452866457885849646663764598466210152088725515983664453741756386842562427028641847065611168086439252745761173904957497751170449409+1$.

ВХОД: нечетное простое a квадратичный вычет $a \in Q_p$.

ВЫХОД: два квадратных корня a по модулю p .

1. Выбирать случайно b, пока не будет получен квадратичный невычет $b^2 - 4a$ по модулю p т.е. $\left(\frac{b^2-4a}{p}\right) = -1$.

2. Пусть $f(X)$ есть полином $X^2 - bX + a$ в $Z_p[X]$.

Вычислить $r = X^{\frac{p+1}{2}} \bmod f(X)$. (r окажется целым.)

4. Вернуть $(r, -r)$.

Временная сложность этого алгоритма $O(\lg p)^3$ битовых операций.

8.9 Расширенный алгоритм Евклида

Расширенный алгоритм Евклида описывается следующим образом:

Вход: два неотрицательных целых числа a и b, $a \geq b$.

Выход: (a, b) и целые числа x и y, такие, что $ax + by = d$.

1. Присвоить $x_2 := 1,\ x_1 := 0,\ y_2 := 0,\ y_1 := 1$.

2. Пока $b > 0$ выполнять

 2.1. $q := \lfloor a/b \rfloor,\ r := a - qb,\ x := x_2 - qx,\ y := y_2 - qy_1$.

 2.2. $a := b,\ b := r,\ x_2 := x_1,\ x_1 := x, y_2 := y_1$, и $y_1 := y$.

4. Присвоить $d := a$, $x := x_2$, $y := y_2$ и возвратить (d, x, y).

Литература.

1. Саломаа А. Криптография с открытым ключом. – М.: Мир, 1986. 2. Венбо Мао. Современная криптография. Теория и практика. – М: Триумф. 2005. 3.Stinson D.R. Cryptography: theory and practice. – CRC Press LLC, Boca Raton, 1995. 4 . Menezes A.J., van Oorschoft P., Vanstone S.A. Handbook of Applied Cryptography. – CRC Press, Boca Raton, New York, London, Tokio, 1997.

Пример BBS-генератора

Пусть $n = 1922649 = 383 \times 503$, $r = 101355$ и $s = 101355^2 \bmod n$=20749. Первые 20 битов, производимые этим BBS-генератором представления в следующей таблице;

i	x_i	z_i	i	x_i	z_i	i	x_i	z_i	i	x_i	z_i
0	20749	1									
1	143135	1	6	80649	1	11	137922	0	16	133015	1
2	177671	1	7	45663	1	12	123175	1	17	106065	1
3	97048	0	8	69442	0	13	8630	0	18	45870	0
4	89992	0	9	186894	0	14	114386	0	19	137171	1
5	174051	1	10	177046	0	15	14863	1	20	48060	0