1. **ФУНКЦИЯ ЭЙЛЕРА, ТЕОРЕМА ЭЙЛЕРА, RSA-КС. ДОКАЗАТЬ МУЛЬПЛИКАТИВНЫЕ СВОЙСТВА И ТЕОРЕМУ ЭЙЛЕРА**

2.8 Функция Эйлера

Число классов вычетов в приведённой системе вычетов обозначают через $\varphi(m)$ и называют ***функцией Эйлера***. Функция Эйлера определена для всех натуральных чисел и представляет собой число чисел ряда $0, 1, \ldots, a-1$ $(1, 2, \ldots, a)$, взаимно простых с a.
Примеры. $\varphi(1) = 1$, $\varphi(2) = 1$, $\varphi(3) = 2$, $\varphi(4) = 2$, $\varphi(5) = 4$, $\varphi(6) = 2$.

Очевидны следующие свойства (p — простое).

Свойство 2.8.1. $\varphi(p) = p - 1$.

Свойство 2.8.2. $\varphi(p^k) = p^k - p^{k-1}, k \in \mathbb{N}$.

При $k = 1$ всё ясно. Пусть $k > 1$. Тогда в ряду $i = 1, 2, 3, \ldots, p^k$ условие $(i, p^k) = 1$ нарушается лишь для каждого p-го члена. Их всего имеется $p^k/p = p^{k-1}$.

Лемма 2.8.1 (мультипликативность функции Эйлера).

$$(a, b) = 1 \Rightarrow \varphi(a, b) = \varphi(a)\varphi(b).$$

Доказательство. Разместим числа $1, 2, \ldots, ab$ в таблицу

$$\begin{array}{ccccc}
1 & 2 & 3 & \ldots & b \\
b+1 & b+2 & b+3 & \ldots & 2b \\
2b+1 & 2b+2 & 2b+3 & \ldots & 3b \\
\vdots & \vdots & \vdots & \ddots & \vdots \\
(a-1)b+1 & (a-1)b+2 & (a-1)b+3 & \ldots & ab
\end{array}$$

Числа, взаимно простые с b, могут быть лишь в столбцах, номера которых взаимно просты с b. Все числа такого столбца взаимно просты с b. Таких столбцов всего $\varphi(b)$. По свойству 2.7.4 любой такой столбец представляет полную систему вычетов по модулю a. Поэтому он содержит $\varphi(a)$ чисел, взаимно простых с a. Воспользуемся теперь тем, что $(i, ab) = 1 \Leftrightarrow (i, a) = (i, b) = 1$ (2.3.1). Поэтому $\varphi(ab) = \varphi(a)\varphi(b)$. ■

Используя лемму и каноническое разложение числа на простые множители $a = p_1^{k_1} p_2^{k_2} \ldots p_s^{k_s}$, имеем

$$\varphi(a) = \left(p_1^{k_1} - p_1^{k_1-1}\right)\left(p_2^{k_2} - p_2^{k_2-1}\right)\ldots\left(p_s^{k_s} - p_s^{k_s-1}\right)$$

или

$$\varphi(a) = p^{k_1} p^{k_2} \ldots p^{k_s} \left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\ldots\left(1 - \frac{1}{p_s}\right),$$

$$\varphi(a) = a \prod_{p|a} \left(1 - \frac{1}{p}\right).$$

Функция Эйлера используется в теории сравнений.

Теорема 2.8.1 (Ферма). $a^{p-1} \equiv 1 (\bmod p)$, *если* $(a, p) = 1$.

Теорема 2.8.2 (Эйлера). $a^{\varphi(m)} \equiv 1 (\bmod m)$, *если* $(a, m) = 1$.

Первая теорема вытекает из второй, которая будет доказана в следующей главе.

Доказательство теоремы Эйлера во многом похоже на доказательство малой теоремы Ферма.

Рассмотрим различные натуральные числа $c_1 = 1, c_2, \ \ldots, c_{\varphi(b)}$ взаимно простые с b и не превосходящие b. Покажем, что числа $a \cdot c_1, a \cdot c_2, \ldots, a \cdot c_{\varphi(b)}$ дают различные остатки при делении на b, взаимно простые с b. Во-первых, все числа взаимно просты с b, т.к. a и c_i взаимно просты, во-вторых, все эти числа дают различные остатки при делении на b. Действительно, если это было бы не так, то

$$ac_i \equiv ac_j \pmod b, \text{ для некоторых } c_i \text{ и } c_j, \text{ где } 1 \leqslant c_i \neq c_j \leqslant b-1.$$

Но тогда возникает проблема с тем, что $a(c_i - c_j) = ac_i - ac_j \equiv 0 \pmod b$, т.е. $a(c_i - c_j) \vdots b$, что возможно, если $c_i - c_j \vdots b$, т.к. a и b взаимно просты. Но $-b < c_i - c_j < b$, поэтому $c_i - c_j = 0$, что неверно по нашему предположению. Значит, все числа ac_i дают различные остатки при делении на b. В-третьих, в наборе $a \cdot c_1, a \cdot c_2, \ldots, a \cdot c_{\varphi(b)}$ ровно $\varphi(b)$ число. Значит, числа $a \cdot c_1$, $a \cdot c_2, \ldots, a \cdot c_{\varphi(b)}$ дают все возможные взаимно простые b остатки при делении на b, т.е. точно такие же какие дают числа в наборе $c_1, \ c_2, \ \ldots, \ c_{\varphi(b)}$. Значит, справедливо сравнение:

$$c_1 c_2 \ldots c_{\varphi(b)} \equiv (ac_1)(ac_2)\ldots(ac_{\varphi(b)}) \equiv (a^{\varphi(b)})(c_1 c_2 \ldots c_{\varphi(b)}) \pmod b.$$

Так как правая и левая части делятся на $c_1 c_2 \ldots c_{\varphi(b)}$, которое взаимно просто с b, то мы можем поделить на это число правую и левую части, и получим требуемое сравнение:

$$a^{\varphi(b)} \equiv 1 \pmod b.$$

Теорема доказана.

RSA

Введение [править | править код]

Криптографические системы с открытым ключом используют так называемые односторонние функции, которые обладают следующим свойством:

- если известно x, то $f(x)$ вычислить относительно просто;
- если известно $y = f(x)$, то для вычисления x нет простого (эффективного) пути.

Под односторонностью понимается не математически доказанная однонаправленность, а практическая невозможность вычислить обратное значение, используя современные вычислительные средства, за обозримый интервал времени.

В основу криптографической системы с открытым ключом RSA положена сложность задачи факторизации произведения двух больших простых чисел. Для шифрования используется операция возведения в степень по модулю большого числа. Для дешифрования (обратной операции) за разумное время необходимо уметь вычислять функцию Эйлера от данного большого числа, для чего необходимо знать разложение числа на простые множители.

В криптографической системе с открытым ключом каждый участник располагает как открытым ключом (англ. *public key*), так и закрытым ключом (англ. *private key*). В криптографической системе RSA каждый ключ состоит из пары целых чисел. Каждый участник создаёт свой открытый и закрытый ключ самостоятельно. Закрытый ключ каждый из них держит в секрете, а открытые ключи можно сообщать кому угодно или даже публиковать их. Открытый и закрытый ключи каждого участника обмена сообщениями в криптосистеме RSA образуют «согласованную пару» в том смысле, что они являются *взаимно обратными*, то есть:

$\forall$ допустимых пар открытого и закрытого ключей (p, s)

$\exists$ соответствующие функции шифрования $E_p(x)$ и расшифрования $D_s(x)$ такие, что

$\forall$ сообщения $m \in M$, где M — множество допустимых сообщений,

$m = D_s(E_p(m)) = E_p(D_s(m)).$

Алгоритм создания открытого и секретного ключей [править | править код]

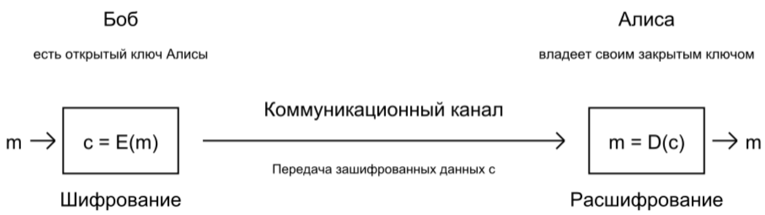
RSA-ключи генерируются следующим образом[15]:

1) выбираются два различных случайных простых числа p и q заданного размера (например, 1024 бита каждое);
2) вычисляется их произведение $n = p \cdot q$, которое называется *модулем*;
3) вычисляется значение функции Эйлера от числа n:
   $\varphi(n) = (p-1) \cdot (q-1);$
4) выбирается целое число e ($1 < e < \varphi(n)$), взаимно простое со значением функции $\varphi(n)$;
   число e называется *открытой экспонентой* (англ. *public exponent*);
   обычно в качестве e берут простые числа, содержащие небольшое количество единичных бит в двоичной записи, например, простые из чисел Ферма: 17, 257 или 65537, так как в этом случае время, необходимое для шифрования с использованием быстрого возведения в степень, будет меньше;
   слишком малые значения e, например 3, потенциально могут ослабить безопасность схемы RSA.[16];
5) вычисляется число d, мультипликативно обратное к числу e по модулю $\varphi(n)$, то есть число, удовлетворяющее сравнению:
   $d \cdot e \equiv 1 \pmod{\varphi(n)}$
   (число d называется *секретной экспонентой*; обычно оно вычисляется при помощи расширенного алгоритма Евклида);
6) пара (e, n) публикуется в качестве *открытого ключа RSA* (англ. *RSA public key*);
7) пара (d, n) играет роль *закрытого ключа RSA* (англ. *RSA private key*) и держится в секрете.

Шифрование и расшифрование [править | править код]

Предположим, Боб хочет послать Алисе сообщение m.

Сообщениями являются целые числа в интервале от 0 до $n-1$, взаимно простые с *n*, т.е. $m \in \mathbb{Z}_n, \gcd(m, n) = 1$.



Алгоритм шифрования[15]:

- Взять *открытый ключ* (e, n) Алисы
- Взять *открытый текст* m
- Зашифровать сообщение с использованием открытого ключа Алисы:
  $c = E(m) = m^e \mod n \quad (1)$

Алгоритм расшифрования:

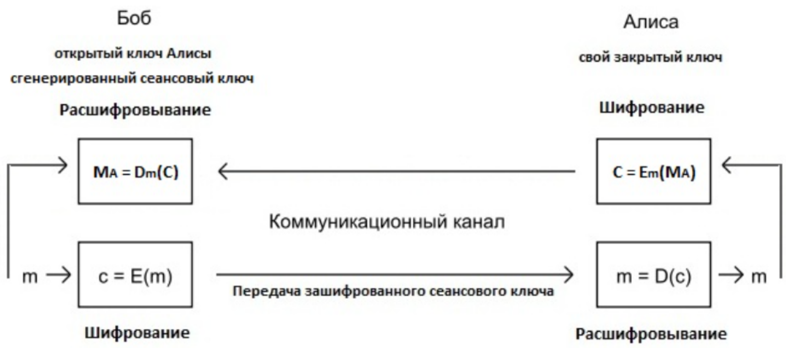
- Принять зашифрованное сообщение c
- Взять свой *закрытый ключ* (d, n)
- Применить закрытый ключ для расшифрования сообщения:
  $m = D(c) = c^d \mod n \quad (2)$

Данная схема на практике не используется по причине того, что она не является *практически надёжной* (semantically secured). Действительно, односторонняя функция E(m) является *детерминированной* — при одних и тех же значениях входных параметров (ключа и сообщения) выдаёт одинаковый результат. Это значит, что не выполняется необходимое условие практической (семантической) надёжности шифра.

Алгоритм шифрования сеансового ключа [править | править код]

Наиболее используемым в настоящее время[когда?] является смешанный алгоритм шифрования, в котором сначала шифруется сеансовый ключ, а потом уже с его помощью участники шифруют свои сообщения симметричными системами. После завершения сеанса сеансовый ключ, как правило, уничтожается.

Алгоритм шифрования сеансового ключа выглядит следующим образом[17]:



Алгоритм:

- Взять *открытый ключ* (e, n) Алисы
- Создать случайный *сеансовый ключ* m
- Зашифровать сеансовый ключ с использованием открытого ключа Алисы:

$$c = E(m) = m^e \mod n$$

- Зашифровать сообщение M_A с помощью сеансового ключа симметричным алгоритмом:

$$C = E_m(M_A)$$

Алгоритм:

- Принять зашифрованный сеансовый ключ Боба c
- Взять свой *закрытый ключ* (d, n)
- Применить закрытый ключ для расшифровывания сеансового ключа:

$$m = D(c) = c^d \mod n$$

- Расшифровать сообщение C с помощью сеансового ключа симметричным алгоритмом:

$$M_A = D_m(C)$$

В случае, когда сеансовый ключ больше, чем модуль n, сеансовый ключ разбивают на блоки нужной длины (в случае необходимости дополняют нулями) и шифруют каждый блок.

2. ПОКАЗАТЕЛИ, ПЕРВООБРАЗНЫЕ КОРНИ, ФОРМУЛИРОВКА ЗАДАЧИ ДИСКРЕТНОГО ЛОГАРИФМА, ПРОТОКОЛ ДХ

1.1 Понятие показателя. Простейшие свойства.

Определение. Будем говорить, что *число* a, $(a, n) = 1$ *принадлежит показателю* $\delta \in \mathbb{N}$ *по модулю* n, если δ - минимальное число, такое что $a^\delta \equiv 1 (mod\, n)$.

Замечание. Из теоремы Эйлера следует, что $1 \leq \delta \leq \varphi(n)$.

Пример. Число 4 принадлежит показателю 3 по модулю 9, так как $4^3 \equiv 64 \equiv 1 (mod\, 9)$, в то время как 4^2 и 4 не сравнимы с 1 по модулю 9.

Число 3 принадлежит показателю 4 по модулю 16, так как $3 \equiv 3 (mod\, 16)$, 3 $9 (mod\, 16)$, $3^3 \equiv 11 (mod\, 16)$, $3^4 \equiv 1 (mod\, 16)$.

Свойства показателей. Пусть a принадлежит показателю δ по модулю n. Тогда:

1)Числа a, $a^2, \ldots, a^\delta$ попарно несравнимы по модулю n.

Доказательство.

Предположим $a^\alpha \equiv a^\beta (mod\, n)$. Пусть $\alpha > \beta$. Тогда $a^{\alpha-\beta} \equiv 1 (mod\, m)$. В тоже время $\alpha - \beta < \delta$, что противоречит тому, что a принадлежит показателю δ по модулю n.

2)Сравнение $a^\alpha \equiv a^\beta (mod\, n)$ выполнено тогда и только тогда, когда $\alpha \equiv \beta (mod\, \delta)$.

Доказательство

Предположим $a^\alpha \equiv a^\beta (mod\, n)$. Пусть $\alpha > \beta$. Тогда $a^{\alpha-\beta} \equiv 1 (mod, m)$. По теореме о делении с остатком $\alpha - \beta = \delta p + q$, $0 \leq q < \delta$. Если $q \neq 0$, то получаем противоречие с минимальностью δ.

3)$\varphi(n)$ делится на δ.

Доказательство.

По теореме Эйлера $a^{\varphi(n)} \equiv 1 (mod\, n)$. Исходя из этого и свойства 2 получаем необходимое.

Пример. Найдём показатель которому принадлежит 7 по модулю 36. Заметим, что $\varphi(36) = \varphi(9)\varphi(4) = 6 \cdot 2 = 12$. Исходя из свойства 3 показатель может быть равен $2, 3, 4, 6$ или 12. С помощью небольшого перебора получаем, что он равен 6.

Замечание. Максимальное δ, такое что a, $a^2, \ldots, a^\delta$ попарно несравнимы по модулю n, является показателем a по модулю δ(доказать самостоятельно). В тоже время, если δ делит $\varphi(n)$, не означает, что a принадлежит показателю δ по модулю n.

1.2 Нахождение показателей.

Утверждение 1. Если a принадлежит показателю $\delta_1\delta_2$ по модулю n, то a^{δ_1} принадлежит показателю δ_2 по модулю n.

Доказательство

От противного. Пусть a^{δ_1} принадлежит показателю $\Delta \neq \delta_2$ по модулю n. Очевидно $\Delta < \delta_2$. Тогда

$$\left(a^{\delta_1}\right)^{\Delta} \equiv a^{\Delta\delta_1} \equiv 1 (mod\, n).$$

Но тогда $\delta_1\delta_2 > \Delta\delta_1$. Получаем противоречие.

Утверждение 2. Если a принадлежит показателю δ_1, а b показателю δ_2 по модулю n, и $(\delta_1, \delta_2) = 1$, то ab принадлежит показателю $\delta_1\delta_2$ по модулю n.

Доказательство

Случай, когда одно из чисел a и b сравнимо с 1 по модулю n очевиден. Далее будем считать, что $a \not\equiv 1 (mod\, n)$, $b \not\equiv 1 (mod\, n)$. Тогда и $\delta_1, \delta_2 \neq 1$.

Пусть ab принадлежит показателю Δ по модулю n. Отметим также, что $\Delta \neq 1$, в противном случае $b \equiv a^{-1} (mod\, n)$ и $\delta_1 = \delta_2$.

Нетрудно видеть, что $(ab)^{\delta_1\delta_2} \equiv 1 (mod\, n)$. Тогда $\Delta | \delta_1\delta_2$, тогда $\Delta = q_1q_2$, где $q_1|\delta_1$ и $q_2|\delta_2$. Отсюда следует что

$$(ab)^{\Delta} \equiv (ab)^{q_1q_2} (mod\, n) \Rightarrow ((ab)^{q_1q_2})^{\frac{\delta_1}{q_1}} \equiv a^{\delta_1 q_2} b^{\delta_1 q_2} \equiv b^{\delta_1 q_2} (mod\, n).$$

Таким образом $\delta_2|\delta_1 q_2$, исходя из того, что $(\delta_1, \delta_2) = 1$ получаем, что $\delta_2 | q_2$. Но как ранее было сказано $q_2|\delta_2$, а значит $q_2 = \delta_2$. Аналогично показываем, что $q_1 = \delta_1$. Таким образом $\Delta = \delta_1\delta_2$, что и требовалось доказать.

Утверждение 3. Пусть a принадлежит показателю δ по модулю n. Тогда a^{γ}, $\gamma \in \mathbb{N}$ принадлежит показателю $\frac{\delta}{(\delta,\gamma)}$ по модулю n.

Доказательство

Пусть a^{γ} принадлежит показателю Δ по модулю n. Тогда $a^{\Delta\gamma} \equiv 1 (mod\, n)$. Это равносильно тому, что $\delta | \Delta\gamma$. Найдём минимальное натуральное Δ удовлетворяющее этому условию. Нетрудно видеть, что это условие равносильно тому, что Δ кратно $\frac{\delta}{(\delta,\gamma)}$. Отсюда получаем, что $\Delta = \frac{\delta}{(\delta,\gamma)}$.

Задача 5. Пусть натуральное число a принадлежит показателю δ по модулю n. Для любого натурального γ найдите такое число принадлежащее показателю (δ, γ) по модулю n.

Решение.

Будем искать такое число в виде a^m. Исходя из Утверждения 3 оно будет иметь показатель $\frac{\delta}{(\delta,m)}$. Получается, что число a^m подходит тогда и только тогда, когда выполняется равенство

$$(\gamma, \delta) = \frac{\delta}{(\delta, m)}.$$

Пусь $d = (\gamma, \delta)$ и $\delta = d\delta_1$, $\gamma = d\gamma_1$, $(\gamma_1, \delta_1) = 1$. Тогда данное равенство можно переписать в виде

$$\delta_1 = (m, d\delta_1).$$

Отсюда очевидно следует, что число $m = \delta_1 = \frac{\delta}{(\delta,n)}$ подходит. То есть число $a^{\frac{\delta}{(\delta,n)}}$ принадлежит показателю (δ, γ) по модулю n.

2.11 Первообразные корни

Говорят, что число a, взаимно простое с модулем m, ***принадлежит показателю*** δ, если δ — такое наименьшее натуральное число, что выполняется сравнение $a^\delta \equiv 1 (\operatorname{mod} m)$. Справедливы следующие свойства.

Свойство 2.11.1. *Числа $a^0, a^1, \ldots, a^{\delta-1}$ попарно несравнимы по модулю m.*

Действительно, $a^l \equiv a^k \ (\operatorname{mod} m)$, $l > k \ \Rightarrow \ a^{l-k} \equiv 1 \ (\operatorname{mod} m)$, где $l-k \in \mathbb{N}$, $l-k < \delta$.

Свойство 2.11.2. $a^\gamma \equiv a^{\gamma'} (\operatorname{mod} m) \Leftrightarrow \gamma \equiv \gamma' (\operatorname{mod} \delta)$.

Разделим γ, γ' на δ с остатками $\gamma = \delta q + r$, $\gamma' = \delta q' + r'$. Тогда $a^\gamma \equiv a^{\gamma'} \Leftrightarrow a^{\delta q + r} \equiv a^{\delta q' + r'} \Leftrightarrow a^r \equiv a^{r'} \Leftrightarrow r' = r$. Отсюда вытекает следующее свойство.

Свойство 2.11.3. $\delta \mid \varphi(m)$.

Число, принадлежащее показателю $\varphi(m)$, называется ***первообразным корнем*** по модулю m.

Свойство 2.11.4. *По любому простому модулю p существует первообразный корень.*

Это свойство будет доказано в следующей главе. Гауссом установлено существование первообразных корней по модулям p^k и $2p^k$ при любом нечётном простом p. Легко убедиться, что при $m = 4$ первообразный корень также существует. Таким образом, первообразные корни существуют по модулям $2, 4, p^\alpha, 2p^\alpha$, где p — нечётное простое, $\alpha \in \mathbb{N}$.

Докажем отсутствие первообразных корней по всем остальным модулям. В этих случаях, если m не является степенью 2, $m = m_1 m_2$, $m_1 > 2$, $m_2 > 2$; $(m_1, m_2) = 1$, $\varphi(m_1) \equiv \varphi(m_2) \equiv 0 (\operatorname{mod} 2)$. Поэтому

$$a^{\varphi(m)/2} = \left(a^{\varphi(m_1)}\right)^{\varphi(m_2)/2} \equiv 1 (\operatorname{mod} m_1),$$

аналогично $a^{\varphi(m)/2} \equiv 1 (\operatorname{mod} m_2)$. Следовательно, $a^{\varphi(m)/2} \equiv 1 (\operatorname{mod} m)$ ввиду свойства 2.6.9. Если $m = 2^i$, то при нечётном a $a^2 \equiv 1 (\operatorname{mod} 8)$. Следовательно, $a^{2^{i-2}} \equiv 1 (\operatorname{mod} 2^i)$.

Следующее свойство упрощает нахождение первообразных корней.

Свойство 2.11.5. *Пусть $c = \varphi(m)$ и $q_1, q_2, \ldots, q_k$ — различные простые делители числа c. Число a, взаимно простое с модулем m, будет первообразным корнем тогда и только тогда, когда не выполнено ни одно из следующих сравнений:*

$$a^{c/q_1} \equiv 1 (\operatorname{mod} m), \ a^{c/q_2} \equiv 1 (\operatorname{mod} m), \ \ldots, \ a^{c/q_k} \equiv 1 (\operatorname{mod} m). \qquad (2.11.1)$$

Необходимость следует из того, что $a^{\varphi(m)} \equiv 1 (\operatorname{mod} m)$ и сравнение не имеет места при меньших показателях степени. Обратно, допустим, что a не удовлетворяет ни одному из сравнений и a принадлежит показателю $\delta < c$. Из этого следует $\delta \mid c \Rightarrow c = \delta n$. Обозначим через q простой делитель u. Тогда легко получить противоречие:

$$a^{c/q} = a^{\delta u/q} = \left(a^{\delta}\right)^{u/q} \equiv 1 (\operatorname{mod} m).$$

Пример. Пусть $m = 41$. Имеем $c = \varphi(41) = 40 = 2^3 \cdot 5$. Итак, первообразный корень не должен удовлетворять двум сравнениям:

$$a^8 \equiv 1 (\operatorname{mod} 41), \quad a^{20} \equiv 1 (\operatorname{mod} 41).$$

Испытываем числа 2,3,4,...: $2^8 \equiv 10$, $2^{20} \equiv \mathbf{1}$, $3^8 \equiv \mathbf{1}$, $4^8 \equiv 18$, $4^{20} \equiv \mathbf{1}$, $5^8 \equiv 18$, $5^{20} \equiv \mathbf{1}$, $6^8 \equiv 10$, $6^{20} \equiv 40$. Отсюда видим, что 6 является наименьшим первообразным корнем по модулю 41.

2.12 Существование первообразных корней

Теорема 2.12.1. *Пусть p — нечётное простое. Тогда по модулям вида p^k и $2p^k$, $k \geq 1$, существуют первообразные корни.*

Доказательство. Пусть a — первообразный корень по модулю p. Покажем, что существует такое целое x, что $a' = a + px$ будет первообразным корнем сразу по всем модулям вида p^k, $k > 1$. Поскольку a — первообразный корень по модулю p, то $a^{p-1} = 1 + py$ при некотором целом y. Применим теперь формулу бинома Ньютона:

$$(a')^{p-1} = (a + px)^{p-1} = a^{p-1} + (p-1)a^{p-2}px + \ldots =$$

$$= 1 + py + (p-1)a^{p-2}px + \ldots = 1 + p(y + (p-1)a^{p-2}x + \ldots).$$

В скобке коэффициент при x не делится на p. Поэтому x можно выбрать так, что эта скобка не будет делиться на p. В этом случае $(a')^{p-1} = 1 + pz$, где $(z, p) = 1$. Пусть теперь a' принадлежит показателю d по модулю p^k. Тогда d делит $p^{k-1}(p-1)$.

С другой стороны, $p-1$ делит d. Поэтому $d = p^l(p-1)$ при некотором $l < k$. Далее,

$$(a')^d = (1 + pz)^{p^l} = 1 + p^{l+1}u, \; (u, p) = 1.$$

Постановка задачи

Пусть в некоторой конечной мультипликативной абелевой группе G задано уравнение

Решение задачи дискретного логарифмирования состоит в нахождении некоторого целого неотрицательного числа x, удовлетворяющего уравнению (1). Если оно разрешимо, у него должно быть хотя бы одно натуральное решение, не превышающее порядок группы. Это сразу даёт грубую оценку сложности алгоритма поиска решений сверху — алгоритм полного перебора нашел бы решение за число шагов не выше порядка данной группы.

Чаще всего рассматривается случай, когда $G = \langle g \rangle$, то есть группа является циклической, порождённой элементом g. В этом случае уравнение всегда имеет решение. В случае же произвольной группы вопрос о разрешимости задачи дискретного логарифмирования, то есть вопрос о существовании решений уравнения (1), требует отдельного рассмотрения.

ПРОТОКОЛ ДИФФИ-ХЕЛЛМАНА

Описание алгоритма[2] [править | править код]

Предположим, существует два абонента: Алиса и Боб. Обоим абонентам известны некоторые два числа g и p, которые не являются секретными и могут быть известны также другим заинтересованным лицам. Для того, чтобы создать неизвестный более никому секретный ключ, оба абонента генерируют большие случайные числа: Алиса — число a, Боб — число b. Затем Алиса вычисляет остаток от деления[3] (1):

$$A = g^a \bmod p \quad (1)$$

и пересылает его Бобу, а Боб вычисляет остаток от деления (2):

$$B = g^b \bmod p \quad (2)$$

и передаёт Алисе. Предполагается, что злоумышленник может получить оба этих значения, но не модифицировать их (то есть, у него нет возможности вмешаться в процесс передачи).

На втором этапе Алиса на основе имеющегося у неё a и полученного по сети B вычисляет значение (3):

$$B^a \bmod p = g^{ab} \bmod p \quad (3)$$

Боб на основе имеющегося у него b и полученного по сети A вычисляет значение (4):

$$A^b \bmod p = g^{ab} \bmod p \quad (4)$$

Как нетрудно видеть, у Алисы и Боба получилось одно и то же число (5):

$$K = g^{ab} \bmod p \quad (5)$$

Его они и могут использовать в качестве секретного ключа, поскольку здесь злоумышленник встретится с практически неразрешимой (за разумное время) проблемой вычисления (3) или (4) по перехваченным $g^a \bmod p$ и $g^b \bmod p$, если числа p, a, b выбраны достаточно большими. Работа алгоритма показана на рисунке[4].

При работе алгоритма каждая сторона:

1. генерирует случайное натуральное число *a* — *закрытый ключ*
2. совместно с удалённой стороной устанавливает *открытые параметры p* и *g* (обычно значения *p* и *g* генерируются на одной стороне и передаются другой), где

   p является случайным простым числом

   (p-1)/2 также должно быть случайным простым числом (для повышения безопасности)[5]

   g является первообразным корнем по модулю *p (также является простым числом)*
3. вычисляет *открытый ключ A*, используя преобразование над *закрытым ключом*

   $A = g^a \bmod p$
4. обменивается *открытыми ключами* с удалённой стороной
5. вычисляет *общий секретный ключ K*, используя открытый ключ удаленной стороны *B* и свой закрытый ключ *a*

   $K = B^a \bmod p$

   K получается равным с обеих сторон, потому что:

   $B^a \bmod p = (g^b \bmod p)^a \bmod p = \mathbf{g^{ab} \bmod p} = (g^a \bmod p)^b \bmod p = A^b \bmod p$

В практических реализациях для *a* и *b* используются числа порядка 10^{100} и *p* порядка 10^{300}. Число *g* не обязано быть большим и обычно имеет значение в пределах первого десятка.

9.4 О поиске секретного ключа d и факторизации модуля N

Теорема 9.4.1. *Если тройка (N, e, d) образует RSA-криптосистему и известно натуральное d такое, что $ed \equiv 1 \pmod{\varphi(N)}$, то существует эффективный вероятностный алгоритм полиномиальной сложности для факторизации N.*

Доказательство. Пусть известны параметры e, d, удовлетворяющие условию теоремы. Тогда $s = ed - 1$ делится на $\varphi(N)$. Следовательно, для любого $x \in (\mathbb{Z}/N)^* = G$ верно

$$x^s \equiv 1 \pmod N.$$

Запишем $s = 2^t u$, где u — нечётное, и рассмотрим множество $A = G \backslash B$, где B состоит из тех $x \in G$, для которых либо при некотором целом $j \in \{1, \ldots, t-1\}$ верно $x^{2^j u} \equiv -1 \pmod N$, либо $x^u \equiv 1 \pmod N$.

Для любого элемента $a \in A$ выберем число k наименьшим с условием $a^{2^k u} \equiv 1 \pmod N$. Поскольку $a \notin B$, то $k \geq 1$. Тогда положим $b =$

$a^{2^{k-1} u} \pmod N$. Следовательно,

$$b^2 \equiv 1 \pmod N, \quad b \not\equiv \pm 1 \pmod N.$$

Из этого следует, что $(b-1, N)$ есть несобственный множитель N. Тем самым достигается факторизация.

Далее запишем $p - 1 = 2^{\nu_1} u_1$, $q - 1 = 2^{\nu_2} u_2$, где u_1, u_2 — нечётные числа. Положим $\nu = \min(\nu_1, \nu_2)$ и $K = (u, u_1) \cdot (u, u_2)$. Используя теорию сравнений, можно получить следующую оценку для числа решений сравнений $x^u \equiv 1 \pmod N$ и $x^{2^j u} \equiv -1 \pmod N$, $j \leq t-1$:

$$|B| = \left(1 + \frac{4^\nu - 1}{3}\right) \cdot K \leq \frac{\varphi(N)}{2} = \frac{1}{2}|G|.$$

Из этого вытекает, что вероятность того, что случайно взятый элемент $x \in G$ будет лежать в A, не менее $1/2$. Тогда за m попыток мы с вероятностью $\geq 1 - 1/2^m$ встретим элемент из A и найдём факторизацию N по алгоритму, вытекающему из доказательства. ■

Замечание 9.4.1. *Эквивалентность задач факторизации и поиска ключа d означает, что нельзя строить многопользовательскую RSA-криптосистему, чтобы различные пользователи имели свои различные ключи с одним и тем же модулем N. Потеря стойкости RSA-криптосистемы с параметрами (N, e, d) вследствие потери секретности ключа d влечёт необходимость не только смены ключа d, но и замены модуля N.*

Это означает, что $l = k - 1$, т. е. $d = p^{k-1}(p-1) = \varphi(p^k)$.

Рассмотрим теперь модуль $2p^k$. Возьмём первообразный корень a по модулю p^k. Одно из чисел a или $a + p^k$ нечётное. Оно также является и первообразным корнем по модулю $2p^k$, так как $\varphi(2p^k) = \varphi(p^k)$. ■

Таким образом, первообразные корни существуют лишь по модулям 2, 4, p^k, $2p^k$, где p — простое нечётное.

2.13 Индексы по модулям $p^k, 2p^k$

Обозначим через m модуль вида p^k или $2p^k$, а через g — первообразный корень по этому модулю. Положим $c = \varphi(m)$. Из свойства 2.11.1 вытекает следующее свойство.

Свойство 2.13.1. *Если число γ принимает последовательно значения $0, 1, \ldots, c-1$, то g^γ пробегает приведённую систему вычетов по модулю m.*

Для чисел a, взаимно простых с m, введём понятие об индексе, называемом иногда ***дискретным логарифмом***.

Пусть $a \equiv g^\gamma \pmod m$. Число $\gamma (\gamma \geq 0)$ называется ***индексом числа a по модулю m при основании g***. Будем использовать обозначения $\gamma = \operatorname{ind}_g a$ или $\gamma = \operatorname{ind}\ a$. В силу теоремы Эйлера индекс определён по модулю c. Тем самым было бы правильнее говорить о классе вычетов по модулю c.

Свойство 2.13.2. $\operatorname{ind}\ ab \equiv \operatorname{ind}\ a + \operatorname{ind}\ b \pmod c$.

Перемножая сравнения $a \equiv g^{\operatorname{ind}\ a} \pmod m$, $b \equiv g^{\operatorname{ind}\ b} \pmod m$, получаем требуемое.

Свойство 2.13.3. $\operatorname{ind}\ a^n \equiv n \operatorname{ind}\ a \pmod c$.

Если воспользоваться таблицами индексов, то можно решать показательные и степенные сравнения путём их индексирования (дискретного логарифмирования). В самом деле, степенное сравнение $x^n \equiv a \pmod m$ равносильно сравнению $n\ \operatorname{ind}\ x \equiv \operatorname{ind}\ a \pmod c$, решение которого при наличии таблиц не составляет труда. Положим $d = (n, c)$.

Свойство 2.13.4. *Сравнение $x^n \equiv a \pmod m$ разрешимо тогда и только тогда, когда d делит $\operatorname{ind} a$. В случае разрешимости имеется d решений.*

4. КВАДРАТИЧНЫЕ ВЫЧЕТЫ И КС РАБИНА

Квадратичный вычет

Материал из Википедии — свободной энциклопедии [править | править код]

Целое число a называется **квадратичным вычетом** по модулю m, если разрешимо сравнение[1]:

$$x^2 \equiv a \pmod m.$$

Если указанное сравнение не разрешимо, то число a называется квадратичным **невычетом** по модулю m. Решение приведенного выше сравнения означает извлечение квадратного корня в кольце классов вычетов.

Квадратичные вычеты широко применяются в теории чисел, они также нашли практические применения в акустике[2], криптографии, теории графов (см. Граф Пэли) и в других областях деятельности.

Понятие квадратичного вычета может также рассматриваться для произвольного кольца или поля. Например, квадратичные вычеты в конечных полях.

Свойства [править | править код]

- Критерий Эйлера: Пусть $p > 2$ простое. Число a, взаимно простое с p, является квадратичным вычетом по модулю p тогда и только тогда, когда[1]:

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

  и является квадратичным невычетом по модулю p тогда и только тогда, когда

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

- Квадратичный закон взаимности
- Квадратичные вычеты, взаимно простые с модулем, образуют мультипликативную подгруппу кольца вычетов индекса 2, в частности:
  - вычет × вычет = вычет;
  - невычет × вычет = невычет.
  - невычет × невычет = вычет.

Количество [править | править код]

По простому модулю [править | править код]

Среди ненулевых чисел $1, 2, \ldots, p-1$, для простого модуля $p \geq 3$ существует ровно $\frac{p-1}{2}$ квадратичных вычетов и $\frac{p-1}{2}$ невычетов.

Доказательство [скрыть]

Так как $x^2 \equiv (p-x)^2 \pmod p$, то достаточно показать, что среди чисел $0^2, 1^2, 2^2, \ldots, \left(\frac{p-1}{2}\right)^2$ нет сравнимых по модулю p.

Пусть такие числа есть и $x^2 \equiv y^2 \pmod p$ при $x \neq y$ и $0 \leq x, y \leq \frac{p-1}{2}$.

Так как $p \mid (x^2 - y^2)$, то $p \mid (x-y)(x+y)$ и, ввиду того, что p - простое, и $0 < |x-y| < p$, имеем $p \mid (x+y)$, что невозможно потому, что $x + y \leq p - 1$

Таким образом, ненулевые квадратичные вычеты образуют подгруппу индекса 2 в мультипликативной группе кольца $\mathbb{Z}_p$.

9.6 Система Рабина

Стойкость RSA-криптосистемы базируется на (предполагаемой) трудности задачи факторизации. Ответа на обратный вопрос пока нет. Остаётся неясным, следует ли из наличия эффективного алгоритма для обращения RSA-функции существование эффективного алгоритма для факторизации модуля N.

И. Рабин предложил систему с открытым ключом, трудность которой доказуемо равносильна трудности проблемы факторизации [92].

В ***системе Рабина*** пользователи выбирают два нечётных простых p, q. Они считаются секретными. Модуль $N = pq$ считается несекретным. Далее каждый пользователь выбирает целое $b < N$. Функция шифрования задаётся формулой

$$E_{N,b}(x) = x(x+b) \bmod N.$$

Дешифрование также несложно, если известна факторизация $N = pq$. Пусть m — зашифрованное сообщение. Используем известные алгоритмы решения сравнений $x(x+b) \equiv m \pmod p$ и $x(x+b) \equiv m \pmod q$. Обозначим их соответственно через r и s. Затем, используя алгоритм Евклида, вычислим k, l такие, что $kp + lq = 1$. Тогда решением сравнения $x(x+b) \equiv m(\operatorname{mod} N)$ будет $lqr + kps$.

Заметим, что решение указанных сравнений легко сводится к решению сравнения вида $x^2 \equiv m(\operatorname{mod} p)$. Это сравнение легко разрешимо при $p \equiv 3 \pmod 4$. В этом случае

$$p = 4k+3, \quad (m^{k+1})^2 = m^{2k+2} = mm^{\frac{p-1}{2}} \equiv m \pmod p.$$

Поэтому в практическом использовании системы Рабина берут простые числа вида $4k+3$. Заметим также, что сравнение $x^2 \equiv m \pmod N$ при $m \not\equiv 0 \pmod p$, $m \not\equiv 0 \pmod q$ имеет четыре решения.

Теорема 9.6.1. *Пусть N — произведение двух нечётных простых. Следующие условия эквивалентны.*

1. *Существует эффективный алгоритм решения сравнения $x^2 \equiv m \pmod N$.*
2. *Существует эффективный алгоритм для факторизации N.*

Доказательство. Случай $2 \Rightarrow 1$ фактически рассмотрен выше. Осталось показать $1 \Rightarrow 2$. Выберем случайно целое a такое, что $(a, N) = 1$, и пусть $m \equiv a^2 \pmod N$. Пусть есть решения сравнения $x^2 \equiv m \pmod N$. Итак, с одной стороны, если $u \notin \{a, N-a\}$, то $(N, u+a)$ — простой делитель N. С другой стороны, если $u \in \{a, N-a\}$, то выберем другое $u \notin \{a, N-a\}$ и повторим предыдущую процедуру. ∎

5. СТРОЕНИЕ КОНЕЧНЫХ ПОЛЕЙ

5.1 Конечные поля

Определение 5.1. *Кольцом* $\langle R, +, *\rangle$ называется множество R с двумя бинарными операциями $+$ и $*$ такими, что

1) $\langle R, +\rangle$ — абелева группа;

2) операция $*$ ассоциативна, т. е. $(a * b) * c = a * (b * c)$ для всех $a, b, c \in R$;

3) выполняются законы дистрибутивности:

$$a * (b + c) = a * b + a * c, \quad (a + b) * c = a * c + b * c, \quad a, b, c \in R.$$

Определение 5.2. Кольцо $\langle R, +, *\rangle$ называется *полем*, если $R \neq \{0\}$, где 0 — единица $\langle R, +\rangle$, и

4) $\langle R \setminus \{0\}, *\rangle$ — абелева группа. □

Для группы $\langle R, +\rangle$ будем использовать аддитивную запись, а для группы $\langle R \setminus \{0\}, *\rangle$ — мультипликативную. Напомним соответствующие системы обозначений:

	мультипликативная запись	аддитивная запись
операция	$a * b$, ab	$a + b$
единица	e, 1, id	0
обратный элемент	a^{-1}	$-a$
кратный	a^n	na
кратный обратный	a^{-n}	$-na$
применение обратного	ab^{-1}, a/b	$a - b$

Упражнение 5.1. Доказать, что $0 * a = a * 0 = 0$ для всех $a \in R$ (R — кольцо). □

Упражнение 5.1. Доказать, что $0 * a = a * 0 = 0$ для всех $a \in R$ (R — кольцо). □

Упражнение 5.2. Доказать, что множества $\mathbb{R}$, $\mathbb{C}$ с обычными операциями сложения и умножения являются полями. Указать, какие из множеств $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ являются кольцами, какие полями. □

Отметим, что если в последнем определении $\langle R \setminus \{0\}, *\rangle$ просто группа (не обязательна абелева), то соответствующая структура называется *телом*. Знаменитая теорема Веддербёрна (1903) гласит, что *каждое конечное тело является полем.* Как видим, введенная система аксиом обладает внутренней логикой, которая позволяет получать нетривиальные выводы. Далее мы, опираясь на аксиомы, исчерпывающим образом опишем строение конечных полей.

Теорема 5.1. Если p — простое, то $\mathbb{Z}_p$ — конечное поле.

Доказательство. Действительно, $\mathbb{Z}_p$ — кольцо, т. е. выполнены аксиомы 1 – 3. Дополнительно, $\langle \mathbb{Z}_p^*, *\rangle$ — абелева группа и $\mathbb{Z}_p^* = \mathbb{Z}_p \setminus \{0\}$, т. е. выполнена аксиома 4. □

Подчеркивая, что $\mathbb{Z}_p$ — поле, будем писать $\mathbb{F}_p$ вместо $\mathbb{Z}_p$.

Пример 5.1. Поле $\mathbb{F}_2$ состоит из двух элементов: 0 и 1. Правила сложения: $0 + 0 = 1 + 1 = 0$, $0 + 1 = 1 + 0 = 1$. Правила умножения: $0 \cdot 0 = 0 \cdot 1 = 1 \cdot 0 = 0$, $1 \cdot 1 = 1$. Иногда, чтобы подчеркнуть, что сложение выполняется по модулю 2 вместо $+$ пишут $\oplus$. □

6. ПОРЯДКИ НЕПРИВОДИМЫХ МНОГОЧЛЕНОВ И ЛРП

Виды многочленов [править | править код]

Примитивные многочлены [править | править код]

Определение. Порядок корней неприводимого многочлена называется показателем, к которому этот многочлен принадлежит. Неприводимый многочлен называется примитивным, если все его корни являются порождающими элементами мультипликативной группы поля[15].

Все корни примитивного многочлена имеют порядок, равный порядку мультипликативной группы расширенного поля $\mathbb{F}_Q$, то есть $Q-1$[11].

3.16 Линейные рекуррентные последовательности

Последовательность элементов $a_0, a_1, \ldots$ поля $GF(q)$, удовлетворяющих условию

$$a_{n+k} = s_{k-1}a_{n+k-1} + s_{k-2}a_{n+k-2} + \ldots + s_0 a_k, \tag{3.16.1}$$

где $s_{k-1}, s_{k-2}, \ldots, s_0$ — фиксированные элементы поля, называется ***линейной рекуррентой*** (ЛРП) k-го порядка над полем $GF(q)$. Эта последовательность вполне определяется вектором начального состояния $A_0 = (a_0, a_1, \ldots, a_{k-1})$ и коэффициентами $s_{k-1}, s_{k-2}, \ldots, s_0$.

С линейной рекуррентой можно связать матрицу

$$S = \begin{pmatrix} 0 & 0 & \ldots & 0 & s_0 \\ 1 & 0 & \ldots & 0 & s_1 \\ 0 & 1 & \ldots & 0 & s_2 \\ \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & \ldots & 1 & s_{k-1} \end{pmatrix}.$$

Рассмотрим последующие состояния ЛРП $A_1 = (a_1, a_2, \ldots, a_k)$, $A_2 = (a_2, a_3, \ldots, a_{k+1})$, ... Определение (3.16.1) теперь можно переписать в виде

$$A_i = A_{i-1}S, \quad i = 1, 2, \ldots. \tag{3.16.2}$$

Далее рассматриваются лишь ЛРП с условием $s_0 \neq 0$. В этом случае матрица S является элементом группы $GL(k, F_q)$ всех невырожденных матриц k-го порядка с элементами из поля $GF(q)$. Поскольку эта группа конечна, то матрица A имеет конечный порядок как элемент группы.

Теорема 3.16.1. *Любая линейная рекуррента при $s_0 \neq 0$ является чисто периодической последовательностью.*

Доказательство. Существует натуральное l, такое, что $A^l = E$, где E — единичная матрица. Следовательно, $A_{i+l} = A_i S^l = A_i E = A_i$. Это означает, что период ЛРП не превосходит l. ■

Линейные рекурренты можно генерировать с помощью регистров сдвига с обратной связью. Особенно просто такой регистр сдвига устроен в случае двоичного поля. Например, для рекурренты

$$a_{n+5} = a_{n+2} + a_{n+1} + a_n, \quad n = 0, 1, 2, \ldots,$$

над полем $GF(2)$ соответствующий регистр имеет вид