Московский институт электроники и математики им. А.Н. Тихонова

Кафедра информационной безопасности киберфизических систем

Москва 2024

Криптографические методы защиты информации

Сложные вычислительные задачи

Целочисленная факторизация

Задача целочисленной факторизации

- **Сложные теоретико-числовые задачи лежат в основе криптографических алгоритмов с открытым ключом.**
- Задача целочисленной факторизации:
  - для данного натурального числа n найти его факторизацию на простые множители, то есть получить представление данного числа в виде $n = p_1^{l_1} p_2^{l_2} \dots p_k^{l_k}$, где p_i — попарно различные простые числа, $l_i > 1$ — натуральные числа для $i = 1, \dots, k$.
- Известные криптосистемы:
  - криптосистема RSA;
  - криптосистема Рабина.

ρ-алгоритм Полларда

Вход: составное число n.

Выход: нетривиальный множитель d числа n.

Шаг 1. Присвоить $a \leftarrow 2$, $b \leftarrow 2$.

Шаг 2. Для $i = 1, 2, \ldots$ выполнить следующее:

Шаг 2.1. Вычислить:

$$a \leftarrow (a^2 + 1) \bmod n,$$
$$b \leftarrow (b^2 + 1) \bmod n,$$
$$b \leftarrow (b^2 + 1) \bmod n\,.$$

Шаг 2.2. Вычислить $d = \text{НОД}(a - b, n)$.

Шаг 2.3. Если $1 < d < n$, то возврат (d);

Шаг 3. Возврат («неудача»).

- Идея ρ-алгоритма Полларда состоит в том, чтобы построить такую последовательность чисел, в которой найдется два соседних числа, имеющих **одинаковый остаток** от деления на некоторый нетривиальный множитель d числа n. Тогда разность этих двух чисел будет делиться на d нацело.

ρ ⟵ Цикл по модулю d

Пример работы ρ-алгоритма Полларда

- **Вход**: $n = 5531563.$

i	a	b	d
—	2	2	—
1	5	26	1
2	26	458330	1
3	677	4072967	1
4	458330	1083392	1
5	5283976	4699821	43

- **Вход**: $n' = {}^{5531563}/_{43} = 128641.$

i	a	b	d
—	2	2	—
1	5	26	1
2	26	72407	1
3	677	85096	1
4	72407	54264	1
5	9695	68745	1
6	85096	71797	1
7	127327	100856	1
8	54264	1271	197

Дискретное логарифмирование

Задача дискретного логарифмирования

- **Сложные теоретико-числовые задачи лежат в основе криптографических алгоритмов с открытым ключом.**
- Если $G = \langle \alpha \rangle$ — конечная мультипликативная циклическая группа порядка n и $\beta \in G$, то дискретным логарифмом β относительно базы α называется единственное целое число $x = \log_\alpha \beta$, $0 \le x \le n-1$, такое, что $\beta = \alpha^x$.
- Задача дискретного логарифмирования:
  - для данной конечной циклической группы $G = \langle \alpha \rangle$, $|G| = n$, образующего α и некоторого элемента $\beta \in G$ найти целое число x, $0 \le x \le n-1$, такое, что $\alpha^x = \beta$.
- Известные криптографические алгоритмы:
  - протокол Диффи-Хеллмана;
  - криптосистема Эль-Гамаля;

Случаи задачи дискретного логарифмирования

- Обобщенная задача дискретного логарифмирования:
  - для данной конечной циклической группы $G = \langle \alpha \rangle$, $|G| = n$, образующего α и некоторого элемента $\beta \in G$ найти целое число x, $0 \leq x \leq n - 1$, такое, что $\alpha^x = \beta$.

- Задача дискретного логарифмирования:
  - для данного простого числа p, образующего элемента $\alpha \in \mathbb{Z}_p^*$ и некоторого элемента $\beta \in \mathbb{Z}_p^*$ найти целое число x, $0 \leq x \leq p - 2$, такое, что $\alpha^x \equiv \beta \pmod{p}$.

Алгоритм «малый шаг — большой шаг»

Вход: образующий α циклической группы G порядка n и $\beta \in G$.

Выход: дискретный логарифм $x = \log_\alpha \beta$.

Шаг 1. Вычислить $m = \left[\sqrt{n}\right]$, где $[\dots]$ – округление до ближайшего целого.

Шаг 2. Построить таблицу из двух строк и m столбцов, заполнить ее значениями $\left(j, \alpha^j\right)$, где $j = 0, \dots, m-1$ и упорядочить по второму значению.

Шаг 3. Вычислить α^{-m} и присвоить $\gamma \leftarrow \beta$.

Шаг 4. Для $i = 0, \dots, m-1$ выполнить следующее:

Шаг 4.1. Проверить является ли γ вторым элементом некоторого столбца построенной таблицы.

Шаг 4.2. Если $\gamma = \alpha^j$, то возврат $(x = im + j)$

Шаг 4.3. Присвоить $\gamma \leftarrow \gamma \cdot \alpha^{-m}$.

Пример выполнения алгоритма «малый шаг — большой шаг»

- **Задание**: найти $\log_5 87$ в группе $\mathbb{Z}_{137}^*$, если известно, что $\mathbb{Z}_{137}^* = \langle 5 \rangle$.
- Шаг 1. $m = \left\lceil \sqrt{136} \right\rceil = [11{,}662] = 12.$
- Шаг 2.

j	0	1	2	3	4	5	6	7	8	9	10	11
α^j	1	5	25	125	77	111	7	35	38	53	128	92

j	0	1	6	2	7	8	9	4	11	5	3	10
α^j	1	5	7	25	35	38	53	77	92	111	125	128

- Шаг 3. $\alpha^{-12} = 14, \gamma \leftarrow 87.$
- Шаг 4.

i	0	1	2	3	4	5	6	7	8	9	10	11
γ	87	122	64	74	77	—	—	—	—	—	—	—

- $x = 4 \cdot 12 + 4 = 52$

Спасибо за внимание!

Евсютин Олег Олегович
Заведующий кафедрой информационной безопасности киберфизических систем
Канд. техн. наук, доцент

+7 923 403 09 21
oevsyutin@hse.ru