RSA

Перший алгоритм кодування з відкритим ключем (Public Key Encryption, далі PKE) було запропоновано Вітфілдом Діффі та Мартіном Хелманом у Стендфордському університеті. Вони, а також незалежно від них Ральф Меркл, розробили основні його поняття у 1976 році. Перевага PKE полягає у відсутності потреби секретної передачі ключа.

PKE базується на нерозв'язності проблеми розкладу натурального числа на прості множники.

RSA схему шифрування було запропоновано у 1978 році та названо іменами трьох його винахідників: Роном Рівестом (Ron Rivest), Аді Шаміром (Adi Shamir) та Леонардом Адлеманом (Leonard Adleman). RSA належить до класу алгоритмів кодування з відкритим ключем.

У 80-х роках криптосистема переважно використовувалася для забезпечення секретності та достовірності цифрових даних. У сучасному світі RSA використовується в web – серверах та браузерах для зберігання таємності даних що передаються по мережі, .

Схема RSA базується на обчисленні виразів зі степенями. Відкритий текст шифрується блоками, довжина кожного із яких менша за деяке число n.

Алгоритм генерації ключа

A повинен згенерувати відкритий та секретний ключі:

1. Згенерувати два великих простих числа p та q приблизно однакової довжини;
2. Обчислити $n = p * q, fi = (p - 1) * (q - 1)$;
3. Вибрати натуральне e, $1 < e < fi$, взаємно просте з fi;
4. Використовуючи розширений алгоритм Евкліда, розв'язати рівняння

$$d * e \equiv 1 \pmod{fi}.$$

Відкритий ключ: (n, e). Секретний ключ: d.

Схема шифрування RSA

B шифрує повідомлення m та надсилає ***A***.

1. Шифрування. ***B*** робить наступні дії:
   а) отримати відкритий ключ (n, e) від ***A***;
   б) представити повідомлення у вигляді натурального числа m з проміжку $[1..n]$;
   в) обчислити $c = m^e \bmod n$;
   г) надіслати шифротекст c до ***A***.
2. Дешифрування. Для отримання повідомлення m із шифроткста c ***A*** робить наступні дії:
   а) використовуючи секретний ключ d, обчислити $m = c^d \bmod n$.

Теорема. Шифр с декодується правильно.

Оскільки p та q – прості числа, то $\varphi(p * q) = \varphi(n) = (p - 1) * (q - 1)$, де φ – функція Ейлера. З умови вибору ключа d маємо: $d * e \bmod \varphi(n) = 1$, або $d * e = \varphi(n) * k + 1$ для деякого натурального k.

$c^d \bmod n = (m^e)^d \bmod n = m^{(e * d)} \bmod n = m \wedge (\varphi(n) * k + 1) \bmod n = (m^{\varphi(n)} \bmod n)^k * m = 1^k * m = m$, оскільки за теоремою Ейлера $m^{\varphi(n)} \bmod n = 1$.

Означення. ***RSA системою*** називають функцію $RSA_{n,e}(x) = x^e \bmod n$ та обернену їй $RSA^{-1}_{n,e}(y) = y^d \bmod n$, де e – кодуюча, а d – декодуюча експонента, $x, y \in Z_n^*$.

Приклад

1. Оберемо два простих числа: $p = 17$, $q = 19$;
2. Обчислимо $n = 17 * 19 = 323$, $fi = (p - 1) * (q - 1) = 16 * 18 = 288$;
3. Оберемо $e = 7$ (НСД(e, fi) = 1) та розв'яжемо рівняння $7 * d \equiv 1 \pmod{288}$, звідки $d = 247$.

Побудовано RSA систему: $p = 17$, $q = 19$, $n = 323$, $e = 7$, $d = 247$.

Відкритий ключ: $n = 323$, $e = 7$, секретний ключ: $d = 247$.

1. $m = 4$. Кодування: $4^7 \bmod 323 = 234$. Декодування: $234^{247} \bmod 323 = 4$.
2. $m = 123$. Кодування: $123^7 \bmod 323 = 251$. Декодування: $251^{247} \bmod 323 = 123$.

Циклічна атака

За відомим шифром c ($c = m^e \bmod n$) злодій, маючи відкритий ключ e та n, бажає знайти повідомлення m. Він починає будувати послідовність чисел

$$c, c^e, c^{e^2}, c^{e^3}, \ldots$$

Оскільки обчислення відбуваються в групі Z_n^*, то елемпнти послідовності знаходяться в межах від 0 до n - 1. Отже існує таке натуральне k, що $c = c^{e^k}$. Враховуючи що $c = m^e \bmod n$, маємо: $m^e = c^{e^k}$ або $m = c^{e^{k-1}}$.

Таким чином для знаходження повідомлення m за його шифром c необхідно побудувати послідовність $c, c^e, c^{e^2}, c^{e^3}, \ldots, c^{e^{k-1}}, c^{e^k} = c$, і взяти її передостаннє число.

Приклад

Розв'язати рівняння: $m^7 \bmod 323 = 251$.

$e = 7$, $n = 323$, $c = 251$.

k	c^{e^k}
0	251

1	310
2	47
3	4
4	234
5	123
6	251

З таблиці маємо: $c = c^{e^6} = 251$. Оскільки $m^e = c^{e^6}$, то $m = c^{e^5} = 123$.

Атака методом осліплення

Припустимо, ***A*** має секретний ключ RSA системи, а ***Z*** – злодій, який перехопив шифр c і хоче декодувати його. При цьому ***A*** відмовляє видати ***Z*** вихідний текст m. Тоді ***Z*** обирає деяке значення $b \in Z_n^*$, обчислює $c' = b^e * c$ і просить ***A*** дешифрувати його. ***A*** погоджується дешифрувати c' своїм секретним ключем d, оскільки зміст повідомлення c' йому ні про що не говорить і виглядає невинним. Отримавши $m' = c'^d \bmod n$, злодій ***Z*** обчислює $m = m' / b$ і отримує шукане m. Шифром m дійсно є c, оскільки $m^e = m'^e / b^e = c'^{de} / b^e = c' / b^e = c$.

Така атака можлива, оскільки ***A*** не знає повної інформації про шифр c', який дає йому злодій ***Z***.

Приклад. Нехай ***A*** має RSA систему: $p = 17$, $q = 19$, $n = 323$, $e = 7$, $d = 247$.

Злодій ***Z*** перехопив шифр $c = 234$ і хоче знайти таке m, що $m^7 = 234 \bmod 323$.

1. ***Z*** обирає $b = 10 \in Z_{323}^*$, обчислює $c' = 10^7 * 234 \bmod 323 = 14$ і просить ***A*** дешифрувати його.

2. ***A*** обчислює $m' = 14^{247} \bmod 323 = 40$ і передає його ***Z***.

3. ***Z*** знаходить шукане повідомлення обчислюючи

$$m = 40 / 10 = 40 * 10^{-1} = 40 * 97 = 4 \bmod 323.$$

Таким чином $4^7 = 234 \bmod 323$.

Прискорення дешифрування

За допомогою китайської теореми про лишки можна прискорити процес дешифрування, знаючи секретні прості числа p та q.

Алгоритм

Дешифрування. ***A*** має декодуючу експоненту d, а також p та q ($n = p * q$). ***A*** отримує від ***B*** шифр c та повинен виконати операцію $c^d \pmod n$.

1. Обчислити $d_p = d \bmod (p - 1)$, $d_q = d \bmod (q - 1)$
2. Обчислити $m_p = c^{d_p} \bmod p$, $m_q = c^{d_q} \bmod q$.
3. Розв'язати систему лінійних порівнянь

$$\begin{cases} m \equiv m_p \pmod p \\ m = m_q \pmod q \end{cases}$$

Розв'язком системи буде декодоване повідомлення: $m = c^d \pmod n$.

Приклад

Нехай RSA система має вигляд: $p = 17$, $q = 19$, $n = 323$, $e = 7$, $d = 247$.

Для розв'язку рівняння $m^7 \bmod 323 = 251$ ($c = 251$) обчислимо $251^{247} \bmod 323$:

1. $d_p = 247 \bmod 16 = 7$, $d_q = 247 \bmod 18 = 13$;
2., $m_p = 251^7 \bmod 17 = 4$, $m_q = 251^{13} \bmod 19 = 9$;
3. Розв'яжемо систему лінійних порівнянь

$$\begin{cases} m \equiv 4 \pmod{17} \\ m = 9 \pmod{19} \end{cases}$$

Розв'язуючи її методом Гауса, отримаємо m = 123.

Отже $123^7 \bmod 323 = 251$.

Мала декодуюча експонента

Приклад. Виберемо аовідомлення $m = 13$ та зашифруємо його трьома різними RSA системами.

1. $p = 5$, $q = 17$, $n = 85$, $e = 3$, $d = 57$,
   $m^3 \bmod 85 = 72$;
2. $p = 11$, $q = 23$, $n = 253$, $e = 3$, $d = 169$,
   $m^3 \bmod 253 = 173$;
3. $p = 17$, $q = 23$, $n = 391$, $e = 3$, $d = 261$,
   $m^3 \bmod 391 = 242$;

Для знаходження повідомлення m за відкритими ключами (n_i, e_i) та перехопленими шифрами c_i складемо систему порівнянь

$$\begin{cases} x \equiv 72 \pmod{85} \\ x \equiv 173 \pmod{253} \\ x \equiv 242 \pmod{331} \end{cases}$$

Одним із її розв'язків буде $x = 2197 = 13^3$. Тобто шуканим повідомленням буде $m = 13$.

Неприховані повідомлення

Означення. Повідомлення m називається *неприхованим*, якщо його шифр дорівнює самому повідомленню, тобто $m^e = m \pmod n$.

Наприклад, повідомлення $m = 0$ та $m = 1$ завжди є неприхованими для довільних значень e та m.

Твердження. Кількість неприхованих повідомлень в RSA системі дорівнює
$$(1 + \text{НСД}(e - 1, p - 1)) * (1 + \text{НСД}(e - 1, q - 1))$$

Оскільки значення $e - 1$, $p - 1$ та $q - 1$ – парні, то $\text{НСД}(e - 1, p - 1) \geq 2$, $\text{НСД}(e - 1, q - 1) \geq 2$, а отже кількість неприхованих повідомлень завжди не менша за 9.