

Асиметрична криптографія



Проблеми симетричної криптографії

- Проблема розповсюдження криптографічних ключів;
- Проблема зберігання ключів;
- Велика кількість ключів для розгалуженої криптосистеми: $K = N(N-1)/2$.

=====

- Чи можна подолати такі недоліки?
- Чи можна розробити таку криптосистему, де зашифровують одним ключем, а розшифровують – іншим?

«Механічна» аналогія

- Нехай ми живемо в країні, де спецслужби на пошті читають усі листи, якщо можуть зробити це непомітно.
- Якщо не можуть непомітно читати його.
- Щоби не прочитали наї кладемо його в скриньку замок.



«Механічна» аналогія

- Спецслужби не можуть відкрити замок без ключа.
- Адресат також не може відкрити замок без ключа – треба якось передати йому ключ.
- Передавати не хочеться – можуть перехопити спецслужби.
 - Як зробити так, щоби **скринька закривалася одним ключем, а відкривалася іншим?**

«Механічна» аналогія

- **Відповідь:**

- Зачинити скриньку на замок і відправити отримувачу;
- Отримувач навішує ще один замок і відправляє відправнику;
- Відправник відчиняє свій замок і відправляє скриньку отримувачу;
- Отримувач відчиняє скриньку і читає листа.

=====

Отже, принципово можна зачинити скриньку одним ключем, а відчинити – іншим.

Асиметрична криптографія

- 1976 рік. Біллі Німфілд та Мартін Гарман опублікували статтю «Нові алгоритми для розподілу ключів».
- У 1978 році було запропоновано абстрактну схему шифрування на основі «односторонніх» функцій.
- Односторонні функції – такі функції, які в прямому напрямку обчислюються легко, а для знаходження оберненої функції треба розв'язати задачу надзвичайної обчислювальної складності.



Асиметрична криптографія

- Приклади односторонніх функцій:
- $y = pq$ - перемножити два великих простих числа легко, а розкласти велике число на прості множники – складна задача, складність якої зростає експоненційно зі зростанням розрядності числа.
- $y = a^x \bmod n$ – в прямому напрямі обчислюється легко, а знаходження x нашо́вхується на дуже складну задачу дискретного логарифмування:
 $x = (\log_a y) \bmod n.$

Особливості систем АК

- Суб'єкт інформаційного обміну генерує два ключі: **приватний** і **публічний**.
- Приватний ключ використовується для розшифрування інформації. Він не розповсюджується, а зберігається в таємниці у власника.
- Публічний ключ використовується для зашифрування інформації. Розшифрувати за його допомогою зашифровану інформацію неможливо (в усякому разі, дуже складно). Публічний ключ розміщується на публічному ресурсі і доступний для усіх.

Особливості систем АК

- Перетворення відкритого тексту повинно бути незворотним без можливості його відновлення на публічному ключі;
- Обчислення приватного ключа на основі публічного також повинно бути неможливим на сучасному технологічному рівні. При цьому бажаною є точна нижня оцінка трудомісткості розкриття шифру.

Використання АК

- Як самостійних засобів захисту інформації;
- Як засобів аутентифікації користувачів;
- Як засоби розповсюдження криптографічних ключів у складі комбінованих криптосистем.

=====

Недоліки АК:

- Мала швидкість (приблизно в 1000 разів) порівняно з симетричними системами;
- Математично не доведено, що не існує простого способу отримання приватного ключа з публічного. Стійкість АК ґрунтується, в принципі, на багаторічному практичному досвіді

Елементи теорії чисел

- Функція Ейлера: $\varphi(n)$ визначає кількість цілих чисел, взаємно простих з n множини $[1, n-1]$.
- Доведено (теорема Ейлера), що якщо n – просте число, то $\varphi(n) = n-1$. Продемонструємо це для множини $[1, 11]$:

n	2	3	4	5	6	7	8	9	10	11
$\varphi(n)$	1	2	2	4	2	6	4	6	4	10

Елементи теорії чисел

- Мала теорема Ферма: Якщо n - просте число то $(x^{n-1} \bmod n) = 1$ для будь-яких x , взаємно простих з n .
- Теорема 2. Нехай число n – просте. Для будь-якого A та $1 \leq B \leq (n-1)$ знайдеться таке $1 \leq X \leq (n-1)$, що $A^X \bmod n = B$. Іншими словами, стверджується, що функція $A^x \bmod n = B$ однозначна на проміжку $0 \dots n-1$.

Приклад

Розглянемо функцію: $y = a^x \bmod 7$



a\х	0	1	2	3	4	5	6
0							
1		1	1	1	1	1	1
2		2	4	1	2	4	1
3		3	2	6	4	5	1
4		4	2	1	4	2	1
5		5	4	6	2	3	1
6		6	1	6	1	6	1



Приклад

- Значення a , для яких встановлюється однозначна залежність, називаються ***первісними коренями*** за модулем 7.
- Такі корені саме й використовують для створення криптосистем.

Криптосистема RSA



Автори RSA



Рон Рівест
Ron **R**ivest



Аді Шамір
Adi **S**hamir



Леон Аделман
Leon **A**ddleman

Криптостійкість RSA ґрунтується на задачі розкладання великого цілого числа на прості множники – задачі факторизації великих чисел.

Криптосистема RSA

- Для того, щоби розгорнути криптосистему RSA, необхідно виконати такі кроки:
- Крок 1. Обираються два цілих числа, p і q , з таким розрахунком, щоби їхній добуток був величини 1024 біти. Тим чи іншим методом перевіряємо, чи обрані числа прості.
- Для цього використовують тести простоти:
 - Решето Ератосфена;
 - Тест Міллера;
 - Вихор Мерсенна;
 - Теорем Вільсона та ін.
- Обчислюємо добуток $n=p \times q$. n – модуль криптосистеми.

Криптосистема RSA

- Крок 2. З числа первісних коренів за модулем криптосистеми обираємо один, який буде публічним ключем криптосистеми.
- Первісний корінь шукати не обов'язково: достатньо, щоби для обраного публічного ключа e виконувалося: $\text{НСД}(e, n)=1$.
- Пара чисел (e, n) буде **публічним ключем** криптосистеми.
- Публічний ключ розміщується на доступному для усіх ресурсі.

Криптосистема RSA

- Публічний ключ використовується для шифрування інформації.
- Його неможливо (в усякому разі, обчислювально складно) використати для розшифрування зашифрованої інформації.

=====

Таким чином, кожен, хто бажає зашифрувати інформацію, може взяти з ресурсу ключ та виконати процес шифрування.

Криптосистема RSA

- Крок 3. Обчислюємо приватний ключ d . Для цього необхідно розв'язати рівняння: $(d \times e) \bmod n = 1$.
- Для цього використовують метод Евкліда розв'язку рівняння Діофанта.
- Для малих чисел можна використати просту формулу:
$$d = \frac{1+k\varphi(n)}{e} = \frac{1+k(p-1)(q-1)}{e}, \text{ де } k = 1, 2, 3 \dots - \text{ціле число, а } \varphi(n) = \varphi(pq) = \varphi(p)\varphi(q) = (p-1)(q-1).$$
- Практично це підбирання приватного ключа.

Криптосистема RSA

- Число (d, n) називається **приватним ключем** криптосистеми.
- Приватний ключ не розповсюджується, а зберігається у його власника в таємниці.
- Приватний ключ використовується для розшифрування інформації, зашифрованої на парному йому публічному ключі.
- Для іншого публічного ключа цей приватний ключ не підходить.
- Криптосистема RSA симетрична відносно використання ключів: можна шифрувати публічним і розшифровувати приватним, і **навпаки**.

Криптосистема RSA

- Публічний ключ ще називається:
 - Public key;
 - Открытый ключ.
- Приватний ключ ще називається:
 - Private key;
 - Закрытый ключ;
 - Секретный ключ.

Криптосистема RSA

- Крок 4. Шифрування інформації:

- Шифруються десяткові числа з діапазону $[1, n-1]$, наприклад, коди літер алфавіту (або груп літер, якщо використовуються великі числа).
- Шифрування виконується в такий спосіб:

$$C_i = (M_i)^e \bmod n$$

- Результат шифрування відправляється у канал зв'язку.
- Крок 5. Розшифрування інформації.

$$M_i = (C_i)^d \bmod n$$

Криптосистема RSA


- Доведемо, що в результаті ми отримаємо розшифроване повідомлення:

$$(C_i)^d \bmod n = ((M_i)^e)^d \bmod n = (M_i)^{ed} \bmod n = M_i$$

оскільки $ed \bmod n = 1$.

Таким чином, пряме та обернене перетворення еквівалентні.

Приклад RSA

- Розглянемо простий приклад:
- Нехай $p=11$; $q=7$  $n=77$ – модуль криптосистеми;
- Знаходимо публічний ключ: $e=13$;
- НСД $(e, n) = 1$, тобто e, n – взаємно прості числа.
- Таким чином, публічний ключ буде $(13, 77)$.
- Тепер треба обчислити приватний ключ:
- $(d \times e) \bmod n = 1$:
- $$d = \frac{1+k\varphi(n)}{e} = \frac{1+k\varphi(pq)}{e} = \frac{1+k\varphi(p)\varphi(q)}{e} =$$
$$\frac{1+k(p-1)(q-1)}{e} = \frac{1+k \times 10 \times 6}{13} = \frac{1+k \times 60}{13};$$

Приклад RSA

- Для $k=8$ отримаємо:

- $d = \frac{1+8 \times 60}{13} = \frac{481}{13} = 37.$

- Таким чином, приватний ключ – $(37, 77).$

- =====

Шифруються десяткові числа з діапазону $[1, n-1]$, тобто від 1 до 76.

Приклад RSA

А	Б	В	Г	Д	Е	Є	Ж	З	И	І	Ї	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ю	Я
1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2

Оскільки ми маємо дуже маленькі числа, ми будемо шифрувати літери по одній.

Зашифруємо слово «БАНК». Замінімо літери за цією таблицею заміни:

02 01 17 14.

Шифруємо публічним ключем:

$$C_1 = 2^{13} \bmod 77 = 30;$$

$$C_2 = 1^{13} \bmod 77 = 01;$$

$$C_3 = 17^{13} \bmod 77 = 73;$$

$$C_4 = 14^{13} \bmod 77 = 49;$$

Послідовність 30 01 73 49 – в канал зв'язку.

Приклад RSA

А	Б	В	Г	Д	Е	Є	Ж	З	И	І	Ї	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ю	Я
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32

Отримали з каналу зв'язку послідовність: 30 01 73 49:

Розшифровуємо за допомогою приватного ключа:

$$M_1 = 30^{37} \bmod 77 = 02;$$

$$M_2 = 1^{37} \bmod 77 = 01;$$

$$M_3 = 73^{37} \bmod 77 = 17;$$

$$M_4 = 49^{37} \bmod 77 = 14;$$

Замінюємо числа на літери за таблицею замін, будемо мати «БАНК».

Алгоритм RSA

- З наведеного прикладу видно недоліки запропонованої схеми: числа 00, 01 та 76 не шифруються. Тому для покращення стійкості необхідно зменшити діапазон до $[2, n-2]$.

=====

Криптосистема Ель Гамала

- Криптосистема Ель Гамала була розроблена у 1985 році.
- В основі криптостійкості лежить задача дискретного логарифмування:
- $y = a^x \bmod n \longrightarrow x = (\log_a y) \bmod n$.
- Ця задача вважається складнішою за задачу факторизації, яка використовується в криптосистемі RSA.
- Для того, щоби розгорнути криптосистему Ель Гамала, необхідно зробити таке.

Криптосистема Ель Гамала

- Крок 1. Підготовчі обчислення.
 - За допомогою криптостійкого генератора випадкових чисел генеруємо модуль криптосистеми, n порядку 1024 біти.
 - Генеруємо випадкові числа g та a з діапазону $[1, n-1]$ порядку 160 бітів.
 - Обчислюємо число $h = g^a \bmod n$.
 - (n, g, h) – публічний ключ;
 - (n, a) – приватний ключ.

Криптосистема Ель Гамала

- Крок 2. Шифрування інформації.
Шифруються числа від 0 до $n-1$. Нехай m – відкрите повідомлення. Тоді:
 - Генерується сеансовий ключ g з діапазону $1- n-1$
 - Обчислюються два числа: $C_1 = g^r \bmod n$, $C_2 = mh^r \bmod n$.
 - C_1 та C_2 будуть зашифрованим повідомленням: (C_1, C_2) .

Криптосистема Ель Гамала

- Крок 3. Розшифрування інформації.
 - Розшифрування інформації виконується за наступною формулою: $m = C_2(C_1^a)^{-1} \bmod n$.
 - Доведемо, що пряме та обернене перетворення еквівалентні.
 - Підставимо значення C_1 та C_2 :
 - $m = C_2(C_1^a)^{-1} \bmod n = mh^r(g^{ra})^{-1} \bmod n = mh^r(g^{ar})^{-1} \bmod n = mh^r(h)^{-r} = m$.
 - Отже, операції шифрування та розшифрування взаємно обернені.

Приклад КС Ель Гамаля

- Розглянемо простий приклад:
- Нехай $n=29$, $g=2$, $a=5$.
- Обчислимо $h=2^5 \bmod 29 = 3$.
- Тоді публічний ключ – $(29, 2, 3)$, приватний – $(29, 5)$.
- Нехай повідомлення $m=11$. Тоді:
- Генеруємо сеансовий ключ: $r=8$.
- Обчислюємо: $C_1=2^8 \bmod 29= 24$; $C_2=11(3^8) \bmod 29 = 19$. Отже зашифроване повідомлення буде $(24, 19)$.

Приклад КС Ель Гамаля

- Розшифровування:
- $C_2(C_1^a) \bmod 29 = 19(24^5)^{-1} \bmod 29 = 11.$