2.10 Системи обміну ключами

Познайомившись з основними теоретико-числовими та алгебраїчними поняттями, розглянемо алгоритми обміну інформацією між абонентами, які ґрунтуються на властивостях чисел, груп, кілець і полів. Перш за все, розглянемо розв'язання проблеми обміну таємними ключами між абонентами.

Розглянемо три алгоритми, які розв'язують цю проблему і вважаються безпечними. Це алгоритми Діффі-Хелмана, Шаміра та Ель-Ґамаля [23], які були побудовані в середині 70-х років і ці алгоритми в певному сенсі призвели до революції в криптографії. Алгоритми ґрунтуються на властивості дискретного логарифму, який є

прикладом *односторонньої функції* (див. підрозділ 2.3.5, приклади NPC-проблем).

Функція дискретного алгоритму діє в полі F_q і має вигляд $y = g^x \pmod q$, де $q = p^n$, p – деяке просте число, а x – ціле число з множини $\{1, 2, \ldots, q-1\}$. Обернена функція має вигляд $x = \log_g y \pmod q$ і називається *дискретним логарифмом*. Далі для простоти будемо розглядати поле F_p, тобто коли $n = 1$. Для забезпечення складності обчислення числа x за умови використання кращих комп'ютерів в даний час використовуються числа, які мають розміри не менше 1024 біт.

Покажемо, що обчислення значення y виконується досить швидко на наприкладі обчислення числа $g^{16} \pmod p$. Запишемо цей вираз таким чином: $g^{16} \pmod p = (((g^2)^2)^2)^2 \pmod p$, звідки бачимо, що обчислення значення даної функції виконується всього за 4 операції множення. А при послідовному обчисленні для цього потрібно було б виконати 15 таких операцій.

Розглянемо детальніше алгоритм обчислення числа y. Для цього введемо величину $t = \lfloor \log_2 x \rfloor$ – цілу частину $\log_2 x$ і обчислимо числа ряду

$$g,\ g^2,\ g^4,\ g^8, \ldots, g^{2^t} \pmod p. \tag{2.51}$$

В цьому ряду кожне число знаходиться шляхом множення попереднього числа на самого себе за модулем p. Запишемо показник степеня x у вигляді двійкового числа: $x = (x_t x_{t-1} \ldots x_1 x_0)$. Тоді число

$$y = \prod_{i=0}^{t} [g^{x_i 2^i} \pmod p]. \tag{2.52}$$

Наприклад, якщо потрібно обчислити число $3^{100} \pmod 7$, то знаходимо $t = \lfloor \log_2 100 \rfloor = 6$. Обчислюємо числа ряду (2.51):

g	g^2	g^4	g^8	g^{16}	g^{32}	g^{64}
3	2	4	2	4	2	4

Двійкове число для показника має вигляд: $100_2 = 1100100$ і, виконуючи обчислення за формулою (2.52), дістаємо

g^{64}	g^{32}			g^4			
4	2	1	1	4	1	1	$= 4.$

Для цього обчислення знадобилося лише 8 операцій множення (6 операцій для обчислення елементів першого ряду та 2 операції для обчислення елементів другого ряду).

Часову характеристику складності обчислення $y = g^x \ (mod\ p)$ дає

Твердження 7. *Кількість операцій множення, необхідних для обчислення значення $y = g^x \ (mod\ p)$ описаним методом, не перевищує $2\log_2 x$.*

Доведення. Для обчислення чисел ряду (2.52) потрібно t множень, для обчислення значення y за наведеною формулою теж потрібно не більше t множень. Оскільки $t = \lfloor \log_2 x \rfloor < \log_2 x$, то вказана оцінка справедлива. ■

Для обчислення значень оберненої функції дискретного логарифму невідомі ефективні алгоритми. Одним із методів обчислення її значень є метод "крок немовляти, крок гіганта", який буде описаний далі. Цей метод потребує $2\sqrt{p}$ операцій множення і нижче в таблиці показані деякі результати таких підрахунків. Звідси можна зробити висновок, що при великих значеннях числа p функція дискретного логарифму дійсно буде односторонньою, якщо для її обчислення використовується метод "крок немовляти, крок гіганта".

Кількість десяткових знаків числа p	Обчислення y ($2\log p$ множ.)	Обчислення x ($2\sqrt{p}$ множ.)
12	$2 \cdot 40 = 80$	$2 \cdot 10^6$
60	$2 \cdot 200 = 400$	$2 \cdot 10^{30}$
90	$2 \cdot 300 = 600$	$2 \cdot 10^{45}$

Нехай суперкомп'ютер виконує множення двох 90-розрядних чисел в часі 10^{-14} секунд (для сучаних комп'ютерів цей час не досяжний). Тоді для обчислення y такому комп'ютеру потрібен час $600 \cdot 10^{-14} = 6 \cdot 10^{-12}$ секунд, а для обчислення значення x – час $10^{45} \cdot 10^{-14} = 10^{31}$ секунд.

2.10.1 Протокол обміну ключами Діффі-Хелмана

Спочатку в цьому протоколі всі учасники домовляються про те, яке буде використовуватися поле F_q і породжуючий елемент $1 < g < p - 1$ його мультиплікативної групи. Нехай вибране поле F_p, де p – велике просте число (про спосіб вибору елементів p і g буде сказано нижче):

$$g \ (mod\ p),\ g^2 \ (mod\ p),\ \ldots,\ g^{p-1} \ (mod\ p).$$

Числа p і g відомі всім абонентам.

ПРОТОКОЛ ОБМІНУ КЛЮЧАМИ ДІФФІ-ХЕЛМАНА

Вхід: пара (p, g), де p – велике просте число, а g – породжуючий елемент групи поля F_p $(1 < g < p-1)$;.

Вихід: елемент групи k, яким необхідно обмінятися абонентам A і B.

1. A генерує елемент $a \in [1, p-1)$, обчислює число $g_a = g^a \ (mod\ p)$ і висилає його абоненту B.

2. B генерує елемент $b \in [1, p-1)$, обчислює число $g_b = g^b \ (mod\ p)$ і висилає його абоненту A.

3. A обчислює число $k = g_b^a \ (mod\ p)$.

4. B обчислює число $k = g_a^b \ (mod\ p)$.

Таким чином обмін ключем k між абонентами A і B відбувся.

Розглянемо роботу цього протоколу на прикладі обміну ключем між трьома абонентами A, B, C. Абоненти A, B, C вибирають великі приватні (таємні) числа X_A, X_B, X_C, в той час як числа p, g відомі всім абонентам A, B, C. Кожний абонент обчислює число Y_X, яке висилає всім абонентам. Число Y_X обчислюється таким чином:

$Y_A = g^{X_A} \ (mod\ p)$, $Y_B = g^{X_B} \ (mod\ p)$, $Y_C = g^{X_C} \ (mod\ p)$.

Звідси дістаємо таку таблицю:

Абонент	Ключ приватний	Ключ відкритий
A	X_A	Y_A
B	X_B	Y_B
C	X_C	Y_C

Нехай A хоче передати B повідомлення. Для цього він висилає до B ключ Y_A, за допомогою якого шифрується повідомлення.

Оскільки інформація про p і g відома всім абонентам, то A висилає до B відкритим каналом інформацію про те, що він хоче вислати повідомлення. Потім A обчислює число $Z_{AB} = (Y_B)^{X_A} \ (mod\ p)$.

Жодна особа, крім A, такого обчислення не може виконати, оскільки X_A є ключем приватним.

Абонент B обчислює число $Z_{BA} = (Y_A)^{X_B} \ (mod\ p)$.

Обґрунтування такого способу дає

Теорема 66. $Z_{AB} = Z_{BA}$.

Доведення. На підставі властивостей мультиплікативної групи поля F_p, отримуємо

$Z_{AB} = (Y_B)^{X_A} \ (mod\ p) = (g^{X_B})^{X_A} \ (mod\ p) = (g^{X_A})^{X_B} \ (mod\ p) =$
$= (Y_A)^{X_B} \ (mod\ p) = Z_{BA}$. ■

Основні властивості протоколу Діффі-Хелмана:

– A і B отримали одне і те саме число $Z = Z_{AB} = Z_{BA}$;

– особі небажаній числа X_A і X_B не відомі і вона не має можливості обчислити число Z (принаймні за розумний відрізок часу).

Вибір елемента g. Як було сказано, стійкість протоколу Діффі-Хелмана до зламання ґрунтується на складності функції дискретного логарифму. Аби ця стійкість була високою, належить вибирати просте число p таким, щоб число $p-1$ мало великий простий дільник p' (великий означає $p' > 2^{160}$). Вибір числа p можна виконати так:

$$p = 2r + 1 \text{ або } p - 1 = 2r.$$

де r теж просте число. Якщо число p вибране таким чином, то елемент g може бути довільним елементом, що задовольняє нерівності: $1 < g < p-1$ і $g^r \not\equiv 1 \ (mod\ p)$. Елемент g не обов'язково повинен бути породжуючим елементом всієї мультиплікативної групи поля F_q. Необхідно тільки, щоб він був породжуючим її підгрупи, порядок якої великий, наприклад, p'.

Приклад 2.10.1. Нехай $p = 23 = 2 \cdot 11 + 1$, тобто $r = 11$. Вибираємо g. Якщо $g = 3$, то $3^{11} \equiv 1 \ (mod\ 23)$ і тоді $g = 3$ не задовольняє умові вибору. Нехай $g = 5$, тоді $5^{11} \equiv 22 \ (mod\ 23)$ і тому $g = 5$ є шуканим елементом.

Тепер кожний абонент обчислює приватний ключ. Припустимо, що були вибрані числа $X_A = 7, X_B = 13$. Обчислюємо

$Y_A = 5^7 \ (mod\ 23) = 17$, $Y_B = 5^{13} \ (mod\ 23) = 21$.

Якщо A і B вирішили згенерувати спільний ключ, то A обчислює

$$Z_{AB} = (Y_B)^{X_A} \ (mod\ p) = (21)^7 \ (mod\ 23) = 10,$$

а B обчислює

$$Z_{BA} = (Y_A)^{X_B} \ (mod\ p) = (17)^{13} \ (mod\ 23) = 10.$$

Отже, A і B мають спільний ключ, який не передавався відкритими каналами. ♠

2.10.2 Шифр Шаміра

Цей шифр був першим шифром, який давав можливість обмінюватися повідомленнями відкритими лініями зв'язку для абонентів, які не мають ніяких захищених каналів і секретних ключів і, можливо, ніколи не бачилися. Описана вище система Діффі-Хеллмана дає можливість лише сформувати секретне слово, а передача повідомлення потребує певного шифру, в якому це секретне слово діятиме як ключ.

Шифр Шаміра має такий вигляд. Нехай два абоненти A і B зв'язані між собою лінією зв'язку. A хоче передати повідомлення m абоненту B так, щоб його ніхто не зміг прочитати. A вибирає випадково велике просте число p і відкрито передає його B. Потім A вибирає два числа c_A і d_A такі, що

$$c_A \cdot d_A \equiv 1 \ (mod \ (p-1)). \tag{2.53}$$

Ці числа A тримає в секреті і нікому їх не передає. B теж вибирає два числа c_B і d_B такі, що

$$c_B \cdot d_B \equiv 1 \ (mod \ (p-1)). \tag{2.54}$$

і теж тримає їх в секреті.

Після цього A передає своє повідомлення m, використовуючи триступеневий протокол. Якщо $m < p$ (m розглядається як число), то повідомлення m передається відразу, а якщо $m \geq p$, то повідомлення подається у вигляді блоків $m_1, m_2, \ldots, m_t$, де всі $m_i < p$, а далі передаються послідовно $m_1, m_2, \ldots, m_t$. При цьому для кодування кожного m_i краще вибирати випадково нові пари (c_A, d_A) і (c_B, d_B). В протилежному випадку стійкість системи знижується. Отже, основним є випадок $m < p$, який розглянемо детальніше. Протокол обміну в шифрі є таким:

крок 1. A обчислює число $x_1 \equiv m^{c_A} \ (mod \ p)$, де m початкове повідомлення і передає його B.

крок 2. B, отримавши x_1, обчислює число

$$x_2 \equiv x_1^{c_B} \ (mod \ p) \tag{2.55}$$

і передає його A.

крок 3. A обчислює число $x_3 \equiv x_2^{d_A} \ (mod \ p)$ і передає його B.

крок 4. B, отримавши x_3, обчислює число

$$x_4 \equiv x_3^{d_B} \ (mod \ p). \tag{2.56}$$

Теорема 67 (про властивість протоколу Шаміра).

a) $x_4 = m$, тобто дійсно B отримав від A початкове повідомлення.

b) зловмисник не може прочитати передане повідомлення.

Доведення. *a*) Відомо, що довільне число $e \geq 0$ можна подати у вигляді $e = k(p-1)+r$, де $r \equiv e \ (mod\ (p-1))$. Тоді на підставі малої теореми Ферма дістаємо

$$x^e \ (mod\, p) = x^{k(p-1)+r} \ (mod\, p) = (1^k x^r) \ (mod\, p) = x^{e \ (mod\ (p-1))} \ (mod\, p). \quad (2.57)$$

Тепер справедливість пункту *a*) випливає з такої послідовності рівностей:

$$\begin{aligned} x_4 \equiv x_3^{d_B} \ (mod\ p) = (x_2^{d_A})^{d_B} \ (mod\ p) = (x_1^{c_B})^{d_A d_B} \ (mod\ p) = \\ = (m^{c_A})^{c_B d_A d_B} \ (mod\ p) = m^{c_A c_B d_A d_B} \ (mod\ p) = \\ = m^{(c_A c_B d_A d_B) \ (mod\ (p-1))} \ (mod\ p) = m. \end{aligned}$$

Передостання рівність випливає із (2.57), а остання – із (2.53) і (2.54).

b) Доведення ґрунтується на припущенні, що для зловмисника, який намагається прочитати m, не існує ефективнішої стратегії, ніж наступна стратегія. Спочатку він знаходить число c_B із (2.55), потім число d_B і, нарешті, обчислює $x_4 = m$ за формулою (2.56). Але для реалізації цієї стратегії зловмисник мусить розв'язати задачу дискретного логарифма (2.55), що практично неможливо зробити при великому значенні p. ■

Метод вибору чисел c_A і d_A, які задовольняють (2.53) і (2.54), опишемо тільки для дій абонента A, оскільки дії абонента B аналогічні.

Число c_A вибирається випадково так, щоб воно було взаємно простим з числом $p-1$ (шукати потрібно серед непарних чисел, оскільки число $p-1$ парне). Потім обчислюється число d_A за допомогою узагальненого алгоритму Евкліда, який був наведений вище.

Приклад 2.10.2. Нехай A хоче передати B повідомлення $m = 10$. A вибирає числа $p = 23$, $c_A = 7$ (НСД(7,22) = 1) і обчислює $d_A = 19$ ($7 \cdot d_A \equiv 1 \ (mod\ 22)$, звідки $d_A = 19$).

Аналогічно B вибирає число $c_B = 5$ (яке взаємно просте з числом 22) і число $d_B = 9$ ($5 \cdot d_B \equiv 1 \ (mod\ 22)$, звідки $d_B = 9$).

Реалізується протокол Шаміра:

крок 1. $x_1 \equiv 10^7 \ (mod\ 23) = 14$.

крок 2. $x_2 \equiv 14^5 \ (mod\ 23) = 15$.

крок 3. $x_3 \equiv 15^9 \ (mod\ 23) = 19$.

крок 4. $x_4 \equiv 19^9 \ (mod\ 23) = 10$.

Таким чином, B отримав повідомлення $m = 10$. ♠

2.10.3 Протокол обміну ключами Ель-Ґамаля

Нехай абоненти A, B, C хочуть обмінюватися між собою повідомленнями через відкритий канал зв'язку. Такий обмін можна виконувати за допомогою протоколу, запропонованого Ель-Ґамалем, який дає можливість передавати повідомлення за допомогою лише одного пересилання.

Для абонентів A, B, C вибирається велике просте число p і число g (число g вибирається так як в протоколі Діффі-Хелмана). Числа p і g висилаються всім абонентам. Після отримання цих чисел кожен абонент вибирає приватне число c_i, $1 < c_i < p-1$, і обчислює число $d_i = g^{c_i} \ mod \ p$. Результати обчислень наведені в таблиці:

Абонент	Ключ приватний	Ключ відкритий
A	c_A	d_A
B	c_B	d_B
C	c_C	d_C

Покажемо як абонент A передає повідомлення m абоненту B. Припустимо, що $m < p$ (якщо $m < p$, то повідомлення передається зразу, а коли $m > p$, то m ділиться на частини $m = m_1, m_2, \ldots, m_k$, де $m_i < p$ – прості числа ($i = 1, 2, \ldots, k$) і висилається кожна з частин з власними c_i і d_i). Реалізація такого способу виконується наступним чином:

крок 1. Абонент A вибирає довільним чином число k, $1 \leq k < p-2$, обчислює числа $r = g^k \ (mod \ p)$, $e = m \cdot d_B^k \ (mod \ p)$ і пересилає пару (r, e) абоненту B.

крок 2. Абонент B, отримавши пару (r, e), обчислює число $m' = e \cdot r^{p-1-c_B} \ (mod \ p)$.

Теорема 68. *a)* $m = m'$;

b) особа небажана знаючи числа p, g, d_B *і е не може обчислити* m *(принаймні за розумний проміжок часу).*

Доведення. a) $m' = m(g_B^c)^k (g^k)^{p-1-c_B} (mod \ p) = m g^{k(p-1)} (mod \ p)$. На підставі теореми Ферма $g^{k(p-1)} \ (mod \ p) = 1^k = 1$. Звідси випливає, що $m' = m \cdot g^{k(p-1)} \ (mod \ p) = m$.

b) Зловмисник не може обчислити k для виразу $r = g^k \ (mod \ p)$, оскільки це функція дискретного логарифму. Отже, він не має змоги обчислити m, оскільки число m множилося на невідоме цій особі число. Крім того, він не має змоги виконати дії абонента

B, тому що не знає числа c_B (обчислення c_B теж є проблемою обчислення дискретного логарифму). ■

Приклад 2.10.3. Нехай $m = 15$ висилається абонентом A до B. Вибираємо $p = 23$ і $g = 5$ (так само як в попередньому прикладі). Нехай абонент B вибрав число $c_B = 13$ і обчислив $d_B = 5^{13} \ (mod\ 23) = 21$.

Абонент A вибрав число $k = 7$ і обчислив

$r = 5^7 \ (mod\ 23) = 17, \ e = 15 \cdot 21^7 \ (mod\ 23) = 15 \cdot 10 \ (mod\ 23) = 12.$

Тепер A висилає до B зашифроване повідомлення (17, 12). B обчислює

$m' = 12 \cdot 17^{23-1-13} \ (mod\ 23) = 12 \cdot 17^9 \ (mod\ 23) = 27 \cdot 7 \ (mod\ 23) = 15.$ ♠

Потрібно зауважити, що в цьому шифрі довжина шифрограми вдвічі перевищує довжину повідомлення, але для передачі повідомлення потрібен лише один сеанс зв'язку.