**Лекція № 9 (НЕ 2.2, 2 год.)**. Асиметричні криптосистеми.

***План лекції:***

1. Елементи теорії чисел.
2. Асиметрична система RSA.

***Зміст лекції:***

Якими би не були надійними симетричні криптоалгоритми, слабким місцем їх практичної реалізації залишається проблема розподілу криптографічних ключів. Для безпечного обміну інформацією між двома суб'єктами, один з них повинен згенерувати ключ та якимось чином конфіденційно передати іншому. Таким чином, для передавання криптографічного ключа необхідно використати або існуючу криптосистему, або захищений інформаційний канал.

Для вирішення цієї проблеми на основі нових результатів сучасної алгебри було запропоновано системи з відкритим ключем (***асиметричні криптосистеми***).

Суть таких систем, як уже зазначалося, полягає в тому, що кожним суб'єктом інформаційного обміну генеруються два ключа, зв'язані між собою певними правилами. Один ключ оголошується ***публічним*** (***відкритим***), а інший – ***приватним*** (***секретним***). Публічний ключ розміщується на доступному усім ресурсі (публікується), тому він доступний для усіх учасників інформаційного обміну. Секретний ключ зберігається суб'єктом, який його створив, і недоступний для інших суб'єктів.

Відкритий текст зашифровується на публічному ключі та передається адресатові. Зашифрований текст принципово не може бути розшифрований на публічному ключі. Розшифрування повідомлення можливо лише на відповідному приватному ключі, відомому лише безпосередньо адресату.

Асиметричні криптосистеми, як вже зазначалося, використовують так звані односторонні функції, які мають таку властивість: при заданому значенні $x$ відносно легко обчислити значення $f(x)$, однак якщо відомо значення $y = f(x)$, то не існує простого способу обчислення значення $x$. Велика кількість класів незворотних функцій і породжують усю різноманітність криптосистем з відкритим ключем. Однак в самому означенні є деяка невизначеність: що означає «не існує простого способу»?

Тому для асиметричних криптосистем ставляться дві важливих вимоги:

- 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.

Алгоритми шифрування з відкритим ключем використовують у трьох напрямках:

1. в якості самостійних засобів захисту інформації;
2. як засоби аутентифікації користувачів;
3. як засоби розповсюдження ключів. Як відомо, асиметричні криптоалгоритми значно повільніші за симетричні. Тому часто на практиці раціонально використати перші для шифрування невеликої кількості інформації, а потім за допомогою симетричних алгоритмів виконувати шифрування великих інформаційних потоків.

Для кращого розуміння принципів функціонування асиметричних криптосистем розглянемо необхідні елементи теорії чисел.

**1. Елементи теорії чисел.**

Нехай $n$ – довільне натуральне число, $x$ та $y$ – цілі числа. Будемо називати числа $x$ та $y$ ***конгруентними за модулем n***, якщо залишки від їх ділення на число $n$ однакові,

тобто $x \bmod n \equiv y \bmod n$. Наприклад, $2 \bmod 7 \equiv 9 \bmod 7$ або $11 \bmod 8 \equiv 33 \bmod 30$, оскільки залишок від ділення у цих чисел однаковий.

Операція взяття числа за модулем має три основні властивості:

- адитивності: $(a+b) \bmod n = ((a \bmod n) + (b \bmod n)) \bmod n$;
- мультиплікативності: $(a \times b) \bmod n = ((a \bmod n) \times (b \bmod n)) \bmod n$;
- збереження степеня: $(a \bmod n)^k \bmod n = a^k \bmod n$.

***Найбільший спільний дільник*** (НСД) чисел $A$ і $B$ – це найбільше з чисел, на яке обидва цих числа діляться без залишку. Наприклад, НСД(56,98)=14; НСД(76,190)=38; НСД(150,19)=1.

***Взаємно прості числа*** – це такі числа $A$ та $B$, які самі по собі, можливо, не є простими, але не мають іншого спільного дільника, на який вони діляться без залишку, окрім 1. Наприклад, числа 32 і 13 – взаємно прості, хоча 32 саме по собі не є простим, оскільки ділиться ще на 2, 4, 8, 16.

***Лишок числа A за модулем n*** – цілий залишок від ділення числа $A$ на число $n$.

***Набір лишків числа A за модулем n*** – це сукупність усіх різних цілих залишків від ділення числа $A \times i$ на число $n$, де $i$ приймає значення від 1 до $n$-1. Наприклад, набір лишків числа 3 за модулем 5 буде таким: {3,1,4,2}. Відмітимо, що довжина вектора лишків максимальна і дорівнює $n$-1, якщо числа $A$ та $n$ взаємно прості.

***Обчислення мультиплікативного оберненого числа***. Мультиплікативним оберненим числом до числа $A$ за модулем $n$ будемо називати таке число $A^{-1}$, що $(AA^{-1}) \bmod n = 1$. Відмітимо, що розв‘язок такої задачі існує не завжди, а лише тоді, коли А та $n$ – взаємно прості числа. Операція знаходження мультиплікативного оберненого дуже часто використовується у двоключовій криптографії.

Мультиплікативне обернене число можна знайти (для невеликих чисел) безпосередньо з розв‘язку рівняння $(AA^{-1}) \bmod n = 1$. Це рівняння можна записати таким чином: $AA^{-1} - 1 = i \times n$, де $i$=1,2,3,… - натуральне число. Тоді $AA^{-1} = 1 + i \times n$, звідки $A^{-1} = (1 + i \times n)/A$.

Наприклад, треба знайти мультиплікативне обернене числа 32 за модулем 29. Для цього отримаємо: $A^{-1} = (1+11 \times 29)/32 = 10$.

Класичним алгоритмом знаходження мультиплікативного оберненого – розв‘язок еквівалентного рівняння *Діофанта* за допомогою методики *Евкліда*.

Таким чином, ми отримали, $x$=10, тобто $(32)^{-1} \bmod 29 = 10$.

Перевірка дає $10 \times 32 \bmod 29 = 320 \bmod 29 = 1$.

Уведемо ***функцію Ейлера*** $\varphi(n)$, яка визначає кількість цілих чисел, взаємно простих з $n$, з множини [1,$n$-1]. Доведено, що для простого $n$ $\varphi(n) = n$-1. Продемонструємо це для множини [2,11]:

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

Як бачимо з таблички, для чисел 3,5,7,11 $\varphi(n) = n$-1.

***Теорема 1. 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 $1 \le B \le (n-1)$ знайдеться таке $1 \le X \le (n-1)$, що $A^x \bmod n = B$. Іншими словами, стверджується, що функція $A^x \bmod n = B$ однозначна на проміжку 0…$n$-1.

Виняток складають лише ступені числа 2 (тобто $A^2, A^4, \ldots$), які не утворюють однозначного перетворення.

Для прикладу розглянемо деяку функцію $y = a^x \bmod n$, $n = 7$. У таблиці подано усі можливі значення $y$ для $a$ та $x$ від 0 до 6. Як бачимо, тут є кілька варіантів. Для $a$=1 усі значення $y$ = 1. Для $a$=2, 4 та 6 бачимо багатозначне відображення $\{x\} \to \{y\}$ ($y$ – періодичне). В той же час для $a$=3 і $a$=5 існує взаємно однозначне відображення $\{x\} \to \{y\}$.

Це означає, що такі числа, 3 та 5, ми можемо використати для практичних потреб. Такі числа називаються ***первісними коренями*** за модулем *n*.

| *a**x* | 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 |

Відмітимо, що 3 та 5 взаємно прості з 7. Крім того, 5 – взаємно просте число з 6, тобто з *n*-1. Ця табличка також ілюструє *малу теорему Ферма*: $a^6 \bmod 7 = 1$ (тобто $a^{n-1} \bmod n = 1$).

Зрозуміло, що у випадку таких малих чисел, які подано в табличці, розв‘язати обернену задачу знаходження числа *x*, якщо відомо *y* та *n* дуже просто. Однак для великих цілих чисел розв‘язок оберненої задачі (яка називається задачею дискретного логарифмування у кінцевому полі) стає обчислювально складним. Така функція називається ***односторонньою***. Аналогічна одностороння функція використовується у криптосистемі Ель-Гамаля.

Іншим представником односторонніх функцій є розкладання великого цілого числа на прості множники. Обчислити добуток двох простих чисел дуже просто. Однак для розв‘язку оберненої задачі, розкладання заданого числа на прості множники, ефективного алгоритму сьогодні не існує. Така одностороння функція використовується у криптосистемі RSA.

В усіх двоключових криптосистемах використовують так звані ***односторонні функції з пасткою***. Це означає, що публічний ключ криптосистеми визначає конкретну реалізацію функції, а приватний ключ дає певну інформацію про пастку. Будь-хто, хто знає приватний ключ, може легко обчислювати функцію в обох напрямках, але той, хто не має такої інформації, може обчислювати функцію лише в одному напрямку. Прямий напрямок використовується для зашифрування інформації та верифікації цифрового підпису. Обернений же напрямок застосовують для розшифрування та створення електронного цифрового підпису.

В усіх криптосистемах з відкритим ключем чим більша довжина ключів, тим більша різниця у зусиллях, необхідних для обчислення функції у прямому та оберненому напрямках (для тих, хто не має інформації про пастку).

Усі практичні криптосистеми з відкритим ключем використовують функції, які вважаються односторонніми, однак цю властивість не доведено для жодної з них. Це означає, що теоретично можливо створення алгоритму, що дозволить легко обчислити обернену функцію без знання інформації про пастку. Однак так само імовірним може бути теоретичне доведення неможливості такого обчислення. В першому випадку це призведе до повного краху відповідної криптосистеми, а у другому – значно зміцнить її позиції.

**2.Криптосистема RSA.**

Не дивлячись на досить велику кількість різних асиметричних криптосистем, широке практичне застосування отримала RSA, назва якої походить від перших літер прізвищ її авторів, Рональда Рівеста (Ron Rivest), Аді Шаміра (Adi Shamir) та Лена Аделмана (Leonard Addleman).

Вони використали той факт, що обчислення добутку двох великих простих чисел значно простіше, ніж розкладання великого цілого числа на прості множники. Доведено (теорема Рабіна), що розкриття криптосистеми RSA еквівалентно такому розкладанню.

Звідси випливає, що можна дати нижню оцінку кількості операцій, необхідних для розкриття шифру, а враховуючи продуктивність сучасних комп‘ютерів, обчислити потрібний для цього час.

Звичайно, що наявність гарантованої оцінки криптостійкості алгоритму створила сприятливі умови для розповсюдження криптосистеми RSA на фоні інших алгоритмів. Це й стало однією з причин її популярності у банківських системах для роботи з віддаленими клієнтами.

Розглянемо алгоритм шифрування за схемою RSA. Звичайно, у навчальних цілях ми будемо використовувати приклад з малими числами, однак для реальної роботи ці числа не підходять, оскільки криптостійкість такої системи практично дорівнює нулю.