Лабораторна робота 2.3

АЛГОРИТМИ ШАМІРА ТА РАБІНА

Мета: отримати навички у створенні програмної реалізації алгоритму асиметричних алгоритмів Шаміра та Рабіна.

Основні завдання:

1. Розробити об'єктно-орієнтованою мовою програмування консольний або віконний додаток, що реалізує шифрування та дешифрування вмісту текстового або виконуваного файлу з використанням асиметричних алгоритмів Шаміра та/або Рабіна. Програма повинна запитувати ім'я вхідного і вихідного файлів, тип шифру та вхідні параметри для проведення криптографічних перетворень. В якості вхідних параметрів виступають: p та q –великі взаємнопрості числа.
2. Представити блок структурну схему своєї програмної реалізації.
3. Зробити висновки на підставі проведених теоретичних та практичних досліджень. У висновках слід зазначити, які навички та знання отримано під час виконання завдань.

Основні теоретичні відомості

Алгоритм Шаміра. Даний алгоритм, запропонований Аді Шаміром (A. Shamir), дозволяє організувати обмін секретними повідомленнями по відкритій лінії зв'язку для осіб, які не мають захищених каналів і секретних ключів. Далі опиишему схему обміну інформаційними повідомленнями.

Сторона *A* хоче передати повідомлення *M* абоненту так, щоб ніхто не дізнався його семантичного зміст. Абонент *A* вибирає випадкове велике просте число *p* і відкрито передає його абоненту *B*. Потім *A* вибирає два секретних числа – k_a і q_a, такі, що задовольняютья умові:

$$k_a q_a \equiv 1 \bmod(p-1)$$

Абонент *B* також вибирає два секретних числа – k_b і q_b, такі, що задовольняютья умові:

$$k_b q_b \equiv 1 \bmod(p-1)$$

Після вибору секретних чисел сторона *A* передає інформаційне повідомлення *M*, використовуючи триступінчастий протокол. Якщо $M < p$ (*M* сприймається як число), то повідомлення M передається

відразу; якщо ж $M > p$ то повідомлення надається як $M = m_1, m_2, ..., m_i$, де всі $m_i < p$, і потім передаються послідовно $m_1, m_2, ..., m_i$. У цьому для шифрування кожного m_i краще вибирати випадково нові пари чисел (k_a, q_a) і (k_b, q_b) – інакше надійність системи знижується. Нині такий шифр використовується переважно передачі чисел, наприклад секретних ключів, значення яких менше *p*. Таким чином, ми розглядатимемо лише випадок $M < p$. Далі розглянемо основні етапи протоколу обміну:

1 етап. Абонент *A* обчислює число Y_a і по відкритій лінії зв'язку пересилає абоненту

$$Y_a \equiv M^{k_a} \pmod{p}.$$

2 етап. Абонент *B*, отримавши Y_a, обчислює число Y_b і по відкритій лінії зв'язку пересилає абоненту *A*

$$Y_b \equiv Y_a^{k_b} \pmod{p}.$$

3 етап. Сторона *A* обчислює число *C* і передає його стороні *B*:

$$C \equiv Y_b^{q_a} \pmod{p}.$$

4 етап. Сторона *B*, отримавши число *C*, обчислює повідомлення *M*:

$$M \equiv C^{q_b} \pmod{p}.$$

Алгоритм Рабіна. Алгоритм Рабіна є модифікацією алгоритму RSA. Безпека алгоритму Рабіна заснована на складності пошуку квадратного коріння за модулем числа. Вибираються два простих числа – *p* і *q*, – порівнянних із 3mod4. Ці прості числа є закритим ключем, а добуток $n = p \cdot q$ – відкритим:

$$p \equiv 3 \pmod{4} \equiv -1 \pmod{4}, \quad q \equiv 3 \pmod{4} \equiv -1 \pmod{4}$$

Вважається, що *e* фіксовано і завжди дорівнює 2, тоді криптограма відкритого повідомлення *M* розраховується наступним чином: $C \equiv M^2 \pmod{n}$.

Введемо допоміжні величини *x* та *y*: $x \equiv C^k \pmod{p}$;

$y \equiv C^1 (\mathrm{mod}\, q)$, де $4k = p + 1$, $4l = q + 1$.

Для x^2 та y^2 отримаємо:

$$x^2 \equiv C^{2k} (\mathrm{mod}\, p) \equiv \left[\left(M^2 \right)^{\frac{p+1}{4}} \right]^2 \mathrm{mod}\, p \equiv M^{p+1} (\mathrm{mod}\, p) \equiv \left(M^{p-1} M^2 \right) \mathrm{mod}\, p \equiv$$

$$\equiv M^2 (\mathrm{mod}\, p)$$

$$y^2 \equiv C^{2l} (\mathrm{mod}\, q) \equiv \left[\left(M^2 \right)^{\frac{q+1}{4}} \right]^2 \mathrm{mod}\, q \equiv M^2 (\mathrm{mod}\, q)$$

Отримуємо чотири системи рівнянь для M_1, M_2, M_3, M_4:

$$\begin{cases} M_1 \equiv x (\mathrm{mod}\, p); \\ M_1 \equiv y (\mathrm{mod}\, q); \end{cases} \quad \begin{cases} M_2 \equiv x (\mathrm{mod}\, p); \\ M_2 \equiv -y (\mathrm{mod}\, q); \end{cases} \quad \begin{cases} M_3 \equiv -x (\mathrm{mod}\, p); \\ M_3 \equiv y (\mathrm{mod}\, q); \end{cases}$$

$$\begin{cases} M_4 \equiv -x (\mathrm{mod}\, p); \\ M_4 \equiv -y (\mathrm{mod}\, q). \end{cases}$$

Одним з цих рішень системи рівнянь M_1, M_2, M_3, M_4 є повідомлення *M*. Якщо повідомлення написано словами, вибрати правильне *M* нескладно. З іншого боку, якщо повідомлення є потоком випадкових бітів (призначених для створення ключів або цифрового підпису), то визначити, яке саме *M* є правильним, складне завдання. Одним із способів вирішити цю проблему є додавання до повідомлення заголовка, яке виконується перед шифруванням.

Запитання для самоперевірки

1. Поясність основні напрями використання алгоритму Шаміра.
2. Поясніть основні умови вибору секретних параметрів алгоритму Шаміра.
3. Охарактеризуйте основні етапи проведення шифрування алгоритму згідно алгоритму Шаміра.
4. Назвіть основні особливості використання алгоритму Рабіна.
5. Охарактеризуйте основні умови вибору секретних параметрів алгоритму Рабіна.