Лабораторна робота №5

Використання шифрувальної системи RSA для цифрового підпису.

Мета:

Створити просту криптографічну систему цифрового підпису на основі системи шифрування RSA та дослідити її роботу.

Обладнання:

- персональний комп’ютер з встановленою операційною системою Windows
- будь-яка мова програмування.

Завдання:

1. Створити просту криптографічну систему цифрового підпису на основі шифру RSA.
2. Перевірити її роботу.

Література:

1. М.Масленников. Практическая криптография. БХВ-Петербург,2003. – 464с.
2. Б.Шнайер. Прикладная криптография. Протоколы, алгоритмы, исходные коды на языке С. 1996.
3. Галицкий А.В., Рябко С.Д., Шаньгин В.Ф. Защита информации в сети. М.”ДМК”, 2004. – 616 с.

Теоретичні відомості.

Криптографічна система RSA (Rivest, Shamir, Adleman), запропонована Рівестом, Шаміром і Едлеманом, належить до криптографічних систем з відкритим ключем. Її стійкість обумовлена великими проблемами при знаходженні розкладання великих простих чисел на множники.

Для того, щоби організувати передачу шифрованих повідомлень за допомогою криптосистеми RSA, необхідно зробити наступне:

1. За допомогою спеціальних алгоритмів згенерувати два великих простих числа p і q, які необхідно тримати у тайні.
2. Повідомити відправнику повідомлень (або розмістити у відкритому каталозі) число $n=pq$, а також випадкове ціле число E, взаємно просте з добутком $(p-1)(q-1)$.
3. Для розшифрування повідомлень, зашифрованих на відкритому ключі n, E, отримувачу необхідно мати число D, яке є мультиплікативним оберненим числа E за модулем $(p-1)(q-1)$, тобто $DE=1 \mod(p-1)(q-1)$. Знайти таке число дуже просто, оскільки найбільший спільний дільник E і $(p-1)(q-1)$ якраз і рівний одиниці за вибором E.

Таким чином, відправник знає свій закритий ключ, n, E, а отримувач, крім того, знає ще свій секретний ключ D.

Довільне відкрите повідомлення можна уявити у вигляді послідовності цілих чисел з деякого інтервалу. Будемо вважати, що відправник передає секретне повідомлення у вигляді $X_1,\ldots,X_n$ $0<X_i<n-1$, для всіх i від 1 до k.

Відправник для кожного блоку X_i вираховує

$$C_i=(X_i^E) \mod n \tag{1}$$

і передає C_i відкритим каналом зв’язку.

Маючи n, E і C_i, отримувач може розшифрувати повідомлення, використовуючи співвідношення

$$X_i=(C_i^D) \bmod n. \qquad (2)$$

Розглянемо в якості прикладу випадок p=3, q=11, n=3x11=33, E=7, D=3. Легко переконатися, що кожне з чисел E=7 і DE=21 взаємно прості з (p-1)(q-1)=20. Для передачі повідомлення M=”02” відправнику треба обчислити C=(2^7) mod 33=29. Отримувач може розшифрувати повідомлення за допомогою такої операції: X=29^3 mod 33=2. =2.

Якщо ж ми маємо текстове повідомлення, алфавіт якого пронумеровано від 00 до 32 (з пробілом), тоді можна зашифрувати довільне повідомлення російською мовою. Наприклад, якщо ми маємо повідомлення „ПРОВЕРИМ ЗНАНИЕ АРИФМЕТИКИ”, то у зашифрованому вигляді на ключі n=33, E=7 воно буде мати вигляд:
27 25 20 29 14 25 02 12 32 28 07 00 07 02 14 32 00 25 02 26 12 14 06 02 10 02
Зрозуміло, що шифром в даному випадку є шифр простої заміни за табл. 1.

Таблиця 1. Таблиця заміни при шифруванні.

А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С
00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17
Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я				
18	19	20	21	22	23	24	25	26	27	28	29	30	31	32			

Одним з відомих алгоритмів дешифрування системи RSA є метод ітерацій. Згідно з ним вихідне повідомлення можна отримати з шифрованого повторним шифруванням доти поки не отримаємо відкритий текст.

П р и к л а д 1. Нехай p=383, q= 563, n=215629, E=49. В цьому випадку відкритий текст повністю отримується уже через 10 ітерацій повторного шифрування. Щоби в цьому впевнитися, достатньо довести, що 49^{10}=1 mod (p-1)(q-1). Виконання цієї рівності можна перевірити навіть на калькуляторі: (49^4=5764801 -> 49^4=183017 mod 214684 … 49^9=56957 mod 214684 -> 49^{10}= 1 mod 214684).

Інший метод атаки на шифр RSA – метод розкриття чисел p і q. Справа в тому, що $n=pq$ (як і самі ці числа p і q) повинні бути досить великими, щоби розкласти його на множники було дуже складно (в цьому і полягає складність цього алгоритму шифрування). Бажано, щоби p і q вибиралися випадковим чином і не були „дуже близькими” одне до одного.

Покажемо, яким чином можна використати близькість значень p і q. Будемо вважати, що $p > q$ (що не накладає зайвих обмежень). Тоді для величин x=(p + q)/2, y=(p – q)/2 справедливе співвідношення: x^2-y^2=n.

Перебираючи у порядку зростання варіанти x $>\sqrt{n}$, легко знайти розв’язок рівняння x^2-y^2=n, так як x=(p + q)/2 буде близьким до $\sqrt{n}$ у випадку близькості p і q.

П р и к л а д 2. Нехай n=pq=851. Використаємо описаний спосіб для знаходження p і q. Так як $\sqrt{n}$ =29.17, беремо x=30 і обчислюємо 30^2-851=49 і з першої спроби знаходимо розв’язок x=30 і y=7. Таким чином, p=30+7=37, q=30-7=23.

Крім вказаних обмежень на p, q, E, D накладаються й інші обмеження.

Система шифрування RSA може бути застосована для цифрового підпису. У випадку підпису повідомлення M відправник обчислює P=M^E mod n. Отримувач, який має M та P, перевіряє справедливість співвідношення P^D=M mod n і впевнюється у справжності повідомлення M.

П р и к л а д 3. Нехай p=3, q=11, n=3x11=33, E=7, D=3. Тоді відправник повідомлення M=”02” обчислює цифровий підпис P=2^7 mod 33=29 і відправляє повідомлення „02, 29” отримувачу. Той, в свою чергу, перевіряє справжність повідомлення „02”, обчисливши M=(29^3) mod 33=2.

Насправді підписують не саме повідомлення, а його т.зв. хеш-функцію. Спочатку оригінальне повідомлення обробляється деякою функцією, яка має таку властивість, що приймає на вході рядки різної довжини, а на виході видає деякий „дайджест”, як правило, однакової і меншої, ніж вхідна, довжини. Хеш-функція виконує математичні обчислення, у результаті яких обчислюється значення хеш-функції. Хеш-функція може бути дуже простою. Наприклад, вона може виконати підсумовування всіх одиниць двійкового коду, або додати значення кодів всіх літер рядка, що обробляється (т.зв. контрольна сума) і т.д. Головне полягає в тому, що значення хеш-функції повинно залежати від усього вхідного рядка, щоби не можна було (в крайньому разі було б дуже важко) підібрати два різних вхідних рядки з однаковим значенням хеш-функції. Якщо таке трапляється, то кажуть що виникла колізія.

Ми будемо користуватися найпростішою хеш-функцією, яка дуже недосконала і може викликати значні колізії. Однак, вона дуже проста і не потребує витрат машинного часу, а також складного програмування. Ця функція просто сумує всі значення символів за табл. 1 за модулем 33:

$$\mathrm{H(M)}=\sum_{i=1,n} m_i \bmod 33. \quad (3)$$

До отриманого таким чином числа застосовують алгоритм прикладу 3, отримуючи, таким чином, зашифрований цифровий підпис.

Отримувач, маючи повідомлення і цифровий підпис, розшифровує текст повідомлення, знаходить хеш-функцію від нього за формулою (3), розшифровує цифровий підпис, і порівнює отримані значення. Якщо вони однакові, повідомлення і цифровий підпис є істинними.

Практична частина.

1. Підгрупа розбивається на пари за бажанням. Один студент виконує цифровий підпис повідомлення, а другий – цей підпис перевіряє.
2. Перший студент створює криптографічну систему на основі алгоритму RSA, що викладений у теоретичній частині. В якості значень ключів візьміть p=3, q=11, n=3x11=33, E=7, D=3.
3. Система шифрування повинна задовольняти наступним вимогам: 1) читати з текстового файлу відкрите повідомлення; 2) шифрувати повідомлення за допомогою ключа 7, 33; 3) обчислювати просту хеш-функцію повідомлення у вигляді (3); 4) обчислювати цифровий підпис знайденої хеш-функції і записувати його значення у файл (той самий, в якому міститься повідомлення або інший).
4. Другий студент створює систему перевірки електронного підпису. Система повинна задовольняти таким вимогам: 1) читати з текстового файлу зашифроване повідомлення та цифровий підпис; 2) розшифровувати повідомлення за допомогою таємного ключа D і знаходити хеш-функцію (3); 3) розшифровувати цифровий ключ і порівнювати отримане значення хеш-функції з обчисленим у п.2); 4) робити висновок про істинність отриманого повідомлення і цифрового підпису.
5. Замініть цифровий підпис довільним числом з діапазону 0-32 і знов перевірте, чи „помітить” програма розшифрування заміну.
6. Зробіть висновок про якість роботи Вашої системи електронного підпису.

Контрольні запитання.

1. До яких систем шифрування належить система RSA?
2. Який алгоритм шифрування використовується у системі RSA?
3. На чому ґрунтується криптостійкість системи RSA?
4. Які обмеження накладаються на ключі криптосистеми RSA?
5. Які ви знаєте способи розкриття шифру криптосистеми RSA?
6. Як можна застосувати криптосистему RSA для цифрового підпису повідомлень?
7. Як Ви розумієте поняття хеш-функції? Які бувають хеш-функції?
8. Які Ви бачите недоліки у запропонованій у цій ЛР хеш-функції?
9. Для чого, на Вашу думку, застосовують цифровий підпис документів?
10. Де у банківській сфері використовують цифровий підпис і яка його роль?