Лабораторна робота №7

Відкритий розподіл криптографічних ключів.

Мета:

Ознайомитися з відкритим розподілом криптографічних ключів за допомогою алгоритму Діффі-Хеллмана.

Обладнання:

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

Завдання:

1. Створити просту систему відкритого розподілу криптографічних ключів за алгоритмом Діффі-Хеллмана.
2. Перевірити її роботу.

Література:

1. Молдовян Н.А., Молдовян А.А. Введение в криптосистемы с открытым ключом. БХВ-Петербург, 2005. – 288 с.
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

Проблема адміністрування криптографічними ключами вважається основним недоліком симетричних криптоалгоритмів. Цю проблему можна вирішити за допомогою асиметричної криптографії, тобто взагалі не використовувати симетричні криптоалгоритми. Однак такий підхід вважають нераціональним, оскільки асиметричні алгоритми працюють значно повільніше за симетричні і не можуть використовуватися у ряді важливих криптографічних застосувань.

Іншим способом розповсюдження ключів є специфічні алгоритми, розроблені спеціально для таких застосувань.

Одним з таких алгоритмів відкритого розповсюдження ключів є алгоритм Діффі-Хеллмана.

Нехай учасники інформаційного обміну, сторони А і В, домовилися використати цей алгоритм для обміну ключами. Для цього необхідно виконати наступні обчислення.

Спочатку А і В обирають велике просте число p, модуль системи. Для цього числа p обирають первісний корінь a. Числа p і a відкрито передають по каналах зв'язку, так щоб їх мали обидві сторони.

Далі виконується наступний протокол:

а. А генерує ціле велике випадкове число x і відправляє В число:

$$X = a^x \bmod p;$$

2) В генерує велике ціле випадкове число y і відправляє А число:

$$Y = a^y \bmod p;$$

3) А обчислює:

$$k = Y^x \bmod p;$$

4) В обчислює:

$$k' = X^y \bmod p.$$

І k, і k' дорівнюють $k = k' = a^{xy} \bmod p$. Отже сторони А і В отримали один і той самий криптографічний ключ, не пересилаючи його каналами зв‘язку. Ніхто з осіб, що прослуховують цей канал, не зможе обчислити значення ключа. Адже їм відомі тільки p, a, X, Y, а для знаходження ключа необхідно розв‘язати задачу дискретного логарифмування. Тому А і В мають цілком таємний ключ, який більше ніхто не знає.

Вибір a і p може помітно впливати на безпеку системи. Найголовніше, це те, що p повинно бути великим, таким, щоби задача дискретного логарифмування у скінченому полі була складною обчислювальною проблемою. Можна обирати довільне a, яке є первісним коренем за модулем p; немає причин, за якими не можна було б обрати a найменшим з можливих, навіть однорозрядним. Навіть необов‘язково, щоби a було первісним коренем, воно повинно лише утворювати досить велику підгрупу мультиплікативної групи за модулем p.

Практична частина

Складіть програму, яка б реалізовувала алгоритм обміну криптографічними ключами за Діффі-Хеллманом. Для цього:

1. Оберіть просте число p та його первісний корінь a. Число p повинно бути як мінімум 4-значним. Для пошуку простих чисел можна скористатися кодом, наведеним у додатку.
2. Для обраного p знайдіть первісний корінь a. Для цього скористайтеся малою теоремою Ферма.
3. Для обраних p і a виконайте обчислення k і k' та порівняйте їх.
4. Зробіть висновок про якість роботи Вашої системи обміну ключами.
5. Підготуйте звіт з лабораторної роботи. Звіт повинен містити: а) результати досліджень; б) протокол Ваших дій; в) код програми; г) висновок з лабораторної роботи; д) відповіді на контрольні запитання.

Контрольні запитання

1. У чому полягає проблема розподілу ключів у симетричних криптосистемах?
2. Як асиметричні криптосистеми вирішують цю проблему?
3. Які переваги і недоліки комбінованих криптосистем?
4. Охарактеризуйте метод відкритого розподілу ключів за алгоритмом Діффі-Хеллмана?
5. На чому ґрунтується крипостійкість цього методу?
6. Що таке односторонні функції?
7. Які односторонні функції Ви знаєте? Охарактеризуйте кожну з них.
8. Які ще алгоритми розподілу криптографічних ключів Ви знаєте? Охарактеризуйте їх.

Додаток

Програма для пошуку простих чисел

```
var
   prime:array[0..1000000]of integer;
   n,i,j:integer;
   o:boolean;
 begin
   assign(input,'input.txt');reset(input);
   assign(output,'output.txt');rewrite(output);
   read(n);
   i:=2;prime[0]:=0;
   while prime[prime[0]]<n do
   begin
     o:=true;
     for j:=1 to prime[0] do
       if prime[j]>trunc(sqrt(i)) then break
       else
         if i mod prime[j] =0 then
         begin
           o:=false;
           break;
         end;
     if o then
     begin
       inc(prime[0]);write(i,' ');
       if prime[0] mod 100 =0 then
         writeln;
       prime[prime[0]]:=i;
     end;
     inc(i)
   end;
 end.
```