Лабораторная работа №3

"Криптографические системы с открытым ключом"

1. ТЕОРЕТИЧЕСКАЯ ЧАСТЬ

Первые криптографические системы с открытым ключом появились в конце 1970-х годов. От классических алгоритмов они отличаются тем, что для шифрования данных используется один ключ (*открытый*), а для расшифрования – другой (*секретный*). Данные, зашифрованные открытым ключом, можно расшифровать *только* секретным ключом. Следовательно, открытый ключ может распространяться через обычные коммуникационные сети и другие открытые каналы. Таким образом, устраняется главный недостаток стандартных криптографических алгоритмов: необходимость использовать специальные каналы связи для распределения ключей. Разумеется, секретный ключ не может быть вычислен из открытого ключа.

В настоящее время лучшим криптографическим алгоритмом с открытым ключом считается RSA (по имени создателей: Rivest, Shamir, Adelman).

Наиболее важной частью алгоритма RSA, как и других алгоритмов с открытым ключом, является процесс создания пары открытый/секретный ключи. В RSA он состоит из следующих шагов.

1. Случайным образом выбираются два секретных простых числа, p и q, $p \neq q$.
2. Вычисляется $r=p*q$.
3. Вычисляется функция Эйлера $\varphi(r)=(p-1)*(q-1)$.
4. Выбираются открытый (K_o) и секретный (K_c) ключи, которые являются взаимно простыми с $\varphi(r)$ и удовлетворяют условию $(K_o * K_c) \bmod \varphi(r) = 1$. То есть, K_o является взаимообратным по модулю $\varphi(r)$ для K_c. Таким образом, ключом шифрования является пара значений (K_o, r). Ключом расшифрования является пара значений (K_c, r). Значение параметра r, так же как и значение ключа K_o, является общедоступной информацией в то время как значения параметров p, q и ключа K_c хранятся в секрете.

Чтобы зашифровать данные открытым ключом K_o, необходимо:

1) разбить исходный текст на блоки, каждый из которых может быть представлен в виде числа $M(i)$ в диапазоне $0 \ldots r-1$;

2) зашифровать последовательность чисел $M(i)$ по формуле:

$$C(i)=(M(i)^{Ko}) \bmod r,$$

где последовательность чисел $C(i)$ представляет шифротекст.

Чтобы расшифровать эти данные секретным ключом K_c, необходимо выполнить следующие вычисления:

$$M(i)=(C(i)^{Kc}) \bmod r.$$

В результате будет получено множество чисел $M(i)$, которые представляют собой исходный текст.

Приведем простой пример использования метода RSA для шифрования сообщения “CAB”. Для простоты будем использовать малые числа (на практике используются намного большие числа).

1. Выберем p=3, q=11.

2. Вычислим r=3*11=33.

3. Вычислим $\varphi(r)=(p-1)*(q-1)=20$.

4. Выберем секретный ключ K_c, который является взаимно простым с $\varphi(r)$, например K_c=3.

5. На основе K_c и $\varphi(r)$ вычислим открытый ключ K_o. Для этого можно использовать расширение алгоритма Евклида. Расширенный алгоритм Евклида позволяет вычислить x_1 и y_1, при которых выполняется равенство $x_1*a+y_1*b=d_1$, где d_1=НОД(a,b). Если a и b – взаимнопростые и $a>b$, то y_1 является взаимообратным для b по модулю a. То есть, $y_1*b \bmod a = 1$.

```
EUCLIDEX(a; b)
1     d0:=a; d1:=b;
2     x0:=1; x1:=0;
3     y0:=0; y1:=1;
4     while d1>1 do
      begin
5           q:=d0 div d1;
6           d2:=d0 mod d1;
7           x2:=x0–q*x1;
8           y2:=y0–q*y1;
9           d0:=d1; d1:=d2;
10          x0:=x1; x1:=x2;
11          y0:=y1; y1:=y2;
      end
12    return (x1; y1; d1)
```

Используя данный алгоритм можно вычислить K_o положив a равным $\varphi(r)$ и b равным K_c:

EUCLIDEX(20; 3)

d_0:=*20*; d_1:=3

x_0:=1; x_1:=0

y_0:=0; y_1:=1

d_1>1 (3>1)

q:=20 div 3 = 6

d_2:=20 mod 3 = 2

x_2:=1–6 *0=1

y_2:=0–6*1=–6

d_0:=3; d_1:=2

x_0:=0; x_1:=1

y_0:=1; y_1:=–6

d_1>1 (2>1)

q:=3 div 2 = 1

d_2:=3 mod 2 = 1

x_2:=0–1*1=–1

y_2:=1–1*(–6)=7

d_0:=2; d_1=1

x_0:=1; x_1=–1

y_0:=–6; y_1=7

d_1=1 (1=1)

return (–1; 7; 1)

В соответствии с алгоритмом получаем K_o=y_1=7.

6. Представим шифруемое сообщение как последовательность целых чисел в диапазоне 2...28. Пусть букве ‘A’ соответствует число 3, букве ‘B’ – число 4, а букве ‘C’ – число 5. Тогда сообщение “CAB” можно представить в виде последовательности чисел {5, 3, 4}. Зашифруем сообщение, используя открытый ключ K_o=7:

$C(1) = (5^7) \bmod 33 = 78125 \bmod 33 = 14,$

$C(2) = (3^7) \bmod 33 = 2187 \bmod 33 = 9,$

$C(3) = (4^7) \bmod 33 = 16384 \bmod 33 = 16.$

7. Для расшифровки полученного сообщения {14, 9, 16} с помощью секретного ключа K_c=3, необходимо:

$M(1) = (14^3) \bmod 33 = 2744 \bmod 33 = 5,$

$M(2) = (9^3) \bmod 33 = 729 \bmod 33 = 3,$

$M(3) = (16^3) \bmod 33 = 4096 \bmod 33 = 4.$

Таким образом, в результате расшифрования сообщения получено исходное сообщение {5, 3, 4} (“CAB”).

Криптостойкость алгоритма RSA основывается на предположении, что исключительно трудно определить секретный ключ по открытому, поскольку для этого необходимо решить задачу о существовании делителей целого числа, то есть, найти множители параметра r. Данная задача не имеет эффективного (полиномиального) решения. Вопрос существования эффективного алгоритма решения данной задачи является до настоящего времени открытым. Традиционные же методы для чисел, состоящих из 200 цифр (именно такие числа рекомендуется использовать), требуют выполнения огромного числа операций (порядка 10^{23}).

2. ПОРЯДОК ВЫПОЛНЕНИЯ РАБОТЫ

2.1. Изучить теоретический материал по лабораторной работе.

2.2. Используя заданные в соответствии с вариантом значения p, q и закрытого ключа K_c вычислить открытый ключ K_o при помощи расширенного алгоритма Евклида и выполнить шифрование по алгоритму RSA открытым ключом (K_o) первых 5 букв своей фамилии. Для представления букв в числовой форме использовать следующее соответствие: ‘А’ – 2, ‘Б’ – 3, ‘В’ – 4, …, ‘Ё’ – 8, …, ‘Я’ – 34.

2.3. Выполнить проверку правильности расшифрования полученных зашифрованных данных при помощи закрытого ключа K_c.

Варианты заданий.

1. p=5, q=7, K_c=11.
2. p=17, q=5, K_c=7.
3. p=11, q=5, K_c=13.
4. p=7, q=11, K_c=19.
5. p=7, q=17, K_c=5.
6. p=3, q=17, K_c=23.
7. p=13, q=3, K_c=11.
8. p=5, q=13, K_c=19.
9. p=7, q=13, K_c=17.
10. p=3, q=19, K_c=7.
11. p=5, q=7, K_c=23.
12. p=17, q=5, K_c=19.
13. p=11, q=5, K_c=17.
14. p=7, q=11, K_c=13.
15. p=7, q=17, K_c=11.
16. p=3, q=17, K_c=13.
17. p=13, q=3, K_c=17.
18. p=5, q=13, K_c=11.
19. p=7, q=13, K_c=19.
20. p=3, q=19, K_c=13.
21. p=5, q=7, K_c=19.
22. p=17, q=5, K_c=23.
23. p=11, q=5, K_c=19.
24. p=7, q=11, K_c=17.
25. p=7, q=17, K_c=23.
26. p=3, q=17, K_c=11.
27. p=13, q=3, K_c=19.
28. p=5, q=13, K_c=17.
29. p=7, q=13, K_c=23.
30. p=3, q=19, K_c=11.