Лабораторная работа №4

Криптосистема RSA

Наиболее популярной современной системой с открытым ключом является RSA – криптосистема (Rivest R., Shamir A., Adleman L.). Берутся 2 больших простых числа p и q. Вычисляется их произведение $n = p \cdot q$. Тогда $\varphi(n) = (p-1)(q-1)$. Выбираем натуральное число e, такое, что $0 < e < n$ и НОД $(e, \varphi(n)) = 1$.

Пара (e, n) и будет открытым ключом. Шифруемая информация переводится в цифровую форму. Например, в первоисточнике буквы латинского алфавита заменялись двузначными числами: «*а*»=01, «*в*»=02, …, пробел = 00. Получается некоторое число *c*. Предполагается, что, $0 < c < n$ и НОД$(c, n) = 1$. Сообщение передается числом $ш = c^e (\mathrm{mod}\, n)$.

Адресат получает сообщение $(n, e, ш)$. Он, как и все, знает n и e. Он также должен знать секретный ключ – такое натуральное $d < n$, что $e \cdot d \equiv 1 (\mathrm{mod}(\varphi(n)))$. Значит, $e \cdot d = \varphi(n) \cdot k + 1$ для некоторого целого k. Тогда по теореме Эйлера $ш^d = c^{ed} = c \cdot (c^n)^{\varphi(k)} \equiv c \cdot 1 = c\, (\mathrm{mod} n)$. Итак, для нахождения c достаточно найти остаток от деления $ш^d$ на n.

Взломать криптотекст RSA можно только, если найти d – решение сравнения $ex \equiv 1 (\mathrm{mod}\, \varphi(n))$. Для этого надо знать $\varphi(n)$. Из свойств $\varphi(n)$ следует, что единственно надежный путь для этого – разложить n на множители – трудоемкая задача, составляющая основу криптографической стойкости криптосистемы RSA.

Пример 1. Зашифруем системой RSA слово: «сад». Его цифровым аналогом в соответствии с выше принятым правилом будет число $c = 190105$. Возьмем два простых числа $p = 47$ и $q = 71$. Тогда открытый ключ $n = p \cdot q = 3337$. Находим $\varphi(n) = 46 \cdot 70 = 3220$. Выберем $e = 79$, такое, что $НОД(79, 3220) = 1$. У нас $c > n$. Поэтому для шифрования сообщения c разделим его на блоки c_1, c_2, так, чтобы $0 < c_i < 3337$, $i = 1,2$. Возьмем $c_1 = 190$; $c_2 = 105$. Запишем $e = 79$ в двоичной системе счисления: $79_{10} = 1001111_2 = 2^6 + 2^3 + 2^2 + 2 + 1 = 64 + 8 + 4 + 2$.

Первый блок шифруется так:

$190^2 = 36100 \equiv 2730 \pmod{3337}$;

$190^4 \equiv 2730^2 = 7452900 \equiv 1379 \pmod{3337}$;

$190^8 \equiv 1379^2 = 1901641 \equiv 2888 \pmod{3387}$;

$190^{16} \equiv 2888^2 = 8340544 \equiv 1381 \pmod{3337}$;

$190^{32} \equiv 1381^2 = 1907161 \equiv 1734 \pmod{3337}$;

$190^{64} \equiv 1734^2 = 3006756 \equiv 119 \pmod{3337}$;

$190^{79} \equiv 119 \cdot 2888 \cdot 1379 \cdot 2730 \cdot 190 \equiv 742 \pmod{3337}$.

Второй блок: $105 = 105 \pmod{3337}$; $105^2 \equiv 1014 \pmod{3337}$;

$105^4 = 1014^2 \equiv 400 \pmod{3337}$; $105^8 \equiv 400^2 \equiv 3161 \pmod{3337}$;

$105^{16} \equiv 3161^2 1 \equiv 943 \pmod{3337}$; $105^{32} \equiv 943^2 \equiv 1607 \pmod{3337}$;

$105^{64} \equiv 1607^2 \equiv 2948 \pmod{3337}$. Тогда

$105^{79} \equiv 2948 \cdot 3161 \cdot 400 \cdot 1014 \cdot 105 \equiv 193 \pmod{3337}$.

Передаваемые сообщения: (742, 79, 3337) и (193, 79, 3337). Конечно, адресат должен знать о разбиении сообщения на блоки. Отметим также, что для большей криптостойкости лучше было бы сообщение не разбивать на блоки, а выбрать $n > c$.

Задание 2. Зашифровать в системе RSA сообщение $c = 51$.

Решение. Выбираем число n, $0 < c < n$, являющееся произведением простых чисел p и q и взаимно простого с c. Например, $n = 55 = 5 \cdot 11$, $p = 5, q = 11$ и НОД(51, 55) = 1. Находим функцию $\varphi(n) = (p-1)(q-1)$. $\varphi(55) = 40$. Далее, выбираем e, такое, что НОД $(e, \varphi(n)) = 1$. Например, $e = 3$. Возводим c в степень e по модулю $n = 55$. Это и будет передаваемое сообщение: $51^3 = 132651 \equiv 46 (\mathrm{mod} 55)$.

Пара (3,55) – открытый ключ. Передаваемое сообщение (46, 3, 55).

Задание 3. Расшифровать в системе RSA (46, 3, 55).

Решение.

1) Раскладываем n на простые множители: $55 = 5 \cdot 11$ $p = 5$, $q = 11$.

2) Находим значение функции Эйлера $\varphi(n)$. В данном случае

$\varphi(55) = 4 \cdot 10 = 40$.

3) Находим секретный ключ d из соотношения Безу: $3u + 40v = 1$, получаемого обратной прогонкой алгоритма Евклида нахождения $НОД(3, 40) = 1$. В данном случае алгоритм Евклида предельно краток:

$40 = 13 \cdot 3 + 1$. Следовательно, $1 = 1 \cdot 40 + (-13) \cdot 3$. Поэтому в кольце $Z/40Z$

$\overline{3}^{-1} = \overline{-13} = \overline{40-13} = \overline{27}$. Таким образом, $d = 27$.

4) Находим $ш^d \equiv c(\mathrm{mod}\, n)$, то есть $46^{27}(\mathrm{mod}55) = c$. Для этого переводим d в двоичную систему счисления:

$d = 27_{10} = 11011_2 = 2^4 + 2^3 + 2^1 + 2^0 = 16 + 8 + 2 + 1$.

$46^2 \equiv 26\,(\mathrm{mod}55)$; $46^4 \equiv 26^2 \equiv 16\,(\mathrm{mod}55)$; $46^8 \equiv 16^2 \equiv 36\,(\mathrm{mod}55)$;

$46^{16} \equiv 36^2 \equiv 31\,(\mathrm{mod}55)$; $46^{27} \equiv 31 \cdot 36 \cdot 26 \cdot 46 = 1334736 \equiv 51\,(\mathrm{mod}55)$.

Ответ: $c = 51$.

Задание 4. Зашифровать в системе RSA сообщение $c = 156$.

Решение. Выбираем $n = 209 = 11 \cdot 19,\ p = 11, q = 19$, такое, что 156<209 и НОД (156, 209) = 1. Здесь $\varphi(209) = \varphi(11) \cdot \varphi(19) = 10 \cdot 18 = 180$. Выбираем

$e = 7$ такое, что $НОД(7, 180) = 1$. Тогда шифровка $ш \equiv c^e = 156^7\,(\mathrm{mod}\,209)$.

$e = 7_{10} = 111_2 = 2^2 + 2 + 1 = 4 + 2 + 1$; $156^7 \equiv 156^4 \cdot 156^2 \cdot 156\,(\mathrm{mod}\,209)$;

$156^2 = 24336 \equiv 92\,(\mathrm{mod}\,209)$; $156^4 \equiv 92^2 = 8464 \equiv 104\,(\mathrm{mod}\,209)$;

$156^7 \equiv 156 \cdot 92 \cdot 104 = 1492608 \equiv 139\,(\mathrm{mod}\,209)$.

Пара (7, 209) – открытый ключ. Передаваемое сообщение (139, 7, 209).

Задание 5. Расшифровать сообщение (139, 7, 209).

Решение. 1) Раскладываем $n = 209$ на простые множители $209 = p \cdot q = 11 \cdot 19$.

2) Находим $\varphi(209) = (p-1)(q-1) = 10 \cdot 18 = 180$.

3) Находим секретный ключ d с помощью алгоритма Евклида.

$180 = 25 \cdot 7 + 5$;

$7 = 1 \cdot 5 + 2$;

$5 = 2 \cdot 2 + 1$. Поэтому

$1 = 5 + (-2) \cdot 2 = 5 + (-2) \cdot (7 - 1 \cdot 5) = 5 + (-2) \cdot 7 + 2 \cdot 5 = (-2) \cdot 7 + 3 \cdot 5 = (-2) \cdot 7 + 3(180 - 25 \cdot 7)$
$= 3 \cdot 180 + (-77) \cdot 7$.

Следовательно, $\overline{e^{-1}} = \overline{-77} = \overline{180-77} = \overline{103}$. Значит, $d = 103$.

4) Находим $ш^d \equiv c \pmod{n}$, то есть $139^{103} \pmod{209}$.

$103_{10} = 1110011_2 = 2^6 + 2^5 + 2^2 + 2 + 1 = 64 + 32 + 4 + 3$.

$139^2 \equiv 93 \pmod{209}$; $139^4 \equiv 93^2 \equiv 80 \pmod{209}$;
$139^8 \equiv 80^2 \equiv 130 \pmod{209}$;

$139^{16} \equiv 130^2 \equiv 180 \pmod{209}$; $139^{32} \equiv 180^2 \equiv 5 \pmod{209}$;

$139^{64} \equiv 5^2 = 25 \pmod{209}$;
$139^{103} \equiv 25 \cdot 5 \cdot 80 \cdot 93 \cdot 139 = 129270000 \equiv 156 \pmod{209}$.

Ответ: присланное сообщение $c = 156$.

1.2. АТАКИ НА АЛГОРИТМ RSA

Для дешифрации необходимо по известным *N*, e и шифртексту y найти такое $x \in ((Z/N))^*$, что $y = x^e \bmod N$.

Взлом RSA при неудачном выборе параметров криптосистемы

Само по себе использование RSA не обеспечивает безопасности. Дело еще в деталях реализации. Приведем ряд примеров. Для простоты вычислений будем работать с небольшими числами. Цель – показать особенности, не зависящие от размера.

Пример 4. Пусть пользователь выбрал $N = 2047$, $e = 179$, $d = 411$. Так как $2047 = 23 \cdot 89$, а $\varphi(23) = 22$, $\varphi(89) = 88$ имеют наименьшее общее кратное 88, то любой обратный к 179 по модулю 88, например 59, будет действовать как *d*.

Пример 5. Число $N = 536813567$ является произведением простого числа Мерсенна 8191 и простого числа Ферма 65537. Это очень плохой выбор.

Пример 6. Число 23360947609 является очень плохим выбором для *N* из-за того, что два его простых делителя слишком близки к друг другу. Пусть $p > q$, тогда имеем $N = (\frac{p+q}{2})^2 + (\frac{p-q}{2})^2$. Обозначим: $t = \frac{p+q}{2}$, $S = \frac{p-q}{2}$. Так как *S* мало, то *t* – целое число, лишь немного большее $\sqrt{N}$, причем $t^2 - N$ является полным квадратом. Проверяем подряд целые числа $t > \sqrt{N}$. В нашем примере $t_1 = 152843$, $t_2 = 152844$, $t_3 = 152845$ и $t^3 - N = 804^2$, тогда $p = 152\,845 + 804$, $p = 152845 - 804$. Таким образом, мы с третьей попытки нашли *p* и *q*. Количество попыток, необходимых для факторизации *N*, можно при известных *p* и *q* вычислить по следующей формуле:

$k=\sqrt{p\cdot q+(\frac{p-q}{2})^2}-\left[\sqrt{p\cdot q}\right]$, где [$x$] – операция округления x до ближайшего целого числа.

Атака повторным шифрованием

Строим последовательность: $y_1=y,\quad y_i=y_{i-1}^e(\mathrm{mod}\ N),\ i>1$. Итак, $y_m=y^{e^m}(\mathrm{mod}\,N)$, а так как $\left(e,\varphi(N)\right)=1$, то существует такое натуральное число m, что $e^m\equiv 1(\mathrm{mod}\,\varphi(N))$. Но тогда $y^{e^m-1}\equiv 1(\mathrm{mod}\,N)$, отсюда следует, что $y^{e^m}\equiv y(\mathrm{mod}\,N)$, значит, y_{m-1} – решение сравнения $y=x^e\left(\mathrm{mod}\,N\right)$.

Пример 7. Пусть у нас имеется открытый ключ N =84517 , e = 397 и зашифрованное им сообщение y = 8646. Необходимо найти исходный текст x. Возведем y в степень e и получим y_2 = 37043. Будем повторять операцию до тех пор, пока не получим $y_n = y$. y_{n-1} – искомое сообщение: y_3 = 5569, y_4 = 61833, y_5 = 83891, y_6 = 16137, y_7 = 8646. y_6 является решением сравнения $y=x^e\left(\mathrm{mod}\,N\right)$, а, следовательно, искомым сообщением x.

Замечание. Анализ метода повторного шифрования хорошо показывает необходимость соблюдения требований на выбор p и q для обеспечения стойкости. В данном примере d = 82 225. Неудачный выбор криптосистемы привел к тому, что атака методом повторного шифрования дала результат почти сразу, тогда как нахождение d потребовало бы на порядок больших вычислений.

Индивидуальные задания

1. Зашифровать свою фамилию и имя, используя следующие пары простых чисел p и q и открытый ключ $e=13$:

2. Расшифровать сообщение (криптосистема RSA).

3. Составьте алгоритмическое и программное обеспечение: процедур шифрования и расшифрования с использованием шифра RSA.

Вариант 1

1. p =8297, q =8293.

2. $n=250483, e=13, ш=242215$.

Вариант 2

1. p =9281, q =9283.

2. $n=1269083, e=13, ш=1101727$.

Вариант 3

1. p =9341, q =9343.

2. $n = 3338287, e = 19683, ш = 2092819$.

Вариант 4

1. p =8291, q =8293.

2. $n = 1897613, e = 161051, ш = 939402$.

Вариант 5

1. p =7949, q =7951.

2. $n = 1457297, e = 1331, ш = 1155557$.

Вариант 6

1. p =7211, q =7213.

2. $n = 5994581, e = 29575, ш = 1452748$.

Вариант 7

1. p =6701, q =6703.

2. $n = 4116037, e = 451737, ш = 833207$.

Вариант 8

1. p =9929, q =9931.

2. $n = 16440383, e = 4225, ш = 6188609$.

Вариант 9

1. p =6359, q =6361.

2. $n = 15678841, e = 1521, ш = 3924343$.

Вариант 10

1. p =6299, q =6301.

2. $n = 120287593, e = 29403, ш = 115658693$.