МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«Юго-Западный государственный университет»
(ЮЗГУ)

Кафедра информационной безопасности

УТВЕРЖДАЮ
Проректор по учебной работе
_____О.Г. Локтионова
«_4_» _04_____2022г.

Алгоритм шифрования RSA

Методические указания по выполнению практических и лабораторных работ для студентов специальностей и направлений подготовки 10.03.01, 38.03.01, 38.03.03, 38.03.05, 38.05.01, 09.03.02, 09.03.03, 09.03.04, 43.03.02, 43.03.03, 45.03.03, 40.05.01, 12.03.04, 11.03.02

Курск 2022

2

УДК 004.725.7

Составители: А.Л. Марухленко

Рецензент
Кандидат технических наук, доцент кафедры
информационной безопасности М.А.Ефремов

Алгоритм шифрования RSA: методические указания к выполнению практических и лабораторных работ / Юго-Зап. гос. ун-т; сост.: А. Л. Марухленко Курск, 2022. 11 с. Библиогр.: с. 11.

Содержат сведения по вопросам шифрования и расшифрования RSA. Указывается порядок выполнения практической работы, пример выполнения работы, правила оформления, содержание отчета, варианты заданий.

Методические указания по выполнению практических работ по дисциплине «Основы информационной безопасности», предназначены для студентов укрупненной группы специальностей и направлений подготовки 10.03.01, 38.03.01, 38.03.03, 38.03.05, 38.05.01, 09.03.02, 09.03.03, 09.03.04, 43.03.02, 43.03.03, 45.03.03, 40.05.01, 12.03.04, 11.03.02 дневной формы обучения.

Методические указания соответствуют требованиям программы, утвержденной учебно-методическим объединением по направлению подготовки «Информационная безопасность».

Текст печатается в авторской редакции

Подписано в печать Формат 60x84 1/16.
Усл. печ. л. . Уч. –изд. л. . Тираж 50 экз. Заказ 1244
Юго-Западный государственный университет.
305040, г. Курск, ул. 50 лет Октября, 94.

СОДЕРЖАНИЕ

1. ЦЕЛЬ РАБОТЫ

Получение навыков создания зашифрованного сообщения при помощи алгоритма шифрования RSA

2. ТЕОРЕТИЧЕСКАЯ ЧАСТЬ

Алгоритм *RSA*, первый из алгоритмов шифрования с открытым ключом, достойно выдержал испытание временем. Этот алгоритм основывается на задаче *RSA*, с которой мы познакомились в предыдущем параграфе. Как Вы помните, она сводится к поиску простых делителей больших натуральных чисел. Так что можно утверждать, что криптостойкость алгоритма *RSA* базируется на сложности проблемы факторизации, хотя и не в полной мере, поскольку задачу *RSA* можно решать, не прибегая к разложению на множители.

Предположим, Алиса считает нужным разрешить всем желающим отправлять ей секретные сообщения, расшифровать которые способна только она. Тогда Алиса подбирает два больших простых числа p и q. Держа их в секрете, Алиса публикует их произведение

$$N = p \cdot q$$

которое называют *модулем* алгоритма. Кроме того, Алиса выбирает шифрующую экспоненту *E,* удовлетворяющую условию

$$НОД\left(E,\left(p-1\right)\left(q-1\right)\right)=1$$

Как правило E берут равным 3, 17 или 65 537. Пара, доступная всем желающим, — это (N, E). Для выбора секретного ключа Алиса применяет расширенный алгоритм Евклида к паре чисел E и $\left(p-1\right)\left(q-1\right)$, получая при этом расшифровывающую экспоненту d. Найденная экспонента удовлетворяет соотношению

$$E \cdot d = 1\left(\mathrm{mod}\left(p-1\right)\left(q-1\right)\right)$$

Секретным ключом является тройка (d, p, q). Фактически, можно было бы выбросить простые делители p и q из ключа и помнить лишь о d и всем числе N.

Допустим теперь, что Боб намерен зашифровать сообщение, адресованное Алисе. Он сверяется с открытым ключом и представляет сообщение в виде числа *m*, строго меньшего модуля *N* алгоритма. Шифротекст *C* получается из га по следующему правилу:

$$C = m^E \pmod N$$

Алиса, получив шифрограмму, расшифровывает её, возводя число *C* в степень *d:*

$$m = C^d \pmod N.$$

Равенство имеет место в связи с тем, что порядок группы $(\square / N\square)^*$ равен $\varphi(N) = (p-1)(q-1)$. Поэтому, по теореме Лагранжа,

$$x^{(p-1)(q-1)} = 1 \pmod N$$

для любого числа. Поскольку *E и d* взаимно обратны по модулю $(p-1)(q-1)$, при некотором целом числе *s* получается равенство

$$Ed - s(p-1)(q-1) = 1.$$

Следовательно,

$$C^d = \left(m^E\right)^d = m^{Ed} = m^{1+s(p-1)(q-1)} = m \cdot m^{s(p-1)(q-1)} = m \pmod N$$

Для прояснения ситуации рассмотрим детский пример. Пусть $p = 7$ и $q = 11$. Тогда $N = 77$, а $(p-1)(q-1) = 6 \cdot 10 = 60$. В качестве открытой шифрующей экспоненты возьмём число *E* = 37, поскольку $НОД(37, 60) = 1$. Применяя расширенный алгоритм Евклида, найдём $d = 13$, т. к.

$$37 \cdot 13 = 481 = 1 \pmod{60}.$$

Предположим, нужно зашифровать сообщение, численное представление которого имеет вид: *m* = 2. Тогда мы вычисляем

$$C = m^E \pmod N = 2^{37} \pmod{77} = 51.$$

Процесс расшифровывания происходит аналогично:

$m = C^d \pmod N = 51^{13} \pmod{77} = 2$.

3. ВЫПОЛНЕНИЕ РАБОТЫ

В RSA открытый и закрытый ключ состоит из пары целых чисел. Закрытый ключ хранится в секрете, а открытый ключ сообщается другому участнику, либо где-то публикуется.

Генерация ключей RSA

Шифрование начинается с генерации ключевой пары (открытый, закрытый ключ). Генерация ключей в RSA осуществляется следующим образом:

1. Выбираются два простых числа p и q (такие что p неравно q).
2. Вычисляется модуль $N = p \cdot q$.
3. Вычисляется значение функции Эйлера от модуля N: $\varphi(N) = (p-1)(q-1)$.Выбирается число её, называемое открытой экспонентой, число e должно лежать в интервале $1 < e < \varphi(n)$,а так же быть взаимно простым со значением функции $\varphi(N)$.
4. Вычисляется число d, называемое секретной экспонентой, такое, что $d \cdot e = 1 \pmod{\varphi(N)}$ то есть является мультипликативно обратное к числу e по модулю $\varphi(N)$.

Итак, мы получили пару ключей:

Пара (e, N) - открытый ключ.

Пара $d(N)$ - закрытый ключ.

Шифрование и расшифровывание в RSA

Есть следующий сценарий: Боб и Алиса переписываются в интернете, но хотят использовать шифрование, чтобы поддерживать переписку в секрете. Алиса заранее сгенерировала закрытый и открытый ключ, а затем отправила открытый ключ Бобу. Боб хочет послать зашифрованное сообщение Алисе:

Шифрование: Боб шифрует сообщение *m*, используя открытый ключ Алисы $(e,N): C = E(M) = M^e \bmod (N)$, и отправляет с Алисе.

Расшифровывание: Алиса принимает зашифрованное сообщение С. Используя закрытый ключ (d,N), расшифровывает сообщение $M = D(C) = C^d \bmod (N)$.

Теорема Эйлера для понижения степени:

Теорема Эйлера. Для любого модуля ***m*** и целого числа ***a***, взаимно простого с ***m***, справедливо сравнение $a^{\varphi(m)} \equiv 1 \bmod m$

Следствие 1 (малая теорема Ферма). Для любого простого числа ***p*** и натурального числа ***a***, взаимно простого с ним, верна формула Ферма:

$$a^{p-1} \equiv 1 \bmod p$$

Следствие 2 (о вычислении обратного элемента).

$$a^{-1} \equiv a^{\varphi(m)-1} \bmod m$$

для любых двух натуральных простых чисел ***a*** и ***m***.

Пример. Вычислите значение выражения $11^{219} \bmod 91$. Решение.

$$91 = 7 \cdot 13;$$

$$\varphi(91) = 6 \cdot 12 = 72;$$

$$(11,91) = 1$$

По теореме Эйлера имеем:

$$11^{219} \bmod 91 = 11^{72 \cdot 3+3} \bmod 91 = \left(11^{72}\right)^3 \cdot 11^3 \bmod 91 \equiv$$

$$\equiv 11^3 \bmod 91 \equiv 121 \cdot 11 \bmod 91 \equiv 330 \bmod 91 \equiv 57 \bmod 91 = 57$$

Пример шифрования и расшифровывания в RSA

Шифрование:

Выбираем простые числа:

$$p = 3,\ q = 11$$

Вычисляем модуль $n = p \cdot q = 3 \cdot 11 = 33$

Вычисляем функцию Эйлера от модуля n : $\varphi(N) = (p-1)(q-1) = 2 \cdot 10 = 20$.

4. Выбираем открытую экспоненту $e = 7$

5. Определяем закрытую экспоненту $d : d * e = 1(\mathrm{mod}\,\varphi(N)) \Rightarrow d = 3$

Будем шифровать сообщение RSA, пусть букве A соответствует цифра 1, B - 2, C - 3 и т.д., тогда:

R=18; S=19; A=1;

Открытый ключ: $(e,n) = (7,33)$

$C_1 = (18^7) \bmod 33 = 6$

$C_2 = (19^7) \bmod 33 = 13$

$C_3 = (1^7) \bmod 33 = 1$

$C("RSA") = 6,13,1$

Пример расшифровывания RSA

Используем закрытый ключ $(d,n) = (3,33)$

$M_1 = (6^3) \bmod 33 = 18$

$M_2 = (13^3) \bmod 33 = 19$

$M_3 = (1^3) \bmod 33 = 1$

$18 = R; 19 = S; 1 = A;$

Получаем исходное сообщение - RSA.

4. ВАРИАНТЫ ЗАДАНИЙ

№	Исходный текст
1	Шумит дубравушка к непогодушке
2	Утром вороны каркают к дождю
3	Сорока на хвосте принесла
4	Снег холодный, а от мороза укрывает
5	Сирень или берёза, а всё дерево
6	Сегодня не тает, а завтра кто знает
7	Розы без шипов не бывает
8	Не высок лесок, а от ветра защищает
9	На всех и солнышко не светит
10	Красна ягодка, да на вкус горька
11	В осеннее ненастье семь погод на дворе
12	Ветром ветра не смеряешь
13	Пропущенный час годом не нагонишь
14	Счастливые часов не наблюдают
15	Друг неиспытанный, как орех не расколотый
16	Дружи с теми, кто лучше тебя самого
17	Крепкую дружбу и топором не разрубишь
18	Кто друг прямой, тот брат родной
19	лучше выслушать упрёки друга, чем потерять его
20	Одна пчела много мёду не принесёт
21	С тем не ужиться, кто любит браниться
22	Старый друг лучше новых двух
23	На чужой сторонушке рад родной воробушке
24	Народы нашей страны дружбой сильны
25	Поднявший меч от меча и погибнет
26	При солнце тепло, при Родине добро
27	Старая слава новую любит
28	Любишь кататься - люби и саночки возить
29	Кто пахать не ленится, у того хлеб родится
30	На печи не храбрись, а в поле не трусь

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1) Панасенко, С. Алгоритмы шифрования [Текст] / С. Панасенко. Спб: БХВ-Петербург, 2009, 576 стр.

2) Ростовцев А.Г., Маховенко Е.Б. Теоретическая криптография [Текст] / А.Г. Ростовцев, Е.Б. Маховенко. М: АНО НПО "Профессионал", 2005, 480 стр.

3) Рябко, Б. Я., Фионов, А. Н. Основы современной криптографии для специалистов в информационных технологиях [Текст] / Б. Я. Рябко, А. Н. Фионов. М: Научный мир, 2004, 179 стр.

4) Смарт, Н. Криптография [Текст] / Н. Смарт. М: Техносфера, 2006, 528 стр.