

Документ подписан простой электронной подписью  
Информация о владельце:  
ФИО: Емельянов Сергей Геннадьевич  
Должность: ректор  
Дата подписания: 01.02.2021 17:01:31  
Уникальный программный ключ:  
9ba7d3e34c012eba476ffd2d064c72781e953be750d12374d1613c0e336101c0

## МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное  
учреждение высшего образования  
«Юго-Западный государственный университет»  
(ЮЗГУ)

Кафедра информационной безопасности



## ШИФРОВАНИЕ С ОТКРЫТЫМ КЛЮЧОМ

Методические указания по выполнению лабораторной работы  
по дисциплине «Введение в криптографию» для студентов  
специальностей 10.05.03, 10.05.02, 10.03.01

Курск 2016

УДК 004.056.55 (076.5)

Составитель М.А. Ефремов

Рецензент

Кандидат технических наук, доцент *И.В. Калуцкий*

**Шифрование с открытым ключом:** методические указания по выполнению лабораторной работы по дисциплине «Введение в криптографию» / Юго-Зап. гос. ун-т; сост.: М.А. Ефремов. Курск, 2016. 14 с.: табл. 2. Библиогр.: с. 14.

Рассматриваются основные практические и теоретические положения этапов шифрования сообщений с помощью систем с открытым ключом. Указывается порядок выполнения лабораторной работы, правила оформления и содержание отчета.

Методические указания соответствуют требованиям программы, утвержденной учебно-методическим объединением по образованию в области информационной безопасности (УМО ИБ).

Предназначены для студентов специальностей 10.05.03, 10.05.02, 10.03.01 дневной формы обучения.

Текст печатается в авторской редакции

Подписано в печать. Формат 60x84 1/16.

Усл.печ. л. . Уч.-изд.л. . Тираж 30 экз. Заказ. Бесплатно.

Юго-Западный государственный университет.

305040, г. Курск, ул. 50 лет Октября, 94.

**СОДЕРЖАНИЕ**

1. ЦЕЛЬ РАБОТЫ	4
2. ЗАДАНИЕ	4
3. ПОРЯДОК ВЫПОЛНЕНИЯ РАБОТЫ	4
4. СОДЕРЖАНИЕ ОТЧЕТА	4
5. ТЕОРЕТИЧЕСКАЯ ЧАСТЬ	5
5.1. Введение	5
5.2. Алгоритмы шифрования и расшифровки в криптосистеме RSA	7
6. ПРАКТИЧЕСКИЕ ЗАДАНИЯ	12
7. КОНТРОЛЬНЫЕ ВОПРОСЫ	14
8. СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ И ЛИТЕРАТУРЫ	14

## **1. ЦЕЛЬ РАБОТЫ**

Цель лабораторной работы – научиться использовать системы с открытым ключом для шифрования и расшифровки сообщений.

## **2. ЗАДАНИЕ**

Ознакомиться с теоретическим материалом. Найти открытый и закрытый ключи, и зашифровать сообщение. Выполнить расшифрование с применением секретного ключа.

## **3. ПОРЯДОК ВЫПОЛНЕНИЯ РАБОТЫ**

1. Получить задание.
2. Изучить теоретическую часть.
3. Выполнить задание под номером, соответствующим номеру по журналу.
4. Составить отчет.

## **4. СОДЕРЖАНИЕ ОТЧЕТА**

1. Титульный лист.
2. Краткая теория.
3. Расчет системы с открытым ключом.
4. Зашифрование сообщения.
5. Расшифровка.
6. Вывод.

## 5. ТЕОРЕТИЧЕСКАЯ ЧАСТЬ

### 5.1. Введение

Наряду с традиционным шифрованием на основе секретного ключа в последние годы все большее признание получают системы шифрования с открытым ключом. В таких системах используются два ключа. Информация шифруется с помощью открытого ключа, а расшифровывается с использованием секретного ключа. В настоящее время наиболее эффективным и распространенным алгоритмом шифрования с открытым ключом является алгоритм RSA. Алгоритм RSA был предложен в 1978 году (Райвест-Шамир-Адлеман).

Надежность алгоритма основывается на трудности вычисления дискретных логарифмов.

В криптосистеме RSA открытый ключ  $e$ , секретный ключ  $d$ , сообщение  $M$  и криптограмма  $C$  принадлежат множеству целых чисел  $Z = \{0, 1, 2, \dots, N-1\}$ , где  $N = P * Q$ .

Здесь  $P$  и  $Q$  - случайные большие простые числа.

Для обеспечения максимальной безопасности выбирают  $P$  и  $Q$  равной длины и хранят в секрете.

Множество  $Z$  с операциями сложения и умножения по модулю  $N$  образует арифметику по модулю  $N$ .

Открытый ключ  $e$  выбирают случайным образом так, чтобы выполнялись условия:

$$1 < e < \varphi(N), \quad \text{НОД}(\varphi(N), e) = 1, \quad \varphi(N) = (P-1)(Q-1)$$

где  $\varphi(N)$ - функция Эйлера.

Функция Эйлера  $\varphi(N)$  указывает количество положительных целых чисел в интервале от 1 до  $N$ , которые взаимно просты с  $N$ .

Второе из указанных выше условий означает, что открытый ключ  $e$  и функция Эйлера  $\varphi(N)$  должны быть взаимно простыми.

Далее, используя соответствующий алгоритм, в том числе расширенный алгоритм Евклида, вычисляют секретный ключ  $d$  такой, что

$$e \cdot d = 1 \pmod{\varphi(N)}$$

Это можно осуществить, так как получатель  $B$  знает пару простых чисел  $(P, Q)$  и может легко найти  $\varphi(N)$ .

Открытый ключ  $e$  используют для шифрования данных, а секретный ключ  $d$ - для расшифрования.

Процедура шифрования определяет криптограмму  $C$  для сообщения  $M$  в соответствии со следующей формулой:

$$C = E_e(M) = M^e \pmod{N}$$

При реализации операции возведения в степень можно использовать коммутативность, ассоциативность и дистрибутивность модулярной арифметики, позволяющие возведение в степень представить рядом последовательных умножений с приведением по модулю, т.е.

$$M^e \pmod{N} = (\dots((R^{k_1}) \pmod{N})^{k_2} \dots)^{k_s} \pmod{N},$$

Где  $e = k_1 * k_2 * \dots * k_s$

Обращение функции  $C=M^e(\text{mod}N)$ , т.е. определение значения  $M$  по известным значениям  $C$ ,  $e$  и  $N$ , практически не осуществимо при  $N>2^{512}$ .

Однако обратную задачу, т.е. задачу расшифрования криптограммы  $C$ , можно решить, используя пару (секретный ключ  $d$ ,  $N$ ) по следующей формуле:

$$M= D_d(C)= C^d(\text{mod}N)$$

Таким образом, получатель  $B$ , который создает криптосистему, защищает два параметра: 1) секретный ключ  $d$  и 2) пару чисел  $(P,Q)$ , произведение которых дает значение модуля  $N$ .

С другой стороны, получатель  $B$  открывает значение модуля  $N$  и открытый ключ  $e$ .

Противнику известны лишь значения  $e$  и  $N$ . Если бы он смог разложить число  $N$  на множители  $P$  и  $Q$ , то он смог бы определить значение секретного ключа  $d$ .

Однако, как уже отмечалось, разложение очень большого  $N$  на множители вычислительно не осуществимо (при условии, что длины выбранных  $P$  и  $Q$  составляют не менее 100 десятичных знаков).

## **5.2. Алгоритмы шифрования и расшифровки в криптосистеме RSA**

Предположим, что пользователь  $A$  хочет передать пользователю  $B$  сообщение в зашифрованном виде, используя криптосистему

RSA. В таком случае пользователь А выступает в роли отправителя сообщения, а пользователь В в роли получателя. Как отмечалось выше, криптосистему RSA должен сформировать получатель сообщения, т.е. пользователь В. Рассмотрим последовательность действий пользователя В и пользователя А.

1. Пользователь В выбирает два произвольных больших простых числа P и Q.

2. Пользователь В вычисляет значение модуля

$$N = P * Q.$$

3. Пользователь В вычисляет функцию Эйлера

$$\varphi(N) = (P-1)(Q-1)$$

и выбирает случайным образом значение открытого ключа e с учетом выполнения условий:

$$1 < e < \varphi(N), \text{ НОД}(\varphi(N), e) = 1$$

4. Пользователь В вычисляет значение секретного ключа d, используя соответствующий алгоритм для решения уравнения вида:

$$e * d = 1 \pmod{\varphi(N)}$$

5. Пользователь В пересылает пользователю А пару чисел (N, e) по незащищенному каналу.



6. Пользователь А разбивает исходный открытый текст М на блоки, каждый из которых может быть представлен в виде числа

$$M_i = 0, 1, 2, \dots, N-1.$$

7. Пользователь А шифрует текст, представленный в виде последовательности чисел  $M_i$  по формуле

$$C_i = M_i^e \pmod{N}$$

и отправляет криптограмму  $C_i$  ( $i=1 \dots$ ) пользователю В.

8. Пользователь В расшифровывает принятую криптограмму  $C_i$  ( $i=1 \dots$ ) используя секретный ключ  $d$ , по формуле

$$M_i = C_i^d \pmod{N}$$

В результате будет получена последовательность чисел  $M_i$  - которые представляют собой исходное сообщение М. Чтобы алгоритм RSA имел практическую ценность, необходимо иметь возможность без существенных затрат генерировать большие простые числа, уметь оперативно вычислять значения ключей  $e, d$ .

### **Пример.**

Пусть необходимо зашифровать сообщения САВ.

Для простоты вычислений будут использоваться небольшие числа. На практике применяются очень большие числа.

### **Действия пользователя В.**

1. Выбирает  $P = 3$  и  $Q = 11$ .

2. Вычисляет модуль  $N = P * Q = 3 * 11 = 33$ .

3. Вычисляет значение функции Эйлера для  $N = 33$ :

$$\varphi(N) = (P - 1)(Q - 1) = 2 * 10 = 20.$$

Выбирает в качестве открытого ключа  $e$  произвольное число с учетом выполнения условий:

$$1 < e < 20 \text{ НОД}(e, 20) = 1. \text{ Пусть } e = 7.$$

4. Вычисляет значение секретного ключа  $k$ , используя уравнение

$$e * d = 1 \pmod{20}$$

Решение дает  $d = 3$ .

5. Пересылает пользователю  $A$  пару чисел ( $N = 33, e = 7$ ).

**Действия пользователя  $A$ .**

6. Представляет шифруемое сообщение как последовательность целых чисел в диапазоне  $0 \dots 32$ . Пусть буква  $A$  представляется как число 1, буква  $B$  - как число 2, буква  $C$  - как число 3.

Тогда сообщение  $СAB$  можно представить как последовательность чисел 3,1,2, т.е.  $M_1 = 3, M_2 = 1, M_3 = 2$ .

7. Шифрует текст, представленный в виде последовательности чисел  $M_1, M_2$  и  $M_3$ , используя ключ  $d = 7$  и  $N = 33$ , по формуле

$$C_j = M_i \pmod{33}.$$

Получаем:

$$C_1 = 3^7 \pmod{33} = (3^3 \pmod{33} * 3^4 \pmod{33}) \pmod{33} = \\ = (27 * 81 \pmod{33}) \pmod{33} = (27 * 15) \pmod{33} = 405 \pmod{33} = 9.$$

$$C_2 = 1^7 \pmod{33} = 1 \pmod{33} = 1,$$

$$C_3 = 2^7 \pmod{33} = 128 \pmod{33} = 29.$$

Отправляет пользователю В криптограмму

$$C_1, C_2, C_3 = 9, 1, 29.$$

### **Действия пользователя В:**

8. Расшифровывает принятую криптограмму  $C_1, C_2, C_3$ , используя секретный ключ  $k, = 3$ . по формуле  $M_i = C_i \pmod{33}$ :

$$M_1 = 9^3 \pmod{33} = (9^2 \pmod{33} * 9) \pmod{33} = ((81) \pmod{33} * 9) \pmod{33} \\ = (15 * 9) \pmod{33} = 135 \pmod{33} = 3$$

$$M_2 = 1^3 \pmod{33} = 1$$

$$M_3 = 29^3 \pmod{33} = ((29^2 \pmod{33} * 29) \pmod{33} = \\ = ((841) \pmod{33} * 29) \pmod{33} = (16 * 29) \pmod{33} = (464) \pmod{33} = 2$$

Таким образом, восстановлено исходное сообщение: САВ

## 6. ПРАКТИЧЕСКИЕ ЗАДАНИЯ

Используя теоретический материал зашифруйте и расшифруйте свою фамилию. Два простых числа брать из таблицы согласно вариантам. Для удобства шифрования используйте Таблицу – 2.

Таблица 1 – Индивидуальные задания

№	Простые числа	
1.	11	23
2.	7	31
3.	17	19
4.	5	29
5.	31	2
6.	13	37
7.	2	13
8.	3	19
9.	41	23
10.	7	37
11.	43	11
12.	19	13
13.	53	41
14.	29	19
15.	31	11
16.	47	23
17.	17	5
18.	59	7
19.	2	37
20.	29	47
21.	59	5
22.	19	23
23.	31	17
24.	5	61
25.	11	41
26.	19	29
27.	23	17
28.	67	29
29.	13	41
30.	29	47

Таблица 2 – Кодировка русского алфавита

А	0
Б	1
В	2
Г	3
Д	4
Е	5
Ё	6
Ж	7
З	8
И	9
Й	10
К	11
Л	12
М	13
Н	14
О	15
П	16
Р	17
С	18
Т	19
У	20
Ф	21
Х	22
Ц	23
Ч	24
Ш	25
Щ	26
Ъ	27
Ы	28
Ь	29
Э	30
Ю	31
Я	32

## **7. КОНТРОЛЬНЫЕ ВОПРОСЫ**

1. Дайте определение алгоритмов с открытым ключом.
2. Какие этапы содержит асимметричный алгоритм?
3. В чем заключается вычисление ключей алгоритма RSA?
4. Как происходит шифрование в алгоритме RSA?
5. Как происходит расшифрование в алгоритме RSA?

## **8. СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ И ЛИТЕРАТУРЫ**

1. Н. Смарт. Криптография [текст] Издательство: М.: Техносфера, 2005. – 528 с.
2. Сингх С. Книга шифров. Тайная история шифров и их расшифровки.[текст] М.: Аст, Астрель, 2006. 447 с.
3. Бауэр Ф. Расшифрованные секреты. Методы и принципы криптологии.[текст] М.: Мир, 2007. 550 с.