Автор:

Швейкин Владислав Витальевич

студент

ФГАОУ ВО «Самарский национальный

исследовательский университет

им. академика С.П. Королева»

г. Самара, Самарская область

АЛГОРИТМ ШИФРОВАНИЯ RSA

Аннотация*: в данной статье демонстрируется принцип работы алгоритма шифрования RSA.*

Ключевые слова*: теория чисел, ассиметричное шифрование, RSA, ключи.*

Генерация ключей

1. Возьмем два случайных простых числа p, q, такие что $p \neq q$. Для обеспечения безопасности они должны быть одного порядка.

2. Посчитаем произведение $n = p \cdot q$ и функцию Эйлера $\varphi(n) = (p-1) \cdot (q-1)$.

3. Выберем случайное целое число $e(1 < e < \varphi(n))$, которое будет взаимно простым со значением функции Эйлера $\varphi(n)$, т.е. $НОД(e, \varphi(n)) = 1$. Пара $\{e, n\}$ называется открытым ключом.

4. Вычислим число $d(1 < d < n)$, обратное к числу e по модулю $\varphi(n)$. То есть $d \cdot e \equiv 1 (\mathrm{mod}\, \varphi(n))$. Пара $\{d, n\}$ называется закрытым ключом.

Алгоритм шифрования

1. Чтобы зашифровать сообщение m нужно разбить его на блоки, длина которых меньше n.

2. С помощью открытого ключа $\{e, n\}$, шифруем все блоки сообщения по формуле $c_i = enc(m_i) = m_i^e \bmod n$

3. Полученное зашифрованное сообщение *c* будет состоять из блоков c_i той же самой длины.

Алгоритм дешифрования

1. Для зашифрованного блока c_i и используя закрытый ключ $\{d, n\}$ вычислим $m_i = c_i^d \bmod n$. Операция восстановления исходного сообщения опирается на теорему Эйлера: $c_i^d = (m_i^e)^d = m_i^{k\cdot\varphi(n)+1} = m_i \cdot m_i^{k\cdot\varphi(n)} = m_i \cdot 1^k = m_i$

2. Преобразуем цифровые блоки в исходное сообщение.

Пример работы алгоритма

Генерация ключей:

1. Возьмем два случайных простых числа $p = 47, q = 53$.

2. Посчитаем произведение $n = 47 \cdot 53 = 2491$, функция Эйлера $\varphi(n) = (47-1)\cdot(53-1) = 46 \cdot 52 = 2392$.

3. Выберем случайное целое число $e = 71 (1 < 71 < 2392)$, $НОД(71,2392) = 1$. Пара $\{71,2491\}$ будет являться открытым ключом шифрования алгоритма RSA.

4. Используя расширенный алгоритм Евклида, вычислим число *d*, обратное к числу 71 по модулю 2392. В первых двух столбцах таблицы запишем числа, для которых необходимо найти наибольший общий делитель, для нашей задачи это *A*=2392 и *B* = 71. Третий столбец содержит остаток от деления *A* на *B*. Четвертый – целая часть от деления *A* на *B*. После заполнения первых четырех столбцов, наибольшим общим делителем будет являться последний остаток отличный от нуля, то есть $НОД(71,2392) = 1$. Начнем заполнять последние два столбца, содержащие *X* и *Y* с конца. В последнюю строчку запишем *X*=0 и *Y*=1. Затем, зная значения x_{i+1} и y_{i+1}, последовательно найдем x_i и y_i по формулам: $x_i = y_{i+1}$, $y_i = x_{i+1} - y_{i+1} \cdot (A div B)$, где *A div B = [A/B]*- целая часть от деления A на B.

Таблица 1

Демонстрация расширенного алгоритма Евклида

A	*B*	*A mod B*	*[A/B]*	*X*	*Y*
2392	71	49	33	29	–977
71	49	22	1	–20	29
49	22	5	2	9	–20
22	5	2	4	–2	9
5	2	1	2	1	-2
2	1	0	2	0	1

Обратным элементом будет являться y = –977, $d = y \bmod \varphi(n) = -977 \bmod 2392 = 1415$. Пара $\{1415,2491\}$ будет в качестве закрытого ключа алгоритма RSA.

Шифрование: в качестве сообщения для примера работы алгоритма RSA выберем: «*самарский университет*».

1. Представим каждую букву алфавита её порядковым номером.

Таблица 2

Сопоставление буквы алфавита и её порядкового номера

$m_1 = 'с' = 19$	$m_2 = 'а' = 1$	$m_3 = 'м' = 14$
$m_4 = 'а' = 1$	$m_5 = 'р' = 18$	$m_6 = 'с' = 19$
$m_7 = 'к' = 12$	$m_8 = 'и' = 10$	$m_9 = 'й' = 11$
$m_{10} = ' ' = 34$	$m_{11} = 'у' = 21$	$m_{12} = 'н' = 15$
$m_{13} = 'и' = 10$	$m_{14} = 'в' = 3$	$m_{15} = 'е' = 6$
$m_{16} = 'р' = 18$	$m_{17} = 'с' = 19$	$m_{18} = 'и' = 10$
$m_{19} = 'т' = 20$	$m_{20} = 'е' = 6$	$m_{21} = 'т' = 20$

2. С помощью закрытого ключа $\{71,2491\}$, зашифруем все блоки сообщения.

Таблица 3

Результат шифрования

$c_1 = 19^{71} \bmod 2491 = 2224$	$c_2 = 1^{71} \bmod 2491 = 1$	$c_3 = 14^{71} \bmod 2491 = 2358$
$c_4 = 1^{71} \bmod 2491 = 1$	$c_5 = 18^{71} \bmod 2491 = 1311$	$c_6 = 19^{71} \bmod 2491 = 2224$
$c_7 = 12^{71} \bmod 2491 = 285$	$c_8 = 10^{71} \bmod 2491 = 1639$	$c_9 = 11^{71} \bmod 2491 = 1289$
$c_{10} = 34^{71} \bmod 2491 = 1062$	$c_{11} = 21^{71} \bmod 2491 = 1381$	$c_{12} = 15^{71} \bmod 2491 = 1561$
$c_{13} = 10^{71} \bmod 2491 = 1639$	$c_{14} = 3^{71} \bmod 2491 = 1889$	$c_{15} = 6^{71} \bmod 2491 = 2104$
$c_{16} = 18^{71} \bmod 2491 = 1311$	$c_{17} = 19^{71} \bmod 2491 = 2224$	$c_{18} = 10^{71} \bmod 2491 = 1639$
$c_{19} = 20^{71} \bmod 2491 = 164$	$c_{20} = 6^{71} \bmod 2491 = 2104$	$c_{21} = 20^{71} \bmod 2491 = 164$

3. Представим зашифрованное сообщение в виде последовательности блоков:

$$c = \{2224, 1, 2358, 1, 1311, 2224, 285, 1639, 1289, 1062, 1381, 1561, 1639, 1889, 2104, 1311, 2224, 1639, 164, 2104, 164\}.$$

Дешифрование:

1. С помощью закрытого ключа $\{1415,2491\}$, расшифруем последовательно все блоки сообщения:

$$c = \{2224, 1, 2358, 1, 1311, 2224, 285, 1639, 1289, 1062, 1381, 1561, 1639, 1889, 2104, 1311, 2224, 1639, 164, 2104, 164\}.$$

.

Таблица 4

Результат дешифрования

$m_1 = 2224^{1415} \bmod 2491 = 19$	$m_2 = 1^{1415} \bmod 2491 = 1$	$m_3 = 2358^{1415} \bmod 2491 = 14$
$m_4 = 1^{1415} \bmod 2491 = 1$	$m_5 = 1311^{1415} \bmod 2491 = 18$	$m_6 = 2224^{1415} \bmod 2491 = 19$
$m_7 = 285^{1415} \bmod 2491 = 12$	$m_8 = 1639^{1415} \bmod 2491 = 10$	$m_9 = 1289^{1415} \bmod 2491 = 11$
$m_{10} = 1062^{1415} \bmod 2491 = 34$	$m_{11} = 1381^{1415} \bmod 2491 = 21$	$m_{12} = 1561^{1415} \bmod 2491 = 15$
$m_{13} = 1639^{1415} \bmod 2491 = 10$	$m_{14} = 1889^{1415} \bmod 2491 = 3$	$m_{15} = 2104^{1415} \bmod 2491 = 6$
$m_{16} = 1311^{1415} \bmod 2491 = 18$	$m_{17} = 2224^{1415} \bmod 2491 = 19$	$m_{18} = 1639^{1415} \bmod 2491 = 10$
$m_{19} = 164^{1415} \bmod 2491 = 20$	$m_{20} = 2104^{1415} \bmod 2491 = 6$	$m_{21} = 164^{1415} \bmod 2491 = 20$

2. После преобразования порядковых номеров букв алфавита в текст, восстановим первоначальное сообщение: «*самарский университет*».

Список литературы

1. Шнайер Б.М. Прикладная криптография / Б.М. Шнайер – ТРИУМФ, 2002. – 816 с.