Защита информации. Лабораторная работа №2

RSA относится к асимметричным шифрам. В асимметричных шифрах используются два ключа – открытый и закрытый, которые создаются получателем сообщения. Открытые ключи доступны всем желающим и передаются по незащищённому каналу связи. Отправляемое сообщение шифруется открытым ключом получателя. Дешифрируется сообщение при его получении закрытым ключом получателя. Обратим внимание, что дешифрировать сообщение не может даже отправитель, что и не требуется. Открытый и закрытый ключи математически связаны друг с другом таким образом, что сообщение, зашифрованное одним ключом из пары, можно дешифрировать только вторым ключом из этой же пары ключей.

RSA использует разложение больших чисел (несколько сот разрядов) на простые множители, что требует большого объема вычислений и эта особенность определяет стойкость данного шифра.

Первым этапом асимметричного шифрования является создание получателем шифрограмм пары ключей. Процедура создания ключей RSA заключается в следующем:

- Выбирается два простых числа p и q, например p = 7 и q = 13
- Вычисляется произведение n = p * q, в нашем примере n = 7 * 13 = 91
- Вычисляется функция Эйлера ϕ(n): ϕ(n) = (p - 1) * (q - 1)

В нашем примере ϕ(n) = (7 - 1) * (13 - 1) = 72. Функция Эйлера определяет количество целых положительных чисел, не превосходящих n и взаимно простых с n.

Справка. Целые числа называются взаимно простыми, если они не имеют никаких общих делителей, кроме 1.

Выбирается произвольное целое e: 0 < e < n взаимно простое с значением функции Эйлера ϕ(n). В нашем примере возьмём e = 5. Пара чисел (e, n) объявляется открытым ключом шифра. В нашем примере (e, n) = (5, 91)

Вычисляется целое число d из соотношения: (d * e) mod ϕ(n) = 1.

Справка. Операция mod вычисляет остаток от целочисленного деления двух чисел.

Это соотношение означает, что результатом деления произведения чисел e и d на значение функции Эйлера должно быть число 1. Поэтому d можно рассчитать по формуле: d = (k * ϕ(n) + 1) / e, придавая k последовательно значения 1, 2, 3, … до тех пор, пока не будет получено целое число d.

Найдём d в рассматриваемом примере: d = (k * 72 + 1) / 5, при k = 1, d – не целое, при k = 2, d = 29. Пара чисел (d, n) будет закрытым ключом шифра. В нашем примере (d, n) = (29, 91).

RSA-шифрование сообщения T выполняется с помощью открытого ключа получателя (e, n) по формуле:

$$C_i = T_i^e \bmod n$$

где Ti и Ci числовые эквиваленты символов исходного и зашифрованного сообщений.

Числовые эквиваленты русских букв, цифр и символа пробела

1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**	**17**	**18**	**19**	**20**	**21**	**22**	**23**
А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х

24	**25**	**26**	**27**	**28**	**29**	**30**	**31**	**32**	**33**	**34**	**35**	**36**	**37**	**38**	**39**	**40**	**41**	**42**	**43**	**44**
Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	_	0	1	2	3	4	5	6	7	8	9

Рассмотрим пример шифрования RSA. Зашифруем сообщение «КАФСИ» с помощью открытого ключа (5, 91).

Вычисление шифрограммы:

Символы исходного сообщения, T_i	**Коды символов T_i**	**Зашифрованные коды символов C_i**
К	12	$12^5 \bmod 91 = 38$
А	1	$1^5 \bmod 91 = 1$
Ф	22	$22^5 \bmod 91 = 29$
С	19	$19^5 \bmod 91 = 80$
И	10	$10^5 \bmod 91 = 82$

Таким образом, мы исходное сообщение «КАФСИ» представили в виде шифрограммы «38, 1, 29, 80, 82».

Расшифровка RSA-закодированного сообщения T выполняется с помощью закрытого ключа получателя (d, n) по формуле:

$$T_i = C_i^d \bmod n$$

Рассмотрим пример восстановления исходного сообщения. В предыдущем примере была получена пара ключей и шифрограмма «38, 1, 29, 80, 82», созданная открытым ключом данной пары. Восстановим исходное сообщение, применив закрытый ключ (d, n) = (29, 91) той же пары

Восстановление сообщения:

Зашифрованные коды символов C_i	**Дешифрованные коды символов T_i**	**Символы исходного сообщения, T_i**
38	$38^{29} mod\ 91 = 12$	К
1	$1^{29} mod\ 91 = 1$	А
29	$29^{29} mod\ 91 = 22$	Ф
80	$80^{29} mod\ 91 = 19$	С
82	$82^{29} mod\ 91 = 10$	И

Таким образом, мы восстановили исходное сообщение «КАФСИ».

Задание

Написать программу на любом языке программирования, реализующую шифрование и расшифровывание RSA. Выполнить проверку.