УКАЗАНИЕ К РЕШЕНИЮ ЗАДАЧИ № 32

Алгоритм RSA был разработан в 1977 году Роном Ривестом, Ади Шамиром и Леном Адлеманом и опубликованный в 1978 году. С тех пор алгоритм Rivest-Shamir-Adleman (RSA) широко применяется практически во всех приложениях, использующих криптографию с открытым ключом.

Алгоритм RSA состоит из трех этапов:

I. *Вычисление ключей*

Важным моментом в этом криптоалгоритме является создание пары ключей: открытого и закрытого. Для алгоритма RSA этап создания ключей состоит из следующих операций:

1. Выбираются два простых числа p и q. Вычисляется их произведение n=p*q, называемое модулем.
2. Вычисляется функция Эйлера Ф(n)=(p - 1)*(q - 1).
3. Выбирается произвольное число e (e <n), такое, что 1< e <Ф(n) и не имеет общих делителей кроме 1 (взаимно простое) с числом (p - 1)*(q - 1).
4. Вычисляется d методом Евклида таким образом, что (e*d - 1) делится на (p - 1)*(q - 1).
5. Два числа (e, n) - публикуются как открытый ключ.
6. Число d хранится в секрете - закрытый ключ есть пара (d, n), который позволит читать все послания, зашифрованные с помощью пары чисел (e, n).

II. *Шифрование*

Шифрование с помощью этих чисел производится так:

- Отправитель разбивает свое сообщение на блоки, равные $k=[\log_2(n)]$ бит, где квадратные скобки обозначают, взятие целой части от дробного числа.
- Подобный блок может быть интерпретирован как число из диапазона (0;2k-1). Для каждого такого числа m_i вычисляется выражение (c_i – зашифрованное сообщение): $c_i = ((m_i)^e) \bmod n$

III. *Дешифрование*

Чтобы получить открытый текст надо исходный зашифрованный текст разбить на блоки, со значением каждого блока c_i < n. Каждый блок дешифруется отдельно: $m_i = ((c_i)^d) \bmod n$

Пример:

Выбрать два простых числа: p = 7, q = 17.

Вычислить n = p·q = 7 · 17 = 119.

Вычислить Φ(n) = (p - 1)·(q - 1) = 96.

Выбрать e так, чтобы e было взаимнопростым с Φ(n) = 96 и меньше, чем Φ(n): e = 5.

Определить d так, чтобы d·e ≡ 1 mod 96 и d < 96.

d = 77, так как 77 · 5 = 385 = 4 · 96 + 1.

Результирующие ключи открытый {5, 119} и закрытый ключ {77, 119}.

Например, требуется зашифровать сообщение M = 19.

$19^5 = 66 \pmod{119}$; C = 66.

Для дешифрования вычисляется $66^{77} \pmod{119} = 19$.