МАТЕРИАЛЫ К ЗАДАНИЮ №33 – RSA

Постановка задачи

Пусть $M = (m_0, m_1, \ldots, m_{t-1})$ – сообщение длины $t \in \mathbb{N}$, причём для каждого $i \in \overline{0, t-1}$ символ m_i имеет шестнадцатеричный ASCII-код, который будем обозначать $\mathrm{Ord}(m_i)$. В итоге сообщению M ставится в соответствие число

$$\mathrm{Ord}(m_{t-1}) \parallel \ldots \parallel \mathrm{Ord}(m_1) \parallel \mathrm{Ord}(m_0),$$

где $\parallel$ – символ конкатенации, то есть склеивания битовых последовательностей. К примеру, в предложении «abcd» символ «a» имеет ASCII-код 97 (или `0x61`), символ «b» – 98 (или `0x62`), символ «c» – 99 (или `0x63`), символ «d» – 100 (или `0x64`). Значит, этому предложению будет соответствовать шестнадцатеричное число `0x64636261`, которое в десятичной системе счисления записывается в виде 1684234849.

Каждое сообщение, зашифрованное с помощью криптосистемы RSA, в числовом представлении не должно превосходить значение ключевого параметра n. В противном случае сообщение разбивается на блоки подходящего размера, каждый из которых зашифровывается отдельно.

В распоряжении криптоаналитика имеются:

- пара чисел (e, n), соответствующих открытому ключу криптосистемы RSA;
- перехваченные блоки закрытого текста y.

$$n = 267298839230019791365144 7, \qquad e = 4238573701454021.$$

y: `0x867947ad1c6669d89d34` `0x17916fede74b1b7981e28` `0x8c151209020f7e476d3`
`0x6c4df621e08ab7277f29` `0x1f25314e30c21bbb9dba0` `0x45f283ae4c71f6cf6cac`
`0xd6cb28d14feae8ed8963` `0xe8978892d61f2d224e99` `0x232cb22631c05989dda9e`
`0x20d40266dd38451d26e60` `0x13988148bb1b5657af27d` `0x19703e0af8b9e9b53515c`
`0x4a55ae7434f2de9218b9` `0xddf382f4ea9b8a02c26` `0x12a601ccf227c77930ca4`
`0xe77e47b69ff418a38fe7` `0x31472ec336a89f3db7e8` `0x1883c628204d4196baf11`

Необходимо выполнить следующее:

- изучить и описать схему работы криптосистемы RSA;
- написать программную реализацию RSA на языке программирования C или Python, способную работать с числами произвольной разрядности;
- изучить и описать метод Ферма факторизации целых чисел;
- написать программную реализацию метода Ферма на языке программирования C или Python, способную работать с числами произвольной разрядности;
- по известному открытому ключу (e, n) криптосистемы RSA определить закрытый ключ (d, n) и с его помощью восстановить открытый текст x, из которого был получен закрытый текст y.

Полезные источники

1. *Глухов М.М., Круглов И.А., Пичкур А.Б., Черемушкин А.В.* Введение в теоретико-числовые методы криптографии: Учебное пособие. – СПб.: Издательство «Лань», 2011.
   Здесь, помимо очевидно необходимого описания метода Ферма, излагается алгоритм извлечения квадратного корня, который понадобится реализовать на определённом этапе работы.
2. *Лось А.Б, Нестеренко А.Ю., Рожков М.И.* Криптографические методы защиты информации: учебник для академического бакалавриата. – 2-е изд., испр. – М.: Издательство Юрайт, 2019.
3. *Черемушкин А.В.* Лекции по арифметическим алгоритмам в криптографии. – М.: МЦНМО, 2002.