МАТЕРИАЛЫ К ЗАДАНИЮ №39 – 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.

$$n = 255081667482450882716008 61, \qquad e = 11364049842347741.$$

y: `0xadc8198c1a51562961468` `0x413909848693963805d4` `0xb8c13411d961af934488b`
`0xe8a8d33c46f511d86219b` `0xe09cb1063b1c4ba8b9560` `0xddf6e0aee5f67840143ec`
`0xccea41765ec8df737e2c9` `0x142ada6b184ad1303a407f` `0x2ec377d1c840c73a8bff5`
`0x8ecc404b166d5f723447` `0x62e8ddc672b121d8c78bd` `0x59bf8e958c97da877764e`
`0xf28ee76de8bd5b3f55d8` `0x130b59f6d938dd5c1af6de` `0x61d818d3a77c6332ab3df`
`0x33c8821cd86d3a6685eef` `0x1be3931ce4f221638d75c` `0x623a46f24a40796e4e358`

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.