Домашнее задание №7
Алгоритмы. 5 курс. Весенний семестр.

Горбунов Егор Алексеевич

30 марта 2016 г.

Задание №1 Алёна отправила сообщение m, зашифрованное через RSA, двум людям. Для каждого человека определено своё e_i , но везде одинаковое $n = pq$, Оказалось, что e_i взаимно простые. Найдите сообщение Алёны за $\mathcal{O}\left(poly(\log n)\right)$.

Решение: Раз e_1 и e_2 взаимнопросты, то расширенный алгоритм Евклида даст нам такие a и b, что:

$$ae_1 + be_2 = 1$$

Окей, тогда можем записать:

$$m = m^1 = m^{ae_1+be_2} = (m^{e_1})^a (m^{e_2})^b$$

Нам известны m^{e_1} и m^{e_2}, а значит посчитать $(m^{e_1})^a (m^{e_2})^b$ мы сумеем используя арифметические операции по модулю n. Если a, например, оказалось отрицательным, то тоже не проблема, т.к. $x^{-|a|} = (x^{-1})^{|a|}$, далее находим обратный по модулю и вперёд...

Ясно, что эти операции укладываются в $\mathcal{O}\left(poly(\log n)\right)$. ■

Задание №2

(a) Пусть $n = pq$ и известно $\varphi(n)$, разложите n на множители. $\mathcal{O}\left(poly(\log n)\right)$.

(b) Пусть вам дано $RSA(n = pq, e, d)$. Пусть $e = 3$. Разложите n на множители.

Решение:

(a) Имеем: $\varphi(n) = (p-1)(q-1) = pq - p - q - 1 = n - p - q - 1$, откуда:

$$\begin{cases} p = n - q - \varphi(n) - 1 \\ n = pq \end{cases} \Rightarrow \begin{cases} p = n - q - \varphi(n) - 1 \\ q^2 - q(n - \varphi(n) - 1) + n = 0 \end{cases}$$

Решаем квадратное уравнение, разумеется, за $\mathcal{O}\left(poly(\log n)\right)$ и подставляем полученное q в первое уравнение системы, чтобы получить p. ■

(b) По построению RSA у нас $3d-1 = 0 \mod \varphi n$, т.е. это значит, что $3d-1 = k\varphi(n)$, $\varphi(n) = \frac{3d-1}{k}$. Переберём k и будем искать решение квадратного уравнения из предыдущего пункта, пока не найдём целочисленного решения. ■

Задание №4 Придумайте, как свести вычисление FFT последовательности размера pn к p вычислениям FFT от последовательностей размера n и $\mathcal{O}(p^2 * n)$ дополнительных арифметических операций. Напишите псевдокод.

Решение: Можно рассмотреть p полиномов вида: $f_i(x) = \sum_{k=0}^{n-1} a_{pk+i}x^k$. Тогда полином, соответствующий исходной последовательности будет такой:

$$f(x) = \sum_{k=0}^{p-1} f_k(x^p)x^k$$

```
def ALG(a[n*p]):
   for i in [0, 1, 2, 3, ..., p-1]:
      fft[i] = FFT(a[i], a[i+p], a[i+2*p], ..., a[i+(n-1)*p])
   for i in [0, 1, 2, 3, ..., np-1]:
      for k in [0, 1, ..., p-1]:
         j = (-i * k) mod n*p
         answer[i] = answer[i] + (j-th power of n-th root of 1) * fft[k][i % n]
```

Как-то так... ■

Задание №6 Заданы картинка a и образец p в виде матриц вещественных чисел из $[0,1]$ размерами n × n и $k \times k$ соответственно $(n \geq k)$. Требуется найти позицию $(x,y), 0 \leq x \leq n-k, 0 \leq y \leq n-k$, для которой:

$$\sum_{i=0}^{k-1}\sum_{j=0}^{k-1}\left(p_{i,j} - a_{(y+i),(x+j))}\right)^2 \longrightarrow \min$$

за время $\mathcal{O}(n^2 \log n)$

Решение: Раскрывая квадрат сумма разбивается на 3 слагаемых: сумма квадратов пикселей образца, сумма квадратов подматрицы картинки и скалярное произведение двух веторов длины k^2. Первое считаем в лоб, второе с использованием предподсчёта на «префиксах» матрицы, а третье сводим к вычислению всевозможных скалярных произведений на циклические сдвиги (emaxx говорит, что это делается за $\mathcal{O}(n^2 \log n)$) ■