Основные алгоритмы 7

Ковалев Алексей

1. Для начала найдем закрытые ключи Алисы и Боба:
$(e_A, n_A) = (107, 187)$ – открытый ключ Алисы $\Rightarrow (d_A, n_A) = (143, 187)$ – закрытый ключ Алисы.
$(e_B, n_B) = (7, 253)$ – открытый ключ Боба $\Rightarrow (d_B, n_B) = (63, 253)$ – закрытый ключ Боба.
Отсюда зашифрованное сообщение c для изначального сообщения $m = 17$:

$$c = m^{e_B} = 17^{63} \equiv 51 \mod 253$$

Подпись Алисы для данного сообщения:

$$s = m^{d_A} = 17^{143} \equiv 51 \mod 187$$

Ответ: $c = 51 \mod 253$ – зашифрованное сообщение,
$s = 51 \mod 187$ – подпись для данного сообщения.

2. Подписанное M сообщение s_y будет выглядить как $s_y \equiv (r^e x)^d \equiv rx^d \mod n$. Тогда получить правильную подпись s сообещения x можно так: $s \equiv s_y \cdot r^{-1} \equiv r \cdot r^{-1} \cdot x^d \equiv x^d \mod n$.

3. Открытые ключи всех друзей Алисы равны 3, значит значит она отправит им сообщения

$$m^3 \mod N_1$$
$$m^3 \mod N_2$$
$$m^3 \mod N_3$$

Зная эту информацию, Ева может, пользуясь КТО, найти $M^3 \mod N_1N_2N_3$ полиномиально быстро. В силу того что число M имеет в своей двоичной записи n битов, число M^3 имеет в своей двоичной записи не более $3n$ битов и не менее $3n-2$ битов. Каждый из простых множителей чисел N_i имеет в своей записи n битов, значит $N_1N_2N_3$ имеет в своей записи от $6n-5$ до $6n$ битов. То есть длина двоичного числа M^3 точно меньше, чем длина $N_1N_2N_3$, значит $M^3 \mod N_1N_2N_3$ совпадает с M^3 в $\mathbb{R}$. Тогда мы можем найти M извлечением кубического корня из $M^3 \mod N_1N_2N_3$.

4. Пусть $N = pq$, где p, q – простые. Тогда $\varphi(N) = (p-1)(q-1) = pq - p - q + 1$. Если Ева будет использовать полный перебор для подбора d, то ей нужно будет перебрать не более $\varphi(N)$ чисел, каждый раз делая полиномиальное число действий. Если же она решила использовать вероятностный подход, выбирая случайное число от 2 до $N-1$, то ей нужно будет сделать не более N попыток. Причем для любых простых p и q

$$1 \geqslant \frac{\varphi(N)}{N} = \frac{pq - p - q + 1}{pq} = 1 - \frac{1}{q} - \frac{1}{p} + \frac{1}{pq} \geqslant \frac{1}{4}$$

То есть $\varphi(N) = \Theta(N)$ и $N = \Theta(\varphi(N))$. Отсюда математическое ожидание числа попыток X при случайном выборе

$$\mathbb{E}[X] = O(N)$$

Математическое ожидание числа попыток Y при полном переборе есть

$$\mathbb{E}[Y] = O(\varphi(N)) = O(N)$$

Значит алгоритм Евы не является более эффективным, чем полный пребор.

5. Будем проводить доказательство по индукции по m, то есть докажем, что на каждом шаге алгоритм возвращает случайное множество:
База $m = 0$ очевидна.
Переход: пусть алгоритм функция $\texttt{RandomSample}(m-1, n-1)$ вернула нам случайное $(m-1)$-элементное подмножество $(n-1)$-элементного множества. Докажем, что тогда каждое m-элементное подмножество n-элементного множество будет возвращено с равной вероятностью. Обозначи данное нам $(m-1)$-элементное подмножество за M. Посчитаем, сколькими способами можно получить множетсво $M \cup \{n\}$ после получения M на предыдущем шаге: его можно получить, если $\texttt{Random}(1, n)$ вернет нам число, которое уже есть в M или само число n, то есть всего m способов. Зафиксируем множество $M_0 = M \cup k$, где $k \neq n$. Множество M_0 на данном шаге можно получить, если на предыдущем шаге было получено любое его $(m-1)$-элементное, то есть $\binom{m}{m-1} = m$ способами. То есть получить любое множество можно m способами из предыдущих множеств. С учетом того, что все $(m-1)$-элементные подмножества на прошлом шаге возвращались равновероятно, все m-элементные подмножества также будут возвращаться равновероятно и случайно. $\square$

6. Введем величину $q_{i,j}$, равную вероятности того, что $X_{i,j,k} = 1$, полагая, что $i < j$

$$q_{i,j} = \begin{cases} \frac{1}{j-k+1} + \frac{1}{1-k+1} = \frac{2}{j-k+1}, & k < i < j \\ \frac{1}{k-i+1} + \frac{1}{k-i+1} = \frac{2}{k-i+1}, & i < j < k \\ \frac{1}{j-i+1} + \frac{1}{j-i+1} = \frac{2}{j-i+1}, & i \leqslant k \leqslant j \end{cases} \tag{1}$$

1. В новых терминах математическое ожидание $X_{i,j,k}$ можно выразить как

$$\mathbb{E}[X_{i,j,k}] = q_{i,j}$$

2. Математическое ожидание числа всех сравнений X_k можно выразить как

$$\mathbb{E}[X_k] = \sum_{i=1}^{k}\sum_{j=k}^{n}\frac{2}{j-i+1} + \sum_{i=1}^{k-2}\sum_{j=i+1}^{k-1}\frac{2}{k-i+1} + \sum_{i=k+1}^{n-1}\sum_{j=i+1}^{n}\frac{2}{j-k+1}$$

Обозначим слагаемые за A, B, C соответственно и преобразуем каждое из них в отдельности:

$$B = \sum_{i=1}^{k-2}\sum_{j=i+1}^{k-1}\frac{2}{k-i+1} = \sum_{i=1}^{k-2}(k-i-1)\frac{2}{k-i+1} = 2\sum_{i=1}^{k-2}\frac{k-i-1}{k-i+1}$$

$$C = \sum_{i=k+1}^{n-1}\sum_{j=i+1}^{n}\frac{2}{j-k+1} = \sum_{j=k+2}^{n}\sum_{i=k+1}^{j-1}\frac{2}{j-k+1} = \sum_{j=k+2}^{n}(j-k-1)\frac{2}{j-k+1} = 2\sum_{j=k+2}^{n}\frac{j-k-1}{j-k+1}$$

Отсюда

$$\mathbb{E}[X_k] \leqslant 2\left(\sum_{i=1}^{k}\sum_{j=k}^{n}\frac{1}{i-j+1} + \sum_{i=1}^{k-2}\frac{k-i-1}{k-i+1} + \sum_{j=k+2}^{n}\frac{j-k-1}{j-k+1}\right)$$

$\square$

3. Теперь оценим сверху каждое из слагаемых A, B, C:

$$\begin{aligned} A &= 2\sum_{i=1}^{k}\sum_{j=k}^{n}\frac{1}{j-i+1} = 2\sum_{j=k}^{n}\frac{1}{j} + 2\sum_{j=k}^{n}\frac{1}{j-1} + \ldots + 2\sum_{j=k}^{n}\frac{1}{j-k+1} = \\ &= 2\left(\frac{1}{k} + \frac{1}{k+1} + \ldots + \frac{1}{n}\right) + 2\left(\frac{1}{k-1} + \frac{1}{k} + \ldots + \frac{1}{n-1}\right) + \ldots + 2\left(1 + \frac{1}{2} + \ldots + \frac{1}{n-k+1}\right) = \\ &= 2(H_n - H_{k-1}) + 2(H_{n-1} - H_{k-2}) + \ldots + 2(H_{n-k+1} - 0) \end{aligned}$$

где H_i – среднее геометрическое первых i натуральных чисел, причем $\forall i \geqslant 2 \;\; \ln i \leqslant H_i < \ln i + 1$. Тогда

$$\begin{aligned} A &= 2(H_n - H_{k-1}) + 2(H_{n-1} - H_{k-2}) + \ldots + 2(H_{n-k+1} - 0) = \\ &= 2(k-n-1)H_{n-k+1} - 2kH_k + 2(n+1)H_{n+1} \leqslant \\ &\leqslant 2(k-n-1)(\ln(n-k+1)+1) - 2k\ln k + 2(n+1)(\ln(n+1)+1) \leqslant \\ &\leqslant 2n \end{aligned}$$

$$B = 2\sum_{i=1}^{k-2} \frac{k-i-1}{k-i+1} \leqslant 2(k-2), \text{ так как } \frac{k-i-1}{k-i+1} \leqslant 1$$

$$C = 2\sum_{j=k+2}^{n} \frac{j-k-1}{j-k+1} \leqslant 2(n-k-1), \text{ так как } \frac{j-k-1}{j-k+1} \leqslant 1$$

Подставляя все в выражения для $\mathbb{E}[X_k]$ получаем

$$\mathbb{E}[X_k] \leqslant 2n + 2(k-2) + 2(n-k-1) = 2n + 2k - 4 + 2n - 2k - 2 \leqslant 4n$$

$$\mathbb{E}[X_k] \leqslant 4n$$

$\square$