57 Отпечатки пальцев-II

Задача. Боб использует в качестве пароля случайную десятичную строку длины n. Пароль вводится на сенсорном устройстве Suxen. Виктор может разглядеть отпечатки пальцев Боба и узнать, сколько в пароле нулей, единиц, двоек и так далее. Виктор может воспользоваться наблюдениями и уменьшить число паролей, которые требуется проверить. Если, например, Виктор знает, что в пароле ровно одна единица, то ему требуется проверить не 10^n, а только $n9^{n-1}$ паролей. Во сколько раз уменьшается среднее число паролей, которые требуется проверить Виктору?

Решение. Обобщим задачу. Будем считать, что пароль — это слово длины n в алфавите $A = \{0, 1, \ldots, k-1\}$.

Пусть $n_0, n_1, \ldots, n_{k-1}$ — неотрицательные целые, сумма которых равняется n. Имеется

$$\binom{n}{n_0\ n_1\ \ldots\ n_{k-1}} = \frac{n!}{n_0! n_1! \ldots n_{k-1}!}$$

паролей, в которых n_i символов принимают значение i, $i \in A$. Вероятность появления описанного пароля:

$$\frac{1}{k^n}\binom{n}{n_0\ n_1\ \ldots\ n_{k-1}}.$$

Поэтому Виктору потребуется проверить $f_k(n)/k^n$ паролей в среднем, где

$$f_k(n) = \sum_{n_0+n_1+\ldots+n_{k-1}=n} \binom{n}{n_0\ n_1\ \ldots\ n_{k-1}}^2.$$

В следующей таблице приводятся значения $\log_k(f_k(n)/k^n)$ — актуальные длины десятичных паролей ($k = 10$) после перехвата отпечатков пальцев. Как видим, перехват дает много информации о пароле — актуальная длина существенно меньше первоначальной.

длина пароля (n)	рабочая длина пароля ($\log_k(f_k(n)/k^n)$)
4	1.24
5	1.85
6	2.51
7	3.22
8	3.96
9	4.73
10	5.53

Среднее число проверяемых паролей в

$$M \sim \frac{k^{2n}}{f_k(n)}$$

раз меньше общего числа. В работе [Richmond L., Shallit J. Counting Abelian Squares, Electronic J. of Combinatorics, v. 16, issue 1 (2009)] найдена асимптотика:

$$f_k(n) \sim k^{2n+k/2}(4\pi n)^{(1-k)/2} \quad (n \to \infty).$$

Поэтому [1]

$$M \sim \sqrt{\frac{(4\pi n)^{k-1}}{k^k}}$$

или

$$M \sim \frac{16}{3125}(\pi n)^{9/2}$$

при $k = 10$. □

[1] спасибо В. Палухе за обсуждение