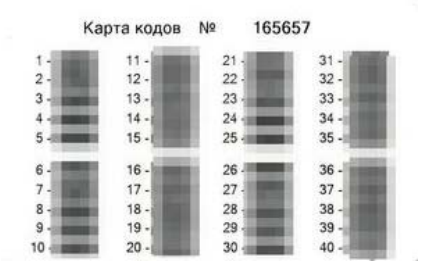
53 Карта кодов

Задача. Алиса получила от Трента карту с 40 кодами. Каждое утро Алиса обращается к серверу Трента, и в ответ получает запрос со случайным номером кода. Алиса находит нужный код на карте и возвращает его Тренту. Если Алиса ошибается, то сервер блокируется на 3 суток. Виктор перехватывает все запросы Трента и все ответы Алисы. После n суток наблюдений, накопив n кодов (некоторые из них могут повторяться), Виктор обращается к серверу Трента от лица Алисы. Если номер кода в запросе Трента уже отправлялся, то Виктор предъявляет нужный код и получает доступ к серверу. Если же номер не отправлялся, то Виктор ошибется (код очень длинный) и сможет повторить попытку аутентификации только через 3 суток. Как Виктору выбрать n, чтобы минимизировать среднее время ожидания успеха аутентификации?



Решение. Пусть $N = 40$ — количество кодов. Наблюдения Виктора можно интерпретировать как случайный эксперимент по размещению n частиц (перехваченных кодов) по N ячейкам (всевозможным кодам). Частицы размещаются случайно равновероятно независимо. Число пустых ячеек $\mu_0(n, N)$ — это количество кодов, не известных Виктору.

Согласно [Колчин В.Ф., Севастьянов Б.А., Чистяков В.П. Случайные размещения. М.: Наука, 1976, стр. 10]

$$\mathsf{P}\{\mu_0(n,N)=k\} = \binom{N}{k}\left(1-\frac{k}{N}\right)^n \sum_{l=0}^{N-k}\binom{N-k}{l}(-1)^l\left(1-\frac{l}{N-k}\right)^n.$$

Пусть Виктор располагает $N-k$ кодами. Тогда он пройдет аутентификацию сразу с вероятностью $p = (N-k)/N$, за 3 суток — с вероятностью $(1-p)p$, за 6 суток — с вероятностью $(1-p)^2 p$ и так далее. Среднее время ожидания успеха:

$$3p\sum_{i=1}^{\infty} i(1-p)^i = \frac{3(1-p)}{p} = \frac{3k}{N-k}.$$

Общее среднее время ожидания:

$$\begin{aligned} f(n,N) &= n + \sum_{k=0}^{N-1} \mathsf{P}\{\mu_0(n,N)=k\}\cdot\frac{3k}{N-k} = \\ &= n + \sum_{k=0}^{N-1}\binom{N}{k}\left(1-\frac{k}{N}\right)^n\left(\frac{3k}{N-k}\right)\sum_{l=0}^{N-k}\binom{N-k}{l}(-1)^l\left(1-\frac{l}{N-k}\right)^n. \end{aligned}$$

Минимум $f(n, 40)$ достигается при $n = 11$. Виктору следует собирать коды 11 суток, а после этого пробовать их угадывать. Тогда среднее время его атаки составит $f(11, 40) = 20.47$ суток. □