1 Первая цифра

Задача. Код сейфа представляет собой последовательность целых чисел от 1 до 9. Алиса и Боб хотят сгенерировать случайный контрольный код. Каждая из сторон желает влиять на результат генерации. Алиса и Боб договорились действовать следующим образом:

1) Алиса выбирает наудачу случайное натуральное число A, не кратное 10;

2) Боб выбирает наудачу случайное натуральное число B;

3) в качестве очередной цифры кода выбирается первая десятичная цифра A^B.

Виктор обрадован. Почему?

Решение. Идея задачи взята из замечательной статьи академика В. Арнольда в журнале «Квант» (1998 г., номер 1, см. `http://kvant.mccme.ru/1998/`).

Пусть A^B является m-разрядным десятичным числом с первой цифрой r:

$$A^B = r10^{m-1} + s, \qquad r \in \{1, 2, \ldots, 9\}, \quad s < 10^{m-1}.$$

Тогда

$$B \lg A = (m-1) + \lg\left(r + \frac{s}{10^{m-1}}\right)$$

или

$$\{B \lg A\} = \left\{\lg\left(r + \frac{s}{10^{m-1}}\right)\right\},$$

где через $\{z\}$ обозначается целая часть z. Следовательно, $r = i$, если

$$\{B \lg A\} \in [\lg i, \lg(i+1)).$$

Число $\lg A$ является иррациональным. Действительно, если $\lg A = u/v$, где u и v — целые, то $A^v = 10^u$. Это противоречит тому, что A не кратно 10. Согласно результатам Г. Вейля, которые цитируются в статье В. Арнольда, при случайном выборе B величина $\{B \lg A\}$ имеет распределение, близкое к равномерному на $(0, 1)$. Поэтому вероятность $\mathsf{P}\{r = i\}$ близка к величине

$$p_i = \lg(i+1) - \lg i.$$

В следующей таблице приводятся значения p_i:

i	p_i	i	p_i	i	p_i
1	0.301	4	0.097	7	0.058
2	0.176	5	0.079	8	0.051
3	0.125	6	0.067	9	0.046

Виктор обрадован тем, что распределение r сильно отличается от равномерного на $\{1, 2, \ldots, 9\}$. Это упрощает подбор кода сейфа.

Конкретнее, энтропия (по основанию 9) цифры r составляет

$$h(r) = -\sum_{i=1}^{9} p_i \log_9 p_i \approx 0.91.$$

Если код сейфа состоит из n цифр, то для подбора кода достаточно перебрать

$$9^{nh(r)} \approx (7.38)^n$$

высоковероятных вариантов (вместо 9^n вариантов при равномерном распределении r). $\square$