31 Перебор ключей DES

Задача. Алиса и Боб поспорили, кто из них быстрее найдет ключ DES, выбранный наудачу Трентом. Алиса и Боб разбили ключевое простанство пополам и Алиса начала проверять ключи, выполняя контрольные зашифрования и сравнивая результаты с данными, предоставленными Трентом. Алиса проверила половину своего ключевого сегмента и не нашла ключ, а Боб еще не начал проверку, что нарушает правила спора. Трент опасается, что спор может затянуться и указывает половину сегмента Боба, которая не содержит ключ. Трент предлагает Алисе поменяться с Бобом оставшимися у них частями сегментов. Следует ли Алисе меняться?

Решение. Оставшаяся у Алисы часть сегмента содержит ключ с вероятностью

$$\mathsf{P}\{\text{сегмент Алисы содержит ключ} \mid \text{первая половина сегмента не содержит ключ}\} = \\ = \frac{\mathsf{P}\{\text{вторая половина сегмента содержит ключ}\}}{\mathsf{P}\{\text{первая половина сегмента не содержит ключ}\}} = \frac{1/4}{3/4} = \frac{1}{3}.$$

На каждую половину сегмента Боба также приходится по $1/3$ вероятностной массы.

Можно представить себе ситуацию следующим образом: перед Алисой три двери, за одной дверью ключ, за двумя другими — пусто. Алиса выбрала некоторую дверь, и тут Трент открывает одну из двух других дверей и показывает, что за ней пусто. Трент предлагает Алисе поменять выбранную дверь на оставшуюся. Ситуация соответствует известному парадоксу Монти Холла (см. `http://en.wikipedia.org/wiki/Monty_Hall_problem`).

На первый взгляд кажется, что шансы Алисы на успех при обмене не изменятся. Однако это не так. Раскрытие Трентом пустой половины сегмента Боба (пустой двери) означает перемещение ее вероятностной массы в другую половину Боба. Алисе обязательно стоит меняться. Вероятность ее успеха увеличивается при обмене в 2 раза! □