27 Секретные материалы

Задача. Активист Нед Вонс разместил в Интернет секретные материалы, зашифрованные с помощью AES-256. Каждый месяц Нед рассылает в редакции газет всего мира ключ, на котором был зашифрован очередной секретный документ, делая его содержимое общедоступным. Документы Неда производят фурор, все редакции пытаются первыми опубликовать выдержки из них. Уже второй раз подряд в газету Gnutiez приходят письма Виктора. Виктор утверждает, что умеет атаковать AES-256 и в качестве доказательства указывает первый байт следующего ключа, который будет раскрыт Недом. Этот прогноз каждый раз оказывается верным! В третьем письме Виктор предлагает заплатить за предсказание всех следующих ключей. Трент, который редактирует газету, отказывается платить, утверждая, что Виктор — мошенник. Почему Трент так считает?

Решение. Трент посчитал, что Виктор разослал письма не в одну, а в $2^{16} = 65536$ газет. [1] В первых 256 письмах Виктор указал байт 0, во вторых 256 — байт 1, и так далее. После опубликования истинного ключа Виктор продолжил работать только с теми 256 газетами, в письмах которым первый байт был угадан. Во втором письме Виктор разослал 256 вариантов первого байта второго ключа и угадал этот байт в письме в Gnutiez.

Атака Виктора была описана в заметках М. Гарднера применительно к предсказанию результатов скачек. □

[1] Только в России на сентябрь 2006 года издавалась 49201 газета (`http://ru.wikipedia.org/wiki/Газета`).