14 Матрицы

Задача. В системе связи используется протокол Диффи — Хэллмана. Выбран простой модуль $p = 2^{127} - 1$ и найден первообразный корень g по модулю p. Алиса, Боб,... выбирают наудачу личные ключи $a, b, \ldots \in \{1, 2, \ldots, p-1\}$ и записывают их на собственные сверхзащищенные носители Dractrams. Для связи друг с другом Алиса и Боб, а также другие пары абонентов, обмениваются открытыми ключами g^a, g^b и определяют общий ключ $K = (g^a)^b = (g^b)^a$ (приведение $\bmod p$ опускается).

Трент обратил внимание на то, что вырабатываемый парами ключ K будет всегда одним и тем же. Это может использовать Виктор, который непрестанно прослушивает каналы связи. Абоненты понимают озабоченность Трента, но не хотят менять надежно защищенные личные ключи. Выход предложил Боб:

1. Публикуется детерминированный алгоритм, который по номеру сеанса строит матрицу M порядка 127 над полем из двух элементов. Матрица M обратима и строится как псевдослучайная.

2. Числа от 0 до $2^{127} - 1$ отождествляются с двоичными векторами размерности 127. Личный ключ k (как вектор) умножается на матрицу M и произведение (как число) обозначается через $M(k)$.

3. Алиса определяет сеансовую матрицу M и посылает Бобу одноразовый открытый ключ $g^{M(a)}$.

4. Боб определяет сеансовую матрицу M и посылает Алисе одноразовый открытый ключ $g^{M(b)}$.

5. Алиса и Боб вычисляют общий сеансовый секретный ключ $K_M = g^{M(a)M(b)}$.

Виктор утверждает, что сможет определить личные ключи Алисы и Боба, перехватив данные 130 сеансов связи. Прав ли Виктор?

Решение. Если $M(a)$ — четное, то $v = g^{M(a)}$ — квадратичный вычет по модулю p, т. е. $v^{(p-1)/2} \equiv 1 \pmod{p}$. Если $M(a)$ — нечетное, то $g^{M(a)}$ — квадратичный невычет.

Перехватывая открытый ключ $g^{M(a)}$, проверяя его на вычет/невычет, Виктор по известной всем матрице M получает одно линейное соотношение для битов a. Это соотношение задается последним столбцом M.

Для того, чтобы определить ключ a полностью, Виктору требуется дождаться использования сеансовых матриц $M_1, M_2, \ldots, M_t$, последние столбцы в совокупности имеют полный ранг.

Известно, что случайная двоичная матрица размера $n \times (n + d)$ имеет полный ранг с вероятностью близкой к

$$\prod_{i=d+1}^{\infty} \left(1 - \frac{1}{2^i}\right),$$

например, близкой к $p = 0.2887880951...$ при $d = 0$.

При $t = 127 + 3$ Виктор действительно получит матрицу полного ранга с высокой вероятностью

$$\frac{p}{\frac{1}{2} \cdot \frac{3}{4} \cdot \frac{7}{8}} \approx 0.880393$$

и определит личный ключ a.

Более того, если Виктор знает g^a, то у него есть еще одно линейное соотношение и вероятность успеха повышается до $\approx 0.880393/\frac{15}{16} \approx 0.939086$. □