Криптография

задачи к экзамену

(весна 2015, лектор Александр Лузгарев)

1. Рассмотрим следующее определение совершенной секретности для зашифровки двух сообщений. Схема шифрования $(\mathrm{Gen}, \mathrm{End}, \mathrm{Dec})$ на пространстве сообщений $\mathcal{M}$ называется **совершенно секретной для двух сообщений**, если для любого распределения вероятностей на $\mathcal{M}$, любых $m, m' \in \mathcal{M}$, любых $c, c' \in \mathcal{C}$ таких, что $P(C = c \wedge C' = c') > 0$, выполнено

$$P(M = m \wedge M' = m' \mid C = c \wedge C' = c') = P(M = m \wedge M' = m'),$$

   где m, m' независимо выбираются из заданного распределения на $\mathcal{M}$. Докажите, что *ни одна* схема шифрования не удовлетворяет этому определению.

2. Рассмотрим следующий протокол обмена ключами:

   a) Алиса выбирает случайным образом k, r из $\{0,1\}^n$, вычисляет $s = k \oplus r$, и посылает s Бобу.

   b) Боб выбирает случайным образом t из $\{0,1\}^n$, вычисляет $u = s \oplus t$ и посылает u Алисе.

   c) Алиса вычисляет $w = u \oplus r$ и посылает w Бобу.

   d) Алиса выводит $k_A = k$, Боб выводит $k_B = w \oplus t$.

   Докажите, что в итоге Алиса и Боб получают один и тот же ключ, и проанализируйте надежность этого протокола (докажите надежность или укажите конкретную атаку на него).

3. Алиса зашифровывает сообщение m с помощью наивной схемы RSA два раза: при этом используется одно и то же число $N = pq$, но два различных показателя e. Докажите, что если эти показатели взаимно просты, то хакер, перехвативший два зашифрованных сообщения, может легко восстановить m.

4. Пусть $N = pq$ — произведение двух различных простых нечетных чисел одной длины, и $\Phi(N^2) = \{(a, 1) \mid a \in \mathbb{Z}/N\mathbb{Z}\}$ — подмножество в $(\mathbb{Z}/N^2\mathbb{Z})^*$ (здесь мы пользуемся изоморфизмом между $(\mathbb{Z}/N^2\mathbb{Z})^*$ и $(\mathbb{Z}/N\mathbb{Z}) \times (\mathbb{Z}/N\mathbb{Z})^*$). Докажите, что не так уж и сложно определить по элементу $y \in (\mathbb{Z}/N^2\mathbb{Z})^*$, лежит ли он в $\Phi(N^2)$ (даже если не знать разложения N на простые множители).

5. Докажите, что если разложение N в произведение двух нечетных простых множителей одной длины известно, то изоморфизм $(\mathbb{Z}/N\mathbb{Z}) \times (\mathbb{Z}/N\mathbb{Z})^* \to (\mathbb{Z}/N^2\mathbb{Z})^*$ эффективно обратим.

6. Пусть $G\colon \{0,1\}^n \to \{0,1\}^{l(n)}$ — псевдослучайный генератор. Обозначим через $G'(s)$ первые n бит вывода $G(s)$. Докажите, что функция $F_k(x) = G'(k) \oplus x$ не является псевдослучайной.