Лекция №1

Часть 2. Принципы криптографии

Елена Киршанова

Курс “Основы криптографии”

Принятая модель вычислений – машина Тьюринга

Полиномиальное время

Алгоритм $\mathcal{A}$ работает за *полиномиальное время*, если, получая на вход данные размера n бит, $\mathcal{A}$ терминирует за время $\mathcal{O}(n^k)$ для константы k.

Примеры:

- умножение двух n-битных чисел: $\mathcal{O}(n \log n)$ – полиномиальное время
- факторизация n-битного числа: $\exp(\mathcal{O}(n^{1/3} \cdot (\log n)^{2/3})$ – субэкспоненциальное время

Алгоритм $\mathcal{A}$ называется *вероятностным полиномиальным* (ppt), если он работает за полиномиальное время и использует случайные биты.

Определения II.

Пренебрежимо малая функция

Функция $f : \mathbb{N} \to \mathbb{R}$ *пренебрежимо мала* (negl), если для всех многочленов p существует $N \in \mathbb{N}$, такое что для любого $n \geq N$

$$f(n) < \frac{1}{p(n)}.$$

Примеры:

- negl:

$$\frac{1}{2^n}, \quad \frac{1}{2^{\sqrt{n}}}, \quad \frac{1}{2^{\log^2(n)}}$$

- non-negl:

$$\frac{1}{\log n}, \quad \frac{1}{n^2}, \quad \frac{1}{2^{\mathcal{O}(\log n)}}$$

Формальное описание шифра

Шифр-схема $\Pi = (\mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Dec})$

включает в себя *ppt* алгоритмы KeyGen, Enc, Dec и множества

$\mathcal{K}$ – множество ключей

$\mathcal{M}$ – множество открытых текстов

$\mathcal{C}$ – множество шифр-текстов

такими, что для

$$k \leftarrow \mathsf{KeyGen}(1^\lambda)$$
$$c \leftarrow \mathsf{Enc}(k, m)$$
$$m' = \mathsf{Dec}(k, c)$$

схема корректна: $\mathsf{Dec}(k, \mathsf{Enc}(k, m)) == m \quad \forall k \in \mathcal{K}, m \in \mathcal{M}$

Шифр-схема (свойства)

Формально: множества $\mathcal{K}, \mathcal{M}, \mathcal{C}$ зависят от пар-ра безопасности λ.

Параметризация шифр-схемы Param(λ) – ppt алгоритм, принимающий на вход пар-р безопасности λ, и выдающий битовую строку $\Lambda = \mathrm{poly}(\lambda)$, задающую параметры шифр-схемы.

Пример: Для криптографической хэш-функции SHA-256 с $\lambda = 128$, Param(λ) выдаст

$$\mathcal{K}_{128} = \{0,1\}^{512} \qquad \mathcal{M}_{128} = \mathcal{C}_{128} = \{0,1\}^{256}$$

Принцип Керкгоффса (Kerckhoffs' principle)[1]:

> Криптосистема должна оставаться безопасной, если злоумышленнику известно всё, кроме секретного ключа

Алгоритмы Enc, Dec, Param являются открытыми и подлежат открытым научным исследованиям

[1] Auguste Kerckhoffs, «La Cryptographie Militaire», 1883