Содержание

Крипта ИСП

Disclaymer: доверять этому конспекту или нет выбирайте сами

1. О криптографии

Определение 1.1: **Криптографические средства защиты информации (КСЗИ)** – основанные на математических методах преобразования защищаемой информации.

Определение 1.2: **Теоретическая криптография (математическая криптография, криптология)** – раздел дискретной математики, изучающий математические модели КСЗИ с научной точки зрения.

Основной предмет теоритической криптографии – криптографический протокол. (о нём в следующей главе).

Пример: **Криптографические примитивы**:
- **Односторонняя функция** – эффективно вычислимая функция, задача инвертирования которой вычислительно трудна.
- **Псевдослучайный генератор** – эффективный алгоритм, генерирующий длинные последовательности, которые никакой эффективный алгоритм не отличит от чисто случайных.
- **Криптографическая хэш-функция** – эффективно вычислимое семейство функций, уменьшающих длину аргумента, для которого задача поиска коллизий вычислительно трудна.

Определение 1.3: **Атака** – совокупность предположений о возможностях противника, о том, какие действия ему доступны (помимо вычислений).

Определение 1.4: **Угроза** – цель противника, состоящая в нарушении одного или нескольких из трёх условий (задач) криптографического протокола.

2. О криптографических протоколах

Определение 2.1: **Криптографический протокол** – это протокол, решающий хотя бы одну из трёх задач:
- Обеспечение **конфиденциальности** данных
- Обеспечение **целостности** сообщений и системы в целом – гарантия отсутствия нежелательных последствий вмешательства противника
- Обеспечение **неотслеживаемости** – невозможность установления противником, кто из участников выполнил определённое действие

Пример: **Прикладные КП**:
- Системы шифрования
- Подбрасование монеты по телефону
- Схемы электронной подписи
- Протоколы аутентификации
- Системы электронных платежей

Пример: **Примитивные КП**:
- bit-commitment (схема обязательства)
- oblivious transfer (протокол с забыванием)

Определение 2.2: **Стойкость** – формализация понятия качества криптографического протокола, его способность решать поставленную перед ним задачу.

Замечание 2.1: Стойкость определяется **только** для конкретной модели противника, состоящей из трёх основных компонентов:
- Вычислительные ресурсы (включая модель вычислений)
- Атака
- Угроза

3. О теории сложности

Замечание 3.1: Задача кодируется множеством строк в некотором конечном алфавите Σ, $|\Sigma| \geq 2$. Без ограничения общности, будем рассматривать только $\Sigma = \{0, 1\} = \mathbb{B}$.

Определение 3.1: Σ^* – множество всех слов в алфавите Σ, то есть $\Sigma^* = \cup_{n=0}^{\infty} \Sigma^n$.

Определение 3.2: **Язык** – некоторое множество слов, то есть подмножество в Σ^*.

Определение 3.3: Модель вычислений, которую мы будем использовать в дальнейшем – **машина Тьюринга**

$$M = \left(Q, q_0, q_f, \Sigma, b, \sigma\right)$$

где:

- Q – множество состояний (конечное, непустое)
- $q_0, q_f \in Q$ – выделенные состояния: начальнео и конечное
- Σ – конечный алфавит
- b – специальный «пустой символ»
- $\sigma : \Sigma \times Q \to \Sigma \times Q \times \{-1, 0, 1\}$ – функция перехода (частично определённая, в общем случае многозначная)

Определение 3.4: С машиной Тьюринга M связаны отображения:

- **Вычисляемая машиной функция** $M(\cdot) : \mathbb{B}^* \to B^* \cup \{\bot\}$, где $M(w)$ – выход машины M, если на вход подана строка w. (Выдаёт $\bot$ если вычисление не закончено)
- **Время её работы** $T_M(\cdot) : \mathbb{B}^* \to \mathbb{N} \cup \{\infty\}$, где $T_M(w)$ – число тактов работы машины M при вычислении на входе w.
- **Используемая ею память** $S_M(\cdot) : \mathbb{B}^* \to \mathbb{N} \cup \{\infty\}$, где $S_M(w)$ – число ячеек ленты, задействованных в вычислении на входе w.

Определение 3.5: Введём $\operatorname{poly}(x)$ – обозначение для «**некоторого полинома**» от переменной x. Важен не сам полином, факт его существования.

Определение 3.6: Введём названия для некоторых видов машин Тьюринга:

- **Детерминированная машина Тьюринга** – функция перехода σ однозначна
- **Полиномиальная (детерминированная) машина Тьюринга M** – обладает свойством:
$$\forall w \in \mathbb{B}^* : T_M(w) \leq \text{poly}(|w|)$$
- **Недетерминированная машина Тьюринга** – функция перехода σ, вообще говоря, многозначна, выбор её значений в конкретном вычислении осуществляется с помощью строки «Недетерминированного выбора» $\psi \in \mathbb{B}^\infty$, записанной на специальную ленту
- **Полиномиальная недетерминированная машина Тьюринга M** – обладает свойством:
$$\forall w \in \mathbb{B}^* : \forall \psi \in \mathbb{B}^* : T_M(\psi; w) \leq \text{poly}(|w|)$$
- **Вероятностная машина Тьюринга** – функция перехода σ принимает случайные значения, $M(w)$ – случайная величина (при фиксированном w). Выбор значения функции перехода в каждом такте осуществляется с помощью случайной строки $\rho \in \mathbb{B}^\infty$, записанной на специальную ленту.
- **Полиномиальная вероятностная машина Тьюринга (п.в.м.Т.) M** – обладает свойством:
$$\forall w \in \mathbb{B}^* : \forall \rho \in \mathbb{B}^\infty : T_M(\rho; w) \leq \text{poly}(|w|)$$
- **Полиномиальная в среднем вероятностная машина Тьюринга M** – обладает свойством:
$$\exists \varepsilon > 0 : \forall n \in \mathbb{N} : \forall \rho \in \mathbb{B}^\infty : \forall w \in \mathbb{B}^n : \mathbb{E}(T_M(\rho; w))^\varepsilon \leq n$$

Определение 3.7: Класс сложностей **Bounded-error Probabilistic Polynomial time**:
$$\text{BPP} = \left\{ L \subseteq \mathbb{B}^* \mid \exists \text{ п.в.м.Т. } M \left\{ {}^{w \in L \ \Rightarrow \mu(\{M(w)=1\}) \geq \frac{2}{3}}_{w \notin \in L \Rightarrow \mu(\{M(w)=1\}) \leq \frac{1}{3}} \right\} \right.$$

Определение 3.8: Класс сложностей **Randomzed Polynomial time**:
$$\text{RP} = \left\{ L \subseteq \mid \exists \text{ п.в.м.Т. M} \left\{ {}^{w \in L \ \Rightarrow \mu(\{M(w)=1\}) \geq \frac{2}{3}}_{w \notin \in L \Rightarrow \mu(\{M(w)=1\}) = 0} \right\} \right\}$$

Определение 3.9: **Однородной моделью вычислителя противника** называется полиномиальная вероятностная машина Тьюринга или полиномальная в среднем вероятностная машина Тьюринга.

Определение 3.10: **Булевой схемой** называется отображение $C : \mathbb{B}^n \to \mathbb{B}^m$, такое, что для каждой координаты образа существует логическая функция от входа, тождественно задающая её.

Размером булевой схемы называется размерность её выхода.

Пример: Булевая схема $C : \mathbb{B}^1 \to \mathbb{B}^3$ имеет размер 3:

$$C(x_1) = (x_1, \neg x_1, x_1 \vee \neg x_1)$$

Определение 3.11: **Неоднородной моделью вычислителя противника** называется семейство булевых схем полиномиального размера $C = \{C_n\}_{n=1}^{\infty}$:

$$\forall n : |C_n| \leq \text{poly}(n)$$

причём для каждого размера входа $|w|$ выбирается $C_{|w|}$ схема.