Содержание

1. Введение 2
1.1. Предмет математической криптографии 2
1.2. Криптографический протоколы 2
1.3. Криптографические примитивы 2
1.4. Модель противника 3

Крипта ИСП

Disclaymer: доверять этому конспекту или нет выбирайте сами

1. Введение

1.1. Предмет математической криптографии

Определение 1.1.1: **Криптографические средства защиты информации (КСЗИ)** – основанные на математических методах преобразования защищаемой информации.

Определение 1.1.2: **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).

1.2. Криптографический протоколы

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)

1.3. Криптографические примитивы

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.

1.4. Модель противника

Определение 1.4.1: **Атака** – совокупность предположений о возможностях противника, о том, какие действия ему доступны (помимо вычислений).

Определение 1.4.2: **Угроза** – цель противника, состоящая в нарушении одного или нескольких из трёх условий (задач) криптографического протокола.