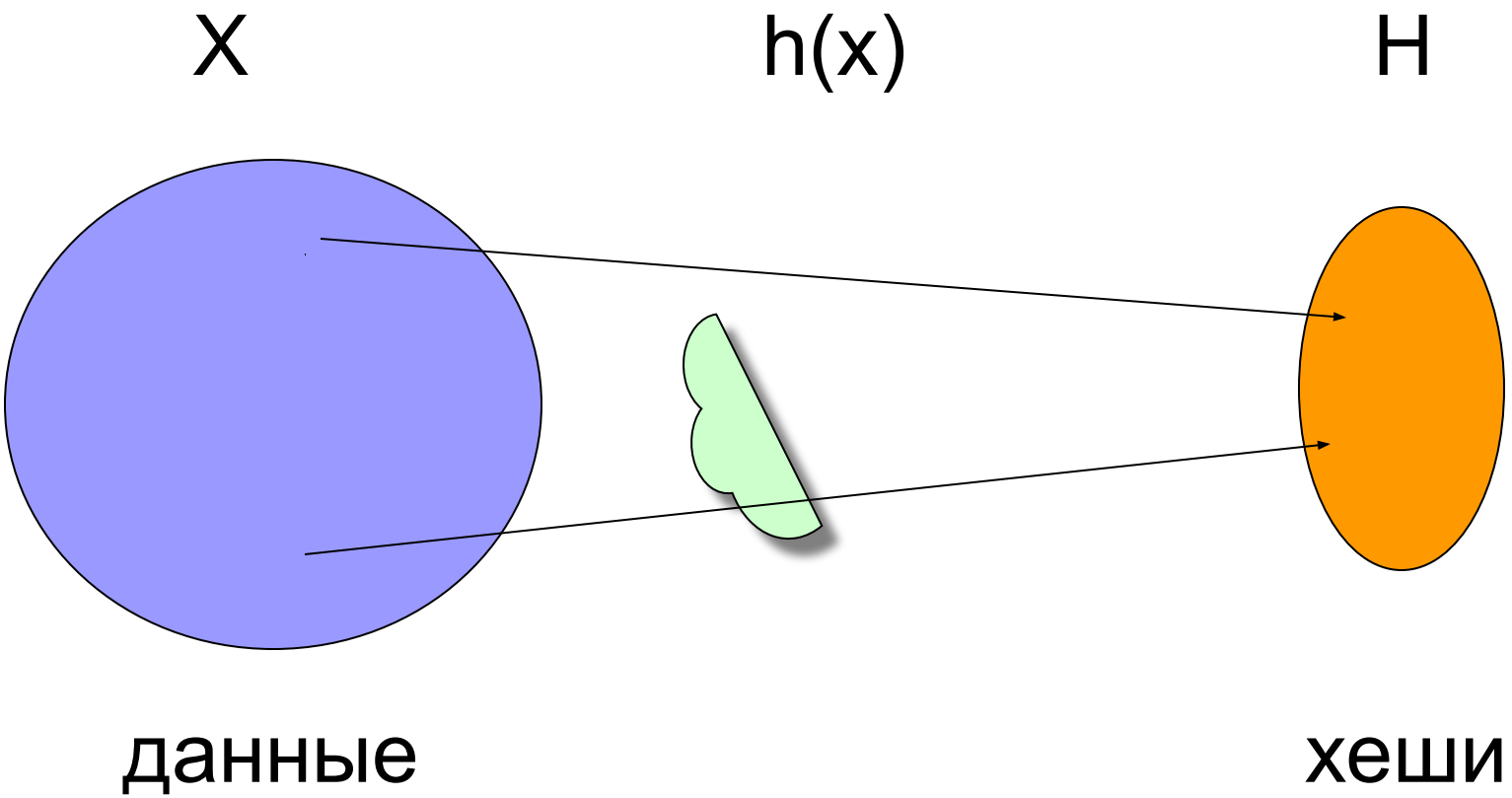
Коллизии хеш-функций

MD5, SHA-0, SHA-1

Московский физико-технический институт (ГУ МФТИ)
Факультет Радиотехники и Кибернетики

Функция хеширования



Функция хеширования

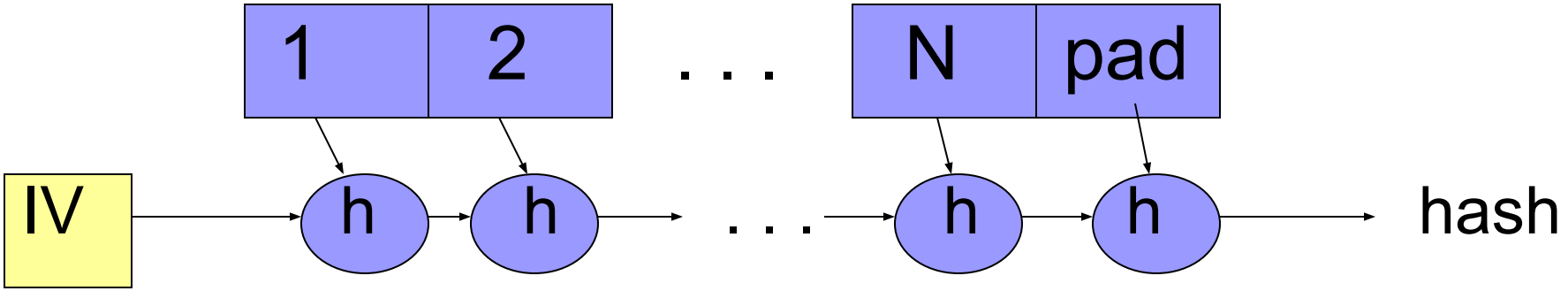
Свойства:

- Необратимость
- Стойкость к коллизиям
  - Слабая
  - Сильная

Применение в криптографии

ЭЦП, пароли и т.д.

Алгоритм Меркла-Дамгарда

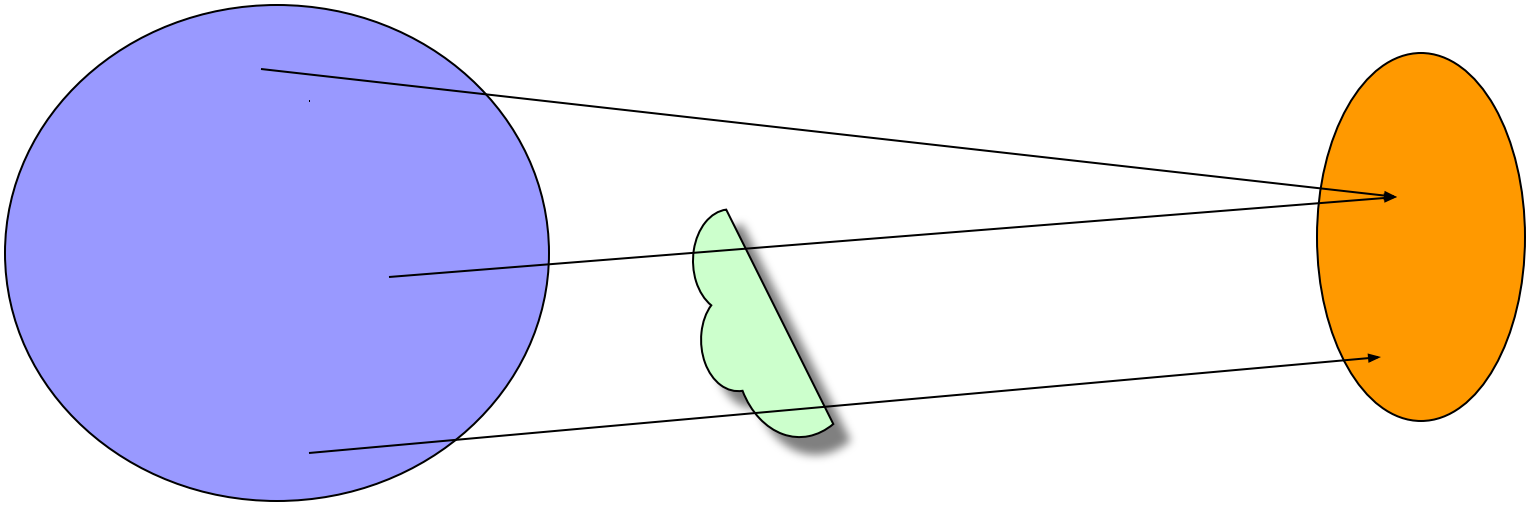


Выравнивание сообщения определённым образом – существенный аспект безопасности

Коллизии хеш-функций

- Практически любая хеш-функция имеет коллизии
- В хороших х.ф. коллизии крайне редки
- «Идеальная х.ф.» - если заранее известны все значения входных данных

Коллизии хеш-функций



Типы атак на хеш-функции

Для n-битной хеш-функции

- Атака на обнаружение коллизий

  Требует ~ $2^{n/2}$ операций (парадокс дней рождения)

- Атака на нахождение прообраза

  Требует ~ 2^{n} операций

MD5

- **Доббертин (1996г)**
  - Псевдоколлизия – использовал свои IV
  - Если MD5(x) = MD5(y), то MD5(x||S) = MD5(y||S)
- **Ванг и Ю**
  - Мощный метод нахождения коллизий, основанный на дифференциальной атаке. ~ 2^{40} операций
  - Были приведены некоторые коллизии и написана программа для генерирования архивов и документов PDF с одинаковыми хешами

SHA-0

- **Ванг**
  - Атака методом дифференциальных путей

    Используется возможность создания локальных коллизий в SHA-0

    Сложность «прямой» реализации ~ 242 операций

    Можно заранее составить таблицу подходящих сообщений, тогда сложность составляет ~ 239 операций

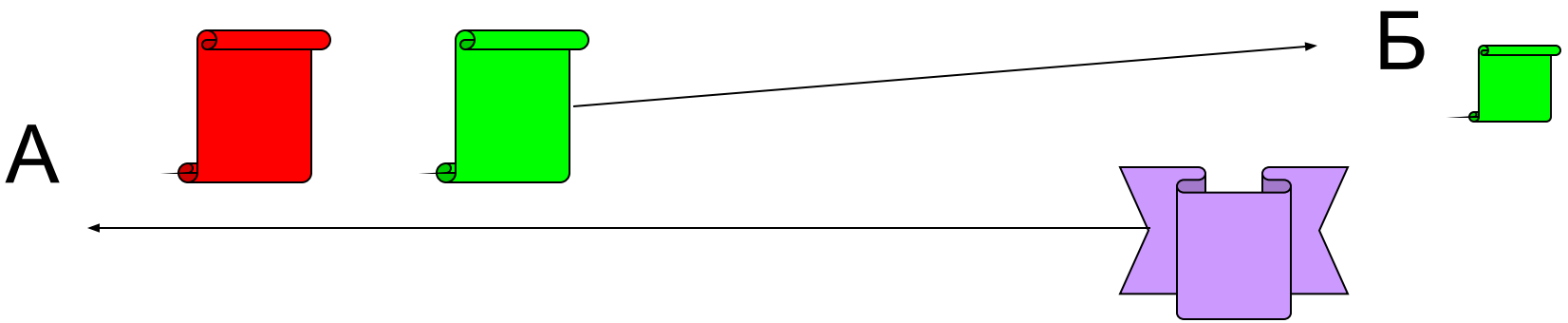
SHA-1

- **Ванг, Йинг, Ю**
  - Расширимые сообщения – разновидность множественной коллизии.
  - Атака с использованием очень длинных сообщений

    Находят все промежуточные хеши для очень длинного сообщения и перебирают около 2106 блоков до совпадения с одним из исходных. Находят расширимое сообщение и расширяют его до длины исходного. Получают второй прообраз.

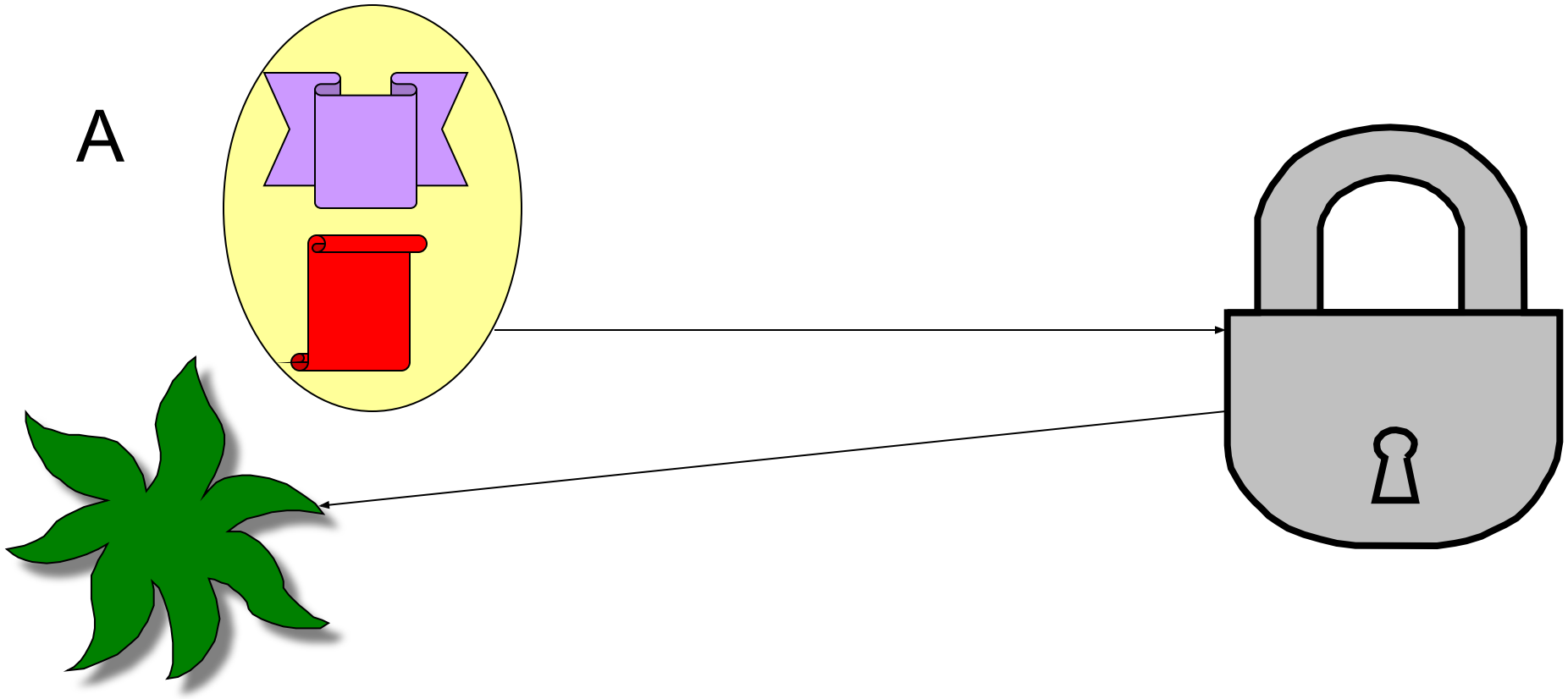
Опасность коллизий

Пример про Алису и её Босса



Опасность коллизий

Пример про Алису и её Босса, прод.



Спасибо за внимание