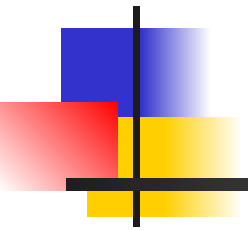
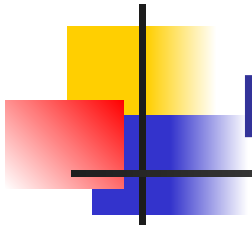


Хэш функции

Нестеров Антон

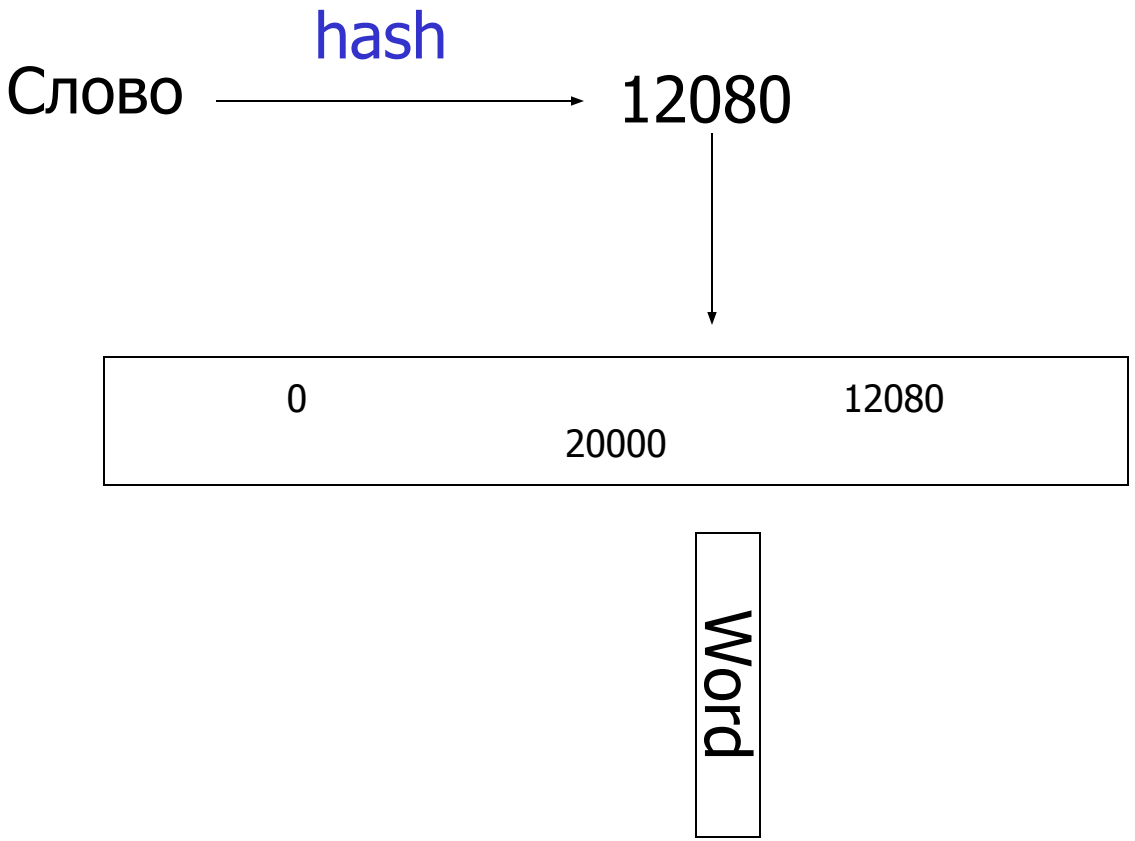


План доклада

- Что это такое
- Зачем оно надо
- Примеры

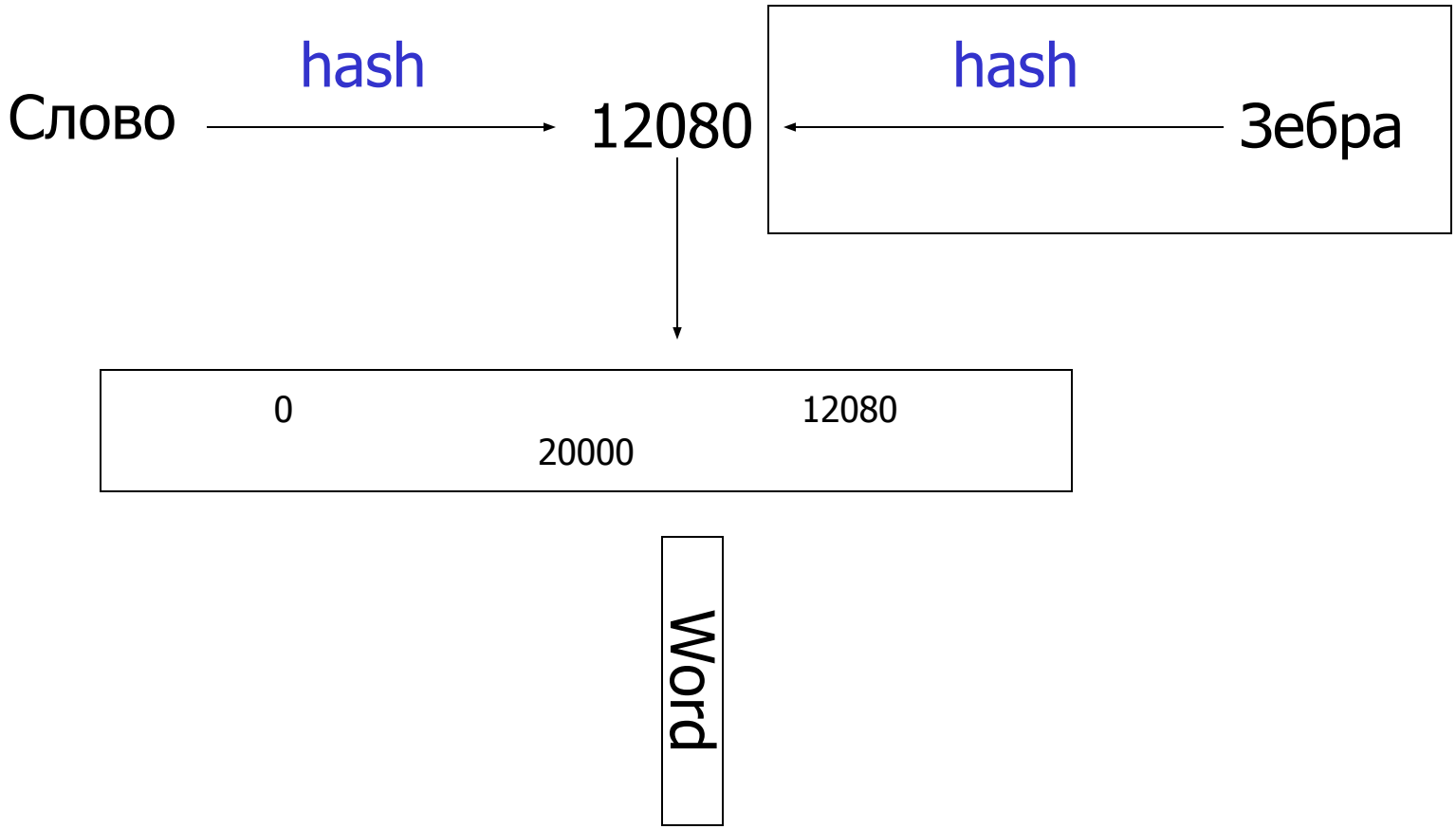
Hash-функция

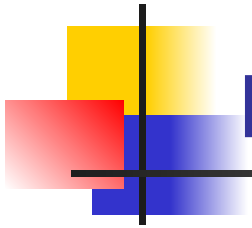
- Пример не из криптографии – Хранение словаря



Коллизии

- Пример не из криптографии – Хранение словаря

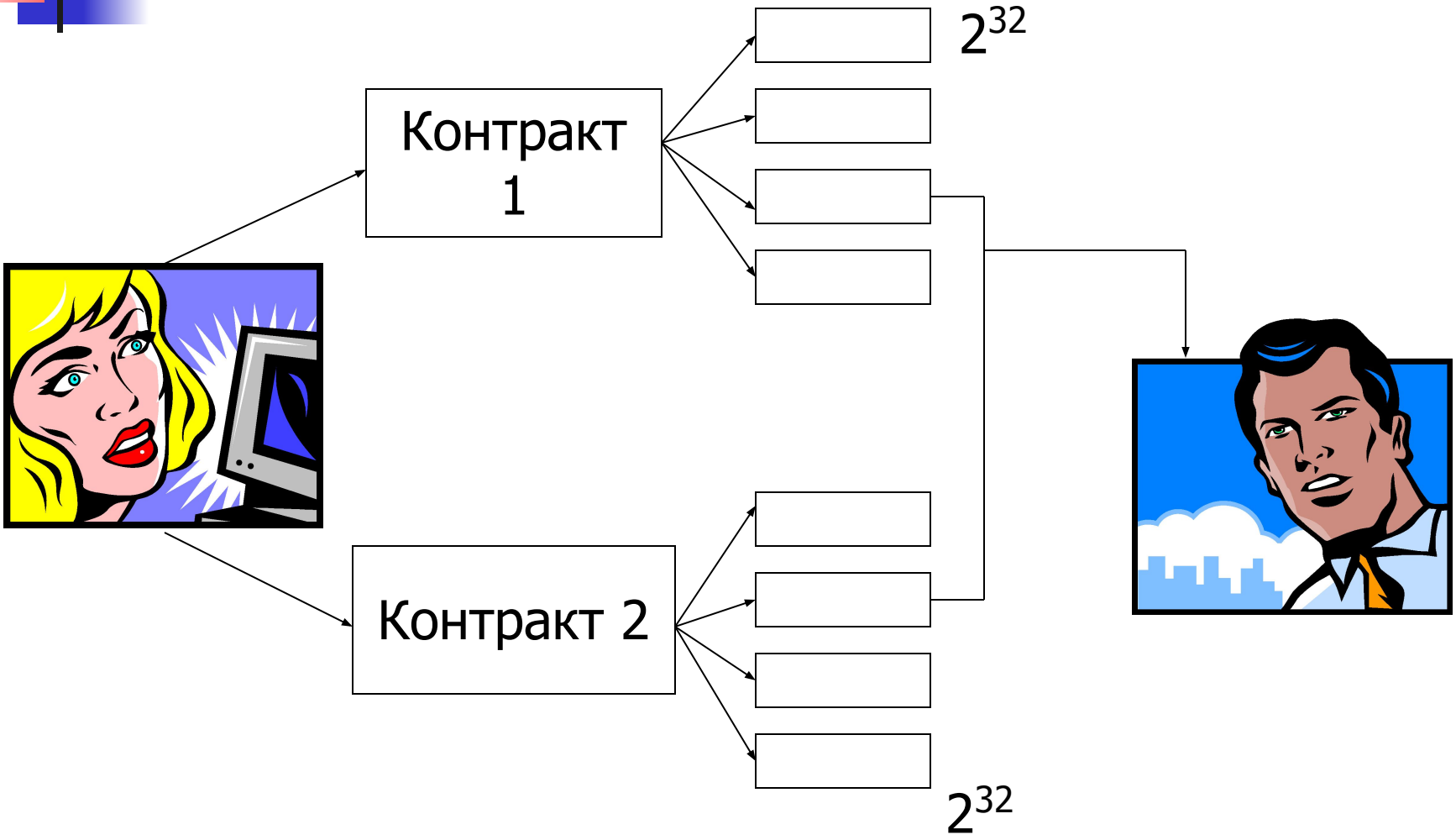


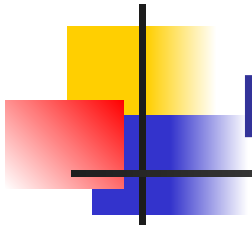


Практическое использование

- Банкомат
- Цифровая подпись
  - Быстро вычислимые
  - Не обратимые
  - Зная M сложно вычислить N такое, что H(M)=H(N)
  - Кроме того, сложно найти такие P и Q, что H(P)=H(Q)
- Авторизация клиент-сервер

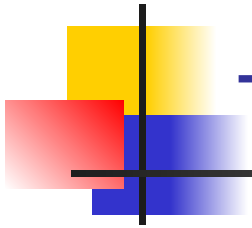
Пример взлома





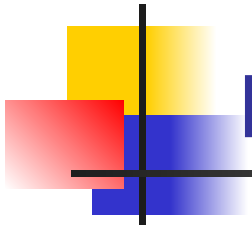
Нахождение коллизий

- Метод дней рождений
  - Сколько человек должно быть в комнате, чтобы вероятность того, что найдется человек родившийса с вами в один день была равна 0.5 ???
  - Сколько человек должно быть в комнате, чтобы вероятность того, чтобы нашлась пара людей, родившихся в один день была 0.5 ???



Требования к функции

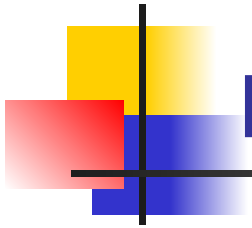
- Актуальный размер кэша
  - Для 16 байтогого кэша (128 бит) 2^{64} различных документов
  - Secure Hash Standard 160 бит 2^{64}
  - Специальный метод для удлиннения хэш-значений
    - Прибавить хэш значение к исходному сообщению, а затем повторить все заново
  - Отсутствие коллизий осмысленных строк



Немного примеров из истории

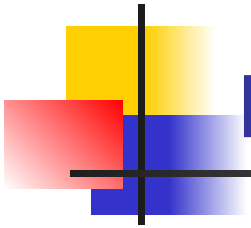
- Snefru Ральф Меркл
- N-hash 1990
- MD4, MD5 Рон Ривест
- SHA
- RIPE-MD
- HAVAL
- ГОСТ Р 34.11.94
- Использование блочных шифров

Алгоритм	Длина хэш-значения	Скорость шифрования (Кбайт/с)
Одновременная схема Davies-Meyer (с IDEA)	128	22
Davies-Meyer (с DES)	64	9
Хэш-функция ГОСТ	256	11
HAVAL (3 прохода)	переменная	168
HAVAL (4 прохода)	переменная	118
HAVAL (5 прохода)	переменная	95
MD2	128	23
MD4	128	236
MD5	128	174
N-хэш (12 этапов)	128	29
N-хэш (15 этапов)	128	24
RIPE-MD	128	182
SHA	160	75
Snerfu (4 прохода)	128	48
Snerfu (8 проходов)	128	23



Взломы и попытки взломов

- Некоторые алгоритмы были вломаны
  - Найдены алгоритмы нахождения коллизий
- Некоторые почти взломаны
  - Найдены алгоритмы нахождения
    - предколлизий
    - коллизий за меньшее время
    - коллизий в укороченных версиях
      - Атака на 7 из 10 уровней AES
      - Антуан Жу – работа о мульти хэш-функциях



MAC

- Message authentication code
  - Хэш функция зависит от ключа
  - Можно менять ключ для дополнительной проверки
  - В качестве MAC можно использовать обычный хэш
    - *H(K,H(K,M))*
    - *H(K,p,H,M)*
  - Сложно подобрать ключ
  - Вычислить значение хэша для другого ключа

Определения

- Определение hash-функции
  - Функция H

$$H: K \times D \rightarrow R.$$

Или семейство

$$H_K: D \rightarrow R$$

Пользуясь предыдущим примером:

- D строчки русских букв
- R число от 0 до 20000

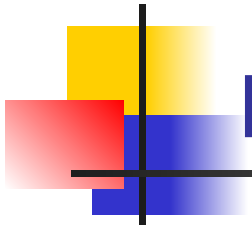
Определения

- Обратная функция

$$H_K^{-1}(y) = \{ x \in D : H_K(x) = y \}$$

- Коллизия

$$H_K(x_1) = H_K(x_2)$$

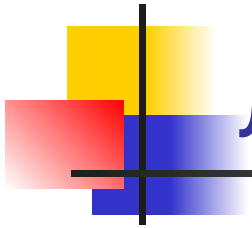


Нахождение коллизий

- Три типа устойчивости
  - CR2-KK
    - Collision free, collision resistant
  - CR1-KK
    - Universal one-way
  - CR0
    - Universal

Три вида атак на нахождение коллизий

- CR2-KK
  - Найти коллизии для конкретной функции
- CR1-KK
  - Подобрать пару к заданному значению, образующую коллизию для конкретгой функции.
- СК0
  - Найти коллизию для семейства функций



Литература

- Брюс Шнайер - Прикладная криптография
- FAQ по криптографии faqs.org.ru
- Mihir Bellare, Phillip Rogaway - Introduction to Modern Cryptography
- www.CyberSecurity.ru
- www.openbsd.org/ru/crypto.html
- www.cryptography.ru
- Shafi Goldwasser, Mihir Bellare - Lecture Notes on Cryptography