


ЗАЩИТА ИНФОРМАЦИИ ПРИ КОДИРОВАНИИ И ПЕРЕДАЧЕ ДАННЫХ



- ▶ Контрольные суммы
- ▶ Контроль CRC
- ▶ Кэширование
- ▶ Цифровая подпись



- ▶ Защита информации - совокупность методов и средств, обеспечивающих целостность, конфиденциальность, достоверность, аутентичность и доступность информации в условиях воздействия на нее угроз естественного или искусственного характера.
- 

- ▶ Контрольная сумма (хеш) — определенное значение, рассчитанное для данных с помощью известных алгоритмов. Предназначается для проверки целостности данных при передаче.

КОНТРОЛЬНЫЕ СУММЫ

Алгоритмы

```
graph TD; A[Алгоритмы] --> B[СRC32]; A --> C[MD5]; A --> D[SHA-1];
```

СRC32

MD5

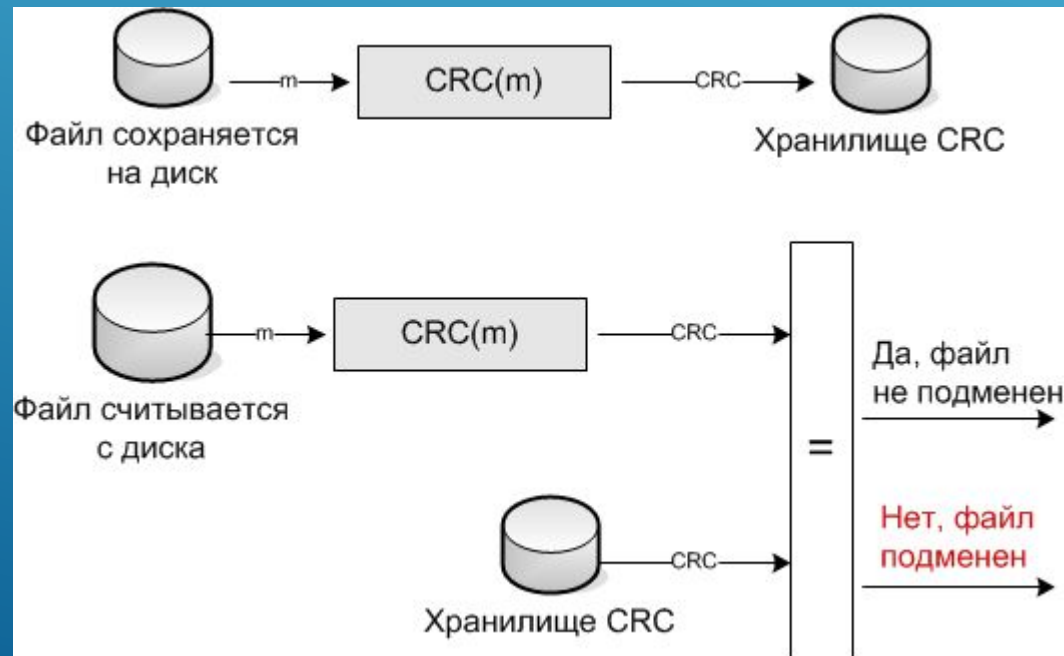
SHA-1

- ▶ Алгоритм контроля CRC уже в течение длительного времени широко используется в системах сетевых адаптеров, контроллеров жесткого диска и других устройств для проверки идентичности входной и выходной информации.

КОНТРОЛЬ CRC



- ▶ Ключевым принципом вычислений для механизма CRC является то, что операции умножения и деления этих полиномов выполняются точно так же, как с обычными числами.
- ▶ Механизм CRC чрезвычайно полезен для проверки файлов, загружаемых из сетевых информационных служб.



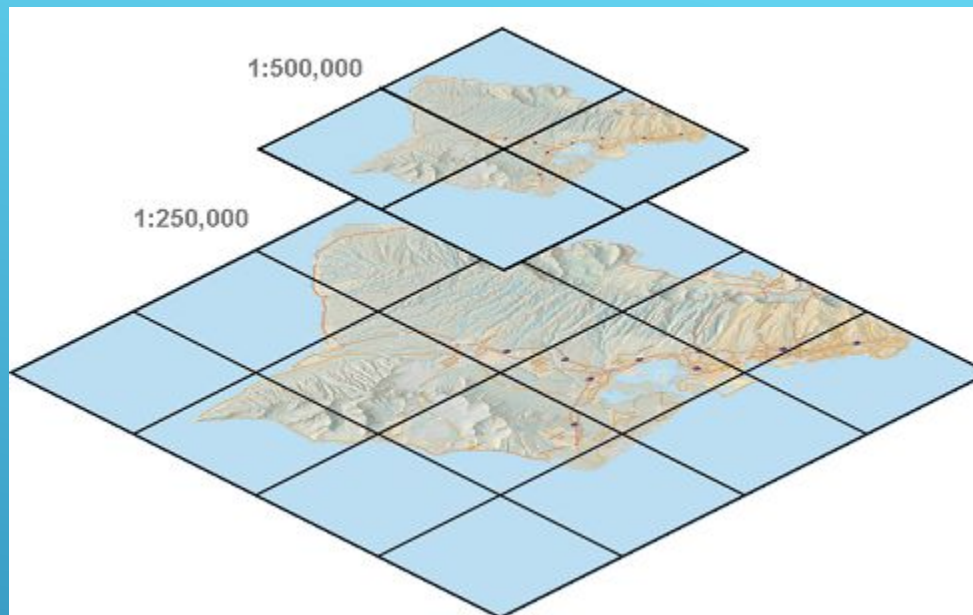
- ▶ Кэш - запоминающее устройство, используемое в качестве буфера между процессором и самой памятью в быстродействующих компьютерных системах.

КЭШИРОВАНИЕ

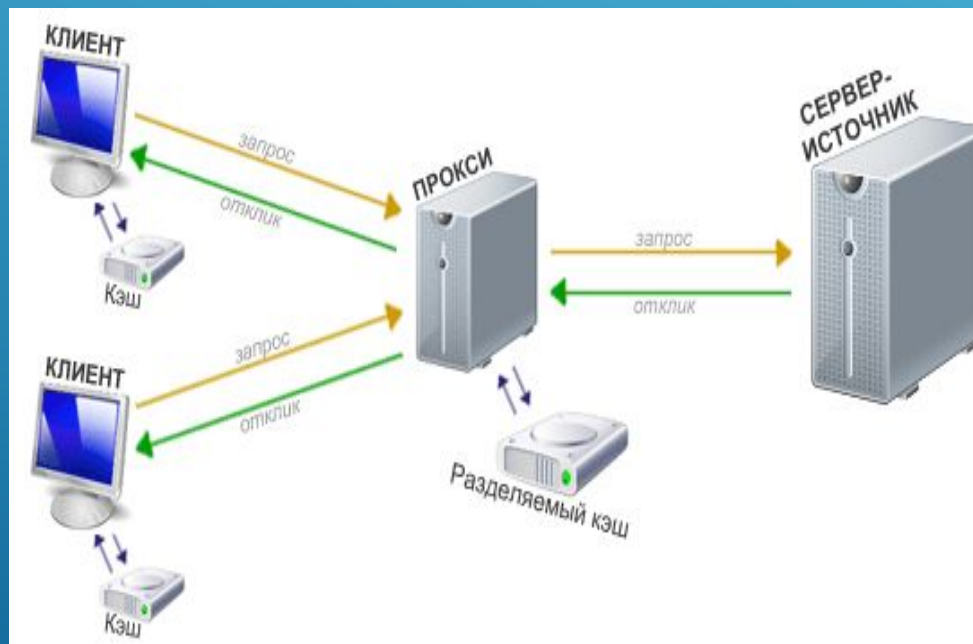
- ▶ При относительно небольшом объеме от 32 до 256 килобайт благодаря большой скорости обмена информацией оно увеличивает производительность компьютера на 10-15%.
- ▶ Кэш центрального процессора разделён на несколько уровней. Максимальное количество кэшей — четыре. В универсальном процессоре в настоящее время число уровней может достигать трёх.



Кэширование карты



Процесс кэширования



- ▶ Электронная цифровая подпись - это особый реквизит документа, который позволяет установить отсутствие искажения информации в электронном документе с момента формирования ЭП и подтвердить принадлежность ЭП владельцу.

ЦИФРОВАЯ ПОДПИСЬ

- ▶ Электронная цифровая подпись применяется для подписи электронных документов, как обычная подпись - для документов бумажных. В России юридическую значимость имеет ЭЦП, выданная (заверенная) удостоверяющим центром.



- ▶ ЭЦП можно разделить на три составляющие: открытый ключ, закрытый ключ и сертификат. Сертификат содержит сведения о владельце ЭЦП и может включать в себя не только персональные данные, но и реквизиты компании, то есть служить аналогом печати.
- ▶ С помощью закрытого ключа осуществляется формирование подписи электронного документа. Открытый ключ служит для верификации подписи. Он виден всем участникам системы электронного документооборота.

