MD5 - Java加密与安全 - 飞扬学院

Java加密与安全

MD5

摘要算法

摘要算法 / 哈希算法 / 数字指纹 / Hash / Digest

计算任意长度数据的摘要，输出固定长度

相同的输入始终得到相同的输出

不同的输入尽量得到不同的输出

碰撞

两个不同的输入得到了相同的输出

Hash算法的安全性：

- 碰撞率低
- 不能猜测输出
- 输入的任意一个bit的变化会造成输出完全不同
- 很难从输出反推输入（只能依靠暴力穷举）

MD5摘要算法

- 验证原始数据是否被篡改
- 存储用户口令

- 需要防止彩虹表攻击

练习

下载练习（推荐使用Eclipse插件直接导入工程）