1. md5和sha-1是一种摘要算法，即hash算法的一种。
2. md5加密是不安全的，因为现在世界上有专门的网站反查，所以需要加盐
3. 一般做法，比如用户注册账号时，得到密码，随机一个盐，然后用密码+盐的自定义排列组合做md5，然后把盐和hash之后的串一起保存到用户数据中，但是这种做法也不是绝对安全