

## 单向散列函数

版权所有 © 2019 作者：杜文亮，保留所有权利。

允许个人使用。利用这些问题只有当作者的书被采用作为该课程的教科书时，该课程才被授予。所有其他用途必须征得作者同意。

- C2.1. 为什么哈希函数  $f(x) = x \bmod 10000$  不是一个好的单向哈希函数？
- C2.2. SHA-2 名称中的数字 2 代表什么？SHA-256 名称中的数字 256 是什么意思？
- C2.3. 请分别列出 PHP、SQL 和 Python 中可用于计算单向哈希的函数。
- C2.4. 攻击者获得了 `shadow` 文件的副本，并尝试猜测 Bob 的密码。有人说，盐会使攻击者更难猜出 Bob 的密码。你是否同意？
- C2.5. `shadow` 文件中的盐以明文保存。把盐也保密是否会更好？请解释。
- C2.6. 一位开发人员写道：“我正在为论坛实现登录功能，准备先在客户端用 JavaScript 对口令求哈希，再发送给服务器。若哈希值与服务器保存的值一致，就允许用户登录。”他认为发送口令的哈希值比直接发送口令更安全。你是否同意？为什么？
- C2.7. Linux 会迭代多轮哈希来生成口令哈希，例如执行 5000 轮 SHA-512。这样看似浪费计算时间，为什么还要这么做？
- C2.8. 1998 年，Alice 对自己的小说计算了 MD5 哈希，并把哈希值刊登在 华尔街日报 上，但此后一直没有机会出版小说。最近上映的一部电影采用了她的构思，许多台词甚至与小说完全相同，她却没有得到署名或版权税。Alice 决定起诉制片公司，但得知 MD5 的抗碰撞性已在 2004 年被攻破，因此不确定当年公布的哈希还能否作为有效的时间戳证据。如果你是 Alice 的律师，会如何说服法官？
- C2.9. 已知  $h = \text{Sha256}(K \parallel M)$ ，其中  $K$  是秘密，“ $\parallel$ ”表示拼接，公式中未显式写出 SHA-256 的内部填充。请说明如何在不知道  $K$  的情况下，为另一个消息  $X$  计算  $\text{Sha256}(K \parallel X)$ 。
- C2.10. 已知  $h = \text{Sha256}(M \parallel K)$ ，其中  $K$  是秘密，“ $\parallel$ ”表示拼接。能否在不知道  $K$  的情况下，为另一个消息  $X$  计算  $\text{Sha256}(X \parallel K)$ ？
- C2.11. 在长度扩展攻击中，我们需要知道密钥的长度吗？
- C2.12. 对下列消息  $K:M$  计算 SHA-256。（1）它会使用什么填充？（2）已知  $\text{hash}(K:M)$ ，希望在不知道  $K$  的情况下计算  $\text{hash}(K:M:N)$ ，并让  $N$  包含消息“extra content”。请写出  $N$  的实际字节内容。

```
K   = abcd9313x
M   = 1234567890123456789012345678901234567890
K:M = abcd9313x:1234567890123456789012345678901234567890
```

C2.13. Charlie 为互不相识的密码学家 Alice 和 Bob 安排了一次相亲，并事先分别把一个秘密数 K 告诉二人，其他人不知道 K。Bob 想确认赴约者确实是 Alice。请说明 Alice 如何在不泄露 K 的前提下证明自己的身份。

C2.14. ★

你负责看守一扇门，任何人通过时都必须报出姓名和口令。周围的人能够听到口令，因此每个口令只能使用一次。你可以预先给每位授权者一张一次性口令表，但自己不想保存整张表，只愿意为每个人保存一个不超过 32 字节的值，并且可以在每次认证后更新它。请说明如何实现。

C2.15. ★

你擅长预测股票价格，并已预测未来 10 天的收盘价。你计划每天收市后公布当天的预测，让公众验证是否准确，同时还要证明这些预测确实是事先作出的。收市前不能泄露预测，以免他人据此获利。开始时你可以在一份知名报纸上刊登一段最多 64 个字符的数据。请设计一种方案。

C2.16. 对于给定消息 M，能否利用哈希碰撞攻击找到 M'，使得  $\text{hash}(M') = \text{hash}(M)$ ？

C2.17. Bob 找到两个不同的 64 字节消息 M1 和 M2，满足  $\text{SHA256}(M1) = \text{SHA256}(M2)$ 。能否再构造一对 M3 和 M4，使  $\text{SHA256}(M3) = \text{SHA256}(M4)$ ？