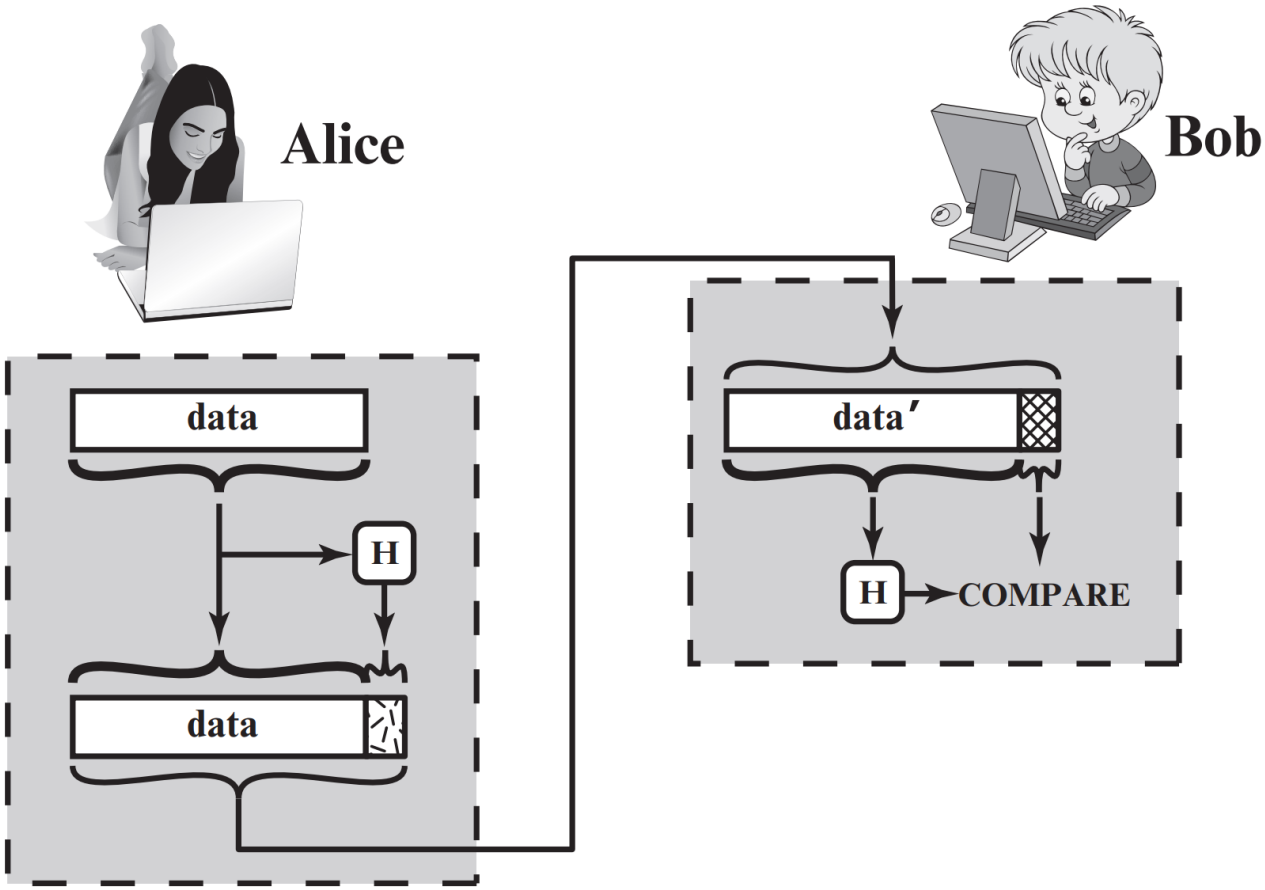
> 教材第十一章

- 哈希函数是密码学中的一类原语
- 哈希函数的安全要求：单向性，抗碰撞
- 了解常用哈希函数的消息长度是多少

密码学中哈希函数的应用

消息认证



(a) Use of hash function to check data integrity

上图过程无法抵抗中间人攻击，因此要想办法防止攻击者生成能被认证通过的哈希值（教材 P236）。一般消息认证是通过使用消息认证码实现的，即带密钥的哈希函数，在下一章。

数字签名

在进行数字签名过程中**使用用户的私钥加密消息的哈希值**。

需求和安全性

表 11.1　密码学 Hash 函数 H 的安全性需求

需　求	描　述
输入长度可变	H 可应用于任意大小的数据块
输出长度固定	H 产生定长的输出
效率	对任意给定的 x，计算 $H(x)$比较容易，用硬件和软件均可实现
抗原像攻击（单向性）	对任意给定的 Hash 码 h，找到满足 $H(y)=h$ 的 y 在计算上是不可行的
抗第二原像攻击（抗弱碰撞性）	对任何给定的分块 x，找到满足 $y \neq x$ 且 $H(x)=H(y)$的 y 在计算上是不可行的
抗碰撞攻击（抗强碰撞性）	找到任何满足 $H(x)=H(y)$的偶对(x,y)在计算上是不可行的
伪随机性	H 的输出满足伪随机性测试标准

- 碰撞攻击穷举的规模比原像攻击和第二原像攻击更小（由生日悖论可印证）
- 穷举攻击，密码分析

安全哈希码

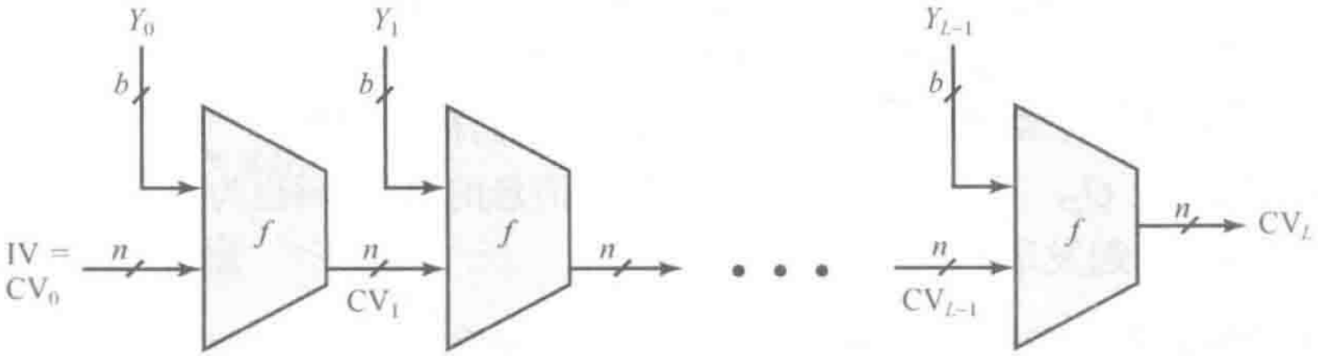


图 11.8　安全 Hash 码的一般结构

SHA 在内的目前所使用的大多数 Hash 函数都是这种结构。Hash 函数将输入消息分为 L 个固定长度的分组，每一分组长为 b 位，最后一个分组不足 b 位时需要将其填充为 b 位，最后一个分组包含输入的总长度。（由于输入中包含长度，所以攻击者必须找出具有相同 Hash 值且长度相等的两条消息，或者找出两条长度不等但加入消息长度后 Hash 值相同的消息，从而增加了攻击的难度）

Hash 函数中重复使用了**压缩函数** f，它的输入包括两部分：前一步中得出的 n 位结果（称为链接变量）和一个 b 位分组，输出为一个 n 位分组。链接变量的初值由算法在开始时指定，其终值即为 Hash 值，通常 $b > n$，因此称为压缩。（实验五应用了此结构）

安全哈希算法（SHA）

表 11.3　SHA 参数比较

	消息长度	分组长度	字长度	消息摘要长度
SHA-1	$<2^{64}$	512	32	160
SHA-224	$<2^{64}$	512	32	224
SHA-256	$<2^{64}$	512	32	256
SHA-384	$<2^{128}$	1024	64	384
SHA-512	$<2^{128}$	1024	64	512
SHA-512/224	$<2^{128}$	1024	64	224
SHA-512/256	$<2^{128}$	1024	64	256

注：所有的长度以二进制位为单位。

思考题

** 11.1 & 11.2 **

> 安全 Hash 函数需要具有哪些特性?

> 抗弱碰撞和抗强碰撞之间的区别是什么?

上方截图。

** 11.3 **

> Hash 函数中的压缩函数的作用是什么?

得到固定的输出长度。

** 11.5 **

> SHA 中使用的基本算术和逻辑函数是什么?

模 2^{64} 或 2^{32} 加，循环移位，与，或，非，异或。