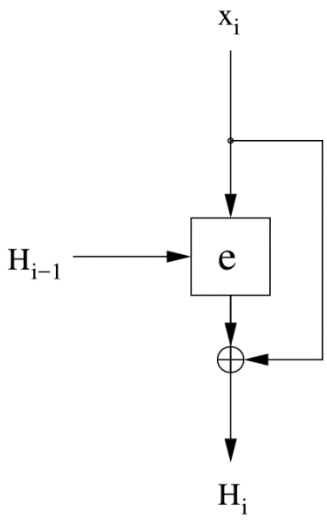
Hash 函数作业

1. 为什么存储口令 (Password) 的 Hash 值的时候往往需要进行加盐 (Salt) 处理?
   说明: 所谓 Salt 就是随机的字符串。加盐存储是指每当用户注册账户时, 服务器会随机生成一个 Salt 字符串, 然后计算口令 (Password) 和 Salt 字符串连接的 Hash 函数值, 将盐 (Salt) 和 Hash 值存储在服务器的口令表中。

2. 考虑用 RSA 加密算法构造哈希函数, 将消息分组后用 RSA 公钥加密第一个分组, 加密结果与第二个分组异或后再对其进行加密, 一直进行下去直到最后一个分组。设一个消息被分成两个分组 M_1 和 M_2, 其哈希值为 $H(M_1, M_2) = RSA(RSA(M_1) \oplus M_2)$。对于该哈希函数, 给定一个分组 C_1, 请给出另外一个分组 C_2 使得 $H(C_1, C_2) = H(M_1, M_2)$。(即对该 Hash 函数, 很容易找到碰撞。)

3. 画出下面由分组密码 $e(\cdot)$ 构造的 hash 函数的块图, 比如图(a)为 $e(H_{i\text{-}1}, x_i) \oplus x_i$ 的块图。
   (a) $e(H_{i\text{-}1}, x_i \oplus H_{i\text{-}1}) \oplus x_i \oplus H_{i\text{-}1}$
   (b) $e(H_{i\text{-}1}, x_i) \oplus x_i \oplus H_{i\text{-}1}$
   (c) $e(H_{i\text{-}1}, x_i \oplus H_{i\text{-}1}) \oplus x_i$
   (d) $e(x_i \oplus H_{i\text{-}1}) \oplus H_{i\text{-}1}$



(a) $e(H_{i-1}, x_i) \oplus x_i$

4. 假设一种 Hash 函数的计算公式如下

$$C_i = b_{i1} \oplus b_{i2} \oplus b_{i3} \oplus b_{i4} \oplus b_{i5} \oplus b_{i6} \oplus b_{i7} \oplus b_{i8}$$

   比如, 对于二进制编码 $(0000\ 0001)_2$, 其 Hash 值可用以上公式计算为 $C = 0 \oplus 0 \oplus 0 \oplus 0 \oplus 0 \oplus 0 \oplus 0 \oplus 1 = 1$。
   每个 8 位的块构成一个 ASCII 编码的字符。
   (a) 将字符串 CRYPTO 编码为二进制。
   (b) 根据以上公式计算 CRYPTO 的 6 bit 的 Hash 值。
   (c) 如何找到此 Hash 函数的碰撞, 试举出有实际意义的字符串说明。