Hash 函数与消息认证

课后习题

1. Hash函数的安全性不包括哪个性质（ D ）
   A. 单向　B. 第二原像稳固　C. 碰撞稳固　D. 输出稳固
2. 下面哪个说法不正确（ C ）
   A. 对Hash函数的攻击就是寻找一对碰撞的过程
   B. 迭代构造Hash函数时，预处理过程必须是单射的
   C. 对Hash函数的生日攻击说明，输出长度与其安全性无关
   D. Hash函数具有压缩功能
3. MAC算法的功能是实现数据的（ B ）
   A. 机密性　B. 完整性　C. 可用性　D. 非否认

Hash

单向散列函数

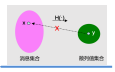
是一个将任意长度的消息映射成固定长度输出的函数

$$H:\{0,1\}^{*}\rightarrow\{0,1\}^{n}$$

input:消息　output:Hash 值　hash是有损的压缩　简单原理

原像稳固

- 给定散列值y，要找到一个x，使得H(x)=y是计算上不可行的



第二原像稳固

- 给定消息x，找到另一个x'，使得H(x)=H(x)是计算上不可行的

将以找到碰撞

生日悖论

只需23人，至少就有两个人生日相同的概率大于½
这个貌似人们直觉小得多，因而称为生日悖论

生日攻击告诉我们：为了能达到n-bit的安全性，你所选择的Hash函数的散列值长度应该是2n。

构建Hash 函数

① 预处理

用一个填充函数pad(.)在消息x右方追加若干比特，得到比特串y，使得y的长度为'的倍数。即有

y = x || pad(x) = y_1 || y_2 || ... || y_r, 其中 |y_i| = t

② 迭代处理

设H_0=IV是一个长度为m的初始比特串，重复使用压缩函数f，依次计算

$$H_i=f(H_{i-1}\|y_i)$$

直到计算出H_r为止。

③ 输出变换（可选）

设函数 $g:\{0,1\}^{m}\rightarrow\{0,1\}^{n}$, 令

$$H(x)=g(H_r)$$

著名的 Hash 函数

- MD5　第一次在 PPT 上见到两颗星
- SHA-0,1,2,3,4
- 现在 MD5,SHA-0,SHA-1 都凉了
- SHA-2-->比特币

消息认证码 MAC

不是口红,也不是笔记本

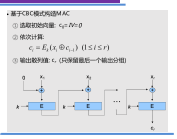
保护"完整性"　抗伪造　不知道密钥就啥都干不了

即便是知道大量的成对的消息和 MAC 也没卵用

消息认证码(MAC)算法便是这种带密钥的算法

- 它是实现数据完整性的重要工具
- 其产生的输出也相应地被称作MAC

- 基于CBC模式构造MAC
  ① 选取初始向量: $c_0=IV=0$
  ② 依次计算:
  $c_i=E_k(x_i\oplus c_{i-1})\ (1\le i\le r)$
  ③ 输出散列值: c_r (只保留最后一个输出分组)



CBC-MAC　CBC分组密码+MAC

- 将任意块一下消息x1长度为一个分组，便可产生一对碰撞
- 因为 $m_1=x_1,x_2\cdots x_r, m_2=c_r\oplus x_1$

$$CBC\text{-}MAC_k(x_1x_2\cdots x_r)=CBC\text{-}MAC_k(c_r\oplus x_1)=c_r$$

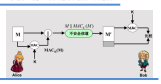
只对定长消息安全,因为如果攻击者
获取了任意消息 m=x1x2.xr-1的 MAC,C r-1=CBC-MAC_K(x1,x2...xr-1)

HMAC　Hash+MAC

其他

消息认证

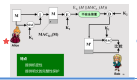
数据源认证,保证传输的完整性,保证消息的发送来自指定发送者



防止篡改

防盲充

基于 MAC 认证



提供抗赖性的消息认证　依赖两个密钥