密码学2025期末

授课教师: 张渊 时间：2025/12/25 9:00-11:30

1

1. 什么是Hybrid Encryption? 其相比单纯使用公钥加密或单独使用私钥加密有何优势 (7')
2. 数字签名的 non-repudiation 性质指的是什么？为什么 MAC 没有这个性质？(7')
3. 什么是Diffie–Hellman key exchange协议？数字签名证书在其中有什么作用？(6')

2

请给出详细计算过程

1. 在Plain-RSA加密方案中，$N = 11 \times 13$, 公钥e为7, 对应的私钥d是多少？(10')
2. 在El Gamel加密方案中，G生成的循环群$< Z_7^*, * >$, 生成元$g = 3$, 私钥$x = 2$, 公钥(G, g, q, h)中的q和h各自是多少？如果消息m的密文是$< 3, 6 >$, 那么消息$2m^2$对应的一个密文可以是多少? (10')

3 Mac

我们已知一个对于消息空间M安全的Mac协议Mac_k, 现在我们希望对于$M^l, l > 1$的消息空间加密

1. 对于每个消息块，新的Mac协议是Mac'定义如下:
   $Mac'(m_0, m_1, .. m_{l-1}) =< Mac_k(m_0), Mac_k(m_1), Mac_k(m_{l-1}) >$
   证明这个新的Mac协议不安全，对手只允许询问$Oracle$一次 (5')
2. 对于每个消息块, 新的Mac协议Mac'定义如下:
   $Mac'(m_0, m_1, .. m_{l-1}) =< Mac_{k_0}(m_0), Mac_{k_1}(m_1), Mac_{k_{l-1}}(m_{l-1}) >$
   这个新的协议安全吗？如果安全，请证明；否则指明攻击方式。(10')

4 Hash Function

$X : \{0,1\}^m, Y : \{0,1\}^n, m > n$，抗碰撞哈希函数$H : X \to Y$

1. 抗碰撞哈希函数一定是一个单向函数吗？请简要解释(5')
2. 单向函数一定是一个抗碰撞哈希函数吗？请简要解释(5')
3. 如果$H_1(x), H_2(x)$是抗碰撞哈希函数，证明$H'(x) = H_1(x) \oplus H_2(x)$不一定抗碰撞 (5')

5 RSA

在Plain-RSA加密方案中，已知A,B两个人的公钥各自为$(N_1, e_1), (N_2, e_2)$

1. 假如$N_1 \neq N_2$ ，且假设对手已知N_1, N_2不互质，证明对手能够高效计算$\phi(N_1), \phi(N_2)$ (10')
2. 假如$N_1 = N_2$, $e_1 \neq e_2$且均为质数，假如对手收到A,B两人关于同一条消息m的密文c_1, c_2, 对手如何获得m? (5')

6 Schnorr协议

考虑标准 Schnorr 签名方案。设 G 是一个阶为素数 q 的循环群，生成元为 g。$H : \{0,1\}^* \to \mathbb{Z}_q$ 是一个抗碰撞的哈希函数。选择随机私钥 $x \in \mathbb{Z}_q$，计算公钥 $y = g^x$。对于消息 m，签名者选择随机数 $b \in \mathbb{Z}_q$（nonce），计算承诺 $R = g^b$，挑战 $c = H(R, m)$，以及响应 $z = b + c \cdot x \pmod q$。输出签名为 $\sigma = (c, z)$。验证者计算 $R' = g^z \cdot y^{-c}$，并检查 $c \stackrel{?}{=} H(R', m)$。
Schnorr 协议的安全性依赖于随机数 b 的不可预测性（类似 One-Time Pad）。
假设有一个密码学库实现存在严重缺陷，并未每次生成强随机的 b，而是错误地使用了计数器模式（Counter Mode）。即：如果第一次签名的随机数为 b，则下一次签名的随机数固定为 $b + 1$。
假设攻击者截获了同一签名者发出的连续两条消息及其签名：
消息 1：(m_1, σ_1)，其中 $\sigma_1 = (c_1, z_1)$
消息 2：(m_2, σ_2)，其中 $\sigma_2 = (c_2, z_2)$
已知两次签名使用的随机数满足关系 $b_2 = b_1 + 1$。
请证明： 攻击者可以利用这两组数据有效地计算出签名者的私钥 x。(15‘)