密码学原理 (2025 秋) 期末

Lecturer: 张渊; Time: 2025/12/25 9:00-11:30; 开卷;

Problem 1. (20 分)

(1) 简述 Alice 和 Bob 如何通过 Hybrid Encryption 加密信息？这个做法相较于直接使用公钥加密/私钥加密有哪些优点？(7 分)

(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 分)

(3) Diffie-Hellman key exchange protocol 有什么应用？数字签名在其中有什么作用？(6 分)

Problem 2. (20 分)

计算题。请给出计算过程。

(1) 在 Plain RSA scheme 中，若取 $N = p \times q = 11 \times 13$、$e = 7$，$d$ 的取值是？(10 分)

(2) 在 El Gamal scheme 下，生成群 $\mathbb{Z}_7^*$ 的阶 q，生成子是 $g = 3$。若私钥 $(\mathbb{Z}_7^*, g, q, x)$ 中 $x = 2$，公钥 $(\mathbb{Z}_7^*, g, q, h)$ 中 h、q 的值是？如果消息 m 的一个 ciphertext 是 $(3, 6)$，给出 $2m^2$ 的一个合法 ciphertext。(10 分)

Problem 3. (15 分)

给定一个在消息空间 M 上 unforgeable 的 MAC $\Pi = (\mathsf{Mac}, \mathsf{Vfry})$，固定 $l > 1$，我们尝试构造 M^l 上 unforgeable 的 MAC，记明文 $m = (m_1, m_2, \cdots, m_l)$：

(1) 方法一：把 $m_1, m_2, \cdots, m_l$ 分别使用同一个密钥加密，具体来说：

$$\mathsf{Mac}'(k, (m_1, \cdots, m_l)) = (\mathsf{Mac}(k, m_1), \cdots, \mathsf{Mac}(k, m_l))$$

并用自然的方式定义 Vfry'，证明这个 MAC 不是 unforgeable 的。*你应该只进行一次询问。* (5 分)

(2) 方法二：把 $m_1, m_2, \cdots, m_l$ 使用不同的密钥加密，具体来说：

$$\mathsf{Mac}'((k_1, \cdots, k_l), (m_1, \cdots, m_l)) = (\mathsf{Mac}(k_1, m_1), \cdots, \mathsf{Mac}(k_l, m_l))$$

这个 MAC 是 unforgeable 的吗？(10 分)

Problem 4. (15 分)

给定函数 $H : \{0,1\}^m \mapsto \{0,1\}^n$，其中 $m > n$。

(1) 如果 H 是 collision-resistant 的 hash function，H 一定是 one-way function 吗？简要说明理由。(5 分)

(2) 如果 H 是 one-way function，H 一定是 collision-resistant 的 hash function 吗？简要说明理由。(5 分)

(3) 证明：若 H_1、H_2 都是 collision-resistant 的 hash function，那么 $H = H_1 \oplus H_2$ 不一定是 collision-resistant 的 hash function。(5 分)

Problem 5. (15 分)

Alice 和 Bob 各有一套 RSA scheme，它们的公钥分别是 (e_1, N_1) 和 (e_2, N_2)。

(1) 若攻击者提前得知 N_1, N_2 不互质，证明攻击者能够快速计算出 $\varphi(N_1)$ 和 $\varphi(N_2)$。(10 分)

(2) 若 $N_1 = N_2$，e_1, e_2 是不同的质数，并且攻击者已知同一条明文 m 经两人的 RSA scheme 加密后得到的密文 c_1, c_2，证明攻击者能够快速还原出明文。(5 分)

Problem 6. (15 分)

回顾 Schnorr 的数字签名技术：选取阶为质数 q 的循环群 $\mathbb{G}$，其生成元是 g，选取私钥 $\alpha \in \mathbb{Z}_q$，公钥 $pk = g^\alpha \in \mathbb{G}$，选取 Hash 函数 $H : M \times \mathbb{G} \mapsto \mathbb{Z}_q^*$:

$$
\begin{aligned}
&\mathsf{Sign}(sk, m):\\
&\quad r \xleftarrow{\$} \mathbb{Z}_q, c \leftarrow H(m, g^r), z \leftarrow c\alpha + r\\
&\quad \mathbf{return}\ (c, z)
\end{aligned}
$$

$$
\begin{aligned}
&\mathsf{Vfry}(pk, m, (c, z)):\\
&\quad \mathbf{return}\ H(m, g^z/(pk)^c) \stackrel{?}{=} c
\end{aligned}
$$

现在，我们考虑一个实现错误的 Schnorr 数字签名：每一次 **Sign** 的时候，我们不在 $\mathbb{Z}_q$ 中均匀随机的选取 r，而是初始时在 $\mathbb{Z}_q$ 中均匀随机选取一个 r_0 作为 r 的初始值，每完成一次 **Sign** 就令 $r \leftarrow r + 1$。

证明，如果一个敌手获得了 **Sign** 相邻两次运行输出的签名 $(m_1, (c_1, z_1))$、$(m_2, (c_2, z_2))$，那么他可以破译出私钥 α。