密码学复习题及答案 ver 1.0

Jer

June 9, 2014

1 密码学的基本安全问题是什么？公钥加密方案必须抵抗的攻击类型有哪些？

1.1 基本安全问题

1.1.1 机密问题

这指的是除了信息的授权人可以拥有信息以外，其他人都不可获得信息内容。在密码学中，主要是通过加密和解密算法来完成这项任务。

1.1.2 数据真实完整问题

这一问题的提出是为了发现对数据的非法变更。为了做到这一点，必须提供发现非授权人对数据变动的机制。许多密码工具可以提供这一机制，如 Hash 函数等。

1.1.3 认证问题

这是一个与识别相关的问题，可以应用于实体也可以应用于信息本身。两方在进行通信之前，一般需要识别对方的身份。而在信道上传输的一条信息也需要识别它是何时、何地、何内容由何人发出。因此，认证在密码学中常常被分成两类：实体认证和数据源认证。可以看出数据源认证隐含了提供数据真实性服务，这是因为数据被修改，数据源也就自然发生了变更。

1.1.4 不可否认问题

这一问题的提出是为了阻止实体否认从前的承诺或行为。争议的发生常常是由于实体否认从前的某个行为。例如，一个实体与另一个实体签署了购买合同，但事后又否认签署过，这时常常需要一个可信第三方来解决争议。这就需要提供必要的手段来解决争议。在密码学中，解决这一问题的手段常常是数字签名。

1.2 公钥必须抵抗的攻击类型

1.2.1 （适应性）选择明文攻击

1.2.2 （适应性）选择密文攻击

1.2.3 已知明文攻击

1.2.4 唯密文攻击

2 扩展 Euclidean 算法计算最大公约数 (a, b) 以及整数 x 和 y 满足 (a, b)=ax+by 的过程，这里 a 和 b 都是整数。如何应用费马小定理计算 $2^{1000000}$ 模 19 的最小正整数。如何应用中国剩余定理计算同余组。群、环、域的基本概念。

3 几种提高 DES 安全强度的方法。修改发现码 (MDC) 的性质有哪些？

3.1 提高 DES 安全强度的方法

1) 双重 DES 加密是使用一个密钥加密明文接着再用另一个不同的密钥加密。Merkle 和 Hellman 使用中间人攻击表明双重 DES 加密与 57 比特而不是 112 比特的安全强度相当。

2) 三重 DES 加密的安全强度大约可以达到 112 比特。至少有两个版本的三重 DES 加密执行，一个是：

$$c = E_{k_1}(E_{k_2}(E_{k_3}(m))), m = D_{k_3}(D_{k_2}(D_{k_1}(c)))$$

另一个是：

$$c = E_{k_1}(D_{k_2}(E_{k_1}(m))), m = D_{k_1}(E_{k_2}(D_{k_1}(c)))$$

这两个版本都可以抵抗中间人攻击。

3) 另一个版本的 DES 加密方法由 Rivest 提出

$$c = K_3 \oplus E_{k_2}(K_1 \oplus m), m = D_{K_2}(K_3 \oplus c) \oplus K_1$$

这一方法也叫做 DESX，已经证明了其有相当的安全强度。DESX 已经自 1986 年起被用于 MailSafe 电子邮件安全系统，自 1987 年起用于 BSAFE 工具包。
这个版本的好处在于它能够很容易地在现有 DES 硬件上执行。

3.2 修改发现码 (MDC) 的性质

(1) 原像不可逆：对于几乎所有的 Hash 输出不可能计算出其的 Hash 输入。也就是，在不知道输入的情况下给定任意一个输出 y，找到任意一个输入 x′ 满足 h(x′)=y 是计算不可能的。(2) 二次原像不可逆：对于任何一个给定的输入 x，找到另一个输入 $x' \neq x$，且满足 h(x)=h(x′)，在计算上不可能。(3) 抵抗碰撞：找到两个不同的输入 x 和 x′，满足 $h(x) = h(x')$，在计算上不可能 (注意：这里两个输入可以自由选择)。

4 AES 的层有哪些? 典型的加密模式有哪些？

5 RSA 公钥加密算法及正确性证明。模 4 余 3 型素数的 Rabin 算法解密技术。

6 ElGamal 加密算法及正确性证明。

7 RSA 数字签名算法及正确性证明。

8 Gordon 强素数生成算法及正确性证明。非邻接表 (NAF) 表示。

9 电子现金的安全要求有哪些？

9.1 认证

交易中的参与者都是真实的不存在冒充者并且签名不存在伪造的情况。

9.2 真实

各种文件如订单和账单不能被变更。

9.3 隐私

具体的交易细节应该尽量保证安全。

9.4 安全

敏感的账户信息如信用卡号应该得到保护。

10 基本的 Shamir 门限方案与性质。

10.1 Shamir 的（t，n）门限方案

10.1.1 建立秘密

可信方 T 有一个秘密 $S \geq 0$ 并希望分给 n 个用户。

1) T 选择一个素数 $p > max(S, n)$, 并定义 $a_0 = S$.

2) T 选择 $t-1$ 个随机相互独立的系数 $a_1, a_2, \ldots, a_{t-1}$，$0 \leq a_j \leq p-1$, 这样可以定义一个在 Z_p 上的随机多项式：$f(x) = \sum_{j=0}^{t-1} a_j \cdot x^j$ |item T 计算 $S_i = f(i)(modp), 1 \leq i \leq n$(或者任意 n 个不同的点 i,$1 \leq i \leq p-1$), 并且安全的传递分享 S_i 以及相应的公开指标 i 给用户 P_i。

10.1.2 恢复秘密

任何 t 或更多个用户提交他们的分享。他们的分享提供了 t 个不同的点 $(x,y)=(i,S_i)$, 通过 $Lagrange$ 插值法, 可以计算出所有多项式 $f(x)$ 的系数 a_j,$1\leq j\leq t-1$, 这样秘密就是 $f(0)=a_0=S$。

10.2 性质

10.2.1 完备

给出任意 $t-1$ 或更少的分享，所有共享的秘密取值 $0\leq S\leq p-1$ 有相等的可能性

10.2.2 理想

分享的数据长度与秘密长度相等。

10.2.3 对新用户的扩展

新的分享（给新用户）可以容易的计算分配并且不影响现有的用户。

10.2.4 多种层次控制

假如单个用户有多个密码分享，其就有相对只有单个秘密分享的用户更多的分享秘密能力，而这样的安排不会影响方案恢复秘密机制。

10.2.5 无不能证明的假设

不同于许多密码方案，该方案的安全性不依赖于任何未经证明的假设（例如：数论困难问题）。

11 公平电子投币协议的安全要求是什么？如何建立一个基于平方根的公平电子投币协议。

11.1 要求

(1) Bob 必须在听到 Alice 猜测之前就已经投币。

(2) Bob 不能够在听到 Alice 猜测之后重复投币。

(3) Alice 不能在其猜测之前得到投币结果。

11.2 基于平方根的公平电子投币协议

1. Alice 选择两个大的随机素数 p 和 q, 都为模 4 余 3 型。她将 p 和 q 保密，而将 $n=p*q$ 发给 Bob。

2. Bob 随机选择一个整数 x 并计算 $y\equiv x^2(mod n)$。他将 x 保密但发送 y 给 Alice。

3. Alice 使用她的 p 和 q 计算 4 个 y 模 n 的平方根 $\pm a, \pm b$。她任意选择一个，假定为 b, 并发给 Bob。

4. 如果 $b \equiv \pm x(modn)$,Bob 告诉 Alice 她赢。如果 $b \not\equiv \pm x(modn)$，Bob 赢。

12 Schnorr 鉴别方案

12.1 系统参数选择

12.1.1

选择一个适当的素数 p 满足 $p-1$ 可以被另一个素数 q 整除。（保证模 p 的离散对数在计算上不可能。）

12.1.2

选择一个乘法阶为 q 的元 $\beta, 1 \leq \beta \leq p-1$。

12.1.3

每一方得到一份真实的系统参数 (p, q, β) 和信任中心 T 的验证公开密钥的函数，它可以验证 T 对消息 m 的签名 $S_t(m)$。(S_t 涉及在签名之前的一个适当的公开的 Hash 函数和任意一个签名机制。)

12.1.4

选择一个安全参数 t（例如，$t \geq 40$),$2^t < q$(定义一个安全等级 2^t)。

12.2 每个用户参数选择

12.2.1

每个实体 A 选择一个唯一身份 I_A。

12.2.2

A 选择一个秘密密钥 a,$0 \leq a \leq q-1$, 并计算 $v \equiv \beta^{-\alpha}(modp)$。

12.2.3

A 向 T 通过传统方式（例如，出示护照）验证自己的身份，接着将真实的 v 传递给 T，最后得到一个由 T 颁发的证书 $cert_A = (I_A, v, S_T(I_A, v))$ 将 I_A 和 v 绑定。

12.3 协议执行

A 按如下步骤向 B 验证自己的身份。

12.3.1

A 选择一个随机数 r(承诺),$1 \leq r \leq q-1$, 计算（证据）$x \equiv \beta^r(modp)$, 并发送 $(cert_A, x)$ 给 B。

12.3.2

B 通过 T 在证书 $cert_A$ 中的签名验证 A 的公开密钥 v 的真实性，接着发送一个 (从未使用过的）随机数 e(提问), $1 \leq e \leq 2^t$, 给 A。

12.3.3

A 检查 $1 \leq e \leq 2^t$ 并发送（回答）$y \equiv a{\cdot}e + r(modq)$□$B$。

12.3.4

B 计算 $z \equiv \beta^y{\cdot}v^e(modp)$, 如果 $z = x$, 接受 A 的身份。

13 密钥协商中的站对站 (STS) 协议。密钥协商协议的基本安全要求有哪些？