信息安全技术

网络安全实用教程.pdf
101.83MB

简答题（每小题5分，共20分）

计算题（每小题15分，共45分）凯撒、围栏、矩阵、RSA、Diffie-Hellman

设计题（每小题10分，20分）

应用题（15分）

重点目录 1.3 2.1 2.2.3 2.2.4 2.3 3.1 4.2

CyberSec2022-General Review-R1.pptx

第 1 章 P12
1.(3)(4)

第 2 章 P48
1.(4)(5)，2，3

第 3 章 P85
1.(1)(2)(4)(12)(13)，2

第 4 章 P108
1.(2)，2.(2)

第 5 章 P128
(2)

第 6 章 P165
1.(1)，2

第 7 章 P194
(8)(9)

信息安全软工划重点.txt

第1章 网络安全概述

1.4.1（3）为什么在网络安全技术体系中必须包括密码技术？

- 网络环境下的数据保密传递离不开数据加密技术，而网络环境下的身份真实性验证也离不开数据加密技术。
- 网络安全核心技术和应用技术依赖于数据加密。数据加密是研究和开发网络安全技术的技术基础。
- 密码技术是网络安全技术体系中的核心组成部分，因为它直接保障了数据的保密性、完整性和真实性。

1.4.1（4）网络安全技术主要保护哪两类对象？试举例说明。

- *网络中传输/存储的数据（防窃听、防篡改、保证正确与机密）；*
- *网络系统本身及其服务/应用（防入侵、DoS、恶意代码破坏，保证服务可用与系统可信）。例如：对登录口令与交易数据加密/签名属于保护数据；对服务器部署访问控制、加固与防火墙属于保护系统与服务。*

另一个版本回答（参考PPT）：

- 网络系统本身的安全性：指保障网络基础设施、硬件设备及运行环境的安全。举例：

路由器、交换机等网络设备的物理安全与配置安全，以及网络架构（如防火墙部署）的安全性。

- 网络应用系统的安全性：指保障在网络上运行的各类业务系统及其数据的安全。举例：电子邮件系统、Web服务（万维网）、电子商务交易系统及其传输和存储的数据（如用户口令、交易金额）的安全。

第2章 数据加密导论

2.4.1（4）传统加密算法的基本原理是什么？DES加密算法是如何运用这些基本原理构成一个安全的加密算法的？

传统数据加密的基本原理就是对明文数据的“替代”和“换位”。

DES算法是一个块加密算法，将明文分为64位的数据块，通过16轮循环处理，每轮采用“替代”和“换位”函数，配合不同的轮回密钥，实现对明文的加密。

2.4.1（5）什么是三重DES算法？从密码学角度分析，为什么三重DES算法可以改善DES加密算法的安全性？

三重DES算法通过多次对数据块执行DES加密算法，扩展密钥长度，以提高密文的安全性。

由于DES的密钥长度过短（56bit），三重DES通过多次加密（如3DES/2使用2个密钥、3DES/3使用3个密钥）将密钥长度扩展至112bit或168bit，从而提高抗穷举攻击能力。

2.4.2 应用题

2.4.3（1）恺撒算法和围栏算法加密

明文： meet you at six

① 恺撒加密（后移3位）：

- 明文：meet you at six
- 密文：phhw brx dw vla

② 围栏加密（两行对角线）：

- 写为对角线：

m e y u t i

e t o a s x

- 按行读：meyuti etoasx
- 合并：meyutietoasx

③ 结合恺撒和围栏：

可以先恺撒再围栏，也可以先围栏再恺撒。假设先恺撒再围栏：

- 恺撒结果：phhwvrxdwvla
- 围栏结果：phbxwlhwrdva

p h b x w l

h w r d v a

（2）矩阵加密法

明文： meet you at six

矩阵： 3×4

密钥： 3142（列顺序）

m e e t

y o u a

t s i x

密文：（按列读取）

eui myt tax eos

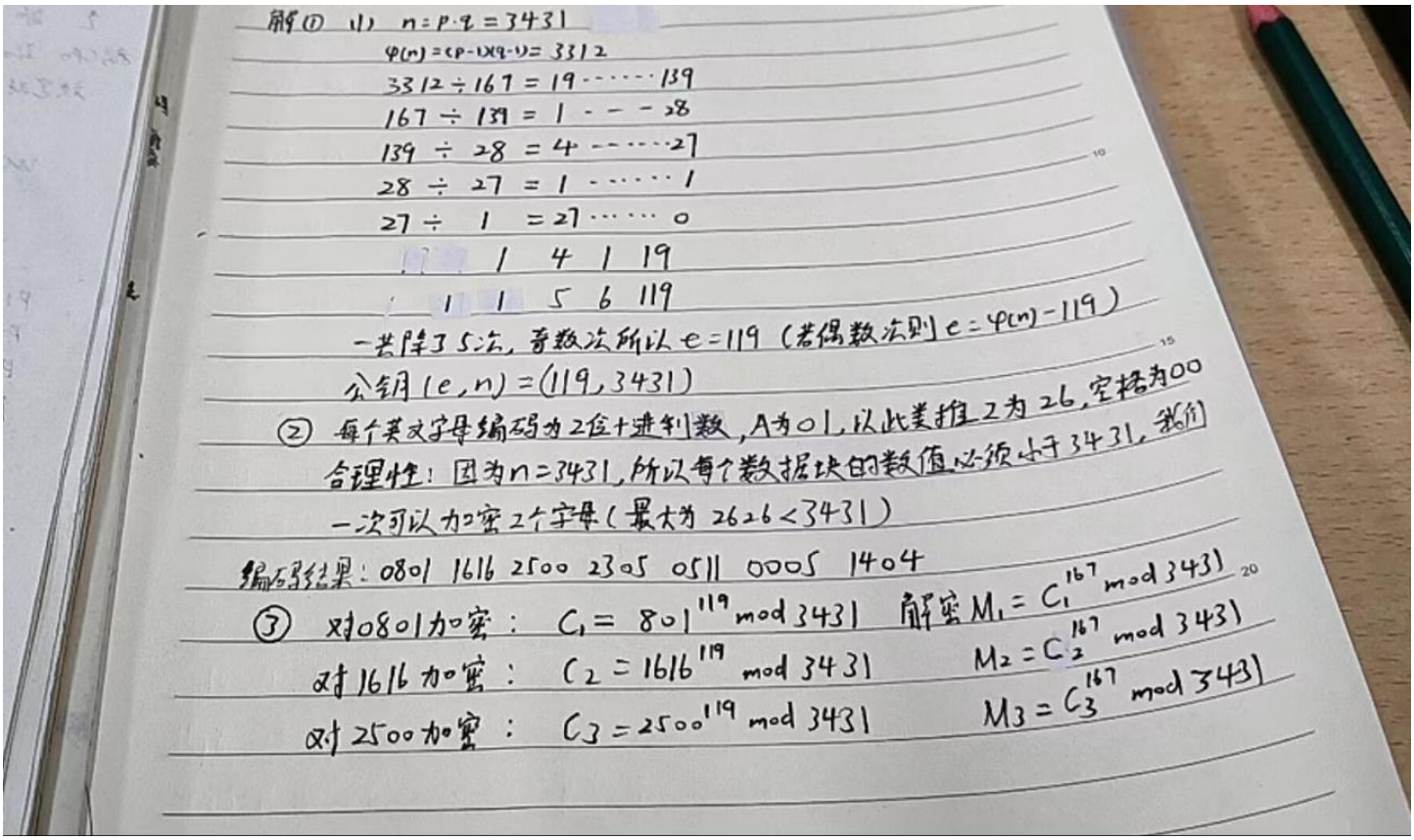
2.4.3（2）RSA 和 DH

3. 计算题

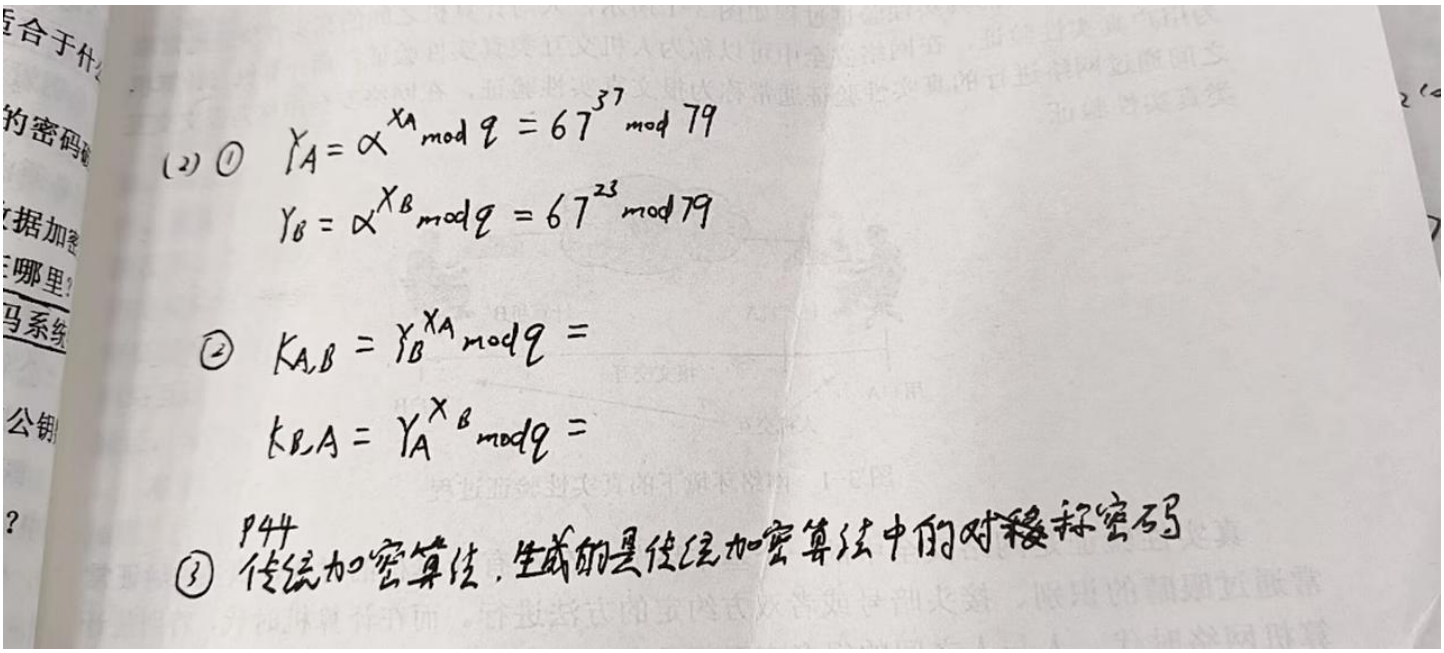
（1）假设选取素数 $p = 47$，$q = 73$，选取私钥 $d = 167$，问题：①计算 RSA 算法对应的公钥。②如果采用 RSA 算法加密“HAPPY WEEK END”，应该如何对该数据进行编码？并且说明这样编码的合理性，给出编码的结果。③采用 RSA 对以上字符串的前 5 个字符进行加密，给出对应的密文。并通过解密，验证使用 RSA 算法的正确性。

（2）对于 Diffie-Hellman 密钥生成算法，假定 q=79，α=67，X_A=37，X_B=23，问题：①写出计算 A 的公钥 Y_A 和 B 的公钥 Y_B 的公式，并求出结果。②分别写出 A 计算密钥的公式和 B 计算密钥的公式，并且分别计算其结果。③Diffie-Hellman 密钥生成算法生成的密钥是用于传统加密算法，还是用于公钥加密算法？为什么？

【数学不好也能听懂的算法 - RSA加密和解密原理和过程】
https://www.bilibili.com/video/BV1XP4y1A7Ui/?share_source=copy_web&vd_source=4e6e3d05c54fbafa49b2a00b5cc81815



$$(x\cdot y)\%m=((x\%m)(y\%m))\%m$$



假设你要算：

$$a^b \bmod m$$

步骤 1：指数写成二进制

比如

$$b = 37 = (100101)_2$$

步骤 2：不断平方并立刻取模

算下面这些（全程 mod m）：

$$a^1 \bmod m$$
$$a^2 \bmod m$$
$$a^4 \bmod m$$
$$a^8 \bmod m$$
$$a^{16} \bmod m$$
$$a^{32} \bmod m$$

每一步都是：

上一步的结果平方，再取模

数值始终 ≤ m²，计算器完全扛得住。

步骤 3：挑选二进制中为 1 的项相乘取模

因为

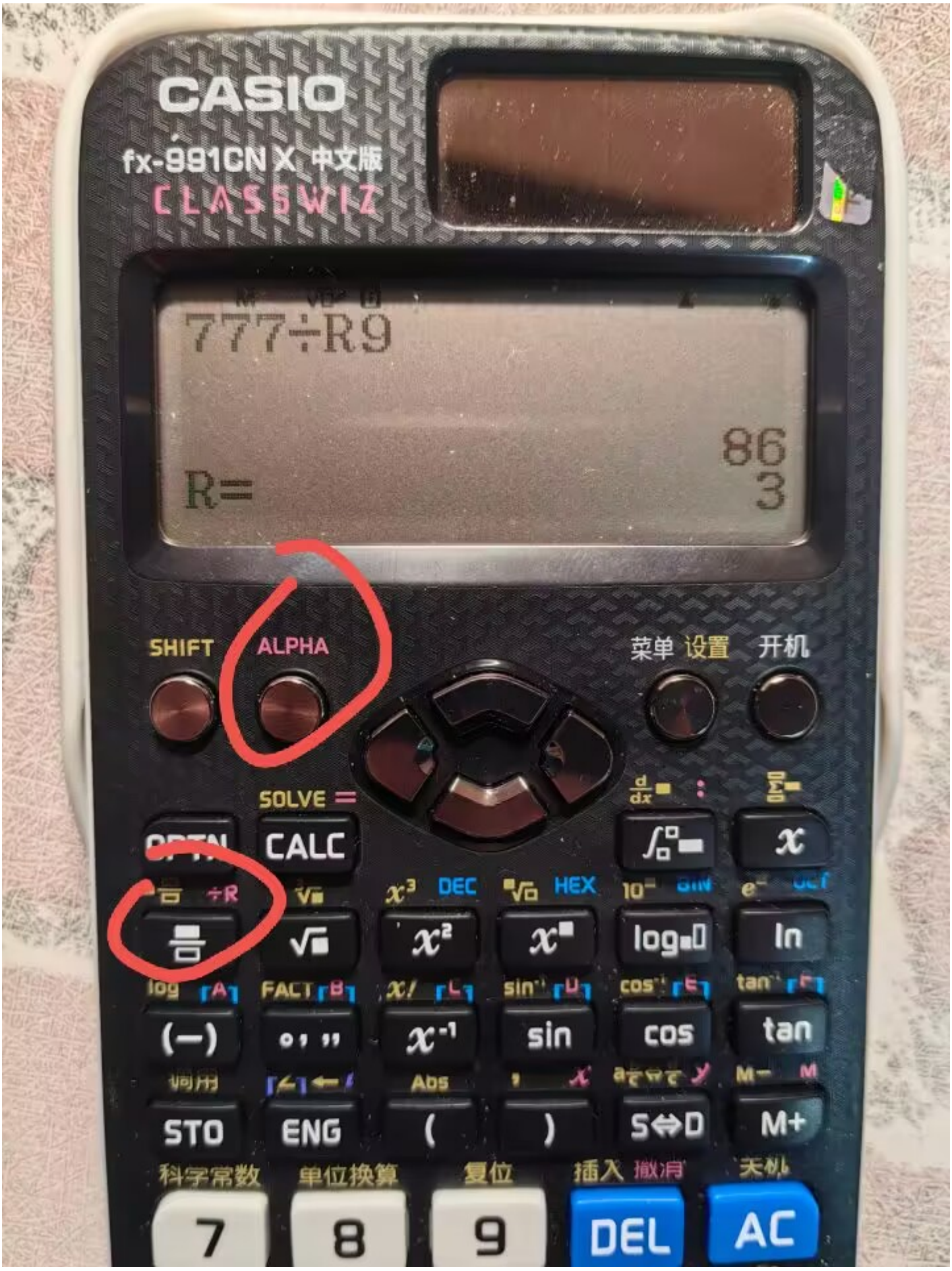
$$37 = 32 + 4 + 1$$

所以答案是：

$$a^{37} \bmod m = (a^{32} \bmod m) \cdot (a^4 \bmod m) \cdot (a^1 \bmod m) \mod m$$

结束。

没有一个“巨大数字”真正诞生过。



计算器取余

第3章 网络真实性验证

3.5.1（1）真实性验证技术可以分成哪几类？这几类真实性验证技术之间有什么关联？

- 分类：

身份真实性验证技术和报文真实性验证技术。

- 关联：

1.身份真实性验证是验证网络服务参与方或某个网络实体身份真实性的方法，也是标识和验证网络服务使用者身份的技术。

2.报文真实性验证是验证网络中传递的报文以及报文中的数据真实性的方法。

3.身份真实性验证主要是识别网络实体的身份真实性，人可以参与该验证过程。

4.网络环境下的人机交互类的真实性验证需要利用报文交互类真实性验证。

3.5.1（2）真实性验证方式有哪些？优缺点及适用环境？

方式：基于知识的真实性验证、基于标志的真实性验证、基于特征的真实性验证。

优缺点及适应环境：

基于知识的真实性验证：

- 最容易掌握，也最容易被假冒。
- 在人工交互中用户登录口令系统，在报文验证中指基于“保密字”的报文验证码技术。

基于标志的真实性验证：

- 不需要记忆数据；一旦标志物丢失，就很容易被假冒。
- 在人工交互中指采用身份识别卡的计算机或者网络登录系统，在报文验证中指采用密钥的报文验证技术。

基于特征的真实性验证：

- 不需要记忆数据，也不会丢失，是现有真实性验证技术中最为安全的一种真实性验证技术；但利用高技术也存在假冒的可能。
- 在人工交互中包括人体虹膜验证以及指纹验证系统，在报文验证中指基于“报文摘要”的报文验证码技术。

一、身份真实性验证方式

1. 基于知识的验证

优点：易掌握、实现成本低，无需额外设备。

缺点：易被猜测、泄露，安全性弱。

适用环境：普通账户登录（如网站密码、APP 登录口令）。

2. 基于标志的验证

优点：验证流程简单，携带便捷。

缺点：标志易丢失、被盗用，需配合其他验证增强安全性。

适用环境：门禁卡、银行 U 盾、硬件令牌验证。

3. 基于特征的验证

优点：生物特征唯一且难假冒，安全性高。

缺点：设备成本高，对采集环境有要求。

适用环境：高安全需求场景（如指纹解锁、虹膜登录、支付验证）

二、报文真实性验证方式

1. 报文摘要

- 优点：计算高效，仅需哈希运算，不占用过多资源。
- 缺点：无身份绑定，仅验证完整性，无法确认发送方身份。
- 适用环境：内部系统数据传输的完整性校验（无身份争议场景）。

2. 报文验证码（MAC）

- 优点：结合密钥，同时验证报文完整性和发送方身份。
- 缺点：需提前协商共享密钥，密钥管理复杂。
- 适用环境：固定双方的保密通信（如企业内部服务器间数据传输）。

3. 数字签名

- 优点：防抵赖，可通过第三方仲裁，同时验证身份和完整性。
- 缺点：依赖公钥基础设施（PKI），计算量较大，效率较低。
- 适用环境：电子商务、电子合同、重要文件传输等需法律认可的场景。

3.5.1（4）报文真实性验证的目的是什么？方法有哪些？

报文真实性验证的目的是**验证报文发送方的真实性，以及报文在传递过程中的完整性**。

方法包括：加密整个报文、加密报文校验和、附加密文块、无加密报文验证方法

3.5.1（12）什么是数字签名？为什么需要数字签名？

数字签名是采用**公钥加密算法**中签名方的私钥，对电子文件的**报文摘要**加密生成的密文。数字签名是公钥加密算法在报文验证技术中的具体应用，用于保证报文的真实性和不可抵赖性。需要数字签名是因为传统加密算法无法在双方不信任的环境下提供不可抵赖性。

数字签名

- 数字签名是采用公钥加密算法中签名方的私钥，对电子文件的报文摘要加密生成的密文。

  数字签名技术＝公钥加密技术＋报文摘要技术
- 数字签名是公钥加密算法在报文验证技术中的具体应用。公钥加密算法最为成功的应用就是数字签名。
- 问题：能否采用传统加密算法进行数字签名？
- 采用传统加密算法的报文验证技术不能进行数字签名，这是因为传统加密算法的密钥是报文发送方A和接收方B共有的。

3.5.1（13）什么是真实性验证协议？为什么需要一次性数和真实性验证服务器？

真实性验证协议是一种通过**报文交互**来验证交互的某一方或者交互双方**身份真实性**的协议。

一次性数用于防范重播攻击。

真实性验证服务器用于在多方环境中集中管理密钥和身份验证。

3.5.2 应用题：

假设已知 A 与 C 之间存在共享密钥 $K_{A,C}$，B 与 C 之间存在共享密钥 $K_{B,C}$，基于以上给定条件，请完成以下设计和分析工作：

（1）试设计一个协议，使得 A 能够向 B 验证其真实身份，并说明 A 和 B 需要进行的关键处理。

（2）如果要求 A 能够生成 A 与 B 之间的共享密钥 $K_{A,B}$，并且安全地将 $K_{A,B}$ 传递给 B，需要如何改进以上设计的真实性验证协议？

（3）具体罗列 A 和 B 分别需要进行的关键处理步骤，分析该协议能够实现真实性验证的理由，以及能够安全传递 A、B 之间共享密钥的理由。

（4）分析该协议是否存在重播攻击的可能，如果存在，应该如何进一步修改协议，并进行防范？

（1）设计协议（A向B验证身份）

M1: A → B: A

M2: B → A: N

M3: A → B: Kac{N}

M4: B → C: A, Kac{N}

M5: C → B: Kbc{N}

B验证N是否匹配。

（2）传递共享密钥Kab

在M5中，C可附加加密的Kab：

M5: C → B: Kbc{N, Kab}

（3）A与B的关键处理步骤

- A生成Kab，用Kac加密发送给C。
- C验证A身份，用Kbc加密Kab发送给B。
- B用Kbc解密获取Kab。

（4）重播攻击分析

可能被重播M3或M5。可引入时间戳或一次性数+时间戳。

第4章 网络访问控制

4.3.1（2）概念题：什么是访问控制的主体？什么是访问控制的客体？

- 访问控制的主体是访问被访问控制系统保护的网络资源的某个网络实体，也是被网络访问控制系统授权的网络实体。在网络安全中，访问网络或网络应用的任何网络实体都是网络访问控制的主体。

- 访问控制的客体是被访问控制系统保护的网络资源。在网络安全中，任何提供服务的网络实体都是网络访问控制的客体，某个网络区域也可以作为访问控制的客体。

主体*

- 在信息安全中，代表用户访问网络或使用网络应用的某个实体是访问控制的“ 主体(Subject)”。
- 在网络安全中，代表用户访问网络或使用网络应用的任何实体都是访问控制的主体，这是访问控制中被控制方。
  - 例如电子邮件的客户端软件、万维网（WWW）客户端软件、文件传送系统的客户端软件
- 主体是访问控制的请求方。

156

客体*

- 在信息安全中，任何被访问网络的实体或被使用网络应用的实体都是访问控制的“ 客体(object)”。
- 在网络安全中，任何提供网络服务或网络应用的实体都是客体。
  - 例如，万维网（WWW）服务器、文件服务

器等。

- 客体是访问控制的被保护方。

157

4.3.2（2）应用题

如果需要设置一个分组过滤器，作为公共互联网与企业外部网之间的网络层防火墙。其安全策略1:只允许公共互联网访问企业外部网中的WWW 服务器(210.110.10.1)和邮件服务器(210.110.10.3)。安全策略:不允许attacker.com域名的子网(220.10.16 0.0)中的站点访问该www服务(端口号为80),不允许spam.com域名的子网(230.1 01.13 0.0)访问该电子邮件服务(端口号为25)。需要解决以下问题:

1)请设计该分组过滤器的访问控制列表，并说明各项含义。

动作	源 IP 地址	源端口号	目的 IP 地址	目的端口号	说明
禁止	220.10.160.0	*	210.110.10.1	80	阻止 attacker.com 子网访问 WWW 服务器
禁止	230.101.130.0	*	210.110.10.3	25	阻止 spam.com 子网访问邮件服务器
允许	*	*	210.110.10.1	80	允许所有公共互联网访问 WWW 服务器
允许	*	*	210.110.10.3	25	允许所有公共互联网访问邮件服务器（已受第二条限制）
禁止	*	*	*	*	默认规则：禁止所有其他未明确允许的流量，符合企业外部网安全策略要

各项含义说明：

动作：分为“允许”或“禁止”。

源 IP 地址：表示发起请求的子网或主机。

目的 IP 地址：表示企业外部网中的服务器地址。

目的端口号：表示服务类型，80 对应 HTTP（WWW），25 对应 SMTP（邮件）。

说明：解释该条规则的安全意图。

通配符“”：表示“任何值”。

规则顺序：必须严格按照顺序执行，先禁止特定子网，再允许合法服务，最后默认禁止。

2)如果发现公共互联网的一个网站(240.10.12.1)是恶意网站，应如何更新网络层防火墙的配置，保护企业外部网的WwW服务器和邮件服务器?

网络防火墙的配置应遵循“先禁止、后允许、最后默认禁止”的原则，确保安全策略的有效性和可维护性。

新增禁止规则：在 ACL 的最前面添加一条规则，禁止该恶意网站的 IP 地址访问企业外部网的所有服务器。规则顺序说明：将新规则置于所有“允许”规则之前，确保在允许合法访问之前先拦截恶意流量。更新后的规则表仍以默认禁止结尾，确保仅允许明确授权的流量。新的访问控制列表如下：

动作	源 IP 地址	源端口号	目的 IP 地址	目的端口号	说明
禁止	240.10.12.1	*	*	*	阻止恶意网站访问任何服务
禁止	220.10.160.0	*	210.110.10.1	80	阻止 attacker.com 子网访问 WWW 服务器
禁止	230.101.130.0	*	210.110.10.3	25	阻止 spam.com 子网访问邮件服务器
允许	*	*	210.110.10.1	80	允许所有公共互联网访问 WWW 服务器
允许	*	*	210.110.10.3	25	允许所有公共互联网访问邮件服务器（已受第二条限制）

禁止	*	*	*	*	默认规则：禁止所有其他未明确允许的流量，符合企业外部网安全策略要

第5章 网络攻击与防御

5.5.1（2）网络攻击目前可以分成哪几种类型？试对照网络安全的三个特性，分析这几类网络攻击的意图有何不同。

网络攻击目前可以分成以下三种类型：

- 基于直接系统渗透的网络攻击
- 基于间接渗透的拒绝服务攻击
- 高级持续威胁攻击

对照网络安全的三个特性（保密性、完整性、可用性），它们的攻击意图不同：

- 基于直接系统渗透的网络攻击：主要破坏网络及其应用系统的**保密性**和**完整性**，如窃取数据、插入恶意代码。
- 基于间接渗透的拒绝服务攻击：主要破坏网络系统的**可用性**，如通过大量无效请求使服务瘫痪。
- 高级持续威胁攻击：综合破坏**保密性**、**完整性**和**可用性**，目的是长期潜伏并窃取、破坏甚至摧毁目标系统。

第6章 网络安全加固

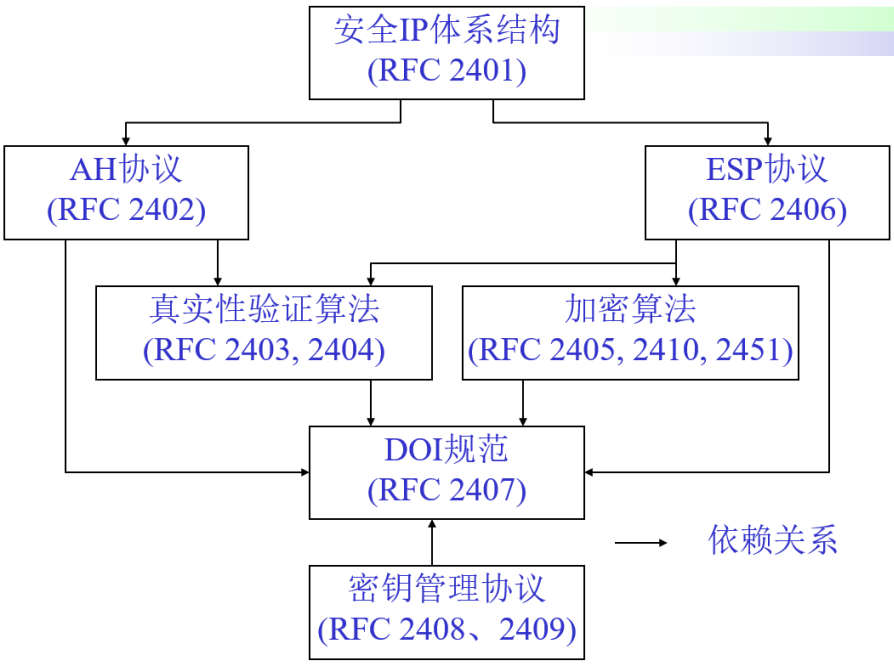
6.3.1(1) 什么是安全IP(IPsec)技术？它由几个部分构成？安全IP协议簇由哪几部分构成？

安全IP是在IP层为IP数据报提供安全服务的一组协议与机制。安全IP技术是互联网工作组标准化的一种面向IP层的安全技术，它是真实性验证技术、加密算法、密钥管理技术在IP层中的具体应用。P130

总体由4个部分构成：安全协议、安全关联、密钥管理以及真实性验证算法与加密算法。P131

协议簇构成：IPsec 协议簇主要由以下部分构成: AH协议、ESP协议、DOI 规范、密钥管理协议、真实性验证算法、加密算法。P135

IPsec协议簇



安全IP协议簇组成结构图

- IPsec由一组IETF定义的IPsec技术标准描述，这组协议称为IPsec协议簇。

17

6.3.2 应用题 P166

一位公司经理在外地洽谈业务，需要通过公共互联网从公司的网络服务器下载一批商业资料和文件，请问：

（1）如果不进行任何的安全防范而直接通过公共互联网下载商业资料，会存在哪些安全风险?

可能被窃听泄密、篡改数据、假冒服务器/中间人攻击、重放攻击、植入恶意代码，甚至导致业务凭据泄露与服务不可用。

（2）如果该公司企业网已经建立了基于安全IP技术（IPsec）的网络安全系统，并对该经理试图访问的企业数据服务器进一步采用IPsec进行了安全保护，则至少需要通过几条安全关联（SA）才能访问到该服务器?

- 至少需要两条安全关联。IPsec 的安全关联是单向（单工）的，客户端到服务器和服务器到客户端分别需要一条 SA。

（3）如果该经理试图通过IPsec保密地与公司服务器传递文件，他应该选择哪种安全协议？该协议应该绑定在哪条安全关联上?

- 应选择 ESP 协议

- 该协议应绑定在 用于数据传输的 IPsec 安全关联（SA） 上。

（4）如果该公司企业网已经建立了基于IPsec的安全系统，并且该经理试图访问的企业数据服务器也已经进一步采用IPsec进行了安全保护，则该经理离开公司前需要进行哪些处理？

1. 预配置IPsec参数：
    - 与IT部门协调，获取IPsec配置（如IKE版本、加密算法、预共享密钥或证书）。
2. 安装VPN客户端：
    - 若企业使用IPsec VPN，需提前安装并配置VPN客户端软件。
3. 密钥/证书分发：
    - 获取个人私钥和服务器公钥（或预共享密钥），并安全存储（如硬件令牌或加密文件）。
4. 测试连接：
    - 在公司内网测试IPsec/VPN连接，确保配置正确。

（5）如果该经理持有他自身私钥和该服务器的公钥，则他可以采用哪种安全关联创建协议来建立安全关联，为什么？

- IKE 协议
- 因为该机制可利用公钥/私钥完成通信双方的身份认证，无需预先共享密钥，安全性较高。

（6）试描述采用该安全关联创建协议来进行协议交互的主要步骤。

补充：IKE有主模式（6步）和自信模式（3步）参考下面例题

M3：A→B 密钥交换与身份标识（HDR, KE, [HASH(1),] PK_B{$<ID_A>$}, PK_B{$<N_A>$}）

- **KE（Key Exchange）**：A生成DH公钥，并发送给B（用于后续密钥计算）。
- **PK_B{$<ID_A>$}**：A用B的公钥（PK_B）加密自己的身份标识（ID_A，如用户名或设备ID），确保身份信息机密性。
- **PK_B{$<N_A>$}**：A用B的公钥加密一个随机数N_A（防重放攻击）。
- **[HASH(1)]**（可选）：对前两步协商的SA参数和KE数据进行哈希，验证完整性（部分实现中包含）。

P157例题

【例题】 假设某个销售人员在外地试图通过公共互联网从公司网络服务器中下载销售资料和文件。请问：

（1）如果该销售人员不采用任何安全技术直接从公司服务器获取数据，会遇到哪几种安全威胁？

（2）该销售人员考虑采用安全技术，则他至少应该从哪几个方面考虑安全技术？

（3）如果他试图保密地传递客户订单，他应该选用何种安全 IP 中的安全协议？

（4）如果他试图完整地传递客户促销计划，他最好选用哪种安全 IP 中的安全协议？

（5）如果他选择安全 IP 技术作为安全防范技术，他该如何进行身份验证？

（6）如果公司服务器提供了访问控制机制，需要根据用户标识来控制对公司服务器的访问权限，这时他应该选择哪种类型的安全关联建立协议？

（7）假定用户已经获得包括自己私钥和公司服务器公钥的证书，试具体描述这种用于身份验证和安全关联建立的协议的主要步骤。

答：（1）如果不采取安全防范技术，他获取的销售资料就可能被窃取、更改、假冒，还可能无法访问到公司的服务器。

（2）他至少应该从身份验证、访问控制和攻击检测三个方面考虑对安全技术的选择。

（3）为了保密地传递数据，应用安全 IP 技术时，必须采用 ESP 协议。

（4）为了完整地传递数据，应用安全 IP 技术时，最好采用 AH 协议。

（5）为了进行身份验证，必须首先通过其他安全途径（如在离开公司之前，直接到公司人力资源部）获得与他相关的用户标识和密钥（可以是公钥，也可以是共享密钥）等个人身份数据，然后，在第一次网络连接过程中输入相关个人身份数据。

（6）由于用户标识是系统进行访问控制的依据，所以，在应用 IPsec 技术创建安全关联时，必须采用具有用户标识保护功能的安全关联来创建协议。

（7）运用 IKE 协议，选用主模式下基于公钥身份验证的安全关联创建协议如下。

$M1$: A→B: HDR, SA

$M2$: B→A: HDR, SA

$M3$: A→B: HDR, KE, [$HASH(1)$,] $PK_B\{<ID_{A1}>\}$, $PK_B\{<N_A>\}$

$M4$: B→A: HDR, KE, $PK_A\{<ID_{B1}>\}$, $PK_A\{<N_B>\}$

$M5$: A→B: HDR*, $HASH_A$

$M6$: B→A: HDR*, $HASH_B$

第7章 网络安全应用

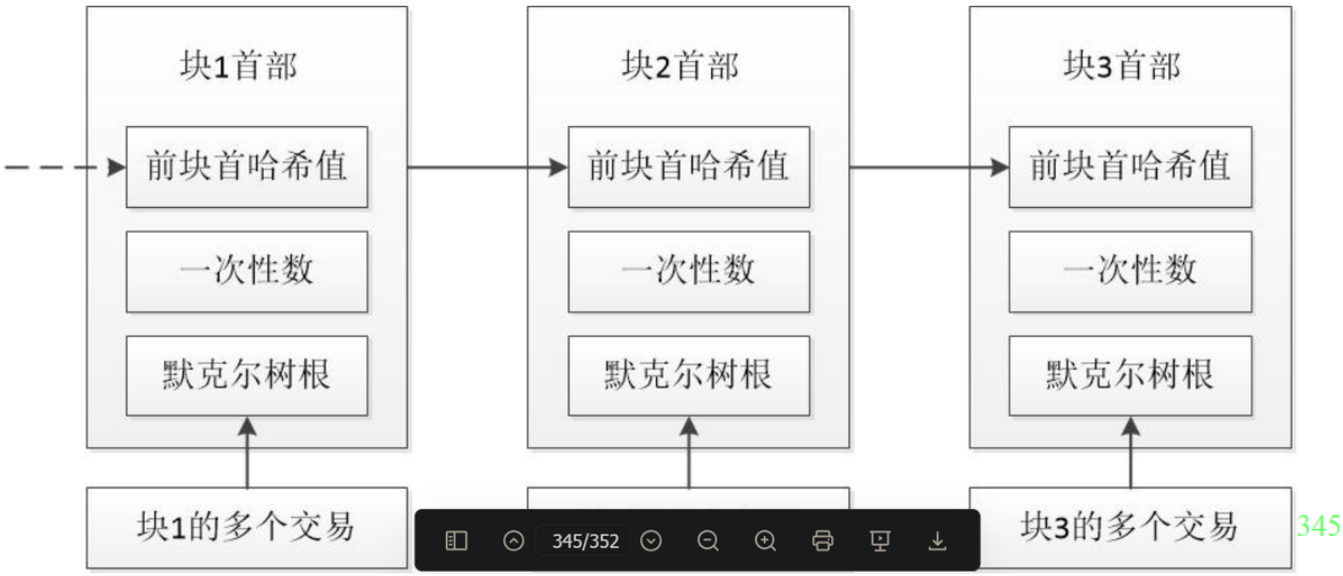
7.4（8）区块链为什么被称为“公用账本”？区块链是如何确保其“账本”的公用性的？

- 公用账本：区块链记录了比特币所有的交易账单，充当了整个系统的公共交易记录簿。

- 确保公用性：比特币系统的每个结点都保存和维护有效的所有区块（即完整的账本副本）。每个区块记录了一次或多个交易，通过对等网络（P2P）广播，确保全网节点拥有一致且公开的账本信息。

区块链是比特币的公共账本

- 区块链记录比特币的所有的交易账单。
- 比特币系统的每个结点保存和维护有效的所有区块链。
- 每个块记录了一次或多个交易。



7.4（9）区块链是如何确保网络环境下的去中心化信任交易的？

- 非对称密钥：用户通过自己生成的私钥和公钥（钱包）来证明身份和资产所有权，无需银行或 PKI 等中心化机构介入。
- 数字签名：利用数字签名技术保证交易的真实性、完整性和不可抵赖性。
- 共识机制 (POW)：采用工作量证明（挖矿）和最长链原则，通过全网算力竞争来记账，有效防止“重播攻击”和“女巫攻击”，从而在无中心化管理的情况下建立信任。