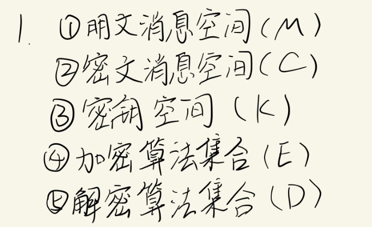
**密码学**

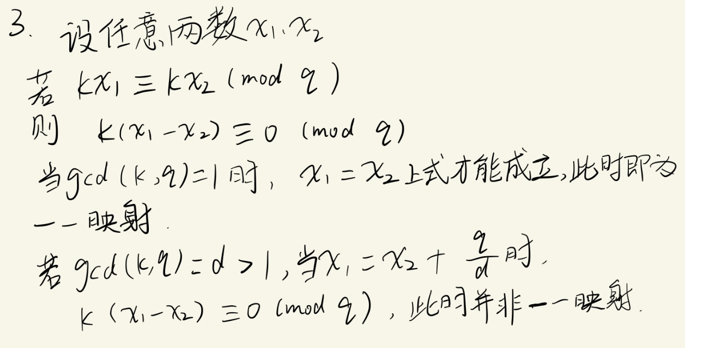
1. **密码体制五要素是什么？**



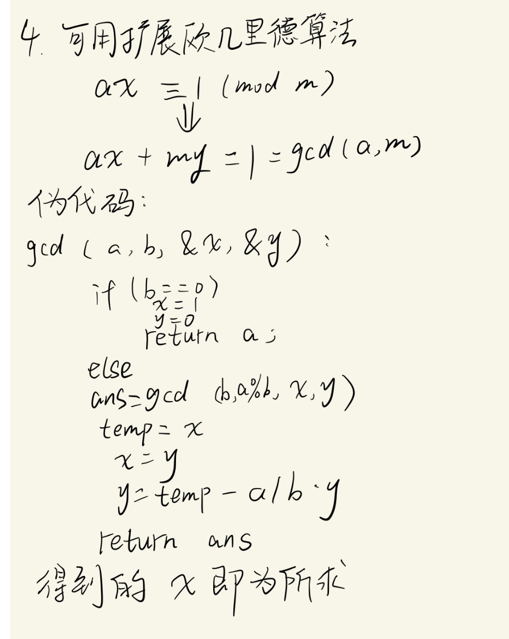
1. **俄语共有32个字母，设计一个乘数密码来加密俄语信息，并计算一下潜在的加密密钥有多少个，并列举。**

gcd(x,32)=1共有15个。如3m%32

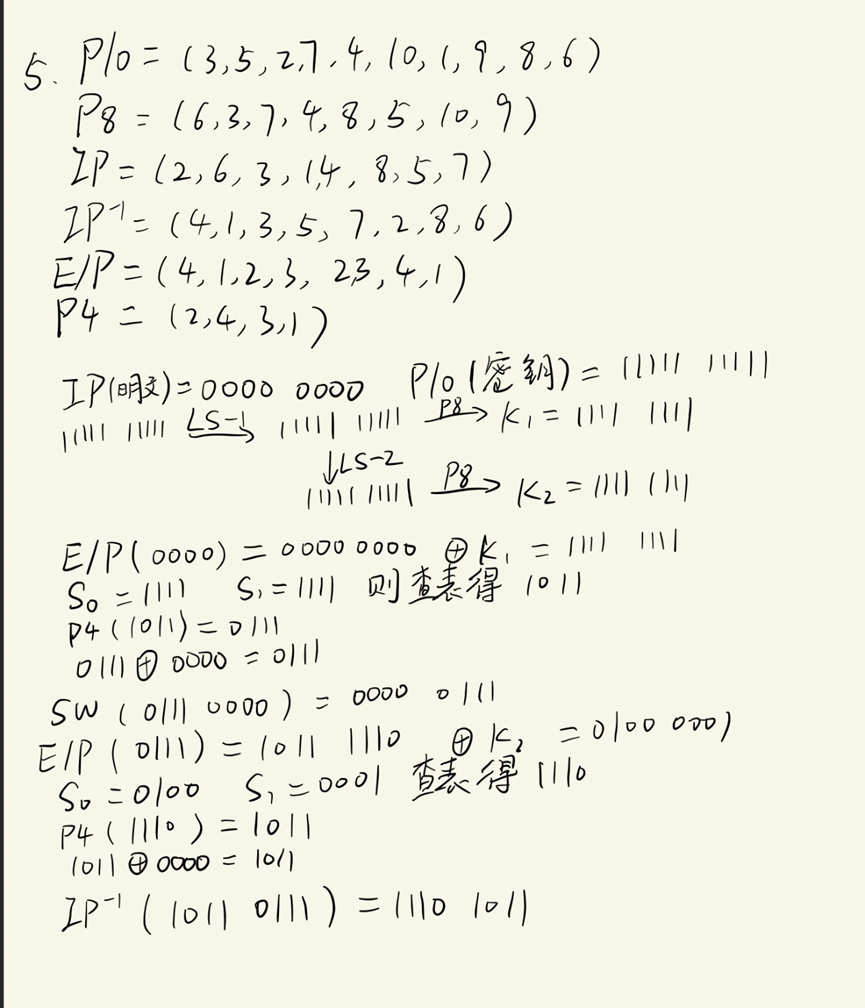
1. **乘数密码中，当gcd(k, q)=1时，加密变换才是一一映射的。试证明之。**



1. **乘数密码中，如何计算k-1？此处k-1为k在模q下的乘法逆元？请给出算法伪代码。**



1. **给定密钥“11 1111 1111”，明文“00000000”，计算S-DES的密文。请按给出主要计算过程。**



6. **Alice和Bob使用Diffie\_Hellman协议协商共享密钥，得知使用的素数q=13，原根a=2。如果Alice传递给Bob YA=12，则Alice的随机数XA是多少？如果Bob传递Alice YB=6，则共享的密钥K是多少？**

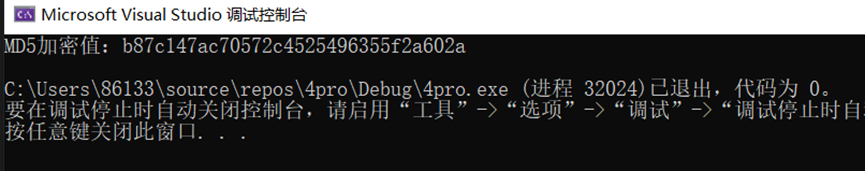
2^6%13=12,故XA=5，K=6^6 mod 13 = 12

**7.如果攻击者截获了Alice发给Bob的消息C为10，并得知加密密码是RSA（公钥：e=5，n=35），那么明文M是什么？**

p=5，q=7

e对24的逆元为d=5，明文为10^5 mod 35 = 5

**8.给定消息“000……000”（512位二进制数），通过编程计算其MD5值。请给出主要计算步骤和中间结果（16进制）。**



**9.有人说“所有的散列函数都存在产生碰撞的问题，很不安全”，你认为正确与否，为什么？**

理论上，所有的散列函数都存在碰撞问题，因而存在安全问题，可以类比生日悖论，可以增大表示消息摘要的位数，在位数较长的情况下，在一段时间内不容易被穷举攻击攻破。

**物理安全**

**1.物理安全主要包括哪些内容？**

物理安全主要包括防盗、防火、防静电、防雷击、防信息泄漏、物理隔离以及基于物理环境的容灾技术和物理隔离技术。

**2.物理隔离和逻辑隔离的区别是什么？**

①物理隔离是通过物理方法将内网与外网隔离从而避免入侵或者信息泄露。

②逻辑隔离的两端仍然存在物理上的连接，但通过技术手段保证被隔离的两端在逻辑上隔离。

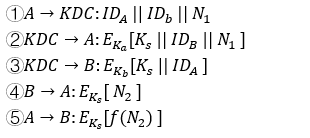
**身份认证**

**1.“挑战应答方式”认证和Needham-Schroeder对称密钥认证协议的区别？模仿Needham-Schroeder设计一个三方通讯认证协议。**

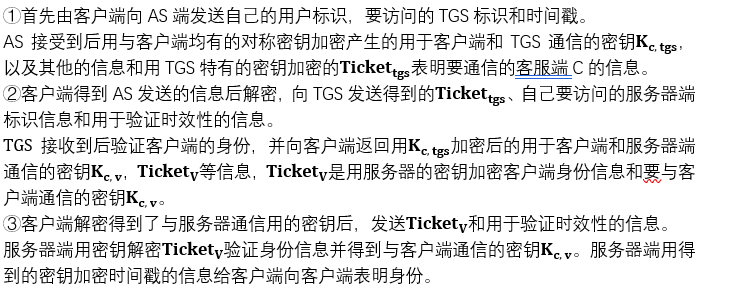
挑战应答方式是由验证方发送一个随机串给示证方，示证方用密钥加密后返回给验证方，验证方通过相同的密钥解密来验证身份，只涉及两方操作。

Needham-Schroeder则存在可信任的第三方，由第三方作为中介，通过分别与两方产生密钥建立联系，最终用第三方产生的密钥建立联系。

可以建立一个类似于Needham-Schroeder的方法：



**2. 解释详细Kerberos认证协议过程。**



**3. 什么是数字证书，如何使用数字证书进行身份认证？**

数字证书是一个经过权威的、可信赖的、公正的第三方机构（即CA认证中心，Certificate Authority）签名的包含拥有者信息及公开密钥的文件。

①A提交资料申请证书

②CA审核并颁发用CA的私钥签名的数字证书

③A向B发送用A的私钥签名的特定信息和数字证书

④B获取CA的公钥并对A发送的数字证书进行验证，验证通过则可获得A的公钥，得到A的公钥后即可对A用私钥签名的特定信息解密，从而确认A的身份及签名的信息。

**4. 什么是PKI，它包含那些主要功能，如何工作？**

PKI是一种遵循一定标准的密钥管理基础平台，为所有网络应用提供加密和数字签名等密码服务所必需的密钥和证书管理。

包含的功能有：

1.接收验证用户数字证书的申请；

2.确定是否接受用户数字证书的申请；

3.向申请者颁发（或拒绝颁发）数字证书；

4.接收、处理用户的数字证书更新请求；

5.接收用户数字证书的查询、撤销；

6.产生和发布证书的有效期；

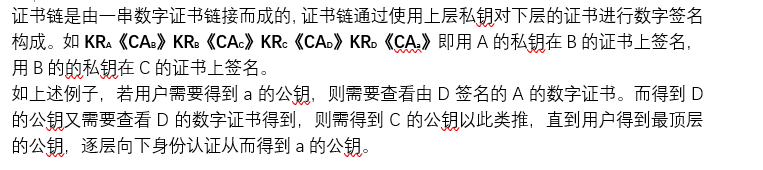
7.数字证书的归档；

8.密钥归档；

9.历史数据归档。

PKI的认证机构完成数字证书的申请注册、证书签发和管理，在生成证书时会完成密钥的备份，当用户丢失密钥需要恢复时，可以通过备份恢复。当用户密钥泄露或其他原因需要撤销原来的证书时，可将原证书加入黑名单。证书库供公众查询颁发和撤销的证书，且提供专门的PKI应用接口供人使用。

**5. 什么是证书链，X.509是如何实现证书认证的？**



**访问控制**

**1.** **DAC与MAC有什么不同？**

DAC是以用户或者用户组为主体来访问客体的，每个用户或用户组有一定的权限来访问特定的客体，且可以自主地把拥有的访问权限授予其他用户。

而MAC是为主体和客体分配了不同的安全级别属性，通过设置的访问规则如向下读、向上写来控制主体对客体的访问操作，故权限没办法从一个主体转移到另一个主体。

**2.** **角色与组的区别是什么？**

组一般是由有某些相同特质的用户组成集合，可以为一个组赋予权限从而使得组内的成员获得该组的权限。

而角色是一个行为和责任的集合，代表了一定的权限，实现了权限和用户分离，所以可以将角色分配给用户或者组，使得用户或组内的用户获得该角色拥有的能力和责任。

组主要指用户的集合，而角色代表了责任和能力。

**3.** **Windows系统的安全体系结构包括哪些内容？**

Windows系统的安全体系结构包括用户认证、访问控制和加密、管理和审计、安全策略。

Windows系统安全开始于用户认证。加密保证了系统与用户之间的通信及数据存储的机密性。访问控制则维护了用户访问的授权原则。

审计和管理处于系统的内核层。审计可以发现系统是否曾经遭受过攻击或正在遭受攻击，并进行追查；管理则是为用户有效控制系统提供功能接口。

**网络威胁**

**1. 传统病毒与蠕虫有什么区别？**

传统病毒是寄生于宿主文件内，以可移动介质为传播途径的计算机病毒。蠕虫病毒是利用网络进行复制和传播，以独立智能程序形式存在的计算机病毒。所以，蠕虫病毒不需要寄生在宿主文件，传播途径主要包括局域网内的共享文件夹、电子邮件、网络中的恶意网页和大量存在着漏洞的服务器等，而传统病毒需要依赖可移动介质。

**2. 木马的传播途径有哪些？**

木马主要通过电子邮件附件、被挂载木马的网页以及捆绑了木马程序的应用软件传播。

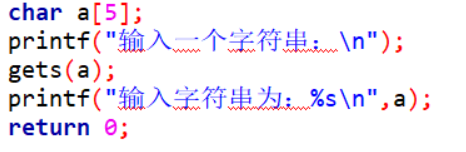
**3. ARP欺骗的原理是什么？**

主机间通信，要把IP地址转化成MAC地址。ARP欺骗就是根据ARP协议，向想要窃听的两个主机发送应答数据包，从而修改被窃听主机的ARP地址缓存表，从而更改了IP地址为自己的MAC地址，这样两个主机通信时就会先把数据包发送给自己，从而窃听。

**4. DNS欺骗是如何实现的？**

当用户要查询一个IP发送DNS请求包后，伪造一个DNS应答包，冒充其要查询的IP返回给用户，从而实现欺骗。

**5. 不使用strcpy()函数，写一个能引起缓冲区溢出的小程序，并简要解释该程序为什么会引起缓冲区溢出。**



**网络防御**

**1. 静态包过滤和动态包过滤有什么区别？**

静态包过滤是防火墙根据定义好的包过滤规则审查每个数据包是否满足规则，动态包过滤是防火墙采用动态配置包过滤规则的方法。

静态包过滤是依据数据包的包头信息进行控管，是静态的。而动态包过滤是基于会话，动态建立和删除规则，且会对批准的连接进行跟踪，是动态的。

**2. DMZ的主要功能是什么？**

DMZ是设立在非安全系统与安全系统之间的缓冲区，通过将需要外网访问的服务器放到这个隔离区，起到内外网隔离，从而更好保护内网的作用。

**3. 代理网关与电路级网关有什么区别？**

代理网关的代理协议以应用层为主，电路级网关代理协议以传输层为主。代理网关的工作量更大，但安全性更好。电路级网关由于不需要审计应用层数据，因而工作量远小于应用代理网关，但安全性低于应用代理网关。

**4. 误用检测和异常检测有什么区别？**

误用检测是事先定义出已知的入侵行为的入侵特征，将实际环境中的数据与之匹配，根据匹配程度来判断是否发生了入侵攻击行为。

异常检测是根据使用者的行为或资源使用状况的程度与正常状态下的标准特征（活动轮廓）之间的偏差来判断是否遭到入侵。如果偏差高于阈值，则发生异常。

因而误用检测依赖于已知的具体行为，要不断更新已知入侵特征，而异常检测不依赖，通用性较强，但确定偏差是否达到阈值有难度。

**5. 什么是CIDF模型，包含哪些内容？**

CIDF是对IDS进行标准化和研究的一个开放组织。CIDF通用模型包括：事件产生器，事件分析器，事件数据库，响应单元。

**6. 有人说，“防火墙的包过滤技术发展到应用层，就可以取代入侵检测系统。”你认为正确与否，为什么？**

我认为不行，防火墙只是静态检测，对已经通过防火墙的数据包就不再检查，而入侵检测系统是动态的，对数据实时进行检测，可以进一步检测防火墙没有发现的入侵行为，从而提高安全性。

**网络安全协议**

**1. IPSec的两个主要协议有什么区别？**

ESP协议对IP数据报文实施加密和可选认证双重服务，而AH协议对IP数据报文实施认证服务，提供数据源认证、无连接的完整性以及一个可选的抗重放服务，没有对数据包的内容加密。

**2. IPSec是如何防范重放攻击的？**

在安全关联SA中定义了序号计数器和抗重放窗口。其中序号计数器提供了设置IPSec包中序列号域的值。序列号按顺序递增，仅当收到的消息序数顺序合法时才接受。

**3. HTTPS是如何实现数据的安全性的？**

HTTPS在HTTP下加入了SSL协议，通过建立一个信息安全通道，用来保证数据传输的安全，通过CA证书以及认证服务确认网站服务器和客户端的真实性，从而实现数据的安全性。

**4. SET协议要解决的主要问题有哪些？**

①保证交易信息在互联网上安全传输，防止数据被黑客或被内部人员窃取。

②保证电子商务参与者信息的相互隔离。客户的资料加密或打包后通过商家到达银行，但是商家不能看到客户的账户和密码信息。

③持卡人和商家相互认证，以确定通信双方的身份，由第三方机构负责为在线通信双方提供信用担保。

④保证网上交易的实时性，使支付过程都是在线的。

⑤要求软件遵循相同协议和报文格式，使不同厂家开发的软件具有兼容性和互操作功能。

**5. SET协议是如何保证商家、顾客和银行之间数据隐私的安全性的。**

在消费者发出付款指令后，消费者、在线商店、支付网关都通过CA来验证通信主体的身份，以确保通信的对方不是冒名顶替。通过双重签名，分离PI与OI，从而确保商家不知道顾客的支付卡信息，银行不知道顾客的订购细节。最终保证商家、顾客和银行之间数据隐私的安全性

**内容安全**

**1. 有人说“数字水印就是在视频或图像中可见的版权信息标识”，你认为正确与否，为什么？**

我认为不正确。数字水印是镶嵌在数据中，并且不影响合法使用的具有可鉴别性的数据。它一般应当具有不可察觉性、抗擦除性、稳健性和可解码性。

**2. 有人说“内容监管技术与入侵检测技术相同，可以通过简单改造IDS实现内容监管功能”，你认为正确与否，为什么？**

我认为不正确。入侵检测技术是主动保护自己免受攻击的一种网络安全技术，是防火墙的一种补充，对通过防火墙的数据继续监测，对检测的异常进行违规处理。而内容监管包括数据获取策略、敏感特征定义、违规定义、违规处理策略。故无法通过简单的改造IDS实现内容监管功能。

**信息安全管理**

**1. 如何理解信息安全管理的内涵？**

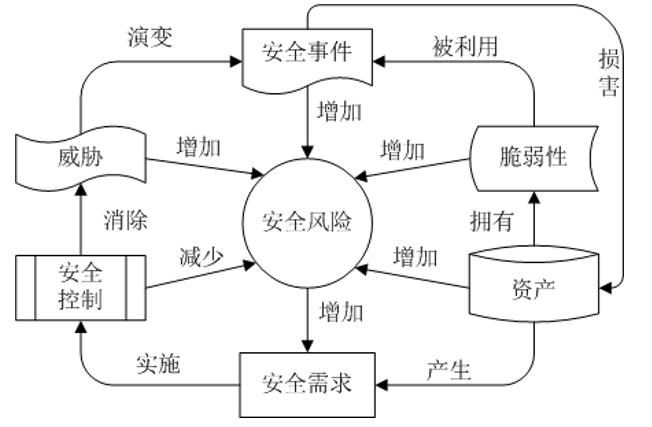
信息安全管理的内涵：体现预防控制为主的思想，强调遵守国家有关信息安全的法律法规，强调全过程的动态调整，从而确保整个安全体系在有效管理控制下，不断改进完善以适应新的安全需求

**2. 各信息安全风险因素之间的关系是怎样的？**

信息安全风险因素主要包括：威胁、脆弱性、资产、安全控制

风险因素之间相互作用、相互影响。安全风险随各因素的变化呈现动态调整演变趋势。

其相互关系可用下图表示：



**3. 风险评估的主要任务有哪些？**

风险评估的主要任务包括：

①识别组织面临的各种风险，了解总体的安全状况

②分析计算风险概率，预估可能带来的负面影响

③评价组织承受风险的能力，确定各项安全建设的优先等级

④推荐风险控制策略，为安全需求提供依据

**4. 实施风险控制主要包括那些步骤？**

实施风险控制主要包括以下步骤：

①对实施控制措施的优先级进行排序，分配资源时，对标有不可接受的高等级的风险项应该给予较高的优先级

②评估所建议的安全选项，风险评估结论中建议的控制措施对于具体的单位及其信息系统可能不是最适合或最可行的，因此要对所建议的控制措施的可行性和有效性进行分析，选择出最适当的控制措施

③进行成本效益分析，为决策管理层提供风险控制措施的成本效益分析报告

④在成本效益分析的基础上，确定即将实施的成本有效性最好的安全措施

⑤遴选出那些拥有合适的专长和技能，可实现所选控制措施的人员（内部人员或外部合同商），并赋以相应责任

⑥制定控制措施的实现计划，计划内容主要包括风险评估报告给出的风险、风险级别以及所建议的安全措施，实施控制的优先级队列、预期安全控制列表、实现预期安全控制时所需的资源、负责人员清单、开始日期、完成日期以及维护要求等

⑦分析计算出残余风险，风险控制可以降低风险级别，但不会根除风险，因此安全措施实施后仍然存在的残余风险

**5. CC标准与BS 7799标准有什么区别？**

CC标准提倡安全工程的思想，通过信息安全产品的开发、评价、使用全过程的各个环节的综合考虑来确保产品的安全性。其主要内容包括安全需求的定义，需求定义的用法，安全可信度级别，安全产品的开发和产品安全性评价等几个方面。

BS7799是英国标准协会（British Standards Institute，BSI）针对信息安全管理而制定的一个标准，共分为两个部分。第一部分BS7799-1是《信息安全管理实施细则》，第二部分BS7799-2是《信息安全管理体系规范》。

CC标准侧重于对系统和产品的技术指标，旨在支持产品中IT安全特征的技术性评估。而BS7799则偏重于安全管理方面的要求。