电子科技大学

2009 年攻读硕士学位研究生入学试题

考试科目：825 密码学基础与网络安全

注：所有答案必须写在答题纸上，写在试卷和草稿纸上均无效。

一、单项选择题（每题 1 分，共 30 题， 30 分）

请在 A、B、C 和 D 四个选项中，选择一个最佳答案填写到答题纸上。

1. 按照古典密码算法和现代密码算法的分类原则，移位密码算法属于（ ）

A. 单表代换密码算法　　B. 置换密码算法

C. 多表代换密码算法　　D. 乘积密码算法

2. 下列关于素数的说法正确的是（ ）

A. 素数的个数是有限的

B. 素数的个数是无限的

C. 不是所有整数都可以分解为几个素数的乘积

D. 任何整数一定可以分解为几个素数的乘积，且其分解是不唯一

3. 通常而言，宏病毒（ ）

A. 感染可执行文件　　B. 既感染模板文件，又感染文本文件

C. 既感染可执行文件，又感染文本文件　　D. 感染文本文件

4. 整数 1000 的欧拉函数 $\varphi(1000)$ 等于（ ）

A. 398　　B. 399

C. 400　　D. 401

5. 根据欧拉定理，11^{803} 的最后两位数字是（ ）

A. 30　　B. 31

C. 40　　D. 41

6. 下列关于高级数据加密标准（AES）的说法正确的是（ ）

A. AES 是非对称加密算法　　B. AES 是序列密码算法

C. AES 是数据加密标准 DES 的变体　　D. AES 是对称加密算法的国际标准

7. 下列关于 RSA 加密算法的说法正确的是（ ）

A. RSA 是典型的对称分组加密算法

B. RSA 的理论基础是离散对数困难问题

C. RSA 的理论基础是大整数因子分解困难问题

D. RSA 的理论基础是椭圆曲线上的离散对数困难问题

8. 以下关于 TCP/IP 协议族的说法不正确的是（ ）

A. TCP/IP 协议在设计之初很少考虑安全问题

B. TCP/IP 协议族中的 TCP 协议在设计之初考虑到了安全问题
C. TCP 协议的三次握手机制不是为解决 TCP 协议的安全问题而提出的
D. TCP/IP 协议的部分安全问题在一定程度上可以通过对各协议进行增补和完善来解决

9. 以下关于序列密码的说法正确的是（　　）
A. 序列密码中的密钥流是非周期性的
B. 序列密码的安全强度在于序列密码算法所采用的运算法则
C. 序列密码中的密钥流是周期性的，且周期越大越好
D. 序列密码中的密钥流是周期性的，且周期越小越好

10. 下列关于数字签名的说法正确的是（　　）
A. 数字签名不一定包括发送方的某些独有特征
B. 数字签名中签名（signature）的产生、识别和验证应较容易
C. 数字签名不具有认证功能
D. 伪造数字签名在计算上说是可行的

11. 选择密文攻击是指（　　）
A. 攻击者拥有明文串　　B. 攻击者可选择密文串而获得相应的明文串
C. 攻击者可获得对解密机的暂时访问　　D. 攻击者可获得对加密机的暂时访问

12. 以下关于三重 DES（3DES）算法的说法正确的是（　　）
A. 3DES 算法使用不同的 DES 算法和相同的密钥对数据进行三次加密
B. 3DES 算法使用不同 DES 算法和不同的密钥对数据进行三次加密
C. 3DES 算法使用相同的 DES 算法和相同的密钥对数据进行三次加密
D. 3DES 算法使用相同的 DES 算法和多个密钥对数据进行三次加密

13. 投掷一个有 n 面的骰子，有 n 个结果，每个结果的概率均为 $1/n$，则该随机事件的熵为（　　）
A. $\log_2(n)$　　B. $-\log_2(n)$
C. $2\log_2(n)$　　D. $-2\log_2(n)$

14. 以下关于数字签名标准（DSS）的说法不正确的是（　　）
A. DSS 只提供数字签名功能　　B. DSS 不能用来加密
C. DSS 没有使用安全 Hash 函数　　D. DSS 不能用来进行密钥交换

15. 以下关于网络互连设备的说法不正确的是（　　）
A. 集线器（Hub）可以作为网络隔离设备　　B. 路由器可以作为网络隔离设备
C. 交换机可以作为网络隔离设备　　D. 防火墙可以作为网络隔离设备

16. 以下关于包过滤（也叫分组过滤）防火墙的说法不正确的是（　　）
A. 数据包中的源 IP 地址可以作为包过滤防火墙的过滤条件
B. 数据包中的目的 IP 地址可以作为包过滤防火墙的过滤条件
C. 数据包中的传输层协议类型字段可以作为包过滤防火墙的过滤条件
D. 应用层协议中的内容可以作为包过滤防火墙的过滤条件

17. 可以用作消息认证函数来产生消息认证符的是（　　）
A. 随机函数　　B. 哈希（Hash）函数
C. 压缩函数　　D. 认证函数

18. 以下关于 Diffie-Hellman 密钥协商协议（DH 协议）的说法正确的是（　　）
A. DH 协议是因特网密钥交换协议（IKE）使用的密钥交换协议
B. DH 协议不是因特网密钥交换协议（IKE）使用的密钥交换协议
C. DH 协议是一个安全的密钥交换协议
D. 因为 DH 协议不安全，所有没有多大作用

19. 以下关于 UDP 协议的说法不正确的是（　　）
A. UDP 是传输层的协议　　B. UDP 是面向连接的协议
C. UDP 是非面向连接的协议　　D. UDP 数据包中不包含源 IP 地址

20. 以下关于 TCP SYN 扫描的说法正确的是（　　）
A. TCP SYN 扫描必须遵循 TCP 协议的三次握手规定
B. TCP SYN 扫描没有遵循 TCP 协议的三次握手规定
C. TCP SYN 扫描中攻击者必须回应 ACK 数据包才能获得对方的信息
D. TCP SYN 扫描不会被入侵检测系统发现

21. 以下关于引用监视器（Reference Monitor）的说法正确的是（　　）
A. 引用监视器自身不一定正确和安全
B. 引用监视器是一种认证机制
C. 引用监视器是一种访问控制
D. 引用监视器必须能够识别系统中的程序，但是不能控制其他程序的运行

22. 以下关于 UNIX 文件系统安全机制的说法正确的是（　　）
A. UNIX 文件系统的安全机制包括用户、组、超级用户管理等机制
B. UNIX 文件系统缺乏硬件安全保护
C. UNIX 文件系统没有提供自主访问控制
D. UNIX 文件系统没有提供强制访问控制

23. 如果 UNIX 系统中用户掩码（umask）以八进制数表示为 022，则当用户创建一个文件时，该文件的初始权限（以八进制数表示）是（　　）
A. 754　　B. 755
C. 756　　D. 757

24. 以下关于 Windows NT 操作系统中安全标识 SID（security identification）的说法正确的是（　　）
A. SID 对于 Window NT 操作系统的安全性至关重要，但它不是最基本的安全对象
B. SID 不能用来识别用户或群组
C. SID 可以作为用户或群组拥有访问权限的标志
D. 当用户登录时系统会为该用户创建一个 SID

25. 以下关于 Windows 操作系统注册表的说法正确的是（　　）
A. 程序和系统的配置参数一般都存放在注册表中
B. 程序的配置参数一般都存放在注册表中，而系统的配置参数一般不存放在注册表中
C. 系统的配置参数一般都存放在注册表中，而程序的配置参数一般不存放在注册表中
D. 程序和系统的配置和控制参数一般都不存放在注册表中

26. 一般来说，工作在网络层的网络设备是（　　）
A. 交换机　　B. 集线器
C. 路由器　　D. 应用网关

27. 以下关于跨站点脚本攻击（Cross-Site Scripting Attack）的说法不正确的是（　　）
A. 如果 Web 应用不支持用户输入，则跨站点脚本攻击无法实现
B. 如果用户输入不能用来生成动态内容，则跨站点脚本攻击无法实现
C. 如果用户输入不能用来生成静态内容，则跨站点脚本攻击无法实现
D. 如果 Web 应用对用户输入进行足够的有效性检验，则跨站点脚本攻击无法实现

28. 以下说法不正确的是（　　）
A.《中华人民共和国电子签名法》开始实施的时间不是 2008 年 4 月 1 日
B. 通用评估准则（CC）作为国际标准是 ISO 9000
C. 可信计算机系统评估准则（TCSEC）是由美国提出来到
D. 得到许多国家认可的信息安全管理标准是 BS7799

29. 以下关于链路加密的说法不正确的是（　　）
A. 链路加密是在通信链路两端加上加密设备对数据进行加密
B. 链路加密可以采用硬件实现
C. 链路加密中每个用户可以选择自己的加密密钥
D. 链路加密中所用用户使用相同的加密密钥

30. 关于病毒和蠕虫的说法正确的是（　　）
A. 病毒和蠕虫都需要依附于驻留文件且通过网络传播
B. 病毒需要依附于驻留文件来进行复制，而蠕虫不使用驻留文件也可在系统之间进行自我复制
C. 病毒和蠕虫都需要用驻留文件才能够进行自我复制
D. 病毒可以进行自我复制，而蠕虫不能进行自我复制

二、多项选择题（每题 2 分，共 10 题，　20 分）

每题有一个或多个正确答案。请将 A、B、C 和 D 四个选中所有正确答案的选项填写到答题纸上。（注意：多选、少选、错选均不得分）

1. 美国国家标准学会（ANSI）制订的 FIPS PUB 180 和 180-1 中关于 SHA-1 的说法不正确的有（　　）
A. SHA-1 是一个消息摘要算法标准
B. SHA-1 的输出是 160 位
C. SHA-1 的输出是可变的，其输出长度为 128 位～160 位
D. 一般而言，消息填充对于 SHA-1 算法不是必须的

2. 以下关于数据加密标准（DES）的说法正确的有（　　）
A. DES 是非对称加密算法　　B. DES 是对称加密算法
C. DES 是流密码算法　　D. DES 是分组加密算法

3. 以下关于密码分组连接模式（CBC）的说法正确的有（　　）
A. CBC 的输入是当前明文组与上一个密文组的异或
B. CBC 的第一块明文必须与一个初始向量（IV）异或后再进行加密
C. CBC 的错误传递仅有一块：出错密文块仅导致对应的明文块错误
D. CBC 模式不容易实现并行加密和解密

4. 以下属于 ITU-T X.800 规定的安全机制的有（　　）

A. 不可抵赖性（non-repudiation）　　B. 数字签名（digital signatures）
C. 公正（notarization）　　D. 业务流填充（traffic padding）

5. RFC 1321 中关于 MD5 的说法正确的有（　　）
A. MD5 的输入可以为任意长，但其输出是 128 位
B. MD5 对输入进行分组的长度是以 256 位为单位
C. MD5 对输入进行分组的长度是以 512 位为单位
D. MD5 算法不论输入多长，都必须进行消息填充

6. 以下哪些方法可提高口令（password）的安全性（　　）
A. 采用短语或单词　　B. 采用口令自检查技术
C. 采用计算机随机产生口令　　D. 采用口令预检查技术

7. 在以下安全服务中，IPSec 可以提供哪些安全服务（　　）
A. 数据完整性　　B. 数据机密性
C. 访问控制　　D. 数据源认证

8. 以下关于公钥基础设施（PKI）的说法正确的是（　　）
（A）PKI 可以解决公钥可信性问题　　（B）PKI 不能解决公钥可信性问题
（C）PKI 只能够由政府来建立　　（D）PKI 可以提供数字证书查询服务

9. 下列关于误用检测（Anomaly Detection）的说法正确的有（　　）
A. 误用检测根据掌握的关于入侵或攻击的知识来识别入侵行为
B. 误用检测根据对用户正常行为的了解和掌握来识别入侵行为
C. 一般而言，误用检测需要建立入侵的行为特征库
D. 一般而言，误用检测需要建立用户的正常行为特征库

10. 以下关于安全漏洞的说法正确的有（　　）
A. 安全漏洞可能在软件设计过程中产生
B. 安全漏洞可能在软件或系统的配置过程中产生
C. 软件是产生安全漏洞的唯一原因
D. 安全漏洞是系统的弱点，没有绝对安全的系统

三、计算选择题（每题 5 分，共 4 题， 20 分）

请在 A、B、C 和 D 四个选项中，选择一个正确答案填写到答题纸上。

1. 有一堆苹果，如果 7 个一组来数，则剩 5 个；如果 11 个一组来数，则剩 3 个；如果 13 个一组来数，则剩 10 个。请问该堆苹果有多少个？（　　）
A. 1000998　　B. 10911
C. 100994　　D. 895

2. 在标准 DES 算法中，已知 DES 算法的第 3 个 S 盒如下：

S_3	列 / 行	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
	0	10	0	9	14	6	3	15	5	1	13	12	7	11	4	2	8
	1	13	7	0	9	3	4	6	10	2	8	5	14	12	11	15	1
	2	13	6	4	9	8	15	3	0	11	1	2	12	5	10	14	7
	3	1	10	13	0	6	9	8	7	4	15	14	3	11	5	2	12

如果该 S 盒的输入为 100011，则其输出的四位二进制数为（　　）

A. 1000　　B. 1001

C. 1010　　D. 1011

3. 已知矩阵 $M=\begin{bmatrix}1 & 1 & 1\\ 1 & 2 & 3\\ 1 & 4 & 9\end{bmatrix}(\text{mod } 11)$，则 M 的逆矩阵 M^{-1} 是（　　）

A. $M^{-1}=\begin{bmatrix}3 & 3 & 6\\ 8 & 4 & 10\\ 1 & 4 & 6\end{bmatrix}(\text{mod } 11)$　　B. $M^{-1}=\begin{bmatrix}3 & 3 & 7\\ 8 & 4 & 10\\ 1 & 4 & 6\end{bmatrix}(\text{mod } 11)$

C. $M^{-1}=\begin{bmatrix}3 & 3 & 8\\ 8 & 4 & 10\\ 1 & 4 & 6\end{bmatrix}(\text{mod } 11)$　　D. $M^{-1}=\begin{bmatrix}3 & 3 & 9\\ 8 & 4 & 10\\ 1 & 4 & 6\end{bmatrix}(\text{mod } 11)$

4. 在 RSA 算法中，Alice 选择了素数 p=11，q=13，公钥 e=7，则 Alice 的私钥是（　　）

A. 101　　B. 102

C. 103　　D. 104

四、简答题（共 4 题，30 分）

1. （5 分）简述 SSL 记录协议（SSL Record Protocol）提供的安全服务及其操作过程。

2. （7 分）简述 ACK 泛洪攻击（ACK Flooding）和 SYN 泛洪攻击（SYN Flooding）的相同点和不同点。

3. （8 分）列举 8 种典型的安全防御产品或工具，并说明各自的作用（注：仅列举而未说明作用将不得分）。

4.（10 分）什么是 hash 函数？它有哪些特点？列举两种 hash 函数在网络安全中的典型应用。

五、（10 分）某计算机系统具有如图 1 所示的堆栈结构，BP 指针(Base Pointer)是基数指针寄存器，是栈内某一单元的地址。假设返回地址和 BP 指针都为 4 字节（Bytes），数据数组长度为 6 字节（Bytes）。当进入程序调用后向数据数组输入数据，请根据下述情况说明：

（1）输入数据数组的数据长度（以字节为单位）在什么范围内是安全且完整的？请简要说明理由。（3 分）

（2）输入数据数组的数据长度（以字节为单位）在什么范围内是完整的，且有一定安全漏洞，但不会直接形成溢出攻击模式？请简要说明理由。（3 分）

（3）输入数据数组的数据长度（以字节为单位）在什么范围内不仅不安全，而且可以直接形成溢出攻击？请简要说明理由。（4 分）

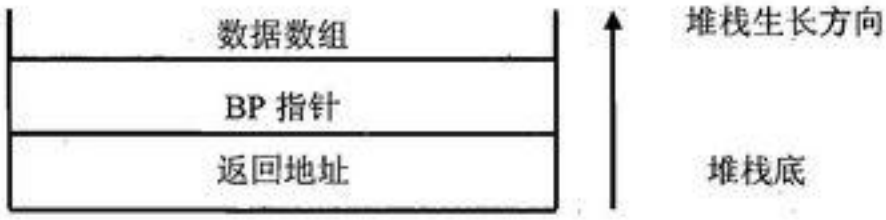

图 1 某系统的堆栈示意图

六、（10 分）Kerberos 协议是经典的安全协议。针对 Kerberos 协议回答以下问题：

（1）Kerberos 协议采用的是对称加密算法还是非对称加密算法？（1 分）

（2）Kerberos 协议是如何防御重放攻击的？（1 分）

（3）Kerberos 协议四个参与方的名字是什么？（2 分）

（4）简述 Kerberos 协议的基本原理和协议过程。（6 分）

七、（10 分）某企业计划部署防火墙系统，以便对 Internet 用户访问内部网络和内部用户访问 Internet 提供安全保护。该企业的安全主管可使用的资源包括外部路由器一台，内部路由器一台，堡垒主机一台，公共服务器一台，交换机若干。在设计防火墙系的方案时，本着节约成本的原则，要求所有资源必须使用且不允许合并使用。请你为该企业的安全主管设计一个防火墙系统，并回答以下问题：

（1）什么是堡垒主机？列举两个堡垒主机必须具备的特点。(2 分)

（2）请将各资源连接构成防火墙系统，画出该防火墙系统的逻辑结构图，并说明设计依据。（5 分）

（3）指出此防火墙系统属于防火墙体系结构中哪一种。（1 分）

（4）说明防火墙系统中各设备的主要作用。（2 分）

八、（8 分）如果 a,b 是两个整数，$b>0$，证明存在唯一的整数对 q,r，使得 $a=bq+r$，其中 $0\le r<b$。

九、（12 分）隶属于某国的军事办公室控制着某型号导弹的发射密码 m。该军事办公室由一个将军、两个上校和五个工作人员组成。为了提供必要的安全保障，导弹发射密码不能由某个人员单独保存，因而该军事办公室决定采取分割存放的方法。请针对以下两个不同的需求，分别设计一个该导弹发射密码 m 的分割存放方案（提示：可以考虑门限密码技术）：

（1）需求 1：军事办公室任意 6 个人员同意，就可以恢复出导弹发射密码 m 而启动导弹发射程序。（4 分）

（2）需求 2：只要将军和任意 1 个上校同意，或者将军和任意 3 个工作人员同意，或者 2 个上校和任意 2 个工作人员同意，或者任意 1 个上校和 5 个工作人员同意，都可以恢复出导弹发射密码 m 而启动导弹发射程序；除此之外，其他任何情况都不能恢复导弹发射密码 m。（8 分）