电子科技大学

2008 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

所有答案必须写在答题纸上，写在试卷或草稿纸上无效。

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. 按照加密和解密密钥是否相同，密码算法可分为（ ）

A. 分组密码算法和序列密码算法　　B. 对称密码算法和非对称密码算法

C. 基于密钥保密的算法和基于算法保密的算法　　D. 古典密码算法和现代密码算法

2. 下列关于安全服务与安全机制的关系正确的说法是（ ）

A. 安全服务由安全机制实现

B. 安全机制由安全服务实现

C. 一种安全机制只能够实现一种安全服务

D. 一种安全服务只能够实现一种安全机制

3. 反病毒软件具有副作用，当正常操作和病毒操作不能辨别时，可能会造成反病毒系统的（ ）

A. 误报　　B. 不报

C. 漏报　　D. 错报

4. 整数 29 的欧拉函数 $\varphi(29)$ 等于（ ）

A. 28　　B. 29

C. 27　　D. 26

5. 根据欧拉定理，7^{804} 的后三位数字是（ ）

A. 400　　B. 401

C. 402　　D. 403

6. 下列关于数据加密标准（DES）正确的说法是（ ）

A. DES 是非对称加密算法　　B. DES 是序列密码算法

C. DES 不是最新的国际加密标准　　D. DES 是最新的国际加密标准

7. 下列关于 RSA 加密算法正确的说法是（ ）

A. RSA 是非对称加密算法　　B. RSA 不是非对称加密算法

C. RSA 是流密码算法　　D. RSA 是对称加密算法

8. 以下关于公钥体制说法不正确的是（ ）

A. 在一个公钥体制中，一般存在公钥和私钥两个密钥

B. 公钥体制中仅根据密码算法和加密密钥来确定解密密钥在计算上是不可行的

C. 公钥体制中仅根据密码算法和加密密钥来确定解密密钥在计算上是可行的

D. 公钥体制中的私钥可以用来进行数字签名

9. 下列关于网络地址转换（NAT）正确的说法是（ ）

A. NAT 和防火墙能协同工作　　B. NAT 不能和防火墙协同工作

C. NAT 不能扩展 IP 地址空间　　D. NAT 不能用来解决 IP 地址紧张的问题

10. 下列关于数字签名说法正确的是（　　）

A. 数字签名是不可信的　　B. 数字签名容易被伪造

C. 数字签名容易抵赖　　D. 数字签名不可改变

11. 下列关于强制访问控制模型说法正确的是（　　）

A. 在该模型中，主体和客体均被赋予一定的安全级别，主体不能改变自身和客体的安全级别

B. 在该模型中，主体和客体均被赋予一定的安全级别，主体不能改变自身的安全级别，但是可以改变客体的安全级别

C. 在该模型中，主体和客体均被赋予一定的安全级别，主体能改变自身的安全级别，但是不能改变客体的安全级别

D. 在该模型中，主体和客体均被赋予一定的安全级别，主体既能改变自身的安全级别，也能改变客体的安全级别

12. 密码分析的目的是（　　）

A. 发现加密算法　　B. 发现解密算法

C. 发现密钥或者密文对应的明文　　D. 发现攻击者

13. 已知明文攻击是指（　　）

A. 攻击者拥有密文串　　B. 攻击者拥有明文串 x 和相应密文串 y

C. 攻击者可获得对加密机的暂时访问　　D. 攻击者可暂时接近解密机

14. 关于电子密码本（ECB）密码操作模式说法正确的是（　　）

A. 对每一个明文数据块采用不同的密钥进行加密

B. 对每一个明文数据块采用不同的密钥进行解密

C. 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. 错误传递有多块：出错密文块将导致多个明文块错误

15. 以下关于蜜罐（Honeypot）说法<u>不正确</u>的是（　　）

A. 蜜罐技术可以用来收集攻击信息　　B. 蜜罐技术可以用来收集计算机病毒代码

C. 蜜罐技术可以用来诱骗攻击者　　D. 蜜罐技术可以用来阻止网络攻击的发生

16. 在以下技术中，<u>不能</u>用作消息认证函数来产生消息认证符的是（　　）

A. 消息加密　　B. 消息认证码（MAC）

C. 压缩函数　　D. 哈希（Hash）函数

17. 以下关于 IPSec 说法正确的是（　　）

A. IPSec 属于网络层的安全解决方案　　B. IPSec 属于传输层的安全解决方案

C. IPSec 属于应用层的安全解决方案　　D. IPSec 属于物理层的安全解决方案

18. 以下关于 IPSec 中的密钥管理说法正确的是（　　）

A. 互联网络安全关联和密钥管理协议（IAKMP）是 IPSec 密钥管理的框架

B. 因特网密钥交换协议（IKE）是 IPSec 密钥管理的框架

C. Diffie-Hellman 密钥交协议是因特网密钥交换协议（IKE）使用的密钥交换协议

D. Oakley 不是因特网密钥交换协议（IKE）使用的密钥交换协议

19. 以下关于 SSL 说法正确的是（　　）

A. SSL 是物理层与网络层之间的安全解决方案，SSL 消息可用 TCP 或 UDP 传输

B. SSL 是传输层与应用层之间的安全解决方案，SSL 消息可用 TCP 或 UDP 传输

C. SSL 是传输层与应用层之间的安全解决方案，SSL 消息只能用 TCP 协议传输

D. SSL 中的握手协议（SSL Handshake protocol）用来安全传输应用层数据

20. 以下关于防火墙说法正确的是（　　）

A、所有防火墙都能检测网络攻击　　B. 所有的防火墙都能检测计算机病毒

C. 防火墙能防御内部攻击　　D. 防火墙能防御外部攻击

21. 以下关于入侵检测系统（IDS）的说法正确的是（　　）

A. 入侵检测系统可分为主机入侵检测系统和网络入侵检测系统

B. 入侵检测系统只能够检测已知攻击

C. 入侵检测系统不能够提供日志功能

D. 网络入侵检测系统（NIDS）不能够保护一个局域网

22. 以下关于计算机犯罪（Computer Crime）最准确的说法是（　　）

A. 攻击别人的计算机并进而获得信息的行为就是计算机犯罪

B. 通过网络攻击获得别人的机密信息一定是计算机犯罪

C. 盗窃计算机是计算机犯罪

D. 行为人通过计算机操作所实施的危害计算机信息系统（包括内存数据及程序）安全以及其他严重危害社会的并应当处以刑罚的行为

23. 2000 年颁布的《计算机病毒防治管理办法》中对计算机病毒的定义最准确的说法是（　　）

A. 计算机病毒是恶意代码的一种

B. 计算机病毒是导致系统功能变坏的恶意代码

C. 计算机病毒是指可以通过互联网传播的、会导致计算机信息系统遭受破坏的一组计算机指令或程序代码

D. 计算机病毒是指编制或者在计算机程序中插入的破坏计算机功能或者毁坏数据，影响计算机使用，并能自我复制的一组计算机指令或程序代码

24. 《中华人民共和国电子签名法》开始实施的时间是（　　）

A. 2005 年 3 月 1 日　　B. 2005 年 4 月 1 日

C. 2005 年 5 月 1 日　　D. 2005 年 6 月 1 日

25. 目前，得到许多国家认可的信息安全管理标准是（　　）

A. BS7799　　B. BS7498

C. ISO 9000　　D. CC

26. 可信计算机系统评估准则（TCSEC）是由哪个国家提出来的？（　　）

A. 中国　　B. 英国

C. 美国　　D. 德国

27. 通用评估准则（CC）作为国际标准是（　　）

A. ISO 9000　　B. ISO 15408

C. ISO 15409　　D. ISO 15407

28. NP 问题的含义是（　　）

A. 非确定性图灵机上不能够在多项式时间内得到处理的问题

B. 非确定性图灵机上能够在多项式时间内得到处理的问题

C. 确定性图灵机上不能够在多项式时间内得到处理的问题

D. 确定性图灵机上能够在多项式时间内得到处理的问题

29. 一般来说，工作在应用层的网络设备是（　　）

A. 交换机　　B. 集线器

C. 路由器　　D. 应用网关

30. 下面关于 TCP 协议的说法中，不正确的是（　　）

A. TCP 是传输层的协议　　B. TCP 协议是面向连接的协议

C. TCP 是非面向连接的协议　　D. TCP 数据包中不包含源 IP 地址

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. 下列关于高级数据加密标准（AES）的说法中正确的有（　　）

A. AES 是非对称加密算法　　B. AES 是对称加密算法

C. AES 是流密码算法　　D. AES 是分组加密算法

2. 下列哪些方法可以用来防止重放攻击？（　　）

A. 挑战一应答机制　　B. 时戳机制

C. 超时一重传机制　　D. 压缩机制

3. 以下关于身份认证的说法不正确的有（　　）

A. 身份认证是验证者获得对声称者所声称的事实的信任

B. 身份认证有单向和双向认证之分，且可以简单地重复两次单向认证来实现双向认证

C. 密码技术和非密码技术都可以用来实现身份认证

D. 只有密码技术才能够用来实现身份认证

4. 以下属于 ISO 7498-2 和 ITU-T X.800 规定的安全服务有（　　）

A. 认证（Authentication）　　B. 访问控制（Access Control）

C. 加密（Encryption）　　D. 数据机密性（Data Confidentiality）

5. RFC 1321 中以下关于 MD5 的说法正确的有（　　）

A. MD5 是一个消息摘要算法标准

B. MD5 的输入可以为任意长，但其输出是 128 位

C. MD5 的输入不能为任意长，但其输出是 128 位

D. MD5 算法不论输入多长，都必须进行消息填充

6. 美国国家标准学会(ANSI)制订的FIPS PUB 180 和 180-1 中关于SHA-1 说法正确的有(　　)

A. SHA-1 是一个消息摘要算法标准

B. SHA-1 的输入可以为任意长，但其输出是 160 位

C. SHA-1 的输入不能为任意长，但其输出是 160 位

D. SHA-1 算法不论输入多长，都必须进行消息填充

7. 以下关于安全协议（Secure Protocol）说法正确的有（　　）

A. 安全协议是在消息处理中使用了若干密码算法的协议

B. 安全协议的参与者至少有两个

C. 安全协议中的主体对于协议是了解的，并且预先知道所要完成的步骤

D. 密钥交换协议属于安全协议

8. 下列关于椭圆曲线加密算法（ECC）的说法中正确的有（　　）

A. ECC 属于密码算法　　B. ECC 属于非对称加密算法

C. ECC 不属于非对称加密算法　　D. ECC 算法的安全强度较 RSA 算法强

9. 以下属于动态安全模型（P^2DR）的内容有（　　）

A. 安全策略（Policy）　　B. 保护（Protection）
C. 检测（Detection）　　D. 恢复（Restore）

10. 在一个密钥管理系统中，可能的密钥类型有（　　）
A. 会话密钥　　B. 个人密钥
C. 密钥加密密钥　　D. 随机密钥

三、计算选择题（每题5分，共5题， 25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. 仿射密码算法的加密函数为 $f(x)=3x+13 \pmod{29}$，则其解密函数 $f^{-1}(x)$ 是（　　）
A. $f^{-1}(x)=(f(x)-13)/3 \pmod{29}$　　B. $f^{-1}(x)=(f(x)/3-13) \pmod{29}$
C. $f^{-1}(x)=9(f(x)-13) \pmod{29}$　　D. $f^{-1}(x)=10(f(x)-13) \pmod{29}$

2. DES算法中，已知DES算法中的第1个S盒如下：

S_1	行\列	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
	0	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
	1	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
	2	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
	3	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13

如果该S盒的输入为101001，则其输出为（　　）
A. 0011　　B. 0100
C. 0110　　D. 0100

3. 已知整数3是整数7的一个本原根，则整数7的另外一个本原根是（　　）
A. 2　　B. 4
C. 5　　D. 6

4. 对于椭圆曲线密码算法（ECC算法），其椭圆曲线为 $y^2 \equiv x^3+x+1 \bmod 23$，该椭圆曲线上的点集合 E_{23}（1，1）如下表所示：

(0, 1)	(6, 4)	(12, 19)
(0, 22)	(6, 19)	(13, 7)
(1, 7)	(7, 11)	(13, 16)
(1, 16)	(7, 12)	(17, 3)
(3, 10)	(9, 7)	(17, 20)
(3, 13)	(9, 16)	(18, 3)
(4, 0)	(11, 3)	(18, 20)
(5, 4)	(11, 20)	(19, 5)
(5, 19)	(12, 4)	(19, 18)

已知该椭圆曲线上两点P=（5，19），Q=（9，7），则P+Q=（　　）
A.（18，20）　　B.（19，18）
C.（18， 3）　　D.（19，5）

5. 有一个（3，5）Sharmir秘密门限拆分方案（即将某个秘密值 s 分成了5份影子，仅需知道其中任意3份影子即可恢复该秘密值）。已知该方案采用的模数 $p=13$，且其中秘密值 s 的三份影子分别为 $s(3)=7$，$s(4)=12$，$s(5)=5$。其中 $s(x)=y$ 表示当取值为 x 时，对应的影子值

为 y。则该秘密值 s 为（　　）

A. 9　　B. 10

C. 11　　D. 12

四、简答题（共 3 题，20 分）

1. （5 分）列举 5 种 IPSec 协议可以提供的安全服务，并说明这 5 种安全服务是由认证头协议（AH）还是封装安全载荷协议（ESP）来实现的。

2. （7 分）简述 TCP 协议三次握手过程，结合 TCP 协议的三次握手原理，简述 ACK 泛洪攻击（ACK Flood）的含义。

3. （8 分）请简述入侵检测系统（IDS）中误用检测（Misuse Detection）和异常检测技术（Anomaly Detection）的含义，并说明入侵检测系统的主要技术指标及其含义。

五、（10 分）认证协议是安全协议的一种。国际标准化组织（ISO）所规定的三次传输双向认证协议是基于公钥技术的一个认证协议，该协议可实现两个用户之间的相互认证，其消息传输过程如下：

$(1)\mathrm{A} \rightarrow B: N_a$

$(2)B \rightarrow A: CB, N_b, N_a, B, \{N_b, N_a, B\}_{k_b^{-1}}$

$(3)A \rightarrow B: CA, N_b, N_a, A, \{N_b, N_a, A\}_{k_a^{-1}}$

其中，A 和 B 是通信双方的身份标示，CA、CB 分别是 A 和 B 的证书；N_a、N_b 是两个新鲜随机数（Nonce）；$k^{-1}{}_a$、$k^{-1}{}_b$ 分别是 A 和 B 的私钥；$\{M\}_k$ 表示用密钥 k 对消息进行加密；逗号“,”表示消息的连接操作（如 M_1, M_2, M_3 表示将消息 M_1、M_2 和 M_3 连接成一个消息）；

“$(i)X \rightarrow Y: M$”表示 X 向 Y 发送消息 M，其中括号内的整数 i 表示消息的序号。

针对以上三次传输双向认证协议，回答以下问题：

（1）A 如何实现对 B 的认证？并说明理由。（3 分）

（2）B 如何实现对 A 的认证？并说明理由。（3 分）

（3）该协议是否存在安全漏洞？并说明理由。（4 分）

六、（10 分）以下是某个程序的源代码片断：

```
void  function(char *str)
{   char buffer[16];
    strcpy(buffer, str);
}
void main ()
{   char large_string[256];
    int i;
    for(i=0; i<256; i++)
        large_buffer[i]= 'A' ;
    function(large_string);
}
```

根据 main 函数和 function 函数的调用关系，并结合计算机程序设计和内存管理等相关技术，回答以下问题：

（1）从 main 函数和 function 函数的源程序及其调用关系来看，上述程序存在什么安全隐患？（2 分）

（2）产生该安全隐患的根源是什么？（3 分）

（3）通过修改 function 函数可以在一定程度上消除该安全因患，请给出正确的 function 函数的源代码。（5 分）

七、（10 分）DH 密钥协商协议（Diffie-Hellman Key Agreement Protocol，简称 DH 协议）是密码学中经典的安全协议。利用 DH 协议通信双方 A 和 B 可以协商一个共享密钥 k_{ab}。结合安全协议的基本原理，回答以下问题：

（1）请简述通信双方 A 和 B 利用 DH 协议如何协商共享密钥 k_{ab}。（5 分）

（2）说明 DH 协议存在的一种安全漏洞，并简述其攻击过程。（5 分）

八、（15 分）RSA 计算题

Alice 和 Bob 要采用 RSA 公钥密码算法进行通信。Alice 选择了两个素数：$p_a=17$，$q_a=11$，以及随机数 $e_a=7$ 作为公钥；Bob 选择两个随机素数：$p_b=11$，$q_b=13$，以及随机数 $e_b=7$ 作为公钥。请依据上述假设，请计算并回答以下问题：

（1）请说明 Alice 和 Bob 选择各自公钥（随机数 e_a 和 e_b）的基本原则和理由（提示：考虑如何计算私钥）（2 分）

（2）请依据 RSA 算法的相关知识，并结合 Alice 和 Bob 的上述选择，分别计算 Alice 的私钥 d_a 和 Bob 的私钥 d_b。（8 分）

（3）如果 Alice 和 Bob 采用以上参数（含第（2）问中计算出的私钥）的 RSA 算法作为加密和解密算法，假设 Alice 向 Bob 发送一个秘密消息，其明文 M 的值为 88（即 M=88）；传输过程中 Alice 只对明文 M 进行加密，而不进行其他额外操作。请计算 Alice 发送给 Bob 的密文 C 的值，以及 Bob 解密的过程和结果（须有计算过程，仅给出结果不记分）。（5 分）

九、（10 分）针对 RSA 算法的安全性问题，有人说可以通过求解 RSA 算法的模数 n 的欧拉函数以破解 RSA 算法。试证明对 RSA 算法的模数 $n=pq$（其中 p 和 q 是两个素数）进行因子分解和求解 n 的欧拉函数 $\varphi(n)$ 是等价的（即对于 $n=pq$，如果可以对 n 进行因子分解，就可以计算 $\varphi(n)$；同样，如果可以计算 $\varphi(n)$，也可以对 n 进行因子分解）。