电子科技大学

2015 年攻读硕士学位研究生入学考试试题

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，写在试卷或草稿纸上均无效。

一、单向选择题（每题 1 分，共 20 题， 20 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. 下列关于安全服务与安全机制的关系不正确的说法是（ ）

A. 安全服务由安全机制实现　　B. 安全机制与安全服务之间没有关系

C. 一种安全机制可以实现一种安全服务　D. 一种安全服务可以由一种安全机制来实现

2. 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. 对称密码算法和公钥密码算法

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

3. 整数 37 的欧拉函数$\varphi(37)$等于（ ）

A. 35　　B. 36　　C. 37　　D. 38

4. 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

5. 7^{804}的后三位数字是（ ）

A. 400　　B. 401　　C. 402　　D. 403

6. 以下关于美国国防部所提出的 PDRR 网络安全模型说法正确的是（ ）

A. 安全策略（Policy）是 PDRR 的重要内容

B. 依据 PDRR 模型，增加系统的保护时间可提高系统的安全性

C. 依据 PDRR 模型，增加系统的检测时间可提高系统的安全性

D. 依据 PDRR 模型，应该尽量增加系统暴露时间来提高系统的安全性

7. 以下说法不正确的是（ ）

A. 非对称加密算法较好地解决了密钥管理问题

B. TCP/IP 协议在设计之初并未考虑网络安全威胁

C. 网络隔离技术不能减少对信息系统的安全威胁

D. 安全协议需要使用某种密码算法且须实现一项或多项安全功能

8. 下列关于网络地址转换（NAT）正确的说法是（ ）

A. NAT 与防火墙能协同工作，但与 VPN 不能协同工作

B. NAT 与 VPN 能协同工作，但与防火墙不能协同工作

C. NAT 与防火墙能协同工作

D. NAT 与 VPN 不能协同工作

9. 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

10. 一般来说，以下哪个不属于设备物理安全的内容（ ）

A. 设备防盗　　B. 设备防毁

C. 设备电磁辐射抗扰　　D. 设备外观保护

11. 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

12. 以下关于蜜罐（Honeypot）说法不正确的是（　　）

A. 蜜罐技术可用来收集攻击信息　　B. 蜜罐技术可用来收集计算机病毒代码

C. 蜜罐技术可用来诱骗攻击者　　D. 蜜罐技术可用来阻止网络攻击的发生

13. 在以下技术中，不能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

14. 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

15. 以下关于防火墙说法正确的是（　　）

A、所有防火墙都能够检测网络攻击　　B. 所有防火墙都能够检测计算机病毒

C. 防火墙能防御内部攻击　　D. 防火墙能防御外部攻击

16. 以下关于入侵防护系统（IPS）的说法不正确的是（　　）

A. 入侵防护系统（IPS）可以检测网络攻击行为

B. 入侵防护系统（IPS）可以保护一个网络

C. 入侵防护系统（IPS）可以阻断检测出的攻击行为

D. 入侵防护系统（IPS）可以对计算机病毒进行检测

17. 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

18. 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

19. 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

20. 下面关于 TCP 协议的说法中，不正确的是（　　）

A. TCP 协议是传输层的协议　　B. TCP 协议是面向连接的协议

C. TCP 协议是非面向连接的协议　　D. TCP 协议数据包中不包含源 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. 下列哪些方法可以用来防止重放攻击？（ ）
   A. 挑战－应答机制　　B. 时戳机制
   C. 超时－重传机制　　D. 序列号机制
2. 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
3. 以下关于数据备份说法正确的有（ ）
   A. 按照备份后数据是否可以更改，数据备份可分为活备份和死备份
   B. 差分备份只备份上次全备份以来变化了的数据
   C. 差分备份只备份上次备份以来变化了的数据
   D. 增量备份只备份上次备份以来变化了的数据
4. 以下属于 ISO 7498-2 和 ITU-T X.800 规定的安全服务的有（ ）
   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. 以下哪些是提高计算机系统可靠性的方法（ ）
   A. 避错　　B. 容错
   C. 硬件冗余　　D. 软件冗余
8. 通常而言，以下哪些是域名解析系统（DNS）潜在的安全威胁（ ）
   A. DNS 劫持攻击　　B. DNS 缓存污染
   C. DNS 拒绝服务攻击　　D. DNS ID 欺骗
9. 以下关于跨站脚本攻击（XSS）说法正确的有（ ）
   A. 跨站脚本攻击包括持久性跨站攻击
   B. 跨站脚本攻击包括非持久性跨站攻击
   C. 跨站脚本攻击包括 DOM 跨站攻击
   D. 跨站脚本攻击包括拒绝服务跨站攻击
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. 主密钥

C. 密钥加密密钥　　D. 随机密钥

三、计算选择题（每题 5 分，共 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. 在 UNIX 系统中，如果用户掩码（umask）为 022，则当该用户创建一个文件时，该文件的初始权限是（　　）

A. 754　　B. 755

C. 756　　D. 757

2. 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. $-2\log_2(n)$

3. 假如 Alice 的 RSA 公钥为 n=323，e=5，Alice 不小心泄露了私钥 d=173。Alice 将 e 换成 7，下列哪一个整数可作为相应的私钥 d（　　）

A. 41　　B. 173

C. 247　　D. 117

4. Hill 加密算法 $C=\begin{pmatrix}1 & 2 & 3\\ 4 & 5 & 6\\ 11 & 9 & 8\end{pmatrix}M \bmod 26$ 的解密函数（C 表示密文，M 表示明文）是（　　）

A. $M=\begin{pmatrix}22 & 5 & 1\\ 6 & 19 & 21\\ 15 & 13 & 1\end{pmatrix}N \bmod 26$　　B. $M=\begin{pmatrix}22 & 5 & 1\\ 6 & 17 & 24\\ 15 & 13 & 1\end{pmatrix}N \bmod 26$

C. $M=\begin{pmatrix}22 & 7 & 8\\ 6 & 17 & 24\\ 15 & 13 & 1\end{pmatrix}N \bmod 26$　　D. $M=\begin{pmatrix}22 & 7 & 9\\ 6 & 17 & 24\\ 15 & 13 & 1\end{pmatrix}N \bmod 26$

四、简答题（共 3 题，20 分）

1. （5 分）请简述入侵检测系统（IDS）中误用检测技术（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。

2. （5 分）根据密码分析者可能取得的分析资料不同，可将密码分析（或攻击）分为哪几类？给出这几类攻击的定义。

3.（10 分）在某应用系统中，将安全等级划分为绝密（Top Secret）、机密（Secret）和公开（Unclassified）三个等级，其中绝密安全等级最高，公开安全等级最低。假设该应用系统中有两个主体（S_1 和 S_2）和三个客体（O_1，O_2 和 O_3），其中主体 S_1 的密级为绝密，S_2 的密级为机密，客体 O_1 的密级为绝密，O_2 的密级为机密，O_3 的密级为公开，请依据访问控制技术的

有关原理，回答以下问题：

（1）如果按照“不上读，不下写”的访问控制模型，S_1 可以对哪些客体进行读和写操作？这样的访问控制模型确保了什么安全属性？

（2）如果按照“不下读，不上写”的访问控制模型，S_2 可以对哪些客体进行读和写操作？这样的访问控制模型确保了什么安全属性？

五、认证协议综合分析题（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：

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

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

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

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 是两个新鲜性随机数（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）；“$(i)X \to Y: M$”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。

2、B 如何实现对 A 的认证？并说明理由。

3、该协议是否存在安全漏洞？并说明理由。

六、软件安全及协议安全综合分析题（20 分）

在 2014 公布的重大安全漏洞中，OpenSSL“心血”（HeartBleed）漏洞是其中危险性最大的漏洞之一。经过分析，发现“心血”漏洞的根源是 OpenSSL 在实现 SSL 协议时，其程序对协议中“心跳”的处理不当所造成的。以下是 OpenSSL 中实现“心跳”功能的部分核心源代码:

```
1.#ifndef OPENSSL_NO_HEARTBEATS
2.int dtls1_process_heartbeat(SSL *s)   //s 用来指向存放请求者发送的心跳数据的结构体
3.{
4.    unsigned char *p = &s->s3->rrec.data[0], *pl; //从收到的 SSL 心跳请求包提取数据
5.    unsigned short hbtype;
6.    unsigned int payload;
7.    unsigned int padding = 16;
8.    hbtype = *p++;            //读取数据部分头部的包类型
9.    n2s(p, payload);          //从指针 p 指向的数组中取出前两个字节数据长度，存入变量 payload
10.   pl = p;                   // pl 指向由访问者提供的心跳包数据
```

```
if (s->msg_callback)
      s->msg_callback(0, s->version, TLS1_RT_HEARTBEAT, &s->s3->rrec.data[0],
    s->s3->rrec.length,  s, s->msg_callback_arg);
 if (hbtype == TLS1_HB_REQUEST)        //如果是 SSL 心跳请求包
      {
         unsigned char *buffer, *bp;
         int r;
         /*分配空间，包括 message type、payload length、payload 和 padding*/
         buffer = OPENSSL_malloc(1 + 2 + payload + padding);    //分配由访问者指定大小的内存
         bp = buffer;      //bp 是用来访问刚分配的内存区域的指针
         *bp++ = TLS1_HB_RESPONSE; //赋值 response type
         s2n(payload, bp); //s2n 将与请求的心跳包载荷长度相同的长度值存入变量 payload
         memcpy(bp, pl, payload);           //从 pl 处开始复制 payload 个字节到 bp
         bp += payload;
         RAND_pseudo_bytes(bp, padding); //随机填充（Random padding）
         r = dtls1_write_bytes(s, TLS1_RT_HEARTBEAT, buffer, 3 + payload + padding);//发送数据
         if (r >= 0 && s->msg_callback)
            s->msg_callback(1, s->version, TLS1_RT_HEARTBEAT,  buffer, 3 + payload + padding,
            s, s->msg_callback_arg);
         OPENSSL_free(buffer);         //释放内存
         if (r < 0)
            return r;
      }
    else if (hbtype == TLS1_HB_RESPONSE)     //如果是 SSL 心跳响应包
      {
         unsigned int seq;
         n2s(pl, seq);
         if (payload == 18 && seq == s->tlsext_hb_seq)
         {
         dtls1_stop_timer(s);
         s->tlsext_hb_seq++;
         s->tlsext_hb_pending = 0;
         }
      }
    return 0;
    }
```

其中，SSL *s 定了一个指针，指向一个 ssl3_record_st 的结构体，其定义如下：

```
typedef struct ssl3_record_st
   {
      int type;               /* type of record */
      unsigned int length;    /* How many bytes available */
      unsigned int off;       /* read/write offset into 'buf' */
      unsigned char *data;    /* pointer to the record data */
      unsigned char *input;   /* where the decode bytes are */
      unsigned char *comp;    /* only used with decompression - malloc()ed */
      unsigned long epoch;    /* epoch number, needed by DTLS1 */
      unsigned char seq_num[8]; /* sequence number, needed by DTLS1 */
   } SSL3_RECORD;
```

针对心血漏洞及以上 OpenSSL 源代码，结合 SSL 协议，回答以下问题：

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

2、OpenSSL “心血”漏洞有什么危害？

3、在以上源代码中，是什么原因带来了“心血”漏洞隐患？

4、针对以上问题 3，如何解决“心血”漏洞？请给出一种解决方案的源代码。

七、安全协议综合分析题（10 分）

在 Kerberos 协议中，存在四类角色：用户（C）、认证服务器（AS）、票据许可服务器（TGS）和服务器（S），用户的目的是通过认证服务器 AS 和票据许可服务器 TGS，获得访问服务器 S 的权限。在 Kerberos 协议中，所有通信都保证了机密性。针对 Kerberos 协议，回答以下问题：

1、从密码算法角度来看，哪类加密算法适用于 Kerberos 协议？

2、在 Kerberos 协议中，用户（C）和票据准许服务器（TGS）之间没有共享密钥，它们之间是如何实现加密通信的？

3、在 Kerberos 协议中，用户（C）和服务器（S）之间没有共享密钥，它们之间是如何实现加密通信的？

八、计算题（20 分）

在某军舰上有 A、B、C 和 D 四人，3 人为合法军事人员，1 人为潜伏的特务。在这 4 人中，3 人拥有采用（2，4）Shamir 门限密码方案对某个秘密值 X 进行分割保存的数对，而特务由于不知道秘密值 X 只能随机拥有一个数对。数据对拥有情况是：A 持有（1，4），B 持有（3，7），C 持有（5，1），而 D 持有（7，2）（所有的数对都是模 11）。

请结合门限密码和秘密分割技术，回答以下问题：

1. A、B、C 和 D 四人中谁是潜伏的特务？为什么？

2. 三位合法军事人员分享的秘密值 X 是多少？

九、证明题（10 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 $0 \pounds r<b$ 。