[南开大学（本部）]《密码学》19秋期末考核 试卷总分:100得分:100

第1题,在下列密码算法中,不属于单表加密的算法是()。 A、凯撒密码 B、移位密码 C、仿射密码 D、希尔密码 正确答案:D

第2题,下面关于DES的描述,不正确的是()A、是由IBM、Sun等公司共同提出的 B、其结构完全遵循Feistel密码结构 C、其算法是完全公开的

1. 是目前应用最为广泛的一种分组密码算法 正确答案:A

**第3题,在以下古典密码体制中,属于置换密码的是( )。 A、移位密码 B、倒序密码 C、仿射密码**

1. **PlayFair密码 正确答案:B**

**第4题,CA的主要功能为()A、确认用户的身份**

1. **为用户提供证书的申请、下载、查询、注销和恢复等操作 C、定义了密码系统使用的方法和原则 D、负责发放和管理数字证书 正确答案:D**

第5题,在数据加密标准DES中,轮函数中有一个E扩展置换运算,该运算的输出是()比特位 A、8B、16C、32D、48

正确答案:D

第6题,在RSA公钥密码算法中,设p=11,q=23,n=pq=253,则有RSA密码体制RSA-253,选取加密密钥e=11,设明文为m=55,则密文c为()

A、11B、23C、220D、231正确答案:D

**第7题,SMS4加密算法中只用到了一个S-盒,其输出是()比特位。 A、4B、6C、8D、16**

**正确答案:C**

第8题,若有一个序列的周期为15,则至少需要()级的线性反馈移位寄存器才能产生该序列 A、3B、4C、5D、6

正确答案:B

**第9题,SMS4加密算法的迭代轮数是()A、8B、16C、32D、64**

**正确答案:C**

第10题,DES算法的入口参数有三个:Key,Data和Mode。其中Key为()位,是DES的工作密钥。 A、64B、56C、7D、8

正确答案:A

第11题,设p=127,q=131,n=pq=16637,则有Rabin密码体制Rabin-16637,设明文为m=4410,则密文c为()A、127B、131C、16084

D、16637正确答案:C

第12题,高级数字加密标准算法AES是在下面那个加密算法的基础上改进而来的 A、RC4

B、RijndaelC、LucifferD、IDEA正确答案:B

第13题,若有一个3级的线性反馈移位寄存器,则其产生的序列周期最大为()。 A、3B、5C、7D、8

正确答案:C

第14题,防止用户被冒名欺骗的方法是()。 A、对信息源发送方进行身份验证 B、进行数据加密

1. 对访问网络的流量进行过滤和保护 D、采用防火墙 正确答案:A

**第15题,以下有关软件加密和硬件加密不正确的是()**

1. **硬件加密对用户是透明的，而软件加密需在操作系统或软件中写入加密程序 B、硬件加密的兼容性比软件加密好 C、硬件加密的安全性比软件加密好 D、硬件加密的速度比软件加密快 正确答案:B**

**第16题,在下列的密码算法中,哪些属于分组密码算法( )A、Rijndael算法 B、RC4算法 C、Geffe算法 D、Lucifer算法 正确答案:A,D**

**第17题,下列哪些算法属于公钥密码算法()A、RSA算法 B、ElGamal算法 C、AES算法**

1. **椭圆曲线密码算法ECC正确答案:A,B,D**

第18题,在以下的攻击类型中属于被动攻击的是()A、数据监听

1. 数据篹改及破坏 C、身份假冒 D、数据流分析 正确答案:A,D

第19题,在解密过程,必须用到的三个主要元素是()A、所传输的信息（明文） B、解密密钥 C、解密函数

1. 需要解密的密文 正确答案:B,C,D

**第20题,以下对于混合加密方式说法正确的是()。**

**A、使用公开密钥密码体制对要传输的信息（明文）进行加解密处理 B、使用对称加密算法对要传输的信息（明文）进行加解密处理**

**C、使用公开密钥密码体制对对称加密密码体制的密钥进行加密后的通信 D、对称密钥交换的安全信道是通过公开密钥密码体制来保证的 正确答案:B,C,D**

**第21题,下列哪些方法可用以生成密码上安全的伪随机数( )A、DES的输出反馈（OFB）模式 B、ANSI X9.17的伪随机数产生器 C、Rabin产生器**

1. **离散指数比特产生器 正确答案:A,B,C,D**

第22题,在下列的密码算法中,哪些属于序列密码算法( )A、Rijndael算法 B、RC4算法 C、Geffe算法 D、Lucifer算法 正确答案:B,C

**第23题,在下面的密码攻击算法中,哪些方法属于唯密文攻击 A、穷举密钥攻击 B、字典攻击**

1. **字母频率统计攻击 D、重放攻击 正确答案:A,B,C**

第24题,人为的恶意攻击分为主动攻击和被动攻击,在以下的攻击类型中属于主动攻击的是()

A、数据监听

B、数据篹改及破坏 C、身份假冒 D、数据流分析 正确答案:B,C

**第25题,在密码系统中,许多地方都需要产生伪随机数,下列哪些方法可用以生成密码上安全的伪随机数( )**

**A、DES的输出反馈（OFB）模式 B、Pless序列生成器 C、线性同余算法**

**D、BBS（blum－blum－shub）产生器 正确答案:A,B,D**

第26题,流密码可以分为同步流密码和异步流密码,其中密钥流的产生并不是独立于明文流和密文流的流密码称为同步流密码。 T、对 F、错

正确答案:F

**【独立于明文的是同步流密码】**

第27题,现代分组密码都是乘法密码,分为Feistel密码和非Feistel密码两类,非Feistel密码只可以运用不可逆成分。 T、对 F、错

正确答案:F

第28题,DES算法中对明文的处理过程分3个阶段:首先是一个初始置换IP,用于重排明文分组的64比特数据。然后是具有相同功能的**64轮变换,**每轮中都有置换和代换运算。最后是一个逆初始置换从而产生64比特的密文。 T、对 F、错

正确答案:F

**【16轮变换】**

第29题,拒绝服务攻击属于被动攻击的一种。 T、对 F、错

正确答案:F

**【拒绝服务攻击是主动攻击】**

第30题,三密钥三重DES的有效密钥长度为128位。 T、对 F、错

正确答案:F

**【56\*3=168】**

第31题,设H是一个Hash函数,如果寻找两个不同的效益x和x1使得H(x)=H(x1)在计算上是不可行的,则称H是随机碰撞的。 T、对 F、错

正确答案:F

**【随即碰撞，需要两个特性】**

第32题,不可能存在理论上安全的密码体质 T、对 F、错

正确答案:F

**【一次一密】**

**第33题,密钥短语密码是一种单字母代换密码。 T、对 F、错**

**正确答案:T**

第34题,Feistel是密码设计的一个结构,而非一个具体的密码产品 T、对 F、错

正确答案:T

**第35题,暴力破解与字典攻击属于同类网络攻击方式,其中暴力破解中所采用的字典要比字典攻击中使用的字典范围要大。 T、对 F、错**

**正确答案:T**

第36题,已知加法密码的加密变换是：若取加密密钥为k=10，试求明文desk对应的密文？ 正确答案:

第37题,Rabin公钥加密算法。 正确答案:

第38题,代换密码。 正确答案:

第39题,IDEA加密算法。 正确答案:

第40题,一次一密加密算法。 正确答案: