1

单选题

1.用来破译古典密码的频度分析法主要利用自然语言中字母出现的频度不同的特性。请问英文字母中出现频度最高的是哪一个（ ）

A. A
B. C
C. I
D. E

正确答案： **D**

2.通常使用( )验证消息的完整性。

A. 消息摘要
B. 数字信封
C. 对称解密算法
D. 公钥解密算法

正确答案： **A**

3.AES算法中，当密钥长度是256位时，分组长度是128位，需要进行加密轮数为（ ）。

A. 6
B. 10
C. 12
D. 14

正确答案： **D**

4.用SM2算法实现一个对1024比特明文的加密，需要（ ）次点乘运算。

A. 1
B. 2
C. 4
D. 8

正确答案： **A**

5.下面哪个是分组密码（）。

A. 凯撒密码
B. AES
C. 轮转机
D. 隐写术

正确答案： **B**

6.一个安全的密码杂凑函数需要能够抵抗生日攻击等强抗碰撞性攻击。生日攻击即：在随机抽出的N个人中，N至少为（ ），就能保证至少两个人生日一样（排除2月29日的情况）的概率大于二分之一。（ ）

A. 20
B. 23
C. 150
D. 182

正确答案： **B**

7.Rabin密码体制的安全性是基于（ ）。

A. 大整数分解问题
B. 欧拉定理
C. 离散对数问题
D. 背包问题

正确答案： **A**

8.一个同步流密码具有很高的密码强度主要取决于（ ）。

A. 密钥流生成器的设计
B. 密钥长度
C. 明文长度
D. 密钥复杂度

正确答案： **A**

9.后量子公钥密码（PQC）是由NIST于（ ）正式启动 PQC 项目，面向全球征集PQC算法，推动标准化。

A. 2015年12月
B. 2016年12月
C. 2017年12月
D. 2018年12月

正确答案： **B**

10.国家密码管理局于（ ）年公布了SM2算法。

A. 1996
B. 2001
C. 2008
D. 2010

正确答案： **D**

11.基域选择Fp-256时，SM2算法的数字签名的私钥长度为（ ）。

A. 128
B. 256
C. 384
D. 512

正确答案： **B**

12.在IPSec VPN协议中，SM4分组密码算法的属性值是（ ）。

A. 128
B. 129
C. 64
D. 256

正确答案： **A**

13.Joe接收了由Grace签名的信息，请问Joe应该使用哪个密钥来验证签名？（ ）

A. Joe的公钥
B. Joe的私钥
C. Grace的公钥
D. Grace的私钥

正确答案： **C**

14.在SM3算法中，分组长度为（ ）位。

A. 56
B. 64
C. 488
D. 512

正确答案： **D**

15.在RSA公钥密码算法中，欧拉函数Φ(77)的值为（ ）。

A. 63
B. 60
C. 48
D. 49

正确答案： **B**

16.如果SM2的密文长度是2048比特，那么相应明文长度是（ ）比特。

A. 1024
B. 1280
C. 2048
D. 2816

正确答案： **B**

17.移位密码通常可用来加密普通的英文句子，假设其密钥为K=11，将明文“wewillmeet”加密后，密文为（ ）。

A. JQJTXXYQQG
B. HPHTWWXPPE
C. JEJUZZXEEQ
D. HQHTXXWQQF

正确答案： **B**

18.利用SM2公钥密码体制两次加密相同的明文，密文相同吗？ ()

A. 不同
B. 相同
C. 有时相同，也有不同
D. 根据具体情况

正确答案： **A**

19.SM3密码杂凑函数的迭代结构是（）。

A. Feistle迭代结构
B. SP结构
C. MD结构
D. Sponge结构

正确答案： **C**

20.SM2算法中的加密算法达到的安全性是（ ）。

A. OW-CPA
B. IND-CPA
C. IND-CCA2
D. NM-CPA

正确答案： **C**

21.祖冲之（ZUC）序列密码主算法一次输出的密钥长度为多少？ ()

A. 32比特
B. 64比特
C. 128比特
D. 256比特

正确答案： **A**

22.SM4算法的密钥和明文长度分别是多少比特（ ）。

A. 128、256
B. 128、128
C. 256、128
D. 256、256

正确答案： **B**

23.SM3密码杂凑算法采用什么结构?

A. MD结构
B. Sponge结构
C. HAIFA结构
D. 宽管道结构

正确答案： **A**

24.SM3密码杂凑算法是中国国家密码管理局公布的中国商用密码杂凑算法标准。SM3密码杂凑算法是哪种类型的算法?

A. 分组密码算法
B. 公钥密码算法
C. 数字签名算法
D. 杂凑函数

正确答案： **D**

25.SM2算法中的密钥交换算法支持（ ）方密钥交换。

A. 2
B. 3
C. 4
D. 多

正确答案： **A**

26.SM3密码杂凑算法的链接变量长度为多少比特?

A. 128
B. 224
C. 256
D. 512

正确答案： **C**

27.在SM4算法中轮密钥的长度为（ ）位。

A. 32
B. 128
C. 256
D. 512

正确答案： **A**

28.SM3密码杂凑算法的压缩函数一共多少轮?

A. 32
B. 64
C. 80
D. 120

正确答案： **B**

29.SM4分组密码算法，该算法的分组长度为128比特，密钥长度为（ ）。

A. 64比特
B. 128比特
C. 192比特
D. 256比特

正确答案： **B**

30.我国商用密码算法SM2是一种椭圆曲线公钥密码算法，其推荐的密钥长度为多少?

A. 128bit
B. 256bit
C. 192bit
D. 512bit

正确答案： **B**

31.SM4加密算法是（ ）。

A. 分组密码体制
B. 序列密码体制
C. 置换密码体制
D. 替代密码体制

正确答案： **A**

32.SM2算法的安全性基于（）困难假设?

A. 双线性映射
B. 椭圆曲线离散对数
C. 多线性映射
D. 丢番图方程求解

正确答案： **B**

33.ZUC算法是一个面向字的序列密码，密钥长度和初始向量的长度分别为多少？ ()

A. 64比特
B. 128比特
C. 256比特
D. 1024比特

正确答案： **B**

34.SM3密码杂凑算法输入的最大消息长度不超过多少比特?

A. 2^32
B. 2^64
C. 2^128
D. 任意长度

正确答案： **B**

35.SM3密码杂凑算法的压缩函数一共有几种不同的布尔函数?

A. 2
B. 3
C. 4
D. 5

正确答案： **A**

36.在2012年，国家密码管理局发布了一系列国产密码算法作为密码行业标准，其中（ ）是分组密码。

A. 祖冲之算法
B. SM4算法
C. SM2算法
D. SM3算法

正确答案： **B**

37.GM/T 0006《密码应用标识规范》定义的标识中，不包括以下哪种分组密码工作模式？ （ ）

A. ECB
B. CBC
C. CFB
D. CTR

正确答案： **D**

38.GM/T 0035《射频识别系统密码应用技术要求》第5部分，密钥体制包括（ ）类。

A. 2
B. 3
C. 4
D. 5

正确答案： **A**

39.GM/T 0006《密码应用标识规范》中的标识符在跨平台传输时，应采用（ ）字节顺序进行传输。

A. 网络字节顺序(Big-endian)
B. 小端(Little-endian)
C. 网络字节序或小端
D. 其它顺序

正确答案： **A**

40.GM/T 0005《随机性检测规范》中，以下关于“显著性水平”，正确的说法是（ ）

A. 随机性检测中错误地判断某一个随机序列为非随机序列的概率
B. 随机性检测中判断某一个随机序列为非随机序列的概率
C. 随机性检测中判断某一个随机序列为随机序列的概率
D. 随机性检测中错误地判断某一个随机序列为随机序列的概率

正确答案： **A**

多选题

1.下列哪些算法既能实现加解密又能实现签名（ ）。

A. RSA
B. ElGamal
C. AES
D. DES

正确答案： **AB**

2.以下关于HASH函数的说法正确的是（ ）。

A. 输入x可以为任意长度；输出数据串长度固定
B. 给定任何x，容易算出h=H（x）；而给出一个HASH值h，很难找到一特定输入x，使h=H（x）
C. 给出一个消息x，找出另一个消息y使H（x）=H（y）是计算上不可行的
D. 可以找到两个消息x、y，使得H（x）=H（y）

正确答案： **ABC**

3.下列密码体制属于计算安全的是（ ）。

A. RSA
B. ECC
C. AES
D. 一次一密系统

正确答案： **ABC**

4.DES分组模式有( )?

A. ECB
B. CBC
C. CFB
D. OFB

正确答案： **ABCD**

5.标准AES加密算法的密钥长度可以是（ ）

A. 128
B. 192
C. 64
D. 256

正确答案： **ABD**

6.下列属于HASH函数的是（ ）。

A. MD5
B. SHA1
C. AES
D. DES

正确答案： **AB**

7.SM3密码杂凑算法的压缩长度可以为多少比特?

A. 2^32
B. 2^48
C. 2^64
D. 任意长度

正确答案： **AB**

8.SM3密码杂凑算法的压缩函数的结构和哪些算法相同?

A. MD5
B. RIPEMD
C. SHA-1
D. SHA-256

正确答案： **ACD**

9.SM2公钥加密算法的加密函数涉及到哪些运算?

A. 随机数生成
B. 杂凑值计算
C. 椭圆曲线点乘
D. 伪随机比特序列生成

正确答案： **ABCD**

10.SM3密码杂凑算法能实现的功能有?

A. 数字签名和验证
B. 消息认证码的生成与验证
C. 随机数的生成
D. 加解密数据

正确答案： **ABC**

11.ZUC算法密钥装载时LFSR中需要装入（ ）。

A. 种子密钥
B. 初始向量
C. 16个常数
D. 15个常数

正确答案： **ABC**

12.SM2公钥加密算法的密文包含哪些元素?

A. 椭圆曲线点乘
B. 杂凑值
C. 比特串
D. 基域元素

正确答案： **ABC**

13.ZUC算法结构的核心部分包括（ ）。

A. LFSR
B. 比特重组BR
C. 非线性函数F
D. Feistel网络

正确答案： **ABC**

14.ZUC算法中使用到的运算包括（ ）。

A. 模2^{31}-1的加法
B. 模2^{32}的加法
C. 右循环移位
D. 左循环移位

正确答案： **ABD**

15.SM2公钥加密算法可以抵抗哪些攻击?

A. 唯密文攻击
B. 选择明文攻击
C. 选择密文攻击
D. 密钥恢复攻击

正确答案： **ABCD**

16.在GM/T 0019《通用密码服务接口规范》中，哪些函数可用于信息机密性保护？（）

A. 计算会话密钥
B. 单块加密运算
C. 结束解密运算
D. 多组数据消息鉴别码运算

正确答案： **ABC**

17.GM/Z 4001《密码术语》中，密钥全生命周期包括（）等。

A. 密钥产生
B. 密钥存储
C. 密钥更新
D. 密钥分量

正确答案： **ABC**

18.GM/T 0023《IPSec VPN网关产品规范》中，设备自检包括( )等操作。

A. 关键部件的正确性检查
B. 密钥等敏感信息的完整性检查
C. 随机数生成部件的检查
D. CPU等物理部件的常规检查

正确答案： **ABCD**

19.GM/T 0021《动态口令密码应用技术规范》动态口令生成算法使用了（）的国密算法。

A. SM1
B. SM2
C. SM3
D. SM4

正确答案： **CD**

20.GM/Z 4001《密码术语》中，哪种算法属于公钥密码算法（）

A. SM9
B. SM2
C. SM3
D. SM4

正确答案： **AB**

判断题

1.LWE问题是格上的困难问题。 ()

- 正确
- 错误

答案: **正确**

2.Rabin密码体制属于分组密码，是抗选择密文攻击的（ ）

- 正确
- 错误

答案: **错误**

3.专门用来提高软件实现效率的序列密码算法是RC4算法。 （ ）

- 正确
- 错误

答案: **错误**

4.著名的Kerberos认证系统采用了对称和非对称加密相结合的技术（ ）。

- 正确
- 错误

答案: **错误**

5.RSA公钥加密算法满足加法同态特性。

- 正确
- 错误

答案: **错误**

6.TLS1.0 版本协议中CBC模式的IV没有使用不可预测的随机数，而是使用了上一次 CBC 模式加密时的最后一个分组，从而导致被攻击。因此，为了防御此类攻击，TLS1.1以上的版本中要求必须隐式地传送IV。 （ ）

- 正确
- 错误

答案: **错误**

7.SM9公钥加密算法消息封装机制包括基于KDF的序列密码及结合KDF的分组密码算法两种类型。

- 正确
- 错误

答案: **正确**

8.SM9密码算法使用256位的BN曲线。

- 正确
- 错误

答案: **正确**

9.在采用SM9数字签名算法生成/验证签名之前，需要使用Hash函数对待签/待验证消息进行压缩。

- 正确
- 错误

答案: **正确**

10.生日攻击是一种密码学攻击手段，基于概率论中生日问题的数学原理。SM3密码杂凑算法可以抵抗生日攻击。

- 正确
- 错误

答案: **正确**

11.SM9密码算法需要保证选取的椭圆曲线上离散对数问题难解。

- 正确
- 错误

答案: **正确**

12.SM9公钥加密算法是密钥封装机制和消息封装机制的结合。

- 正确
- 错误

答案: **正确**

13.SM9密码算法的用户私钥由KGC通过随机数发生器产生。

- 正确
- 错误

答案: **错误**

14.SM3密码杂凑算法的消息填充方式和SHA-256相同。

- 正确
- 错误

答案: **正确**

15.SM9标识密码算法密钥交换过程中不需要计算群中的元素。（）

- 正确
- 错误

答案: **错误**

16.我国《密码法》所称密码，是指采用特定变换的方法对信息等进行加密保护、安全认证的技术、产品和服务。（）

- 正确
- 错误

答案: **正确**

17.GM/T 0015《基于SM2密码算法的数字证书格式规范》中，CA应确保使用大于20个8位字节的证书序列号。

- 正确
- 错误

答案: **错误**

18.GM/T 0023《IPSec VPN网关产品规范》中规定，IPSec VPN网关产品开机后应重新发起密钥协商。（）

- 正确
- 错误

答案: **正确**

19.GM/T 0005《随机性检测规范》中，“块内频数检测”用于检测整个待检序列中0和1的个数是否相近。

- 正确
- 错误

答案: **错误**

20.GM/T 0010《SM2密码算法加密签名消息语法规范》中的数字信封envelopedData数据类型由加密数据和至少一个接收者的数据加密密钥的密文组成。

- 正确
- 错误

答案: **正确**

2

单选题

1.DES算法属于对称加密体制，它的迭代次数是( )。

A. 16
B. 8
C. 24
D. 52

正确答案： **A**

2.以下不属于密码破解方法的是（ ）。

A. 字典攻击
B. 暴力攻击
C. 混合攻击
D. 拒绝服务攻击

正确答案： **D**

3.下列选项不是密码系统基本部分组成的是（ ）。

A. 明文空间
B. 密码算法
C. 初始化
D. 密钥

正确答案： **C**

4.序列密码是美国电报电话公司G. W. Vernam在（ ）年发明的。

A. 1917
B. 1918
C. 1919
D. 1920

正确答案： **A**

5.用SM2算法实现一个对1024比特明文的加密，需要（ ）次点乘运算。

A. 1
B. 2
C. 4
D. 8

正确答案： **A**

6.在SM3算法中，分组长度为（ ）位。

A. 56
B. 64
C. 488
D. 512

正确答案： **D**

7.下列不属于对称算法的是（ ）。

A. 祖冲之ZUC算法
B. SM2
C. SM7
D. SM4

正确答案： **B**

8.在AES算法中轮密钥的长度为（ ）位。

A. 64
B. 128
C. 256
D. 512

正确答案： **B**

9.在（k,n）门限秘密分享方案中，由少于（ ）个参与者所持有的部分信息则无法重构秘密。

A. k
B. n
C. k+1
D. k-1

正确答案： **A**

10.如果有6个成员组成的团体希望互相通信，那么在点到点的对称密钥分发结构中，需要人工分发密钥加密密钥（KEK）的数量为（）。

A. 18
B. 3
C. 15
D. 18

正确答案： **C**

11.在IPSec VPN协议中，SM4分组密码算法的属性值是（ ）。

A. 128
B. 129
C. 64
D. 256

正确答案： **A**

12.MD5是一种杂凑函数，用于将任意长度的消息映射为固定长度的输出。它通常用于检查文件完整性、数字签名、消息认证码等方面。MD5算法迭代运算包括（ ）轮处理过程。

A. 2
B. 3
C. 4
D. 5

正确答案： **C**

13.SHA接收任何长度的输入消息，并产生长度为（ ）位的杂凑值。

A. 64
B. 160
C. 512
D. 128

正确答案： **B**

14.在分布式密钥分配方案中，如果要求每个用户都能和其他用户安全的通信，那么有n个通信方的网络需要保存（）个主密钥。

A. n(n-1)/2
B. n(n-1)
C. n^2
D. n^2/2

正确答案： **A**

15.一个序列密码具有很高的安全强度主要取决于（）

A. 密钥流生成器的设计
B. 密钥长度
C. 明文长度
D. 加密算法

正确答案： **A**

16.在标准的DES的算法中，其分组的长度为（ ）位。

A. 56
B. 64
C. 112
D. 128

正确答案： **B**

17.HASH算法MD5的摘要长度为（）

A. 64位
B. 128位
C. 256位
D. 512位

正确答案： **B**

18.SM2算法中的加密算法达到的安全性是（ ）。

A. OW-CPA
B. IND-CPA
C. IND-CCA2
D. NM-CPA

正确答案： **C**

19.SM2算法是（）国家商用密码算法?

A. 美国
B. 我国
C. 欧盟
D. 俄罗斯

正确答案： **B**

20.SM3密码杂凑函数的迭代结构是（）。

A. Feistle迭代结构
B. SP结构
C. MD结构
D. Sponge结构

正确答案： **C**

21.ZUC算法是一个面向字的序列密码，初始向量的长度分别为多少？（）

A. 64比特
B. 128比特
C. 256比特
D. 1024比特

正确答案： **B**

22.SM4算法共有多少轮迭代？（ ）

A. 16
B. 32
C. 48
D. 64

正确答案： **B**

23.在SM4加密算法中明文分组长度为（ ）。

A. 64
B. 128
C. 256
D. 512

正确答案： **B**

24.SM2算法的安全性基于（）困难假设？

A. 双线性映射
B. 椭圆曲线离散对数
C. 多线性映射
D. 丢番图方程求解

正确答案： **B**

25.SM3密码杂凑算法的消息分组长度为多少比特？

A. 256
B. 512
C. 768
D. 1024

正确答案： **B**

26.SM4算法的密钥和明文长度分别是多少比特（ ）。

A. 128、256
B. 128、128
C. 256、128
D. 256、256

正确答案： **B**

27.SM2算法是（）密码算法?

A. 序列密码
B. 对称密码算法
C. 公钥密码
D. 密码杂凑函数

正确答案： **C**

28.我国商用分组密码算法SM4中使用的S盒的输入是多少位？（）

A. 4位
B. 6位
C. 8位
D. 16位

正确答案： **C**

29.SM3密码杂凑算法的压缩函数一共有几种不同的布尔函数?

A. 2
B. 3
C. 4
D. 5

正确答案： **A**

30.SM3密码杂凑算法是中国国家密码管理局公布的中国商用密码杂凑算法标准。SM3密码杂凑算法是哪种类型的算法?

A. 分组密码算法
B. 公钥密码算法
C. 数字签名算法
D. 杂凑函数

正确答案： **D**

31.SM4分组密码算法，该算法的分组长度为128比特，密钥长度为（）。

A. 64比特
B. 128比特
C. 192比特
D. 256比特

正确答案： **B**

32.在SM4算法中轮密钥的长度为（ ）位。

A. 32
B. 128
C. 256
D. 512

正确答案： **A**

33.SM2算法中的密钥交换算法支持（ ）方密钥交换。

A. 2
B. 3
C. 4
D. 多

正确答案： **A**

34.SM3密码杂凑算法的压缩函数一共多少轮?

A. 32
B. 64
C. 80
D. 120

正确答案： **B**

35.我国商用密码算法SM2是一种椭圆曲线公钥密码算法，其推荐的密钥长度为多少?

A. 128bit
B. 256bit
C. 192bit
D. 512bit

正确答案： **B**

36.GM/T 0035《射频识别系统密码应用技术要求》第5部分，密钥体制包括（ ）类。

A. 2
B. 3
C. 4
D. 5

正确答案： **A**

37.GM/T 0009《SM2密码算法使用规范》中，用户身份标识ID的默认值的长度为（）个字节。

A. 8
B. 16
C. 32
D. 64

正确答案： **B**

38.国家支持社会团体、企业利用自主创新技术制定（）国家标准、行业标准相关技术要求的商用密码团体标准、企业标准。

A. 低于
B. 等于
C. 高于
D. 相当于

正确答案： **C**

39.GM/T 0091《基于口令的密钥派生规范》定义的基于口令的密钥派生函数 PBKDF ,盐值为不小于 64 比特的随机比特串，迭代次数不小于（）次。

A. 256
B. 512
C. 1024
D. 2048

正确答案： **C**

40.GM/T 0009《SM2密码算法使用规范》中，Z值计算公式Z = SM3(ENTL‖ID‖a‖b‖xG‖yG‖xA‖yA)中ENTL的内容表示ID的比特长度，ENTL自身的长度为（ ）字节。

A. 1
B. 2
C. 4
D. 8

正确答案： **B**

多选题

1.下列关于Blowfish算法的说法，错误的是（ ）

A. Blowfish算法是一种流密码算法
B. Blowfish算法分组长度为64比特
C. Blowfish算法密钥固定为128比特
D. Blowfish算法的提出时间是1993年

正确答案： **AC**

2.序列密码算法有哪些？（ ）

A. ZUC
B. RC4
C. AES
D. DES

正确答案： **AB**

3.公钥密码体制使用不同的加密密钥和解密密钥。以下哪种密码算法是公钥密码体制？（ ）

A. SM2
B. SM4
C. Rabin
D. RSA

正确答案： **ACD**

4.以下哪种算法属于分组密码算法（ ）。

A. IDEA
B. RC4
C. Blowfish
D. RC5

正确答案： **ACD**

5.Camellia是分组密码，它的密钥长度可以为（）比特。

A. 64
B. 128
C. 192
D. 256

正确答案： **BCD**

6.下列密码体制不可以抗量子攻击的是（ ）。

A. RSA
B. Rabin
C. AES
D. NTRU

正确答案： **ABC**

7.SM2算法与（）算法属于同一类数学结构?

A. ECDH
B. RSA
C. ECDSA
D. SM9

正确答案： **ACD**

8.SM4分组密码算法轮函数中的T置换，包括哪些运算?

A. 非线性变换
B. 4个并行的S盒运算
C. 线性变换
D. 列混合变换

正确答案： **ABC**

9.SM3密码杂凑算法的应用有哪些?

A. 计算机安全登录系统
B. 数字签名
C. 数字证书
D. 电子政务

正确答案： **ABCD**

10.ZUC算法驱动部分产生的素域上序列的性质包括（ ）。

A. 权位序列平移等价
B. 序列集合模2压缩保熵
C. 所有权位序列周期相同
D. 所有权位序列线性复杂度相同

正确答案： **ABCD**

11.ZUC算法非线性函数F部分使用的两个线性变换L1，L2采用（ ）运算设计，降低了实现代价。

A. 右循环移位
B. 左循环移位
C. 比特串异或运算
D. 有限域乘法

正确答案： **BC**

12.SM2公钥加密算法的密文包含哪些元素?

A. 椭圆曲线点乘
B. 杂凑值
C. 比特串
D. 基域元素

正确答案： **ABC**

13.SM3密码杂凑算法的运算中哪些起到混淆的作用?

A. 循环移位
B. P置换
C. 模加
D. 布尔函数

正确答案： **CD**

14.SM4算法的轮函数包括什么运算？（ ）

A. 异或
B. 非线性变换
C. 线性变换
D. 相乘

正确答案： **ABC**

15.ZUC算法中使用到的运算包括（ ）。

A. 模2^{31}-1的加法
B. 模2^{32}的加法
C. 右循环移位
D. 左循环移位

正确答案： **ABD**

16.GM/T 0021《动态口令密码应用技术规范》动态口令生成算法使用了（ ）的国密算法。

A. SM1
B. SM2
C. SM3
D. SM4

正确答案： **CD**

17.GM/T 0021《动态口令密码应用技术规范》参与动态口令运算的因素包括（ ）。

A. 时间因子
B. 事件因子
C. 挑战因子
D. 种子密钥

正确答案： **ABCD**

18.在GM/T 0024标准中，选用以下哪些密钥交换算法时，是由客户端单独完成预主密钥产生的（ ）。

A. ECC
B. IBC
C. ECDHE
D. RSA

正确答案： **ABD**

19.GM/T 0021《动态口令密码应用技术规范》动态口令的生成使用到了（ ）过程。

A. 算法函数
B. 截位函数
C. 数据组装
D. 求余运算

正确答案： **ABCD**

20.GM/Z 4001《密码术语》中，密钥全生命周期包括（ ）等。

A. 密钥产生
B. 密钥存储
C. 密钥更新
D. 密钥分量

正确答案： **ABC**

判断题

1.自同步序列密码比同步序列密码更好地抗击基于明文冗余的攻击（ ）

- 正确
- 错误

答案: **正确**

2.AES 可以抵抗包括差分攻击、线性攻击等已知的各种攻击手段， 且在软硬件实现速度、内存要求方面都具有很好的性质。 ()

- 正确
- 错误

答案: **正确**

3.Rabin密码体制属于分组密码，是抗选择密文攻击的（ ）

- 正确
- 错误

答案: **错误**

4.DES算法可以用软件实现，也可以用硬件实现（ ）

- 正确
- 错误

答案: **正确**

5.专门用来提高软件实现效率的序列密码算法是RC4算法。 （ ）

- 正确
- 错误

答案: **错误**

6.最佳仿射逼近分析方法不属于唯密文攻击的攻击方法（　）。

- 正确
- 错误

答案: **正确**

7.SM3密码杂凑算法在2012年被批准成为行业标准算法。

- 正确
- 错误

答案: **正确**

8.SM3密码杂凑算法的压缩函数共有80轮操作。

- 正确
- 错误

答案: **错误**

9.SM3密码杂凑算法中没有使用循环移位运算。

- 正确
- 错误

答案: **错误**

10.SM9密钥封装机制封装的秘密密钥由解封装用户使用主私钥进行解密。

- 正确
- 错误

答案: **错误**

11.SM3密码杂凑算法的前16轮采用非线性的布尔函数。

- 正确
- 错误

答案: **错误**

12.根据目前公开的分析结果，SM3密码杂凑算法的安全性高于SHA-256。

- 正确
- 错误

答案: **正确**

13.SM3密码杂凑算法消息字的存储采用小端形式，左边为低有效位，右边为高有效位。

- 正确
- 错误

答案: **错误**

14.SM2与SM9都是基于椭圆曲线设计的。

- 正确
- 错误

答案: **正确**

15.SM9密码算法使用256位的BN曲线。

- 正确
- 错误

答案: **正确**

16.商用密码检测、认证机构应当对其在商用密码检测认证中所知悉的国家秘密和商业秘密承担保密义务。（ ）

- 正确
- 错误

答案: **正确**

17.机密信息是重要的国家秘密，泄露会使国家安全和利益遭受严重的损害。（ ）

- 正确
- 错误

答案: **正确**

18.国家鼓励和支持密码科学技术研究和应用，依法保护密码领域的知识产权，促进密码科学技术进步和创新。（ ）

- 正确
- 错误

答案: **正确**

19.根据GM/T 0029-2014《签名验签服务器技术规范》，签名验签服务器能够配置时间源服务器，自动同步时间。（ ）

- 正确
- 错误

答案: **正确**

20.GM/T 0005《随机性检测规范》中，“离散傅立叶检测”用于检测待检序列进行傅立叶变换后得到不正常的峰值个数是否超过了允许值。

- 正确
- 错误

答案: **正确**

3

单选题

1.如果有6个成员组成的团体希望互相通信，那么在点到点的对称密钥分发结构中，需要人工分发密钥加密密钥（KEK）的数量为（）。

A. 18
B. 3
C. 15
D. 18

正确答案： **C**

2.IDEA算法加密共需要（　　）个子密钥。

A. 16
B. 32
C. 48
D. 52

正确答案： **D**

3.RSA（　）用于数字签名。

A. 不应
B. 不能
C. 可以
D. 不可

正确答案： **C**

4.AES算法中，当密钥长度是256位时，分组长度是128位，需要进行加密轮数为（ ）。

A. 6
B. 10
C. 12
D. 14

正确答案： **D**

5.不属于公钥密码体制的是（ ）。

A. ECC
B. RSA
C. ElGamal
D. DES

正确答案： **D**

6.在IPSec VPN协议中，SM4分组密码算法的属性值是（ ）。

A. 128
B. 129
C. 64
D. 256

正确答案： **A**

7.在标准的DES的算法中，其分组的长度为（ ）位。

A. 56
B. 64
C. 112
D. 128

正确答案： **B**

8.用来破译古典密码的频度分析法主要利用自然语言中字母出现的频度不同的特性。请问英文字母中出现频度最高的是哪一个（ ）

A. A
B. C
C. I
D. E

正确答案： **D**

9.Rabin密码体制的安全性是基于（ ）。

A. 大整数分解问题
B. 欧拉定理
C. 离散对数问题
D. 背包问题

正确答案： **A**

10.在DES算法中子密钥的长度为（ ）位。

A. 48
B. 49
C. 64
D. 52

正确答案： **A**

11.在IDEA中，有( )个加密轮次。

A. 16
B. 12
C. 8
D. 10

正确答案： **C**

12.如果有6个成员组成的团体希望互相通信，那么在在基于密钥中心的对称密钥分发结构中，需要人工分发KEK的数量为（）。

A. 5
B. 6
C. 9
D. 15

正确答案： **B**

13.MD5和SHA-1的输出杂凑值长度分别是多少比特（ ）

A. 80，128
B. 128，160
C. 128，192
D. 160，192

正确答案： **B**

14.在AES算法中轮密钥的长度为（ ）位。

A. 64
B. 128
C. 256
D. 512

正确答案： **B**

15.移位密码通常可用来加密普通的英文句子，假设其密钥为K=11，将明文“wewillmeet”加密后，密文为（ ）。

A. JQJTXXYQQG
B. HPHTWWXPPE
C. JEJUZZXEEQ
D. HQHTXXWQQF

正确答案： **B**

16.HASH算法MD5的摘要长度为（）

A. 64位
B. 128位
C. 256位
D. 512位

正确答案： **B**

17.在SM3算法中，分组长度为（ ）位。

A. 56
B. 64
C. 488
D. 512

正确答案： **D**

18.SM2算法是（）国家商用密码算法?

A. 美国
B. 我国
C. 欧盟
D. 俄罗斯

正确答案： **B**

19.SM2算法的安全性基于（）困难假设?

A. 双线性映射
B. 椭圆曲线离散对数
C. 多线性映射
D. 丢番图方程求解

正确答案： **B**

20.SM2算法与（）基于相同数学结构设计?

A. SM4
B. SM9
C. SM1
D. SM3

正确答案： **B**

21.SM3密码杂凑算法的消息分组长度为多少比特?

A. 256
B. 512
C. 768
D. 1024

正确答案： **B**

22.SM3密码杂凑算法的压缩函数一共多少轮?

A. 32
B. 64
C. 80
D. 120

正确答案： **B**

23.SM2算法中的密钥交换算法支持（ ）方密钥交换。

A. 2
B. 3
C. 4
D. 多

正确答案： **A**

24.SM2算法是（）密码算法?

A. 序列密码
B. 对称密码算法
C. 公钥密码
D. 密码杂凑函数

正确答案： **C**

25.SM4分组密码算法，该算法的分组长度为128比特，密钥长度为（）。

A. 64比特
B. 128比特
C. 192比特
D. 256比特

正确答案： **B**

26.SM3密码杂凑算法的压缩函数的输入一共有多少比特?

A. 256
B. 512
C. 768
D. 1024

正确答案： **C**

27.我国商用分组密码算法SM4中使用的S盒的输入是多少位？（）

A. 4位
B. 6位
C. 8位
D. 16位

正确答案： **C**

28.ZUC算法是一个面向字的序列密码，密钥长度和初始向量的长度分别为多少？（）

A. 64比特
B. 128比特
C. 256比特
D. 1024比特

正确答案： **B**

29.在SM4加密算法中明文分组长度为（ ）。

A. 64
B. 128
C. 256
D. 512

正确答案： **B**

30.SM3密码杂凑函数的迭代结构是（）。

A. Feistle迭代结构
B. SP结构
C. MD结构
D. Sponge结构

正确答案： **C**

31.SM3密码杂凑算法采用什么结构?

A. MD结构
B. Sponge结构
C. HAIFA结构
D. 宽管道结构

正确答案： **A**

32.SM3密码杂凑算法的链接变量长度为多少比特?

A. 128
B. 224
C. 256
D. 512

正确答案： **C**

33.祖冲之（ZUC）序列密码主算法一次输出的密钥长度为多少？（）

A. 32比特
B. 64比特
C. 128比特
D. 256比特

正确答案： **A**

34.我国商用密码算法SM2是一种椭圆曲线公钥密码算法，其推荐的密钥长度为多少?

A. 128bit
B. 256bit
C. 192bit
D. 512bit

正确答案： **B**

35.SM4算法的密钥和明文长度分别是多少比特（ ）。

A. 128、256
B. 128、128
C. 256、128
D. 256、256

正确答案： **B**

36.GM/T 0009《SM2密码算法使用规范》中，Z值计算公式Z = SM3(ENTL‖ID‖a‖b‖xG‖yG‖xA‖yA)中ENTL的内容表示ID的比特长度，ENTL自身的长度为（ ）字节。

A. 1
B. 2
C. 4
D. 8

正确答案： **B**

37.GM/T 0006《密码应用标识规范》定义的标识中，不包括以下哪种分组密码算法？（ ）

A. SM1
B. SM4
C. AES
D. ZUC祖冲之算法

正确答案： **C**

38.GM/T 0035《射频识别系统密码应用技术要求》第5部分，哪个不属于密钥管理范围（ ）。

A. 生成
B. 分发
C. 注入
D. 混淆

正确答案： **D**

39.GM/Z 4001《密码术语》中，一种利用大量互相对应的明文和密文进行分析的密码攻击方法称为（ ）

A. 线性密码分析
B. 选择明文攻击
C. 选择密文攻击
D. 已知明文攻击

正确答案： **D**

40.GM/T 0006《密码应用标识规范》中的标识符在跨平台传输时，应采用（ ）字节顺序进行传输。

A. 网络字节顺序(Big-endian)
B. 小端(Little-endian)
C. 网络字节序或小端
D. 其它顺序

正确答案： **A**

多选题

1.下列哪些算法既能实现加解密又能实现签名（ ）。

A. RSA
B. ElGamal
C. AES
D. DES

正确答案： **AB**

2.以下哪种算法属于分组密码算法（ ）。

A. IDEA
B. RC4
C. Blowfish
D. RC5

正确答案： **ACD**

3.基于多变量的公钥密码系统的基本结构可分为哪两类（ ）。

A. “双极”型系统
B. “混合”型系统
C. “单极”型系统
D. “独立”型系统

正确答案： **AB**

4.下列密码体制不可以抗量子攻击的是（ ）。

A. DES
B. RSA
C. AES
D. NTRU

正确答案： **ABC**

5.下面属于PKI组成部分的是（ ）。

A. 数字证书库
B. 安全应用接口
C. CA数字证书签发系统
D. 密钥备份及恢复系统

正确答案： **ABCD**

6.试求出29(mod299)的所有平方根（ ）。

A. 35
B. 126
C. 173
D. 264

正确答案： **ABCD**

7.ZUC算法中使用到的运算包括（ ）。

A. 模2^{31}-1的加法
B. 模2^{32}的加法
C. 右循环移位
D. 左循环移位

正确答案： **ABD**

8.有关SM9标识密码算法描述错误的是

A. 用户的公钥由用户标识唯一确定，用户需要通过第三方保证其公钥的真实性。
B. SM9密钥交换协议可以使通信双方通过对方的标识和自身的私钥经2次或可选3次信息传递过程，计算获取一个由双方共同决定的共享秘密密钥。
C. SM9密码算法的密钥长度为512比特，算法的应用与管理不需要数字证书。
D. 在基于标识的加密算法中，解密用户持有一个标识和一个相应的私钥，该私钥由密钥生成中心通过主私钥和解密用户的标识结合产生。加密用户用解密用户的标识加密数据，解密用户用自身私钥解密数据。

正确答案： **AC**

9.ZUC算法非线性函数F部分使用的两个线性变换L1，L2采用（ ）运算设计，降低了实现代价。

A. 右循环移位
B. 左循环移位
C. 比特串异或运算
D. 有限域乘法

正确答案： **BC**

10.SM2公钥加密算法的加密函数涉及到哪些运算?

A. 随机数生成
B. 杂凑值计算
C. 椭圆曲线点乘
D. 伪随机比特序列生成

正确答案： **ABCD**

11.SM3密码杂凑算法的运算中哪些起到扩散的作用?

A. 循环移位
B. P置换
C. 模加
D. 布尔函数

正确答案： **AB**

12.ZUC算法非线性函数F部分两个线性变换L1和L2具有性质（ ）。

A. 均为置换
B. 差分分支数均为5
C. 线性分支数均为5
D. 实现代价较高

正确答案： **ABC**

13.ZUC算法密钥装载时LFSR中需要装入（ ）。

A. 种子密钥
B. 初始向量
C. 16个常数
D. 15个常数

正确答案： **ABC**

14.SM3密码杂凑算法的压缩长度可以为多少比特?

A. 2^32
B. 2^48
C. 2^64
D. 任意长度

正确答案： **AB**

15.下列我国商密算法中，被纳入国际标准化组织ISO/IEC的包括（ ）。

A. SM2数字签名算法
B. SM3密码杂凑算法
C. SM4分组密码算法
D. 祖冲之密码算法

正确答案： **ABCD**

16.GM/T 0021《动态口令密码应用技术规范》动态口令的生成使用到了（ ）过程。

A. 算法函数
B. 截位函数
C. 数据组装
D. 求余运算

正确答案： **ABCD**

17.GM/T 0021《动态口令密码应用技术规范》动态口令生成算法使用了（ ）的国密算法。

A. SM1
B. SM2
C. SM3
D. SM4

正确答案： **CD**

18.GM/T 0023《IPSec VPN网关产品规范》中，设备自检包括( )等操作。

A. 关键部件的正确性检查
B. 密钥等敏感信息的完整性检查
C. 随机数生成部件的检查
D. CPU等物理部件的常规检查

正确答案： **ABCD**

19.2004年8月28日，十届人大常委会第十一次会议审议通过了《中华人民共和国电子签名法》，确立了电子签名的法律效力。明确规定“可靠的电子签名与手写签名或者盖章具有同等的法律效力”，为我国信息化建设提供了重要的法律制度保障。下列说法正确的是（ ）。

A. 具有安全可靠性和经济实用性的电子签名实现技术的核心是密码技术
B. 在电子签名应用中，通常采用对称密钥的密码体制
C. 我国《电子签名法》明确规定，开展电子认证服务必须事先取得国家密码管理机构同意使用的证明文件
D. 网络环境中，电子签名认证证书作为"网上身份证"来确认相互的身份

正确答案： **ACD**

20.GB/T 15852《信息技术 安全技术 消息鉴别码》标准中定义的消息鉴别码可以基于（）机制实现。

A. 分组密码
B. 泛杂凑函数
C. 非对称密码
D. 专用杂凑函数

正确答案： **ABD**

判断题

1.Rabin算法是基于二次剩余的公钥密码体制。（ ）

- 正确
- 错误

答案: **正确**

2.NP问题是指用非确定性算法在多项式时间内解决的问题（ ）

- 正确
- 错误

答案: **正确**

3.自同步序列密码比同步序列密码更好地抗击基于明文冗余的攻击（ ）

- 正确
- 错误

答案: **正确**

4.RIJNDAEL算法不存在弱密钥和半若密钥，能有效抵抗目前已知的攻击（ ）。

- 正确
- 错误

答案: **正确**

5.周期置换密码是将明文串按固定长度分组，然后对每个分组中的子串按某个置换重新排列组合从而得到密文（）。

- 正确
- 错误

答案: **正确**

6.IPSec VPN相比于其它VPN更适合中小型企业（　）

- 正确
- 错误

答案: **正确**

7.SM3密码杂凑算法的压缩函数共有80轮操作。

- 正确
- 错误

答案: **错误**

8.SM3密码杂凑算法的前16轮采用非线性的布尔函数。

- 正确
- 错误

答案: **错误**

9.SM9密码算法的主公钥由KGC通过随机数发生器产生。

- 正确
- 错误

答案: **错误**

10.SM9密钥封装机制封装的秘密密钥由解封装用户使用主私钥进行解密。

- 正确
- 错误

答案: **错误**

11.SM3密码杂凑算法可以用来加解密数据。

- 正确
- 错误

答案: **错误**

12.SM3密码杂凑算法的轮函数每次更新2个字。

- 正确
- 错误

答案: **正确**

13.SM3密码杂凑算法的消息填充方式和SHA-256相同。

- 正确
- 错误

答案: **正确**

14.SM3密码杂凑算法消息字的存储采用小端形式，左边为低有效位，右边为高有效位。

- 正确
- 错误

答案: **错误**

15.SM2包含了数字签名、密钥交换、公钥加密三个算法。

- 正确
- 错误

答案: **正确**

16.GM/T 0010《SM2密码算法加密签名消息语法规范》中SignerInfo的digestEncryptionAlgorithm字段用于给出SM2-1数字签名算法标识符。

- 正确
- 错误

答案: **正确**

17.机密信息是重要的国家秘密，泄露会使国家安全和利益遭受严重的损害。（ ）

- 正确
- 错误

答案: **正确**

18.根据GM/T 0029-2014《签名验签服务器技术规范》，签名验签服务器能够配置时间源服务器，自动同步时间。（ ）

- 正确
- 错误

答案: **正确**

19.在我国，行政机关可在法律允许的范围内，利用行政手段强制转让商用密码技术。（ ）

- 正确
- 错误

答案: **错误**

20.GM/T 0010《SM2密码算法加密签名消息语法规范》中的数字信封envelopedData数据类型由加密数据和至少一个接收者的数据加密密钥的密文组成。

- 正确
- 错误

答案: **正确**

4

单选题

1.A5算法的主要组成部分是三个长度不同的线性移位寄存器，即A，B，C。其中A有（）位， B有（）位， C有（）位。 ()

A. 19,20,22
B. 19,22,23
C. 19,20,23
D. 19,20,19

正确答案： **B**

2.下列不属于对称算法的是（ ）。

A. 祖冲之ZUC算法
B. SM2
C. SM7
D. SM4

正确答案： **B**

3.Rabin密码体制的安全性是基于（ ）。

A. 大整数分解问题
B. 欧拉定理
C. 离散对数问题
D. 背包问题

正确答案： **A**

4.DES加密算法共经过( )次迭代运算的处理。

A. 8
B. 9
C. 16
D. 18

正确答案： **C**

5.以下各种加密算法属于古典加密算法的是（ ）。

A. DES算法
B. Caesar算法
C. IDEA算法
D. DSA算法

正确答案： **B**

6.在DES算法中子密钥的长度为（ ）位。

A. 48
B. 49
C. 64
D. 52

正确答案： **A**

7.基域选择Fp-256时，SM2算法的数字签名的私钥长度为（ ）。

A. 128
B. 256
C. 384
D. 512

正确答案： **B**

8.在普通数字签名中，签名者使用（ ）进行信息签名。

A. 签名者的公钥
B. 签名者的私钥
C. 签名者的公钥和私钥
D. 以上都不对

正确答案： **B**

9.SHA接收任何长度的输入消息，并产生长度为（ ）位的杂凑值。

A. 64
B. 160
C. 512
D. 128

正确答案： **B**

10.在一般的英文语言中，出现频率最高的字母为（ ）。

A. O
B. T
C. A
D. E

正确答案： **D**

11.DES算法属于加密技术中的（)

A. 对称加密
B. 不对称加密
C. 不可逆加密
D. 以上都是

正确答案： **A**

12.DES算法中进行S盒压缩时，对于输入110011，查找S6表，则列号是（ ）。

A. 3
B. 6
C. 9
D. 13

正确答案： **C**

13.IDEA算法加密共需要（ ）个子密钥。

A. 16
B. 32
C. 48
D. 52

正确答案： **D**

14.在（k,n）门限秘密分享方案中，由少于（ ）个参与者所持有的部分信息则无法重构秘密。

A. k
B. n
C. k+1
D. k-1

正确答案： **A**

15.国家密码管理局于（ ）年公布了SM2算法。

A. 1996
B. 2001
C. 2008
D. 2010

正确答案： **D**

16.用SM2算法实现一个对1024比特明文的加密，需要（ ）次点乘运算。

A. 1
B. 2
C. 4
D. 8

正确答案： **A**

17.基于椭圆曲线问题的公钥密码体制有（ ）。

A. Pohlig-Hellman
B. Pollard
C. ECDSA
D. DSS

正确答案： **C**

18.SM4加密算法是（ ）。

A. 分组密码体制
B. 序列密码体制
C. 置换密码体制
D. 替代密码体制

正确答案： **A**

19.祖冲之（ZUC）序列密码主算法一次输出的密钥长度为多少？ ()

A. 32比特
B. 64比特
C. 128比特
D. 256比特

正确答案： **A**

20.SM3密码杂凑算法的链接变量长度为多少比特?

A. 128
B. 224
C. 256
D. 512

正确答案： **C**

21.我国商用分组密码算法SM4中使用的S盒的输入是多少位？ ()

A. 4位
B. 6位
C. 8位
D. 16位

正确答案： **C**

22.SM2算法是（）国家商用密码算法?

A. 美国
B. 我国
C. 欧盟
D. 俄罗斯

正确答案： **B**

23.在SM4算法中轮密钥的长度为（ ）位。

A. 32
B. 128
C. 256
D. 512

正确答案： **A**

24.基域选择Fp-256时，SM2算法的数字签名的长度为（ ）比特。

A. 128
B. 256
C. 384
D. 512

正确答案： **D**

25.SM4分组密码算法，该算法的分组长度为128比特，密钥长度为（ ）。

A. 64比特
B. 128比特
C. 192比特
D. 256比特

正确答案： **B**

26.我国商用分组密码算法SM4中使用的S盒的输出是多少位? ()

A. 4位
B. 6位
C. 8位
D. 16位

正确答案： **C**

27.SM3密码杂凑算法采用什么结构?

A. MD结构
B. Sponge结构
C. HAIFA结构
D. 宽管道结构

正确答案： **A**

28.SM3密码杂凑算法的消息分组长度为多少比特?

A. 256
B. 512
C. 768
D. 1024

正确答案： **B**

29.利用SM2公钥密码体制两次加密相同的明文，密文相同吗？ ()

A. 不同
B. 相同
C. 有时相同，也有不同
D. 根据具体情况

正确答案： **A**

30.SM3密码杂凑算法的压缩函数一共有几种不同的布尔函数?

A. 2
B. 3
C. 4
D. 5

正确答案： **A**

31.SM3密码杂凑算法的压缩函数一共多少轮?

A. 32
B. 64
C. 80
D. 120

正确答案： **B**

32.我国商用密码算法SM2是一种椭圆曲线公钥密码算法，其推荐的密钥长度为多少?

A. 128bit
B. 256bit
C. 192bit
D. 512bit

正确答案： **B**

33.SM2算法是（）密码算法?

A. 序列密码
B. 对称密码算法
C. 公钥密码
D. 密码杂凑函数

正确答案： **C**

34.SM2算法中的密钥交换算法支持（ ）方密钥交换。

A. 2
B. 3
C. 4
D. 多

正确答案： **A**

35.SM3密码杂凑算法输入的最大消息长度不超过多少比特?

A. 2^32
B. 2^64
C. 2^128
D. 任意长度

正确答案： **B**

36.GM/T 0006《密码应用标识规范》定义的标识中，不包括以下哪种数据编码格式？（ ）

A. DER编码
B. Huffman编码
C. Base64编码
D. PEM编码

正确答案： **B**

37.GM/T 0006《密码应用标识规范》定义的标识中，不包括以下哪种分组密码算法？（ ）

A. SM1
B. SM4
C. AES
D. ZUC祖冲之算法

正确答案： **C**

38.GM/T 0009《SM2密码算法使用规范》中，Z值计算公式Z = SM3(ENTL‖ID‖a‖b‖xG‖yG‖xA‖yA)中ENTL的内容表示ID的比特长度，ENTL自身的长度为（ ）字节。

A. 1
B. 2
C. 4
D. 8

正确答案： **B**

39.GM/T 0035《射频识别系统密码应用技术要求》第4部分，双向鉴别前，读写器系统通过UID获得电子标签芯片的（ ）。

A. 根密钥
B. 分散密钥
C. 分散因子
D. 标签数据

正确答案： **B**

40.GM/T 0006《密码应用标识规范》定义的标识中，不包括以下哪种分组密码工作模式？（ ）

A. ECB
B. CBC
C. CFB
D. CTR

正确答案： **D**

多选题

1.以下属于多表代换古典密码体制的有（）。

A. Playfair体制
B. Vigenere体制
C. Beaufort体制
D. Hill体制

正确答案： **ABCD**

2.m序列每（ ）中 1 的个数比 0 的个数多 （ ） 个

A. 一周期
B. 二周期
C. 1
D. 4

正确答案： **AC**

3.以下属于现代密码体制的有（）。

A. DES密码体制
B. Vigenere体制
C. Beaufort体制
D. RSA密码体制

正确答案： **AD**

4.基于格理论密码是重要的后量子密码技术之一。下述属于格理论困难问题的是（ ）。

A. 最短向量问题(Shortest Vector Problem, SVP)
B. 最近向量问题(Closest Vector Problem,CVP)
C. 容错学习问题(Learning With Errors Problem, LWE)
D. 小整数解问题(Small Interger Solutions Problem,SIS)

正确答案： **ABCD**

5.但为了提高DES的安全性，并充分利用现有的软硬件资源，人们已设计开发了DES的多种变异版本，下面（）属于DES变异版本。

A. 2DES
B. 3DES
C. 4DES
D. 5DES

正确答案： **AB**

6.Camellia是分组密码，它的加解密轮数可以为（ ）。

A. 9
B. 18
C. 24
D. 48

正确答案： **BC**

7.ZUC算法密钥装载时LFSR中需要装入（ ）。

A. 种子密钥
B. 初始向量
C. 16个常数
D. 15个常数

正确答案： **ABC**

8.ZUC算法驱动部分产生的素域上序列的性质包括（ ）。

A. 权位序列平移等价
B. 序列集合模2压缩保熵
C. 所有权位序列周期相同
D. 所有权位序列线性复杂度相同

正确答案： **ABCD**

9.有关SM9标识密码算法描述错误的是

A. 用户的公钥由用户标识唯一确定，用户需要通过第三方保证其公钥的真实性。
B. SM9密钥交换协议可以使通信双方通过对方的标识和自身的私钥经2次或可选3次信息传递过程，计算获取一个由双方共同决定的共享秘密密钥。
C. SM9密码算法的密钥长度为512比特，算法的应用与管理不需要数字证书。
D. 在基于标识的加密算法中，解密用户持有一个标识和一个相应的私钥，该私钥由密钥生成中心通过主

私钥和解密用户的标识结合产生。加密用户用解密用户的标识加密数据，解密用户用自身私钥解密数据。

正确答案： **AC**

10.ZUC算法非线性函数F部分两个线性变换L1和L2具有性质（ ）。

A. 均为置换
B. 差分分支数均为5
C. 线性分支数均为5
D. 实现代价较高

正确答案： **ABC**

11.ZUC算法非线性函数F部分使用的两个线性变换L1，L2采用（ ）运算设计，降低了实现代价。

A. 右循环移位
B. 左循环移位
C. 比特串异或运算
D. 有限域乘法

正确答案： **BC**

12.SM2公钥密码算法一般包括如下哪些功能（ ）。

A. 密钥分散
B. 签名
C. 密钥交换
D. 加密

正确答案： **BCD**

13.SM2公钥加密算法可以抵抗哪些攻击?

A. 唯密文攻击
B. 选择明文攻击
C. 选择密文攻击
D. 密钥恢复攻击

正确答案： **ABCD**

14.SM3密码杂凑算法的压缩函数的结构和哪些算法相同?

A. MD5
B. RIPEMD
C. SHA-1
D. SHA-256

正确答案： **ACD**

15.SM3密码杂凑算法的运算中哪些起到扩散的作用?

A. 循环移位
B. P置换
C. 模加
D. 布尔函数

正确答案： **AB**

16.在GM/T 0003.1-2012《SM2椭圆曲线公钥密码算法》中，包含哪几个部分？（ ）

A. 公钥加密
B. 数字签名
C. 密钥交换
D. 身份认证

正确答案： **ABC**

17.GM/T 0010《SM2密码算法加密签名消息语法规范》中的属于结构类型的包括（ ）。

A. Data
B. SignedData
C. SignerInfos
D. Parameters

正确答案： **BCD**

18.在GM/T 0019《通用密码服务接口规范》中，哪些函数可用于信息机密性保护？（ ）

A. 计算会话密钥
B. 单块加密运算
C. 结束解密运算
D. 多组数据消息鉴别码运算

正确答案： **ABC**

19.GM/T 0034《基于SM2密码算法的证书认证系统密码及其相关安全技术规范》中，证书认证系统在逻辑上可分为（ ）。

A. 核心层
B. 管理层
C. 服务层
D. 公共层

正确答案： **ABC**

20.GM/T 0021《动态口令密码应用技术规范》动态口令系统中动态令牌负责（ ）动态口令。

A. 产生
B. 显示
C. 比对
D. 验证

正确答案： **AB**

判断题

1.最佳仿射逼近分析方法不属于唯密文攻击的攻击方法（ ）。

- 正确
- 错误

答案: **正确**

2.RC4密码算法是典型的序列密码算法。

- 正确
- 错误

答案: **正确**

3.PGP采用RSA进行密钥管理和数字签名，采用MD5作为单向散列函数（ ）

- 正确
- 错误

答案: **正确**

4.著名的Kerberos认证系统采用了对称和非对称加密相结合的技术（ ）。

- 正确
- 错误

答案: **错误**

5.Nonce是Number once的缩写，在加密技术中的初始向量和加密散列函数都发挥着重要作用，在各类验证协议的通信应用中确保验证信息不被重复使用以对抗重放攻击。Nonce就是一个伪随机数。

- 正确
- 错误

答案: **错误**

6.S-HTTP除了提供机密性以外，还提供了对公钥密码及数字签名的支持。（ ）

- 正确
- 错误

答案: **正确**

7.SM3密码杂凑算法一共有2个置换函数。

- 正确
- 错误

答案: **正确**

8.SM9标识密码算法密钥交换过程中不需要计算群中的元素。（ ）

- 正确
- 错误

答案: **错误**

9.SM9密码算法的消息认证码函数需要调用Hash函数。

- 正确
- 错误

答案: **正确**

10.SM3密码杂凑算法和SHA-256的结构相同。

- 正确
- 错误

答案: **正确**

11.SM3密码杂凑算法的消息分组长度是可变的。

- 正确
- 错误

答案: **错误**

12.SM3密码杂凑算法中没有使用循环移位运算。

- 正确
- 错误

答案: **错误**

13.在采用SM9数字签名算法生成/验证签名之前，需要使用Hash函数对待签/待验证消息进行压缩。

- 正确
- 错误

答案: **正确**

14.SM9公钥加密算法是密钥封装机制和消息封装机制的结合。

- 正确
- 错误

答案: **正确**

15.SM9是基于标识的密码算法。

- 正确
- 错误

答案: **正确**

16.商用密码用于保护属于国家秘密的信息。（ ）

- 正确
- 错误

答案: **错误**

17.GM/T 0021《动态口令密码应用技术规范》动态口令系统中密钥管理系统负责种子密钥的生成、传输，保证种子密钥的同步性。（ ）

- 正确
- 错误

答案: **正确**

18.国家鼓励和支持密码科学技术研究和应用，依法保护密码领域的知识产权，促进密码科学技术进步和创新。（ ）

- 正确
- 错误

答案: **正确**

19.国家支持社会团体、企业利用自主创新技术制定高于国家标准、行业标准相关技术要求的商用密码团体标准、企业标准。（ ）

- 正确
- 错误

答案: **正确**

20.GM/T 0034《基于SM2密码算法的证书认证系统密码及其相关安全技术规范》中规定，密钥恢复操作应由密钥管理中心业务操作员和司法取证人员同时在场。（ ）

- 正确
- 错误

答案: **错误**

5

单选题

1.Rabin密码体制的安全性是基于（ ）。

A. 大整数分解问题
B. 欧拉定理
C. 离散对数问题
D. 背包问题

正确答案： **A**

2.RSA（ ）用于数字签名。

A. 不应
B. 不能
C. 可以
D. 不可

正确答案： **C**

3.SHA接收任何长度的输入消息，并产生长度为（ ）位的杂凑值。

A. 64
B. 160
C. 512
D. 128

正确答案： **B**

4.在普通数字签名中，签名者使用（ ）进行信息签名。

A. 签名者的公钥
B. 签名者的私钥
C. 签名者的公钥和私钥
D. 以上都不对

正确答案： **B**

5.DES算法，密钥的长度（即有效位数）是( )位。

A. 44
B. 56
C. 64
D. 128

正确答案： **B**

6.下列的加密方案基于格理论的是（ ）。

A. ECC
B. RSA
C. AES
D. Regev

正确答案： **D**

7.在IPSec VPN协议中，SM4分组密码算法的属性值是（ ）。

A. 128
B. 129
C. 64
D. 256

正确答案： **A**

8.（ ）年，德国柏林大学教授普朗克首先提出了“量子论”

A. 1895
B. 1900
C. 1945
D. 1947

正确答案： **B**

9.以下各种加密算法属于古典加密算法的是（ ）。

A. DES算法
B. Caesar算法
C. IDEA算法
D. DSA算法

正确答案： **B**

10.移位密码通常可用来加密普通的英文句子，假设其密钥为K=11，将明文“wewillmeet”加密后，密文为（ ）。

A. JQJTXXYQQG
B. HPHTWWXPPE
C. JEJUZZXEEQ
D. HQHTXXWQQF

正确答案： **B**

11.一个同步流密码具有很高的密码强度主要取决于（ ）。

A. 密钥流生成器的设计
B. 密钥长度
C. 明文长度
D. 密钥复杂度

正确答案： **A**

12.Skipjack是一个密钥长度为（ ）位分组加密算法。

A. 56
B. 64
C. 80
D. 128

正确答案： **C**

13.如果SM2的密文长度是2048比特，那么相应明文长度是（ ）比特。

A. 1024
B. 1280
C. 2048
D. 2816

正确答案： **B**

14.下列选项不是密码系统基本部分组成的是（ ）。

A. 明文空间
B. 密码算法
C. 初始化
D. 密钥

正确答案： **C**

15.对输入为448比特的消息，SM3密码杂凑算法生成杂凑值时需要调用几次压缩函数?

A. 1
B. 2
C. 3
D. 4

正确答案： **B**

16.在分布式密钥分配方案中，如果要求每个用户都能和其他用户安全的通信，那么有n个通信方的网络需要保存（ ）个主密钥。

A. n(n-1)/2
B. n(n-1)
C. n^2
D. n^2/2

正确答案： **A**

17.基域选择Fp-256时，SM2算法的数字签名的私钥长度为（ ）。

A. 128
B. 256
C. 384
D. 512

正确答案： **B**

18.SM2算法中的（ ）算法已经进入ISO国际标准。

A. 数字签名
B. 公钥加密
C. 密钥交换
D. 身份认证

正确答案： **A**

19.SM3密码杂凑算法采用什么结构?

A. MD结构
B. Sponge结构
C. HAIFA结构
D. 宽管道结构

正确答案： **A**

20.SM3密码杂凑算法的消息分组长度为多少比特?

A. 256
B. 512
C. 768
D. 1024

正确答案： **B**

21.利用SM2公钥密码体制两次加密相同的明文，密文相同吗？ ()

A. 不同
B. 相同
C. 有时相同，也有不同
D. 根据具体情况

正确答案： **A**

22.SM3密码杂凑算法的压缩函数的输入一共有多少比特?

A. 256
B. 512
C. 768
D. 1024

正确答案： **C**

23.SM2算法与（）基于相同数学结构设计?

A. SM4
B. SM9
C. SM1
D. SM3

正确答案： **B**

24.SM3密码杂凑算法的压缩函数一共多少轮?

A. 32
B. 64
C. 80
D. 120

正确答案： **B**

25.我国商用分组密码算法SM4中使用的S盒的输入是多少位？（）

A. 4位
B. 6位
C. 8位
D. 16位

正确答案： **C**

26.基域选择Fp-256时，SM2算法的数字签名的长度为（）比特。

A. 128
B. 256
C. 384
D. 512

正确答案： **D**

27.SM4算法的密钥和明文长度分别是多少比特（）。

A. 128、256
B. 128、128
C. 256、128
D. 256、256

正确答案： **B**

28.SM3密码杂凑算法的压缩函数一共有几种不同的布尔函数?

A. 2
B. 3
C. 4
D. 5

正确答案： **A**

29.SM2算法是（）国家商用密码算法?

A. 美国
B. 我国
C. 欧盟
D. 俄罗斯

正确答案： **B**

30.在SM4算法中轮密钥的长度为（ ）位。

A. 32
B. 128
C. 256
D. 512

正确答案： **A**

31.我国商用分组密码算法SM4中使用的S盒的输出是多少位？（）

A. 4位
B. 6位
C. 8位
D. 16位

正确答案： **C**

32.SM3密码杂凑函数的迭代结构是（）。

A. Feistle迭代结构
B. SP结构
C. MD结构
D. Sponge结构

正确答案： **C**

33.SM3密码杂凑算法输入的最大消息长度不超过多少比特?

A. 2^32
B. 2^64
C. 2^128
D. 任意长度

正确答案： **B**

34.SM2算法的安全性基于（）困难假设?

A. 双线性映射
B. 椭圆曲线离散对数
C. 多线性映射
D. 丢番图方程求解

正确答案： **B**

35.祖冲之（ZUC）序列密码主算法一次输出的密钥长度为多少？ ()

A. 32比特
B. 64比特
C. 128比特
D. 256比特

正确答案： **A**

36.国家支持社会团体、企业利用自主创新技术制定（）国家标准、行业标准相关技术要求的商用密码团体标准、企业标准。

A. 低于
B. 等于
C. 高于
D. 相当于

正确答案： **C**

37.GM/T 0006《密码应用标识规范》中的标识符在跨平台传输时，应采用（ ）字节顺序进行传输。

A. 网络字节顺序(Big-endian)
B. 小端(Little-endian)
C. 网络字节序或小端
D. 其它顺序

正确答案： **A**

38.GM/T 0009《SM2密码算法使用规范》中，Z值计算公式Z = SM3(ENTL‖ID‖a‖b‖xG‖yG‖xA‖yA)中ENTL的内容表示ID的比特长度，ENTL自身的长度为（ ）字节。

A. 1
B. 2
C. 4
D. 8

正确答案： **B**

39.GM/T 0035《射频识别系统密码应用技术要求》第5部分，分散因子长度不小于（ ）。

A. 2字节
B. 4字节
C. 8字节
D. 16字节

正确答案： **B**

40.GM/T 0091《基于口令的密钥派生规范》定义的基于口令的密钥派生函数 PBKDF ,盐值为不小于 64 比特的随机比特串，迭代次数不小于（）次。

A. 256
B. 512
C. 1024
D. 2048

正确答案： **C**

多选题

1.下列属于HASH函数的是（ ）。

A. MD5
B. SHA1
C. AES
D. DES

正确答案： **AB**

2.下列是基于有限域上取幂运算的公钥密码体制的是（ ）。

A. Diffie-Hellman
B. RSA
C. AES
D. ElGamal

正确答案： **AD**

3.流加密算法有以下哪些( )。

A. A5
B. RC4
C. AES
D. DES

正确答案： **AB**

4.以下分组密码算法的工作模式IV要求每个消息必须唯一，不能重用，且不可预测的是（ ）。

A. OFB
B. CFB
C. CBC
D. GCM

正确答案： **BC**

5.DES分组模式有( )?

A. ECB
B. CBC
C. CFB
D. OFB

正确答案： **ABCD**

6.3GPP LTE算法标准的3个核心算法为（ ）。

A. ZUC
B. DES
C. AES
D. SNOW 3G

正确答案： **ACD**

7.我国SM2公钥密码算法包含哪3个算法（）？

A. 数字签名算法
B. 密钥封装算法
C. 密钥交换协议
D. 公钥加密解密算法

正确答案： **ACD**

8.关于ZUC算法初始化过程描述正确的是（ ）。

A. 迭代64轮
B. 初始化完成后直接输出密钥流
C. 迭代32轮
D. 非线性函数的输出会参与LFSR的反馈运算

正确答案： **CD**

9.SM3密码杂凑算法的运算中哪些起到混淆的作用?

A. 循环移位
B. P置换
C. 模加
D. 布尔函数

正确答案： **CD**

10.SM4分组密码算法轮函数中的T置换，包括哪些运算?

A. 非线性变换
B. 4个并行的S盒运算
C. 线性变换
D. 列混合变换

正确答案： **ABC**

11.ZUC算法结构的核心部分包括（）。

A. LFSR
B. 比特重组BR
C. 非线性函数F
D. Feistel网络

正确答案： **ABC**

12.SM2签名结果用ASN.1 DER表示时，如果签名值为71字节，可能的情形是（）。

A. 签名值中，r的最高位为1，s的最高位为0
B. 签名值中，r的最高位为0，s的最高位为1
C. 签名值中，r的最高位为0，s的最高位为0
D. 签名值中，r的最高位为1，s的最高位为1

正确答案： **AB**

13.SM2算法涉及到的数据格式包括?

A. 椭圆曲线点乘
B. 域元素
C. 比特串
D. 字符串

正确答案： **ABCD**

14.ZUC算法中使用到的运算包括（）。

A. 模2^{31}-1的加法
B. 模2^{32}的加法
C. 右循环移位
D. 左循环移位

正确答案： **ABD**

15.SM2的安全特性主要体现在哪些方面（）?

A. 算法具备单向性
B. 密文不可区分性
C. 密文具有抗碰撞性
D. 密文具有不可延展性

正确答案： **ABD**

16.GB/T 33560-2017《信息安全技术 密码应用标识规范》中，包括以下哪些密钥操作标识？（）

A. 密钥生成
B. 密钥分发
C. 密钥导入
D. 密钥销毁

正确答案：**ABCD**

17.GM/T 0010《SM2密码算法加密签名消息语法规范》中规范了使用SM2密码算法时相关的（）。

A. 加密和签名消息语法
B. 加密和签名操作结果的标准化封装
C. 对象标识符
D. 椭圆曲线参数语法

正确答案：**ABCD**

18.GM/Z 4001《密码术语》中，密钥全生命周期包括（）等。

A. 密钥产生
B. 密钥存储
C. 密钥更新
D. 密钥分量

正确答案：**ABC**

19.GM/Z 4001《密码术语》中，哪种算法属于公钥密码算法（）

A. SM9
B. SM2
C. SM3
D. SM4

正确答案：**AB**

20.GM/T 0021《动态口令密码应用技术规范》参与动态口令运算的因素包括（）。

A. 时间因子
B. 事件因子
C. 挑战因子
D. 种子密钥

正确答案：**ABCD**

判断题

1.著名的Kerberos认证系统采用了对称和非对称加密相结合的技术（）。

- 正确
- 错误

答案: **错误**

2.X.509是基于对称加密的认证协议，它提供跨网络的认证。（）

- 正确
- 错误

答案: **错误**

3.AES 可以抵抗包括差分攻击、线性攻击等已知的各种攻击手段， 且在软硬件实现速度、内存要求方面都具有很好的性质。()

- 正确
- 错误

答案: **正确**

4.RSA、ElGamal、Paillier公钥加密体制都满足加法同态特性。（）

- 正确
- 错误

答案: **错误**

5.Nonce是Number once的缩写，在加密技术中的初始向量和加密散列函数都发挥着重要作用，在各类验证协议的通信应用中确保验证信息不被重复使用以对抗重放攻击。Nonce就是一个伪随机数。

- 正确
- 错误

答案: **错误**

6.IPSec VPN相比于其它VPN更适合中小型企业（）

- 正确
- 错误

答案: **正确**

7.SM3密码杂凑算法的消息扩展过程一共生成128个消息字。

- 正确
- 错误

答案: **错误**

8.SM3密码杂凑算法的字长为16比特。

- 正确
- 错误

答案: **错误**

9.SM3密码杂凑算法和SHA-256的消息扩展方式相同。

- 正确
- 错误

答案: **错误**

10.SM9密码算法的用户私钥由KGC通过随机数发生器产生。

- 正确
- 错误

答案: **错误**

11.SM3密码杂凑算法的前16轮采用非线性的布尔函数。

- 正确
- 错误

答案: **错误**

12.SM3密码杂凑算法的轮函数每次更新2个字。

- 正确
- 错误

答案: **正确**

13.SM2与SM9都是基于椭圆曲线设计的。

- 正确
- 错误

答案: **正确**

14.SM3密码杂凑算法的压缩函数共有80轮操作。

- 正确
- 错误

答案: **错误**

15.SM9密码算法的消息认证码函数需要调用Hash函数。

- 正确
- 错误

答案: **正确**

16.GM/T 0009《SM2密码算法使用规范》中，SM2签名过程和SM2密钥协商过程中都使用了Z值。

- 正确
- 错误

答案: **正确**

17.GM/T 0023《IPSec VPN网关产品规范》中规定，IPSec VPN网关产品开机后应重新发起密钥协商。（）

- 正确
- 错误

答案: **正确**

18.我国《密码法》所称密码，是指采用特定变换的方法对信息等进行加密保护、安全认证的技术、产品和服务。（）

- 正确
- 错误

答案: **正确**

19.机密信息是重要的国家秘密，泄露会使国家安全和利益遭受严重的损害。（）

- 正确
- 错误

答案: **正确**

20.国务院商务主管部门、国家密码管理部门依法对涉及国家安全、社会公共利益且具有加密保护功能的商用密码实施进口许可，对涉及国家安全、社会公共利益或者中国承担国际义务的商用密码实施出口管制。（）

- 正确
- 错误

答案: **正确**

6

单选题

1.DES加密算法中共用（ ）个S盒。

A. 6
B. 7
C. 8
D. 9

正确答案： **C**

2.密码学中的HASH函数按照是否使用密钥分为两大类：带密钥的HASH函数和不带密钥的HASH函数。下面（）是带密钥的哈希函数。

A. MD4
B. SHA-1
C. Whirlpool
D. MD5

正确答案： **C**

3.下列哪种协议需要由双方或多方共同提供信息建立起共享会话密钥？（）

A. 密钥建立协议
B. 密钥传输协议
C. 密钥共享协议
D. 密钥协商协议

正确答案： **D**

4.在一般的英文语言中，出现频率最高的字母为（ ）。

A. O
B. T
C. A
D. E

正确答案： **D**

5.在IPSec VPN协议中，SM4分组密码算法的属性值是（ ）。

A. 128
B. 129
C. 64
D. 256

正确答案： **B**

6.国家密码管理局于（ ）年公布了SM2算法。

A. 1996
B. 2001
C. 2008
D. 2010

正确答案： **D**

7.MD5和SHA-1的输出杂凑值长度分别是多少比特（ ）

A. 80，128
B. 128，160
C. 128，192
D. 160，192

正确答案： **B**

8.在IDEA中，有( )个加密轮次。

A. 16
B. 12
C. 8
D. 10

正确答案： **C**

9.若Alice想向Bob分发一个会话密钥，采用ElGamal公钥加密算法，那么Alice应该选用的密钥是？（ ）

A. Alice的公钥
B. Alice的私钥
C. Bob的公钥
D. Bob的私钥

正确答案： **C**

10.基域选择Fp-256时，SM2公钥加密算法的私钥长度为（ ）。

A. 128
B. 256
C. 384
D. 512

正确答案： **B**

11.用SM2算法实现一个对1024比特明文的加密，需要（ ）次点乘运算。

A. 1
B. 2
C. 4
D. 8

正确答案： **A**

12.下列的加密方案基于格理论的是（ ）。

A. ECC
B. RSA
C. AES
D. Regev

正确答案： **D**

13.在SM3算法中，分组长度为（ ）位。

A. 56
B. 64
C. 488
D. 512

正确答案： **D**

14.美国已决定在（）以后将不再使用DES。

A. 1997年12月
B. 1998年12月
C. 1999年12月
D. 2000年12月

正确答案： **B**

15.DES算法属于对称加密体制，它的迭代次数是( )。

A. 16
B. 8
C. 24
D. 52

正确答案： **A**

16.AES的轮函数当中用来实现混淆的是（ ）

A. 轮密钥加
B. S盒
C. 列混合
D. 行移位

正确答案： **B**

17.一个同步流密码具有很高的密码强度主要取决于（ ）。

A. 密钥流生成器的设计
B. 密钥长度
C. 明文长度
D. 密钥复杂度

正确答案： **A**

18.SM3密码杂凑算法的压缩函数一共有几种不同的布尔函数?

A. 2
B. 3
C. 4
D. 5

正确答案： **A**

19.SM4算法的密钥和明文长度分别是多少比特（ ）。

A. 128、256
B. 128、128
C. 256、128
D. 256、256

正确答案： **B**

20.SM4算法共有多少轮迭代? （ ）

A. 16
B. 32
C. 48
D. 64

正确答案： **B**

21.基域选择Fp-256时，SM2算法的数字签名的长度为（ ）比特。

A. 128
B. 256
C. 384
D. 512

正确答案： **D**

22.SM3密码杂凑函数的迭代结构是（）。

A. Feistle迭代结构
B. SP结构
C. MD结构
D. Sponge结构

正确答案： **C**

23.ZUC算法是一个面向字的序列密码，密钥长度和初始向量的长度分别为多少？（）

A. 64比特
B. 128比特
C. 256比特
D. 1024比特

正确答案： **B**

24.SM3密码杂凑算法的消息分组长度为多少比特?

A. 256
B. 512
C. 768
D. 1024

正确答案： **B**

25.SM4分组密码算法，该算法的分组长度为128比特，密钥长度为（）。

A. 64比特
B. 128比特
C. 192比特
D. 256比特

正确答案： **B**

26.SM2算法的安全性基于（）困难假设?

A. 双线性映射
B. 椭圆曲线离散对数
C. 多线性映射
D. 丢番图方程求解

正确答案： **B**

27.在SM4加密算法中明文分组长度为（ ）。

A. 64
B. 128
C. 256
D. 512

正确答案： **B**

28.我国商用分组密码算法SM4中使用的S盒的输入是多少位？（）

A. 4位
B. 6位
C. 8位
D. 16位

正确答案： **C**

29.SM3密码杂凑算法输入的最大消息长度不超过多少比特?

A. 2^32
B. 2^64
C. 2^128
D. 任意长度

正确答案： **B**

30.SM4加密算法是（ ）。

A. 分组密码体制
B. 序列密码体制
C. 置换密码体制
D. 替代密码体制

正确答案： **A**

31.SM2算法是（）密码算法?

A. 序列密码
B. 对称密码算法
C. 公钥密码
D. 密码杂凑函数

正确答案： **C**

32.我国商用密码算法SM2是一种椭圆曲线公钥密码算法，其推荐的密钥长度为多少?

A. 128bit
B. 256bit
C. 192bit
D. 512bit

正确答案： **B**

33.在SM4算法中轮密钥的长度为（ ）位。

A. 32
B. 128
C. 256
D. 512

正确答案： **A**

34.我国商用分组密码算法SM4中使用的S盒的输出是多少位？（）

A. 4位
B. 6位
C. 8位
D. 16位

正确答案： **C**

35.利用SM2公钥密码体制两次加密相同的明文，密文相同吗？（）

A. 不同
B. 相同
C. 有时相同，也有不同
D. 根据具体情况

正确答案： **A**

36.GM/T 0035《射频识别系统密码应用技术要求》第5部分，哪个不属于密钥管理范围（ ）。

A. 生成
B. 分发
C. 注入
D. 混淆

正确答案： **D**

37.GM/Z 4001《密码术语》中，保证信息不被泄露给非授权的个人、进程等实体的性质称为密码的（ ）

A. 真实性
B. 完整性
C. 机密性
D. 不可否认性

正确答案： **C**

38.GM/T 0035《射频识别系统密码应用技术要求》第4部分，双向鉴别前，读写器系统通过UID获得电子标签芯片的（ ）。

A. 根密钥
B. 分散密钥
C. 分散因子
D. 标签数据

正确答案： **B**

39.GM/T 0015《基于SM2密码算法的数字证书格式规范》中，颁发者Issuer中AttributeValue部分首选的编码类型是（ ）。

A. PrintableString
B. TeletexString
C. BMPString
D. UTF8String

正确答案： **D**

40.GM/T 0015《基于SM2密码算法的数字证书格式规范》中，对于双证书，标准的证书扩展域的（ ）一定为关键项。

A. 密钥用法keyUsage
B. 主体密钥标识符subjectKeyIdentifier
C. 扩展密钥用途extKeyUsage
D. 认证机构authority

正确答案： **A**

多选题

1.混淆和扩散是密码设计的一般原则，所以在很多密码设计中，都采用了代换和置换等变化来达到混乱和扩散的效果。下列哪些密码体制中，采用了置换的处理思想（）。

A. RSA
B. 凯撒（CAESAR）密码
C. AES
D. DES

正确答案： **CD**

2.Camellia是分组密码，它的加解密轮数可以为（）。

A. 9
B. 18
C. 24
D. 48

正确答案： **BC**

3.下列不是A5算法初始密钥的长度是（ ）bit。

A. 16
B. 32
C. 64
D. 128

正确答案： **ABD**

4.序列密码算法有哪些？（ ）

A. ZUC
B. RC4
C. AES
D. DES

正确答案： **AB**

5.量子密码学是（ ）与（ ）的交叉学科。

A. 量子力学
B. 数学
C. 密码学
D. 天体物理学

正确答案： **AC**

6.以下哪种分组密码的工作模式类似于流密码（ ）。

A. CFB
B. CBC
C. CTR
D. OFB

正确答案： **CD**

7.SM3密码杂凑算法的运算中哪些起到混淆的作用？

A. 循环移位
B. P置换
C. 模加
D. 布尔函数

正确答案： **CD**

8.SM2公钥加密算法可以抵抗哪些攻击？

A. 唯密文攻击
B. 选择明文攻击
C. 选择密文攻击
D. 密钥恢复攻击

正确答案： **ABCD**

9.SM4算法的轮函数包括什么运算？（ ）

A. 异或
B. 非线性变换
C. 线性变换
D. 相乘

正确答案： **ABC**

10.有关SM9标识密码算法描述错误的是

A. 用户的公钥由用户标识唯一确定，用户需要通过第三方保证其公钥的真实性。
B. SM9密钥交换协议可以使通信双方通过对方的标识和自身的私钥经2次或可选3次信息传递过程，计算获取一个由双方共同决定的共享秘密密钥。
C. SM9密码算法的密钥长度为512比特，算法的应用与管理不需要数字证书。
D. 在基于标识的加密算法中，解密用户持有一个标识和一个相应的私钥，该私钥由密钥生成中心通过主私钥和解密用户的标识结合产生。加密用户用解密用户的标识加密数据，解密用户用自身私钥解密数据。

正确答案： **AC**

11.ZUC算法密钥装载时LFSR中需要装入（ ）。

A. 种子密钥
B. 初始向量
C. 16个常数
D. 15个常数

正确答案： **ABC**

12.ZUC算法结构的核心部分包括（ ）。

A. LFSR
B. 比特重组BR
C. 非线性函数F
D. Feistel网络

正确答案： **ABC**

13.ZUC算法中使用到的运算包括（ ）。

A. 模2^{31}-1的加法
B. 模2^{32}的加法
C. 右循环移位
D. 左循环移位

正确答案： **ABD**

14.关于ZUC算法初始化过程描述正确的是（ ）。

A. 迭代64轮
B. 初始化完成后直接输出密钥流
C. 迭代32轮
D. 非线性函数的输出会参与LFSR的反馈运算

正确答案： **CD**

15.A利用B的SM2公钥直接加密消息，将SM2密文传输给B，以下说法正确的是（ ）。

A. 这种方式可以实现消息源真实性鉴别
B. 这种方式不常用，SM2一般用于加密一个对称加密密钥
C. 这种方式可以对消息的机密性进行保护
D. 这种方式可以防范对消息的恶意替换

正确答案： **BC**

16.GB/T 17903 《信息技术 安全技术 抗抵赖》提供的抗抵赖机制可用于如下阶段的抗抵赖（ ）。

A. 证据生成
B. 证据传输、存储和检
C. 证据验证
D. 争议仲裁

正确答案： **ABC**

17.GM/T 0021《动态口令密码应用技术规范》参与动态口令运算的因素包括（ ）。

A. 时间因子
B. 事件因子
C. 挑战因子
D. 种子密钥

正确答案： **ABCD**

18.GM/T 0010《SM2密码算法加密签名消息语法规范》中规范了使用SM2密码算法时相关的（）。

A. 加密和签名消息语法
B. 加密和签名操作结果的标准化封装
C. 对象标识符
D. 椭圆曲线参数语法

正确答案： **ABCD**

19.GB/T 33560-2017《信息安全技术 密码应用标识规范》中，包括以下哪些公钥密码算法的标识？ （ ）

A. RSA
B. SM2
C. ECDSA
D. SM9

正确答案： **ABD**

20.GM/T 0005《随机性检测规范》中，关于检测原理以下说法正确的是（ ）

A. “Maurer通用统计检测”用于检测待检序列能否被无损压缩，如果待检序列能被显著地压缩，那么就认为该序列是不随机的。
B. “重叠子序列检测”通过比较m位可重叠子序列模式的频数和m+1位可重叠子序列模式的频数来检测其随机性。
C. “扑克检测”用于检测待检序列中m位非重叠子序列的每一种模式的个数是否接近。
D. “矩阵秩检测”用于检测待检序列中给定长度的子序列之间的线性独立性。

正确答案： **ACD**

判断题

1.Vigenere密码是古典密码算法

- 正确
- 错误

答案: **正确**

2.安全多方计算是分布式密码学的理论基础，也是分布式计算研究的一个基本问题。

- 正确
- 错误

答案: **正确**

3.最短向量问题是格上的困难问题（ ）

- 正确
- 错误

答案: **正确**

4.周期置换密码是将明文串按固定长度分组，然后对每个分组中的子串按某个置换重新排列组合从而得到密文（）。

- 正确
- 错误

答案: **正确**

5.Diffie-Hellman密钥交换协议不包括通信双方的身份认证过程，易受到中间人攻击。（ ）

- 正确
- 错误

答案: **正确**

6.著名的Kerberos认证系统采用了对称和非对称加密相结合的技术（）。

- 正确
- 错误

答案: **错误**

7.SM2与SM9都是基于椭圆曲线设计的。

- 正确
- 错误

答案: **正确**

8.SM9密码算法使用256位的BN曲线。

- 正确
- 错误

答案: **正确**

9.SM3密码杂凑算法的前16轮采用非线性的布尔函数。

- 正确
- 错误

答案: **错误**

10.SM3密码杂凑算法的压缩函数共有64轮操作。

- 正确
- 错误

答案: **正确**

11.SM3密码杂凑算法中的P置换是线性运算。

- 正确
- 错误

答案: **正确**

12.SM9密码算法的主公钥由KGC通过随机数发生器产生。

- 正确
- 错误

答案: **错误**

13.生日攻击是一种密码学攻击手段，基于概率论中生日问题的数学原理。SM3密码杂凑算法可以抵抗生日攻击。

- 正确
- 错误

答案: **正确**

14.SM3密码杂凑算法的布尔函数输出2个字。

- 正确
- 错误

答案: **错误**

15.SM3密码杂凑算法可以用来加解密数据。

- 正确
- 错误

答案: **错误**

16.GM/T 0023《IPSec VPN网关产品规范》中规定，IPSec VPN网关产品开机后应重新发起密钥协商。（ ）

- 正确
- 错误

答案: **正确**

17.GM/T 0006《密码应用标识规范》的用途是对密码算法或数据实体等标识进行统一，以便于密码协议、密码接口间的互联互通。

- 正确
- 错误

答案: **正确**

18.GM/T 0009《SM2密码算法使用规范》中，SM2签名过程和SM2密钥协商过程中都使用了Z值。

- 正确
- 错误

答案: **正确**

19.商用密码用于保护属于国家秘密的信息。（ ）

- 正确
- 错误

答案: **错误**

20.GM/T 0006《密码应用标识规范》定义了C和Java等语言实现密码算法时的密钥结构体等具体数据结构。

- 正确
- 错误

答案: **错误**

7

单选题

1.A5算法的主要组成部分是三个长度不同的线性移位寄存器，即A，B，C。其中A有（）位， B有（）位， C有（）位。 ()

A. 19,20,22
B. 19,22,23
C. 19,20,23
D. 19,20,19

正确答案： **B**

2.IDEA算法加密共需要（　　）个子密钥。

A. 16
B. 32
C. 48
D. 52

正确答案： **D**

3.DES加密算法中共用（ ）个S盒。

A. 6
B. 7
C. 8
D. 9

正确答案： **C**

4.在IPSec VPN协议中，SM4分组密码算法的属性值是（ ）。

A. 128
B. 129
C. 64
D. 256

正确答案： **B**

5.通常使用(　)验证消息的完整性。

A. 消息摘要
B. 数字信封
C. 对称解密算法
D. 公钥解密算法

正确答案：**A**

6.如果SM2的密文长度是2048比特，那么相应明文长度是（ ）比特。

A. 1024
B. 1280
C. 2048
D. 2816

正确答案：**B**

7.（ ）加密算法属于公钥密码算法。

A. AES
B. DES
C. IDEA
D. RSA

正确答案：**D**

8.DES加密算法共经过( )次迭代运算的处理。

A. 8
B. 9
C. 16
D. 18

正确答案：**C**

9.基域选择Fp-256时，SM2算法的数字签名的私钥长度为（ ）。

A. 128
B. 256
C. 384
D. 512

正确答案：**B**

10.IDEA的分组长度是（ ）bit。

A. 56
B. 64
C. 96
D. 128

正确答案：**B**

11.在（k,n）门限秘密分享方案中，由少于（　）个参与者所持有的部分信息则无法重构秘密。

A. k
B. n
C. k+1
D. k-1

正确答案：**A**

12.在标准的DES的算法中，其分组的长度为（ ）位。

A. 56
B. 64
C. 112
D. 128

正确答案：**B**

13.将文本写成对角线序列并一行一行地读取的技术称为（　）。

A. 栅栏加密技术
B. 简单分栏式变换技术
C. 单码加密
D. 同音替换加密

正确答案：**A**

14.在RSA公钥密码算法中，欧拉函数Φ(77)的值为（ ）。

A. 63
B. 60
C. 48
D. 49

正确答案：**B**

15.DES算法属于加密技术中的（)

A. 对称加密
B. 不对称加密
C. 不可逆加密
D. 以上都是

正确答案：**A**

16.密码学中的HASH函数按照是否使用密钥分为两大类：带密钥的HASH函数和不带密钥的HASH函数。下面（ ）是带密钥的哈希函数。

A. MD4
B. SHA-1
C. Whirlpool
D. MD5

正确答案： **C**

17.Skipjack是一个密钥长度为（ ）位分组加密算法。

A. 56
B. 64
C. 80
D. 128

正确答案： **C**

18.祖冲之（ZUC）序列密码主算法一次输出的密钥长度为多少？ ()

A. 32比特
B. 64比特
C. 128比特
D. 256比特

正确答案： **A**

19.我国商用密码算法SM2是一种椭圆曲线公钥密码算法，其推荐的密钥长度为多少?

A. 128bit
B. 256bit
C. 192bit
D. 512bit

正确答案： **B**

20.ZUC算法是一个面向字的序列密码，密钥长度和初始向量的长度分别为多少？ ()

A. 64比特
B. 128比特
C. 256比特
D. 1024比特

正确答案： **B**

21.SM2算法是（）密码算法?

A. 序列密码
B. 对称密码算法
C. 公钥密码
D. 密码杂凑函数

正确答案： **C**

22.SM4分组密码算法，该算法的分组长度为128比特，密钥长度为（）。

A. 64比特
B. 128比特
C. 192比特
D. 256比特

正确答案： **B**

23.SM4算法的密钥和明文长度分别是多少比特（ ）。

A. 128、256
B. 128、128
C. 256、128
D. 256、256

正确答案： **B**

24.SM3密码杂凑算法的消息分组长度为多少比特?

A. 256
B. 512
C. 768
D. 1024

正确答案： **B**

25.SM2算法与（）基于相同数学结构设计?

A. SM4
B. SM9
C. SM1
D. SM3

正确答案： **B**

26.SM3密码杂凑函数的迭代结构是（）。

A. Feistle迭代结构
B. SP结构
C. MD结构
D. Sponge结构

正确答案： **C**

27.SM3密码杂凑算法采用什么结构?

A. MD结构
B. Sponge结构
C. HAIFA结构
D. 宽管道结构

正确答案： **A**

28.SM4算法共有多少轮迭代？（ ）

A. 16
B. 32
C. 48
D. 64

正确答案： **B**

29.SM3密码杂凑算法的压缩函数一共多少轮?

A. 32
B. 64
C. 80
D. 120

正确答案： **B**

30.SM3密码杂凑算法输入的最大消息长度不超过多少比特?

A. 2^32
B. 2^64
C. 2^128
D. 任意长度

正确答案： **B**

31.SM3密码杂凑算法的压缩函数的输入一共有多少比特?

A. 256
B. 512
C. 768
D. 1024

正确答案： **C**

32.我国商用分组密码算法SM4中使用的S盒的输入是多少位？（）

A. 4位
B. 6位
C. 8位
D. 16位

正确答案： **C**

33.基域选择Fp-256时，SM2算法的数字签名的长度为（ ）比特。

A. 128
B. 256
C. 384
D. 512

正确答案： **D**

34.ZUC算法是一个面向字的序列密码，初始向量的长度分别为多少？（）

A. 64比特
B. 128比特
C. 256比特
D. 1024比特

正确答案： **B**

35.SM4加密算法是（ ）。

A. 分组密码体制
B. 序列密码体制
C. 置换密码体制
D. 替代密码体制

正确答案： **A**

36.GM/T 0091《基于口令的密钥派生规范》定义的基于口令的密钥派生函数 PBKDF ,盐值为不小于 64 比特的随机比特串，迭代次数不小于（）次。

A. 256
B. 512
C. 1024
D. 2048

正确答案： **C**

37.GM/T 0006《密码应用标识规范》定义的标识中，不包括以下哪种分组密码工作模式？ （ ）

A. ECB
B. CBC
C. CFB
D. CTR

正确答案： **D**

38.GM/T 0015《基于SM2密码算法的数字证书格式规范》中，关于证书扩展项说法不正确的是（ ）。

A. 扩展项包括两部分：扩展关键度和扩展项值
B. 采用关键性扩展项可能导致在通用的应用中无法使用证书
C. 颁发机构密钥标识符authorityKeyIdentifier也可用作CRL扩展
D. 如果不能识别关键扩展项，应拒绝接受该证书

正确答案： **A**

39.以下关于GM/T 0034《基于SM2密码算法的证书认证系统密码及其相关安全技术规范》描述错误的是（ ）。

A. 证书申请和下载可以采用在线或离线两种方式。
B. 用户签名密钥对和加密密钥对均由用户自己产生。
C. 用户的数字证书由CA签发，根CA的数字证书由根CA自己签发，下级CA的数字证书由上级CA签发。
D. 证书状态查询系统所提供的服务可以采用CRL查询或在线证书状态查询两种方式。

正确答案： **B**

40.GM/T 0015《基于SM2密码算法的数字证书格式规范》中，对于双证书，标准的证书扩展域的（ ）一定为关键项。

A. 密钥用法keyUsage
B. 主体密钥标识符subjectKeyIdentifier
C. 扩展密钥用途extKeyUsage
D. 认证机构authority

正确答案： **A**

多选题

1.在A5算法的LFSR中a的抽头系数为（ ）。

A. 18
B. 17
C. 16
D. 13

正确答案： **ABCD**

2.若Bob给Alice发送一封邮件，并想让Alice确信邮件是由Bob发出的，并且只能由Alice进行解密，则整个过程中涉及到的密钥有（）。

A. Alice的公钥
B. Alice的私钥
C. Bob的公钥
D. Bob的私钥

正确答案： **ABCD**

3.以下分组密码算法工作模式，说法是正确的（ ）。

A. 在CRT模式中，主动攻击者可以通过反转密文分组中的某些比特，引起解密后明文中的相应比特也发生反转。
B. 在OFB模式中，如果对密钥流的一个分组进行加密后其结果碰巧和加密前是相同的，那么这一分组之后的密钥流就会变成同一值的不断反复。
C. CFB模式与OFB模式的区别仅仅在于密码算法的输入。
D. 假设CBC模式加密的密文分组中有一个分组损坏了（如由于硬盘故障导致密文分组的值发生了改变），在这种情况下，只要密文分组的长度没有发生变化，则解密时最多只会有2个分组受到数据损坏的影响。

正确答案： **ABCD**

4.下列关于CA及其用户产生密钥对的说法是正确的（ ）。

A. 用户可以自己产生加密密钥对
B. 用户可以自己产生签名密钥对
C. CA可以产生自己的密钥对
D. CA可以产生用户的所有密钥对

正确答案： **BC**

5.以下属于多表代换古典密码体制的有（）。

A. Playfair体制
B. Vigenere体制
C. Beaufort体制
D. Hill体制

正确答案： **ABCD**

6.对称密码体制的优点是（ ）。

A. 加密速度快
B. 适合批量加密数据
C. 可用于签名
D. 可解决密钥分配、管理问题

正确答案： **AB**

7.下列我国商密算法中，被纳入国际标准化组织ISO/IEC的包括（）。

A. SM2数字签名算法
B. SM3密码杂凑算法
C. SM4分组密码算法
D. 祖冲之密码算法

正确答案： **ABCD**

8.SM2签名结果用ASN.1 DER表示时，如果签名值为71字节，可能的情形是（ ）。

A. 签名值中，r的最高位为1，s的最高位为0
B. 签名值中，r的最高位为0，s的最高位为1
C. 签名值中，r的最高位为0，s的最高位为0
D. 签名值中，r的最高位为1，s的最高位为1

正确答案： **AB**

9.ZUC算法密钥装载时LFSR中需要装入（ ）。

A. 种子密钥
B. 初始向量
C. 16个常数
D. 15个常数

正确答案： **ABC**

10.SM2算法与（）算法属于同一类数学结构?

A. ECDH
B. RSA
C. ECDSA
D. SM9

正确答案： **ACD**

11.SM3密码杂凑算法的运算中哪些起到扩散的作用?

A. 循环移位
B. P置换
C. 模加
D. 布尔函数

正确答案： **AB**

12.SM2公钥密码算法一般包括如下哪些功能（ ）。

A. 密钥分散
B. 签名
C. 密钥交换
D. 加密

正确答案： **BCD**

13.ZUC算法驱动部分产生的素域上序列的性质包括（ ）。

A. 权位序列平移等价
B. 序列集合模2压缩保墒
C. 所有权位序列周期相同
D. 所有权位序列线性复杂度相同

正确答案： **ABCD**

14.SM2公钥加密算法可以抵抗哪些攻击?

A. 唯密文攻击
B. 选择明文攻击
C. 选择密文攻击
D. 密钥恢复攻击

正确答案： **ABCD**

15.A利用B的SM2公钥直接加密消息，将SM2密文传输给B，以下说法正确的是（ ）。

A. 这种方式可以实现消息源真实性鉴别
B. 这种方式不常用，SM2一般用于加密一个对称加密密钥
C. 这种方式可以对消息的机密性进行保护
D. 这种方式可以防范对消息的恶意替换

正确答案： **BC**

16.在GM/T 0019《通用密码服务接口规范》中，哪些函数可用于信息机密性保护？（ ）

A. 计算会话密钥
B. 单块加密运算
C. 结束解密运算
D. 多组数据消息鉴别码运算

正确答案： **ABC**

17.在GM/T 0003.1-2012《SM2椭圆曲线公钥密码算法》中，包含哪几个部分？（ ）

A. 公钥加密
B. 数字签名
C. 密钥交换
D. 身份认证

正确答案： **ABC**

18.GM/T 0021《动态口令密码应用技术规范》动态口令的生成使用到了（ ）过程。

A. 算法函数
B. 截位函数
C. 数据组装
D. 求余运算

正确答案： **ABCD**

19.根据GM/T 0054-2018《信息系统密码应用基本要求》，密钥生命周期包括密钥生成、分发、存储、使用、更新、归档、撤销、备份、恢复和销毁。以下关于密钥的使用描述正确的是（）。

A. 在密钥使用过程中，应防止密钥的泄露和更换，并根据密钥安全策略及时更新密钥
B. 建立密钥应急机制，应对突发事件，如密钥丢失、密钥泄露、密钥算法缺陷公告等
C. 不需要保护公钥的机密性，但是在使用前(如签名验证或密钥协商过程)需要验证公钥的完整性和实体与公钥的关系，以保证公钥来源的真实性
D. 公钥是公开的，在使用时既不需要做机密性，也不需要做完整性保护

正确答案： **ABC**

20.GB/T 15852《信息技术 安全技术 消息鉴别码》标准中定义的消息鉴别码可以基于（）机制实现。

A. 分组密码
B. 泛杂凑函数
C. 非对称密码
D. 专用杂凑函数

正确答案： **ABD**

判断题

1.HASH函数的单向性也称为抗原像性（）

- 正确
- 错误

答案: **正确**

2.专门用来提高软件实现效率的序列密码算法是RC4算法。（）

- 正确
- 错误

答案: **错误**

3.NP问题是指用非确定性算法在多项式时间内解决的问题（）

- 正确
- 错误

答案: **正确**

4.Rabin算法是基于二次剩余的公钥密码体制。（）

- 正确
- 错误

答案: **正确**

5.SHA256的输出为256bit的杂凑值。

- 正确
- 错误

答案: **正确**

6.X.509是基于对称加密的认证协议，它提供跨网络的认证。（）

- 正确
- 错误

答案: **错误**

7.SM3密码杂凑算法的压缩函数共有80轮操作。

- 正确
- 错误

答案: **错误**

8.SM3密码杂凑算法的前16轮采用非线性的布尔函数。

- 正确
- 错误

答案: **错误**

9.SM3密码杂凑算法不是单向函数。

- 正确
- 错误

答案: **错误**

10.SM2包含了数字签名、密钥交换、公钥加密三个算法。

- 正确
- 错误

答案: **正确**

11.SM3密码杂凑算法在2016年被批准成为国家标准算法。

- 正确
- 错误

答案: **正确**

12.SM3密码杂凑算法中没有使用循环移位运算。

- 正确
- 错误

答案: **错误**

13.SM9密码算法的主公钥由KGC通过随机数发生器产生。

- 正确
- 错误

答案: **错误**

14.SM3密码杂凑算法一共有2个置换函数。

- 正确
- 错误

答案: **正确**

15.根据目前公开的分析结果，SM3密码杂凑算法的安全性高于SHA-256。

- 正确
- 错误

答案: **正确**

16.GM/T 0005《随机性检测规范》中，“离散傅立叶检测”用于检测待检序列进行傅立叶变换后得到不正常的峰值个数是否超过了允许值。

- 正确
- 错误

答案: **正确**

17.GM/T 0021《动态口令密码应用技术规范》使用SM3算法产生的动态口令比使用SM4算法产生的动态口令长。（ ）

- 正确
- 错误

答案: **错误**

18.国家鼓励和支持密码科学技术研究和应用，依法保护密码领域的知识产权，促进密码科学技术进步和创新。（ ）

- 正确
- 错误

答案: **正确**

19.GM/T 0015《基于SM2密码算法的数字证书格式规范》中，CA应确保使用大于20个8位字节的证书序列号。

- 正确
- 错误

答案: **错误**

20.GM/T 0021《动态口令密码应用技术规范》动态口令是身份鉴别的唯一算法。（ ）

- 正确
- 错误

答案: **错误**

8

单选题

1.DES加密算法共经过( )次迭代运算的处理。

A. 8
B. 9
C. 16
D. 18

正确答案： **C**

2.移位密码通常可用来加密普通的英文句子，假设其密钥为K=11，将明文“wewillmeet”加密后，密文为（ ）。

A. JQJTXXYQQG
B. HPHTWWXPPE
C. JEJUZZXEEQ
D. HQHTXXWQQF

正确答案： **B**

3.以下各种加密算法属于古典加密算法的是（ ）。

A. DES算法
B. Caesar算法
C. IDEA算法
D. DSA算法

正确答案： **B**

4.下列选项不是密码系统基本部分组成的是（ ）。

A. 明文空间
B. 密码算法
C. 初始化
D. 密钥

正确答案： **C**

5.（ ）年，德国柏林大学教授普朗克首先提出了“量子论”

A. 1895
B. 1900
C. 1945
D. 1947

正确答案： **B**

6.下列不属于对称算法的是（ ）。

A. 祖冲之ZUC算法
B. SM2
C. SM7
D. SM4

正确答案： **B**

7.一个同步流密码具有很高的密码强度主要取决于（ ）。

A. 密钥流生成器的设计
B. 密钥长度
C. 明文长度
D. 密钥复杂度

正确答案： **A**

8.MD5是一种杂凑函数，用于将任意长度的消息映射为固定长度的输出。它通常用于检查文件完整性、数字签名、消息认证码等方面。MD5算法迭代运算包括（ ）轮处理过程。

A. 2
B. 3
C. 4
D. 5

正确答案： **C**

9.AES的轮函数当中用来实现混淆的是（ ）

A. 轮密钥加
B. S盒
C. 列混合
D. 行移位

正确答案： **B**

10.Skipjack是一个密钥长度为（ ）位分组加密算法。

A. 56
B. 64
C. 80
D. 128

正确答案： **C**

11.如果有6个成员组成的团体希望互相通信，那么在在基于密钥中心的对称密钥分发结构中，需要人工分发KEK的数量为（）。

A. 5
B. 6
C. 9
D. 15

正确答案： **B**

12.下面哪个是分组密码（）。

A. 凯撒密码
B. AES
C. 轮转机
D. 隐写术

正确答案： **B**

13.SHA1算法输出报文杂凑值的长度为（ ）。

A. 120
B. 128
C. 144
D. 160

正确答案： **D**

14.基域选择Fp-256时，SM2公钥加密算法的私钥长度为（ ）。

A. 128
B. 256
C. 384
D. 512

正确答案： **B**

15.通常使用( )验证消息的完整性。

A. 消息摘要
B. 数字信封
C. 对称解密算法
D. 公钥解密算法

正确答案： **A**

16.对输入为448比特的消息，SM3密码杂凑算法生成杂凑值时需要调用几次压缩函数?

A. 1
B. 2
C. 3
D. 4

正确答案： **B**

17.密码学在信息安全中的应用是多样的，以下（ ）不属于密码学的具体应用。

A. 生成各种网络协议
B. 消息认证，确保信息完整性
C. 加密技术，保护传输信息
D. 进行身份认证

正确答案： **A**

18.我国商用密码算法SM2是一种椭圆曲线公钥密码算法，其推荐的密钥长度为多少?

A. 128bit
B. 256bit
C. 192bit
D. 512bit

正确答案： **B**

19.基域选择Fp-256时，SM2算法的数字签名的长度为（ ）比特。

A. 128
B. 256
C. 384
D. 512

正确答案： **D**

20.SM4加密算法是（ ）。

A. 分组密码体制
B. 序列密码体制
C. 置换密码体制
D. 替代密码体制

正确答案： **A**

21.SM3密码杂凑算法采用什么结构?

A. MD结构
B. Sponge结构
C. HAIFA结构
D. 宽管道结构

正确答案： **A**

22.SM4算法的密钥和明文长度分别是多少比特（ ）。

A. 128、256
B. 128、128
C. 256、128
D. 256、256

正确答案： **B**

23.在SM4加密算法中明文分组长度为（ ）。

A. 64
B. 128
C. 256
D. 512

正确答案： **B**

24.在SM4算法中轮密钥的长度为（ ）位。

A. 32
B. 128
C. 256
D. 512

正确答案： **A**

25.SM2算法是（）国家商用密码算法?

A. 美国
B. 我国
C. 欧盟
D. 俄罗斯

正确答案： **B**

26.祖冲之（ZUC）序列密码主算法一次输出的密钥长度为多少？ ()

A. 32比特
B. 64比特
C. 128比特
D. 256比特

正确答案： **A**

27.SM3密码杂凑算法的压缩函数一共有几种不同的布尔函数?

A. 2
B. 3
C. 4
D. 5

正确答案： **A**

28.SM2算法是（）密码算法?

A. 序列密码
B. 对称密码算法
C. 公钥密码
D. 密码杂凑函数

正确答案： **C**

29.SM3密码杂凑算法是中国国家密码管理局公布的中国商用密码杂凑算法标准。SM3密码杂凑算法是哪种类型的算法?

A. 分组密码算法
B. 公钥密码算法
C. 数字签名算法
D. 杂凑函数

正确答案： **D**

30.SM3密码杂凑算法的压缩函数一共多少轮?

A. 32
B. 64
C. 80
D. 120

正确答案： **B**

31.ZUC算法是一个面向字的序列密码，密钥长度和初始向量的长度分别为多少？ ()

A. 64比特
B. 128比特
C. 256比特
D. 1024比特

正确答案： **B**

32.我国商用分组密码算法SM4中使用的S盒的输入是多少位？ ()

A. 4位
B. 6位
C. 8位
D. 16位

正确答案： **C**

33.SM2算法的安全性基于（）困难假设?

A. 双线性映射
B. 椭圆曲线离散对数
C. 多线性映射
D. 丢番图方程求解

正确答案： **B**

34.SM3密码杂凑算法的压缩函数的输入一共有多少比特?

A. 256
B. 512
C. 768
D. 1024

正确答案： **C**

35.我国商用分组密码算法SM4中使用的S盒的输出是多少位？（）

A. 4位
B. 6位
C. 8位
D. 16位

正确答案： **C**

36.GM/T 0036《采用非接触卡的门禁系统密码应用技术指南》。门禁系统鉴别协议遵循（ ）。

A. GM/T 0032 基于角色的授权与访问控制技术规范
B. GM/T 0033 时间戳接口规范
C. GM/T 0034 基于SM 2 密码算法的证书认证系统密码及其相关安全技术规范
D. GM/T 0035 射频识别系统密码应用技术要求

正确答案： **D**

37.GM/T 0010《SM2密码算法加密签名消息语法规范》中私钥表达是一个（ ）。

A. CHOICE
B. SEQUENCE
C. OBJECT IDENTFIFIER
D. INTEGER

正确答案： **B**

38.2019年10月26日下午，十三届全国人大常委会第十四次会议表决通过《密码法》，于（ ）起施行。

A. 2019年12月1日
B. 2020年1月1日
C. 2020年5月1日
D. 2020年10月1日

正确答案： **B**

39.GM/T 0006《密码应用标识规范》定义的标识中，不包括以下哪种分组密码算法？（ ）

A. SM1
B. SM4
C. AES
D. ZUC祖冲之算法

正确答案： **C**

40.GM/T 0005《随机性检测规范》中，“线性复杂度检测”中计算线性复杂度，通常采用以下哪种算法（ ）

A. Miller-Rabin算法
B. Berlekamp-Massey算法
C. 最小二乘法
D. 中国剩余定理

正确答案： **B**

多选题

1.下列哪些算法既能实现加解密又能实现签名（）。

A. RSA
B. ElGamal
C. AES
D. DES

正确答案： **AB**

2.下列密码体制不可以抗量子攻击的是（ ）。

A. RSA
B. Rabin
C. AES
D. NTRU

正确答案： **ABC**

3.人工智能的数据安全保护是密码学在人工智能安全领域的重要应用方向. 当前的一个研究热点是在机器学习的模型训练和推理阶段利用新型密码学机制, 保证在得到精确模型或者准确预测结果的同时, 不泄露用户的数据。相关新型密码学体制主要包括以下哪两种（）

A. 同态加密
B. 安全多方计算
C. 格密码
D. 密钥分享

正确答案： **AB**

4.混淆和扩散是密码设计的一般原则，所以在很多密码设计中，都采用了代换和置换等变化来达到混乱和扩散的效果。下列哪些密码体制中，采用了置换的处理思想（）。

A. RSA
B. 凯撒（CAESAR）密码
C. AES
D. DES

正确答案： **CD**

5.为了提高DES的安全性，并充分利用现有的软硬件资源，人们已设计开发了DES的多种变异版本，下面（）属于DES变异版本。

A. 2DES
B. 3DES
C. 4DES
D. 5DES

正确答案： **AB**

6.流加密算法有以下哪些( )。

A. A5
B. RC4
C. AES
D. DES

正确答案： **AB**

7.SM3密码杂凑算法的压缩函数的结构和哪些算法相同?

A. MD5
B. RIPEMD
C. SHA-1
D. SHA-256

正确答案： **ACD**

8.SM2公钥加密算法的加密函数涉及到哪些运算?

A. 随机数生成
B. 杂凑值计算
C. 椭圆曲线点乘
D. 伪随机比特序列生成

正确答案： **ABCD**

9.ZUC算法中使用到的运算包括（ ）。

A. 模2^{31}-1的加法
B. 模2^{32}的加法
C. 右循环移位
D. 左循环移位

正确答案： **ABD**

10.SM2公钥密码算法一般包括如下哪些功能（ ）。

A. 密钥分散
B. 签名
C. 密钥交换
D. 加密

正确答案： **BCD**

11.关于ZUC算法初始化过程描述正确的是（ ）。

A. 迭代64轮
B. 初始化完成后直接输出密钥流
C. 迭代32轮
D. 非线性函数的输出会参与LFSR的反馈运算

正确答案： **CD**

12.A利用B的SM2公钥直接加密消息，将SM2密文传输给B，以下说法正确的是（ ）。

A. 这种方式可以实现消息源真实性鉴别
B. 这种方式不常用，SM2一般用于加密一个对称加密密钥
C. 这种方式可以对消息的机密性进行保护
D. 这种方式可以防范对消息的恶意替换

正确答案： **BC**

13.SM2公钥加密算法的密文包含哪些元素?

A. 椭圆曲线点乘
B. 杂凑值
C. 比特串
D. 基域元素

正确答案： **ABC**

14.SM3密码杂凑算法的运算中哪些起到混淆的作用?

A. 循环移位
B. P置换
C. 模加
D. 布尔函数

正确答案： **CD**

15.SM2算法涉及到的数据格式包括?

A. 椭圆曲线点乘
B. 域元素
C. 比特串
D. 字符串

正确答案： **ABCD**

16.GB/T 15843《信息技术安全技术实体鉴别》，下列说法正确的是（ ）。

A. 给出了采用对称加密算法、数字签名技术和密码校验函数实现机制
B. 采用时间戳、序号或随机数等时变参数防止重放攻击
C. 当采用使用随机数的挑战响应方法时，相互鉴别需要四次传递
D. 生成方在反馈验证方B的权标（TokenAB）中，可通过单向密钥取代可区分标识符

正确答案： **ABD**

17.GM/T 0009《SM2密码算法使用规范》中，在SM2密钥协商过程中, 发起方计算共享密钥时的输入数据包括（ ）。

A. 自身的公钥
B. 自身的临时公钥
C. 自身的私钥
D. 自身的用户身份标识

正确答案： **ABCD**

18.GM/Z 4001《密码术语》中提及的几种密码攻击方法包括（ ）

A. 重放攻击
B. 唯密文攻击
C. 穷举攻击
D. 选择明文攻击

正确答案： **ABCD**

19.GM/T 0021《动态口令密码应用技术规范》参与动态口令运算的因素包括（ ）。

A. 时间因子
B. 事件因子
C. 挑战因子
D. 种子密钥

正确答案： **ABCD**

20.GM/T 0005《随机性检测规范》中，关于检测原理以下说法正确的是（ ）

A. “Maurer通用统计检测”用于检测待检序列能否被无损压缩，如果待检序列能被显著地压缩，那么就认为该序列是不随机的。
B. “重叠子序列检测”通过比较m位可重叠子序列模式的频数和m+1位可重叠子序列模式的频数来检测其随机性。
C. “扑克检测”用于检测待检序列中m位非重叠子序列的每一种模式的个数是否接近。
D. “矩阵秩检测”用于检测待检序列中给定长度的子序列之间的线性独立性。

正确答案： **ACD**

判断题

1.RIJNDAEL算法不存在弱密钥和半若密钥，能有效抵抗目前已知的攻击（ ）。

- 正确
- 错误

答案: **正确**

2.SHA256的输出为256bit的杂凑值。

- 正确
- 错误

答案: **正确**

3.S-HTTP除了提供机密性以外，还提供了对公钥密码及数字签名的支持。（ ）

- 正确
- 错误

答案: **正确**

4.著名的Kerberos认证系统采用了对称和非对称加密相结合的技术（）。

- 正确
- 错误

答案: **错误**

5.IPSec体系中，AH只能实现地址源发认证和数据完整性服务，ESP只能实现信息保密性（数据加密）服务。

- 正确
- 错误

答案: **错误**

6.Rijndael算法的密钥长度是128位，分组长度也为128位。（）

- 正确
- 错误

答案: **错误**

7.椭圆曲线双线性对的安全性是SM9密码算法安全性的重要基础。

- 正确
- 错误

答案: **正确**

8.SM3密码杂凑算法的压缩函数共有64轮操作。

- 正确
- 错误

答案: **正确**

9.SM3密码杂凑算法消息字的存储采用小端形式，左边为低有效位，右边为高有效位。

- 正确
- 错误

答案: **错误**

10.SM3密码杂凑算法的消息分组长度是可变的。

- 正确
- 错误

答案: **错误**

11.SM3密码杂凑算法的布尔函数输出2个字。

- 正确
- 错误

答案: **错误**

12.SM9密码算法的消息认证码函数需要调用Hash函数。

- 正确
- 错误

答案: **正确**

13.SM2与SM9都是基于椭圆曲线设计的。

- 正确
- 错误

答案: **正确**

14.SM9标识密码算法密钥交换过程中不需要计算群中的元素。（）

- 正确
- 错误

答案: **错误**

15.SM9公钥加密算法是密钥封装机制和消息封装机制的结合。

- 正确
- 错误

答案: **正确**

16.根据GM/T 0029-2014《签名验签服务器技术规范》，签名验签服务器能够配置时间源服务器，自动同步时间。（）

- 正确
- 错误

答案: **正确**

17.国务院商务主管部门、国家密码管理部门依法对涉及国家安全、社会公共利益且具有加密保护功能的商用密码实施进口许可，对涉及国家安全、社会公共利益或者中国承担国际义务的商用密码实施出口管制。（）

- 正确
- 错误

答案: **正确**

18.GM/T 0021《动态口令密码应用技术规范》使用SM3算法产生的动态口令比使用SM4算法产生的动态口令长。（ ）

- 正确
- 错误

答案: **错误**

19.GM/T 0005《随机性检测规范》中，“离散傅立叶检测”用于检测待检序列进行傅立叶变换后得到不正常的峰值个数是否超过了允许值。

- 正确
- 错误

答案: **正确**

20.我国《密码法》所称密码，是指采用特定变换的方法对信息等进行加密保护、安全认证的技术、产品和服务。（ ）

- 正确
- 错误

答案: **正确**

9

单选题

1.（）基于IDEA算法。

A. S/MIME
B. PGP
C. SET
D. SSL

正确答案： **B**

2.在（k,n）门限秘密分享方案中，由少于（）个参与者所持有的部分信息则无法重构秘密。

A. k
B. n
C. k+1
D. k-1

正确答案： **A**

3.下列选项不是密码系统基本部分组成的是（ ）。

A. 明文空间
B. 密码算法
C. 初始化
D. 密钥

正确答案： **C**

4.一个同步流密码具有很高的密码强度主要取决于（ ）。

A. 密钥流生成器的设计
B. 密钥长度
C. 明文长度
D. 密钥复杂度

正确答案： **A**

5.采用SM4算法的CBC-MAC，其输出的标签无法支持哪一个长度?

A. 32
B. 64
C. 128
D. 256

正确答案： **D**

6.下列的加密方案基于格理论的是（ ）。

A. ECC
B. RSA
C. AES
D. Regev

正确答案： **D**

7.美国已决定在（ ）以后将不再使用DES。

A. 1997年12月
B. 1998年12月
C. 1999年12月
D. 2000年12月

正确答案： **B**

8.IDEA的分组长度是（ ）bit。

A. 56
B. 64
C. 96
D. 128

正确答案： **B**

9.DES是分组密码，它所取的迭代次数是（ ）。

A. 8
B. 16
C. 32
D. 64

正确答案： **B**

10.Skipjack是一个密钥长度为（ ）位分组加密算法。

A. 56
B. 64
C. 80
D. 128

正确答案： **C**

11.下列哪种协议需要由双方或多方共同提供信息建立起共享会话密钥？（ ）

A. 密钥建立协议
B. 密钥传输协议
C. 密钥共享协议
D. 密钥协商协议

正确答案： **D**

12.一个安全的密码杂凑函数需要能够抵抗生日攻击等强抗碰撞性攻击。生日攻击即：在随机抽出的N个人中，N至少为（ ），就能保证至少两个人生日一样（排除2月29日的情况）的概率大于二分之一。（ ）

A. 20
B. 23
C. 150
D. 182

正确答案： **B**

13.在标准的DES的算法中，其分组的长度为（ ）位。

A. 56
B. 64
C. 112
D. 128

正确答案： **B**

14.密码学在信息安全中的应用是多样的，以下（ ）不属于密码学的具体应用。

A. 生成各种网络协议
B. 消息认证，确保信息完整性
C. 加密技术，保护传输信息
D. 进行身份认证

正确答案： **A**

15.在IPSec VPN协议中，SM4分组密码算法的属性值是（ ）。

A. 128
B. 129
C. 64
D. 256

正确答案： **B**

16.在DES算法中子密钥的长度为（ ）位。

A. 48
B. 49
C. 64
D. 52

正确答案： **A**

17.基域选择Fp-256时，SM2算法的数字签名的公钥长度为（ ）。

A. 128
B. 256
C. 384
D. 512

正确答案： **D**

18.SM3密码杂凑算法输入的最大消息长度不超过多少比特?

A. 2^32
B. 2^64
C. 2^128
D. 任意长度

正确答案： **B**

19.在SM4加密算法中明文分组长度为（ ）。

A. 64
B. 128
C. 256
D. 512

正确答案： **B**

20.祖冲之（ZUC）序列密码主算法一次输出的密钥长度为多少？（）

A. 32比特
B. 64比特
C. 128比特
D. 256比特

正确答案： **A**

21.SM4分组密码算法，该算法的分组长度为128比特，密钥长度为（）。

A. 64比特
B. 128比特
C. 192比特
D. 256比特

正确答案： **B**

22.SM2算法中的加密算法达到的安全性是（）。

A. OW-CPA
B. IND-CPA
C. IND-CCA2
D. NM-CPA

正确答案： **C**

23.SM3密码杂凑算法的消息分组长度为多少比特?

A. 256
B. 512
C. 768
D. 1024

正确答案： **B**

24.SM2算法中的密钥交换算法支持（）方密钥交换。

A. 2
B. 3
C. 4
D. 多

正确答案： **A**

25.SM3密码杂凑函数的迭代结构是（）。

A. Feistle迭代结构
B. SP结构
C. MD结构
D. Sponge结构

正确答案： **C**

26.SM4加密算法是（ ）。

A. 分组密码体制
B. 序列密码体制
C. 置换密码体制
D. 替代密码体制

正确答案： **A**

27.SM3密码杂凑算法的链接变量长度为多少比特?

A. 128
B. 224
C. 256
D. 512

正确答案： **C**

28.SM3密码杂凑算法的压缩函数一共有几种不同的布尔函数?

A. 2
B. 3
C. 4
D. 5

正确答案： **A**

29.SM3密码杂凑算法是中国国家密码管理局公布的中国商用密码杂凑算法标准。SM3密码杂凑算法是哪种类型的算法?

A. 分组密码算法
B. 公钥密码算法
C. 数字签名算法
D. 杂凑函数

正确答案： **D**

30.在SM4算法中轮密钥的长度为（ ）位。

A. 32
B. 128
C. 256
D. 512

正确答案： **A**

31.利用SM2公钥密码体制两次加密相同的明文，密文相同吗？ ()

A. 不同
B. 相同
C. 有时相同，也有不同
D. 根据具体情况

正确答案： **A**

32.基域选择Fp-256时，SM2算法的数字签名的长度为（ ）比特。

A. 128
B. 256
C. 384
D. 512

正确答案： **D**

33.SM2算法是（）国家商用密码算法?

A. 美国
B. 我国
C. 欧盟
D. 俄罗斯

正确答案： **B**

34.SM2算法是（）密码算法?

A. 序列密码
B. 对称密码算法
C. 公钥密码
D. 密码杂凑函数

正确答案： **C**

35.SM3密码杂凑算法的压缩函数一共多少轮?

A. 32
B. 64
C. 80
D. 120

正确答案： **B**

36.以下关于GM/T 0034《基于SM2密码算法的证书认证系统密码及其相关安全技术规范》描述错误的是（ ）。

A. 证书申请和下载可以采用在线或离线两种方式。
B. 用户签名密钥对和加密密钥对均由用户自己产生。
C. 用户的数字证书由CA签发，根CA的数字证书由根CA自己签发，下级CA的数字证书由上级CA签发。
D. 证书状态查询系统所提供的服务可以采用CRL查询或在线证书状态查询两种方式。

正确答案： **B**

37.GM/T 0009《SM2密码算法使用规范》中，Z值计算公式Z = SM3(ENTL‖ID‖a‖b‖xG‖yG‖xA‖yA)中ENTL的内容表示ID的比特长度，ENTL自身的长度为（ ）字节。

A. 1
B. 2
C. 4
D. 8

正确答案： **B**

38.GM/T 0015《基于SM2密码算法的数字证书格式规范》中，关于证书扩展项说法不正确的是（ ）。

A. 扩展项包括两部分：扩展关键度和扩展项值
B. 采用关键性扩展项可能导致在通用的应用中无法使用证书
C. 颁发机构密钥标识符authorityKeyIdentifier也可用作CRL扩展
D. 如果不能识别关键扩展项，应拒绝接受该证书

正确答案： **A**

39.GM/T 0035《射频识别系统密码应用技术要求》第4部分，双向鉴别前，读写器系统通过UID获得电子标签芯片的（ ）。

A. 根密钥
B. 分散密钥
C. 分散因子
D. 标签数据

正确答案： **B**

40.GM/T 0035《射频识别系统密码应用技术要求》第3部分，电子标签对读写器的身份鉴别出现在哪个级别以上（ ）。

A. 1
B. 2
C. 3
D. 4

正确答案： **C**

多选题

1.DES分组模式有( )?

A. ECB
B. CBC
C. CFB
D. OFB

正确答案： **ABCD**

2.下面属于PKI组成部分的是（）。

A. 数字证书库
B. 安全应用接口
C. CA数字证书签发系统
D. 密钥备份及恢复系统

正确答案： **ABCD**

3.下列选项中不是序列密码起源的算法是（）。

A. DES
B. Vernam
C. AES
D. RSA

正确答案： **ACD**

4.混淆和扩散是密码设计的一般原则，所以在很多密码设计中，都采用了代换和置换等变化来达到混乱和扩散的效果。下列哪些密码体制中，采用了置换的处理思想（）。

A. RSA
B. 凯撒（CAESAR）密码
C. AES
D. DES

正确答案： **CD**

5.下列说法观点正确的是（）。

A. 1978年，R. L. Rivest提出一种基于秘密同态的数据库加密技术。
B. 2002年，Hakan Hacigumus
等人提出一种基于DAS模式的加密数据库两阶段查询策略。
C. 1997年，戴一奇等人基于非同态密文提出了利用分治原则建立特殊索引的方法对数据进行快速检索。
D. DES算法是美国国家标准技术研究所公布的新一代加密标准。

正确答案： **ABC**

6.序列密码算法有哪些？（）

A. ZUC
B. RC4
C. AES
D. DES

正确答案： **AB**

7.SM3密码杂凑算法的运算中哪些起到扩散的作用？

A. 循环移位
B. P置换
C. 模加
D. 布尔函数

正确答案： **AB**

8.ZUC算法结构的核心部分包括（ ）。

A. LFSR
B. 比特重组BR
C. 非线性函数F
D. Feistel网络

正确答案： **ABC**

9.SM2签名结果用ASN.1 DER表示时，如果签名值为71字节，可能的情形是（ ）。

A. 签名值中，r的最高位为1，s的最高位为0
B. 签名值中，r的最高位为0，s的最高位为1
C. 签名值中，r的最高位为0，s的最高位为0
D. 签名值中，r的最高位为1，s的最高位为1

正确答案： **AB**

10.SM2公钥密码算法一般包括如下哪些功能（ ）。

A. 密钥分散
B. 签名
C. 密钥交换
D. 加密

正确答案： **BCD**

11.SM4算法的轮函数包括什么运算？（ ）

A. 异或
B. 非线性变换
C. 线性变换
D. 相乘

正确答案： **ABC**

12.ZUC算法非线性函数F部分两个线性变换L1和L2具有性质（ ）。

A. 均为置换
B. 差分分支数均为5
C. 线性分支数均为5
D. 实现代价较高

正确答案： **ABC**

13.SM2算法涉及到的数据格式包括?

A. 椭圆曲线点乘
B. 域元素
C. 比特串
D. 字符串

正确答案： **ABCD**

14.ZUC算法非线性函数F部分使用的非线性运算包括（ ）。

A. S-盒变换
B. 模2^{32}的加法
C. 模2^{31}-1的加法
D. 比特串异或运算

正确答案： **AB**

15.SM4分组密码算法轮函数中的T置换，包括哪些运算?

A. 非线性变换
B. 4个并行的S盒运算
C. 线性变换
D. 列混合变换

正确答案： **ABC**

16.GM/Z 4001《密码术语》中，哪种算法属于公钥密码算法（ ）

A. SM9
B. SM2
C. SM3
D. SM4

正确答案： **AB**

17.在GM/T 0003.1-2012《SM2椭圆曲线公钥密码算法》中，包含哪几个部分？（ ）

A. 公钥加密
B. 数字签名
C. 密钥交换
D. 身份认证

正确答案： **ABC**

18.GB/T 15852《信息技术 安全技术 消息鉴别码》标准中定义的消息鉴别码可以基于（）机制实现。

A. 分组密码
B. 泛杂凑函数
C. 非对称密码
D. 专用杂凑函数

正确答案： **ABD**

19.GM/T 0031-2014 《安全电子签章密码技术规范》电子印章中一般包含哪些原文信息（ ）。

A. 原文内容本身
B. 原文杂凑
C. 原文属性信息
D. 原文名称

正确答案： **BC**

20.GM/T 0021《动态口令密码应用技术规范》对提交的动态口令进行认证的认证方式包括（ ）。

A. 静态口令
B. 动态口令
C. 动态口令+静态口令
D. 免口令

正确答案： **BC**

判断题

1.RIJNDAEL算法不存在弱密钥和半若密钥，能有效抵抗目前已知的攻击（ ）。

- 正确
- 错误

答案: **正确**

2.Vigenere加密法和Beaufort加密法是多码替换加密法的两个例子。（ ）

- 正确
- 错误

答案: **正确**

3.自同步序列密码比同步序列密码更好地抗击基于明文冗余的攻击（ ）

- 正确
- 错误

答案: **正确**

4.WPA/WPA2无线加密协议安全性很高，目前没有破解的途径。

- 正确
- 错误

答案: **错误**

5.S-HTTP除了提供机密性以外，还提供了对公钥密码及数字签名的支持。（）

- 正确
- 错误

答案: **正确**

6.Diffie-Hellman密钥交换协议可用于对会话消息进行加密和解密。

- 正确
- 错误

答案: **错误**

7.SM3密码杂凑算法的字长为16比特。

- 正确
- 错误

答案: **错误**

8.SM9密码算法的用户私钥由KGC通过随机数发生器产生。

- 正确
- 错误

答案: **错误**

9.SM3密码杂凑算法的消息分组长度是可变的。

- 正确
- 错误

答案: **错误**

10.椭圆曲线双线性对的安全性是SM9密码算法安全性的重要基础。

- 正确
- 错误

答案: **正确**

11.SM3密码杂凑算法的消息扩展过程一共生成128个消息字。

- 正确
- 错误

答案: **错误**

12.SM9密码算法需要保证选取的椭圆曲线上离散对数问题难解。

- 正确
- 错误

答案: **正确**

13.SM2包含了数字签名、密钥交换、公钥加密三个算法。

- 正确
- 错误

答案: **正确**

14.SM3密码杂凑算法在2012年被批准成为行业标准算法。

- 正确
- 错误

答案: **正确**

15.SM9公钥加密算法消息封装机制包括基于KDF的序列密码及结合KDF的分组密码算法两种类型。

- 正确
- 错误

答案: **正确**

16.国家支持社会团体、企业利用自主创新技术制定高于国家标准、行业标准相关技术要求的商用密码团体标准、企业标准。（）

- 正确
- 错误

答案: **正确**

17.GM/T 0034《基于SM2密码算法的证书认证系统密码及其相关安全技术规范》中规定，证书认证中心对数据变化量少的服务器，可每周做一次备份。（）

- 正确
- 错误

答案: **正确**

18.GM/T 0006《密码应用标识规范》定义了C和Java等语言实现密码算法时的密钥结构体等具体数据结构。

- 正确
- 错误

答案: **错误**

19.根据GM/T 0029-2014《签名验签服务器技术规范》，签名验签服务器能够配置时间源服务器，自动同步时间。（）

- 正确
- 错误

答案: **正确**

20.商用密码检测、认证机构应当对其在商用密码检测认证中所知悉的国家秘密和商业秘密承担保密义务。（）

- 正确
- 错误

答案: **正确**

10

单选题

1.Skipjack是一个密钥长度为（ ）位分组加密算法。

A. 56
B. 64
C. 80
D. 128

正确答案： **C**

2.在SM3算法中，分组长度为（ ）位。

A. 56
B. 64
C. 488
D. 512

正确答案： **D**

3.如果有6个成员组成的团体希望互相通信，那么在点到点的对称密钥分发结构中，需要人工分发密钥加密密钥（KEK）的数量为（）。

A. 18
B. 3
C. 15
D. 18

正确答案： **C**

4.基域选择Fp-256时，SM2公钥加密算法的私钥长度为（ ）。

A. 128
B. 256
C. 384
D. 512

正确答案： **B**

5.在（k,n）门限秘密分享方案中，由少于（ ）个参与者所持有的部分信息则无法重构秘密。

A. k
B. n
C. k+1
D. k-1

正确答案： **A**

6.若Alice想向Bob分发一个会话密钥，采用ElGamal公钥加密算法，那么Alice应该选用的密钥是？（ ）

A. Alice的公钥
B. Alice的私钥
C. Bob的公钥
D. Bob的私钥

正确答案： **C**

7.（ ）基于IDEA算法。

A. S/MIME
B. PGP
C. SET
D. SSL

正确答案： **B**

8.DES算法属于加密技术中的（）

A. 对称加密
B. 不对称加密
C. 不可逆加密
D. 以上都是

正确答案： **A**

9.如果有6个成员组成的团体希望互相通信，那么在在基于密钥中心的对称密钥分发结构中，需要人工分发KEK的数量为（）。

A. 5
B. 6
C. 9
D. 15

正确答案： **B**

10.不属于公钥密码体制的是（ ）。

A. ECC
B. RSA
C. ElGamal
D. DES

正确答案： **D**

11.IDEA的分组长度是（ ）bit。

A. 56
B. 64
C. 96
D. 128

正确答案： **B**

12.以下各种加密算法属于古典加密算法的是（ ）。

A. DES算法
B. Caesar算法
C. IDEA算法
D. DSA算法

正确答案： **B**

13.采用SM4算法的CBC-MAC，其输出的标签无法支持哪一个长度?

A. 32
B. 64
C. 128
D. 256

正确答案： **D**

14.后量子公钥密码（PQC）是由NIST于（ ）正式启动 PQC 项目，面向全球征集PQC算法，推动标准化。

A. 2015年12月
B. 2016年12月
C. 2017年12月
D. 2018年12月

正确答案： **B**

15.下列的加密方案基于格理论的是（ ）。

A. ECC
B. RSA
C. AES
D. Regev

正确答案： **D**

16.（ ）加密算法属于公钥密码算法。

A. AES
B. DES
C. IDEA
D. RSA

正确答案： **D**

17.在标准的DES的算法中，其分组的长度为（ ）位。

A. 56
B. 64
C. 112
D. 128

正确答案： **B**

18.SM2算法中的加密算法达到的安全性是（ ）。

A. OW-CPA
B. IND-CPA
C. IND-CCA2
D. NM-CPA

正确答案： **C**

19.SM2算法是（）密码算法?

A. 序列密码
B. 对称密码算法
C. 公钥密码
D. 密码杂凑函数

正确答案： **C**

20.SM3密码杂凑函数的迭代结构是（）。

A. Feistle迭代结构
B. SP结构
C. MD结构
D. Sponge结构

正确答案： **C**

21.我国商用密码算法SM2是一种椭圆曲线公钥密码算法，其推荐的密钥长度为多少?

A. 128bit
B. 256bit
C. 192bit
D. 512bit

正确答案： **B**

22.SM2算法中的密钥交换算法支持（ ）方密钥交换。

A. 2
B. 3
C. 4
D. 多

正确答案： **A**

23.ZUC算法是一个面向字的序列密码，初始向量的长度分别为多少?（）

A. 64比特
B. 128比特
C. 256比特
D. 1024比特

正确答案： **B**

24.SM3密码杂凑算法的压缩函数一共多少轮?

A. 32
B. 64
C. 80
D. 120

正确答案： **B**

25.SM3密码杂凑算法的消息分组长度为多少比特?

A. 256
B. 512
C. 768
D. 1024

正确答案： **B**

26.在SM4加密算法中明文分组长度为（ ）。

A. 64
B. 128
C. 256
D. 512

正确答案： **B**

27.SM2算法是（）国家商用密码算法?

A. 美国
B. 我国
C. 欧盟
D. 俄罗斯

正确答案： **B**

28.SM3密码杂凑算法的压缩函数的输入一共有多少比特?

A. 256
B. 512
C. 768
D. 1024

正确答案： **C**

29.SM3密码杂凑算法的链接变量长度为多少比特?

A. 128
B. 224
C. 256
D. 512

正确答案： **C**

30.SM4分组密码算法，该算法的分组长度为128比特，密钥长度为（ ）。

A. 64比特
B. 128比特
C. 192比特
D. 256比特

正确答案： **B**

31.SM4加密算法是（ ）。

A. 分组密码体制
B. 序列密码体制
C. 置换密码体制
D. 替代密码体制

正确答案： **A**

32.SM2算法与（）基于相同数学结构设计?

A. SM4
B. SM9
C. SM1
D. SM3

正确答案： **B**

33.ZUC算法是一个面向字的序列密码，密钥长度和初始向量的长度分别为多少？（）

A. 64比特
B. 128比特
C. 256比特
D. 1024比特

正确答案： **B**

34.祖冲之（ZUC）序列密码主算法一次输出的密钥长度为多少？（）

A. 32比特
B. 64比特
C. 128比特
D. 256比特

正确答案： **A**

35.我国商用分组密码算法SM4中使用的S盒的输入是多少位？（）

A. 4位
B. 6位
C. 8位
D. 16位

正确答案： **C**

36.GM/T 0006《密码应用标识规范》中的标识符采用 ( ) 位无符号整数类型。

A. 8
B. 16
C. 32
D. 64

正确答案： **C**

37.GM/T 0015《基于SM2密码算法的数字证书格式规范》中，颁发者Issuer中AttributeValue部分首选的编码类型是（ ）。

A. PrintableString
B. TeletexString
C. BMPString
D. UTF8String

正确答案： **D**

38.GM/T 0010《SM2密码算法加密签名消息语法规范》中私钥表达是一个（ ）。

A. CHOICE
B. SEQUENCE
C. OBJECT IDENTFIFIER
D. INTEGER

正确答案： **B**

39.GM/T 0035《射频识别系统密码应用技术要求》第3部分，电子标签对读写器的身份鉴别出现在哪个级别以上（ ）。

A. 1
B. 2
C. 3
D. 4

正确答案： **C**

40.国家支持社会团体、企业利用自主创新技术制定（）国家标准、行业标准相关技术要求的商用密码团体标准、企业标准。

A. 低于
B. 等于
C. 高于
D. 相当于

正确答案： **C**

多选题

1.认证协议是具有认证功能的一类密码协议，可用干实现身份认证和消息源确认两大目标。从参与者的角度来看，认证协议可分为（）

A. 单向认证
B. 双向认证
C. 多向认证
D. 混合认证

正确答案： **ABD**

2.下列是属于基于PKI的组密钥协商协议的是（　）。

A. GDH协议
B. STR协议
C. BD协议
D. TGDH协议

正确答案：**ABCD**

3.SEAL算法本身通过（　）次迭代来改变（　）个内部寄存器的值，每个迭代包括（　）轮

A. 4
B. 8
C. 32
D. 64

正确答案：**ABD**

4.对于线性同余码，若加密映射函数为：y=(ax+b）mod26,那么下列的对a、b的赋值选项中,哪些赋值是错误的（）。

A. a=5 b=28
B. a=13 b=6
C. a=6 b=13
D. a=7 b=13

正确答案：**ABC**

5.对称密码体制的优点是（ ）。

A. 加密速度快
B. 适合批量加密数据
C. 可用于签名
D. 可解决密钥分配、管理问题

正确答案：**AB**

6.对于一次同余式33x≡22 mod 77,求其解，下列哪些结果是正确的解（　）

A. 3，10,17，24
B. 31,38,45,52
C. 59,66,73
D. 3,10,45,50

正确答案：**ABC**

7.SM3密码杂凑算法的运算中哪些起到扩散的作用?

A. 循环移位
B. P置换
C. 模加
D. 布尔函数

正确答案： **AB**

8.SM3密码杂凑算法的运算中哪些起到混淆的作用?

A. 循环移位
B. P置换
C. 模加
D. 布尔函数

正确答案： **CD**

9.SM2的安全特性主要体现在哪些方面（ ）?

A. 算法具备单向性
B. 密文不可区分性
C. 密文具有抗碰撞性
D. 密文具有不可延展性

正确答案： **ABD**

10.SM2公钥加密算法可以抵抗哪些攻击?

A. 唯密文攻击
B. 选择明文攻击
C. 选择密文攻击
D. 密钥恢复攻击

正确答案： **ABCD**

11.ZUC算法驱动部分产生的素域上序列的性质包括（ ）。

A. 权位序列平移等价
B. 序列集合模2压缩保熵
C. 所有权位序列周期相同
D. 所有权位序列线性复杂度相同

正确答案： **ABCD**

12.我国SM2公钥密码算法包含哪3个算法（）?

A. 数字签名算法
B. 密钥封装算法
C. 密钥交换协议
D. 公钥加密解密算法

正确答案： **ACD**

13.SM3密码杂凑算法的压缩函数的结构和哪些算法相同?

A. MD5
B. RIPEMD
C. SHA-1
D. SHA-256

正确答案： **ACD**

14.以ZUC算法为核心，成为3GPP LTE标准的算法为（ ）。

A. 128EEA-3
B. 128EIA-3
C. 128UEA-3
D. 128UIA-3

正确答案： **AB**

15.SM2公钥加密算法的加密函数涉及到哪些运算?

A. 随机数生成
B. 杂凑值计算
C. 椭圆曲线点乘
D. 伪随机比特序列生成

正确答案： **ABCD**

16.GM/T 0021《动态口令密码应用技术规范》动态口令系统中动态令牌负责（ ）动态口令。

A. 产生
B. 显示
C. 比对
D. 验证

正确答案： **AB**

17.2004年8月28日，十届人大常委会第十一次会议审议通过了《中华人民共和国电子签名法》，确立了电子签名的法律效力。明确规定“可靠的电子签名与手写签名或者盖章具有同等的法律效力”，为我国信息化建设提供了重要的法律制度保障。下列说法正确的是（ ）。

A. 具有安全可靠性和经济实用性的电子签名实现技术的核心是密码技术
B. 在电子签名应用中，通常采用对称密钥的密码体制
C. 我国《电子签名法》明确规定，开展电子认证服务必须事先取得国家密码管理机构同意使用的证明文件
D. 网络环境中，电子签名认证证书作为"网上身份证"来确认相互的身份

正确答案： **ACD**

18.GB/T 33560-2017《信息安全技术 密码应用标识规范》中，包括以下哪些密钥分类标识？（ ）

A. 主密钥
B. 设备密钥
C. 用户密钥
D. 密钥加密密钥

正确答案： **ABCD**

19.GB/T 33560-2017《信息安全技术 密码应用标识规范》中，包括以下哪些密钥操作标识？（ ）

A. 密钥生成
B. 密钥分发
C. 密钥导入
D. 密钥销毁

正确答案： **ABCD**

20.GM/Z 4001《密码术语》中，密钥全生命周期包括（ ）等。

A. 密钥产生
B. 密钥存储
C. 密钥更新
D. 密钥分量

正确答案： **ABC**

判断题

1.AES 可以抵抗包括差分攻击、线性攻击等已知的各种攻击手段， 且在软硬件实现速度、内存要求方面都具有很好的性质。 ()

- 正确
- 错误

答案: **正确**

2.X.509签名证书中，signatureAlgorithm域包含了该证书对应私钥签名时所使用的的密码算法标识符。

- 正确
- 错误

答案: **错误**

3.VPN不是物理上真正的专用网络，但却能够实现物理专用网络的功能。（ ）

- 正确
- 错误

答案: **正确**

4.VPN只能使用拨号连接。（ ）

- 正确
- 错误

答案: **错误**

5.HASH函数不可以用于完整性保护。

- 正确
- 错误

答案: **错误**

6.安全多方计算是分布式密码学的理论基础，也是分布式计算研究的一个基本问题。

- 正确
- 错误

答案: **正确**

7.SM3密码杂凑算法的字长为16比特。

- 正确
- 错误

答案: **错误**

8.SM3密码杂凑算法在2016年被批准成为国家标准算法。

- 正确
- 错误

答案: **正确**

9.SM3密码杂凑算法不是单向函数。

- 正确
- 错误

答案: **错误**

10.SM3密码杂凑算法的消息分组长度是可变的。

- 正确
- 错误

答案: **错误**

11.生日攻击是一种密码学攻击手段，基于概率论中生日问题的数学原理。SM3密码杂凑算法可以抵抗生日攻击。

- 正确
- 错误

答案: **正确**

12.SM3密码杂凑算法和SHA-256的结构相同。

- 正确
- 错误

答案: **正确**

13.SM3密码杂凑算法在2012年被批准成为行业标准算法。

- 正确
- 错误

答案: **正确**

14.SM3密码杂凑算法中的P置换是线性运算。

- 正确
- 错误

答案: **正确**

15.SM9密码算法的用户私钥由KGC通过随机数发生器产生。

- 正确
- 错误

答案: **错误**

16.国务院商务主管部门、国家密码管理部门依法对涉及国家安全、社会公共利益且具有加密保护功能的商用密码实施进口许可，对涉及国家安全、社会公共利益或者中国承担国际义务的商用密码实施出口管制。（ ）

- 正确
- 错误

答案: **正确**

17.国家支持社会团体、企业利用自主创新技术制定高于国家标准、行业标准相关技术要求的商用密码团体标准、企业标准。（ ）

- 正确
- 错误

答案: **正确**

18.GM/T 0009《SM2密码算法使用规范》中，SM2签名过程和SM2密钥协商过程中都使用了Z值。

- 正确
- 错误

答案: **正确**

19.机密信息是重要的国家秘密，泄露会使国家安全和利益遭受严重的损害。（ ）

- 正确
- 错误

答案: **正确**

20.在我国，行政机关可在法律允许的范围内，利用行政手段强制转让商用密码技术。（ ）

- 正确
- 错误

答案: **错误**