**A**

1、1976 年，提出公开密码系统的美国学者是( )

A、Bauer 和 Hill B、Diffie 和 Hellman C 、Diffie 和 Bauer D、Hill 和 Hellman

2、 DES 算法中扩展运算 E 的功能是

A、对 16 位的数据组的各位进行选择和排列，产生一个 32 位的结果

B、对 32 位的数据组的各位进行选择和排列，产生一个 48 位的结果

C、对 48 位的数据组的各位进行选择和排列，产生一个 64 位的结果

D、对 56 位的数据组的各位进行选择和排列，产生一个 64 位的结果

3、 KASUMI 算法采用 Feistel 结构，其安全性主要由轮函数提供，轮函数包括

A、 非线性混合函数 FO 和非线性混合函数 F L 组成

B、 非线性混合函数 FO 和线性混合函数 F L 组成

C、 线性混合函数 FO 和线性混合函数 F L 组成

D、 线性混合函数 FO 和非线性混合函数 F L 组成



5、 RSA 密码的安全性基于

A、离散对数问题的困难性 B、子集和问题的困难性

C、大的整数因子分解的困难性 D、线性编码的解码问题的困难性

6、 如果某一个系统利用数字签名的方法来验证用户的口令，则用户的口令是

A、用户保密的解密密钥 Kdi B、用户公开的加密密钥 Kei C、用户与系统共享的秘密密钥 K D、以上说法都不对

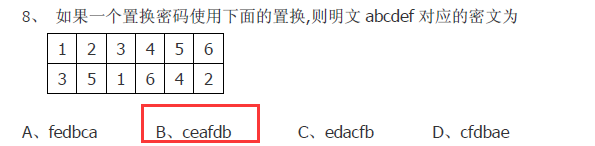
7、 报文的时间性认证是指

A、接收者每收到一份报文后能够确认报文的发送时间

B、接收者每收到一份报文后能够解密出报文的发送时间

C、接收者每收到一份报文后能够确认报文是否保持正确的顺序、有无断漏和重复

D、接收者每收到一份报文后能够确认报文是否按正确的时间发送

9、 RIJNDAEL 算法中的许多运算是按字节定义的，把一个字节看成是

A、整数域上的一个元素 B、有限域 (2 )8 GF 上的一个元素

C、有限域 GF(2) 上的一个元素 D、有限域 (2 ) 16 GF 上的一个元素

10、目前公开密钥密码主要用来进行数字签名，或用于保护传统密码的密钥，而不主要用于数据加

密，主要因为

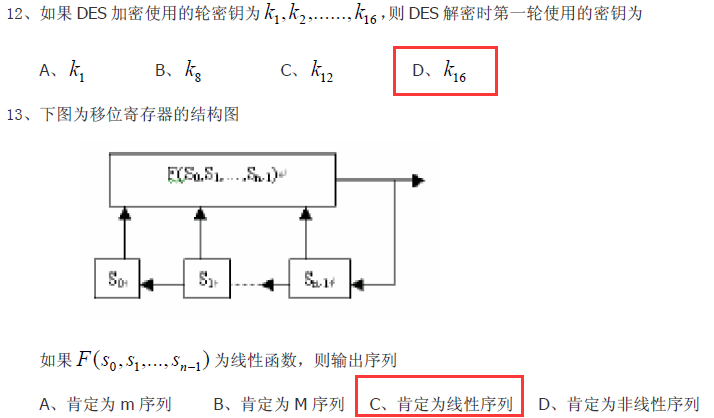
A、公钥密码的密钥太短 B、公钥密码的效率比较低

C、公钥密码的安全性不好 D、公钥密码抗攻击性比较差

11、一个密码系统如果用 E 表示加密运算，D 表示解密运算，M 表示明文，C 表示密文，则下面哪

个式子肯定成立

A、E(E(M))=C B、D(E(M))=M C、D(E(M))=C D、D(D(M))=M

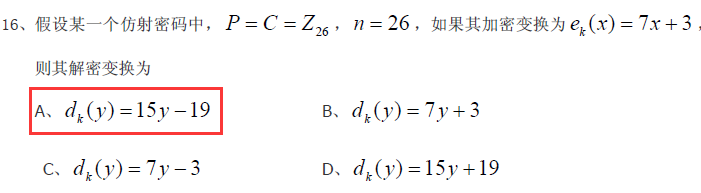


14、在 ElGamal 密码中，如果选择 p =11，生成元 = 2 ，私钥为 x = 8 ，则其公钥为

A、3 B、4 C、5 D、7

15、在 RSA 密码体制中，已知 p = 3,q = 7, 同时选择 e = 5则其私钥 d 为

A、3 B、4 C、5 D、6

17、下面关于签名的说法中，那些是错误的

A、为了安全，不要直接对数据进行签名，而应对数据的 HASH 值签名

B、为了安全，要正确的选择签名算法的参数

C、为了安全，应采用先签名后加密的方案

D、为了安全，应采用先加密后签名的方案

18、下面的那种攻击不属于主动攻击

A、窃听 B、中断 C、篡改 D、伪造

19、把明文中的字母重新排列，字母本身不变，但位置改变了这样编成的密码称为

A、代替密码 B、置换密码 C 代数密码 D 仿射密码

20、KMC 或 KDC 主要负责

A、密钥的产生 B、密钥的分配 C、密钥的销毁 D、密钥的产生和分配

**B**

1、 l998 年 8 月 20 日，美国国家标准技术研究所(NlST)召开了第一次 AES 候选会议 同时公布的

符合基本要求的候选算法有( ) A 5 个 B 6 个 C、10 个 D、l5 个

2、 AES 算法中的状态可表为一个二维数组，如果明文长度为 128 比特，则明文状态为

A、4 行 4 列 B、4 行 6 列 C、4 行 8 列 D、4 行 10 列

3、 设一个公开密钥密码的加密运算为 E ，解密运算为 D ，加密密钥为 Ke ，解密密钥为 Kd ， M 为明文消息，如果要确保数据的真实性，则发送方要发送的密文为



4、 如果 hash 函数的函数值为 64 位，则对其进行生日攻击的代价为



5、 如果用 DES 算法实现一次性口令，系统产生的随机数为 R，并加密 R 得到 E(R,K)，然后将 E(R,K) k 为用户与系统之间共享的秘密密钥 发送给用户，则用户的口令为

A、E(R,k)+1 B、E(D(E(R,k),k),k) C、D(E(R,K),K)+1 D、E(D(E(R,K),K)+1,K)

6、 著名的 Kerckhoff 原则是指

A、系统的保密性不但依赖于对加密体制或算法的保密，而且依赖于密钥

B、系统的保密性不依赖于对加密体制或算法的保密，而依赖于密钥

C、系统的保密性既不依赖于对加密体制或算法的保密，也不依赖于密钥

D、系统的保密性只与其使用的安全算法的复杂性有关

7、 下面那种密码可以抵抗频率分析攻击

A、置换密码 B、仿射密码 C、多名代替密码 D、加法密码

8、 一个数字签名体制都要包括

A、加密和解密两个方面 B、加密和认证两个方面

C、施加签名和验证签名两个方面 D、认证和身份识别两个方面

9、 《保密系统的通信理论》这篇论文把密码学置于坚实的数学基础之上，标志着密码学作为一

门学科的形成，该论文的作者是

A、香农 B、图灵 C、布尔 D、W. Diffie

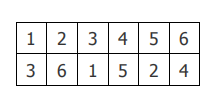
10、下面关于 AES 算法的叙述，那一个是正确的 ( )

A、AES 算法是用 56 比特的密钥加密 64 比特的明文得到 64 比特的密文

B、AES 算法属于非对称密码算法

C、AES 是一个数据块长度和密钥长度可分别为 128 位、192 位或 256 位的分组密码算法

D、AES 是一个数据块长度和密钥长度可分别为 64 位或 128 位的分组密码算法

11、如果一个置换密码系统使用下面的置换 则其逆置换为 A B、 C、 D、

12、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

13、如果签名者为 A，对 RSA 数字签名的一般攻击方法为

A、攻击者随意选择一个Y ，计算 X Y n e = ( ) mod ，则 X 是 A 对Y 的一个有效的签名

B、攻击者随意选择一个Y ，计算 X Y n e = ( ) mod ，则Y 是 A 对 X 的一个有效的签名

C、攻击者随意选择一个Y ，计算 X Y n d = ( ) mod ，则 X 是 A 对Y 的一个有效的签名

D、攻击者随意选择一个Y ，计算 X Y n d = ( ) mod ，则Y 是 A 对 X 的一个有效的签名

14、对于一个给定的散列函数 H，其单向性是指

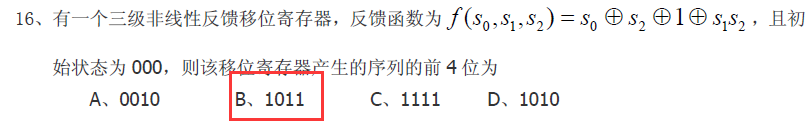
A、对于给定的 hash 码 h，找到满足 H(x)=h 的 x 在计算上是不可行的

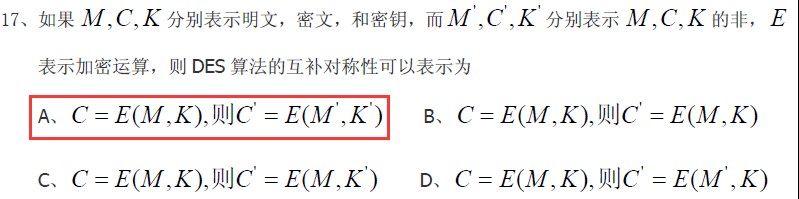
B、对于给定的分组 x，找到满足 y x 且 H(x)=H(y)的 y 在计算上是不可行的

C、找到任何满足 H(x)=H(y)的偶对(x，y)在计算上是不可行的

D、以上说法都不对

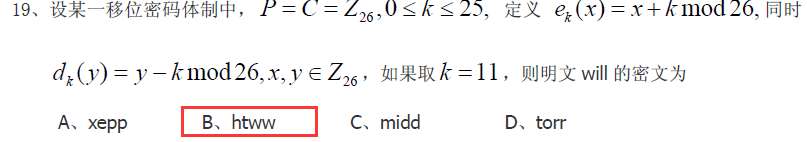
15、安全 hash 算法(SHA)输出报文摘要的长度为 A、120 B、128 C、144 D、160





18、在不可否认签名中，如果签名者不执行否认协议，则表明

A、签名是假的 B、签名是真实的 C、无法判断真假 D、该签名无效



20、下面关于站点认证的说法中，错误的是

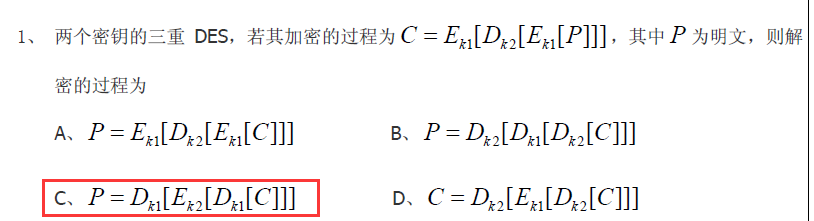
A、站点认证是要认证通信是否在意定的两个站点之间进行

B、站点认证是通过验证加密的数据能否成功的在两个站点之间进行传送来实现

C、站点认证只能用对称密钥密码进行

D、站点认证即可以用对称密钥密码进行，也可以用公开密钥密码进行

**C**



2、 IDEA 算法中关键非线性部件是乘/加 MA 单元，它的主要功能是

A、混淆 B、扩散 C、迭代 D、以上答案都不对

3、 第三代移动通信国际组织(3GPP)规定了两个新的算法 f8 和 f9 作为标准，其中 f9 主要用来

( ) A、加密 B、认证 C、密钥分配 D、身份识别

4、 认证主要用来

A、确保数据的保密性

B、确保报文发送者和接收者的真实性以及报文的完整性

C、阻止对手的被动攻击

D、上说法都不对

5、 MD5 报文摘要算法是由 MIT 的 Ron Rivest 提出，其输出长度为

A、64 位 B、128 位 C、160 位 D、192 位

6、 MD5 算法报文填充的目的是

A、使报文长度与 448 模 512 同余 B、使报文长度为 512 的整数倍

C、使报文长度为 1024 的整数倍 D、使报文长度与 448 模 1024 同余

7、 Diffe-Hellman 密钥分配方案的数学基础是

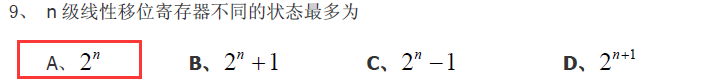
A、离散对数问题的困难性 B、子集和问题的困难性

C、大的整数因子分解的困难性 D、线性编码的解码问题的困难性

8、 CLIPPER 密码芯片使用的密码算法 SKIPJACK 属于分组密码，明文和密文分组长度为 64 位，

密钥长度为

A、56 B、64 C、80 D、128



10、同步序列密码是指

A、密钥序列的产生与密钥有关 B、密钥序列的产生与密钥无关

C、密钥序列的产生与明文有关 D、密钥序列的产生与明文无关

11、如果某系统利用单向函数实现一次性口令，假设用户 A 与用户 B 要进行通信，A 选择随机数 x 并

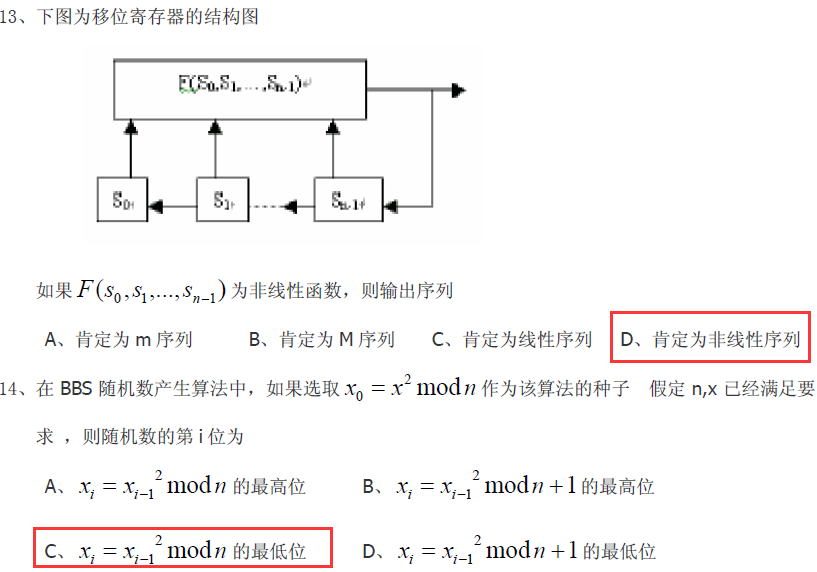
计算y0=fn (x)，A 将 0 y 发给 B，用户 A 第 i 次通信的口令为

A、 yi=fi (x) B、 yi=fn-i(x) C、yi=fn (x) D、 yi=fi+1 (x)

12、在第三代移动通信系统中，以 KASUMI 算法为基础的 9f 算法主要用来产生消息认证码，其中

KASUMI 算法的使用模式为

A、ECB 模式 B、CBC 模式 C、OFB 模式 D、CFB 模式



15、设散列函数 H 的输出为 m 比特，如果 H 的 k 个随机输入中至少有两个产生相同输出的概率大于

0.5,则 k 的值近似为

A、2m/2 B、 2m/4 C、2m/6 D、 2m/8

16、AES 算法中的 S 盒是

A、8 位输入到 6 位输出的非线性变换 B、8 位输入到 8 位输出的非线性变换

C、6 位输入到 6 位输出的非线性变换 D、6 位输入到 8 位输出的非线性变换

17、CLIPPER 密码所使用的密钥中，那一个是在编程过程中产生的

A、FK 族密钥 B、SN 芯片序列号 C、UK 单元密钥 D、Ks 会话密钥

18、下面关于 RSA 算法参数 p，q 的选择，那个是不恰当的

A、p，q 要足够大的素数 B、p 和 q 的差的绝对值要小

C、p 和 q 要为强素数 D、(p-1)和(q-1)的最大公因子要小

19、DES 算法经过了 16 轮迭代，每一轮需要一个轮密钥，轮密钥的长度为

A、32 位 B、48 位 C、56 位 D、64 位

20、设散列函数 H 的输出为 m 比特，如果 H 的 k 个随机输入中至少有两个产生相同输出的概率

大于 0.5,则 k 的值近似为

A、2m/2 B、 2m/4 C、2m/6 D、 2m/8