密码学原理 模拟试题(B)

一、单项选择题(每小题 1 分，共 20 分).

1、 l998 年 8 月 20 日，美国国家标准技术研究所(NIST)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 K_e，解密密钥为 K_d，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

A、$E(M,K_e)$ B、$D(M,k_d)$ C、$E(M,K_d)$ D、$D(M,k_e)$

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

A、2^{16} B、2^{32} C、2^{48} D、2^{64}

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

1	2	3	4	5	6
3	5	1	6	4	2

则其逆置换为

A

1	2	3	4	5	6
3	5	1	6	4	2

B、

1	2	3	4	5	6
3	6	1	5	2	4

C、

1	2	3	4	5	6
1	2	3	4	5	6

D、

1	2	3	4	5	6
2	4	1	6	5	3

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 $X=(Y)^e \bmod n$，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 $X=(Y)^e \bmod n$，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 $X=(Y)^d \bmod n$，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 $X=(Y)^d \bmod n$，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 $y \neq x$ 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

16、有一个三级非线性反馈移位寄存器，反馈函数为 $f(s_0,s_1,s_2)=s_0 \oplus s_2 \oplus 1 \oplus s_1 s_2$，且初始状态为 000，则该移位寄存器产生的序列的前 4 位为

A、0010 B、1011 C、1111 D、1010

17、如果 M,C,K 分别表示明文，密文，和密钥，而 M',C',K' 分别表示 M,C,K 的非，E 表示加密运算，则 DES 算法的互补对称性可以表示为

A、$C=E(M,K),则C'=E(M',K')$　　B、$C=E(M,K),则C'=E(M,K)$

C、$C=E(M,K),则C'=E(M,K')$　　D、$C=E(M,K),则C'=E(M',K)$

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

19、设某一移位密码体制中，$P=C=Z_{26},0\le k\le 25,$ 定义 $e_k(x)=x+k \bmod 26,$ 同时 $d_k(y)=y-k \bmod 26,x,y\in Z_{26}$，如果取 $k=11$，则明文 will 的密文为

A、xepp　　B、htww　　C、midd　　D、torr

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

二、多项选择题　错选、多选不得分　每小题 2 分，共 10 分

1、RIJNDAEL 算法中的轮函数由下面的那些运算部件组成　abcd

A、行移位　　B、字节代换　　C、列混合　　D、密钥加

2、链接技术是一种掩盖明文数据模式的有效方法，下面关于链接技术正确的说法是　abd

A、 链接是算法的当前输出不仅与当前的输入和密钥有关，而且还与以前的输入与输出有关

B、 采用链接技术，即使明文和密钥相同，所产生的密文也可能不相同

C、 采用链接技术，如果明文和密钥相同，所产生的密文也一定不相同

D、 会产生错误传播

3、公钥密码体制的基本思想包括　acd

A、 将传统密码的密钥一分为二，分为加密密钥 k_e 和解密密钥 k_d

B、 k_e 由加密方确定，k_d 由解密方确定

C、 由加密密钥 k_e 推出解密密钥 k_d 在计算上是不可行的

D、 k_e 公开，k_d 保密

4、身份识别对确保系统的安全是极其重要的，下面那些方法可以用来进行用户身份认证　acd

A、 用户知道什么　　B、用户能做什么　　C、用户拥有什么　　D、用户的生理特征

5、DES 算法的 S 盒满足下面的那些准则　abd

A、 输出不是输入的线性和仿射函数

B、 任意改变输入中的 1 位，输出中至少有 2 位发生变化

C、 任意改变输入中的 1 位，输出中至少有 3 位发生变化

D、 保持输入中的 1 位不变，其余 5 位变化，输出中的 0 和 1 的个数接近相等

三、判断题　每小题 1 分，共 10 分

1、DES 算法存在弱密钥，但不存在半弱密钥

2、为了序列密码的安全，应使用尽可能长的密钥

3、SKIPJACK 算法不是对合运算，所以加密和解密过程不一致

4、如果一个密码，无论密码分析者截获了多少密文和用什么技术方法进行攻击都不能被攻破，则称为是绝对不可破译的

5、对于 CLIPPER 密码算法，如果需要，可经法律部门许可破译密码进行监听

6、Vernam 密码不属于序列密码

7、DES 算法是面向二进制的密码算法，所以可以加解密任何形式的计算机数据

8、Hash 函数要能够用于报文认证，它必须可应用于任意大小的数据块并产生定长的输出

9、M 序列的 0，1 分布及游程分组都是均匀的，而且周期达到最大

10、RIJNDAEL 算法在整体结构上采用的是代替－置换网络构成圈函数，多圈迭代

四、解释概念题　每小题 3 分，共 9 分

1、单钥密码体制　　2、扩散　　3、PKC

五、简答题　每小题 5 分，共 20 分

1、简述密码技术的基本思想　　2、试简述 DES 算法的加密过程

3、简述认证和数字签名的区别　　4、在 DSA 签字算法中，参数 k 泄露会产生什么后果?

六、计算题　每小题 10 分，共 20 分

1、Diffie-Hellman 密钥交换过程中，设大素数 p=11, α=2 是 Z_p 的本原元，用户 U 选择的随机数是 5 用户 V 选择的随机数是 7，试确定 U 和 V 之间共享的密钥

2、在 BBS 随机数产生算法中，选择 p=5, q=7, n=pq=35, 如果取 x=11, 试计算出由该算法生成的序列的前 5 位

七、分析题　11 题　在公钥体制中，每一用户 U 都有自己的公开钥 pk_u 和秘密钥 sk_u　如果任意两个用户 A、B 按以下方式通信，A 发给 B 消息 $(E_{pk_B}(m),ID_A)$，B 收到后，自动向 A 返回消息 $(E_{pk_A}(m),ID_B)$，以使 A 知道 B 确实收到报文 m　问用户 C 怎样通过攻击手段获取报文 m?　假设两个用户有相同的 n

密码学原理 模拟试题(B)参考答案

一、单项选择题(每小题1分，共20分)

DABBD　BCCAC　BDBAD　BABBC

二、多项选择题　错选、多选不得分　每小题 2 分，共 10 分

1、ABCD　　2、ABD　　3、ACD　　4、ACD　　5、ABD

三、判断题　每小题1分，共10分

×√√√√　×√√√√

四、解释概念题　每小题 3 分，共 9 分

复习资料　5　前面部分)；10　1；89

五、简答题　每小题 5 分，共 20 分

复习资料　2；18；75；68

六、计算题　每小题 10 分，共 20 分

1、解　用户 U 计算出 $2^5 \bmod 11 = 10$ 发送给 V，用户 V 计算出 $2^7 \bmod 11 = 7$ 发送给 U，

则 U 可以计算出密钥 $7^5 \bmod 11 = 10$，

V 可以计算出密钥 $10^7 \bmod 11 = 10 \bmod 11 = 10$，

所以双方共享的密钥为 10

2、根据 BBS 随机数产生的算法有

$$x_0 = x^2 \bmod n = 11^2 \bmod 35 = 16$$

所以有　$x_1 = x_0^{\ 2} \bmod n = 16^2 \bmod 35 = 11$　该序列的第一位为 x_1 的最低位 1

$x_2 = x_1^{\ 2} \bmod n = 11^2 \bmod 35 = 16$　该序列的第二位为 x_2 的最低位 0

$x_3 = x_2^{\ 2} \bmod n = 16^2 \bmod 35 = 11$　该序列的第三位为 x_3 的最低位 1

$x_4 = x_3^{\ 2} \bmod n = 11^2 \bmod 35 = 16$　该序列的第四位为 x_4 的最低位 0

$x_5 = x_4^{\ 2} \bmod n = 16^2 \bmod 35 = 11$　该序列的第五位为 x_5 的最低位 1

所以该 BBS 算法产生的前五位为 10101

七、分析题　11 题

解　用户C攻击的过程如下　令 $c_1 = E_{pk_A}(m)$　　$c_2 = E_{pk_B}(m)$

攻击者C可以在信道中截获 c_1 和 c_2　同时由于 pk_A 和 pk_B 是公开的，所以C可以知道　且 pk_A 和 pk_B 是互素的　一般情况都满足），则C使用推广的欧几里得算法可以求出满足 $rpk_A + spk_B = 1$ 的r和s，这两个数一个为负，另一个为正　假设r为负，则用户C可以求出 $c_1^{-1} \bmod n$，然后用下面的式子计算出m

$$(c_1^{-1})^{-r} c_2^{\ s} = m^{rpk_A + spk_B} \bmod n = m \bmod n = m$$