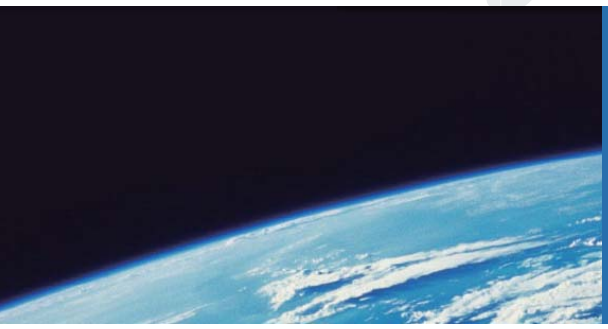
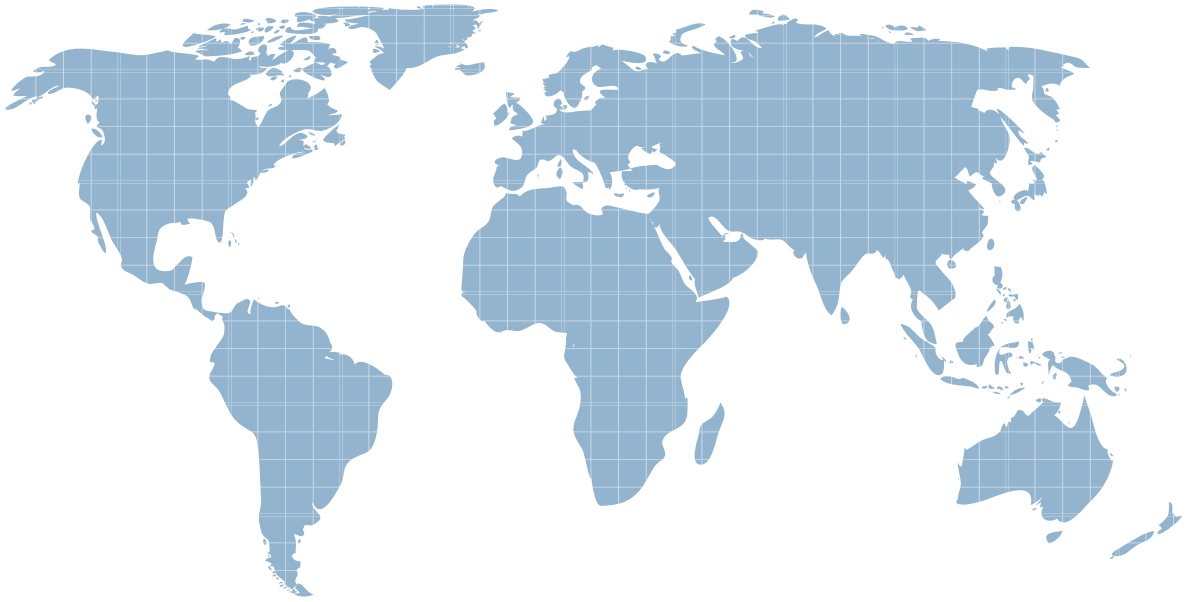


ITTEST

QUESTION & ANSWER

Guías de estudio precisos, Alta tasa de paso!



Ittest ofrece información actualizada de forma gratuita en un año!

http://www.ittest.es/

Exam : **GB0-521**

Title : Building Secure Virtual Private Networks

Version : DEMO

1.下列技术中，可以用于进行密钥协商的是_____。

A.利用密钥分配中心KDC来协商密钥

B.利用Diffie-Hellman密钥交换算法协商密钥

C.利用中间人攻击来协商密钥

D.利用非对称密码算法来协商密钥

答案：abd

2.关于数字签名算法和哈希函数的关系，以下哪个说法是正确的？

A.数字签名算法和哈希函数都是用来进行加密的算法

B.数字签名算法和哈希函数都是用来签名的算法

C.哈希函数产生消息摘要，而数字签名算法对消息摘要进行加密

D.数字签名对消息进行签名，然后由哈希函数产生摘要

答案：c

3.根据国际标准化组织的定义，信息安全的含义主要是指信息的_____。

A.机密性

B.完整性

C.重要性

D.不可否认性

答案：abd

4.以下属于块加密算法的是 _____。

A.SHA-1
B.MD5
C.DES
D.RC4

答案：c

5.如果在IP网络中使用GRE协议来承载IPX 协议，则报文的封装过程为_____。

A.链路层协议 - > GRE - > IP - > IPX。

B.链路层协议 - > IP - > GRE - > IPX。

C.链路层协议 - > GRE - > IPX - > IP。

D.链路层协议 - > IPX - > GRE - > IP。

答案：b

6.L2TP建立隧道时使用的消息有_____。

A.SCCRQ（Session-Control-Connecting-Request）

B.SCCRP（Session-Control-Connecting-Reply）

C.ICRQ（Incoming-Call-Request）

D.ICRP（Incoming-Call-Reply）

答案：ab

7. IKE野蛮模式下，IKE协商发起者发送第一个消息中包含_____。

A.加密算法；

B.散列算法；

C.验证方法；

D.Diffe-Hellman公共值。

答案：abcd

8.在下列哪种密码应用中，使用公钥加密、私钥解密？

A.对称密码

B.非对称密码

C.数字签名

D.DH交换

答案：b

9.下列密码体制中，可以保证绝对安全性的是_____。

A.置换密码

B.代换密码

C.一次一密

D.移位密码

答案：c

10.下列密码体制中，无法保证绝对安全性的是_____。

A.一次一密

B.置换密码

C.代换密码

D.凯撒密码

答案：bcd

11.下列关于加密和解密的说法，正确的是_____。

A.加密和解密是互逆的两个过程，因此加解密的密钥需要相同

B.将密文解码为明文的过程称之为解密，它是加密的相反过程

C.一般来讲，加密比解密要消耗更多的设备性能

D.密码算法的安全性不仅和密钥相关，也和加解密算法相关，因此算法不能公开

答案：b

12.下列关于密钥的说法，不正确的是_____。

A.不管是加密和解密，都要用到密钥

B.密钥和密码算法的关系类似于我们生活中锁和钥匙的关系，密钥就是锁，而密码算法就是钥匙

C.密钥除了被通信双方拥有外，原则上也可以被可信第三方拥有

D.密钥是保证通信安全的根本

答案：bc

13.密码体制是一个使得通信双方能能够进行秘密通信的协议，它是由_____组成的。

A.明文、密文

B.密钥

C.信道

D.加密算法、解密算法

E.通信双方

答案：abd

14.根据加密时对明文消息是否分组，密钥体制可以分为_____。

A.序列密码

B.私钥密码体制

C.公钥密码体制

D.分组密码

答案：ad

15.根据由加密密钥得到解密密钥的算法复杂度差异，密码体制可以分为_____。

A.公钥密码体制

B.私钥密码体制

C.流密码

D.分组密码

答案：ab

16.对于密码体制的描述，正确的说法为_____。

A.从数学上讲，密码体制是一个五元组(P,C,K,E,D)，对于某段明文消息p，存在相应的加密算法e(属于E)和解密算法d(属于D)，使得e(d(p))=p

B.在相同的加密密钥的情况下，相同的明文分组得到相同的密文，而流密码一般不是这样

C.一般意义下，加密密钥和解密密钥是成对的关系

D.在公钥密码体制中，由于密钥的公开性，从加密密钥推导解密密钥非常容易

答案：bc

17.密码分析是衡量密码算法安全性的重要手段，常见的密码分析攻击类型有_____。

A.仅有密文攻击

B.已知明文攻击

C.可选算法攻击

D.可选明文攻击

答案：abd

18.对称密码体制和非对称密码体制的最大区别在于_____。

A.加解密密钥的推导关系不同

B.算法的密钥强度不同

C.算法安全性不同

D.算法实现难易度不同

答案：a

19.以下密码算法中，不属于对称密码算法的是_____。

A.DES
B.AES

C.RSAD.DH密钥交换算法

E.3DES

答案：cd

20.以下密码算法中，属于对称密码算法的是_____。

A.DES
B.RC5
C.IEDA
D.RSA

答案：abc