2022 考题回忆版

填空题（20 分）

1.被动攻击不易被察觉的原因是_____。

2.3A 的构成_____,_____,_____。

3.证书的构成：主体公钥值,_____,_____,_____。

4.IPsec 协议中，提供密钥协商的是_____，提供认证服务的是_____，提供保密性服务的是_____。

5.SET 协议参与的主要实体是_____，_____，_____。

6.对于 WEP 协议升级改进的两个版本,其中国际提出的是_____,国内提出的是_____。

7.会话重用的判断条件是_____。

8.同时实现 AH 和 ESP 需要_____个 SA。

9.在计网和网络安全协议中防火墙实验采用的软件是_____。

10.PKI 中发放证书的是_____，进行资格审查的是_____。

选择题（20 分）

1.关于防火墙提供的服务说法不正确的是（ ）

A.不能阻止那些绕开防火墙的攻击

B.不能防止内部攻击

C.不能防止病毒感染程序或文件的传输

D.不能防止使用端-端加密的过程

2.下面选项中防火墙一般不检测的是（ ）

A.端口号　B.IP 地址　C.协议号　D.载荷

3.SA 三元组内容不包括（ ）

A.安全参数索引　B.目的 IP 地址　C.协议　D.源 IP 地址

4.检查一个证书的内容（即需要检查什么）

5.WEP 协议的相关内容

6.VPN 的适用场景

7.数字签名的使用条件（即采用什么方法）（记不清了，不确定）

8.下列不是 AH 协议提供的服务是（ ）

A.无连接的数据完整性　B.抗重放保护　C.数据源认证　D.保密性服务

9.下列不是 PRF 伪随机数函数起到的作用是（ ）

A.协商主密钥　B.协商预主密钥　C.?　D.?

10.下面说法正确的有（ ）

A．PGP 中的基 64 转换扩展率为 50%，目的是为了兼容性

B．SSL 是基于 UDP 的协议

C．SSL 中服务器端认证是可选择的，客户端认证是必须的

D．PGP 中加密、压缩、签名的先后顺序为:签名--->压缩--->加密

E．?

解答题（60 分）

1.（8 分）（1）什么是数字信封；（2）Alice 向离线的 Bob 发送一个 200M 的文件，设计一个方案使之满足完整性、保密性、?（还有一个忘了）。

2.（6 分）数据完整性保护的基本方法有两种，叙述之，并说明源端的处理办法以及适用场

景**（小测原题）**

3.（5 分）叙述 SNAT 和 DNAT 的作用

4.（4+4=8 分）画出 AH 头标在传输模式和隧道模式下的位置，以及相应的认证范围

5.（6 分）给出非对称加密（不是数字签名）下的一种提供身份认证的办法**（小测原题）**

6.（6 分）双重数字签名的实现方法

7. （3+3=6 分）（整个题目背景是 PGP）（1）怎么保存一个私钥；（2）多个密钥对怎么具体识别是哪一个

8.（3+3+3=9 分）（1）证书的撤销和过期的区别；（2）证书的撤销条件（场景）；（3）如何撤销一个证书

9.（3+3=6 分）（1）密钥派生的好处；（2）如何派生密钥