参考答案 A 卷

〔07172〕信息安全 参考答案.

一 单项选择题答案

1 C
2 A
3 C
4 B
5 C
6 A
7 A
8 A
9 B
10 B
11 B
12 D
13 A
14 A
15 C
16 D
17 A
18 B
19 A
20 A
21 A
22 C
23 A
24 A
25 D
26 C
27 A
28 B
29 A
30 B

二 多项选择题答案

1 ABCDE
2 ABCE
3 AC
4 ABD
5 ACDE
6 ABCDE
7 ABCDE
8 ABE
9 ABCE
10 AB

三 名词解释（每小题 3 分，共 12 分）

1 信息

信息就是客观世界中各种事物的变化和特征的最新反映，是客观事物之间联系的表征，也是客观事物状态经过传递后的再现。

2 站点认证

为了确保通信安全，在正式传送报文之前，应首先认证通信是否在双方确定的站点之间进行，这一过程为站点认证。站点认证是通过验证加密的数据是否成功地在两个站点间进行传送来实现的。

3 虚拟专用网

虚拟专用网是指将物理上分布在不同地点的网络通过公用网络连接在逻辑上的虚拟子网，采用认证、访问控制、密码技术等在公用网络上构建专用网络的技术。

4 计算机犯罪

计算机犯罪是指行为人违反国家规定，故意侵入国家事务，国防建设，尖端科学技术等计算机信息系统，或者利用各种技术手段对计算机信息系统的功能及有关数据、应用程序等进行破坏，制作，传播计算机病毒，影响计算机系统正常运行且造成严重后果的行为。

简答题 （每小题 5 分，共 20 分）

1 什么是对称密码体制，其特点包括哪些

答

对称密码体制是指所用的解密算法就是加密算法的逆运算，加密密钥就是解密密钥这样一类加密体制。他通常用来加密带有大量数据的报文和文卷通信的信息，因为这个两种通信需要告诉加密算法。 3 分

该体制的特点是：在秘密密钥密码体制中，发送者和接收者之间的密钥必须安全传送，而双方用户通信所用的秘密密钥必须妥善保管。 2 分

2 DES 的 IP 与 IP^{-1} 作用是什么？

答

初始置换的作用是对输入进行预白化，达到消除明文的格式和固定输入的目的。2 分

逆初始置换的作用是对输出进行后白化，达到消除密文格式和可能的密钥泄露的目的。2 分

白化就是对输入进行白噪声化处理，立即高斯化处理，使得结果呈现白噪声特征，对输入进行白化叫做预白化，对输出进行白化叫做后白化 1 分

3 证书存档的目的有哪些？

答

一、 保存证书中请者的原始信息以及证书的有关信息（如生成，使用，到期无效，废除等），以供日后核查； 2 分

二、 保证在证书无效或被废除后，仍能验证在其有效期内由其对应私钥所进行的数字签名，即所谓的可追溯性，这对于许多商务活动是十分必要的。因此证书存档是 CA 的一项重要职责。 3 分

4 简述今后入侵检测技术可能的发展方向

答