**2017年信息安全工程师考试下午试题加答案（四）**

新开的**信息安全工程师考试**分属该考试“信息系统”专业，位处中级资格。大家在找试题做练习的时候是否苦恼没有资源？希赛软考学院为大家整理了一些下午试题的练习，供大家参考，希望能有所帮助。

阅读下列说明，回答问题1至问题4，将解答写在答题纸的对应栏内。

   【说明】

   用户的身份认证是许多应用系统的第一道防线、身份识别对确保系统和数据的安全保密及其重要，以下过程给出了实现用户B对用户A身份的认证过程。

   1.B –> B：A

   2.B –> A：{B，Nb}pk（A）

   3.A –> B：b（Nb）

   此处A和B是认证实体，Nb是一个随机值，pk（A）表示实体A的公钥、{B，Nb}pk（A）表示用A的公钥对消息BNb进行加密处理，b（Nb）表示用哈希算法h对Nb计算哈希值。

   【问题1】（5分）

   认证和加密有哪些区别？

  【问题2】（6分）

   （1）包含在消息2中的“Nb”起什么作用？

   （2）“Nb”的选择应满足什么条件？

   【问题3】（3分）

   为什么消息3中的Nb要计算哈希值？

   【问题4】（4分）

   上述协议存在什么安全缺陷？请给出相应的解决思路。

**参考答案**

   1.加密是对数据加密，认证是对数据加密的同时保证数据的完整性，还可以还来认证身份

   2.（1）是b的摘要，用于核对完整性（2）不能在其他报文推出一样的nb,不能从nb推出源数据

   3.要和发送来的摘要做对比以确保数据传送时违背修改等

   4.没有验证b的身份b可以用自己的私钥加密自己发送给a

阅读下列说明和图，回答问题1至问题3，将解答填入答题纸的对应栏内。

   【说明】

   研究密码编码的科学称为密码编码学，研究密码破译的科学称为密码分析学，密码编码学和密码分析学共同组成密码学。密码学作为信息安全的关键技术，在信息安全领域有着广泛的应用。

   【问题1】（9分）

   密码学的安全目标至少包括哪三个方面？具体内涵是什么？

   【问题2】（3分）

   对下列违规安全事件，指出各个事件分别违反了安全目标中的哪些项？

   （1）小明抄袭了小丽的家庭作业。

   （2）小明私自修改了自己的成绩。

   （3）小李窃取了小刘的学位证号码、登录口令信息、并通过学位信息系统更改了小刘的学位信息记录和登陆口令，将系统中小刘的学位信息用一份伪造的信息替代，造成小刘无法访问学位信息系统。

   【问题3】（3分）

   现代密码体制的安全性通常取决于密钥的安全，为了保证密钥的安全，密钥管理包括哪些技术问题？

   【问题4】（5分）

   在图1-1给出的加密过程中，Mi，i=1，2，…，n表示明文分组，Ci，i=1,2，…，n表示密文分组，Z表示初始序列，K表示密钥，E表示分组加密过程。该分组加密过程属于哪种工作模式？这种分组密码的工作模式有什么缺点？

**参考答案**

   1，保密性，完整性，可用性。

   保密性：非授权用户不能访问未授权的信息。

   完整性：信息的完整性不被破坏和篡改。

   可用性：授权用户可以随时使用信息。

   2，（1）保密性（2）完整性（3）保密性，完整性，可用性

   3，密钥的有效周期，算法管理，数字认证技术。

   4，cbc工作模式、容易被破解，异或相加