自测练习一参考答案

判断正误题

① （错）绝大多数基于网络的对称加密应用程序使用流密码。

② （对） **Feistel**密码结构，基于**1945**年**Shannon**的建议，是目前许多重要的对称分组密码使用的结构。

③ （错）数据加密标准**DES**使用的是**56**位分组和**64**位密钥。

④ （对）使用较小分组尺寸的理想分组密码的一个问题是，它容易受到明文统计分析的影响。

⑤ （对）如果位流生成器是密钥控制算法，则两个用户只需要共享生成密钥，然后每个用户都可以生成密钥流。

判断正误题

⑥ （错）在所有其他条件相同的情况下，分组较小的分组密码具有较大的安全性。

⑦ （错）混淆试图使明文和密文之间的统计关系尽可能复杂，以阻止试图推断出密钥

⑧ （错） **AES采用Feistel结构。**

⑨ （对）可以使用密码反馈、输出反馈和计数器模式将分组密码转换为流密码。

选择题

⑩ _ D_____密码是一次对数字数据流进行一位或一字节加密的密码。

A. 乘积

B. 分组

C. 密钥

D. 流

选择题

⑪____B_____密码是将明文分组作为一个整体来处理，并用于产生等长的密文分组的密码。

A. 乘积

B. 分组

C. 密钥

D. 流

选择题

⑫Feistel密码的轮数越多，进行密码分析就越（　D　）。

A. 更容易

B. 难度更小

C. 同样困难

D. 更难

选择题

⑬Feistel提出，我们可以通过使用___D_____密码的概念来近似理想分组密码，即按顺序执行两个或多个简单密码，从而使最终的密码强度大于任何组成密码。

A. 线性的

B. 置换

C. 差分的

D. 乘积

选择题

⑭对明文元素序列的____A___变换，这意味着序列中没有添加、删除或替换元素，而是改变了元素在序列中出现的顺序。

A. 置换

B. 扩散

C. 流

D. 代替

选择题

⑮三重DES使用___D_____级的DES算法，总共使用两个或三个不同的密钥。

A. 九

B. 六

C. 十二

D. 三

选择题

⑯这两个____B_____都产生独立于明文和密文的输出。这使得它们成为流密码的自然候选者，流密码通过XOR一次加密一个完整分组的明文。

A. CBC和ECB

B. OFB和CTR

C. ECB和OFB

D. CTR和CBC

选择题

⑰（A ）最显著的特点是，如果相同的b位明文块在消息中出现多次，它总是产生相同的密文。

A. ECB

B. CTR

C. CBC

D. CFB

选择题

⑱___A____指以给定格式获取明文并以相同格式生成密文的任何加密技术。

A. format-preserving encryption (FPE)
B. Cipher Feedback (CFB)
C. electronic codebook mode (ECB)
D. Cipher Block Chaining (CBC)

选择题

⑲_____A__是明文或密钥的小变化都会使密文产生大的变化。

A. 雪崩效应

B. 密钥扩展

C. 辅助交换

D. Rcon

选择题

⑳在AES加密过程的一般结构中，加密和解密算法处理的分组长度是_____A____。

A. 128位

B. 64位

C. 256位

D. 32位