

主管  
领导  
审核  
签字

密码学基础（A）试题

考试时间：120 分钟      试卷满分：100 分

题号	一	二	三	四	五	六	总分
得分							
阅卷人							

注：本试卷为回忆版，在浏览本试卷前，请先阅读最后一页的备注。

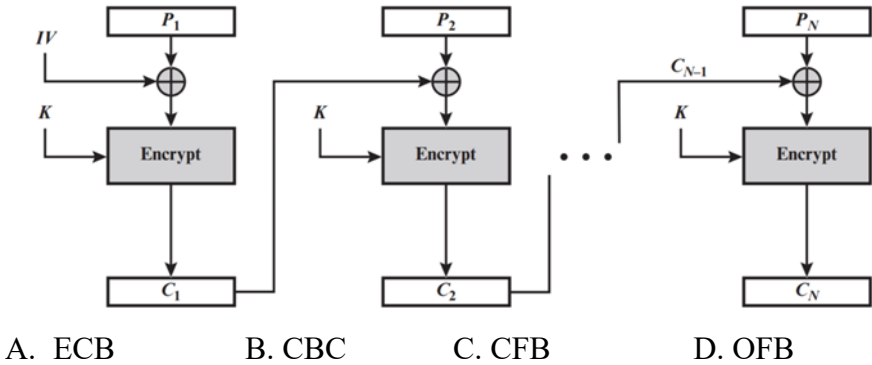
姓名

学号

班号

学院

- 一、选择题（每小题 1 分，共 15 小题，满分 15 分，每小题中给出的四个选项中只有一个是符合题目要求的，把所选项的字母填在题后的括号内）
1. 一个完整的密码体制，不包括\_\_\_\_\_要素。 ( )
- A. 明文空间    B. 密文空间    C. 数字签名    D. 密钥空间
2. 2000 年 10 月 2 日，NIST 正式宣布将\_\_\_\_\_候选算法作为高级数据加密标准，该算法是由两位比利时密码专家研究所得。 ( )
- A. MARS    B. Rijndael    C. Twofish    D. Bluefish
3. 根据所依据的数学难题，除了\_\_\_\_\_以外，公钥密码体制可以分为以下几类。 ( )
- A. 模幂运算问题    B. 大整数因子分解问题
- C. 离散对数问题    D. 椭圆曲线离散对数问题
4. 被公认为在给定密钥长度下最安全的加密算法是 ( )
- A. AES    B. RSA    C. ElGamal    D. 椭圆曲线加密算法
5. 下图中的分组密码操作模式为 ( )



- 
6. 会暴露明文数据的格式和统计特性的分组密码操作模式为 ( )
- A. ECB                      B. CBC                      C. CFB                      D. OFB
7. DH 密钥交换协议中假设密钥交换过程中使用了素数  $p$  及其本原根  $g$ 。用户 A 和用户 B 分别选择密钥  $c$  和  $d$ , 则共享密钥为 ( )
- A.  $g^c$                       B.  $g^d$                       C.  $g^{c+d}$                       D.  $g^{cd}$
8. 哈希函数  $H(x)$  中, 找出任意两个不同的  $x$  和  $x'(x \neq x')$  使得  $H(x) = H(x')$  计算上是不可行的, 这体现出哈希函数的 ( )
- A. 单向性                      B. 抗弱碰撞性                      C. 抗强碰撞性                      D. 抗第二原像性
9. 下列关于 MAC 消息认证码的说法中, 错误的是 ( )
- A. 需要通信双方事先共享密钥                      B. 本身无法抵抗重放攻击
- C. MAC 函数是多对一函数                      D. 具有不可抵赖性
10. 基于一般的离散对数困难性的公钥算法是 ( )
- A. DES                      B. RSA                      C. Elgamal                      D. ECC
11. 公钥密码学是由\_\_\_\_\_最先提出的 ( )
- A. 费马(Fermat)
- B. 欧拉(Euler)
- C. 迪菲(Diffie)和赫尔曼(Hellman)
- D. 李维斯特(Rivest)、沙米尔(Shamir)、艾德曼(Adleman)
12. 代换密码通过\_\_\_\_\_得到密文 ( )
- A. 把明文中的字符适当减少                      B. 把明文中的各字符替换为其他字符
- C. 在明文中的各字符之后增加其他字符                      D. 把明文中的各字符的位置重新排列
13. 实现不可抵赖性的措施是 ( )
- A. 报文鉴别                      B. 数字签名                      C. 完整性技术                      D. 消息认证码
14. 若 Bob 给 Alice 发送一封邮件, 并想让 Alice 确信邮件是由 Bob 发出的, 则 Bob 应该选用 ( )
- A. Alice 的公钥                      B. Alice 的私钥                      C. Bob 的公钥                      D. Bob 的私钥
15. 维吉尼亚密码是 ( )
- A. 置换密码                      B. 单字母单表密码
- C. 单字母多表密码                      D. 多字母密码

## 二、填空题（每空 2 分，满分 30 分）

16. 香农提出了两个密码系统设计的基本原则，分别是混淆和\_\_\_\_\_。
17. 在基本 RSA 数字签名体制中,验证公钥为 $(N, e)$ , 签名私钥为  $d$ , 这里  $ed \equiv 1 \pmod{\phi(N)}$ 。如果消息  $m_1$  的签名为  $t_1$ , 消息  $m_2$  的签名为  $t_2$ , 则消息  $m_1 m_2 \pmod n$  的数字签名为\_\_\_\_\_（用含  $t_1$  和  $t_2$  的式子表示）。
18. CTR\_\_\_\_\_（支持/不支持）预处理和并行处理，\_\_\_\_\_（存在/不存在）错误传播，\_\_\_\_\_（支持/不支持）数据流加密。
19. AES 算法的基本变换有字节变换、\_\_\_\_\_、\_\_\_\_\_、加轮密钥。
20. AES 算法的分组长度比 DES 更大，为\_\_\_\_\_位。
21. 在数字签名体系之中，消息发送方 Alice 使用\_\_\_\_\_（公钥/私钥）对消息进行签名，接收方 Bob 使用\_\_\_\_\_（公钥/私钥）对签名进行验证。
22. 分组密码的 5 个工作模式为电子密码本模式、\_\_\_\_\_、\_\_\_\_\_、输出反馈模式、计数器模式。
23. 仿射加密算法之中， $P = C = \mathbf{Z}_{26}$ ,  $n = 26$ ，且加密算法为  $Enc(x) = 7x + 3$ ，加密后结果为  $y$ ，则解密算法为\_\_\_\_\_。
24. 在 RSA 公钥密码体系之中，已知  $p = 3, q = 7, e = 5$ ，则私钥  $d$  为\_\_\_\_\_。
25. 一种置换加密算法如下表所示，则明文 abcdef 加密后的密文为\_\_\_\_\_。

1	2	3	4	5	6
3	5	1	6	4	2

## 三、判断题（每小题 1 分，共 15 小题，满分 15 分，把“√”或“×”填在题后的括号内）

26. RSA 加密算法的安全性基于大数因数分解问题的困难性。（ ）
27. 唯密文攻击指的是在仅知己加密文字（即密文）的情况下进行攻击。（ ）
28. 密码设计的基本原则为混淆和扩散。其中扩散原则指使密文和密钥之间的统计关系变得尽可能复杂。（ ）
29. PRNG 随机数发生器只要 PRNG 算法相同，选取的种子相同,则每次生成的随机数序列也相同。（ ）
30. 采用具备同等机密性的密钥长度的情况下，公钥加密算法通常比对称加密算法快。（ ）
31. 117 的欧拉函数  $\phi(n)$  的值是 89。（ ）
32. 现代密码体制把算法和密钥分开,算法是可以公开的,只需要保证密钥的保密

性。 ( )

33. 公钥签名中, 公钥证书由用户产生, 由证明中心验证。 ( )

34. 采用具备同等机密性的密钥长度的情况下, 椭圆曲线加密安全性比 RSA 加密好。 ( )

35. 公钥加密的公私钥可以对应的一个加密, 另一个解密。 ( )

36. 3DES 密钥长度为 168 比特。 ( )

37. RSA 是一种基于公钥密码体制的优秀加密算法, 1978 年由美国麻省理工学院 (MIT) 提出的, 旨在代替 DES 称为广泛使用的标准。 ( )

38. 缺失

39. 缺失

40. 缺失

#### 四、(共 2 小题, 满分 15 分)

41.

有限域  $GF(2^8)$  上的不可约多项式为  $m(x)=x^8+x^4+x^3+x+1$ , 请计算:

(1)  $(x^7+x^4+x^2+x+1)+(x^6+x+1)$

(2)  $(x^7+x^4+x^2+x+1)\times(x^6+x+1)$

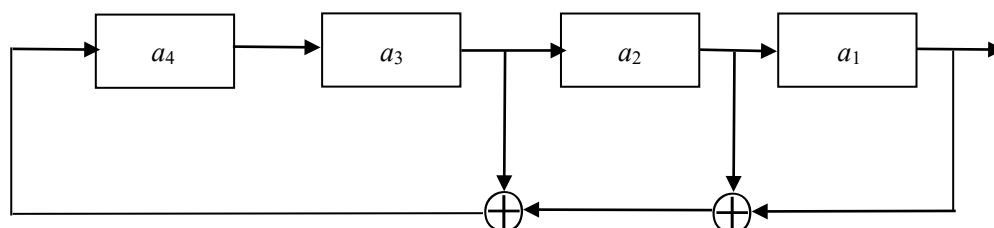
42.

利用费马小定理计算  $8^{1003} \bmod 11$

#### 五、(共 1 小题, 满分 10 分)

43. (10 分)

下图为一个 4 级线性反馈移位寄存器 (LFSR) 的框图, 初始输入为  $(a_1, a_2, a_3, a_4)=(0, 1, 1, 0)$



(1) 请给出  $f(a_1, a_2, a_3, a_4)$  以及特征多项式  $f(x)$

(2) 请给出输出的前 8 位

## 六、(共 1 小题, 满分 15 分)

44. (15 分)

在 RSA 公钥密码体制之中, 选取  $p = 11, q = 13$ , 乘积  $n = 143$ , Alice 的公钥为  $e = 7$

- (1) 计算 Alice 的私钥
- (2) Bob 有一个消息  $m = 7$ , 计算 Bob 使用 Alice 的公钥加密后的密文
- (3) 使用 Alice 的私钥, 写出对 Bob 的加密消息的解密过程和解密结果 (要求使用快速模幂算法)

备注:

- 判断题中第 30、34 题原卷可能没有使用“采用具备同等机密性的密钥长度的情况下”的说法, 而是使用“相同密钥长度”, 本回忆版试卷选用了更严谨的说法, 这应该不是这两道题的考点, 无需在意。
- 选择题部分题目的选项 (如第 4、7、9、13 题) 回忆不全, 这些题已在保证该题大的考点不变的情况下尽可能地还原。
- 作业题中给出了 RSA 算法的流程, 但原卷中并没有给, 在复习过程中一定要把 RSA 算法的流程背下来。
- 原卷中第 16、21 题可以在其他题中找到答案 (记不清第 16 题是不是在第 17 题中找的答案了, 总之是可以找到), 相当于送了 6 分。
- 无法保证选择题和判断题 (尤其是判断题) 的题目顺序与原卷完全一致。
- 判断题有 3 道题回忆不起来。
- 原卷每道大题中的小题的题号都是重新计数的, 本回忆版试卷由于个人喜好没有重新计数。
- 2020 级的学长提到 2020 级的密码学基础期末考试最后一道大题也考到了快速模幂 (原话是“快速幂”, 但应该指的就是快速模幂)。

回忆版试题贡献者:

- 本试卷的题目由本人、自救群的群友 B 和群友 C 共同回忆而成 (顺序不分先后, 下同) 同时附上本人整理的其他回忆版试卷的来源:
  - 2023 秋编译原理期末试题: 本人、群友 B
  - 2022 春大学物理 II (补考) 期末试题: 本人
  - 2021 秋计算机专业导论期末试题: 本人、群友 D
- 具体哪道题是哪位群友回忆出来的这里就不赘述了。

群友 B、C、D 均在自救群中分享了他们回忆的试题, 但本人不确保他们的回忆版试题来源, 若还有其他回忆者因此被遗漏, 抱歉 (该条备注仅是严谨起见, 没有其他含义)