2025-2026 学年南开大学数学科学学院期末测试
近代密码学

命题人：吴亚男　　回忆人：xzqbear　　考试用时：100 分钟

部分题目实际数字有出入，请谨慎参考。

一、 选择题（共 24 分，每题 3 分）

1. 对于密码体制 $\mathcal{S}$，其安全性主要来源于（　）

   A. 加密算法　　B. 解密算法　　C. 密钥　　D. 密文

2. 对于 RSA 体制，Alice 和 Bob 进行通讯，那么在 Alice 进行加密后，应该发送给 Bob 的是（　）

   A. Alice 的公钥　　B. Alice 的私钥　　C. Bob 的公钥　　D. Bob 的私钥

3. Bob 给 Alice 发送数字签名信息，Bob 应该使用什么来进行数字签名？（　）

   A. Alice 的公钥　　B. Alice 的私钥　　C. Bob 的公钥　　D. Bob 的私钥

4. 数字签名的流程当中，在验证签名之前的流程是（　）

   A. 签名　　B. 加密变换　　C. 解密变换　　D. 哈希变换

5. 下列哪个不是公钥密码基于的难解数学问题？（　）

   A. 大整数素因子分解　　B. 离散对数　　C. 模幂运算　　D. 域上的椭圆曲线

6. 如果一个密码体制，攻击者在使用计算资源的情况下无法在合理时间内破解成功，那么称这个密码体制具有什么性质？（　）

   A. 可计算安全　　B. 无条件安全　　C. 可证明安全　　D. 绝对安全

7. 第一个被广泛用于商业数据加密的算法是（　）

   A. AES　　B. DES　　C. IDEA　　D. SM4

8. Vigenere 密码体制是什么类型的密码体制？（　）

   A. 单表古典密码　　B. 多表古典密码　　C. 公钥密码体制　　D. 分组密码体制

二、 计算题（共 50 分）

9. (10 分) 使用 Vigenere 密码，明文为 YOU CAN DO THIS，密文为 ZSM VBR VH ULAL，请计算密钥。

10. (10 分) 现使用 RSA 算法进行加密，已知 $n = 35$ ，公钥为 $e = 5$ ，现在密文为 $c = 7$ ，则：

（1）请求解密钥 d；（2）利用密钥对密文进行解密得到明文；

11. (10 分)

对于密码体制 $\mathcal{S}$ ，如果明文空间 $\mathcal{M} = \{a, b\}$ ，密文空间 $\mathcal{C} = \{1, 2, 3\}$ ，密钥空间 $\mathcal{K} = \{k_1, k_2, k_3\}$，且有概率：

$$\Pr(a) = 0.5, \Pr(b) = 0.5$$

以及

$$\Pr(k_1) = 1/2, \Pr(k_2) = 1/4, \Pr(k_3) = 1/4$$

加密规则如下所示：

$$E_{k_1}(a) = 1, E_{k_2}(a) = 2, E_{k_3}(a) = 3, E_{k_1}(b) = 2, E_{k_2}(b) = 3, E_{k_3}(b) = 1.$$

尝试求解 $H(M), H(C), H(K), H(K \mid C)$.

12. (10 分) 使用 EIGamal 体制时，如果 $p = 29$，选取 $\alpha = 2$ 作为本原元，当 $\beta = 3$ 时，

（1）随机选取整数 $k = 3$ ，请对明文 $m = 17$ 进行加密；

（2）如果对 $m = 17$ 加密得到 $(18, c_2)$ ，尝试求解 k 和 c_2.

13. (10 分)

对于流密码，使用 LFRS 密钥序列生成时，设联系多项式最高次数为 3，那么在 $a_3 = 1$ 时，可能的 LFRS 有四种，请分别写出对应的多项式，并利用其计算 $(a_1, a_2, a_3) = (1, 0, 1)$ 的生成序列，说明周期。

三、 证明题（共 26 分）

14. (13 分)

在 DES 中，如果

$$\mathrm{DES}_k(x) = \mathrm{DES}_k^{-1}(x)$$

即

$$\mathrm{DES}_k(\mathrm{DES}_k(x)) = x$$

则称 k 为自对偶的密钥. 证明下列四个密钥是自对偶的:

- 0101010101010101
- FEFEFEFEFEFEFEFE
- 1F1F1F1F1F1F1F1F
- E0E0E0E0F1F1F1F1

这里我们用十六进制表示密钥.

15. (13 分) 在 RSA 算法当中，对于给定整数 $n = pq$ ，证明：总存在公钥 e ，使得对于任意明文 x 都有 $x^e \equiv x \pmod{n}$.