华中科技大学计算机与科学技术学院 2025~2026 第一学期

“离散数学（二）”期中考试试卷（A 卷）

考试方式 闭卷 考试日期 2025-10-09 考试时长 50 分钟

专业班级 _____ 学 号 _____ 姓 名 _____

题号	1	2	3	4	5	6	7	总分	总分人	核对人
分值	20	10	10	20	10	10	20	100		
得分										

解答内容不得超过装订线

1. 分别计算 2^{100} mod 33 以及 87^{10}mod 101的值。（20 分）

答：$33 = 3 \times 11$，欧拉函数 $\phi(33) = \phi(3) \times \phi(11) = 2 \times 10 = 20$。
$\gcd(2, 33) = 1$, 根据欧拉定理：$2^{20} \equiv 1 \bmod 33$.
故 $2^{100} = (2^{20})^5 \equiv 1^5 = 1 \bmod 33$。

$87^2 \bmod 101 = 95$, $87^4 \bmod 101 = 36$, $87^8 \bmod 101 = 84$
故 $87^{10} \bmod 101 = 1$

2. 解方程组：$x \equiv 2 \pmod 3$，$x \equiv 3 \pmod 5$，$x \equiv 4 \pmod 7$，$x \equiv 5 \pmod 8$。(10 分)

答：$x \equiv 53 \pmod{840}$

3. 用扩展欧几里得算法求 gcd(1248, 858)，并写成线性组合。(20 分)

答：欧几里得算法求得 gcd(1246，858)=78

- 第 1 步：1248 = 1 * 858 + 390
- 第 2 步：858 = 2 *390 + 78（
- 第 3 步：390 = 5 *78 + 0

用扩展欧几里得算法回代得 1248*(-2) + 3 * 858 = 78

4. 用字母 B, A, N, A, N, A 进行排列（字母顺序不同即为不同字符串），请解答以下问题：

(a) 这些字母能形成多少个不同的字符串？(5 分)

(b) 在这些字符串中，有多少个是不以两个相同字母相邻开头的？（5 分）

答：（a）

$$\frac{6!}{3!\cdot 2!\cdot 1!} = \frac{720}{6\cdot 2\cdot 1} = \frac{720}{12} = 60$$

(b) 前两个字符是 AA 的字符串有 12 个，前两个字符是 NN 得字符串有 4 个，即不以两个相同字母相邻开头的字符串数量为 60 – 12 – 4 = 44.

5. (a)使用仿射密码$F(x) = 5x + 2(\mathrm{mod}26)$加密明文 ″CODDE″。(5 分)

(b)对加密后的密文进行解密，恢复明文。（3 分）

(c)使用转置密码，置换函数为$\sigma: 1 \to 3, 2 \to 4, 3 \to 5, 4 \to 2,\ 5 \to 1$对明文 ″CODDE″ 进行加密。（7 分）

答：（a）MURRW

(b) 解密函数为 G(y) = 21(y--2) (mod 26)

(c) EDCOD

6. RSA 与 Diffie-Hellman

(1) RSA: 给定 $p=11$, $q=17$, $e=7$，求私钥d。（5 分）

(2) 使用 RSA 加密消息$m=88$，然后解密回明文。（5 分）

(3) Diffie-Hellman: 给定 $p=23$, $g=5$, $a=6$, $b=13$，求共享密钥k。（5 分）

答：（a）d = 23。$p=11$, $q=17$, $e=7$ 计算 $n=p\times q=11\times 17=187$

则 $\phi(n)=(p-1)(q-1)=10\times 16=160$，求求 d 满足 $e\cdot d\equiv 1(\mathrm{mod}\phi(n))$，即解方程：$7d\equiv 1(\mathrm{mod}160)$。

（b）加密：计算密文 $c=m^e \mathrm{mod}\ n=88^7 \mathrm{mod}\ 187$，c = 11

解密：计算明文 $m=c^d \mathrm{mod}\ n=11^{23} \mathrm{mod}\ 187$，m = 88

（c）Alice 的公开值 $A=g^a \mathrm{mod}\ p=5^6 \mathrm{mod}\ 23$

- $5^2=25\equiv 2(\mathrm{mod}23)$
- $5^4=(5^2)^2=2^2=4(\mathrm{mod}23)$
- $5^6=5^4\times 5^2=4\times 2=8(\mathrm{mod}23)$
- 所以 $A=8$

Bob 的公开值 $B=g^b \mathrm{mod}\ p=5^{13} \mathrm{mod}\ 23$

- $5^2=2$
- $5^4=4$
- $5^8=(5^4)^2=4^2=16(\mathrm{mod}23)$
- $5^{13}=5^8\times 5^4\times 5^1=16\times 4\times 5=320 \mathrm{mod}\ 23$:
  $23\times 13=299$, 余数 $320-299=21$
- 所以 $B=21$

共享密钥 $K=A^b \mathrm{mod}\ p=8^{13} \mathrm{mod}\ 23$ 或 $K=B^a \mathrm{mod}\ p=21^6 \mathrm{mod}\ 2$，K=18

7. 证明：当 p 是质数且 a 和 b 是整数，如果 p|(a*b)，则必有 p|a 或 p|b。(10 分)

证明：如果 gcd(p,a)=1，则根据贝祖定理推理，因为 p|(a*b)且 gcd(p,a)=1，有 p|b；

如果 gcd(p,a)=p，必有 p|a；无论哪种情况结论得证。

根据 gcd(p,b)是为 1 还是为 b，得到类似结论。