《离散数学二》第三次作业

1. ISBN-13有13位数字 a1a2…a13，其中校验位 a13 由同余式 (a1 + a3 +⋯+ a13) + 3(a2 + a4 +⋯+ a12) ≡ 0 (mod 10) 确定。下列两个ISBN-13是否为有效ISBN-13？(a) 978-0-45424-521-1； （b）978-3-16-148410-0 **(10分)**

**参考答案：（a）**(9 + 8 + 4 + 4 + 4 + 2 + 1) + 3(7 + 0 + 5 + 2 + 5 + 1) mod 10 = 2; 无效

**(b)** (9 + 8 + 1 + 1 + 8 + 1 + 0) + 3(7 + 3 + 6 + 4 + 4 + 0) mod 10 = 0; 有效

1. (1) 利用仿射加密函数F(x)=5x+8 mod 26对字符串“HELLO”进行加密，并对该密文进行解密，要求写出具体过程；（2）请证明仿射加密函数F(x)=ax+b mod 26为双射函数，当且仅当gcd(a, 26)=1，这里a,b均为整数. [说明：每个字符对应Z26里一个数字，譬如A对应0，C对应2.]**（20分）**

**参考答案：**

1. 先将每个字母转换为数字（H=7, E=4, L=11, L=11, O=14）。

**加密：**应用加密公式 F(x) = (5x + 8) mod 26 对每个字母进行加密。

以下是加密步骤：

对于 H (7): F(7) = (5\*7 + 8) mod 26 = 43 mod 26 = 17，对应字母 R。

对于 E (4): F(4) = (5\*4 + 8) mod 26 = 28 mod 26 = 2，对应字母 C。

对于 L (11): F(11) = (5\*11 + 8) mod 26 = 63 mod 26 = 11，对应字母 L（这里加密后还是L）。

对于 O (14): F(14)= (5\*14 + 8) mod 26 = 78 mod 26 = 0，对应字母 A。

因此，明文 “HELLO” 被加密为 “RCLLA”。

**解密：**解密需要找到加密函数的逆函数。为了找到逆元，我们需要一个与 a 互质且小于26的数 a-1 mod 26 = 21，因为 (5 \* 21) mod 26 = 105 mod 26 = 1。

解密公式为 x = a-1 \* (y - b) mod 26。

以下是解密步骤：

对于 R (17): x = 21 \* (17 - 8) mod 26 = 21 \* 9 mod 26 = 189 mod 26 = 7，对应字母 H。

对于 C (2): x = 21 \* (2 - 8) mod 26 = 21 \* (-6) mod 26 = -126 mod 26 = 4，对应字母 E。

对于 L (11): x = 21 \* (11 - 8) mod 26 = 21 \* 3 mod 26 = 63 mod 26 = 11，对应字母 L。

对于 A (0): x = 21 \* (0 - 8) mod 26 = 21 \* (-8) mod 26 = -168 mod 26 = 14，对应字母 O。

因此，密文 “RCLLA” 被解密为原始的明文 “HELLO”。

1. **先证明F(x)=ax+b mod 26为双射，则推出gcd(a,26)=1:**

**反证法**：

**假设** gcd(*a*,26)=*d*>1，可得 a=*kd* 和 26=*jd*，其中 *k* 和 *j* 是整数。

**再构造两个不同的输入** x1​ 和 x2​，使得 x1≡x2 mod  j (即 x1​ 和 x2​ 在模 j 下同余)

由于 x1​ 和 x2​ 在模 j 下同余，我们可以写成 x1=x2+lj 对于某个整数 *l*。

现在计算 f(x1) 和 f(x2)：

f(x1)=a(x2+lj)+b mod  26，f(x1)=ax2+alj+b mod  26

因为 a=kd，我们有：

f(x1)=kdx2+kdlj+b mod  26

由于 kd=a 和 jd=26，我们可以将 kdlj 替换为 alj 并简化：

f(x1)=ax2+alj+b mod  26，因为 alj 是 26 的倍数（alj=kdlj=k(26)l=26kl），我们有：

f(x1)=ax2+b mod  26， 这与 f(x2) 相同：f(x2)=ax2+b mod  26

因此，f(x1)≡f(x2) mod  26，即使 x1≠x2。这与 f(x) 是单射的假设相矛盾。

因此假设 gcd(a,26)=d>1 错误。所以，如果 f(x) 是单射的，则 gcd(a,26)=1。

**再证明如果gcd(a,26)=1，则F(x)为双射函数：**

首先，证明 f(x) 是单射：

假设 f(x1)=f(x2)，则 ax1+b≡ax2+b mod  26。简化得到 a(x1−x2)≡0 mod  26。因为 gcd(a,26)=1， a 在模 26 下有逆元。这意味着 x1−x2必须是 26 的倍数，但由于 x1​ 和 x2​ 都在 {0,1,...,25} 范围内，唯一的可能是 x1=x2​。因此，f(x) 是单射。

接下来，证明 f(x) 是满射：

因为 gcd(a,26)=1，存在一个整数 a−1 使得 a\*a−1≡1 mod  26。对于任何 y∈{0,1,...,25}，我们需要找到一个 x 使得 f(x)=y。设 x= a−1 (y−b) mod  26，那么：

f(x)=ax+b≡a(a−1 (y−b))+b≡y−b+b≡y mod  26，因此，对于任何 y，我们都能找到一个对应的 x，使得 f(x)=y。这表明 f(x) 是满射。

1. 使用五个字母为一组的块，以及基于排列 {1, 2, 3, 4, 5} 的转置密码，其中 𝜎(1) = 3, 𝜎(2) = 5, 𝜎(3) = 1, 𝜎(4) = 2, 𝜎(5) = 4，来加密消息 “GRIZZLY BEARS”；再根据该转置函数的逆还原成明文。[说：如果最后一个块不足五个字母，则使用字母 “X” 来填充]。**（10分）**：

**参考答案**：分成3个块，GRIZZ LYBEA RSXXX，则每个块中字符装置后为IZGZR BELAY XXRXS; 转置函数的逆为：𝜎-1(1) = 3, 𝜎-1 (2) = 4, 𝜎-1 (3) = 1, 𝜎-1 (4) = 5, 𝜎-1 (5) = 2，则密文IZGZR BELAY XXRXS解密后为：GRIZZ LYBEA RSXXX.

1. 利用RSA密码系统进行加解密，其中公钥(n,e)=(391,3)；(1)请给出私钥d；(2)对字符串HELLO中各个字符进行加密；(3)对加密后的密文进行解密，从而恢复出明文HELLO。[说明：每个字符对应Z26里一个数字，譬如A对应0，C对应2.] **(20分)**

**参考答案**：(1)n=391=17\*23,则φ(391)=16\*22=352；所以d=3-1 mod 352=235；

1. 先将每个字母转换为数字（H=7, E=4, L=11, L=11, O=14）, 则：

对于 H (7): 7^3 mod 391=343;

对于 E (4): 4^3 mod 391=64;

对于 L (11): 11^3 mod 391=158

对于 O (14): 14^3 mod 391=7

1. 343对应的明文为：343^235 mod 391=7;

64对应的明文为：64^235 mod 391=4

158对应的明文为：158^235 mod 391=11

7对应的明文为：7^235 mod 391=14

1. 描述 Alice 和 Bob 使用 Diffie-Hellman 密钥交换协议生成共享密钥时所遵循的步骤。假设他们使用素数 p = 101，并取 a = 2，(1)在Z101中选择 3,6,9,100四个数来验证a=2是 模101 的原根；（2） Alice 选择私钥k1 = 7，而Bob选择私钥k2 = 9，计算他们各自使用的公钥和共享密钥. **（20分）**

**参考答案：**

1. 硬算，根据费马小定理，2^100 mod 101=1, 2^x mod 100中x从1到99都对应 2到100中某个数，逐个计算，可以分别算出基数为2的9模101的离散对数为38，即 2^38 mod 101=9；基数为2的100模101的离散对数为50，即 2^50 mod 101=100；基数为2的3模101的离散对数为69,即 2^69 mod 101=3; 基数为2的6模101的离散对数为70，即 2^70 mod 101=6.

(2)Alice计算其公钥2^7 mod 101=27；

Bob计算其公钥2^9 mod 101=7；

Alice和Bob各自向对方发送其公钥27 和7；

Alice计算其共享密钥 7^7 mod 101=90;

Bob计算其共享密钥27^9 mod 101=90.

1. 设Alice和Bob利用RSA公钥密码体系进行通信，Alice的公钥: NA=21, eA=5；Bob的公钥NB=39,eB=7，(1)分别计算Alice和Bob的私钥dA和dB；（2）Alice 想要向 Bob 发送数字消息11，以便他知道她发送了该消息，并且只有 Bob可以阅读该消息。假设她签署了该消息，然后使用 Bob 的公钥对其进行加密，她应该向 Bob 发送什么？（3）给出Bob解密Alice所发送的密文过程。**(20分)**

参考答案：(1) dA=5-1 mod φ(21)= 5-1 mod 12=5;

dB=7-1 mod φ(39)= 7-1 mod 24=7;

(2) Alice向Bob发送的明文11并加了其签名的密文为：

EB(DA(11))= EB(11^5 mod 21)= EB(2)=2^7 mod 39=128 mod 39=11;

(3) Bob的解密过程为：

EA(DB(11))= EA(11^7 mod 39)= EA(2)=2^5 mod 21=11