《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

2. (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 Z_{26} 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): $x = 21 * (11 - 8) \bmod 26 = 21 * 3 \bmod 26 = 63 \bmod 26 = 11$，对应字母 L。
对于 A (0): $x = 21 * (0 - 8) \bmod 26 = 21 * (-8) \bmod 26 = -168 \bmod 26 = 14$，对应字母 O。
因此，密文“ RCLLA ”被解密为原始的明文“ HELLO ”。

（2） 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 $x1 \equiv x2 \bmod j$ (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):
$f(x1)=a(x2+lj)+b \bmod 26$，$f(x1)=ax2+alj+b \bmod 26$
因为 a=kd，我们有:
$f(x1)=kdx2+kdlj+b \bmod 26$
由于 kd=a 和 jd=26，我们可以将 kdlj 替换为 alj 并简化:
$f(x1)=ax2+alj+b \bmod 26$，因为 alj 是 26 的倍数（$alj=kdlj=k(26)l=26kl$），我们有:
$f(x1)=ax2+b \bmod 26$， 这与 f(x2) 相同：$f(x2)=ax2+b \bmod 26$
因此，$f(x1) \equiv f(x2) \bmod 26$，即使 $x1 \neq x2$。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 $ax1+b \equiv ax2+b \bmod 26$。简化得到 $a(x1-x2) \equiv 0 \bmod 26$。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 $a*a^{-1} \equiv 1 \bmod 26$。对于任何 $y \in \{0,1,...,25\}$，我们需要找到一个 x 使得 f(x)=y。设 $x= a^{-1}(y-b) \bmod 26$，那么:
$f(x)=ax+b \equiv a(a^{-1}(y-b))+b \equiv y-b+b \equiv y \bmod 26$，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。

3. 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 $\sigma(1) = 3, \sigma(2) = 5, \sigma(3) = 1, \sigma(4) = 2, \sigma(5) = 4$，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：$\sigma^{-1}(1) = 3, \sigma^{-1}(2) = 4, \sigma^{-1}(3) = 1, \sigma^{-1}(4) = 5, \sigma^{-1}(5) = 2$，则密文 IZGZR　BELAY XXRXS 解密后为：GRIZZ LYBEA RSXXX.

4. 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 Z_{26} 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；

(2) 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

(3) 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

5. 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 Z_{101} 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.

6. 设 Alice 和 Bob 利用 RSA 公钥密码体系进行通信，Alice 的公钥: N_A=21, e_A=5；Bob 的公钥 N_B=39,e_B=7，(1)分别计算 Alice 和 Bob 的私钥 d_A 和 d_B；（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) $d_A=5^{-1} \bmod \phi(21)= 5^{-1} \bmod 12=5$;

$d_B=7^{-1} \bmod \phi(39)= 7^{-1} \bmod 24=7$;

(2) Alice 向 Bob 发送的明文 11 并加了其签名的密文为:

$E_B(D_A(11))= E_B(11^5 \bmod 21)= E_B(2)=2^7 \bmod 39=128 \bmod 39=11$;

(3) Bob 的解密过程为:

$E_A(D_B(11))= E_A(11^7 \bmod 39)= E_A(2)=2^5 \bmod 21=11$