

$$P = 5087, Q = 5051; P-1 = 5086, Q-1 = 5050$$

$$N = PQ = 5087 \times 5051 = 25694437$$

$$\text{计算: } PP' \equiv 1 \pmod{Q-1}$$

$$\text{由 } \gcd(P, Q-1) = Px + (Q-1)y$$

$\therefore$  题目要求  $P$  与  $Q-1$  互质

$\therefore$  符合  $ax \equiv 1 \pmod{b}$  的使用条件.

$$\text{且 } ax \equiv 1 \pmod{b} \Rightarrow x \equiv a^{-1} \pmod{b}$$

$$\text{可得: } P' \equiv P^{-1} \pmod{Q-1}$$

$$P' = P^{\varphi(Q-1)-1} \pmod{Q-1}$$

$$P' = 5087^{\varphi(5050)-1} \pmod{5050}$$

$$\text{由欧拉函数可得: } \varphi(Q-1) = 2000$$

$$\text{代入可得: } P' = 273$$

$$\text{同理: } Q' = Q^{\varphi(P-1)-1} \pmod{P-1}$$

$$Q' = 5051^{\varphi(5086)-1} \pmod{5086}$$

$$\text{由欧拉函数可得: } \varphi(P-1) = 2542$$

$$\text{代入可得 } Q' = 2325$$

加密:  $C = M^N \bmod N$

代入  $m = 5555555$ ,  $N = 25694437$  可得:

得  $C = 24132225$

解密:  $M_1 \equiv C^{P'} \bmod Q$

代入  $P' = 273$ ,  $C = 24132225$ ,  $Q = 5051$

得:  $M_1 = 4506$

$(M_1, Q) \Rightarrow (4506, 5051)$

$M_2 \equiv C^{Q'} \bmod P$

代入  $Q' = 2325$ ,  $C = 24132225$ ,  $P = 5087$

得:  $M_2 = 551$

$(M_2, P) \Rightarrow (551, 5087)$

将  $(M_1, Q)$ ,  $(M_2, P)$  代入中国剩余定理

可得:  $M = x = 5555555$