PROBLEM 1:

$C \equiv p \cdot a + b \pmod{73}$

- 52 is enciphered as '66'
- 20 is enciphered as '15'
- 4 is enciphered as '26'

- $66 = 52a + b \pmod{73}$ (1)
  $15 = 20a + b \pmod{73}$ (2)
  $26 = 4a + b \pmod{73}$ (3)

→ Subtract (2) from (1)

$(52a + b) - (20a + b) \equiv 66 - 15 \pmod{73}$

$32a \equiv 51 \pmod{73}$

$32^{-1} \equiv 16 \pmod{73}$

$a \equiv 51 \cdot 16 \pmod{73}$

$51 \cdot 16 = 816 = 13 \therefore a \equiv 13 \pmod{73}$

- $4a + b \equiv 26 \pmod{73}$

  $a = 13$

  $4 \cdot 13 + b \equiv 26 \pmod{73}$

  $52 + b \equiv 26 \pmod{73}$

  $b = 26 - 52 = -26 \bmod 73$

  $-26 \equiv 73 - 26 = 47 \pmod{73}$

  $b \equiv 47 \pmod{73}$

PROBLEM 4:

Given: $m = 467$ $R_2 = 339$, $R_3 = 156$, $R_4 = 390$ $R_5 = 420$, $R_6 = 107$

Find a, b, c, R_0, R_1 & R_7

→ Use Recurrence Relation:

(1) $R_4 \equiv aR_3 + bR_2 + c \pmod{467}$

(2) $R_5 \equiv aR_4 + bR_3 + c \pmod{467}$

(3) $R_6 \equiv aR_5 + bR_4 + c \pmod{467}$

→ Subtract to eliminate 1 from 2 & 2 from 3

(4) $R_5 - R_4 \equiv a(R_4 - R_3) + b(R_3 - R_2)$

(5) $R_6 - R_5 \equiv a(R_5 - R_4) + b(R_4 - R_3)$

→ Compute the differences: → adjust by adding 467 to the ones in (4)

$x = R_3 - R_2 = 156 - 339 = -183 \equiv 284$

$y = R_4 - R_3 = 390 - 156 = 234$

$z = R_5 - R_4 = 420 - 390 = 30$

$w = R_6 - R_5 = 107 - 420 = -313 \equiv 154$

→ (4) → $z \equiv a(y) + b(x)$ (6)

(5) → $w \equiv a(z) + b(y)$ (7)

* multiply (6) by y, (7) by x

$zy \equiv ay^2 + bxy$

$wx \equiv azx + bxy$

$zy - wx \equiv ay^2 - azx$

$zy - wx \equiv a(y^2 - zx)$

↳ let $D = y^2 - zx$

$\therefore a \equiv (zy - wx) \cdot D^{-1}$

$b \equiv (wy - z^2) \cdot D^{-1}$

$y^2 = 234^2 = 54756$

$zx = 30 \cdot 284 = 8520$

So: $D \equiv 54756 - 8520 = 46236 \pmod{467}$

$D \equiv 3 \pmod{467}$

→ Find $D^{-1} \pmod{467}$

→ Inverse of 3 mod 467

* $3x \; 156 = 468 \mod 467 = 1$

$\therefore D^{-1} = 156 \pmod{467}$

(1) Solve for a:

Sub $D^{-1} = 156 \pmod{467}$

$a \equiv (zy - wx) \cdot D^{-1} \bmod 467$

$zy = 30 \cdot 234 = 7020$

$wx = 154 \cdot 284 = 43736$

$zy - wx = 7020 - 43736 \equiv -36716 \pmod{467}$

$\equiv -290 \pmod{467}$

$= 177 \bmod 467$

$a \equiv 177 \cdot 156 \pmod{467}$

$\equiv 27612 \pmod{467}$

$a \equiv 59$

→ Solve for b:

$b \equiv (wy - z^2) \cdot D^{-1} \pmod{467}$

$wy - z^2$:

$\cdot wy = 154 \cdot 234 = 36036$

$\cdot z^2 = 30^2 = 900$

* multiply (6) by z, (7) by y

$z^2 \equiv ayz + bxz$

$wy \equiv ayz + by^2$

$wy - z^2 \equiv by^2 - bxz$

$wy - z^2 \equiv b(y^2 - zx)$

$wy - z^2 = 36036 - 900 = 35136 \pmod{467}$

$\equiv 399 \pmod{467}$

$b \equiv 111 \cdot 156 \pmod{467}$

$\equiv 17316 \pmod{467}$

$\equiv 37$

→ Solve for c:

→ Using (1)

$R_4 \equiv aR_3 + bR_2 + c \pmod{467}$

$c \equiv R_4 - aR_3 - bR_2 \pmod{467}$

$59 \cdot 156 = 9204$

$37 \cdot 339 = 12543$

21747

$\equiv 390 - 21747 = -21357 \pmod{467}$

$\equiv -342 \pmod{467}$

$\equiv 125 \bmod 467$

$\therefore a = 59, b = 37, c = 125 \pmod{467}$

↳ Find R_0, R_1 & R_7

→ $a=59,\ b=37,\ c=125\ \ m=467\ \ \ R_2=339,\ \ R_3=156$

* $R_{i+2} = aR_{i+1} + bR_i + c \pmod{467}$

→ $i=1$

$R_3 \equiv aR_2 + bR_1 + c \pmod{467}$

$156 \equiv (59\cdot 339) + 37(R_1) + 125 \mod 467$

$37R_1 \equiv 156 - (59\cdot 339) - 125 \pmod{467}$

$\equiv -19970 \pmod{467}$

$\equiv -356 \pmod{467}$

$\equiv 111 \pmod{467}$

$37R_1 \equiv 111 \pmod{467}$

$R_1 \equiv 111 \cdot 37^{-1}$

$467 = 12\cdot 37 + 23$

$37 = 1\cdot 23 + 14$

$23 = 1\cdot 14 + 9$

$14 = 1\cdot 9 + 5$

$9 = 1\cdot 5 + 4$

$5 = 4\cdot 1 + 1$

$1 = 5 - 1\cdot 4$

$= 5 - 1\cdot(9 - 1\cdot 5)$

$= 2\cdot 5 - 9$

$= 2\cdot(14-9) - 9 =$

$= (2\cdot 14 - 2\cdot 9) - 9$

$= 2\cdot 14 - 3\cdot 9$

$= 2\cdot 14 - 3(23 - 1\cdot 14)$

$= 5\cdot 14 - 3\cdot 23$

$= 5\cdot(37 - 23\cdot 1) - 3\cdot 23$

$= 5\cdot 37 - 8\cdot 23$

$= 5\cdot 37 - 8\cdot(467 - 37\cdot 12)$

$1 = 5\cdot 37 - 8\cdot 467 + 96\cdot 37$

$= 101\cdot 37 - 8\cdot 467$

A ⇒ $23 = 2\cdot 32 + 9$

$9 = 73 - 32\cdot 2$

$32 = 9\cdot 3 + 5$

$5 = 32 - 9\cdot 3$

$5 = 14 - 1\cdot 9 = 5\cdot 14 - 3\cdot 23$

$9 = 23 - 1\cdot 14$

$14 = 37 - 23\cdot 1$

$23 = 467 - 37\cdot 12$

* $467 \equiv 0 \pmod{467}$

$-8\cdot 467 \equiv 8\cdot 0 \equiv 0 \mod 467$

$1 = 101\cdot 37 + 0 \mod 467$

$101\cdot 37 \equiv 1 \mod 467$

$\therefore 37^{-1} = 101 \pmod{467}$

$R_1 = 111\cdot 101 \pmod{467}$

$= 11211 \pmod{467}$

$R_1 \equiv 3 \pmod{467}$

→ $i=0$

$R_2 \equiv aR_1 + bR_0 + c \pmod{467}$

$339 \equiv 59\cdot 3 + 37\cdot R_0 + 125 \pmod{467}$

$339 \equiv 302 + 37R_0$

$37R_0 = 339 - 302 \pmod{467}$

$R_0 \equiv 37\cdot 101 \pmod{467}$

$\equiv 3737 \pmod{467}$

$\equiv 1 \mod 467$

$R_0 = 1$

$R_7 = aR_6 + bR_5 + c \mod 467$

$\equiv 59\cdot 107 + 37\cdot 420 + 125 \pmod{467}$

$6313 + 15540 + 125 = 21978$

$R_7 \equiv 21978 \pmod{467}$

$\equiv 29 \pmod{467}$

$R_7 = 29$

$R_0 = 1,\ R_1 = 3,\ R_7 = 29$