Problem 1

$C = p \cdot a + b \pmod{71}$

∴ "52" enciphered as "6"

$\therefore 6 = 52a + b \pmod{71} \quad \cdots (1)$

∴ "20" enciphered as "51"

$\therefore 51 = 20a + b \pmod{71} \quad \cdots (2)$

∴ "4" enciphered as "38"

$\therefore 38 = 4a + b \pmod{71} \quad \cdots (3)$

(2) − (3)

$\rightarrow 51 = 20a + b \pmod{71} \quad \cdots (2)$

$-38 = -4a + b \pmod{71} \quad \cdots (3)$

$13 = 16a \pmod{71}$

$\therefore 13 = 16a \pmod{71}$

$a = 13 \times \text{modInv}(16) \bmod 71$

We need to find the modular inverse of 16 mod 71 using the Extended Euclidean Algorithm

Step 1

$71 = 16 \times 4 + 7 \quad (1)$

$16 = 7 \times 2 + 2 \quad (2)$

$7 = 2 \times 3 + 1 \quad (3)$

Step 2

From (3) in Step 1

$1 = 7 - (2 \times 3) \quad (1)$

From (2) in Step 1

$2 = 16 - 7 \times 2$

Sub in (1) in step 2

$1 = 7 - (3(16 - 7 \times 2))$

$1 = 7 - 3(16) + 6(7)$

$1 = 7(7) - 3(16)$ ... (2)

from (3) in Step 1

$7 = 71 - (16 \times 4)$

Sub in (2) in Step 2

$1 = 7(71 - (16 \times 4)) - 3(16)$

$1 = 7(71) - 28(16) - 3(16)$

$1 = 7(71) - 31(16)$

Mod Inverse (16) mod 71 $= -31$

We want the number btwn 1 & 71 so we add 71 till its positive

$= -31 + 71$

$= 40$

Mod Inverse (16) mod 71 $= 40$

$a = 13 \times 40$

$a = 23 \pmod{71}$

Sub in equat (3)

$38 = 4a + b \pmod{71}$

$38 = 4(23) + b$

$38 - 92 = b$

$-54 = b$

add 71 → $b = 17 \bmod 71$

Check (1)

$6 = 52(a) + b \pmod{71}$

$6 = 52(23) + 17 \pmod{71}$

$6 = 1213 \pmod{71}$

$6 = 6 \bmod 71$

$\therefore a = 23$ & $b = 17$

$bR_3 - bR_2$

$b(R_3 - R_2)$

Problem 3 $\quad m = 467$

$$R_{i+2} = (aR_{i+1} + bR_i + c) \pmod m \quad i \geq 0$$

$$R_4 = aR_3 + bR_2 + c \pmod m \quad \cdots (1)$$

$$R_5 = aR_4 + bR_3 + c \pmod m \quad \cdots (2)$$

$$R_6 = aR_5 + bR_4 + c \pmod m \quad \cdots (3)$$

(2) − (1) & (3) − (2)

$$R_5 - R_4 = a(R_4 - R_3) + b(R_3 - R_2) \pmod m$$

$$R_6 - R_5 = a(R_5 - R_4) + b(R_4 - R_3) \pmod m$$

multiply both by mod inverse of the coefficient of b

$$\underbrace{(R_3 - R_2)^{-1} \times (R_5 - R_4)}_{A} = \underbrace{a(R_4 - R_3)(R_3 - R_2)^{-1}}_{B} + b \pmod m \quad -(4)$$

$$\underbrace{(R_4 - R_3)^{-1}(R_6 - R_5)}_{C} = \underbrace{a(R_5 - R_4)(R_4 - R_3)^{-1}}_{D} + b \pmod m \quad -(5)$$

(5) − (4)

$$C - A = a(D - B) \pmod m$$

$$a = (C - A)(D - B)^{-1} \pmod m$$

$$\therefore a = \left[(R_6 - R_5)(R_4 - R_3)^{-1} - (R_5 - R_4)(R_3 - R_2)^{-1}\right]\left[(R_5 - R_4)(R_4 - R_3)^{-1} - (R_4 - R_3)(R_3 - R_2)^{-1}\right]^{-1}$$

from (5) $\quad b = C - aD$

$$\therefore b = (R_6 - R_5)(R_4 - R_3)^{-1} - a\left[(R_5 - R_4)(R_4 - R_3)^{-1}\right]$$

$$a = [(105-118)(41-137)^{-1}] - [(118-41)(137-28)^{-1}]$$

$$*$$

$$[(118-41)(41-137)^{-1}] - [(41-137)(137-28)^{-1}]^{-1}$$

$$a = [(-13)(-96)^{-1} - (77)(109)^{-1}][(77)(-96)^{-1} - (-96)(109)^{-1}]^{-1}$$

$$(-96)^{-1} = (371)^{-1} = 287 \pmod{467}$$
$$(109)^{-1} = 30 \pmod{467}$$

$$a = [(-13)(287) - (77)(30)][(77)(287) - (-96)(30)]^{-1}$$
$$a = [-3731 - 2310][22099 + 2880]^{-1}$$
$$a = [-6041][24979]^{-1}$$
$$a = [-6041][297]$$
$$a = -1794177 \pmod{467}$$
$$a = 37$$

$$b \equiv (105-118)(41-137)^{-1} - 37((118-41)(41-137)^{-1})$$

$$b = (-13)(-96)^{-1} - 37((77)(-96)^{-1})$$

$$b = (-13)(287) - 37((77)(287))$$
$$b = -3731 - 817663$$
$$b = -821394 \pmod{467}$$
$$b = 59$$

from (1) $c = P_4 - aP_3 - bP_2 \pmod{n}$

$$c = 41 - 37(137) - 59(28)$$
$$c = -6680 \pmod{467}$$
$$c = 325$$

When $i = 1$

$R_3 = aR_2 + bR_1 + c$

$bR_1 = R_3 - aR_2 - c$

$R_1 = (R_3 - aR_2 - c)\, b^{-1} \pmod{467}$

$R_1 = (137 - 37(28) - 325)(59)^{-1} \pmod{467}$

$R_1 = (-1224)\, 95\, 3 \pmod{467}$

$R_1 = -116280 \pmod{467}$

$R_1 = 3$

When $i = 0$

$R_0 = (R_2 - aR_1 - c)\, b^{-1} \pmod{467}$

$R_0 = (28 - 37(3) - 325)(59)^{-1}$

$R_0 = (-408)(95)$

$R_0 = -38760 \pmod{467}$

$R_0 = 1$

When $i = 5$

$R_7 = aR_6 + bR_5 + c \pmod{m}$

$R_7 = 37(105) + 59(118) + 325 \pmod{467}$

$R_7 = 11172 \pmod{467}$

$R_7 = 431$

$\therefore a = 37,\ b = 59,\ c = 325,\ R_1 = 3,\ R_0 = 1,\ R_7 = 431$