<u>Problem 1:</u> Given: $e = 59,\ i = 63,\ H = 60,\ Y = 2$ and knowing that e enciphers to H and i enciphers to y, we get the following equations **<u>Answer:</u>** $a = 26,\ b = 65$

$$(59 * A + B)\ mod\ 81 = 60$$
$$(63 * A + B)\ mod\ 81 = 2$$
$$((63 - 59) * A + (B - B))\ mod\ 81 = 2 - 60$$
$$(4 * A)\ mod\ 81 \equiv -58 \equiv 23$$

Using the extended euclidian algorithm to find the modular inverse for 4 and 81

$$4x \equiv 1\ mod\ 81$$
$$x \equiv \frac{1}{4}\ mod\ 81$$
$$x \equiv 4^{-1}\ mod\ 81$$
$$81 = 4 * 20 + 1$$
$$1 = 81 - 20 * 4$$
$$\therefore 4^{-1} mod 81 \equiv -20 \equiv 61$$

Multiplying both sides with the modular inverse we get

$$A = (23 * 61) \therefore A = 26$$

Plugging A into the equation we can solve for B

$$(63 * 26 + B)\ mod\ 81 = 2$$
$$(1638 + B)\ mod\ 81 = 2$$
$$\therefore B = 65$$

we can check this by plugging A and B into both equations

$$(59 * 26 + 65)\ mod\ 81 = 60$$
$$And$$
$$(63 * 26 + 65)\ mod\ 81 = 2$$

Since both of these are true, we know $\therefore a = 26,\ b = 65$

<u>Problem 3:</u> For $m = 16,\ R_1 = 2,\ R_2 = 11,\ R_3 = 8$ Determine $a = ?,\ b = ?,\ R_0 = ?,\ R_4 = ?$

<u>The answer is</u> $A = 5,\ B = 1,\ R_0 = 13,\ R_4 = 9$

My work follows...

$$(R_1 * A + B)\ mod\ m = R_2$$
$$(R_2 * A + B)\ mod\ m = R_3$$
$$((R_2 - R_1) * A + (B - B))\ mod\ m = R_3 - R_2$$
$$((R_2 - R_1) * A)\ mod\ m = R_3 - R_2$$
$$((11 - 2) * A)\ mod\ 16 = 8 - 11$$
$$(9 * A)\ mod\ 16 = -3$$

Now we must isolate A by finding the modular inverse of 9 & 16. This is done by using the extended Euclidian Algorithm

$$9x \equiv 1\ mod\ 16$$
$$x \equiv \frac{1}{9}\ mod\ 16$$
$$x \equiv 9^{-1}\ mod$$
$$16 = 9 * 1 + 7$$
$$9 = 7 * 1 + 2$$
$$7 = 2 * 3 + 1$$
$$1 = 7 - 2 * 3$$

$$sub.\ 2 = 9 - 7$$
$$1 = 7 - (9 - 7 * 3)$$
$$1 = 7 - 3(9 - 7)$$
$$1 = 7 - 3 * 9 + 3 * 7$$
$$1 = -3 * 9 + 4 * 7$$

$$sub.\ 7 = 16 - 9$$
$$1 = -3 * 9 + 4(16 - 9)$$
$$1 = -3 * 9 + 4 * 16 - 4 * 9$$
$$1 = -7 * 9 + 4 * 16$$

Since we are using mod 16 anything multiplied by 16 evaluates as zero,

$$\therefore 9^{-1}\ mod\ 16 \equiv -7\ mod\ 16 \equiv 9 \leftarrow inverse$$

To isolate A we must multiply both sides by the inverse, resulting in

$$A = -3 *\ Inverse\ mod\ m$$
$$A = -3 * 9\ mod\ 16$$
$$A = 5$$

And to isolate B, we can use the equation $(R_1 * A - B)\ mod\ m = R_2$ as our starting point.

$$B = R_2 - R_1 * A\ mod\ m$$
$$B = 11 - 2 * 5\ mod\ 16$$
$$B = 1$$

Now We can find R_4 using the LCG equation

$$R_4 = (R_3 * A + B) \, mod \, m$$
$$R_4 = (8 * 5 + 1) \, mod \, 16$$
$$R_4 = 9$$

Finding R_0 is simply finding the inverse of 5 & 16, using the extended Euclidian algorithm we get

$$5 \, x \equiv 1 \, mod \, 16$$
$$x \equiv \frac{1}{5} \, mod \, 16$$
$$x \equiv 5^{-1} \, mod \, 16$$
$$16 = 5 * 3 + 1$$
$$1 = 16 - 3 * 5$$
$$\therefore 5^{-1} \, mod \, 16 \equiv -3 \equiv 13 \leftarrow \, inverse$$
$$R_0 = 13$$

We can check this by inputting our value into the equation $(R_0 * A + B) \, mod \, m = R_1$ since $(13 * 5 + 1) \, mod \, 16 = 2$ we know it is correct