$n := 7$

$r := 2^n = 128$

$m := 21$

$a := 24 \qquad b := 10$

$$b := \begin{pmatrix} 0 \\ 1 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

$A := \mathrm{mod}(a \cdot r, m) = 6$

$i = 0$

$S_{00} := 0$

$q_0 := \mathrm{mod}\left(S_{00}, 2\right) = 0$

$$S_0 := \mathrm{floor}\left(\frac{S_{00} - q_0}{2}\right) + q_0 \cdot \left(\mathrm{floor}\left(\frac{m+1}{2}\right)\right) + b_0 A = 0$$

$\mathrm{mod}(a \cdot b, m) = 9$

$\gcd(r, m) = 1$

$i = 1$

$q_1 := \mathrm{mod}\left(S_0, 2\right) = 0$

$$S_1 := \mathrm{floor}\left(\frac{S_0 - q_1}{2}\right) + q_1 \cdot \left(\mathrm{floor}\left(\frac{m+1}{2}\right)\right) + b_1 A = 6$$

$i = 2$

$q_2 := \mathrm{mod}\left(S_1, 2\right) = 0$

$$S_2 := \mathrm{floor}\left(\frac{S_1 - q_2}{2}\right) + q_2 \cdot \left(\mathrm{floor}\left(\frac{m+1}{2}\right)\right) + b_2 A = 3$$

$i = 3$

$q_3 := \mathrm{mod}\left(S_2, 2\right) = 1$

$$S_3 := \mathrm{floor}\left(\frac{S_2 - q_3}{2}\right) + q_3 \cdot \left(\mathrm{floor}\left(\frac{m+1}{2}\right)\right) + b_3 A = 18$$

$i = 4$

$q_4 := \mathrm{mod}(S_3, 2) = 0$

$$S_4 := \mathrm{floor}\left(\frac{S_3 - q_4}{2}\right) + q_4 \cdot \left(\mathrm{floor}\left(\frac{m+1}{2}\right)\right) + b_{4}A = 9$$

$i = 5$

$q_5 := \mathrm{mod}(S_4, 2) = 1$

$$S_5 := \mathrm{floor}\left(\frac{S_4 - q_5}{2}\right) + q_5 \cdot \left(\mathrm{floor}\left(\frac{m+1}{2}\right)\right) + b_{5}A = 15$$

$i = 6$

$q_6 := \mathrm{mod}(S_5, 2) = 1$

$$S_6 := \mathrm{floor}\left(\frac{S_5 - q_6}{2}\right) + q_6 \cdot \left(\mathrm{floor}\left(\frac{m+1}{2}\right)\right) + b_{6}A = 18$$

$i = 7$ FOR $n = 7$

$q_7 := \mathrm{mod}(S_6, 2) = 0$

$$S_7 := \mathrm{floor}\left(\frac{S_6 - q_7}{2}\right) + q_7 \cdot \left(\mathrm{floor}\left(\frac{m+1}{2}\right)\right) + b_{7}A = 9$$

$i = 8$ FOR $n = 8$

$q_8 := \mathrm{mod}(S_7, 2) = 1$

$$S_8 := \mathrm{floor}\left(\frac{S_7 - q_8}{2}\right) + q_8 \cdot \left(\mathrm{floor}\left(\frac{m+1}{2}\right)\right) + b_{7}A = 15$$

$x := a$

$e := \begin{pmatrix} 0 \\ 1 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}$ $\quad e := \sum_{i=0}^{n-1} \left(e_i 2^i\right) = 10$

$y_{00} := \mathrm{mod}(1r, m) = 2$

$z_{00} := x$

for $i = 0$ **to** $n - 1 = 6$
do

$i = 0$

$\mathrm{mod}\left(x^e, m\right) = 18$

$e_0 = 0 \qquad y_0 := y_{00} = 2$

$x^e = 63403380965376$

$z_0 := \mathrm{mod}\left(z_{00} \cdot z_{00}, m\right) = 9$

$i = 1$

$e_1 = 1 \qquad y_1 := \mathrm{mod}\left(y_0 \cdot z_0, m\right) = 18$

$z_1 := \mathrm{mod}\left(z_0 \cdot z_0, m\right) = 18$

$i = 2$

$e_2 = 0 \qquad y_2 := y_1 = 18$

$z_2 := \mathrm{mod}\left(z_1 \cdot z_1, m\right) = 9$

$i = 3$

$e_3 = 1 \qquad y_3 := \mathrm{mod}\left(y_2 \cdot z_2, m\right) = 15$

$z_3 := \mathrm{mod}\left(z_2 \cdot z_2, m\right) = 18$

$i = 4$

$e_4 = 0$ $\quad y_4 := y_3 = 15$

$z_4 := \mathrm{mod}(z_3 \cdot z_3, m) = 9$

$i = 5$

$e_5 = 0$ $\quad y_5 := y_4 = 15$

$z_5 := \mathrm{mod}(z_4 \cdot z_4, m) = 18$

$i = 6$ FOR $n = 7$

$e_6 = 0$ $\quad y_6 := y_5 = 15$

$z_6 := \mathrm{mod}(z_5 \cdot z_5, m) = 9$

$i = 7$ FOR $n = 8$

$e_7 = 0$ $\quad y_7 := y_6 = 15$

$z_7 := \mathrm{mod}(z_6 \cdot z_6, m) = 18$