CS60004: Hardware Security Class Test-1 Solutions..

1. (a) Squarings = $m-1 = 193-1 = 192$

Multiplications = $m-2 = 193-2 = 191$

(b) Length of addition chain = 9

$\therefore$ No. of multiplications = $9-1 = 8$

Squaring = $m-1 = 192$

(c) Both have the same delay of 1LUT

2. Modulus polynomial = x^4+x^3+1

Let $a = a_3x^3 + a_2x^2 + a_1x + a_0 \in GF(2^4)$

$a^2 = a_3x^6 + a_2x^4 + a_1x^2 + a_0$

$= a_3(x^3+x^2+x+1) + a_2(x^3+1) + a_1x^2 + a_0$

$= (a_3 \oplus a_2)x^3 + (a_3 \oplus a_1)x^2 + a_3x + (a_0 \oplus a_2 \oplus a_3)$

Note $x^4 = x^3+1$

$x^5 = x^4 + x$

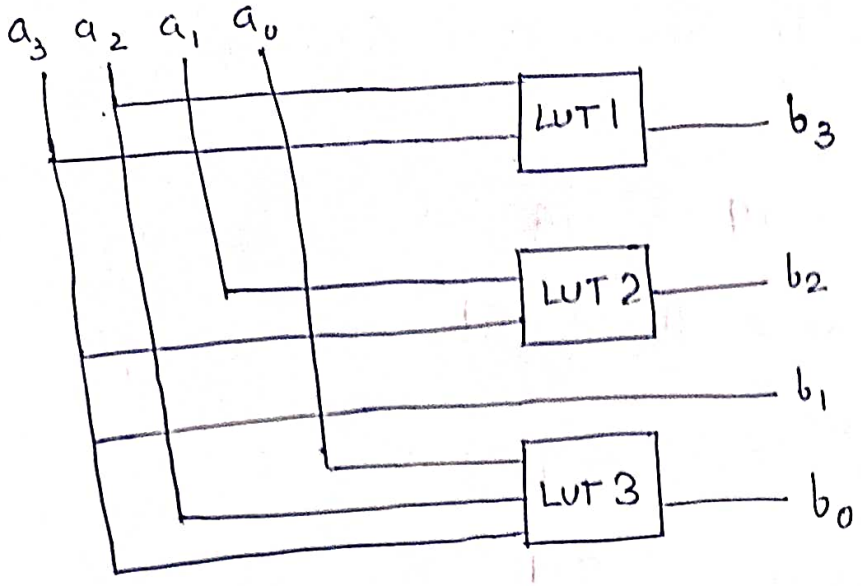
$= x^3 + x + 1$

$x^6 = x^4 + x^2 + x$

$= x^3 + x^2 + x + 1$

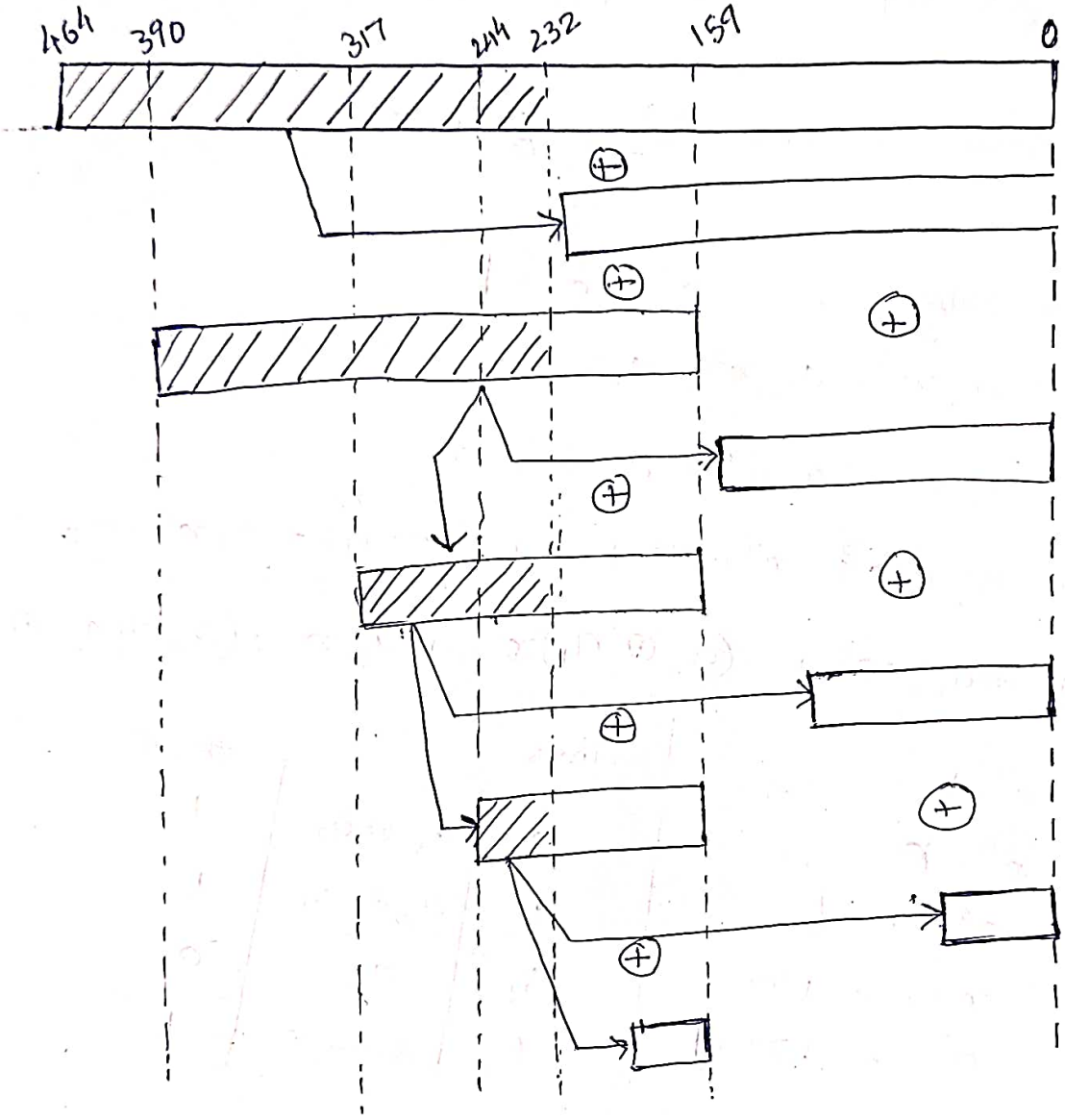
Thus,

		#LUT
b_3	$a_3 \oplus a_2$	1
b_2	$a_3 \oplus a_1$	1
b_1	a_3	0
b_0	$a_3 \oplus a_2 \oplus a_0$	1



Circuit using 4-input LUTs.

3.



Critical Path contains 5 XOR