SC 1, FF 4-6

SC1) CT: 0101 0101 1110 1001

2 generates $\mathbb{F}_{83}$ 5 generates $\mathbb{F}_{167}$ Secret Key = 7

$5^7 \bmod 167 = 136 \bmod 2 = 0$

$136^2 \bmod 167 = 126 \bmod 2 = 0$

$126^2 \bmod 167 = 11 \bmod 2 = 1$

$11^2 \bmod 167 = 121 \bmod 2 = 1$

$121^2 \bmod 167 = 112 \bmod 2 = 0$

$112^2 \bmod 167 = 19 \bmod 2 = 1$

$19^2 \bmod 167 = 27 \bmod 2 = 1$

$27^2 \bmod 167 = 61 \bmod 2 = 1$

$61^2 \bmod 167 = 47 \bmod 2 = 1$

$47^2 \bmod 167 = 38 \bmod 2 = 0$

$38^2 \bmod 167 = 108 \bmod 2 = 0$

$108^2 \bmod 167 = 141 \bmod 2 = 1$

$141^2 \bmod 167 = 8 \bmod 2 = 0$

$8^2 \bmod 167 = 64 \bmod 2 = 0$

$64^2 \bmod 167 = 88 \bmod 2 = 0$

$88^2 \bmod 167 = 62 \bmod 2 = 0$

	0101	0101	1110	1001
	0011	0111	1001	0000	⊕
PT:	0110	0010	0111	1001

ASCII: by

FF-4)

Polynomials of Degree 3	Irreducible form
x^3+0x^2+0x+0	$x^2(x)$
x^3+0x^2+0x+1	$(x^2+x+1)(x+1)$
x^3+0x^2+x+0	$x(x^2+1)$
x^3+0x^2+x+1	Irreducible
x^3+x^2+0x+0	$x^2(x+1)$
x^3+x^2+0x+1	Irreducible
x^3+x^2+x	$x(x^2+x+1)$
x^3+x^2+x+1	$(x^2+1)(x+1)$

FF-5) $x^3=x+1$

Power of 2	mod (x^3+x+1)	Reduced
$(x^2)^1$	x^2	x^2
$(x^2)^2$	x^4	x^2+x
$(x^2)^3$	x^6	x^2+1
$(x^2)^4$	x^8	x
$(x^2)^5$	x^{10}	$x+1$
$(x^2)^6$	x^{12}	x^2+x+1
$(x^2)^7$	x^{14}	1

Yes

FF-6) a)

$$\begin{array}{r} x^3 \quad x \mid 1 \\ x^3 \quad x^2 \mid 1 \\ \hline x^3 \quad x \mid 1 \\ x^5 \quad x^3 \quad x^2 \\ x^6 \quad x^4 \quad x^3 \\ \hline x^6 + x^5 + x^4 + x^3 + x^2 + x + 1 \end{array}$$

$x^4 = x + 1$

$x^5 = x^4 \cdot x = (x+1)(x) = x^2 + x$

$x^6 = x^3 + x^2$

$(x^3 + x^2) + (x^2 + x) + (x+1) + x^3 + x^2 + x + 1$

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

b) $x^4 = x + 1$

x	x
x^2	x^2
x^3	x^3
x^4	$x+1$
x^5	$x^2 + x$
x^6	$x^3 + x^2$
x^7	$(x+1) + x^3$
x^8	$x^2 + 1$
x^9	$x^3 + x$
x^{10}	$x^2 + x + 1$

x^{11}	$x^3 + x^2 + x$
x^{12}	$x^3 + x^2 + x + 1$
x^{13}	$x^3 + x^2 + 1$
x^{14}	$x^3 + 1$
x^{15}	x

c) No.

LM-3) i)

a = nextprime(2^50) = 1125...

b = nextprime(3^50) = 7178...

$m = 11^{27} = 1310...$

mod(a,m)^b = 4860...

ii) mod(a,m)^-1 = 1105...

iii) (d*a) - 1)/m = 9494...

iv) gcd(m, 8689...) = 11

vi) That is all.