1) $p=7,\ q=17,\ e=91$

a) $n = p \cdot q = 7 \cdot 17 = 119 \quad \Theta(n) = (6)(16) = 96$

$d = e^{-1} \bmod (\Theta(n)) = 91^{-1} \bmod (96)$

$96 = 91 \cdot 1 + 5$

$91 = 5 \cdot 18 + 1 \qquad 1 = 91 - 5 \cdot 18$

$1 = 91 - 18(96 - 91)$

$1 = 19 \cdot 91 - 18 \cdot 96$

$d = 19 \qquad 91^{-1} = 19$

ii) $M = 88^{19} \bmod 119 = 95$

$S = 1\ 0\ 0\ 1\ 1 \qquad b = 88 \quad n = 19 \quad m = 119$

$a = 88$

i	$b = b^2 \% m$	a
1	9	78
2	81	78
3	16	78
4	18	95

$M = 95$

iii) $y = 95$

$a' = 95/26 = 3 \qquad b' = 17$

iv) $P = a'C + b' \pmod{26}$

$V = 21$	$3(21) + 17 \pmod{26} = 2$	C
$B = 1$	$3(1) + 17 \pmod{26} = 20$	U
$S = 18$	$3(18) + 17 \pmod{26} = 19$	T
$X = 23$	$3(23) + 17 \pmod{26} = 8$	I
$N = 13$	$3(13) + 17 \pmod{26} = 4$	E

3) $n = 84$

5) $p = 37$ $g = 2$ $a_B = 22$ $g^k \bmod p = 17$

$M g^{a_B k} \bmod p = 34$

i) $M = 34 \cdot (g^{a_B k})^{-1} \bmod p$

$M(17^{22}) \bmod 37$

$22 = 1\ 0\ 1\ 1\ 0$

	b	a
0	—	1
1	30	30
2	12	27
3	33	27
4	16	25

$M = 34(25)^{-1} \bmod 37$

$37 = 25 \cdot 1 + 12$ $\quad 1 = 25 - 12 \cdot 2$

$25 = 13 \cdot 2 + 1$ $\quad 1 = 25 - 2(37 - 25 \cdot 1)$

3·25 ~~2·37~~

$M = 28$

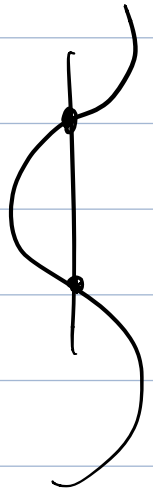
ii) No

iii) No, since she can't solve for M without a_B.

4) $t^2 = t+1$

$y^2 + txy = x^3 + t + 1$

$x = t$



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

4583

$n = 43 \cdot 107 = 4601$

$z = (42)(106) = 4452$

$D = 6704$

$C = 19$