$AB = (0)(1)_{(30)} = 1$

$AC = (0)(2)_{(30)} = 2$

$FP = (5)(15)_{30} = 5 \cdot 30 + 15 = 165$

$m^d = c^d \pmod n = 1^3 \pmod{187} = 1 \in AA$

$2^3 \pmod{187} = 8 \in AC$

$165^3 \pmod{187} = (-22)^3 = -22 \cdot 484 =$

$= -22 \cdot \underbrace{110}_{-77} = 22 \cdot 77 = \underbrace{121}_{-66} \cdot 14 =$

$= -910 = -162 = 25$

$= (-22)^3 = -22 \cdot 22^2 = -22 \cdot 484 =$

$= -22 \cdot 110 = -2 \cdot 11 \cdot 11 \cdot 10 = -20 \cdot \underbrace{121}_{-66} =$

$= \underbrace{132}_{-55} \cdot 10 = -550 = -(-11) = \underline{11} \in FP$

$1 : 30 = 0$	$8 : 30 = 0$	$11 \cdot 30 = 0$
0	0	1
(1)	(8)	

$AB\,AC\,FP\,FP \longrightarrow (1)(8)(11)(11) = BILL$

4. $p = 7, q = 11$

$d > 1$ minim.

a) (n, e)

b) $B!BTBL \qquad j = 1, l = 2$

a) $n = p \cdot q = 7 \cdot 11 = 77$.

$\varphi(n) = (p-1)(q-1) = 6 \cdot 10 = 60. = 2^2 \cdot 3 \cdot 5$

$(d, \varphi(n)) = 1 \Rightarrow d \neq 2, 3, 5$

$\Rightarrow \boxed{d_{min} = 7}$

$e = d^{-1} \pmod{\varphi(n)} = 7^{-1} \pmod{60}$

$(60, 7) = 1$

$60 = 8 \cdot 7 + 4$

$7 = 1 \cdot 4 + 3$

$4 = 1 \cdot 3 + 1$

$x_{60} = (1, 0)$, $x_7 = (0, 1)$

$x_4 = x_{60} - 8 x_7 = (1, 0) - (0, 8) = (1, -8)$

$x_3 = x_7 - x_4 = (0, 1) - (1, -8) = (-1, 9)$

$x_1 = x_4 - x_3 = (1, -8) - (-1, 9) = (2, -17)$

$\Rightarrow 7^{-1} \pmod{60} = -17 = 43 \Rightarrow n = 77, e = 43$

b) $B! = (1)(28)_{(30)} = 30 + 28 = 58$

$BT = (11)(19)_{(30)} = 30 + 19 = 49$

$BL = (11)(11)_{(30)} = 30 + 11 = 41$

$m = c^d \pmod{n}$

$\rightarrow 58^7 \pmod{77} = (-19)^7 = -19 \cdot (19^2)^3 = -19 \cdot \underbrace{53}_{-24}^3 =$

$= -19 \cdot (-24) \cdot \underbrace{24}_{37}^2 = 19 \cdot 24 \cdot 37 = \underline{\underline{9}}$

$\rightarrow 49^7 \pmod{77} = (-28)^7 = -28 \cdot (\underbrace{28^2}_{14})^3 = -\underbrace{28 \cdot 14}_{2 \cdot 42} \cdot \underbrace{14}_{42}^2 =$

$= -2 \cdot 42 \cdot 42 = -\underbrace{84}_{7} \cdot 42 = -7 \cdot 42 = -63 = \underline{\underline{14}}$

$\rightarrow 41^7 \pmod{77} = (-36)^7 = -36 \cdot (\underbrace{36^2}_{64})^3 = -36 \cdot (-13) \cdot 15^2 =$

$= \cancel{3 \cdot 13^3 \cdot 13^2 = 3 \cdot 11 = -18 = 15} = \cancel{-36}$

$\underbrace{15}_{7} \quad \underbrace{15}_{-6}$

h)

$= 36 \cdot 13 \cdot 15 = \underline{13}$

B ! BTBL $\longrightarrow$ (9)(14)(13) = JON

5. $k_u = (m = 1189,\ e = 747)$

a) $d = ($

b) $N^d \le m \le N^{d+1}$ BFCATNBIW

//

a) $d = e^{-1} (\mathrm{mod}\ \varphi(m))$

$\sqrt{1189} \mid 34$

9

289

256

$= 33$

$64 \cdot 4 = 256$

$\lfloor \sqrt{m} \rfloor = 34$

$t = 35$

$t^2 - m = (34+1)^2 - m = 34^2 + 68 + 1 - m = 69 - 33 = 36 = 6^2$

$35^2 - m = 6^2 \Rightarrow m = 35^2 - 6^2 = (35-6)(35+6) = 29 \cdot 41$

$\varphi(n) = 28 \cdot 40 = 1120.$

$d = e^{-1} (\mathrm{mod}\ \varphi(n)) = 747^{-1} (\mathrm{mod}\ 1120)$

$(1120, 747) = 1$

$1120 = 1 \cdot 747 + 373$

$747 = 2 \cdot 373 + 1$

$x_{1120} = (1, 0),\quad x_{747} = (0, 1)$

$x_{373} = (1, 0) - (0, 1) = (1, -1)$

$x_1 = (0, 1) - 2(1, -1) = (-2, 3) \Rightarrow \boxed{d = 3}$

h) $N^d \leq m < N^{d+1} \Rightarrow 30^d \leq 1189 \leq 30^{d+1} \Rightarrow \underline{d=2}, \underline{l_p=5}$

2nd clan cuplet.

$BFC = (1)(5)(2)_{(30)} = 30^2 + 5 \cdot 30 + 2 = 900 + 150 + 2 = 1052$

$AFN = (0)(5)(13)_{(30)} = 5 \cdot 30 + 13 = 150 + 13 = 163$

$BIW = (1)(8)(22)_{(30)} = 30^2 + 8 \cdot 30 + 22 = 900 + 240 + 22 = 1162$

$\underline{m = c^d \pmod n}$

$\rightarrow 1052^3 \pmod{1189} = (-137)^3 = -137 \cdot 137^2 = 137 \cdot 255 = 454$

$137^2 = 18769$: 1189 = 15
934
-255

$\rightarrow 163^3 \pmod{1189} = 163 \cdot 163^2 = 163 \cdot 411 = 409$

$\rightarrow 1162^3 \pmod{1189} = \cancel{1162 \cdot 1162} \quad -27 \cdot 27^2 = -27 \cdot 729 = 27 \cdot 460 =$

$729 : 1189 = 0$
-460

$= 9 \cdot 4380 = 9 \cdot 191 = 1719 = 530$

$454 : 30 = 15$
30
154
150
4

$15 : 30 = 0$
0
15

$\rightarrow \cancel{PE(15)(4)}$
$454 = (15)(4) = PE$

$409 : 30 = 13$
30
109
90
19

$\rightarrow 409 = (13)(19) = NT$

$530 : 30 = 17$
30
230
210
20

$\rightarrow 530 = (17)(20) = RU$

$\rightarrow$ PENTRU

$d = e^{-1} \pmod{\varphi(n)} \equiv 3 \cdot 91^{-1} \pmod{\ldots}$

6. $j = 1, \ell = 2$

$p = 23, q = 17$ $(m, \ell = 3)$

a) HELP_ME!

b) d, EBMMAAE OMMLIESAIHI

---

c) $M = p \cdot q = 23 \cdot 17 = 391$

$c = m^{\ell} \pmod{n} = m^3 \pmod{391}$

HELP_ME!

m 7 4 11 15 26 12 4 28

---

343 64 158 247

$7^3 \bmod 391 = 343$

$4^3 \bmod 391 = 64$

$11^3 \bmod 391 = 158$

$15^3 \bmod 391 = -144 = 247$

$26^3 \bmod 391 = 26 \cdot 26^2 = 26 \cdot \underbrace{205}_{-106} = -19 = 372$

$12^3 \bmod 391 = 164$

$4^3 \bmod 391 = 64$

$28^3 \bmod 391 = 28 \cdot 28^2 = 28 \cdot \underbrace{784}_{2} = 56$

$343 : 30 = 11 \rightarrow 343 = (11)(13) = LN$

$\underline{30}$

43

$\underline{30}$

13

$64 : 30 = 2 \rightarrow 64 = (2)(4) = CE$

$\underline{60}$

(4)

$158 : 30 = 5 \rightarrow 158 = (5)(8) = FI$

$\underline{150}$

8

$247 : 30 = 8 \rightarrow 247 = (8)(7) = IH$

$\underline{240}$

7

372 : 30 = 12 → 372 = (12)(12) = MM

30
72
60
12

164 : 30 = 5 → 164 = (5)(14) = FO

140
14

64 = CE

56 : 30 = 1 → 56 = (1)(26) = B_

30
26

→ LNCEF1IHMMFOB_

b) ~~d~~ ≡ φ(n) = (23−1)(17−1) = 22·16 = 352

$d = e^{-1} \pmod{\varphi(n)} = 3^{-1} \pmod{352}$

(352, 3) = 1.

~~352 = (1,0)~~

352 = 117·3 + 1 ⇒ $x_1 = (1,0) - (0, 117) = (1, -117)$ ⇒

⇒ $3^{-1} \equiv -117 = 235$ ⇒ **d = 235**

EB = (14)(1)$_{30}$ = 4·30 + 1 = 121

MM = (12)(12)$_{30}$ = 12·30 + 12 = 12·31 = 372

AA = (0)(0)$_{30}$ = 0

F = (5)(26)$_{30}$ = 5·30 + 26 = 176

OM = (14)(12)$_{30}$ = 14·30 + 12 = 420 + 12 = 432

ML = (12)(11)$_{30}$ = 12·30 + 11 = 360 + 11 = 371

!E = (28)(4)$_{30}$ = 28·30 + 4 = 844

BA = (11)(0)$_{30}$ = 330

IH = (8)(7)$_{30}$ = 8·30 + 7 = 247

I = (8)(26)$_{30}$ = 240 + 26 = 266

FO = (5)(14) = 164

MM = (12)(12) = 372

L! = (11)(28) = 358

EB = (14)(1) = 121

Ai = (0)(8) = 8

Hi = (7)(8) = 218

$m = c^{d} (\mod M) = c^{235} (\mod 391)$

$\rightarrow 121^{235} \pmod{391} = \cdot 8 = 1$

$\rightarrow 372^{235} (\mod 391) = 26 = \_$

$\rightarrow 0^{235} (\mod 391) = 0 = A$

$\rightarrow 169^{235} (\mod 391) = 12 = M$

$\rightarrow 372^{235} (\mod 391) = 26 = \_$

$\rightarrow 358^{235} (\mod 391) = 18 = S$

$\rightarrow 121^{235} (\mod 391) = 8 = I$

$\rightarrow 8^{235} (\mod 391) = 2 = C$

$\rightarrow 218^{235} (\mod 391) = 10 = K$

$\rightarrow$ I_AM_SICK

7. $K_1 = (n_1 = 9991, e_1 = 3517)$.

a). $k = 2$

b) BMHAX $\qquad j = 2, l =>$

---

a) $\sqrt{9991} = 99$

81

1891

1701

190

$182 \cdot 7 = 1701$

$[\sqrt{n}] = 99$

$t = 100$

$t^2 - n = (99+1)^2 - n = 99^2 + 199 - n = 199 - 190 = 9$

$100^2 - n = 3^2 \Rightarrow n = 100^2 - 3^2 = (100-3)(100+3) = 97 \cdot 103$

$\varphi(n) = (97-1)(103-1) = 96 \cdot 102 = 9792$

$d = e^{-1} \pmod{\varphi(n)} \equiv 3917^{-1} \pmod{9792}$

$(9792, 3917) = 1$

$9792 = 2 \cdot 3917 + 1958$

$3917 = 2 \cdot 1958 + 1$

$\times 9792 = (1,0), \quad \times 3917 = (0,1)$

$\times 1958 = (1,0) - (0,2) = (1,-2)$

$\times 1 = (0,1) - (2,-4) = (-2,5) \Rightarrow \boxed{d = 5}$

b) $BMH = (1)(12)(7)_{(30)} = 1 \cdot 30^2 + 12 \cdot 30 + 7 = 900 + 360 + 7 = 1267$

$A\_X = (0)(26)(23)_{(30)} = 26 \cdot 30 + 23 = 803$

$m = c^d \pmod{n} = c^5 \pmod{9991}$

$\rightarrow 1267^5 \pmod{9991} = 404$

$\rightarrow 803^5 \pmod{9991} = 570$

$404 : 30 = 13 \rightarrow 404 = (13)(14) = NO$

30
104
90
14

$570 : 30 = 19 \rightarrow 570 = (19)(0) = TA$

30
270
270
0

$\rightarrow NOTA$