Tema 7

1) $n = 12827 \quad d = 2291$

$\sqrt{1.28.27}$ | 113

1

$= 28$ | $21 \cdot 1 = 21$

21

$= 727$ | $223 \cdot 3 = 669$

669

$= 58.$

$\Rightarrow [\sqrt{n}] = 113 = n'$

$t = 114$

$t^2 - n = (n'+1)^2 - n = 113^2 + 2 \cdot 113 + 1 - n$

$= (113^2 - n) + 227 = (-58) + 227 = 169$

$= 13^2$

$\Rightarrow n = 114^2 - 13^2 = (114 - 13)(114 + 13)$

$= 101 \cdot 127$

$\Rightarrow p = 101 \quad ; \quad q = 127$

$\varphi(n) = (p-1)(q-1) = 100 \cdot 126 = 12600$

$e \cdot d \equiv 1 \pmod{\varphi(n)}$

$e \cdot 2291 \equiv 1 \pmod{12600}$

$\Rightarrow e \equiv 2291^{-1} \pmod{12600}$

$12600 : 2291 = 5$ Rest 1145
11455
$= 1145$

$X_{12600} = (1,0) \quad X_{2291} = (0,1)$

$X_{1145} = X_{12600} - 5 \cdot X_{2291}$
$= (1,0) - (0,5)$
$= (1, -5)$

$2291 : 1145 = 2$ Rest 1
2290
$= = = 1$

$X_1 = X_{2291} - 2 \cdot X_{1145}$
$= (0,1) - (2, -10)$
$= (-2, 11)$

$\Rightarrow e \equiv 11 \pmod{12600}$

$m : ERI = (8)(4)(17)(8)_{(30)} = 8 \cdot 30^0 + 17 \cdot 30^1 + 4 \cdot 30^2 + 8 \cdot 30^3$

$= 8 + 17 \cdot 30 + 4 \cdot 900 + 8 \cdot 27000 =$

$j = 2$

$l = 1 + j = 3$

m: IE, RI

m_1: $IE = (8)(4)_{(30)} = 4 \cdot 30^0 + 8 \cdot 30 = 244$

m_2: $RI = (17)(8)_{(30)} = 8 \cdot 30^0 + 17 \cdot 30 = 518$

$C_1 = m_1^e \pmod n \equiv 244^{11} \pmod{12600}$

$\equiv 244 \cdot (244^2)^5 = 244 \cdot 9136 \cdot (9136^2)^2$

$\equiv 244 \cdot (-3464) \cdot ((-3464)^2)^2$

$\equiv (-1016) \cdot (4096)^2 \equiv (-1016) \cdot (6616)$

$\equiv 6544 \pmod{12600}$

$6544 = 30 \cdot 218 + 4$

$= 30(30 \cdot 7 + 8) + 4$

$= 30^2 \cdot 7 + 30 \cdot 8 + 4$

$\Rightarrow C_1 = (7)(8)(4)_{(30)} = HIE$

$C_2 = m_2^e \pmod n = 518^{11} \pmod{12600}$

$= 518 \cdot (518^2)^{10} = 518 \cdot (3724^2)^5$

$= 518 \cdot 8176 \cdot (8176^2)^2 = 1568 \cdot (3976)^2$

$= 1568 \cdot 8176 = 5768 \pmod{12600}$

$5768 = 30 \cdot 192 + 8$

$= 30(30 \cdot 6 + 12) + 8$

$= 30^2 \cdot 6 + 3 \cdot 12 + 8$

$\Rightarrow C_2 = (6)(12)(8)_{(30)} = GM1$

C : HIEGM1

2) $n = 2733$

e - minim

$\sqrt{27 \cdot 33}$ | 52

25 | 102 · 2 = 204

= 233

204

29

$\Rightarrow [\sqrt{n}] = 52 = n'$

$t = 53$

$t^2 - n = (n'+1)^2 - n = (n'^2 - n) + 52 \cdot 2 + 1$

$= (-29) + 105 = 76$ - nu este pp.

$t = 52 + 2 = 54$

$t^2 - n = (-29) + 52 \cdot 2 \cdot 2 + 4 = 183$

$t = 54 + 1 = 52 + 3$

$t^2 - n = (-29) + 52 \cdot 2 \cdot 3 + 9 = 292$

$t = 52 + 4$

$t^2 - n = (-29) + 52 \cdot 2 \cdot 4 + 16 = 403$

$t = 52 + 5$

$t^2 - n = (-29) + 52 \cdot 2 \cdot 5 + 25 = 516$

$t = 52 + 6$

$t^2 - n = (-29) + 52 \cdot 2 \cdot 6 + 36 = 631$

$t = 52 + 7$

$t^2 - n = (-29) + 52 \cdot 2 \cdot 7 + 49 = 748$

$t = 52 + 8$

$t^2 - n = (-29) + 52 \cdot 2 \cdot 8 + 64 = 867$

$t = 52 + 9$

$t^2 - n = (-29) + 52 \cdot 2 \cdot 9 + 81 = 988$

$t = 52 + 10$

$t^2 - n = (-29) + 52 \cdot 2 \cdot 10 + 100 = 1111$

$t = 52 + 11$

$t^2 - n = (-29) + 52 \cdot 2 \cdot 11 + 121 = 1236$

$t = 52 + 12$

$t^2 - n = (-29) + 52 \cdot 2 \cdot 12 + 144 = 1363$

$n = (457+454)\cdot(457-454)$

$= 3 \cdot 911$

$p = 3 \quad q = 911$

$H = 30$

$j = 2 \quad l = 3$

~~OK~~

$f(n) = (p-1)(q-1) = 2 \cdot 910 = 1820$

$(l, f(n)) = 1 \;,\; l \in \{3, 4, \ldots, f(n)-1\}$

1820	2·5
182	2
91	7
13	13
1	

cum e - minim $\Rightarrow e = 3$

$m : OK = (14)(10)_{(30)} = 10 \cdot 30^0 + 14 \cdot 30 = 430$

$C = m^e \pmod n = 430^3 \pmod{2733}$

$= 430 \cdot 430^{\frac{3-1}{2}} = 430 \cdot 1789 = 1297$

$1297 = 30 \cdot 43 + 7 = 30(30+13) + 7$

$= 30^2 + 30 \cdot 13 + 7$

$\Rightarrow C : (1)(13)(7)_{(30)} = BHH$

3.a) $n = 187 \quad e = 107$

$\sqrt{187} \mid 13$

$1 \quad \mid 23 \cdot 3 = 69$

$\equiv 87$

69

$\star 8$

$[\sqrt{n}] = 13 = n'$

$t = n' + 1 = 13 + 1 = 14$

$t^2 - n = (-18) + 13 \cdot 2 + 1 = 9 = 3^2$

$\Rightarrow n = (14+3)(14-3) = 17 \cdot 11$

$p = 11 \quad q = 17$

$f(n) = (p-1)(q-1) = 10 \cdot 16 = 160$

$ed \equiv 1 \pmod{f(n)}$

$d \cdot 107 \equiv 1 \pmod{160}$

$d \equiv 107^{-1} \pmod{160}$

$160 : 107 = 1 \text{ rest } 53$

107

$= 53$

$X_{160} = (1, 0) \qquad X_{107} = (0, 1)$

$X_{53} = X_{160} - X_{107} = (1, -1)$

$107 : 53 = 2$ rest 1
106
$= = 1$

$$X_1 = X_{107} - 2X_{53}$$
$$= (0,1) - 2(1,-1)$$
$$= (-2,3)$$

$\Rightarrow d \equiv 3 \pmod{160}$

b)

ABACFPFP$_{(30)}$

$C_1 : AB_{(30)} = (0)(1)_{(30)} = 1 \cdot 30^0 = \Lambda$

$m_1' = C_1^d \pmod n$
$= 30^3 \pmod{187} = 30 \cdot 900 \pmod{187}$
$= 30 \cdot 152 = 72$

$72 = 30 \cdot 2 + 12$

$\Rightarrow m_1' = (2)(12)_{(30)} = CM$

$m_1' = 1^3 \pmod{187}$
$m_1' = B$

$C_2 : AC_{(30)} = (0)(2)_{(30)} = 2 \cdot 30^0 = 2$

$m_2' = C_2^d \pmod n = 60 \cdot 3600 \pmod{187}$
$= 15$

$m_2' = C$

$C_3 : FP_{(30)} = (5)(15)_{(30)} = 15 \cdot 1 + 5 \cdot 30 = 165$

$m_3' = C_3^d \pmod n = 165 \cdot 165^2 \pmod{187}$

$= 165 \cdot 110 \pmod{187} = 11$

$m_3' = L$

$C_4 : FP \Rightarrow m_4' = L$

$m' : BCLL$

4) $p = 7 \quad q = 11$, d-minim

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

$f(n) = 6 \cdot 10 = 60 = 2^2 \cdot 3 \cdot 5$ / $\Rightarrow d = 7$

d - minim

$ed \equiv 1 \pmod{f(n)}$

$e \cdot 7 \equiv 1 \pmod{60}$

$e \equiv 7^{-1} \pmod{60}$

$60 : 7 = 8$ rest 4

56

$= 4$

$X_{60} = (1, 0)$, $X_7 = (0, 1)$

$X_4 = X_{60} - 8 X_7 = (1, 0) - (0, 8) = (1, -8)$

$7 : 4 = 1$ rest 3

$X_3 = X_7 - X_4 = (0,1) - (1,-8) = (-1,9)$

$4 : 3 = 1$ rest 1

$X_1 = X_4 - X_3 = (1,-8) - (-1,9) = (2,-17)$

$\Rightarrow e \equiv -17 \pmod{60}$

$e \equiv 43 \pmod{60}$

b) B ! BTBL

$C_1 : B!_{(30)} = (1)(28)_{(30)} = 28 + 30 = 58$

$m_1' = C_1^d \pmod{n} = 58^7 \pmod{77} = 58 \cdot (58^3)$

$= 58 \cdot 53^3 \pmod{77} = 58 \cdot 53 \cdot 53^2 \pmod{77}$

$= 71 \cdot 37 \pmod{77} = 9$

$m_1' = J$

$C_2 : BT_{(30)} = (1)(19)_{(30)} = 19 + 30 = 49$

$m_2' = C_2^d \pmod{n} = 49^7 \pmod{77} = 49 \cdot (49^2)^3$

$= 49 \cdot 14^3 \pmod{77} = 49 \cdot 14 \cdot 14^2 \pmod{77}$

$= 70 \cdot 42 \pmod{77} = 14$

$m_2' = 0$

$C_3 : BL_{(30)} = (1)(11)_{30} = 11 + 30 = 41$

$m_3' = C_3^d \pmod n = 41^7 \pmod{77} = 41 \cdot (41^2)^3$

$= 41 \cdot 64^3 \pmod{77} = 41 \cdot 64 \cdot 64^2 \pmod{77}$

$= 6 \cdot 15 \pmod{77} = 13$

$m_3' : H$

$m : JOH$

5) $n = 1189 \quad e = 747$

$\sqrt{1189}$ | 34

9

289

256

33

$61 \cdot 1 = 256$

$[\sqrt{n}] = 34 = n'$

$t = n' + 1 = 34 + 1 = 35$

$t^2 - n = (n'^2 - n) + 34 \cdot 2 + 1 = (-33) + 69$

$= 36 = 6^2$

$\Rightarrow n = (35 - 6)(35 + 6) = 41 \cdot 29$

$\Rightarrow p = 29 \quad q = 41$

$\Rightarrow f(n) = (p-1)(q-1) = 40 \cdot 20 = 800$

$e \cdot d \equiv 1 \pmod{f(n)}$

$747 \cdot d \equiv 1 \pmod{800}$

$d \equiv 747^{-1} \pmod{800}$

$X_{800} = (1,0), \quad X_{747} = (0,1)$

$800 : 747 = 1$ rest 53

$\underline{747}$

$= 53$

$X_{53} = X_{800} - X_{747} = (1, -1)$

$747 : 53 = 14$ rest 5

$X_5 = X_{747} - 14 X_{53} = (-14, 15)$

$53 : 5 = 10$ rest 3

$X_3 = X_{53} - 10 X_5 = (141, -151)$

$5 : 3 = 1$ rest 2

$X_2 = X_5 - X_3 = (-155, 166)$

$3 : 2 = 1$ rest 1

$X_1 = X_3 - X_2 = (296, -317)$

$\Rightarrow d \equiv -317 \pmod{800}$

$d \equiv 483 \pmod{800}$

b) $N = 30$

$30^j \leq 1189 \leq 30^{j+1}$

$30^2 \leq 1189 \leq 30^3$

$900 \leq 1189 \leq 2700$

$\Rightarrow j = 2 \Rightarrow l = 3$

BFC AFN BIW

$C_1 : BFC_{(30)} = (1)(5)(2)_{(30)} = 2 + 5 \cdot 30 + 900$

$= 1052$

$m_1' = C_1^d \pmod{800}$

$= 1052^{483} \pmod{800} = 252^{483} \pmod{800}$

$= 252 \cdot (252^2)^{241} \pmod{800}$

$= 252 \cdot 304 \cdot (304^2)^{120} \pmod{800}$

$= 608 \cdot (416^2)^{60} \pmod{800} = 608 \cdot (256^2)^{30} \pmod{800}$

$= 608 \cdot (736^2)^{15} \pmod{800} = 608 \cdot 96 \cdot (96^2)^7 \pmod{800}$

$= 768 \cdot 416 \cdot (416^2)^3 \pmod{800} = 288 \cdot 256 \cdot 256^2$

$= 128 \cdot 736 \pmod{800} = 608 \pmod{800}$

$608 = 30 \cdot 20 + 8$

$m_1' = (20)(8)_{(30)} = UI$

$C_2 : AFH_{(30)} = (0)(5)(13)_{(30)} = 13 + 5 \cdot 30 = 163$

$m_2' = C_2^{\,d} \pmod n = 163^{483} \pmod{800}$

$= 163 \cdot (163^2)^{241} \pmod{800} = 163 \cdot (169^2)^{120} \pmod{800}$

$= 163 \cdot (561^2)^{60} \pmod{800} = 163 \cdot (321)^{30} \pmod{800}$

$= 163 \cdot (641^2)^{15} \pmod{800} = 163 \cdot 481 \cdot (481^2)^{7} \pmod{800}$

$= 3 \cdot 161 \cdot (161^2)^3 \pmod{800} = 483 \cdot 321 \cdot 321^2$

$= 643 \cdot 641 \pmod{800} = 163 \pmod{800}$

$163 = 30 \cdot 5 + 13$

$m_2' = (5)(13)_{(30)} = FH$

$C_3 : BIH_{(30)} = (1)(8)(22)_{(30)} = 22 + 8 \cdot 30 + 900$

$= 1162$

$m_3' = C_3^{\,d} \pmod n = 1162^{483} \pmod{800}$

$= 362 \cdot (362^2)^{241} \pmod{800}$

$= 362 \cdot 644 \cdot (644^2)^{120} \pmod{800}$

$= 328 \cdot (336^2)^{60} \pmod{800} = 328 \cdot (96^2)^{30} \pmod{800}$

$= 328 \cdot (416^2)^{15} \pmod{800} = 328 \cdot 256 \cdot (256)^7$

$= 768 \cdot 736 \cdot (736^2)^3 \pmod{800} = 448 \cdot 96 \cdot 96^2$

$= 608 \cdot 416 \pmod{800} = 128 \pmod{800}$

$128 = 30 \cdot 4 + 8$

$m_3 = (4)(8)_{(30)} = EI$

m: UIFNEI

6) j=1, l=2, p=23, q=17, e=3

a) $n = p \cdot q = 391$

HELP_ME!

$C_1 = m_1^e \pmod{n} = 7^3 \pmod{391} = 343 \pmod{391}$

$343 = 30 \cdot 11 + 13$

$C_1 : (11)(13)_{(30)} = LN$

$C_2 = m_2^e \pmod{n} = 4^3 \pmod{391} = 64 \pmod{391}$

$64 = 30 \cdot 2 + 4$

$C_2 : (2)(4)_{(30)} = CE$

$C_3 = m_3^e \pmod{n} = 11^3 \pmod{391} = 1331 \pmod{391}$

$= 158 \pmod{391}$

$158 = 30 \cdot 5 + 8$

$C_3 = (5)(8)_{(30)} = FI$

$C_4 = m_4^{\ell} (\text{mod } n) = 15^3 (\text{mod } 391) = 3375 (\text{mod } 391)$

$= 247$

$247 = 30 \cdot 8 + 7$

$C_4 = (8)(7)_{(30)} = IH$

$C_5 = m_5^{\ell} (\text{mod } n) = 26^3 (\text{mod } 391) = 17576 (\text{mod } 391)$

$= 372 (\text{mod } 391)$

$372 = 30 \cdot 12 + 12$

$C_5 = (12)(12)_{(30)} = MM$

$C_6 = m_6^{\ell} (\text{mod } n) = 12^3 (\text{mod } 391) = 1728 (\text{mod } 391)$

$= 164 (\text{mod } 391)$

$164 = 30 \cdot 5 + 14$

$C_6 = (5)(14)_{(30)} = FO$

$C_7 = C_2 = CE$

$C_8 = m_8^{\ell} (\text{mod } n) = 28^3 (\text{mod } 391) = 21952 (\text{mod } 391)$

$= 56 (\text{mod } 391)$

$56 = 30 + 26$

$C_8 = (1)(26)_{(30)} = B-$

C: ΔHCEFIIHMMMFOCEB-

b) $f(n) = (p-1)(q-1) = 22 \cdot 16 = 352$

$ed \equiv 1 \pmod{f(n)}$

$3 \cdot d \equiv 1 \pmod{352}$

$d \equiv 3^{-1} \pmod{352}$

$352 : 3 = 117$ rest 1

3
=5

3
=2

21
=1

$1 = 352 - 117 \cdot 3 \Rightarrow d \equiv -117 \pmod{352}$

$d \equiv 235 \pmod{352}$

EBMMAAF_OMML!EBAIHI

$C_1 = EB_{(30)} = (4)(1)_{(30)} = 1 + 30 \cdot 4 = 121$

$m_1' \equiv C_1^{d} \pmod{n} = 121^{235} \pmod{391} = 8$

$m_1' = 1$

$C_2 = MM_{(30)} = 12 + 12 \cdot 30 = 372$

$m_2' = C_2^d \pmod n = 372^{235} \pmod{391} = 26$

$m_2' = \_$

$C_3 = AA_{(30)} = 0$

$m_3' = A$

$C_4 = F\leftarrow_{(30)} = 26 + 30 \cdot 5 = 176$

$m_4' = C_4^d \pmod n = 176^{235} \pmod{391} = 30 \pmod{391}$

$m_4' = A$

$C_5 = OM_{(30)} = (14)(12)_{(30)} = 12 + 14 \cdot 30 = 432$

$m_5' = C_5^d \pmod n = 432^{235} \pmod{391} = 303$

7) $n_1 = 9991 \quad l_1 = 3917$

a)

$\sqrt{9991}$	99
81	$189 \cdot 9 = 1701$
1891	
1701	
190	

$[\sqrt{n}] = 99 = n'$

$t = n' + 1 = 100 = 99 + 1$

$t^2 - n = (n'^2 - n) + 99 \cdot 2 + 1 = (-190) + 199 = 9 = 3^2$

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

$p = 97 \quad q = 103$

$\varphi(n) = (p-1)(q-1) = 96 \cdot 102 = 9996$

$ed \equiv 1 \pmod{\varphi(n)}$

$d \cdot 3917 \equiv 1 \pmod{9996}$

$d \equiv 3917^{-1} \pmod{9996}$

$9996 : 3917 = 2 \text{ rest } 2162$

$X_{9996} = (1,0), \quad X_{3917} = (0,1)$

$X_{2162} = X_{9996} - 2 \cdot X_{3917} = (1,-2)$

$3917 : 2162 = 1 \text{ rest } 1755$

$X_{1755} = X_{3917} - X_{2162} = (-1,3)$

$2162 : 1755 = 1 \text{ rest } 407$

$X_{407} = X_{2162} - X_{1755} = (2,-5)$

$1755 : 407 = 4 \text{ rest } 127$

$X_{127} = X_{1755} - 4X_{407} = (-9,23)$

$407 : 127 = 3 \text{ rest } 26$

$X_{26} = X_{407} - 3X_{127} = (29, -74)$

$127 : 26 = 4$ rest 23

$X_{23} = X_{127} - 4X_{26} = (-125, 319)$

$26 : 23 = 1$ rest 3

$X_3 = X_{26} - X_{23} = (154, -393)$

$23 : 3 = 7$ rest 2

$X_2 = X_{23} - 7X_3 = (-1203, 3070)$

$3 : 2 = 1$ rest 1

$X_1 = X_3 - X_2 = (1357, -3463)$

$d \equiv -3463 \pmod{9996}$

$d \equiv 6533 \pmod{9996}$

b) $l = 3$, $j = 2$

BMHA - X

$C_1 = BMH_{(30)} = (1)(12)(7)_{(30)} = 7 + 12 \cdot 30 + 900$

$= 1267$

$m_1' \equiv C_1^{\,d} \pmod{n} \equiv 1267^{6533} \pmod{9991}$

$= 404 \pmod{9991}$

$404 = 30 \cdot 13 + 14$

$m_1' = (13)(14)_{(30)} = HO$

$C_2 = A - X_{(30)} = (0)(26)(23)_{(30)} = 23 + 26 \cdot 30$

$= 803$

$m_2' = C_2^{\,d} \pmod{n} = 803^{6533} \pmod{9991}$

$= 570 \pmod{9991}$

$570 = 30 \cdot 19$

$m_2' = (19)(0)_{(30)} = TA$

m: NOTA