(7) RSA

Chapter - 4

$m = p' \phi q'$

$\phi(m) = 1P$

$m = pq$

$m = 377$

$k = 139$

gcd (377, 139)

p   q

13   29

$(p-1)$ $(q-1)$

$\phi(m) = (13-1) \times (29-1)$

$= 12 \times 28 = 336$.

13
29
117
26×
377

K.

~~K d = 139~~

$Kd = 1 \bmod \phi m$

$139d = 1 \bmod 336$

d = mod pm.

$336 = 2 \times 139 + 58$

$139 = 2 \times 58 + 23$

$58 = 2 \times 23 + 12$

$23 = 1 \times 12 + 8$

$12 = 1 \times 8 + 4$

$8 = 2 \times 4 + 0$

4 =

139
3
417

139
2
278

58
2
116

58
3
174

$50x \equiv 100 \bmod 236$

$\overset{a}{56}x + \overset{b}{236}y = 100$

$\gcd(56, 236) = 4$

$236 = 4\times56 + 12$

$56 = 4\times12 + 8$

~~$12 = 1\times10 + 2$~~

~~$10 = 5\times2 + 0$~~

$2 = 12 = 1\times8 + 4$

$8 = 2\times4 + 0$

$4 = 12 - 8\times1 = (~~56\times4~~)$

$= 12 - \{56 - (4\times12)\}$

$= 12 - \{56 - (236 - (4\times56))\}$

$\rightarrow 12 - 56 + 4\times12$

$\Rightarrow 5\times12 - 56$

$\Rightarrow 5(236 - 4\times56) - 56$

$\Rightarrow 5\times236 - 21\times56$

50) 236 (4
200
36) 50 (1
36
14) 36 (2
28
8) 14 (1
8
6) 8 (1
6
2)

$12\times4 = 48$

$56\times2 = 112$

$56\times3 = 168$

$56\times5 = 280$

$56\times4 = 224$

$224 + 12 = 236$

$4 = 12 - 8 \times 1$

$= 12 - \left((56 - 4 \times 12)\ 1\right\}$

$= 12 - (1 \times 56) + (4 \times 12)$

$=$ ~~12~~

$=$ ~~236 - (4×56)~~

$= 12 - (1 \times 56) - (4 \times 12)$

$= 1 \times 12 - 4 \times 12 - 1 \times 56$

$= -3\,(12) - 1 \times 56$

$= -3\,[(236 - 4 \times 56)] - 1 \times 56$

$= -3 \times 236 + 3 \times 4 \times 56 - 1 \times 56$

$= -3 \times 236 - 11 \times 56$

Chapter - 3

smallest positive integer.

(1) 2014^{16} mod 17.

$a^{p-1} = 1 \bmod p.$

2014^{16} mod 17.

(ii) 57^{102} mod 101

$a^{101-1} = 1 \bmod 101$

$a^{100} = 1 \bmod 100$

$1)101(1$
11
$10)$

19

2

$\begin{array}{r} 198 \\ 4 \\ \hline 792 \end{array}$

(iii) 2^{600} mod (199).

$a^{p-1} = 1 \bmod \boxed{p}$

$2^{199-1} = 1 \bmod 199$

$2^{198} = 1 \bmod 199$

$\begin{array}{r} 198 \\ 3 \\ \hline \end{array}$

$2^{6} \equiv \bmod 199$

2^6 mod 199

~~= 64 mo~~

$= \underline{64}$ mod 199

Chapter 4

Sucesive squaring!

(i) 7^{32} mod 101

(ii) 7^{11} mod 101

(iii) 7^{152} mod 101

$101 \overline{)6084} (6$
606
24

$2 \overline{)32} (16$
2
11
12

32 → binary

2 | 32 - 0
2 | 16 - 0
2 | 8 → 0
2 | 4 → 0
2 | 2 → 0
1

$2 \overline{)4} (2$
4
0

1 00000

∴ 7^{32} can be repeated. -)

32 ~~32~~ 16 8 4 2 1
1 0 0

sossive

$7^1 = 7$ mod 101

$7^2 = 7 \cdot 7 = 49$ mod 101

$7^4 = 49 \cdot 49 = \cdot 2401$ mod 101

$\therefore 2401 \div 101 = 23$ remaindr 78

so $7^4 = 78$ mod 101

$7^8 =$ ~~2401 · 2.1~~
$78 \cdot 78 = 6084$ mod 101

= 60 remainder 24

= 24 mod 101.

$7^{16} = 24 \cdot 24.$

$101 \overline{)2401} (23$
202
381
303
78.

$2 \overline{)5} (2$
4
1

$2 \overline{)91} (2$
4
1

$\boxed{}$ 7^{41} mod 101

91 = 101001

$= 7^{32} \cdot 7^8 \cdot 7^1$

2 | 41 - 1
20 - 1

$2 \overline{)91} (2$
4
1

91
32 16 8 4 2 1
1 0 1 0 0 1

: Sucesive Sauaring

$7^1 = 7 \bmod 101$

$7^2 = 49 \bmod 101$

$7^4 = 78 \bmod 101$

$7^8 = 24 \bmod 101$

$7^{16} = 71 \bmod 101$

$7^{32} = 92 \bmod 101$

combine using binary decomposition:

$7^{41} = 7^{32} \cdot 7^8 \cdot 7^1$

$= (92 \cdot 24 \cdot 7) \bmod 101$

$92 \cdot 24 = 2208$ $2208 \div 101 = 21$ remainder $87 = 87 \bmod 101$

$87 \cdot 7 = 609$ $609 \div 101 = 6$ remaind $3 = 3 \bmod 101$

$7^{4} \bmod 101 = 3$

Smallest integer:

$n^{17} \equiv 10 \bmod 29$

(1) check 29 is prime

$n^{28} \equiv 1 \bmod 29$

Need to find modular inverse 17 mod 28.

$17x = 1 \bmod 28$.

EEE

$28 = 1 \times 17 + 11$

$17 = 1 \times 11 + 6$

$11 = 1 \times 1 + 5$

$6 = 1 \times 5 + 1$

$5 = 5 \times 1 + 0$

$1 = 6 - 1.5$

$= 6 - 1(11 - 6.1)$

~~$= 6.1 - 6.11 - 6.1$~~

$= 6.1 - 1.11 + 6.1$

$= 2.6 - 1.11$

$= 2.6 - 1.(28 - 17)$

$\equiv$

$1 = 5.17 . 3.28$

$\therefore 17^{-1} = \underline{5} \bmod 28.$

$\boxed{17}^{5}$

$(n^{17})^5 = 10^5 \bmod 29$

$n = 10^5 . \bmod 29$

Compute $10^5 \bmod 29$

$10^2 = 100 \bmod 29$

$100 \div 29 = 3$ remaindr 13 $10^2 = 13 \bmod 29$

$10^4 = 13 . 13 = 169 \bmod 29.$

$169 \div 29 = 5$ remaindr $24 = 24 \bmod 29$

$10^5 = 10.4 . 10 = 24.10 = 240 \bmod 29$

$= 240 \div 29 = 8$ remaindr 8 $10^5 = 8 \bmod 29.$

$n = 8 \mod 29.$

~~Chap~~

RSA :-

d = private key

k = public key.

m ~~n~~ $= p \times q$

$\varphi(m) = (p-1)(a-1)$

$m = 377 \quad k = 139.$

$\gcd(377, 139)$

$377 = 13 \times 29$

$\varphi m = (13-1)(29-1)$

☑ Chapter 3

smallest positive integer.

(1) 2014^{16} mod 17.

2014 ÷ 17 = 118 remainder. 10 $\quad$ 17)2014(

2019 = 10 mod 17. $\quad$ 2).

⇒ $2019^{16} \equiv 10^{16}$ mod 17. $\quad$ $a^{p-1} \equiv 1$ mod p

fermates theory $\quad$ p = 101

a = 57.

$a^{p-1} \equiv 1$ mod p $\quad a \not\equiv 1$'

$57^{100} \equiv 1$ mod 101

a = 10 $\quad$ p = 17

2016^{16} mod 17 = 1

101x'

(11) 57^{102} mod 101 = 17.

here 57 < 101.

57 ≡ 57 mod 101

$57 = 57^{100} . 57^{2}$

$57^{102} \equiv 1 . 57^{2}$ mod 101.

$57^{2} = 3249$

$3249 \div 101 = 32$ Remai 17

$57^{2} = 17$ mod 101.

$\therefore 57^{102}$ mod $101 \equiv 17$

4) Smallest positive integer.

2^{600} mod 199

199 টিক করলে
600 আসবে.

a^{p-1} = ~~p mod~~ 1 mod P

199 × 7

$a = 2$
$P = 199$

$2^{597} . 2^{2} . 2^{2}$

$\therefore 2^{600} = \left(2^{198}\right)^{3} . 2^{6}$

= ?

$2^{600} = 2^{6}$ mod 199

$2^{6} = 64$

64 mod $199 = 2^{6}$

$\therefore 2^{6} = 64$

(Ans)

Pri:

① Find $\phi((60))$ then calculate 7^{50} mod 60.

$2\,|\,60$

$2\,|\,30$

$3\,|\,15$

5

$\phi(60) = 2^2 \cdot 3^1 \cdot 5^1$

$= \phi(2^2 - 2^1) \cdot (3^1 - 3^0)(5^1 - 5^0)$

$= 2^1 .$

$= (4-2) \cdot (3-1)(5-1)$

$= 2.2.4$

$= 16$

49 mod 60

7^{50} mod 60

$(7, 50) = 1$

$7^{50} = 7^{16} \cdot 7^{16} \cdot 7^{16} \cdot 7^2 = 7^{48} \cdot 7^2 =$

[illegible] $\phi(1001)$ Calculate 2^{7927} mod 1001

$$\begin{array}{r|l} 7 & 1001 \\ \hline 11 & 143 \\ \hline & 13 \end{array}$$

$\phi(1001) = \phi(7^1 \cdot 11^1 \cdot 13^1)$

$= (7^1 - 7^0)(11^1 - 11^0)(13^1 - 13^0)$

$= (7-1)(11-1)(13-1)$

$= 6 \cdot 10 \cdot 12$

$= \underline{\underline{720}}$ $720 \mid 1001$

2^{7927} mod 1001

$720 \div 1001 = \underline{17}$ remainder $\underline{7}$

$(7927, 1001) = 1$

$\therefore 2^{7927} = 2^{7}$ mod 1001

$2^{7927} = 1001 \overline{)7927} 7$
$$\begin{array}{r} 7007 \\ \hline 920 \end{array}$$

Compute 2^7.

$2^7 = 128$ mod 1001.

128.

Find $\phi(1001)$, then calculate 2^{7927} mod 1001.

$$7 \,|\, 1001 \qquad 11 \,|\, 143 \qquad 13$$

$1001) = 7^1 . 11^1 . 13^1$

$= \phi(7^1) . \phi(11)\, \phi(13)$

$= \phi(7^1 - 7^0)\, \cancel{\phi}\, \phi(11^1 - 11^0)\, \phi(13^1 - 13^0)$

$= (7-1)\,(11-1)\,(13-1)$

$= 6 \times 10 \times 12$

$= 720.$

$2 \times 2 \ldots 128$

$2 \times 2 \times 2 \times 2 \times 2 \times 2 \times 2$

$\therefore\ 2^{7927}$ mod 1001

gcd$(2, 1001) = 1$

$= 2^{11 \times 720} . 2^{7}$

$= 2^{7920} . 2^{7}$

$= 1 . 2^{7}.$

128 mod 1001

$\boxed{2^{7927}} = 2^{720} . 2^{720} . 2^{720}$

$2^{720} . 2^{720} . 2^{720} . 2^{720} . 2^{720} . 2^{720}$

$2^{720} . 2^{720}$

$2^{198} \bmod 199 = \boxed{1}$

600

$$2^{600} = 2^{198} \times 2^{198} \times 2^{199} \times 2^{6}$$

$$= 2^{198+198+198+6}$$

$$= 1 \times 1 \times 1 \times 2^{6}$$

$$= 64 \bmod 199$$

4. Problem 2:-

(1) Find $\phi(60)$, then calculate $7^{50} \bmod 60$.

$$\phi 60 = \phi(2^2 \cdot 3^1 \cdot 5^1)$$

$$= \phi(2^2) \cdot \phi(3^1) \cdot \phi(5^1)$$

$$= (2^2 - 2^1) \cdot (3^1 - 3^0)(5^1 - 3^0)$$

$$= (4-2) * (3-1) * (5-1)$$

$$= 2 \cdot 2 \cdot 4$$

$$= 16$$

$$\begin{array}{r|l} 2 & 60 \\ \hline 2 & 30 \\ \hline 3 & 15 \\ \hline 5 & 5 \\ \hline & 1 \end{array}$$

$7^{50} \bmod 60$

22
16
8

$\gcd(7, 60) = 1$.

$$7^{50} = 7^{16} \cdot 7^{16} \cdot 7^{16} \cdot 7^{2}$$

$$= 7^{48} \cdot 7^{2}$$

$$= 1 \times 7^{2} = 49 \bmod 60$$

⊞ $n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)$ .... we get.

$\phi 84 = 84\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)\left(1-\frac{1}{7}\right)$

$= 84 \cdot \frac{1}{2} \cdot \frac{2}{3} \cdot \frac{6}{7}$

$= 84 \cdot \frac{12}{42} = 24$

⊞ $A = \{1, 5, 7, 11\}$

$B = \{1, 2, 3, 4, 5, 6\}$

$\phi(12) = 4$

$\phi(7) = 6.$

$x = a \bmod 12$

$x = b \bmod 7$

$\phi(12) = 2^2 \cdot 3$

$\phi(12) = 12\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right) = 12 \cdot \frac{1}{2} \cdot \frac{2}{3} = 4$

$\phi(7) = 7 \cdot \left(1-\frac{1}{7}\right) = 7 \cdot \frac{6}{7} = 6$

Verifying: $\phi(84) = \phi(12) \cdot \phi(7)$

$= 4 \cdot 6 = \phi = 24$ ∴

$\phi(84) = \phi(12)\phi(7).$

$-12)$

1

4] $x \equiv 1 \mod 7$

$x \equiv 3 \mod 11$

$x \equiv 5 \mod 13$

$m_1 \quad m_2 \quad m_3$

$M = 7 \times 11 \times 13$

$= 1001$

$$M_i = \frac{m_1 m_2 m_3}{m_i}$$

$$= \frac{1001}{3}$$

$M_1 = 11 \times 13 = 33 \quad 143$

$M_2 = 7 \times 13 = 91$

$M_3 = 7 \times 11 = 77$

$N_i = (M_1 \times N_1)\, a_1 \mod M + (M_2 \times N_2)$

$a_2 \mod M + (M_3 \times N_3)\, a_3 \mod M$

$M_i N_i = 1 \mod m_i$

$\bar{N_1} =$

$M_1 N_1 = 1 \mod m_1$

$\Rightarrow 143 N_1 = 1 \mod 7$

$= 2$

N_2

$M_2 N_2 = 1 \mod m_2$

$\Rightarrow 143 N_2 = 1 \mod 13$

$= 4$

$N_3 \quad M_3 N_3$

$N_3 = -1$

Non linea - 1.3 (3)

$3x = 5 \bmod (8)$

$7x = 9 \bmod (17)$

$11x = 17 \bmod (25)$.

$M =$

$3x \cdot 3 \equiv 5 \cdot 3 \ (8)$

$\Rightarrow \underline{9x} = \underline{15 \ (8)}$

$\Rightarrow x = 7 \bmod 8$.

$(3, 8) = 1$

$8 \mid 15 \mid 1$
8
7.

$7x = 9 \bmod (17)$

$5 \times 7 = 5 \times 9 \bmod 17$

$\Rightarrow 35 = 45 \bmod 17$

$\Rightarrow x = 11 \bmod 17$.

$17 \mid 45 \mid 2$
34
11.

$11x = 17 \bmod 25$

$25 \mid 187 \mid$
175

$\Rightarrow 77$

$\boxed{4}$ $5x + 7y = 23$.

$\Rightarrow 5u + 7v = 1$

$5(3) + 7 \cdot (-2) = 1$

$= 15 - 14 = 1$.

$5(\underset{x_0}{69}) + 7(\underset{y_0}{-46}) = 23$.

$x_0 = 69$

$y_0 = -46$ $\quad x_k = 69 + k$

$y_k = -46 - k$.

$x_k = 69 + k \frac{7}{1}$

$y_k = -1 - k \frac{5}{1}$.

$3x + 8y = 5$.

$a = 8 \quad b = 3$

$y = 0$

$3x + 8 \cdot 0 = 5$

$3x = 5 + 8 \cdot 0$

$\Rightarrow 3x =$

$x = 4 \bmod 7$

$x = 8 \bmod 11$

$x = 10 \bmod 13$

$M = m_1 \times m_2 \times m_3$

$= 7 \times 11 \times 13$

$= 1001$

$$M_i = \frac{m_1 m_2 m_3}{m_i}$$ m_i - 3 eqn numbers

$$= \frac{1001}{3}$$

$M_1 = 11 \times 13 = 143$

$M_2 = 7 \times 13 = 91$

$M_3 = 7 \times 11 = 77$

N_1

$7)143(21$
14
3

$11)91($
90
1

$$N_i = \left(\overset{143}{M_1} \times N_1\right) \overset{4}{a_1} \bmod \overset{1001}{M} + \left(\overset{91}{M_2} \times N_2\right) \overset{8}{a_2} \bmod \overset{1001}{M} + \left(\overset{77}{M_3} \times N_3\right) \overset{10}{a_3} \bmod \overset{1001}{M}$$

$=$

$M_i N_i \equiv 1 \mod m_i$

$n=1$

$M_1 N_1 \equiv 1 \mod m_1$

$143 \times N_1 \equiv 1 \mod 7$

$N_1 = -2 \leftarrow$

$\gcd(143, 7)$ $143x + 7y = 1$

$(143, 7) = 1$

$2)143(2$ 14 $3)7(2$ 6 1

$M_2 N_2 \equiv 1 \mod m_2$

$91 N_2 : 1 \mod 11$

$N_2 = 4$

$11)91(8$ 88 $2)11(5$ 10 1

$M_3 N_3$

$= 1 \mod m_3$

$= 77 N_3$

$= 1 \mod 13$

$N_3 = -1.$

$= (143 \times (-2)) \mod 1001 + (91 \times 4) \mod 1001$

$+ (77 \times (-1)) \mod 1001$

$M3$

$= 4x - 286 + 8x364 - 77 \times 10 \mod 1001$

$\Rightarrow$

$=$ ~~1 mod 1001~~

$= -1144 + 2912 - 770$

$= 998 \mod 1001.$

$7)143(2$ 14 3

$143x + 7y = 1$

x

$143 =$

~~(2) $\boxed{57^{102} \text{ mod } 101}$~~

~~$a^{P-1} = 1 \text{ mod } (P)$~~

~~$a\,\cancel{e2}^{101} = 1 \text{ mod } (102)$~~

~~=> smallest is 1.~~

$57 \overline{)102} (1$
$\underline{57}$
$\underline{\underline{45}}$

57
$\underline{2}$
114

$\underline{\underline{2}}$ $57^{\underline{102}}$ mod 101

$101 = P-1$ ✗

↓

$P-1 = 101-1 = 100$

$a^{P-1} = 1 \text{ mod } P$

$\Rightarrow a^{100} = 1 \text{ mod } 101$

$\underline{57^{100} = 1 \text{ mod } 101.}$

$\underline{57^{100} \text{ mod } 101} = 1$ ✓

$57^2 \times \underline{57^{100}}$

$57^2 \times 1$

$\Rightarrow (57)^2 = \underline{3249 \text{ mod } 101}$

$\Rightarrow 3249 = 3249 \text{ mod } 101$

$\Rightarrow 3249 \div 101 = \underline{32}$ remaind. 17

$\therefore 17 \text{ mod } 101$

$101 \,|\, 3249 \,|\, \underline{32}$
300
249
$\underline{200}$
49

$6x = 4 \bmod \boxed{10}$ $\rightarrow$ gcd (6, 10) = $\boxed{2}$ $\underline{\text{no. of sol}^n}$

$6x + 10y = 4$ $\qquad 6x + 10y = 4$

$\underset{a}{6}x + \underset{b}{10}y = 4$

gcd (a, b) - gcd (6, 10) = 2 - you $\underline{\text{have}}$ $\underline{2 \text{ sol}^n}$.

Euclid Algo

$\underline{b} = 6 \times 1 + 4$

$\overset{-b}{10} = \overset{a}{6} \times \overset{\text{value}}{\boxed{1}} + 4$

$\Rightarrow 10 = 10$

$10 = (\cancel{6} + 4$

$\Rightarrow 10(-1) = 6(-1) + 4(-1)$

$\Rightarrow -10 = -6 - 4$

$\Rightarrow \underline{-10} = -\underline{10}$ $\quad \underline{(-1)}$ divident = 9

what/ val?/

$6x = 4 \bmod 10$

$\boxed{3}x = 2 \bmod 10$

~~10 = 6×1 + 4~~

$\boxed{10} = 1 \times \boxed{6} + 4$ $\quad$ di × r

$d = q \times$

$10 = 1 \times 6 + 4$

$6 = 1 \times 4 + \boxed{2}$ $\rightarrow$ ~~gcd~~ $\boxed{1}$

$4 = 2 \times 2 + \boxed{0}$

$a = 2 \times 1 + \boxed{2}$

$d =$

Q4] $x^3 \equiv 1 \bmod 7$

find the values $(0<x\le 7)$.

Here the test .

For $x=0$

$0^3 = 0 = 0 \bmod 7$

$x=1$

$1^3 = 1 \equiv 1 \bmod 7$

$x=2$

$2^3 \equiv 8 \bmod 7$

$x=3$

$3^3 = 27 = 6 \bmod 7$

7) 27 (3
21
6

$x=4$

$4^3 \equiv 64 \equiv X$ 1 mod 7

7 | 64 | 12.
7
14
14

7) 64 (1.
72
1

$x=6$

$4^3 = 64 \equiv 1 \bmod 7$

$x=5$

$5^3 = 125 = 6 \bmod$

$x=$ 7 (125) 1.
7
55
49
6

যেগুলো 1 ওইগুলো

Sol^n