RSA Algorithm:

1. $P=7$, $q=13$, $e=5$, $M=10$.

1. Key Generation:

$n = P \times q$

$= 7 \times 13$

$n = 91$

$\phi(n) = (P-1)(q-1)$

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

$= 6 \times 12.$

$\phi(n) = 72.$

$GCD(\phi(n), e) = 1]$.

$GCD(72, 5) = 1$

$e = 5.$

$d = e^{-1} \bmod (\phi(n)]$

$= 5^{-1} \bmod 72.$

$72 \times 1 = 72 * 1 \bmod 5$

$72 = 73 \bmod 5 \neq 0$

$72 \times 2 = 144 + 1 \bmod 5$

$= 145 \bmod 5$

$= 29$

$d = 29.$

$PU - \{e, n\} = \{5, 91\}$

$PR = \{d, n\} = \{29, 91\}.$

Encryption:

$C = M^e \bmod n$

$= 10^5 \bmod 91$

$= (10^2 \times \cancel{10^2} \times 10) \bmod 91$

$10^2 \Rightarrow 10^2 \bmod 91$

$\Rightarrow 9.$

$= (9 \times 9 \times 10) \bmod 91$

$\boxed{C. = 82.}$

8

91 | 810

728

82

Decryption:

$M = C^d \bmod n.$

$= 82^{29} \bmod 91.$

$82 \bmod 91 = 82$

$82^2 \bmod 91 = (82 \times 82) \bmod 91$

$= 6724 \bmod 91$

$= 81$

$82^4 \bmod 91 = (82^2 \times 82^2) \bmod 91$

$= (81 \times 81) \bmod 91$

$= 6561 \bmod 91$

$= 9.$

$82^8 \bmod 91 = (82^4 \times 82^4) \bmod 91$

$= (9 \times 9) \bmod 91$

$= 81 \bmod 91$

$= 81.$

$82^{16} \bmod 91 = (82^8 \times 82^8) \bmod 91$

$= (81 \times 81) \bmod 91$

$= 9.$

$82^{29} \bmod 91 = (82^{16} \times 82^8 \times 82^4 \times 82) \bmod 91$

$= (9 \times 81 \times 9 \times 82) \bmod 91$

5912 $= 10$

$\boxed{M = 10}$

17/5

1 Given two prime numbers, $p = 17$, $q = \cancel{1}7$,

$e = 5$, $n = 119$, $M = 6$.

Solution:

Key Generation:

$n = p \times q = 17 \times 7 = 119$

$\phi(n) = (p-1)(q-1)$.

$= (17-1)(7-1)$.

$= 16 \times 6$

$\phi(n) = 96$

$GCD(\phi(n), e) = 1$.

$GCD(96, 5) = 1$

$e = 5$

$d \equiv e^{-1} \bmod \phi(n)$

$= 5^{1} \bmod 96$

$96 \times 1 = 96 + 1 \bmod 5 \neq 0$.

$96 \times 2 = \frac{1988+1}{5} \neq 0$

~~96x3~~ $96 \times 3 + 7 \frac{289}{5} \neq 0$

$96 \times 4 = 384 + 1 = \frac{385}{5} = 77$.

$d = 77$.

$PU = \{e, n\} = \{5, 119\}$, $PR = \{d, n\} = \{77, 119\}$.

Encryption:

$C = M^e \bmod n$

$= 6^5 \bmod 119$.

$6^2 \bmod 119 = 36$.

$6^4 \bmod 119 = (6^2 \times 6^2) \bmod 119$

$= (36 \times 36) \bmod 119$

$= 1296 \bmod 119$

$= 106$.

$6^5 \bmod 119 = (6^4 \times 6) \bmod 119$

$= (106 \times 6) \bmod 119$

$= 636 \bmod 119$.

$\boxed{C = 41}$

Decryption:

$M = C^d \bmod n$.

$= 41^{77} \bmod 119$

$41^2 \bmod 119 = (41 \times 41) \bmod 119$

$= 1681 \bmod 119$

$= 15$.

$1681 \div 119$

$= 14.12 \ldots \rightarrow 14$

$= 0.1260 \times$

$= 15$

$41^{4} \bmod 119 = (41^{2} \times 41^{2}) \bmod 119$

$= (15 \times 15) \bmod 119$

$= 225 \bmod 119$

$= 106.$

$41^{8} \bmod 119 = (41^{4} \times 41^{4}) \bmod 119$

$= (106 \times 106) \bmod 119$

$= 11236 \bmod 119$

$= 50$

$41^{10} \bmod 119 = 41^{8} \times 41^{2} \bmod 11$

$= (50 \times 15) \bmod 119$

$= 750 \bmod 10$

$=$

$$\begin{array}{r|l} & \ \ 6 \\ 119 & 750 \\ & \underline{714} \\ & \ \ 36 \end{array}$$

$41^{15} \bmod 119 = (41^{10} \times 41^{4} \times 41)$

$= 36 \times 106 \times 41$

$= 156456 \bmod 119 = 90$

$41^{30} \bmod 119 = (41^{15} \times 41^{15})$

$= (90 \times 90) \bmod 119 = 8100 \bmod 119$
$= 8$

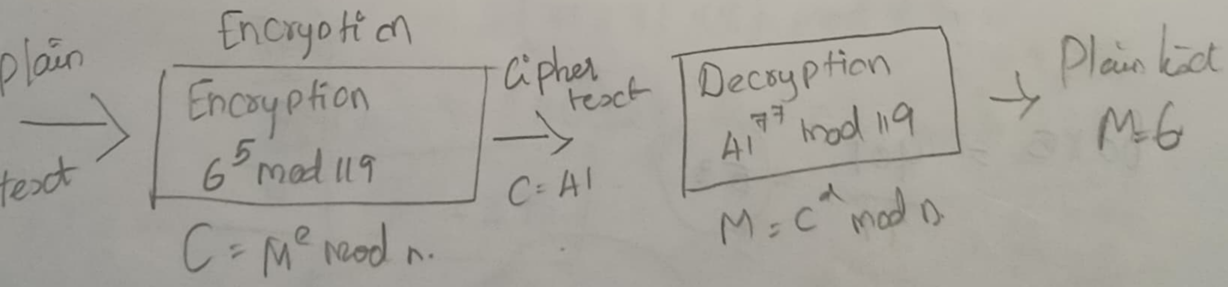
$41^{77} \bmod 119 = (41^{30} \times 41^{30} \times 41^{15} \times 41^{2}) \bmod 119$

$= (8 \times 8 \times 90 \times 15) \bmod 119.$

$= 86400 \bmod 119.$

$= 6.$

$M = 6$



③ $P=7, q=11, e=17, M=8$

PU PT

$n = P \times q$

$= 7 \times 11$

$\boxed{n = 77}$

$\phi(Pq) = (P-1)(q-1)$

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

$= 6 \times 10$

$\phi(Pq) = 60$

$\boxed{GCD(\phi(n), e) = 1}$

$GCD(60, e) = 1$

$e = 17$

Pr $\boxed{d \equiv e^{-1} \bmod \phi(n)}$

$= 17^{-1} \bmod \underline{60}$

17 mod 60 =

$\frac{17}{60}$

$60 \times 1 = \frac{60+1}{17} \neq 0$

+1

$60 \times 2 = \frac{120+1}{17} \neq 0$

$\vdots$

$60 \times 15 = \frac{901}{17} = 53$

$$\begin{array}{r} 52 \\ 17 \overline{)901} \\ 901 \\ \hline 0 \\ \hline \end{array}$$

$\boxed{d = 53}$

$PU = \{e, n\} = \{17, 77\}$

$PR = \{d, n\} = \{53, 77\}$.

$17 \times 1 = \frac{17+1}{60} =$

17×2 $\frac{1}{60}$

Encryption:

$$\boxed{C = M^{e} \bmod n.}$$

$= 8^{17} \bmod 77$.

8

64 mod 77

$8^1 \bmod 77 = 8$

$8^2 \bmod 77 = 64$

$8^4 \bmod 77 = (8^2 \times 8^2) \bmod 77$

$= (64 \times 64) \bmod 77$

$= 4096 \bmod 77$

$= 15$

$8^8 \bmod 77 = (8^4 \times 8^4) \bmod 77$

$= (15 \times 15) \bmod 77$

$= (225) \bmod 77$

$= 71$.

$8^{17} \bmod 77 = (8^8 \times 8^8 \times 8) \bmod 77$

$= (71 \times 71 \times 8) \bmod 77$

$= 40328 \bmod 77$

$$\boxed{C = 57}$$

```
       50 914
77 ) 40328
     39193
     ------
      1135
      1078
     ------
        57
```

Decryption:

$\underline{M} = c^{d} \bmod n$

$= 57^{\boxed{53}} \bmod 77$

$57 \bmod 77 = 57.$

$57^{2} \bmod 77 = 114 \bmod 77$

~~$= 37.$~~

~~$57^{10} \bmod 77 = 185.$~~

~~$57^{50} \bmod 77 = 925.$~~

~~$57^{53} \bmod \overset{7}{8}7 = 6019.$~~

~~$M =$~~

$57^{8} \bmod 77 = (71 \times 71) \bmod 77$

$= (5041) \bmod 77$

$= 36$

$57^{10} \bmod 77 = (36 \times 15) \bmod 77$

$= (540) \bmod 77$

$= 1.$

$57^{53} \bmod 77 = (1 \times 1 \times 1 \times 1 \times 1 \times$

$15 \times 57) \bmod 77$

$= 855 \bmod 77$

$\boxed{M = 8}$

$57^{2} \bmod 77 = 3249 \bmod 77$

$= 15.$

$57^{4} \bmod 77 = (15 \times 15) \bmod 77$

$= 225 \bmod 77$

$= 71.$

15 × 5 55

10 × 50 + 3

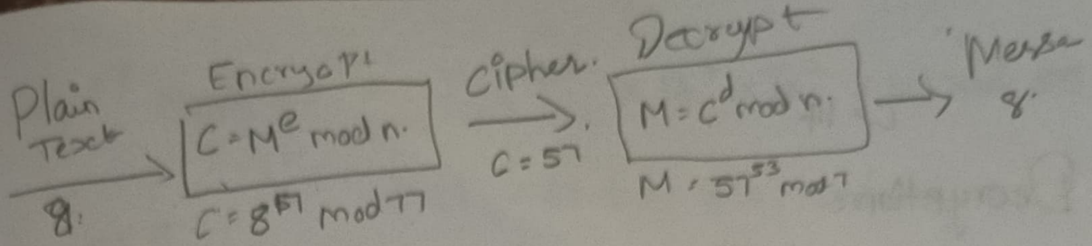
$\Rightarrow 57^{53} \Rightarrow$

$(57^{10} \times 57^{10} \times 57^{10} \times 57^{10} \times$

$\times 57^{2} \times 57)$

$(1 \times 15 \times 57) \bmod$

$= 8.$



4. $P = 11, \ q = 5, \ e = 3, \ M = 9$

$n = Pq$

$= 11 \times 5$

$n = 55.$

$\phi(Pq) = (P-1)(q-1)$

$= 10 \times 4$

$= 40$

$GCD(\phi(n), e) = 1.$

$d \equiv e^{-1} \bmod \phi(n)$

$= 3^{-1} \bmod 40$

$40 \times 1 = \frac{40+1}{3}.$

$40 \times 2 = \frac{81}{3} = 27.$

$d = 27.$

Encryption:

$C = M^e \bmod n.$

$= 9^3 \bmod 55.$

$= 729 \bmod 55.$

$$\begin{array}{r|l} & 13 \\ \hline 55 & 729 \\ & 715 \\ \hline & 14 \end{array}$$

$C = 14$

Decryption:

$M = C^{d} \bmod n$

$= 14^{27} \bmod 55.$

$14 \bmod 55 = 14$

$14^{2} \bmod 55 = 196 \bmod 55.$

$= 31.$

$$\begin{array}{r} 3 \\ 55\overline{)196} \\ 165 \\ \hline 31. \end{array}$$

$14^{4} \bmod 55 = (31 \times 31) \bmod 55$

$= 961 \bmod 55$

$= 26$

$$\begin{array}{r} 17 \\ 55\overline{)961} \\ 935 \\ \hline 26. \end{array}$$

$14^{8} \bmod 55 = (26 \times 26) \bmod 55$

$= 676 \bmod 55$

$= 16.$

$$\begin{array}{r} 12 \\ 55\overline{)676} \\ 660 \\ \hline 16. \end{array}$$

$14^{10} \bmod 55 = (14^{8} \times 14^{2}) \bmod 55$

$= (16 \times 31) \bmod 55$

$= 496 \bmod 55.$

$= 1$

$$\begin{array}{r} 9 \\ 55\overline{)496} \\ 495 \\ \hline 1. \end{array}$$

$14^{20} \bmod 55 = (14^{10} \times 14^{10}) \bmod 55$

$= (1 \times 1) \bmod 55$

$= 1.$

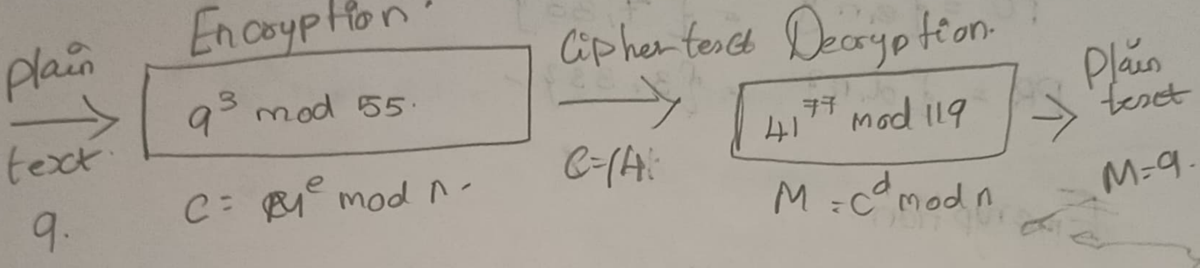
$14^{27} \bmod 55 = (14^{20} \times 14^{4} \times 14^{2} \times 14) \bmod 55$

$= (1 \times 26 \times 31 \times 14) \bmod 55$

$= 11284 \bmod 55.$

$= 9.$

```
     205
55 | 11284
     1100
      284
      275
        9.
```



Plain text 9.

Encryption: $9^3 \bmod 55.$

$C = M^e \bmod n.$

Cipher text $C = 14$

Decryption: $41^{77} \bmod 119$

$M = C^d \bmod n$

Plain text $M = 9.$

RSA

30/5

5. $P = 3,\ q = 11,\ e = 7,\ d = ?,\ M = 5.$

Key Generation:

$n = P \times q$

$= 3 \times 11$

$n = 33.$

$\phi(n) = n - 1$

$\phi(pq) = (p-1)(q-1)$

$= (3-1)(11-1)$

$= 20.$

$\text{Gcd}(\phi(n), e) = 1.$

$\text{GCD}(20, 7) = 1$

$e = 7$

$d = e^{-1} \bmod n$

$= 7^{-1} \bmod 20$

$20 \times 1 = \frac{20+1}{2} = \frac{21}{7} = 3.$

$d = 3$

$PU = \{e, n\} = \{7, 33\}$

$PR = \{d, n\} = \{3, 33\}$

Encryption:

$C = M^e \bmod n$

$= 5^7 \bmod 33.$

$5 \bmod 33 = 33$

$5^2 \bmod 33 = 25.$

$5^4 \bmod 33 = (5^2 \times 5^2) \bmod 33$

$= (25 \times 25) \bmod 33$

$= 625 \bmod 33.$

$= 31.$

$$\begin{array}{r} 18 \\ 33\overline{)625} \\ 594 \\ \hline 31. \end{array}$$

$5^7 \bmod 33 = (5^4 \times 5^2 \times 5) \bmod 33$

$= (~~33~~ (31 \times 25 \times 5) \bmod 33$

$= 3875 \bmod 33.$

$$\begin{array}{r} 117 \\ 33\overline{)3875} \\ 33 \\ \hline 57 \\ 33 \\ \hline 245 \\ 231 \\ \hline 14 \end{array}$$

$C = 14.$

Decryption:

$M = c^d \bmod n$

$= 14^3 \bmod 33$

$14 \bmod 33 = 14$

$14^2 \bmod 33 = (14 \times 14) \bmod 33$

$= 196 \bmod 33.$

$31.$

$$33 \overline{)\,196\,}^{\,5} \quad 165 \quad \overline{31}$$

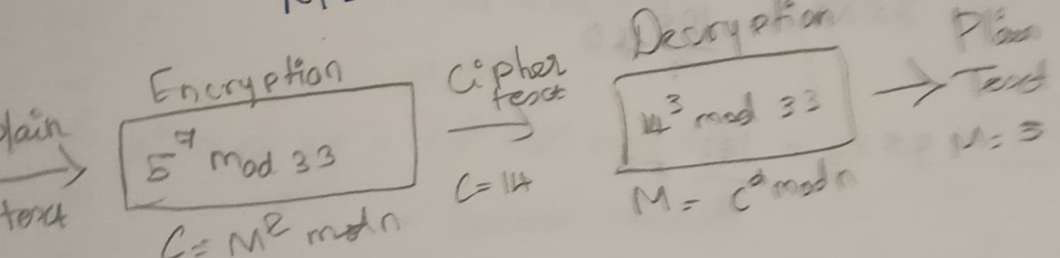
$14^3 \bmod 33 = (14^2 \times 14) \bmod 33$

$= (31 \times 14) \bmod 33$

$= 434 \bmod 33.$

$$33 \overline{)\,434\,}^{\,13} \quad 429 \quad \overline{5}$$

$M = 5.$



6. In the public key system, using RSA you a intercepts the cipher text C=10, send to a user whose public key e=5, n=35, what is the plain text.

$C=10, \; e=5, \; n=35, \; d=? \; , D.T\,(M)=?.$

~~$d \equiv e^{-1} \bmod n$~~

~~$\equiv 5^{-1} \bmod 35.$~~

~~$35\times1 = \frac{36}{7} \neq 0$~~

~~$35\times2 = 70+1 = \frac{71}{7} \neq 0$~~

~~$35\times3 = \frac{106}{7} \neq 0$~~

~~$35\times4 = \frac{141}{7} \neq 0$~~

~~35×5~~

$$\begin{array}{r} 15 \\ 7\,\overline{)\,106} \\ 7\downarrow \\ \hline 36 \end{array} \qquad \begin{array}{r} 2 \\ 7\,\overline{)\,141} \\ 14 \\ \hline 0 \end{array} \qquad \begin{array}{r} 2 \\ 7\,\overline{)\,176} \\ 14 \\ \hline 3 \end{array}$$

$n=35$

$P=7, \; q=5.$

$\phi(n) = (P-1)(q-1) = (7-1)(5-1) = 6\times4 = 24.$

$d \equiv e^{-1} \bmod n.$

$= 5^{-1} \bmod 24$

$24\times1 = \frac{25}{5} = 5.$

$d = 5.$

~~Encryption:~~

~~$C = M^e \bmod n$~~

~~$M = c^d$~~ m

Decryption:

$M = c^d \bmod n$

$= 10^5 \bmod 35.$

$10 \bmod 35 = 10$

$10^2 \bmod 35 = (10 \times 10) \bmod 35$

$= 100 \bmod 35$

$= 30.$

35) 100
70
30

$10^4 \bmod 35 = (10^2 \times 10^2) \bmod 35$

$= (30 \times 30) \bmod 35$

$= 900 \bmod 35.$

$= 25$

25
35) 900
70
200
175
25

35
5
175

35
6
210

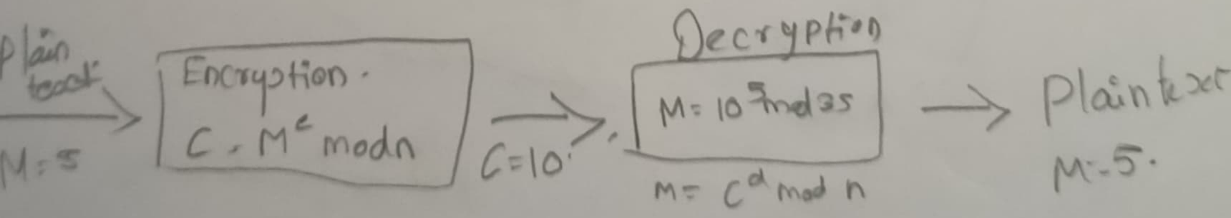
$10^5 \bmod 35 = (10^4 \times 10) \bmod 35$

$= (25 \times 10) \bmod 35.$

$= 250 \bmod 35.$

61
35.) 250
210
40
35
5.

$\boxed{M = 5.}$


Plain text
M=5
Encryption.
C = M^e mod n
C=10
Decryption
M = 10^5 mod 35
M = C^d mod n
Plaintext
M = 5.