RSA Sum.

1. $\boxed{p = 11}$ $\boxed{q = 5}$

$n = p * q = 55$ $\boxed{n = 55}$

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

$= 10 \times 4$

$\boxed{\phi(n) = 40}$

3, 7, 9, 11, 13, 17 . . . relatively prime

→ select $\boxed{e = 7}$

$e * d \bmod \phi(n) = 1$

Solve for d.

use the extended Euclidean Algorithm to solve for this

$7 * d \bmod 40 = 1$

Step 1. Euclidean Algorithm

$40x + 7y = 1$

$40 = 5(\underline{7}) + \underline{5}$

$7 = 1(5) + 2$

$5 = 2(2) + \underline{1}$ adding one step.

Step 2 : Back substitution

$1 = 5 - 2(2)$

$1 = 5 - 2(7 - 1(5))$

$1 = 3(5) - 2(7)$

$1 = 3(40 - 5(7)) - 2(7)$

$1 = 3(40) \underbrace{-17}_{\text{Negative number}}(7)$

it positive d = that Number.

So $d = 40 - 17$

$\boxed{d = 23}$

private key (d, n)
$(23, 55)$

public key (e, n)
$(7, 55)$

$\boxed{M = 6}$

$C = M^e \bmod n$

$= 6^7 \bmod 55$

$\boxed{C = 41}$

$M = C^d \bmod n$

$= 41^{23} \bmod 55$

$\boxed{M = 6}$

(2) RSA Sum.

$p = 7$ $\quad Q = 17$

$\boxed{E = 5}$ $\quad \boxed{M = 6}$ ✓

$n = p * q = 119$ $\quad \boxed{n = 119}$

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

$= 6 * 16$

$\boxed{\phi(n) = 96}$

$e * d \bmod \phi(n) = 1$

$5 * d \bmod 96 = 1$

Calculate d.:

Step 1 Euclidean Algorithm

$96x + 5y = 1$

$96 = 19(5) + 1$

Step 2 back substitution

$1 = 96 - \underline{19}(5)$

$=$

$C = M^e \bmod n$

$= 6^5 \bmod 119$

$\boxed{C = 41}$ ✓

$M = 41^{77} \bmod 119$

$\boxed{M = 6}$ ✓

$\phi(n) - 19$

$= 96 - 19$

$\boxed{d = 77}$

(3)

$p = 3 \quad Q = 11 \quad \boxed{E = 3} \quad \boxed{M = 5.}$ ✓

$n = p * Q = 3 * 11$

$\boxed{n = 33}$

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

$= 2 * 10$

$\boxed{\phi(n) = 20}$

$e * d \bmod \phi(n) = 1$

$3 * d \bmod 20 = 1$

Calculate d: using Extended Euclidean Algo.

Step 1: Euclidean Algorithm

$20x + 3y = 1$

$20 = 6(3) + 2$

$3 = 1(2) + 1$ stop.

Step 2: Back substitution

$1 = 3 - 1(2)$

$= 3 - 1(20 - 6(3))$

$= 7(3) \cancel{(20)} - 1(20)$

$= -1(20) + \underline{7}(3)$

$\boxed{d = 7.}$ ✓

$C = 5^3 \bmod \cancel{20}\ 33$

$\boxed{C = 26}$ ✓

$M = 26^{7} \bmod \cancel{20}\ 33$

$\boxed{M = 5}$ ✓

(4). $\boxed{c = 10}$ $\boxed{e = 5}$ $\boxed{n = 35}$

$M = ?$

$n = 35.$ $p = 7$ $q = 5.$

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

$= (6)(4)$

$\boxed{\phi(n) = 24}$

Calculate d:

$e * d \bmod \phi(n) = 1$

$5 * d \bmod 24 = 1$

Step 1: Euclidean Algo

$24x + 5y = 1$

$24 = 4(5) + 4$

$5 = 1(4) + 1$ Stop

Step 2: back Substitution

$1 = 5 - 1(4)$

$= 5 - 1(24 - 4(5))$

$= 5(5) - 24$

$= -24 + 5(5)$ $\boxed{d = 5}$

$M = c^d \bmod (n)$

$= 10^5 \bmod \cancel{24}\ 35$

$\boxed{M = 5}$ ✓

proof:

$C = M^e \bmod (n)$

$= 5^5 \bmod \cancel{24}\ 35$

$\boxed{C = 10}$ ✓

(5) $\boxed{p=3}$ $\boxed{q=11}$ $\boxed{e=7}$ $\boxed{M=5}$

$n = p*q = 33$

$\boxed{n=33}$ $\phi(n) = (p-1)(q-1)$

$= 2 \times 10$

$\boxed{\phi(n) = 20}$

Calculate d:

$e * d \bmod \phi(n) = 1$

$7 * d \bmod 20 = 1$

Step 1: Euclidean Algo.

~~200~~ $20x + 7y = 1$

$20 = 2(7) + 6$

$7 = 1(6) + 1$ stop.

Step 2: back substitution

$1 = 7 - 1(6)$

$= 7 - 1(20 - 2(7))$

$= -20 + 3(7)$

$\boxed{d=3}$

$C = M^e \bmod n)$

$= 5^7 \bmod 33$

$\boxed{C = 14}$

$M = C^d \bmod n$

$= 14^3 \bmod 33 = 5$ $\boxed{M=5}$

(6) 5 , 7

$p = 5$ $q = 7$ $\boxed{E = 11}$ $M = 2$

$n = p * q = 35$

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

$(5-1) \times (7-1)$

$\boxed{\phi(n) = 24}$

Calculate d

$e \times d \bmod \phi(n) = 1$

$11 \times d \bmod 24 = 1$

Step 1: Euclidean Algo

$24x + 11y = 1$

$24 = 2(11) + 2$

$11 = 5(2) + 1$ stop

Step 2: Back substitution

~~1 = 7 - 2(3)~~

~~1 = 7 - 2(24 - 3(7))~~

~~= 7 - 48 + 6(7)~~

~~= 7(7) - 48~~

$\boxed{\cancel{d = 7}}$

$C = M^e \bmod n$

$= 2^{11} \bmod 35$

$\boxed{C = 18}$

$M = c^d \bmod n$

$= \cancel{8^7 \bmod 35}$

$= 18^{11} \bmod 35$

$\boxed{M = 2}$

$1 = 11 - 5(2)$

$= 11 - 5(24 - 2(11))$

$= 11 - 120 + 10(11)$

$= 11(11) - 120$

$\boxed{d = 11}$

(6) $p = 5$ $\quad q = 7$ $\quad \boxed{e = 11}$ $\quad \boxed{M = 2}$ ✓

prime numbers $\quad$ encryption key $\quad$ plaintext.

$n = p \times q = 7 \times 5 = 35.$

$\boxed{n = 35}$

$\varphi(n) = (p-1) \times (q-1)$

$= 4 \times 6$

$\boxed{\varphi(n) = 24}$

Calculate d

$e \times d \bmod \varphi(n) = 1$

$11 \times d \bmod 24 = 1$

Step 1: Euclidean Algo.

$24x + 11y = 1$

$24 = 2(11) + 2$

$11 = 5(2) + 1.$ Stop.

Step 2: Back Substitution

$1 = 11 - 5(2)$

$= 11 - 5(24 - 2(11))$

$= 11 - 120 + 10(11)$

$= 11(11) - 120$

$\boxed{d = 11}$ ✓

$C = M^e \bmod n$

$= 2^{11} \bmod 35$

$\boxed{C = 18}$ ✓

$M = C^d \bmod n$

$= 18^{11} \bmod 35$

$\boxed{M = 2}$ ✓

(7) $p=7 \quad Q=17 \quad \boxed{E=7.}$

Assume $M=5$.

$n = p \times Q = 119$

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

$= 6 \times 16$

$\phi(n) = 96$

$e \times d \bmod \phi(n) = 1$

$7 \times d \bmod 96 = 1$

Calculate d:

Step 1 Euclidean Algo.

$96x + 7y = 1$

$96 = 13(7) + 5$

$7 = 1(5) + 2$

$5 = 2(2) + 1$

Step 2. Back substitution

$1 = 5 - 2(2)$

$= 5 - 2(7 - 1(5))$

$= \cancel{5 - 14 + 2(5)}$

$= \cancel{3(5) - 14}$

$= \cancel{3(96 - 13(7)) - 14}$

$= \cancel{288 - 39(7) - 14}$

$= \cancel{274 - 39(7)}$

$d = \dfrac{\phi(n) * i + 1}{}$

$= \dfrac{96 * i + 1}{7}$

$C = M^e \bmod n$

$= 5^7 \bmod 119$

$\boxed{C = 61}$

$M = C^d \bmod 119$

$= 61^{55} \bmod 119$

$\boxed{M = 5}$

$\phi(n) - 41$

$96 - 41 = 55$

$\boxed{d = 55}$

$3(5) - 2(7)$

$3(96 - 13(7)) - 2(7)$

$3(96) - \cancel{26}\,39(7) - 2(7)$

$3(96) - 41(7)$

$\cancel{\phi(n) - 15}$

$\cancel{\phi(n) - 39}$

$\cancel{96 - 39}$ $\cancel{d = 81}$

$\cancel{d = 57}$