RSA Solved examples.

(1)

$p, q = 13, 11$ $\quad n = 143$

$e = 13,$ $\quad \varphi(n) = 120$

$13, \gcd(13, 120) = 1$

$$d = \frac{(\varphi(n) \times i) + 1}{e}$$

$$= \frac{120+1}{13} = 9.30 \quad (i=1)$$

$$= \frac{(120 \times 2) + 1}{13} = \frac{241}{13} = 18.53$$

$$= \frac{(360+1)}{13} = \frac{361}{13} = 27.76$$

$$= \frac{(120 \times 4) + 1}{13} = \frac{481}{13} = 37.$$

$\boxed{d = 37}$

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

$\boxed{M = 13}$ $\quad m < n$

$$= 13^{13} \bmod 143$$

$$= (13^1 \bmod 143) \times (13^4 \bmod 143) \times (13^8 \bmod 143) \bmod 143$$

$$= (13 \times 26 \times 104 \times 91) \bmod 143$$

$\boxed{C = 52}$

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

$= (52)^{37} \bmod n.$

$= ((52)^{32} \times (52)^{4} \times 52^{1}) \bmod 143$

$= (130 \times 26 \times 52) \bmod 143$

$\boxed{M. = 13}$

(2) Prime numbers 3, 11

$e = 3$

$m = 59.$

- Calculate private key d and cipher text C.

$\Rightarrow p, q = 3, 11$

$n = 21$

$\phi(n) = 20,$

$e = 3$ given

$d = \frac{(20 \times 1) + 1}{3} = \frac{21}{3} = 7.$

$d = 7$

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

$= (59)^{3} \bmod 33$

$= [(59^{2} \bmod 33) \times (59^{1} \bmod 33)] \bmod 33$

$= (16 \times 26) \bmod 33$

$\boxed{= 20}$

$M = c^d \bmod n$

$= 20^7 \bmod 33$

$= [20^4 \bmod 33 \times 20^2 \bmod 33 \times 20 \bmod 33] \bmod 33$

$= [41 \times 4 \times 4] \bmod 33 \;/(1280 \bmod 33)$

$M = 26$

(3) Prime numbers 7, 17

PT = 10

① $n = 119$

② $\phi(n) = 96$

we select $e = 5$, $\gcd(5, 96) = 1$

$d = \frac{(96 * 1) + 1}{5} = 19.4$

$= \frac{(96 \times 2 + 1)}{5} = 38.6$

$= \frac{(96 \times 3) + 1}{5} = 57.8$

$d = \frac{(96 \times 4) + 1}{5} = 77.$

$d = 77$

$c = M^e \bmod n$

$= 10^5 \bmod 119$

$= (10^4 \times 10) \bmod 119$

$c = 40$

$M = c^d \bmod n$

$= 40^{77} \bmod 119$

$= 40^{32} \times 40^{32} \times 40^{8} \times 40^{4} \times 10^{1}$

$= 10$

$72 X$

(4) $P, q = 13, 17$

$m = 12$

$e = 19.$

$n = 221$

$\phi(n) = 192$

$e = 19$

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

$= \frac{(192 * 1) + 1}{19} = \frac{193}{19} = 10.1$

$\frac{(192 * 9) + 1}{19} = 91$

$d = 91$

Public key : $\{e, n\} = \{19, 221\}$

Private key $\{d, n\} = \{91, 221\}$

$C = M^e \bmod n$

$= 12^{19} \bmod 221$

$= 181$

$M = C^d \bmod n$

$= 181^{91} \bmod 221$

$M = 12$

(5) $N = 187$

encryption key $(e) = 17$.

find corresponding private key d

$n = p * q$

$187 = 17 * 11$

$\phi(n) = 160$

$\frac{(\phi(n) * 1) + 1}{e} = \frac{(160 * 1) + 1}{17} = 9.4$

$\frac{(160 * 12) + 1}{17} = 113$

$d = 113$

MU-15

Using RSA algo

(i) p=3, q=11, e=7, m=12
(ii) p=7, q=11, e=17, m=25
(iii) Find the corresponding d's for (i) and (ii) and decrypt the ciphertext.

(i) p, q = 3, 11

$n = 33$

$\phi(n) = 20$

$e = 7$,

$c = M^e \bmod n$

$= 12^7 \bmod 33$

$\boxed{c = 12}$

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

$d = \frac{(20 \times 1) + 1}{7}$

$\boxed{d = 3}$

$M = c^d \bmod n$

$= 12^3 \bmod n$

$= 12^3 \bmod 33$

$\boxed{M = 12}$

1.

(ii) P = 7, q = 11, e = 17, m = 25

n = 77

$\phi(n) = 60$

e = 17

$c = m^e \bmod n$

$= 25^{17} \bmod 77$.

$c = 9$

$d = \frac{(\phi(n) \times 1 + 1)}{e}$

$= \frac{(60 \times 15) + 1}{17}$

$= 53$

Plaintext $m = c^d \bmod n$

$= 9^{53} \bmod 77$

$m = 25$

Dec 2016

RSA

A = Public Key (e, n) = (7, 247)

B = (e, n) = (5, 221)

A:

$n = 247$

247 = 19 × 13

$= 18 \times 12$

$= 216$

B

221 = 13 × 17

$\phi(n) = 12 \times 16$

$= 192$

Calculate their private keys.

A

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

$= \frac{216 + 1}{7} = 31$

1 = 25.47

2 = 38.12

3 = 50.88

4 = 63.64

5 = 76.4

6 = 89.16

7 = 89

d = 89

B

$\phi(n) = 192$

$\frac{(192 * 1) + 1}{5} = 38.4$

d = 77

Cipher text send by A to B.

$n = 5$

$C = M^e \bmod n$

$= 5^7 \bmod 247$

CT = 73

Dec' 15

RSA,

$(e, n) = (7, 119)$

Calculate $\phi(n) = ?$

Ciphertext = ?

$M = 10$ //

$\phi(n) = 160$ //.

119

7 17

6 x 10

ciphertext

$C = M^e \bmod n$

$= 10^7 \bmod 119$

$= 73$