RSA

Example ① :

Find two prime factors p and q if public modulus parameter $n = 33$.

$\Rightarrow$ $n = p \times q$

$\therefore p \times q = 33$

$\rightarrow$ $n = 33 = 3 \times 11$ [two smallest non-decomposable numbers, so these are two prime numbers p and q] $\therefore p = 3$ & $q = 11$

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

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

$\therefore \phi(n) = 20$

Example ② :

Find two prime numbers p and q, if $n = 35$.

$\Rightarrow$ $n = p \times q$

$= 35$

$= 7 \times 5$

$\therefore p = 7$ & $q = 5$ / $\therefore p = 5$ & $q = 7$

Example ③:

Find p, q and $\phi(n)$ - Euler's Totient function if $n = 20$.

$\Rightarrow$ $n = 20$
$= 4 \times 5$
$= 2^2 \times 5$

$\therefore$ p can be 2 and q is 5.
$a = 2$

$\rightarrow \phi(n) = (p-1)\, p^{a-1} \times (q-1)$ where p^a is one of the multiplier in n.
$= (2-1)\, 2^{2-1} \times (5-1)$
$= 1 \times 2^1 \times 4$
$\therefore \phi(n) = 8$

Example ④:

Find Euler's Totient function $\phi(n)$ if $n = 36$ using RSA algorithm.

$\Rightarrow$ $n = 36$
$= 6 \times 6$
$= 3 \times 2 \times 3 \times 2$
$= 3^2 \times 2^2$
$\therefore p = 3$ & $q = 2$

OR

$n = 36$

$= 9 \times 4$

$= 3 \times 3 \times 2 \times 2$

$= 3^2 \times 2^2$

$\therefore p = 3$ & $q = 2$ OR $p = 2$ & $q = 3$

$a = 2, b = 2$

$\phi(n) = (p-1)\, p^{a-1} \times (q-1)\, q^{b-1}$

$= (3-1)\, 3^{2-1} \times (2-1)\, 2^{2-1}$

$= 2 \times 3^1 \times 1 \times 2^1$

$\therefore \phi(n) = 12$

Example ⑤ :

Find $\phi(n)$ if $n = 24$ using RSA algorithm

$\Rightarrow$ $n = 24$

$= 6 \times 4$

$= 3 \times 2 \times 2 \times 2$

$= 3 \times 2^3$

$\therefore p = 3$ & $q = 2$

$b = 3$

$$\rightarrow \phi(n) = (p-1) \times (q-1) q^{b-1}$$

$$= (3-1) \times (2-1) 2^{3-1}$$

$$= 2 \times 1 \times 2^2$$

$$\therefore \phi(n) = 8$$

ECC

Example: Suppose that user A wishes to send a message to user B by agreeing on the Elliptic Curve $y^2 \equiv x^3 - x + 8 \pmod 7$ and $G = (0,3)$. User A sends the message to user B that is encoded in the elliptic point $(2,1)$ and that user A selects the random number 3. If user B's public key is $(2,5)$ then what is the cipher-text sent by user A to user B ?

⇒ Given data:

$y^2 \equiv x^3 - x + 8 \pmod 7$

$\therefore E_7(-1, 8)$

$\therefore p = 7, \quad a = -1, \quad b = 8$

$P_m = (2,1)$

$k = 3$

$PU_B = (2,5) = PU$

$G = (0,3)$

Ciphertext sent by user A to user B

$C = (kG, (P_m + kPU))$

$= (3(0,3), (2,1) + 3(2,5))$

→ for 3(2,5):

$$3(2,5) = 2(2,5) + (2,5)$$

→ for 2(2,5)

since P = Q

$$\lambda = \frac{3x^2 + a}{2y} \pmod p$$

$$= \frac{3(2)^2 + (-1)}{2(5)} \bmod 7$$

$$= \frac{11}{10} \bmod 7$$

$$= 11 \times 10^{-1} \bmod 7$$

$$= 11 \times 3^{-1} \bmod 7$$

$$= 11 \times 5 \bmod 7$$

$$= 55 \bmod 7$$

$\therefore \lambda = 6$

$$x_3 = \lambda^2 - x - x \pmod p$$

$$= 6^2 - 2 - 2 \pmod 7$$

$$= 32 \bmod 7$$

$\therefore x_3 = 4$

$$y_3 = \lambda(x - x_3) - y \pmod p$$

$$= 6(2-4) - 5 \pmod 7$$

$$= -17 \bmod 7 = -10 \bmod 7 = -3 \bmod 7$$

$\therefore y_3 = 4$

$\therefore 2(2,5) = (x_3, y_3) = (4,4)$

→ $\therefore 3(2,5) = 2(2,5) + (2,5)$

$\therefore 3(2,5) = (4,4) + (2,5)$

for $(4,4) + (2,5)$

since $P \neq Q$

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1} \pmod p$$

$$= \frac{5-4}{2-4} \pmod 7$$

$$= \frac{-1}{2} \bmod 7$$

$$= -1 \times 2^{-1} \bmod 7$$

$$= -1 \times 4 \bmod 7$$

$\therefore \lambda = 3$

$$x_3 = \lambda^2 - x_1 - x_2 \pmod p$$

$$= 3^2 - 2 - 4 \pmod{11}$$

$$= 3 \bmod 11$$

$\therefore x_3 = 3$

$$y_3 = \lambda(x_1 - x_3) - y_1 \pmod p$$

$$= 3(4-3) - 4 \pmod 7$$

$$= -1 \bmod 7$$

$\therefore y_3 = 6$

$\therefore 3(2,5) = (x_3, y_3) = (3,6)$

→ $C = (kG, (Pm + kPU))$

$= (3(0,3), ((2,1) + 3(2,5)))$

$= (3(0,3), ((2,1) + (3,6)))$

→ for $(2,1) + (3,6)$

since $P \neq Q$

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1} \bmod p$$

$$= \frac{6-1}{3-2} \pmod 7$$

$$= \frac{5}{1} \bmod 7$$

$\therefore \lambda = 5$

$$x_3 = \lambda^2 - x_1 - x_2 \pmod p$$

$$= 5^2 - 2 - 3 \pmod 7$$

$$= 20 \bmod 7$$

$\therefore x_3 = 6$

$$y_3 = \lambda(x_1 - x_3) - y_1 \pmod p$$

$$= 5(2-6) - 1 \pmod 7$$

$$= -21 \bmod 7$$

$\therefore y_3 = 0$

$\therefore (2,1) + (3,6) = (x_3, y_3) = (6,0)$

→ $C = (kG, (Pm + kPU))$

$= (3(0,3), ((2,1) + 3(2,5)))$

$= (3(0,3), ((2,1) + (3,6)))$

$= (3(0,3), (6,0))$

→ for $3(0,3)$

$3(0,3) = 2(0,3) + (0,3)$

→ for $2(0,3)$

since $P = Q$

$$\lambda = \frac{3x^2 + a}{2y} \pmod p$$

$$= \frac{3(0)^2 - 1}{2(3)} \pmod 7$$

$$= \frac{-1}{6} \bmod 7$$

$$= -1 \times 6^{-1} \bmod 7$$

$$= -6 \bmod 7$$

$\therefore \lambda = 1$

$$x_3 = \lambda^2 - x - x \pmod p$$

$$= 1^2 - 0 - 0 \pmod 7$$

$$= 1 \bmod 7$$

$\therefore x_3 = 1$

$$y_3 = \lambda(x - x_3) - y \pmod p$$
$$= 1\,(0-1) - 3 \pmod 7$$
$$= -4 \bmod 7$$
$$\therefore y_3 = 3$$

$$\therefore 2(0,3) = (x_3, y_3) = (1,3)$$

→ for $3(0,3)$

$$3(0,3) = 2(0,3) + (0,3)$$
$$= (1,3) + (0,3)$$

for $(1,3) + (0,3)$
since $P \neq Q$

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1} \pmod p$$
$$= \frac{3-3}{0-1} \pmod 7$$
$$= 0 \bmod 7$$
$$\therefore \lambda = 0$$

$$x_3 = \lambda^2 - x_1 - x_2 \pmod p$$
$$= 0^2 - 1 - 0 \pmod 7$$
$$= -1 \bmod 7$$
$$\therefore x_3 = 6$$

$$y_3 = \lambda(x_1 - x_3) - y_1 \pmod p$$
$$= 0(1-6) - 3 \pmod 7$$
$$= -3 \bmod 7$$
$$\therefore y_3 = 4$$

$$\therefore 3(0,3) = (1,3) + (0,3)$$
$$\therefore 3(0,3) = (6,4)$$

$\Rightarrow$ Ciphertext

$$C = (K_G, (P_m + K P_U))$$
$$= (3(0,3), ((2,1) + 3(0,5)))$$
$$= (3(0,3), ((2,1) + (3,6)))$$
$$= (3(0,3), (6,0))$$
$$\therefore \boxed{C = ((6,4), (6,0))}$$

ECDH

Example (2) :

Find the shared secret key for the Elliptic Curve $E_{11}(1,1)$ with a point on the curve $(3,3)$ and the private keys of user A and B are 2 and 3 respectively.

⇒ Given data :

$E_{11}(1,1) \rightarrow p = 11$
$a = 1$
$b = 1$

$G = (3,3)$
$n_A = 2$
$n_B = 4$

→ Global Public Elements
$E_{11}(1,1)$ - Elliptic Curve
$G = (3,3) \in E_{11}(1,1)$

→ User A User B

Private key $n_A = 2$ $n_B = 3$

Calculate Public Key

$P_A = n_A \times G$
$= 2(3,3)$

$P_B = n_B \times G$
$= 3(3,3)$

→ for 2(8,3)

since P = Q,

$$\lambda = \frac{3x^2 + a}{2y} \pmod p$$

$$= \frac{3(8)^2 + 1}{2(3)} \pmod{11}$$

$$= \frac{28}{6} \bmod 11$$

$$= \frac{14}{3} \bmod 11$$

$$= 14 \times 3^{-1} \bmod 11$$

$$= 14 \times 4 \bmod 11$$

$$= 56 \bmod 11$$

$\therefore \lambda = 1$

$$x_3 = \lambda^2 - x - x \pmod p$$

$$= 1^2 - 3 - 3 \pmod{11}$$

$$= -5 \bmod 11$$

$\therefore x_3 = 6$

$$y_3 = \lambda(x - x_3) - y \pmod p$$

$$= 1(3 - 6) - 3 \pmod{11}$$

$$= -6 \bmod 11$$

$\therefore y_3 = 5$

$\therefore 2P = 2(8,3) = (x_3, y_3) = (6,5)$

→ for 3(3,3)

$3(3,3) = 2(3,3) + (3,3)$
$= (6,5) + (3,3)$

Since $P \neq Q$

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1} \pmod p$$
$$= \frac{3-5}{3-6} \bmod 11$$
$$= \frac{-2}{-3} \bmod 11$$
$$= 2 \times 3^{-1} \bmod 11$$
$$= 2 \times 4 \bmod 11$$
$$= 8 \bmod 11$$
$\therefore \lambda = 8$

$$x_3 = \lambda^2 - x_1 - x_2 \pmod p$$
$$= 8^2 - 6 - 3 \pmod{11}$$
$$= 55 \bmod 11$$
$\therefore x_3 = 0$

$$y_3 = \lambda (x_1 - x_3) - y_1 \pmod p$$
$$= 8(6-0) - 5 \pmod{11}$$
$$= 43 \bmod 11$$
$\therefore y_3 = 10$

$\therefore 3P = (6,5) + (3,3)$

$\therefore 3P = (0,10)$

→ User A

$n_A = 2$

$P_A = 2(3,3)$

$= (6,5)$

User B

$n_B = 3$

$P_B = 3(3,3)$

$= (0,10)$

exchanging public keys

Calculation of shared secret key

$K = n_A \times P_B$

$= 2(0,10)$

$= (3,8)$

$K = n_B \times P_A$

$= 3 \times (6,5)$

$= (3,8)$

→ for $2(0,10)$

since $P = Q$

$$\lambda = \frac{3x^2 + a}{2y} \pmod p$$

$$= \frac{3(0)^2 + 1}{2(10)} \mod 11$$

$$= \frac{1}{20} \mod 11$$

$= 1 \times 20^{-1} \mod 11$

$= 9^{-1} \mod 11$

$\therefore \lambda = 5$

$X_3 = \lambda^2 - x - x \pmod p$

$= 6^2 - 0 - 0 \pmod{11}$

$= 36 \mod 11$

$\therefore X_3 = 3$

$Y_3 = \lambda (x - x_3) - y \pmod p$

$= 5 (0 - 3) - 10 \pmod{11}$

$= -25 \mod 11$

$= -14 \mod 11$

$= -3 \mod 11$

$\therefore Y_3 = 8$

$\Rightarrow K = n_A P_B$

$\therefore K = 2 (0, 10)$

$\therefore K = (3, 8)$

→ for $3(6, 5)$

$3(6, 5) = 2(6, 5) + (6, 5)$

→ for 2(6,5)
since P = Q

$$\lambda = \frac{3x^2 + a}{2y} \pmod p$$

$$= \frac{3(6)^2 + 1}{2(5)} \mod 11$$

$$= \frac{109}{10} \mod 11$$

$$= 109 \times 10^{-1} \mod 11$$

$$= 109 \times (-1 + 11) \mod 11$$

$$= 1090 \mod 11$$

$\therefore \lambda = 1$

$$x_3 = \lambda^2 - x - x \pmod p$$

$$= 1^2 - 6 - 6 \pmod{11}$$

$$= -11 \mod 11$$

$\therefore x_3 = 0$

$$y_3 = \lambda(x - x_3) - y \pmod p$$

$$= 1(6 - 0) - 5 \pmod{11}$$

$$= 1 \mod 11$$

$\therefore y_3 = 1$

$\therefore 2(6,5) = (x_3, y_3)$

$\therefore 2(6,5) = (0,1)$

$$3(6,5) = 2(6,5) + (6,5)$$
$$= (0,1) + (6,5)$$

Since $P \neq Q$

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1} \pmod p$$
$$= \frac{5-1}{6-0} \mod 11$$
$$= \frac{4}{6} \mod 11$$
$$= \frac{2}{3} \mod 11$$
$$= 2 \times 3^{-1} \mod 11$$
$$= 2 \times 4 \mod 11$$
$$= 8 \mod 11$$
$$\therefore \lambda = 8$$

$$x_3 = \lambda^2 - x_1 - x_2 \pmod p$$
$$= 8^2 - 0 - 6 \pmod{11}$$
$$= 58 \mod 11$$
$$\therefore x_3 = 3$$

$$y_3 = \lambda(x_1 - x_3) - y_1 \pmod p$$
$$= 8(0-3) - 1 \pmod{11}$$
$$= -19 \mod 11 = -8 \mod 11$$
$$= -3 \mod 11$$
$$\therefore y_3 = 8$$

$\Rightarrow K = n_B \times P_A$

$\therefore K = 3\,(6,5)$

$\therefore K = (3,8)$

Example ③:

Find sender A's ECDH key for the Elliptic Curve $E_{11}(0,7)$ with the point on the Elliptic Curve $G = (2,2)$ and the private keys of Users A and B are 2 and 3 respectively.

$\Rightarrow$ Given data:

$E_{11}(0,7) \longrightarrow p = 11$

$a = 0$

$b = 7$

$G = (2,2)$

$n_A = 2$

$n_B = 3$

Sender A's ECDH key

$K = n_A \times P_B$

where $P_B = n_B \times G$

→ $P_B = n_B G$

$= 3 (2, 2)$

$= 2 (2, 2) + (2, 2)$

→ for $2 (2, 2)$

since $P = Q$

$$\lambda = \frac{3x^2 + a}{2y} \pmod p$$

$$= \frac{3(2)^2 + 0}{2(2)} \pmod{11}$$

$$= \frac{12}{4} \mod 11$$

$= 3 \mod 11$

$\therefore \lambda = 3$

$$x_3 = \lambda^2 - x - x \pmod p$$

$= 3^2 - 2 - 2 \pmod{11}$

$= 5 \mod 11$

$\therefore x_3 = 5$

$$y_3 = \lambda (x - x_3) - y \pmod p$$

$= 3 (2 - 5) - 2 \pmod{11}$

$= -11 \mod 11$

$\therefore y_3 = 0$

$\therefore 2P = 2 (2, 2) = (x_3, y_3) = (5, 0)$

→ $P_B = n_B G$
$= 3(2,2)$
$= 2(2,2) + (2,2)$
$= (5,0) + (2,2)$

→ for $(5,0) + (2,2)$
since $P \neq Q$

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1} \pmod p$$
$$= \frac{2-0}{2-5} \pmod{11}$$
$$= -\frac{2}{3} \bmod 11$$
$$= -2 \times 3^{-1} \bmod 11$$
$$= -2 \times 4 \bmod 11$$
$$= -8 \bmod 11$$
$$\therefore \lambda = 3$$

$$x_3 = \lambda^2 - x_1 - x_2 \pmod p$$
$$= 3^2 - 5 - 2 \pmod{11}$$
$$= 2 \bmod 11$$
$$\therefore x_3 = 2$$

$$y_3 = \lambda(x_1 - x_3) - y_1 \pmod p$$
$$= 3(5-2) - 0 \pmod{11}$$
$$= 9 \bmod 11$$
$$\therefore y_3 = 9$$

$\therefore P_B = n_B G$

$= (5,0) + (2,2)$

$\therefore P_B = (2,9)$

$\rightarrow K = n_A \times P_B$

$= 2(2,9)$

→ for $2(2,9)$

Since $P = Q$

$$\lambda = \frac{3x^2 + a}{2y} \pmod p$$

$$= \frac{3(2)^2 + 0}{2(9)} \pmod{11}$$

$$= \frac{12}{18} \bmod 11$$

$$= \frac{2}{3} \bmod 11$$

$$= 2 \times 3^{-1} \bmod 11$$

$$= 2 \times 4 \bmod 11$$

$$= 8 \bmod 11$$

$\therefore \lambda = 8$

$$x_3 = \lambda^2 - x - x \pmod p$$

$$= 8^2 - 2 - 2 \pmod{11}$$

$$= 60 \bmod 11$$

$\therefore x_3 = 5$

$$y_3 = \lambda(x - x_3) - y \pmod{p}$$
$$= 8(2 - 5) - 9 \pmod{11}$$
$$= -33 \bmod 11$$
$$\therefore y_3 = 0$$

$$\Rightarrow \therefore K = n_A \times P_B$$
$$\therefore K = 2(2,9)$$
$$\therefore K = (5,0)$$