9/4/21

☆ RSA algorithm:-

1) Find large prime no's p & q.
2) Calculate $n = pq$
3) Calculate $\phi(n) = (p-1)(q-1)$
4) Select e such that $\gcd(e, \phi(n)) = 1$, $1 < e < \phi(n)$
5) Calculate d, $d \equiv e^{-1} \bmod \phi(n)$ or $ed \equiv 1 \bmod \phi(n)$
6) $PU \rightarrow \{e, n\}$
7) $PR \rightarrow \{d, n\}$

$\left.\begin{matrix} \\ \end{matrix}\right\} C = M^e \bmod n$

$M = C^d \bmod n$

✗ Examples:-

1) $p = 3, q = 5, M = 2$

$\rightarrow$ $n = pq = 3 \times 5 = 15$

$\phi(n) = (p-1)(q-1) = 2 \times 4 = 8$

$e = 3$

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

$d = \frac{1 + K\phi(n)}{e}$ $\rightarrow$ Trial & error method

$= \frac{1 + K \times 8}{3}$ (to get whole no.)

at $K = 1$, $d = \frac{1+8}{3} = 3$

or

$ed \equiv 1 \bmod \phi(n)$ (extended euclidean)

$C = M^e \bmod n = 2^3 \bmod 15 = 8$

$M = C^d \bmod n = 8^3 \bmod 15 = 2$

$ed \equiv 1 \bmod \phi(n)$
$3d \equiv 1 \bmod 8$ of type $ax \equiv b \bmod n$

q	n	b	r	t_1	t_2	t
2	8	3	2	0	1	-2
1	3	2	1	1	-2	3
2	2	1	0	-2	3	-8
	1	0		3	-8	

$(t = t_1 - q t_2)$

$d = 3$

★ Computation Complexity / Aspects:-

1) $\left((a^b \bmod n)(a^c \bmod n)(a^d \bmod n)\right) \bmod n = (a^{b+c+d} \bmod n)$

Ex: $88^{11} \bmod 187 = \left((8^5 \bmod 187)(8^5 \bmod 187)(8^1 \bmod 187)\right) \bmod 187$
$= \left((22)(22)(88)\right) \bmod 187$
$= 143$

2) $c = 0,\ f = 1$ $\qquad 8^{11} \bmod 187$

$11 \longrightarrow \underbrace{\overset{3}{1}\overset{2}{0}\overset{1}{1}\overset{0}{1}}_{\text{k-values}}$

for $i = 3$,
$c = 2 \times c = 0$
$f = f \times f \bmod 187 = 1 \times 1 \bmod 187 = 1$
if $b_3 == 1$ (True)
$c = c + 1 = 0 + 1 = 1$
$f = (f \times a) \bmod n = (1 \times 88) \bmod 187 = 88$

$c = 1, f = 88$

for $i = 2$

$c = 2 \times 1 = 2$

$f = (88 \times 88) \bmod 187 = 77$

if $b_2 == 1$ (False)

$\vdots$

return f (77)

$c = 2, f = 77$

for $i = 1$

$c = 2 \times 2 = 4$

$f = (77 \times 77) \bmod 187 = 132$

if $b_1 == 1$ (True)

$c = 4 + 1 = 5$

$f = (132 \times 88) \bmod 187 = 22$

$c = 5, f = 22$

for $i = 0$

$c = 2 \times 5 = 10$

$f = (22 \times 22) \bmod 187 = 110$

if $b_0 == 1$ (True)

$c = 10 + 1 = 11$

$f = (110 \times 88) \bmod 187 = \underline{143}$

return $\underline{143}$ → Answer

Find value of c gives value of b in a^$b \bmod n$