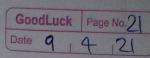
	Jait - Z
9/4/21	RSA algorithm:
4)	Find longe prime nois plq. Calculate $n = pq$ Calculate $\phi(n) = (p-1)(q-1)$ Select e such that $\gcd(e, \phi(n)) = 1$ Calculate d, $d = e^{-1} \mod \phi(n)$ or $\gcd(e) \mod \phi(n)$ PV $\rightarrow \{e_1 n\}^2$ $g \in e^{-1} \mod \phi(n)$ PR $\rightarrow \{d_1 n\}^2$ $g \in e^{-1} \mod \phi(n)$
	Examples:- $P = 3$ $Q = 5$ $M = 2$ M
\rightarrow	$ \begin{array}{c} $
	d= 1+ KØ(n) -> Triol & error method = 1+ KX8 (to get whole no.)
	ot $K=1$, $d = 1+8 = 3$
	ed = 1 mod g(n) (extended enclidean) (- Me mod a mod
	$C = M^{e} \mod n = 2^{3} \mod 15 = 8$ $M = c^{d} \mod n = 8^{3} \mod 15 = 2$



ed =
$$1 \mod \phi(n)$$

3d = $1 \mod 8$ of type $0 = b \mod n$

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

d =3

* Computation Complexity/Aspects:-

Ex:
$$88^{11}$$
 mod $187 = (8^{5} \mod 187) (8^{5} \mod 187) (8^{1} \mod 187) (8^{$

for i=3,

$$c = 2Xc = 0$$

$$if b_3 == 1$$
 (True)
 $c = c + 1 = 0 + 1 = 1$

$$c = 2 \times 1 = 2$$

$$c = 4 + 1 = 5$$

$$c = 4 + 1 = 5$$

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

$$c=5, f=22$$

Fretwon 143 -> Answer

Find volue et c gives volue et b in a 16 modes