Formulae :

ECC

→ $y \bmod p = x^3 + ax + b \bmod p$

→ $P = Q \quad \lambda = \dfrac{3 * x_p^2 + a}{2 * y_p} \bmod p$

$P \neq Q \quad \lambda = \dfrac{y_q - y_p}{x_q - x_p} \bmod p$

→ $R \Rightarrow x_r = \lambda^2 - x_p - x_q \bmod p$

$y_r = [\lambda * (x_p - x_r) - y_p] \bmod p$

→ $2P = P + P \ldots$

$p - x \rightarrow$ 1st +ve

$-x \bmod p$

$\frac{a}{b} \bmod p$

↳

$a \bmod p = u$

$b \bmod p = v$

↳ $\frac{u}{v} \bmod p$

$= uv^{-1} \bmod p$

↑

$v * \_ \bmod p = 1$

RSA

1. $\phi(n) = (p-1)(q-1)$ $\quad n = p * q$

prime nos

2. e such that $\gcd(e, \phi(n)) = 1$

$1 < e < \phi(n)$

3. $d \rightarrow$

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

4. PK $\Rightarrow (e, n)$

Pr. K $\Rightarrow (d, n)$

5. $E(M) = M^e \bmod n$

6. $D(C) = C^d \bmod n$

DHE

Public key = $g^{\wedge \text{priv.}} \bmod P$

Shared secret Key $= ex \cdot pk^{\wedge \text{priv}} \bmod p$

P → Prime no. = 13

g → Generator = 6

Alice

Pvt = 5

Public Key = $6^5 \bmod 13$

$= 2$

Shared = $9^5 \bmod 13$

$= 3$

Bob

Pvt = 4

$PK = 6^4 \bmod 13$

$= \boxed{9}$

$2^4 \bmod 13$

$= 3$

Extended Euclidean Algo.

MI of $\underset{R_2}{\underline{\underline{11}}}$ in $Z_{\underset{R_1}{\underline{\underline{26}}}}$ + GCD

$Q = R_1 / R_2$	R_1	R_2	R	T_1	T_2	$T = T_1 - Q T_2$
2	26	11	4	0	1	-2
2	11	4	3	1	-2	5
1	4	3	1	-2	5	-7
3	3	1	0	5	-7	26
	$\underline{\underline{1}}$	0		$\underline{\underline{-7}}$	5	

↑ GCD

↳ MI

$26 - 7 = \underline{\underline{19}}$