Modular Arithematic :- ($a \equiv r \bmod m$ then m divides $a-r$).

Goal :- computation in finite sets.

Ex:- clock.

Modulus :-

$a = 42, m = 9 \Rightarrow 42 = 4 \times 9 + 6 \Rightarrow \boxed{r = 6}$

$\Rightarrow 42 = 3 \times 9 + 15 \Rightarrow \boxed{r = 15}$

$\Rightarrow 42 = 5 \times 9 + (-3) \Rightarrow \boxed{r = -3}$

Equivalence class:-

Ex:- $a = 12, m = 5$

$12 \equiv 2 \bmod 5$

$12 \equiv 7 \bmod 5$

$12 \equiv -3 \bmod 5$

The set $\{\ldots -8, -3, 2, 7, 12, \ldots\}$ forms an "equivalence class" modulo 5. All members of the class behave equivalent modulo 5.

→ All equivalent classes of modulo 5 :-

$\{\ldots -10, -5, 0, 5, 10, \ldots\}$ A

$\{\ldots -9, -4, 1, 6, 11, 16 \ldots\}$ B

$\{\ldots -8, -3, 2, 7, 12, \ldots\}$ C

$\{\ldots -7, -2, 3, 8, 13, \ldots\}$ D

$\{\ldots -6, -1, 4, 9, 14, \ldots\}$ E

→ $\boxed{\overset{D}{13} \times \overset{B}{16} - \overset{D}{8}} = 208 - 8 = 200 \equiv 0 \bmod 5$.

↳ we can replace these numbers with any no. of equivalent class.

$\boxed{3 \cdot 1 - 3 = 0 \equiv 0 \bmod 5}$

$8 \cdot 6 - (-7) = 48 + 7 = 55 \equiv 0 \bmod 5$

→ $3^8 \bmod 7 = ?$ $\Rightarrow 3^8 = 6561 \equiv 2 \bmod 7$.

2nd way ⇒ $3^8 = 3^4 \cdot 3^4 = 81 \times 81 = 4 \cdot 4 = 16 \equiv 2 \bmod 7$

$81 \% 7 = 4$

Rings (An algebraic view on modular Arithmetic):

The 'integer ring' consists of

(1) the set $Z_m = \{0, 1, \ldots m-1\}$

(2) Two operators '+' and '·' such that for all $a, b, c, d \in Z_m$

(i) $a + b \equiv c \mod m$

(ii) $a \cdot b \equiv d$ "

The properties of the rings are:-

* We can add or multiply any two numbers and the result is always in the ring. A ring is said to be closed
* Addition and multiplication are associative.
* There is a neutral element in a ring '0' ~~with~~ w.r.t addition i.e, for every $a \in Z_m$ it hold $a + 0 \equiv a \mod m$.
* For an element 'a', there exists a negative number $-a$ such that $a + (-a) \equiv 0 \mod m$.
* Netural element w.r.t multiplication. : $a \times 1 \equiv a \mod m$.
* multiplicative inverse exists only for some,

Let $a \in Z$, the inverse a^{-1} is defined such that

$$a \cdot a^{-1} \equiv 1 \mod m.$$

If an inverse exists for a. We can divide this element since $b/a = b \cdot a^{-1} \mod m$.

Ex:- multiplicative inverse

$m = 9$ $\quad Z = \{0, 1, 2, 3, 4, \ldots, 9\}$

$a = 2$ $\quad a^{-1} = ?$

$\cancel{2^{-1} = 1/2 = 0.5}$ Not in the ring.

$2 \cdot 2^{-1} \equiv 1 \mod 9$

$2 \cdot 5 \equiv 1 \mod 9$ $\quad \boxed{\gcd(2, 9) = 1}$

$\boxed{2^{-1} \equiv 5 \mod 9}$

6 · $\equiv 1 \mod 9$ $\quad \gcd(6,9) = 3 \neq 1 \rightarrow$ inverse doesn't exists.

↳ doesn't exist.

→ $\gcd(a,m) = 1$ then inverse exists.

RSA :-

Ex :- Alice

$m = 4$

Bob

$p = 3, q = 11$

$n = 33$

$\phi(n) = 2 \cdot 10 = 20$

$e = 3$

$d = e^{-1} \equiv 7 \mod 20$

check

$d \cdot e = 7 \cdot 3 \equiv 1 \mod \underset{\phi(n)}{20}$

$(37)^7 \equiv (-2)^7 \mod 33$

$\equiv -128 \mod 33$

$\equiv -4 \times 33 + 4 \mod 33$

$\equiv 4 \mod 33.$

$c \equiv 4^3 = 64 \mod 33$

$c = 31 \quad \rightarrow \quad m = c^d = 37^7 \equiv 4 \mod 33$

Fast Exponentiation:-

$x^8 = ?$

naive

$x \cdot x = x^2$

$x^2 \cdot x = x^3$

$\vdots$

$x^7 \cdot x = x^8$

7 mul

better

$x \cdot x = x^2$

$x^2 \cdot x^2 = x^4$

$x^4 \cdot x^4 = x^8$

3 mul

$x^{2^{1024}} = ?$

$x \cdot x = x^2$

$\vdots$

$x^{2^{1024}-1} \cdot x = x^{2^{1024}}$

↓

Linear complexity

$x \cdot x = x^2$

$x^2 \cdot x^2 = x^4$

$\vdots$

$x^{2^{1023}} \cdot x^{2^{1023}} = x^{2^{1024}}$

↓

logarithmic complexity

Square and Multiply Algorithm (Fast exponentiation):-

Ex :- $x^{26} = x^{11010_2}$

sq $\quad x \cdot x = x^2$

mul $\quad x \cdot x^2 = x^3$

sq $\quad x^3 \cdot x^3 = x^6$

sq $\quad x^6 \cdot x^6 = x^{12}$

mul $\quad x \cdot x^{12} = x^{13}$

$(x^1)^2 = x^{10_2}$

$x^1 \cdot x^{10_2} = x^{11_2}$

$(x^{11})^2 = x^{110_2}$

If square shifts and multiplication adds to the binary Representation

So $x^{13} \cdot x^{13} = x^{26}$

$(x^{110})^2 = x^{1100_2}$

$x^{1100_2} \cdot x = x^{1101_2}$

$(x^{1101})^2 = x^{11010_2} \rightarrow x^{26}$

Euclidean Algorithm:

Goal: given r_0, r_1, find $\gcd(r_0, r_1) = ?$

Ex:- $r_0 = 27$, $r_1 = 21$ $\Rightarrow$

$27 = \boxed{3} \cdot 3$

$21 = \boxed{3} \cdot 7$

$\gcd(27, 21) = 3$

Idea:- $\gcd(r_0, r_1)$ is same as $\gcd(r_0 \bmod r_1, r_1)$

or $\gcd(r_0, r_1 \bmod r_0)$

$\gcd(\overset{r_0}{973}, \overset{r_1}{301}) = ?$

$973 = 3 \cdot 301 + \overset{r_2}{70}$

$301 = 4 \cdot 70 + \overset{r_3}{21}$

$70 = 3 \cdot 21 + \overset{r_4}{7}$

$21 = 3 \cdot 7 + 0$

Extended Euclidean Algorithm:-

given r_0, r_1

$\gcd(r_0, r_1) = s \cdot r_0 + t \cdot r_1$

Ex: $\gcd(973, 307) = s \cdot 973 + t \cdot 301 = 7$

$\overset{r_0}{973} = 3 \cdot \overset{r_1}{301} + \overset{r_2}{70}$

$301 = 4 \cdot 70 + \overset{r_3}{21}$

$70 = 3 \cdot 21 + \overset{r_4}{7}$

$7 = \gcd(r_0, r_1)$

$r_2 = 70 = [1]\, 973 + [-3]\, 307$

$r_3 = 21 = 301 - 4 \cdot 70 = 301 - 4[973 - 3 \cdot 307]$

$r_3 = (-4)\, 973 + (13)\, 307$

$r_4 = 70 - 3 \cdot 21$

$= [973 - 3 \cdot 307] - 3 \cdot [-4 \cdot 973 + 13 \cdot 307]$

$$\boxed{7 = \gcd(r_0, r_1) = r_4 = [13]\, 973 + [-42]\, 307}$$

Formula:-

$s_i = s_{i-2} - q_{i-1} s_{i-1}$ $\quad i \geq 2$

$t_i = t_{i-2} - q_{i-1} t_{i-1}$

where $s_0 = 1 \quad t_0 = 0$

$s_1 = 0 \quad t_1 = 1$

Main application ~~EGCD~~: Extended euclidean Algo:-

→ computing inverse modulo n.

$a^{-1} \equiv ?\ \bmod n$

$a^{-1} \cdot a \equiv 1 \bmod n$

$\gcd(n, a) = 1 \Rightarrow s \cdot n + t \cdot a = 1$

$s \cdot n + t \cdot a \equiv 1 \bmod n$

or

$t \cdot a \equiv 1 \bmod n$

$\rightarrow a^{-1}$

$$\boxed{t \text{ of the EEA is the inverse of } r_1 \bmod r_0}$$

* Euler's phi function:-

Ex:- $m = 240$ $\phi(240) = ?$

$m = 16 \cdot 15 = 2^4 \cdot 3^1 \cdot 5^1$

$= p_1^{e_1} \cdot p_2^{e_2} \cdot p_3^{e_3}$

$\phi(240) = \prod_{i=1}^{3} (p_i^{e_i} - p_i^{e_i - 1})$

$= (2^4 - 2^3) \cdot (3^1 - 3^0)(5^1 - 5^0)$

$= 8 \cdot 2 \cdot 4 = 64$

* Fermat's little theorem:-

Let a be an integer and p be a prime no.

then $a^p \equiv a \pmod{p}$.

* Euler's theorem:-

Let a and m be integers and $\gcd(a, m) = 1$ then

$a^{\phi(m)} \equiv 1 \pmod{m}$.

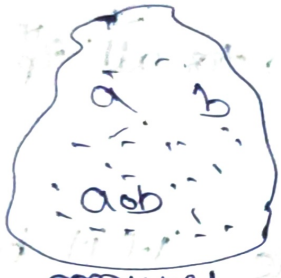
Diffie-Hellman key exchange:

Alice	public parameters p, α	Bob
$a = k_{prA} \in \{2,3,\dots p-2\}$	$\xrightarrow{A}$	$b = k_{prB} \in \{2,3,\dots p-2\}$
$A \equiv \alpha^a \bmod p = k_{pubA}$	$\xleftarrow{B}$	$B \equiv \alpha^b \bmod p = k_{pubB}$
$k_{AB} = B^a \bmod p$	$=$	$k_{AB} = A^b \bmod p$

Finite Groups:

Groups ≈ "set with elements and 1 group operation"

G



* Properties of groups:

** closeness $a o b = c \in G$

* Associativity $(a o b) o c = a o (b o c)$

* Nutral ele: $a o 1 = a$

* Inverse ele. $a o a^{-1} = 1$

* Commutativity $a o b = b o a$

all group

Abelian group

Experiment:

Is $(Z_9, \times)$ a group?

$Z_9 = \{0, 1, 2, \ldots 9\}$

$a \equiv x \bmod 9$.

inverse doesn't exists ~~for~~ all the numbers in Z_9
i.e, $\gcd(a, 9) = 1$

→ $Z_9^* = \{1, 2, 4, 5, 7, 8\}$ is a multiplicative group.

* Note :- Z_p^* p is prime, forms a mult. group.

$Z_p^* = \{1, 2, 3, \ldots p-1\}$

$\gcd(a, p) = 1$ → for all Z_p^*

Finite group def:-

A group $(G, \circ)$ is finite if it has ~~order~~ a finite no. of elements. We denote the cardinality or order of the group G by $|G|$.

$|Z_9^*| = 6$ ⇒ no. of elements in Z_9^*.

Cyclic Groups:

Experiment:

$\mathbb{Z}^*_{11} = \{1,2,3,4,5,6,7,8,9,10\}$

Q. What happens when we compute all powers of $a=3$?

$a^1 = 3$

$a^2 = 9$

$a^3 = 27 \equiv 5$

$a^4 = a^3 \cdot a = 5 \cdot 3 \equiv 4$

$a^5 = a^4 \cdot a = 4 \cdot 3 \equiv 1$

$a^6 = a^5 \cdot a = 1 \cdot 3 \equiv 3$

$a^7 = a^6 \cdot a = 3 \cdot 3 \equiv 9$

$3^{12852258} \bmod 11 = ?$

will be in the set $\{3,9,5,4,1\}$

$\text{ord}(3) = 5 \rightarrow$ length of cycle.

Order of an element:-

The order $\text{ord}(a)$ of an element a of a group $(G,\circ)$ is the smallest positive integer k such that

$$a^k = \underbrace{a \circ a \circ a \cdots a}_{k \text{ times}} = 1,$$

where 1 is identitity element of G.

→ A group which contains an element α with maximum order $\text{ord}(\alpha) = |G|$ is said to be "cyclic". Elements w/ maximum order are called "primitive element" or "generators".

$\mathbb{Z}_{11}^* = \{1,2,3,4,5,6,7,8,9,10\}$

$a^1 = 2$
$a^2 = 4$
$a^3 = 8$
$a^4 = 5$
$a^5 = 10$
$a^6 = 9$
$a^7 = 7$
$a^8 = 3$
$a^9 = 6$
$a^{10} = 1$
$a^{11} = 2$

$ord(2) = 10$

If we have a generator or premitive element we have a cyclic group

$a=2$ is the generator of $\mathbb{Z}_{11}^*$.

* Cyclic groups are basics of DLP.

→ For every prime p, $(\mathbb{Z}_p^*, \cdot)$ is an Abelian finite cyclic group

<u>Properties of cyclic groups:-</u>

Let $a \in G$, G is a cyclic group.

1. $a^{|G|} = 1$
2. $ord(a)$ divides $|G|$.

Cyclic group $\mathbb{Z}_{11}^* = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$

primitiv element $\xrightarrow{def}$ $ord(\alpha) = |G|$

$\quad\quad\quad

Diffie-Hellman problem (DHP):

(α, p) → Public

Alice	Oscar	Bob
$a = k_{PRIVA} = \{2, \dots p-2\}$	Listening the network.	$b = k_{PRIVB} = \{2, \dots p-2\}$
$A = k_{PUBA} = \alpha^a \bmod p$		$B = k_{PUBB} = \alpha^b \bmod p$
	$\xrightarrow{A}$	
	$\xleftarrow{B}$	
$k_{AB} = B^a \bmod p$		$k_{AB} = A^b \bmod p$

Oscar knows α, p, A, B and want to know $k_{AB} = \alpha^{ab}$ } DHP

One way of solving the DHP

1. Step compute $a = \log_\alpha A \bmod p$ (This is hard when p is large enough)
2. $\therefore$ $B^a = k_{AB} = \alpha^{ab} \bmod p$

* If the only way solving DHP requires the DLP, one would say that "the DHP is equivalent to the DLP". However this is not proven (yet).

* In the case of RSA the situation is similar, the only way of breaking RSA is factoring.

Generalized DLP (GDLP):-

One powerful feature of DLP. Not restricted to Z_p^* but other cyclic groups can also be used for building DL crypto-systems.

$G = \{\alpha, \alpha^2, \alpha^3, \ldots\ldots \alpha^{|G|} = 1\}$

α - prim ele.

$\alpha \quad \alpha^2$

$\alpha^3 \ldots$

* Generalized DLP given cyclic groups $(G, \circ)$ and $|G| = n$. Let α be prim. ele. and $\beta \in G$. Find x such that

$$\beta = \underbrace{\alpha \circ \alpha \circ \alpha \circ \ldots \circ \alpha}_{x \text{ times}} = \begin{cases} \alpha^x & \text{if } \circ = \text{mul} \\ x\alpha & \text{if } \circ = \text{add} \end{cases}$$

→ Which of groups make good DL problems?

1) Z_p^* multiplicative group of a prime feild.

2) $GF(2^m)^*$ " " " " extended feild.

3) Elliptic curves :- The group consists of points on a curve.

4) Generalization of 3, eg. hyper elliptic curves.

Attacks on DLP:

Solve $\log_{\alpha} \beta = x$

$\alpha, \beta \in G$, $n = |G|$, $\alpha^x = \beta$

1) Brute force. Analyzing all possible values of x.
then $n > 2^{80}$.

2) Square-root attacks:-

Baby-step giant-step and pollard's-rho method compute x in $\sqrt{n}$ steps.

if $n = 2^{80}$ $\sqrt{n} = \sqrt{2^{80}} = 2^{40}$ → can be brute-forced.

$n = 2^{160}$. $\sqrt{n} = 2^{80}$ → not possible.

→ Important square root attacks work in any group. For elliptic curves. they are the best known attacks.
[HAC, Babystep giant step, pollard's rho]

Introduction to Elliptic curves:-

Motivation: Find PK family with shorter operands.

RSA - 1024 bit

DL- Elgamal, DSA/DH - 1024 bits

Eliptic curves

ECDH, ECDSA - 160 bits

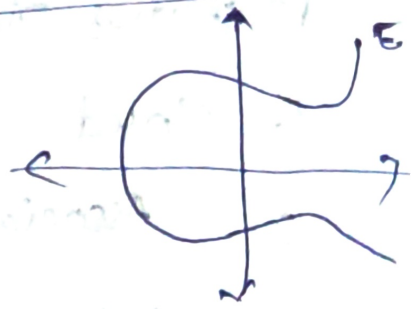
→ Can we find another cyclic group in which DLP is difficult? Ideally more difficult than a $\mathbb{Z}_p$? Yes

For the use in crypto we need to consider polynomials over $\mathbb{Z}_p$.

* the EC over $\mathbb{Z}_p$, $p>3$, is the set of all pairs $(x,y) \in \mathbb{Z}_p$

$$y^2 \equiv x^3 + ax + b \mod p$$

together with an imaginary point at infinity O, where $a, b \in \mathbb{Z}_p$ and $4a^3 + 27b^2 \not\equiv 0 \mod p$.



→ For a DLP we need a cyclic group.

for a group we need

a) set of elements

b) a group operation that fullfills the group laws.

→ These elliptic curves are symmetric to x-axis.

$$y^2 = x^3 + ax + b$$

$$y = \pm\sqrt{x^3 + ax + b}$$

Elliptic Curve point Addition and point Doubling:-

$$x_3 = \lambda^2 - x_1 - x_2 \mod p.$$

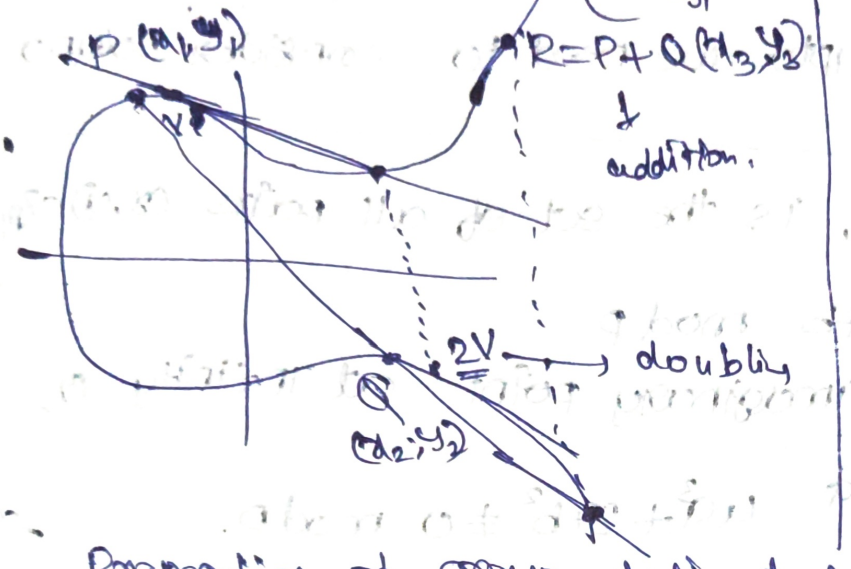
$$y_3 = \lambda(x_1 - x_3) - y_1 \mod p$$

where,

$$S = \begin{cases} \dfrac{y_2 - y_3}{x_2 - x_1} \mod p & ; \text{if } P \neq Q \text{ (point addition)} \\ \dfrac{3x_1^2 + a}{y_1} \mod p & ; \text{if } P = Q \text{ (Point Doubling)} \end{cases}$$

$E: y^2 \equiv x^3 + ax + b$

$P = (x_1, y_1)$ $Q = (x_2, y_2)$



$y = Sx + m$

$(Sx + m)^2 = x^3 + ax + b$

$S^2x^2 + 2Sxm + m^2 = x^2 + ax + b$

3 solutions x_1, x_2, x_3

Properties of group defined for EC:-

1. Closed $P + Q = R \in E$

2. Associative $P + (Q + R) = (P + Q) + R$

3. Netural element $a + \theta = 1$

   ↳ Infinity.

   (There won't be any point on the curve satisfying this condition, so we take a imaginary point at infinity.)

4) Inverse $P + (-P) = \theta$ $\forall P \in E$.

   $-P$ of $P = (x, y)$ is defined as $P = (x, -y)$.

* $E: y^2 \equiv x^3 + 2x + 2 \cdot \bmod 17.$

We want to double the point $P = (5,1)$

$2P = P + P = (5,1) + (5,1) = (x_3, y_3)$

$$s = \frac{3x_1^2 + a}{2y_1} = (2 \cdot 1)^{-1}(3 \cdot 5^2 + 2) = 2^{-1} \cdot 9 \equiv 9 \cdot 9$$
$$\equiv 13 \bmod 17.$$

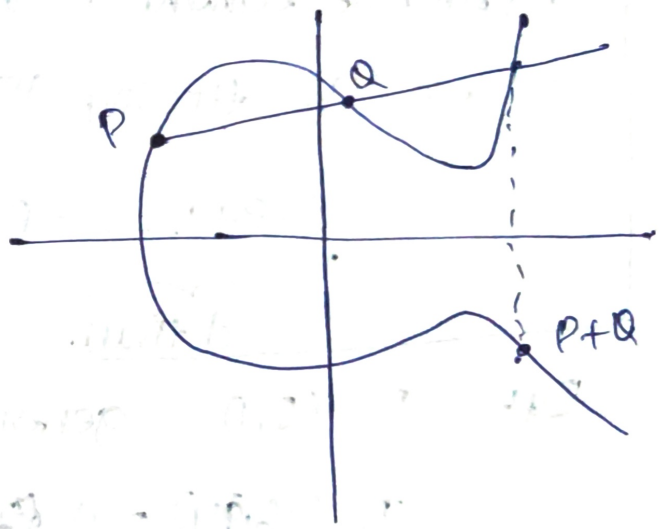
$\underline{x_3} = s^2 - x_1 - x_2 = 13^2 - 5 - 5 = 159 \equiv 6 \bmod 17.$

$\underline{y_3} = s(x_1 - x_3) - y_1 = 13(5-6) - 1 = -14 \equiv 3 \bmod 17.$

$2P = (5,1) + (5,1) = (6,3).$

* The points on EC, including $\mathcal{O}$, have cyclic subgroups under. Under certain conditions all points on an EC form a cyclic group.

<u>Elliptic Curve Discrete logarithm problem:-</u>



Ex:- EC is a cyclic group.

$E: \quad y^2 \equiv x^3 + 2x + 12 \mod 17.$

For this specific curve, all points form a cyclic group.

primitive element $P = (5,1)$

$2P = P+P = \ldots = (6,3)$

$3P = 2P+P = \ldots = (10,6)$

$\vdots$

$18P = (5,16) = (5,-1) = -P$

$19P = 18P+P = -P+P = \mathcal{O}.$

$20P = 19P+P = \mathcal{O}+P = (5,1).$

$21P = 20P+P = P+P = (6,3)$

Cycle

ECDLP:- Given an elliptic curve E we consider a primitive element P and unknown element T. the DL problem is finding integer d. where $1 < d \leq \#E$. such that

$$\underbrace{P+P+\ldots+P}_{d \text{ times}} = dP = T$$

Ex:- $P = (5,1)$ generator

$T = (16,4) = d\,P$

$(16,4) = d\,(5,1)$

$d = ?$ → private key

* For ECDLP,

$d = k_{pri}$ is int

$t = k_{pub}$ is point on curve i.e, group element.

→ Group cardinality of E is #E.

$\#E = 19 \Rightarrow$ No. of elements in the group.

Hasse's theorem:-

Given an elliptic curve E modulo p, the no. of points on the curve is denoted by #E and bounded by

$$p+1-2\sqrt{p} \le \#E \le p+1+2\sqrt{p}.$$

→ This theorem gives us lower and upper bound for E.

$\#E \approx p$ → #E is close to p as $2\sqrt{p}$ is relatively small.

→ In practice we need exact no. of points in order to attack.

→ Finding #E exactly is computationally difficult.

* All EC protocols rely on the hardness of ECDLP.

↳ If an EC is choosen carefully the best known algo for computing ECDLP requires $\approx \sqrt{p}$ steps.

i.e, $\sqrt{2^{160}} = 2^{80}$ steps.

EC Diffie-Hellman key exchange:

→ Straightforward adoption of DH in $\mathbb{Z}_p$.

I. Phase set-up:

$E: y^2 \equiv x^3 + ax + b \mod p$.

~~pm~~ ele. $P = (x_P, y_P)$

I. Protocol:

Alice $\qquad E, P \rightarrow$ Public $\qquad$ Bob

$a = k_{priA} \in \{2, 3, \ldots \#E-1\}$ $\qquad$ $b = k_{priB} \in \{2, 3, \ldots \#E-1\}$

$A = k_{pubA} = a \cdot P = (x_A, y_A)$ $\qquad$ $B = k_{pubB} = b \cdot P = (x_B, y_B)$

$$\xrightarrow{\quad A \quad}$$

$$\xleftarrow{\quad B \quad}$$

$a \cdot B = (x_{AB}, y_{AB})$ $\qquad$ $b \cdot A = (x_{AB}, y_{AB})$

Encryption:

$AES_{x_{AB}}(m) \xrightarrow{\quad c \quad} AES^{-1}_{x_{AB}}(c)$.

$a \cdot B = a(b \cdot P) = a \cdot b \cdot P$

$b \cdot A = b \cdot (a \cdot P) = a \cdot b \cdot P$.

→ How to compute $aP = \underbrace{P+P+\cdots+P}_{a \text{ times}}$.

* The point multiplication $a \cdot P$ can be done with 'double-and-add' algo.

Ex:- $26P = ?$

$26P = (11010_2)P$.

Steps:-

$\emptyset$ $P = 1_2 P$.

1a.	$P+P = 2P = (10_2)P$	D $26 - 11010_2$
1b.	$2P + P = 3P = 11_2 P$	A
2a.	$3P + 3P = 6P = 110_2 P$	D
3a.	$6P + 6P = 12P = 1100_2 P$	D
3b.	$12P + P = 13P = 1101_2 P$	A
4a.	$13P + 13P = 26P = 11010_2 P$.	D