~~Def~~ $\boxed{\text{Diffie–Hellman Key Exchange}}$

(DH-key Xchange)

- AES or DES "keys"
- RSA provides one soln for key
- DH-key xchange

(1) Either Alice or Bob selects a large, secure prime p and a primitive root $\alpha \pmod{p}$. Both p & α can be made public.

(2) Alice chooses a secret random x $(1 \le x \le p-2)$ and Bob selects a secret random y $(1 \le y \le p-2)$

(3) Alice sends $\alpha^{x} \pmod{p}$ to Bob and Bob sends $\alpha^{y} \pmod{p}$ to Alice

(4) Using the messages they recive they can calculate the session key

For Alice $K = (\alpha^{y})^{x} \pmod{p}$

For Bob $K = (\alpha^{x})^{y} \pmod{p}$

$\because$ Both have same no. K, a key could be, say, middle 56 bits of K to obtain a DES key.

- System is secure $\because$ discrete log is difficult to solve

Formally,

Problem 7.1. Discrete Log

Instance: A x gp. $(G, \circ)$, an element $\alpha \in G$ having order n and an element $\beta \in \langle\alpha\rangle$

$$\langle\alpha\rangle = \{\alpha^i : 0 \le i \le n-1\}$$

Question: Find the unique integer a, $0 \le a \le n-1$ s.t.

$$\alpha^a = \beta$$

$$a := L_\alpha(\beta)$$

THE ELGAMAL CRYPTOSYSTEM

- Dis. log problem in $(\mathbb{Z}_p^*, \cdot)$

Cryptosystem 7.1 ElGamal Public-key cryptosystem in $\mathbb{Z}_p^*$

Let p be prime s.t. Dis. log problem in $(\mathbb{Z}_p^*, \cdot)$ is infeasable and let $\alpha \in \mathbb{Z}_p^*$ be a p.e. Let $P = \mathbb{Z}_p^*$, $C = \mathbb{Z}_p^* \times \mathbb{Z}_p^*$

and define

$$K = \{(p, \alpha, a, \beta) : \beta \equiv \alpha^a \pmod{p}\}$$

The values p, α, and β are public key. a is a private key

For $K = (p, \alpha, a, \beta)$ and for a (secret)

random no. $K \in \mathbb{Z}_{p-1}$ define

$$e_K(\underset{\text{Plaintext}}{x}, K) = (y_1, y_2) \rightarrow \text{ciphertext}$$

where $y_1 = \alpha^K \bmod p$

& $y_2 = x\beta^K \bmod p$

For $y_1, y_2 \in \mathbb{Z}_p^*$ define

$$d_K(y_1, y_2) = y_2 (y_1^a)^{-1} \bmod p$$

$\boxed{\text{Example}}$ $p = 2579$ and $\alpha = 2$

Note $o(\alpha) = p-1$

let $a = 765$

$\beta = 2^{765} \bmod 2579 = 949$

Suppose Alice wishes to send the message $x = 1299$ to Bob, say $K = 853$ is the random integer she chooses. Then

$y_1 = 2^{853} \bmod 2579 = 435$

& $y_2 = 1299 \times 949^{853} \bmod 2579$

$= 2396$

when Bob receives cipher text $(435, 2396)$

he computes $x = 2396 \times (435^{765})^{-1} \bmod 2579$

$= 1299$

plaintext

Elgamal cryptosystem can be implemented in

① The $\times$ gp. of the $<\infty$ field $\mathbb{F}_{p^n}$

② The group of an elliptic curve defined over a $<\infty$ field.

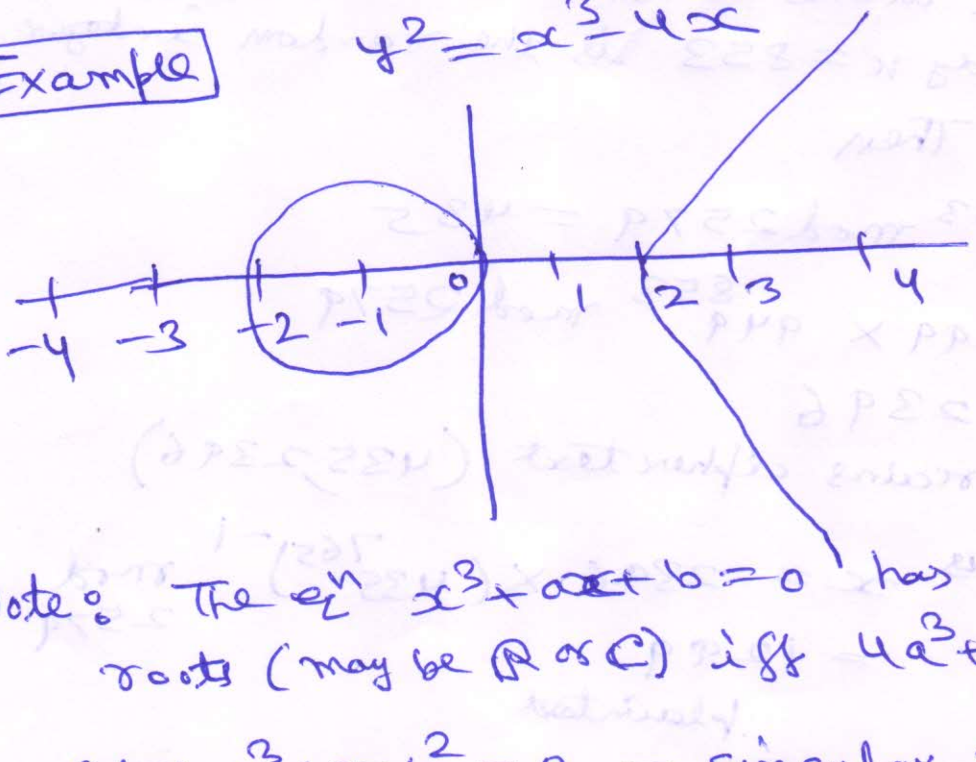
$\boxed{\text{Elliptic Curves}}$

① $\boxed{\mathbb{R}}$ $a, b \in \mathbb{R}$ s.t. $4a^3 + 27b^2 \neq 0$

A non-singular elliptic curve is the set $\mathcal{E}$ of solns. $(x,y) \in \mathbb{R} \times \mathbb{R}$ to the eq^n $y^2 = x^3 + ax + b$

together with a special pt. $\mathcal{O}$ the pt. at ∞.

$\boxed{\text{Example}}$ $y^2 = x^3 - 4x$



Note: The eq^n $x^3 + ax + b = 0$ has 3 distinct roots (may be $\mathbb{R}$ or $\mathbb{C}$) iff $4a^3 + 27b^2 \neq 0$

— If $4a^3 + 27b^2 = 0$ — singular elliptic curve.

$\boxed{\text{Group}}$ $\mathcal{E}$: Non-singular elliptic curve

$\langle \mathcal{E}, + \rangle$ abelian gp.

① $P + \mathcal{O} = \mathcal{O} + P = P \ \forall P \in \mathcal{E}$ $\mathcal{O} \to$ pt. at ∞

② $P, Q \in \mathcal{E}$, $P = (x_1, y_1)$ & $Q = (x_2, y_2)$

Case ① $x_1 \neq x_2$

Case ② $x_1 = x_2$ & $y_1 = -y_2$

Case ③ $x_1 = x_2$ & $y_1 = y_2$

case ① L line through P & Q, L intersects in two pts P & Q
L will intersect in one other pt. R'
if we reflect R' in the x-axis we get a pt. R
∴ we define $P + Q = R$

$\boxed{\text{Formula}}$ Eqn of L is $y = \lambda x + \vartheta$

slope $\lambda = \dfrac{y_2 - y_1}{x_2 - x_1}$ and

$\vartheta = y_1 - \lambda x_1 = y_2 - \lambda x_2$

To find pts. in $\mathcal{E} \cap L$ put $y = \lambda x + \vartheta$ in eqn of $\mathcal{E}$ we get

$$(\lambda x + \vartheta)^2 = x^3 + ax + b \quad \text{—— } (*)$$

$$\Rightarrow x^3 - \lambda^2 x^2 + (a - 2\lambda\vartheta)x + b - \vartheta^2 = 0$$

Roots are x-coordinates of pts. in $\mathcal{E} \cap L$

We know 2 pts in $\mathcal{E} \cap L$, P & Q ∴
x_1, x_2 are roots of eqn (*)
∵ x_1, x_2 are reals $\Rightarrow x_3$ is also real

Also sum of roots $x_1 + x_2 + x_3 = \lambda^2$

$\therefore x_3 = \lambda^2 - x_1 - x_2$

x_3 is the x-coordinate of R'

If y-coordinate of R' is $-y_3$

So y-coordinate of $R = y_3$

Now slope of L, namely λ is determined by any 2 pts on L

(x_1, y_1) and $(x_3, -y_3)$ are pts.

$$\Rightarrow \lambda = \frac{-y_3 - y_1}{x_3 - x_1}$$

$$\therefore \; y_3 = \lambda(x_1 - x_3) - y_1$$

$\therefore$ the formula for $P+Q$ in case ① is

if $x_1 \neq x_2$ then

$$(x_1, y_1) + (x_2, y_2) = (x_3, y_3)$$

where $x_3 = \lambda^2 - x_1 - x_2$

$y_3 = \lambda(x_1 - x_3) - y_1$ and

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

Case ② where $x_1 = x_2$ & $y_1 = -y_2$ is simple.

$$(x, y) + (x, -y) = \mathcal{O} \quad \forall (x, y) \in \mathcal{E}$$

$\therefore$ (x, y) & $(x, -y)$ are inv. w.r.to $+$

Case ③ Adding a pt $P = (x_1, y_1)$ to itself

We can assume that $y_1 \neq 0$ (otherwise we will have case ②)

similar to case 1 except that L is tangent to $\mathcal{E}$ at the pt. P.

Diff. eqn of $\mathcal{E}$,

$$2y \frac{dy}{dx} = 3x^2 + a$$

Put $x = x_1$ & $y = y_1$ slope of the tangent is

$$\lambda = \frac{3x_1^2 + a}{2y_1}$$

λ is defined

$\boxed{\text{Example}}$

$\mathcal{E} : y^2 = x^3 + x + 6$ over $\mathbb{Z}_{11}$

$\forall x \in \mathbb{Z}_{11}$ check if $z = x^3 + x + 6 \pmod{11}$ is q.r. using Euler's Criteria

For prime $p \equiv 3 \pmod 4$

$$\left(\pm y^{(p+1)/4}\right)^2 \equiv y^{(p+1)/2} \bmod p$$

$$\equiv y^{(p-1)/2} \cdot y \bmod p$$

$$\equiv y \bmod p)$$

y is q.r. mod p then $y^{(p-1)/2} \equiv 1 \bmod p$

$$\Rightarrow \pm z^{(11+1)/4} \bmod 11 = \pm z^3 \bmod 11$$

Pts. on elliptic curve $y^2 = x^3 + x + 6$ over $\mathbb{Z}_{11}$

x	$x^3+x+6 \bmod 11$	q.r.?	y
0	6	no	
1	8	no	
✓ 2	5	yes	4, 7
✓ 3	3	yes	5, 6
4	8	no	
✓ 5	4	yes	2, 9
6	8	no	
✓ 7	4	yes	2, 9
✓ 8	9	yes	3, 8
9	7	no	
✓ 10	4	yes	2, 9

$\mathcal{E}$ has 13 pts. $\Rightarrow \mathcal{E} \cong \mathbb{Z}_{13}$ (cyclic grp.)

let $\alpha = (2,7) \in \mathcal{E}$

$\Rightarrow 2\alpha = (2,7) + (2,7)$

$\Rightarrow \lambda = (3 \times 2^2 + 1)(2 \times 7)^{-1} \bmod 11$

$= 8$

$\Rightarrow x_3 = 8^2 - 2 - 2 \bmod 11 = 5$

& $y_3 = 8(2-5) - 7 \bmod 11 = 2$

$\therefore 2\alpha = (5,2)$

$\Rightarrow 3\alpha = 2\alpha + \alpha = (5,2) + (2,7) = (8,3)$

& so on

$\alpha = (2,7) \quad 2\alpha = (5,2) \quad 3\alpha = (8,3)$

$4\alpha = (10,2) \quad 5\alpha = (3,6) \quad 6\alpha = (7,9)$

$7\alpha = (7,2) \quad 8\alpha = (3,5) \quad 9\alpha = (10,9)$

$10\alpha = (8,8) \quad 11\alpha = (5,9) \quad 12\alpha = (2,4)$

$\therefore \alpha = (2,7)$ is a p.e. one pt. O at ∞.

Properties of Elliptic Curves

$\mathcal{E}$ is an E.C. over $\mathbb{F}_q$ $(q = p^n)$

then $q+1-2\sqrt{q} \le \# \mathcal{E} \le q+1+2\sqrt{q}$

<u>Th.</u> $\mathcal{E}$ E.C. over $\mathbb{F}_q$ $(q = p^n)$ for some prime p

then $\exists$ n_1 & n_2 (>0) integers s.t.

$(\mathcal{E},+)$ is $\cong \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2}$. Further, $n_2 | n_1$

Remark: ① $n_2 = 1$ iff $\mathcal{E}$ is a cyclic gp.

② If $\# \mathcal{E}$ is a prime or $\times$ of distinct primes then $\mathcal{E}$ must be a cyclic gp.

③ If integers n_1 & n_2 are computed then $(\mathcal{E},+)$ has a cyclic $\le \cong \mathbb{Z}_{n_1}$ that can be used as a setting for an Elgamal cryptosystem.

Elgamal Cryptosystem on Elliptic Curves

Dis. Log. on $\mathcal{E}$ $\quad P, Q \in \mathcal{E}$

$Q = mP$ $\quad m \to$ private key
difficult to determine

— A (non-∞) pt. on an elliptic curve $\mathcal{E}$ is a pair (x,y), where $y^2 \equiv x^3+ax+b \pmod{p}$

— Given a value for x, there are two possible values for y (unless $x^3+ax+b \equiv 0 \pmod{p}$)

These values are $-$ve of each other mod p. Since p is odd one of the value y mod p is even and other is odd.

$\therefore$ we can determine a $\underset{\circ}{!}$ pt. $P = (x, y)$ on $\mathcal{E}$ by specifying the value of x together with single bit y mod 2. This reduces storage 50%.

$$\text{Point-compress} : \mathcal{E}\setminus\{O\} \to \mathbb{Z}_p \times \mathbb{Z}_2$$

$$\text{Point-compress}(P) = (x, y \bmod 2), \quad P = (x, y) \in \mathcal{E}$$

The inv. Point decompress is

$\boxed{\text{Algo } 7.5}$ Point-Decompress (x, i)

$z \leftarrow x^3 + ax + b \bmod p$

if z is a q.n.r. mod p
    then return ("failure")
else
    $y \leftarrow \sqrt{z} \bmod p$
    if $y \equiv i \pmod 2$
    then return (x, y)
    else return $(x, p-y)$

Note $\sqrt{z}$ can be computed as $z^{(p+1)/4} \bmod p$ provided $p \equiv 3 \bmod 4$ and z is q.r. mod p (or $z=0$)

Elliptic Curve ElGamal

$\mathcal{E}$ elliptic curve defined over $\mathbb{Z}_p$ $(p>3)$

s.t. that $\mathcal{E}$ containing a cyclic $\leq H = \langle P \rangle$ of prime order n in which Disc. Log prob is infeasable.

let $h: \mathcal{E} \to \mathbb{Z}_p$ be a secure hash fn.

$\mathcal{P} = \mathbb{Z}_p$ and $\mathcal{C} = (\mathbb{Z}_p \times \mathbb{Z}_2) \times \mathbb{Z}_p$

Define $\mathcal{K} = \{ (\mathcal{E}, P, m, Q, n, h) : Q = mP \}$

$P, Q \in \mathcal{E}$ & $m \in \mathbb{Z}_n^*$

$\mathcal{E}, P, Q, n$ & h are public key

m private key

For $K = (\mathcal{E}, P, m, Q, n, h)$, for a (secret) random no. $k \in \mathbb{Z}_n^*$ and for a plaintext $x \in \mathbb{Z}_p$

$$e_K(x, k) = (\text{Point-compress}(kP), x + h(kQ) \bmod p)$$

For a cipher text $y = (y_1, y_2)$

$y_1 \in \mathbb{Z}_p \times \mathbb{Z}_2$ & $y_2 \in \mathbb{Z}_p$

$$d_K(y) = y_2 - h(R) \bmod p$$

$$R = m \text{ Point-decompress}(y_1).$$

$\boxed{\text{Example}}$ E.C. $y^2 = x^3 + x + 6$ over $\mathbb{Z}_{11}$

$P = (2,7)$ Bob's private key is $m = 7$

$\therefore Q = 7P = (7,2)$

Alice wants to encrypt the plaintext $x = 9$
she chooses the random value $k = 6$

$\Rightarrow kP = 6(2,7) = (7,9)$

& $kQ = 6(7,2) = (8,3)$

Suppose $h(8,3) = 4$ (only for illustration)

$\Rightarrow y_1 =$ POIN compress $(7,9) = (7,1)$

& $y_2 = 9 + 4 \bmod 11 = 2$

$\therefore$ ciphertext is $y = (y_1, y_2) = ((7,1), 2)$
After receiving the ciphertext Bob computes

POINT-DECOMPRESS $(7,1) = (7,9)$

$7(7,9) = (8,3)$

$h(8,3) = 4$

and $2 - 4 \bmod 11 = 9$ (plaintext)