Elliptic Curve Cryptography

DR. ODELU VANGA

COMPUTER SCIENCE AND ENGINEERING

INDIAN INSTITUTE OF INFORMATION TECHNOLOGY SRI CITY

What's wrong with RSA?

Security strength	Key size	
	ECC	RSA/DSA/DH
80 bits	160 bits	1024 bits
112 bits	224 bits	2048 bits
128 bits	256 bits	3072 bits
192 bits	384 bits	7680 bits
256 bits	521 bits	15360 bits

EC: Elliptic Curve

- Let $a \in \mathbb{R}$, $b \in \mathbb{R}$, be constants such that

$$\mathbf{4a^3 + 27b^2 \neq 0}$$

A *non-singular elliptic curve* is the set *E* of solutions $(x, y) \in \mathbb{R} \times \mathbb{R}$ to the equation:

$$\mathbf{y^2 = x^3 + ax + b}$$

together with a special point *O* called the ***point at infinity***.

Singularity

- For an elliptic curve $y^2=f(x)$, define $F(x,y)=y^2-f(x)$.
- A singularity of the EC is a pt (x_0,y_0) such that:

$$\frac{\partial F}{\partial x}(x_0,y_0)=\frac{\partial F}{\partial y}(x_0,y_0)=0$$

$$or, 2y_0=-f'(x_0)=0$$

$$or, f(x_0)=f'(x_0)$$

$$\therefore \text{ f has a double root}$$

It is usual to assume the EC has no singular points

Elliptic Curves modulo p

Let $p > 3$ be prime.

The elliptic curve $y^2 = x^3 + ax + b$ over $\mathbb{Z}_p$ is the set of solutions $(x,y) \in \mathbb{Z}_p \times \mathbb{Z}_p$ to the congruence:

$$y^2 \equiv x^3 + ax + b \pmod{p}$$

where $a \in \mathbb{Z}_p$, $b \in \mathbb{Z}_p$, are constants such that

$4a^3 + 27b^2 \not\equiv 0 \pmod{p}$, together with

a special point O called the *point at infinity*.

Solutions form an Abelian group

Finding a point on EC

$$y^2 = x^3 + x + 1 \; over \; Z_7$$

For prime p>2 and a in Z_p^*,
$\left(\frac{a}{p}\right)$ = $a^{(p-1)/2}$ (mod p)

$4a^3 + 27b^2 \not\equiv 0 \mod 7$

$4(1) + 27(1) = 31 \mod 7 = 3 \neq 0$

x	0	1	2	3	4	5	6
y^2	1	3	4	3	6	5	6
Q_7	Y	N	Y	N	N	N	N
y	1, 6	–	2, 5	–	–	–	–

Q_7 : Euler's criteria.

$\left(\frac{a}{p}\right) = a^{(p-1)/2} \mod p$

$= 1$, QR

$= -1$, QNR

$1^3 \mod 7 = 1, \in Q_7$

$3^3 \mod 7 = 6 = -1 \mod 7 \notin Q_7$

$4^3 \mod 7 = 1, \in Q_7$

$\frac{(p-1)}{2} = \left(\frac{7-1}{2}\right) = 3.$

Points: $\{(0,1), (2,2), (0,6), (2,5), O\}$

For prime p>2 and a in Z_p^*,
$\left(\frac{a}{p}\right) = a^{(p-1)/2} \pmod p$

Elliptic curve:

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

Cipolla's Algorithm.

Let a is a quadratic residue modulo p
Choose t such that $u = t^2 - a$ is quadratic non-residue
Then $b = (t+w)^{(p+1)/2}$ gives a square root of a,
where $w = \sqrt{u}$
That is, $b^2 = a \bmod p$

x	0	1	2	3	4	5	6	7	8	9	10
$x^3 + x + 6$ mod 11	6	8	5	3	8	4	8	4	9	7	4
QR?	N	N	Y	Y	N	Y	N	Y	Y	N	Y
y	–	–	7, 4	?	–	?	–	?	?	–	?

$(1+\sqrt7)^2 = 1 + 2\sqrt7 + 7$
$= 8 + 2\sqrt7$

$y^2 = 5 \Rightarrow y = \sqrt5$

$t = 1,\quad u = t^2 - a$
$= 1 - 5$
$= -4 \bmod 11$
$= 7$ QNR

$(p+1)/2$

$(1+\sqrt7)^4 = 64 + 2\times16\sqrt7 + 28$
$= 4 + 10\sqrt7$

$y = (t+w)^6$

$(1+\sqrt7)^6 = (8+2\sqrt7)(4+10\sqrt7)$
$= 32 + \cancel{88}\sqrt7 + 140$

$= (1+\sqrt7)^6$
$= 7$

$7^2 \bmod 11 = 49$
$= 5$

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

x	0	1	2	3	4	5	6	7	8	9	10
$x^3 + x + 6 \bmod 11$	6	8	5	3	8	4	8	4	9	7	4
QR?	N	N	Y	Y	N	Y	N	Y	Y	N	Y
y			4,7	5,6		2,9		2,9	3,8		2,9

Sources Used

“Recommended Elliptic Curves For Federal Government Use” July 1999

Cryptography Theory and Practice. Douglas Stinson, 3rd ed

A Friendly Introduction to Number Theory. Joseph Silverman, 3rd ed

Elements of Modern Algebra. Gilbert and Gilbert, 6th edition