Elliptic Curve Cryptography

What’s wrong with RSA?

- RSA is based upon the ‘belief’ that factoring is ‘difficult’ – never been proven
- Prime numbers are getting too large
- Amount of research currently devoted to factoring algorithms
- Quantum computing will make RSA obsolete overnight

What exactly is an elliptic curve?

- Let $a \in \mathbb{R}$, $b \in \mathbb{R}$, be constants such that $4a^3 + 27b^2 \neq 0$. A *non-singular elliptic curve* is the set *E* of solutions $(x,y) \in \mathbb{R} \times \mathbb{R}$ to the equation:

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

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

Singular Elliptic Curve

- If $4a^3 + 27b^2 = 0$, then we have a *singular elliptic curve*
- This could potentially lead to having to not having 3 distinct roots
- Therefore, we must deal with non-singular elliptic curves with the condition $4a^3 + 27b^2 \neq 0$, in order to assure that we have 3 distinct roots.
- This will allow us to establish the fact that the solution set E forms an Abelian group.

What is a Group?

- Suppose we have any binary operation, such as addition (+), that is defined for every element in a *set* G, which is denoted *(G,* +)
- Then G is a *group* with respect to addition if the following conditions hold:

1.) **G is *closed* under addition**: $x \in G$, $y \in G$,

imply $x + y \in G$

2.) **+ is associative**. For all x, y, z, $\in G$,

$x + (y + z) = (x + y) + z$

3.) **G has an identity element *e***. There is an e in G such that $x + e = e + x = x$ for all $x \in G$.

4.) **G contains inverses**. For each $x \in G$, there exists $y \in G$, such that $x + y = y + x = e$.

What is an Abelian Group

- An Abelian group contains all the rules of a group, but also must meet the following criteria:

5.) **+ is commutative**. For all $x \in G$, $y \in G$, $x + y = y + x$.

3 Cases for Solutions

- Suppose $P, Q \in E$, where $P = (x_1,y_1)$ and $Q = (x_2,y_2)$, we must consider three cases:

  1.) $x_1 \neq x_2$

  2.) $x_1 = x_2$ and $y_1 = - y_2$

  3.) $x_1 = x_2$ and $y_1 = y_2$

- These cases must be considered when defining "addition" for our solution set

Defining Addition on *E*: Case 1

For the case $x_1 \neq x_2$, addition is defined as follows:

$$(x_1,y_1) + (x_2,y_2) = (x_3,y_3) \in E \text{ where}$$

$$x_3 = \lambda^2 - x_1 - x_2$$
$$y_3 = \lambda(x_1 - x_3) - y_1, \text{ and}$$
$$\lambda = (y_2 - y_1) / (x_2 - x_1)$$

Defining Addition on *E* : Case 2

For the case $x_1 = x_2$ and $y_1 = - y_2$, addition is defined as follows:

$(x_1,y_1) + (x_2,y_2) = (x_3,y_3) \in E$ where

$(x,y) + (x,-y) = O$, the point at infinity

Defining Addition on *E* : Case 3

For the case $x_1 = x_2$ and $y_1 = y_2$, addition is defined as follows:

$(x_1,y_1) + (x_2,y_2) = (x_3,y_3) \in E$ where

$$x_3 = \lambda^2 - x_1 - x_2$$
$$y_3 = \lambda(x_1 - x_3) - y_1, \text{ and}$$
$$\lambda = (3x_1^2 + a) / 2y_1$$

Defining the Identity

- The point at infinity O, is the identity element. $\mathrm{P} + O = O + \mathrm{P} = \mathrm{P}$, for all $\mathrm{P} \in E$.
- From Case 2, and the Identity Element, we now have the existence of inverses
- Beyond the scope here to prove that we have commutativity and associativity as well
- Therefore the set of solutions E, forms an Abelian group (Importance of this will be shown later)

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 still form an Abelian group

So now for an example

- Let's examine the following elliptic curve as an example:

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

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

Generating our group

- From the previous chart, and including the point at infinity O, we have a group with 13 points.
- Since the O(E) is prime, the group is cyclic.
- We can generate the group by choosing any point other then the point at infinity.
- Let our generator = α = (2,7)

The Group

We can generate this by using the rules of addition we defined earlier where $2\alpha = \alpha + \alpha$

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

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

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

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

Encryption Rules

- Suppose we let $\alpha = (2,7)$ and choose the private key to be 7
- then $\beta = 7\alpha = (7,2)$
- Encryption:

$$e_K(x,k) = (k(\alpha), x + k(\beta))$$

$$e_K(x,k) = (k(2,7), x+k(7,2)) \ ,$$

where $x \in E$ and $0 \leq k \leq 12$

Decryption Rule

- Decryption:

$$d_K(y_1, y_2) = y_2 - K_{priv} y_1$$

$$d_K(y_1, y_2) = y_2 - 7 y_1$$

- This is based on the ElGamal scheme of elliptic curve encryption

Using this Scheme

- Suppose Alice wants to send a message to Bob.
- Plaintext is $x = (10,9)$ which is a point in E
- Choose a random value for k, $k = 3$
- So now calculate (y_1, y_2):
- $y_1 = 3(2,7) = (8,3)$
- $y_2 = (10,9) + 3(7,2) = (10,9) + (3,5) = (10,2)$
- Alice transmits $y = ((8,3),(10,2))$

Bob Decrypts

- Bob receives $y = ((8,3),(10,2))$
- Calculates

$$
\begin{aligned}
x &= (10,2) - 7(8,3) \\
&= (10,2) - (3,5) \\
&= (10,2) + (3,6) \\
&= (10,9)
\end{aligned}
$$

Which was the plaintext

Real example from the NSA

- **Curve P-192**

$p = 6277101735386680763835789423207666416083908700390324961279$

$r = 6277101735386680763835789423176059013767194773182842284081$

$a = $ 3099d2bb bfcb2538 542dcd5f b078b6ef 5f3d6fe2 c745de65

$b = $ 64210519 e59c80e7 0fa7e9ab 72243049 feb8deec c146b9b1

$G_x = $ 188da89e b03090f6 7cbf20eb 43a18800 f4ff0afd 82ff1012

$G_y = $ 07192b95 ffc8da78 631011ed 6b24cdd5 73f977a1 1e794811