Definitions

Cyclic group: G is a group that can be generated by a single element (called generator) a, so that every element in G has the form ai for some integer i. We denote the cyclic group of order n by Zn, since the additive group of Zn is a cyclic group of order n.

Finite field crypto: group based crypto over the integers modulo a prime.

ECC: Elliptic curve cryptography: is a method of public key cryptography based on the use of elliptic curves over finite fields like RSA.

shared secret: in cryptography, a shared secret is a piece of data, known only to the parties involved, in a secure communication. may be directly used as a key, or to derive another key. The key, or the derived key, can then be used to encrypt subsequent communications using a symmetric-key cipher.

Elliptic curve overview:

EC formula: y^2=X^3+a*x+b mod p, including infinity point (identity element)

Where

1-a,b € field K

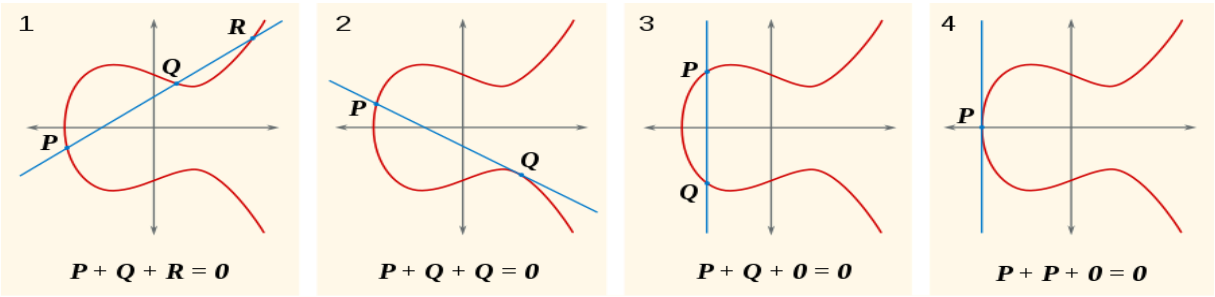
2-p is a prime number

3- 4*a^3+27*b^2 != 0 mod p

For our concern Diffie Hellman EC a=0, b=7 and k is integers modular p z/zp (finite field) .

The points on an EC, including 0 (point at infinity) have cyclic subgroups. Under certain conditions all points on an EC form a cyclic group.

Group Operations:



1)Addition:

With 2 distinct points, *P* and *Q*, addition is defined as the negation of the point resulting from the intersection of the curve(-R) P+Q=R.

Point R coordinates:

Line Slope = (Yp-Yq/Xp-Xq)modp

So Xr=(slope-Xp-Xq)modp

Yr=(slope(Xp-Xr)-Xp)modp

2)Point Doubling:

Tangent line at a point Q means 2Q with the third point P 2Q=P

Here to get line slop, slope= (3*Xp^2+a/2*Yp)modp

And Xp and Yp as above

Notes:

1)EC is symmetric around y axis, so in the third figure Q=-P and by definition the third point on the line is the infinity point P+-P=inf

2) the tangent vertical line in the fourth figure means P+P=inf

3)Scalar Multiplication:

If P € EC and k € Z then point Q=k P

Q=P+P+P+P+……..+p k times where 1<=k<=n-1

Note: in EC cyclic groups n point is the infinity point

And if n is very large number it is very difficult to compute k

even though you know both Q and P.

The only way to do so is to factorize the generator point P and get all the multiplications and compare which is insane!

So this is called elliptic curve discrete logarithm problem.

Note: k represents the private key

why ECC?

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

The most important difference in ECC from RSA is the key size. ECC provides the same cryptographic strength as the RSA-system, but with much smaller keys. For example, a 256-bit ECC key is the same as 3072-bit RSA key which is ideal choice for devices with limited storage or data processing resources + Very fast key generation. + Fast signatures.

ECC key exchange

Public Domain Parameters:

{n,G,P,a,b)

G:generator point (fixed point)

n:order of cyclic group

P: field (Zp)

a,b :curve parameters

Example:

for the 256-bit secp256k1 curve parameters are

n = FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFE BAAEDCE6 AF48A03B BFD25E8C D0364141

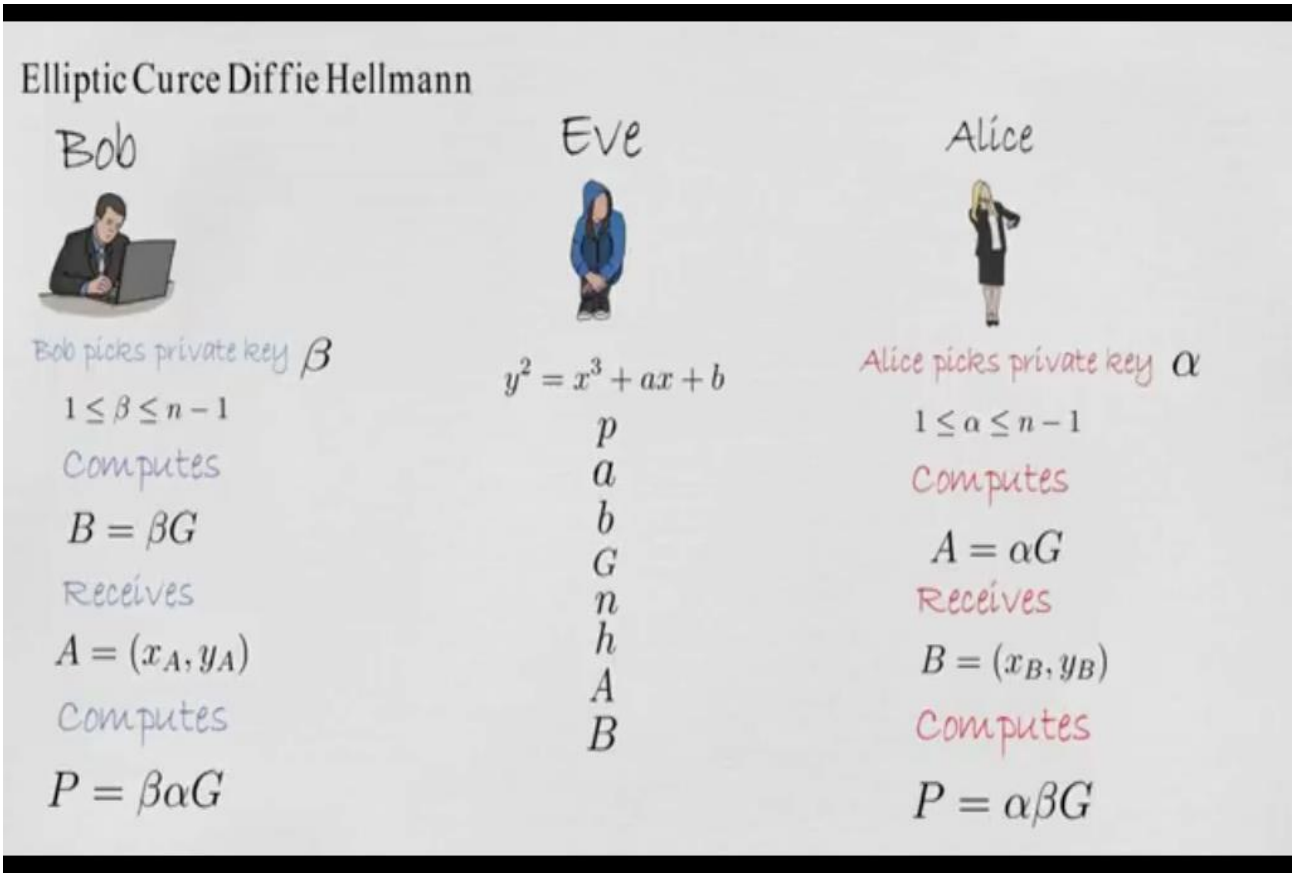
Gx= 55066263022277343669578718895168534326250603453777594175500187360389116729240

Gy=32670510020758816978083085130507043184471273380659243275938904335757337482424

p = FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFE FFFFFC2F

a=0 , b=7

How does it work?



B: Bob public key

A: Alice Public key

P: a new point on EC known only by bob & alice represents the shared secret (x coordinate of it).

And as motioned before because of n is very large number Eve can't compute P if she doesn't have β or α or if she doesn't solve DLP.

So, till now we get public key for each party and a shared key between them .