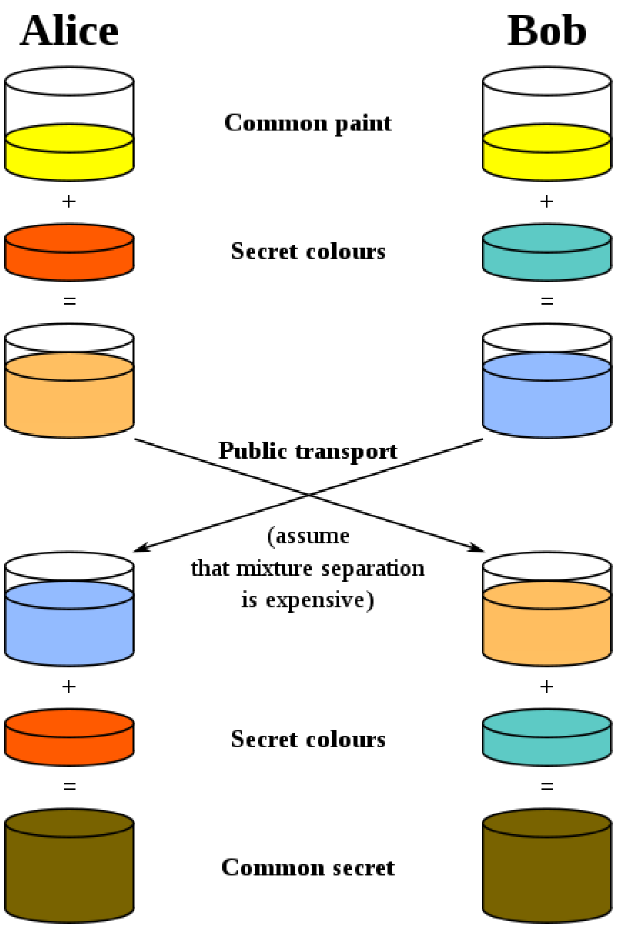
Diffie–Hellman key exchange

CHITRANG SRIVASTAVA

An Example



Source: Wikipedia

DH in TLS

1. Alice and Bob agree to use a prime number $p = 23$ and base $g = 5$.
2. Alice chooses a secret integer $a = 6$, then sends Bob $A = g^a \bmod p$
   - $A = 5^6 \bmod 23$
   - $A = 15{,}625 \bmod 23$
   - $A = 8$
3. Bob chooses a secret integer $b = 15$, then sends Alice $B = g^b \bmod p$
   - $B = 5^{15} \bmod 23$
   - $B = 30{,}517{,}578{,}125 \bmod 23$
   - $B = 19$
4. Alice computes $s = B^a \bmod p$
   - $s = 19^6 \bmod 23$
   - $s = 47{,}045{,}881 \bmod 23$
   - $s = 2$
5. Bob computes $s = A^b \bmod p$
   - $s = 8^{15} \bmod 23$
   - $s = 35{,}184{,}372{,}088{,}832 \bmod 23$
   - $s = 2$
6. Alice and Bob now share a secret (the number **2**).

Math behind DH

- Alice and Bob agree on a finite **cyclic** **group** G of order n and a **generating** element g in G. (This is usually done long before the rest of the protocol; g is assumed to be known by all attackers.) The group **G is written multiplicatively**.

Set

- Natural Number(N) - counted 1, 2, 3
- Whole Number includes 0
- Integer(Z) – no factional component
- Rational(Q) : Quotient and fractional part i.e. 3/2
- Irrational which are not rational, do not terminate, do not repeat ($\sqrt{2}$, π, e)
- Real Number(R): can be measured on scale $\sqrt{-1}$ is not a real.
- Fundamental Theorem of Arithmetic.

  Any number can be written as product of prime number

  1200 = 2*2*2*2 * 3 * 5 *5
- Property: Closure, Associativity, Commutative, Distributive, Identity, Inverse.

Groups

- **Closure** property: Take any two elements from set and perform binary operation, result should also be in same set , like + on Integer.
- **Associative** property: a+(b+c) = (a+b)+c , this is true for (I,+)
- **Identity** Element: there exists an element in e such that a + e = a , in case of I this will be 0 and 0 exists in I.
- **Inverse** , there exists an element in set such that a + a-1 = e (Identity element) , in set I if we take 2 , its invers would be -2 since 2 + (-2) = 0
- **Abelian Group** : Commutative law also hold i.e **a+b = b+a**

Multiplicative Group

- multiplicative group modulo p, (Z_p , *) for example (Z_7, *) = [1,2, 3, 4, 5, 6]
- 2 * 4 mod 7 = 1
- 2 *(3*4) mod 7 = (2*3)*4 mod 7
- 2 *1 mod 7 = 2 $\therefore$ <u>1 is identity element</u>
- 2 * 4 mod 7 = 1 , 4 is inverse of 2
- 2*4 mod 7 = 4*2 mod 7
- Hence (Z_7, *) is a group under binary operation of *.
- (Z_{10}, *) =? [1,3,7,9] Why because for 2,4,etc you cant find inverse

Cyclic Groups

- Using at least one element of group we can generate all other element of group. G =(Z_7, *)

g = 3

3 mod 7	3^0	1
3 * 3 mod 7	3^1	3
3*3 mod 7	3^2	2
3*3*3 mod 7	3^3	6
3*3*3*3 mod 7	3^4	4
3*3*3*3*3 mod 7	3^5	5

g = 2

2 mod 7	2^1	2
2*2 mod 7	2^2	4
2*2*2 mod 7	2^3	1
2*2*2*2 mod 7	2^4	2
2*2*2*2*2 mod 7	2^5	4
2*2*2*2*2*2 mod 7	2^6	1

Every element of G = {1, 2, 3, 4, 5, 6, 7} can be written in form of **g**

4 => 3^4 mod 7 => h = g^x mod p

Order of Group : How man element can be obtained using generator.

Cyclic Group: Generate all elements & g is called generator

Generator (Primitive Roots)

- Total Number of generator = ***φ* (*φ* (p))**
- Example p=19 ***φ* (*19*) = 18, *φ* (18) = 2.3²= 18 . (1-1/2)(1-1/3)=6**
- What are those **6** generator?
- Determine all the prime factors of s: p1,…,pk
- Choose any **a** and test if $a^{(p-1)/p1} = 1 \bmod p$?
- a= 2 p = 19 {p1=2, p2=3}
- $2^{(19-1)/2} = 2^9 \not\equiv 1 \bmod 19$
- $2^{(19-1)/3} = 2^6 \not\equiv 1 \bmod 19$ ∴ <u>2 is generator</u>
- All others : a^k gcd(p−1,k) = 1; k=[1, 5, 7, 11, 13, 17]
- Generator = [2, 13, 14, 15, 3, 10]

Generator of p =19

Powers of Integers, Modulo 19

a	a^2	a^3	a^4	a^5	a^6	a^7	a^8	a^9	a^{10}	a^{11}	a^{12}	a^{13}	a^{14}	a^{15}	a^{16}	a^{17}	a^{18}
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
2	4	8	16	13	7	14	9	18	17	15	11	3	6	12	5	10	1
3	9	8	5	15	7	2	6	18	16	10	11	14	4	12	17	13	1
4	16	7	9	17	11	6	5	1	4	16	7	9	17	11	6	5	1
5	6	11	17	9	7	16	4	1	5	6	11	17	9	7	16	4	1
6	17	7	4	5	11	9	16	1	6	17	7	4	5	11	9	16	1
7	11	1	7	11	1	7	11	1	7	11	1	7	11	1	7	11	1
8	7	18	11	12	1	8	7	18	11	12	1	8	7	18	11	12	1
9	5	7	6	16	11	4	17	1	9	5	7	6	16	11	4	17	1
10	5	12	6	3	11	15	17	18	9	14	7	13	16	8	4	2	1
11	7	1	11	7	1	11	7	1	11	7	1	11	7	1	11	7	1
12	11	18	7	8	1	12	11	18	7	8	1	12	11	18	7	8	1
13	17	12	4	14	11	10	16	18	6	2	7	15	5	8	9	3	1
14	6	8	17	10	7	3	4	18	5	13	11	2	9	12	16	15	1
15	16	12	9	2	11	13	5	18	4	3	7	10	17	8	6	14	1
16	9	11	5	4	7	17	6	1	16	9	11	5	4	7	17	6	1
17	4	11	16	6	7	5	9	1	17	4	11	16	6	7	5	9	1
18	1	18	1	18	1	18	1	18	1	18	1	18	1	18	1	18	1

Credit: Table 8.3 in Stallings, *Cryptography and Network Security*, 5th Ed., Pearson 2011

Discrete Logarithm

- Logarithm: $100 = 10^x \Rightarrow x = \log_{10} 100 = 2$
- Discrete logarithm is of form **$h = g^x \bmod p$**
- **p is a large prime, g is generator of Cyclic Group G**
- g is selected a **primitive root** i.e. GCD(g, p) = 1
- ompute x for carefully chosen G.

g = 2
p = 11

$h = g^x \bmod p$	x
1	0
2	1
3=2^^{8}mod 11	8
4	2
5	?
6	9
7	7
8	3
9	6
10	5

Discrete Logarithm Problem

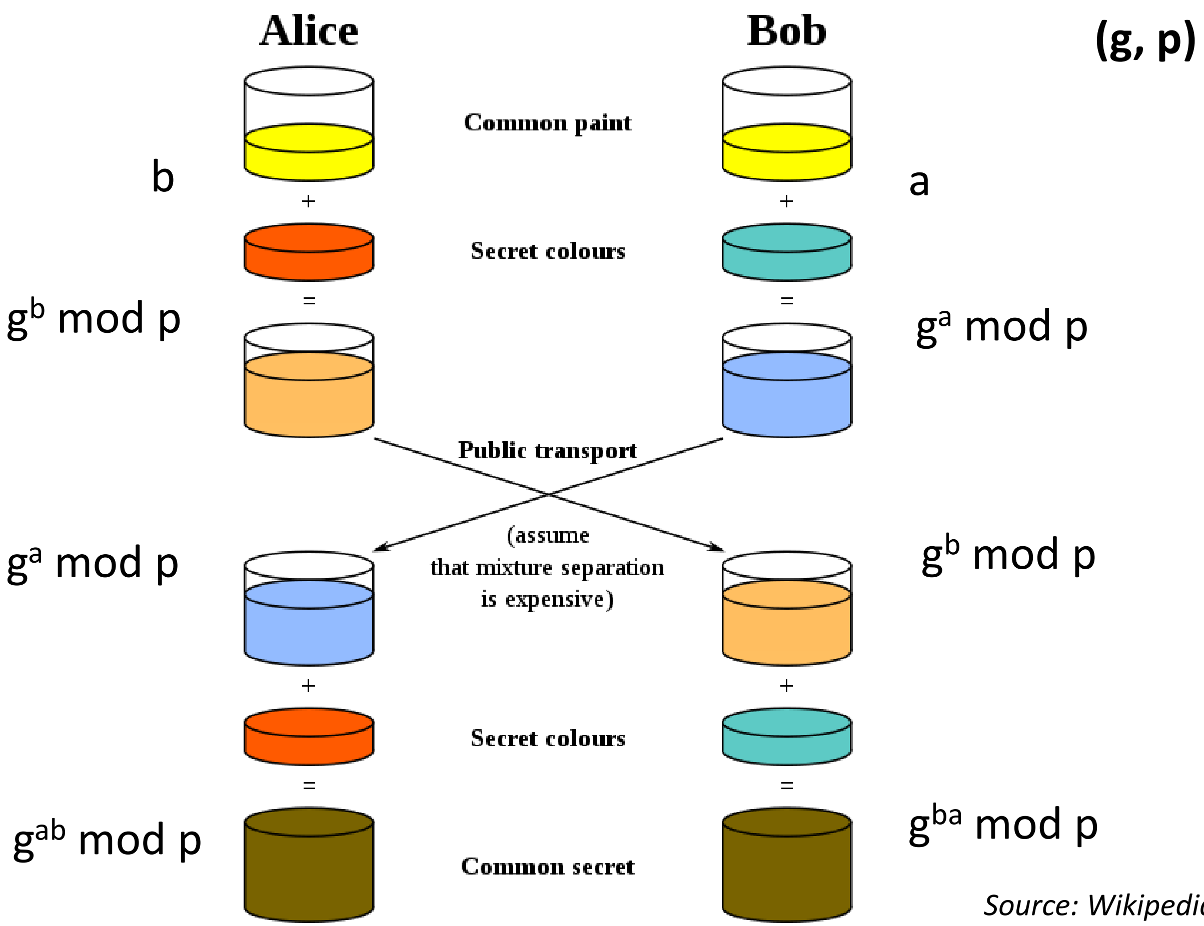
- During TLS Handshake Server communicate

(**g**, **p**) and choose a secret **x** and send **g^x mod p**

```
▷ Handshake Protocol: Certificate
▽ Handshake Protocol: Server Key Exchange
    Handshake Type: Server Key Exchange (12)
    Length: 342
  ▽ Diffie-Hellman Server Params
      p Length: 96
      p: e9e642599d355f37c97ffd3567120b8e25c9cd43e927b3a9...
      g Length: 96
      g: 30470ad5a005fb14ce2d9dcd87e38bc7d1b1c5facbaecbe9...
      Pubkey Length: 96
      Pubkey: 77b93a27c5d1e17755cd63a139b8c09f0e4f07b66d584a7d...
      Signature Length: 46
      Signature: 302c02146f4b8e2d573192e7cabe9849d2bf774688c9ec16...
```

```
openssl dhparam -inform PEM -in certs/dh -check -text
  PKCS#3 DH Parameters: (1024 bit)
    prime:
      00:ee:fe:6f:8a:c1:07:af:3c:91:22:44:76:3c:76:
      bf:9a:fc:7c:26:f2:0d:66:71:ad:fe:91:25:4c:9a:
      61:53:33:ce:03:e2:19:ee:c2:4e:bd:67:96:cf:0d:
      ac:14:36:0d:05:14:eb:d9:47:c2:49:fb:9a:ef:6a:
      31:97:62:f3:55:fa:55:a9:d0:c1:29:20:36:dd:41:
      9f:5c:c0:8c:ec:8b:dd:ef:ff:7a:ae:54:21:21:f9:
      39:cd:b8:55:42:10:9b:f2:cd:18:24:80:b4:ef:0f:
      df:e5:ac:da:ee:b7:c2:6a:be:cd:45:bc:86:fc:1d:
      6a:5c:ad:ad:ba:39:b1:86:03
    generator: 2 (0x2)
DH parameters appear to be ok.
```

Diffie Hellman Key Exchange in TLS



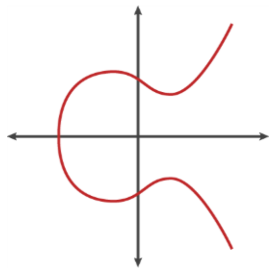
Source: Wikipedia

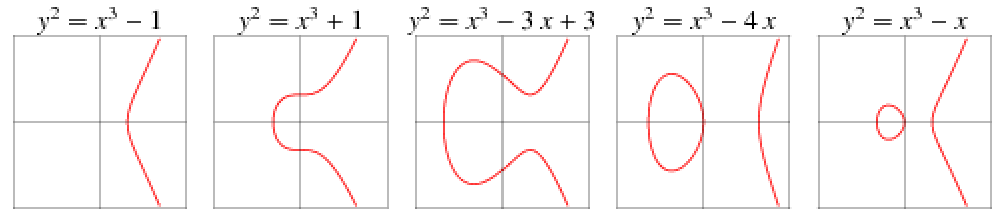
Perfect Forward Secrecy

- With **RSA,** main problem is if private key is compromised, all previous session can also be decrypted, since pre-master secret is encrypted with public key of server.
- With DH, exchange always uses new random values *a* and *b*, it is called *Ephemeral Diffie-Hellman* (EDH or DHE). **DHE-RSA-AES128-SHA** cipher suites uses this mechanism.

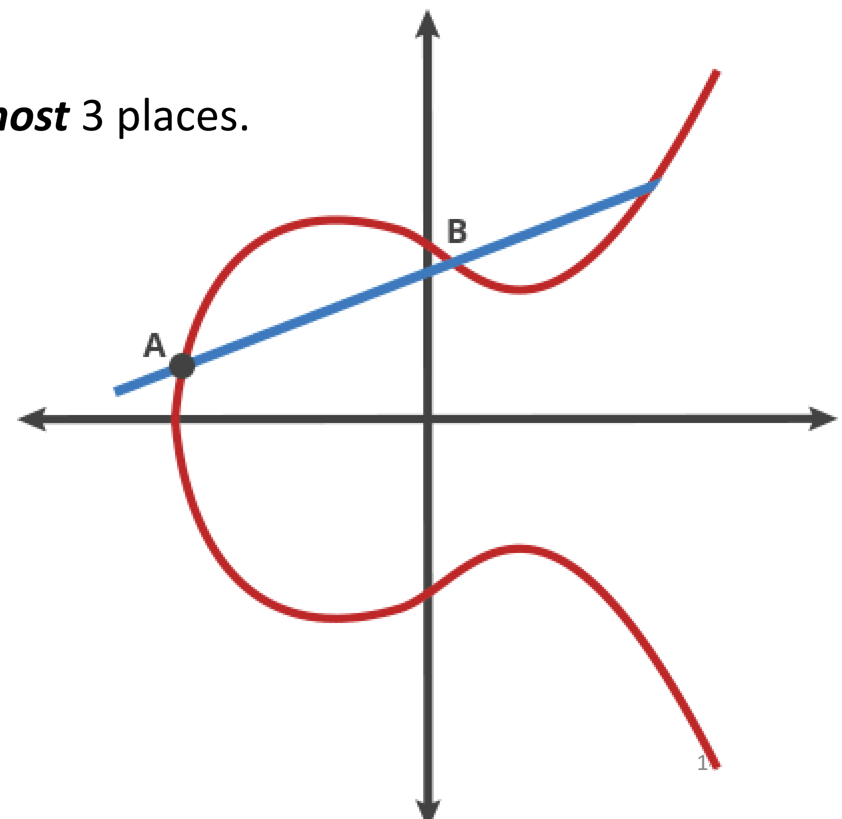
Elliptic Curve Cryptography

$y^2 = x^3 + \alpha x + \beta\ ; 4a^3+27b^2 \neq 0,\ a, b \in R\ Q\ C$





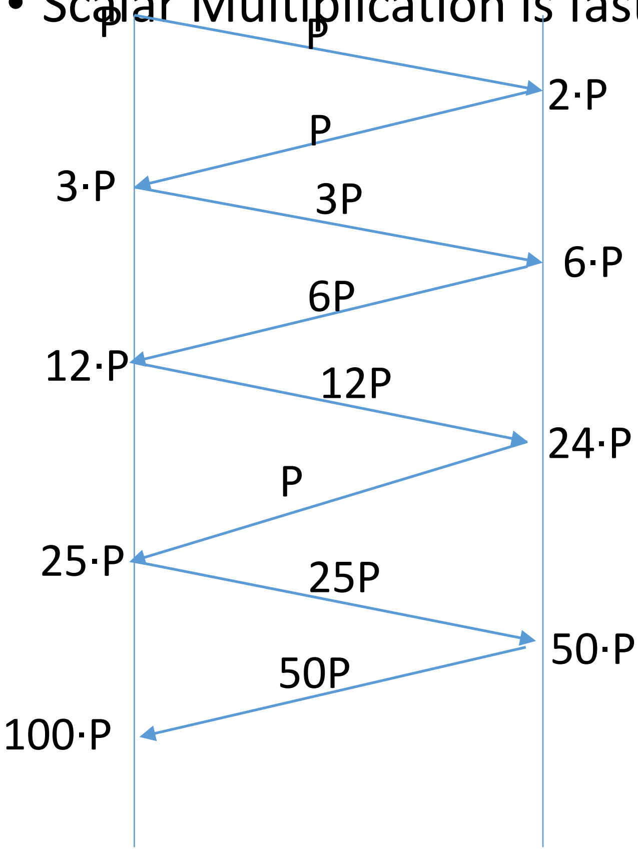
- Horizontal Symmetry.
- Non-vertical line intersect the curve ***at-most*** 3 places.
- Scalar Multiplication
- Fewer memory access & CPU resources.



- Existence of Inverse.
- Existence of Identity element(∞).
- Associativity & Closure also holds.

Elliptic Curve Discrete Logarithm Problem

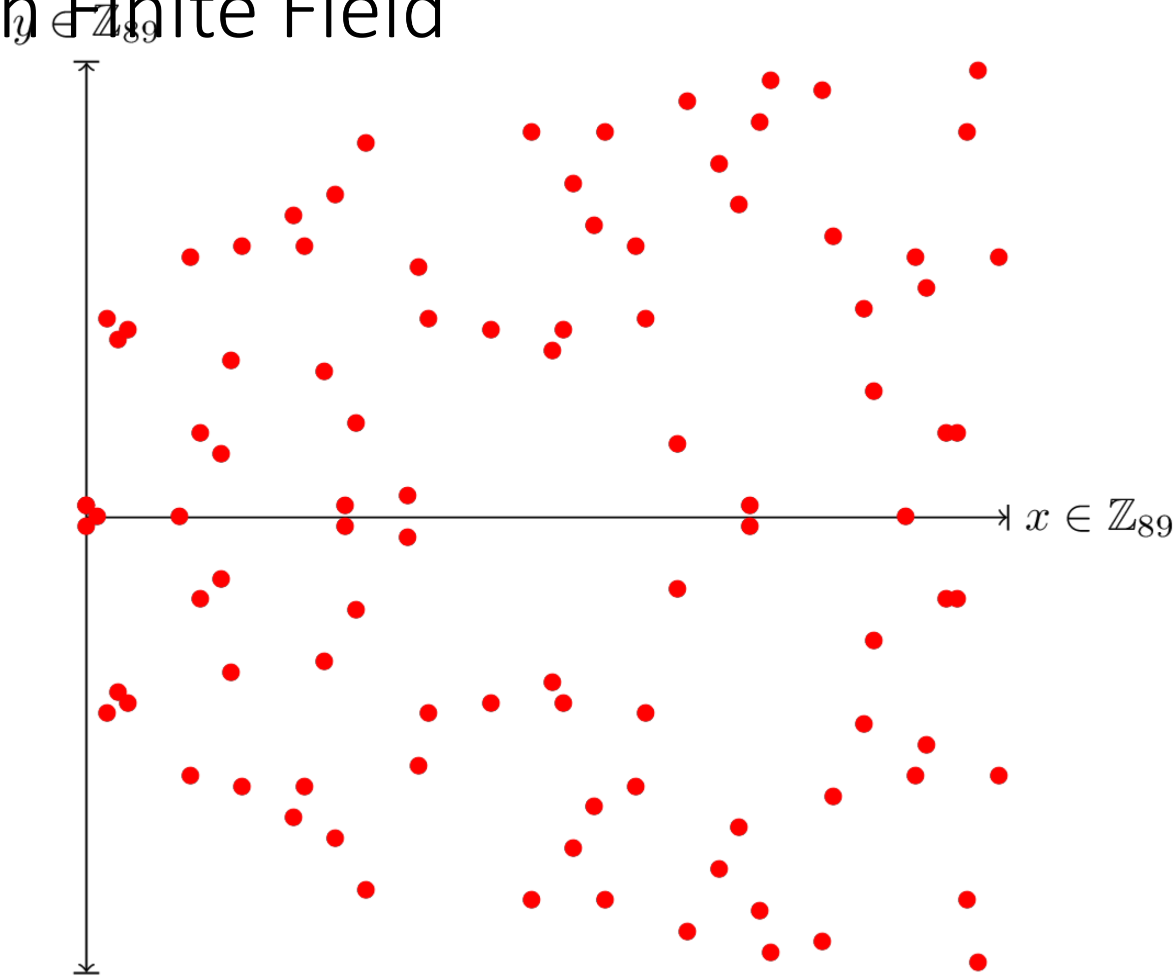
- Scalar Multiplication is fast **100·**P



Continued…

- Given starting point ***g*** and end point(**n.g**) , it is not easy to compute ***n(*****ECDLP*****).***
- Public Key: Starting Point A, Ending Point E
- Private Key: Number of hops from A to E
- Real curve : whole number, restrict to some prime.

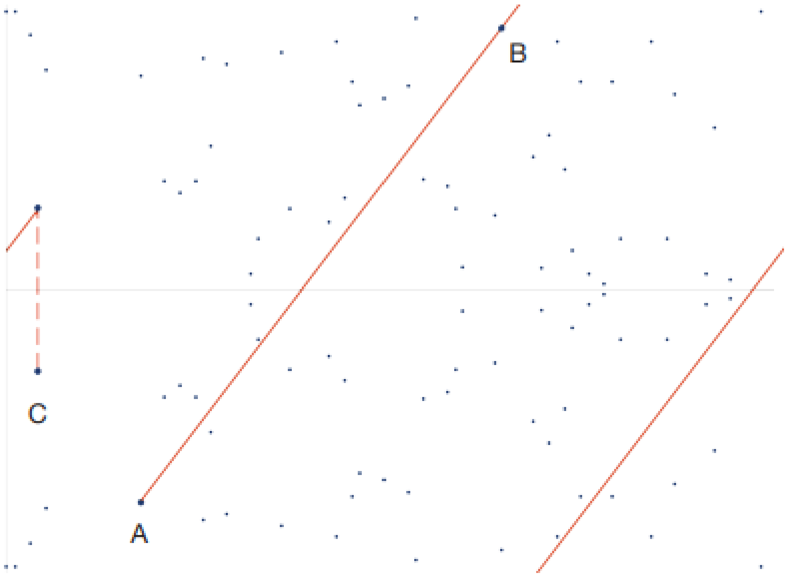
EC in Finite Field



$y^2 = x^3 - 2x + 1$ over Z_{89}

For $x = 4$, $y^2 = 57 \bmod 89$, Solve using Shank Tonelli Algorithm give {71,18}

Elliptical Curve in Practice



Curves

- Domain Parameter (g_x, g_y p, a, b, n), Typically known by CurveID in Cryptography
- Curve can be represented in different form
  - Montgomery form
  - Edward Curve
  - Koblitz Curve

Curve Name	Equation	
Secp256k1/secp256r1	$y^2 = x^3+7$	Key Share Entry: Group: secp256r1, Key Exchange length: 65 Group: secp256r1 (23) Key Exchange Length: 65 Key Exchange: 04dec803344e129156958317c1e6e2c201f437141a5c1e35…
Curve25519 https://tools.ietf.org/html/rfc7748	$y^2 = x^3+486662x^2+x$ then converted to **Montgomery Curve**. $v^2 = u^3+Au^2+u$	Key Share Entry: Group: x25519, Key Exchange length: 32 Group: x25519 (29) Key Exchange Length: 32 Key Exchange: 88641a8db264c7965f0515f762da6f85bb136e35638377f2…
Curve448	$y^2 + x^2 = 1 - 39081x^2y^2$	

https://safecurves.cr.yp.to/

Montgomery Curve

- http://web.math.princeton.edu/swim/SWIM%202010/Yao-Zhan%20Presentation%20SWIM%202010.pdf
- https://www.nayuki.io/page/elliptic-curve-point-addition-in-projective-coordinates

Elliptic Curve in TLS

- **ClientHello** specifies cipher suites like **ECDHE**-**ECDSA**-AES256-GCM-SHA384, **ECDHE**-**RSA**-AES256-GCM-SHA384 and also tells **supported groups** like secp256r1, x256519.
- **ServerHello** choose curve id and tells public key in **ServerKeyExchange** Extension. It also signs

```
TLSv1.2 Record Layer: Handshake Protocol: Server Hello
TLSv1.2 Record Layer: Handshake Protocol: Certificate
TLSv1.2 Record Layer: Handshake Protocol: Server Key Exchange
    Content Type: Handshake (22)
    Version: TLS 1.2 (0x0303)
    Length: 172
  ▽ Handshake Protocol: Server Key Exchange
      Handshake Type: Server Key Exchange (12)
      Length: 168
    ▽ EC Diffie-Hellman Server Params
        Curve Type: named_curve (0x03)
        Named Curve: x25519 (0x001d)
        Pubkey Length: 32
        Pubkey: 287efb7934ca39e1cf5c404bf2e29276d210d2ce7c0bdac9...
      ▽ Signature Algorithm: rsa_pss_rsae_sha256 (0x0804)
          Signature Hash Algorithm Hash: Unknown (8)
          Signature Hash Algorithm Signature: Unknown (4)
        Signature Length: 128
        Signature: 7f4141287ada8a317e3259d9addb4813739f89dc822ab375...
TLSv1.2 Record Layer: Handshake Protocol: Server Hello Done
```

```
▽ TLSv1.2 Record Layer: Handshake
    Content Type: Handshake (22)
    Version: TLS 1.2 (0x0303)
    Length: 37
  ▽ Handshake Protocol: Client K
      Handshake Type: Client K
      Length: 33
    ▽ EC Diffie-Hellman Client
        Pubkey Length: 32
        Pubkey: a099aabf73afc
▽ TLSv1.2 Record Layer: Change Ci
    Content Type: Change Cipher
    Version: TLS 1.2 (0x0303)
    Length: 1
    Change Cipher Spec Message
▽ TLSv1.2 Record Layer: Handshake
    Content Type: Handshake (22)
    Version: TLS 1.2 (0x0303)
    Length: 40
```

- **ClientKeyExchange** send its public value based on chosen curve-id.
- Both client and server now has shared secret i.e pre-master secret.

Conclusion

- Some NIST curve have backdoor.
  - https://en.wikipedia.org/wiki/Dual_EC_DRBG

Symmetric Key Size (bits)	RSA and Diffie-Hellman Key Size (bits)	Elliptic Curve Key Size (bits)
80	1024	160
112	2048	224
128	3072	256
192	7680	384
256	15360	521

Table 1: NIST Recommended Key Sizes