Cryptography and Network Security

ELLIPTIC CURVES

ELLIPTIC CURVE CRYPTOGRAPHY

Session Meta Data

Author	**Dr T Sree Sharmila**
Reviewer	
Version Number	1.0
Release Date	10 July 2018

Revision History

Revision Date	Details	Version no.
		1.0

Agenda

- Introduction
- Elliptic curve
- Elliptic curve cryptography
- Summary
- Test your understanding
- References

Lets start with a puzzle…

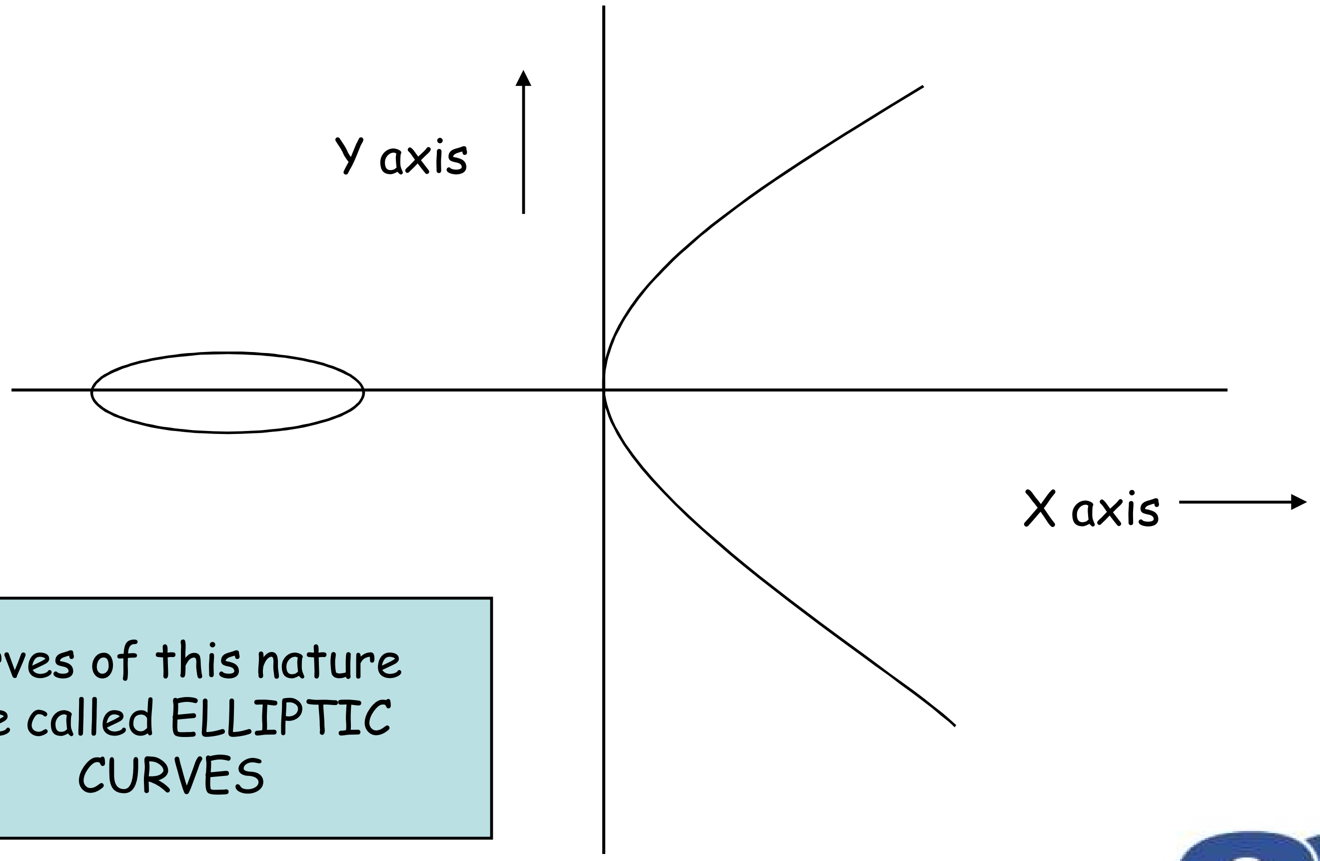
- **What is the number of balls that may be piled as a square pyramid and also rearranged into a square array?**
- **Soln:** Let x be the height of the pyramid…

Thus, $$1^2 + 2^2 + 3^2 + ... + x^2 = \frac{x(x+1)(2x+1)}{6}$$

We also want this to be a square:

Hence, $$\boxed{y^2 = \frac{x(x+1)(2x+1)}{6}}$$

Graphical Representation



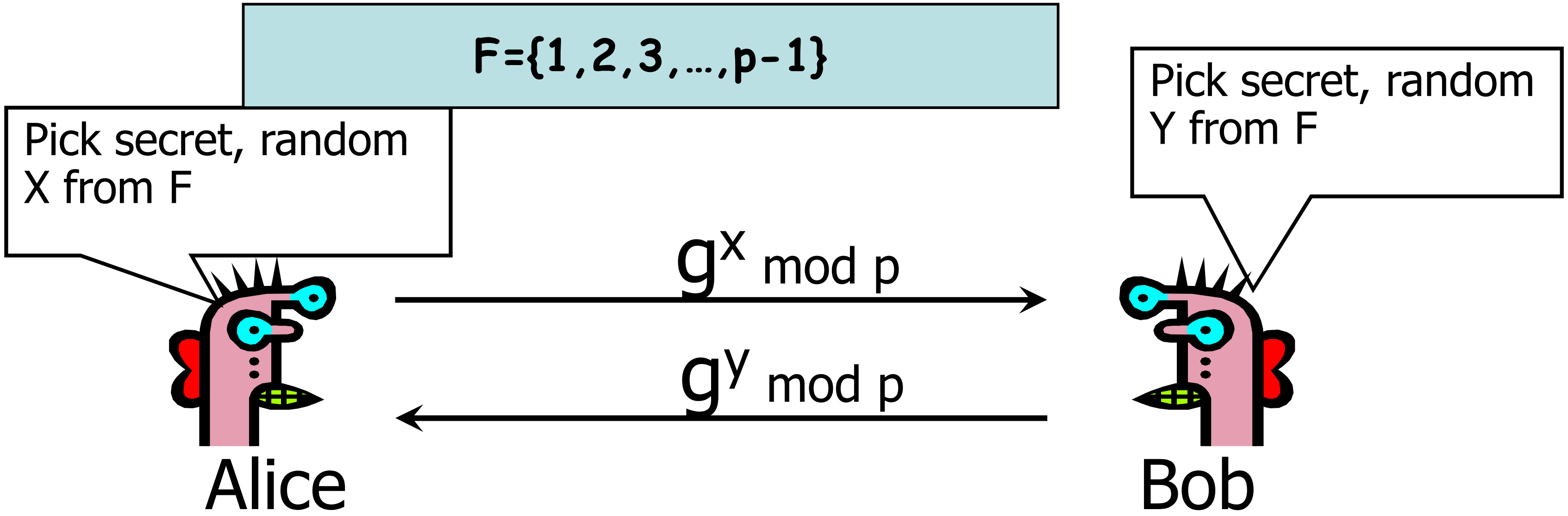
Curves of this nature are called ELLIPTIC CURVES

Introduction - ECC

- Elliptic Curve (EC) systems as applied to cryptography were first proposed in 1985 independently by Neal Koblitz and Victor Miller.

- The discrete logarithm problem on elliptic curve groups is believed to be more difficult than the corresponding problem in (the multiplicative group of nonzero elements of) the underlying finite field.

Discrete Logarithms in Finite Fields



Compute $k=(g^y)^x=g^{xy}$ mod p

Compute $k=(g^x)^y=g^{xy}$ mod p

Eve has to compute g^{xy} from g^x and g^y without knowing x and y…
She faces the Discrete Logarithm Problem in finite fields

Agenda

- Introduction
- Elliptic curve
- Elliptic curve cryptography
- Summary
- Test your understanding
- References

Elliptic Curve on a finite set of Integers

- Consider $y^2 = x^3 + 2x + 3 \pmod{5}$

  $x = 0 \Rightarrow y^2 = 3 \Rightarrow$ no solution $\pmod{5}$

  $x = 1 \Rightarrow y^2 = 6 = 1 \Rightarrow y = 1,4 \pmod{5}$

  $x = 2 \Rightarrow y^2 = 15 = 0 \Rightarrow y = 0 \pmod{5}$

  $x = 3 \Rightarrow y^2 = 36 = 1 \Rightarrow y = 1,4 \pmod{5}$

  $x = 4 \Rightarrow y^2 = 75 = 0 \Rightarrow y = 0 \pmod{5}$

- Then points on the elliptic curve are

  (1,1) (1,4) (2,0) (3,1) (3,4) (4,0)

  and the point at infinity: ∞

Using the finite fields we can form an Elliptic Curve Group where we also have a DLP problem which is harder to solve…

Definition of Elliptic curves

- An elliptic curve over a field ***K*** is a nonsingular cubic curve in two variables, *f(x,y) =0* with a rational point (which may be a point at infinity).

- The field ***K*** is usually taken to be the complex numbers, reals, rationals, algebraic extensions of rationals, p-adic numbers, or a **finite field**.

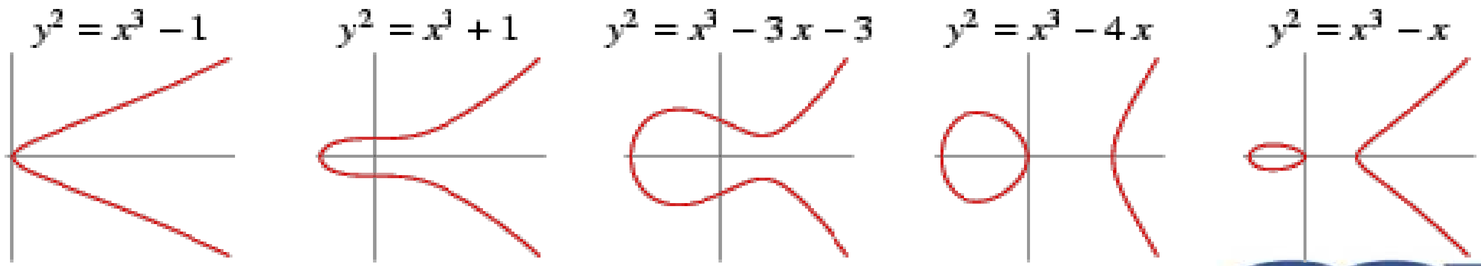
- Elliptic curves groups for cryptography are examined with the underlying fields of $\boldsymbol{F_p}$ (*where p>3 is a prime*) and $\boldsymbol{F_{2^m}}$ (*a binary representation with* 2^m *elements*).

General form of a EC

- An *elliptic curve* is a plane curve defined by an equation of the form

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

Examples



Weierstrass Equation

- A two variable equation F(x,y)=0, forms a curve in the plane. We are seeking geometric arithmetic methods to find solutions

- Generalized Weierstrass Equation of elliptic curves:

$$y^2 + a_1 xy + a_3 y = x^2 + a_2 x^2 + a_4 x + a_6$$

Here, A, B, x and y all belong to a field of say rational numbers, complex numbers, finite fields (F_p) or Galois Fields ($GF(2^n)$).

- **If Characteristic field is not 2:**

$$(y+\frac{a_1x}{2}+\frac{a_3}{2})^2 = x^3+(a_2+\frac{a_1^2}{4})x^2+a_4x+(\frac{a_3^2}{4}+a_6)$$
$$\Rightarrow y_1^{\ 2} = x^3+a_2^{'}x^2+a_4^{'}x+a_6^{'}$$

- **If Characteristics of field is neither 2 nor 3:**

$$x_1 = x+a_2^{'}/3$$
$$\Rightarrow y_1^{\ 2} = x_1^{\ 3}+Ax_1+B$$

Points on the Elliptic Curve (EC)

- Elliptic Curve over field L

$$E(L) = \{\infty\} \cup \{(x, y) \in L \times L \mid y^2 + \ldots = x^3 + \ldots\}$$

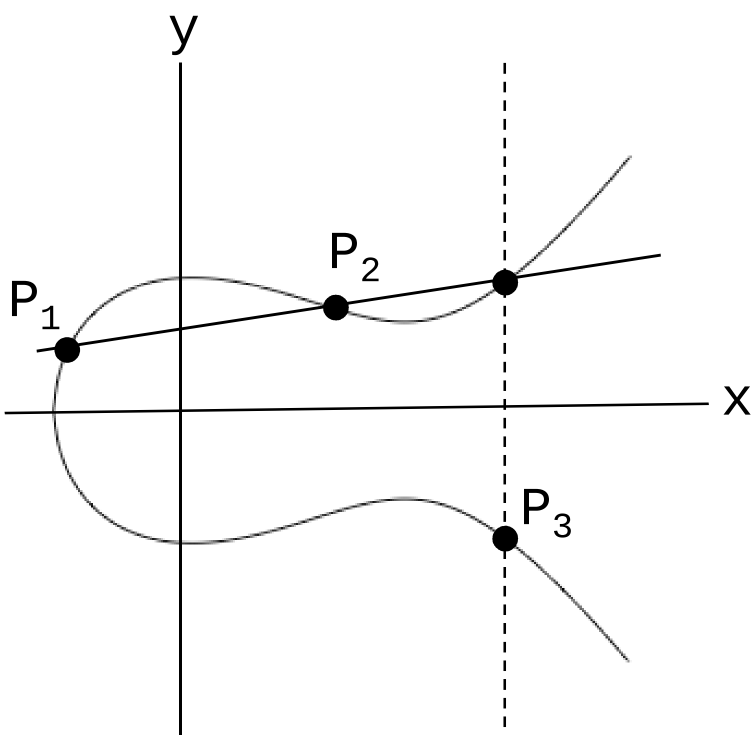
- It is useful to add the point at infinity
- The point is sitting at the top of the y-axis and any line is said to pass through the point when it is vertical
- It is both the top and at the bottom of the y-axis

The Abelian Group

Given two points P,Q in *E(Fp)*, there is a third point, denoted by *P+Q* on *E(Fp)*, and the following relations hold for all P,Q,R in *E(Fp)*

- $P + Q = Q + P$ (*commutativity*)
- $(P + Q) + R = P + (Q + R)$ (*associativity*)
- $P + O = O + P = P$ (*existence of an identity element*)
- there exists $(-P)$ such that $-P + P = P + (-P) = O$ (*existence of inverses*)

Elliptic Curve Picture



- Consider elliptic curve

  $E: y^2 = x^3 - x + 1$

- If P_1 and P_2 are on E, we can define

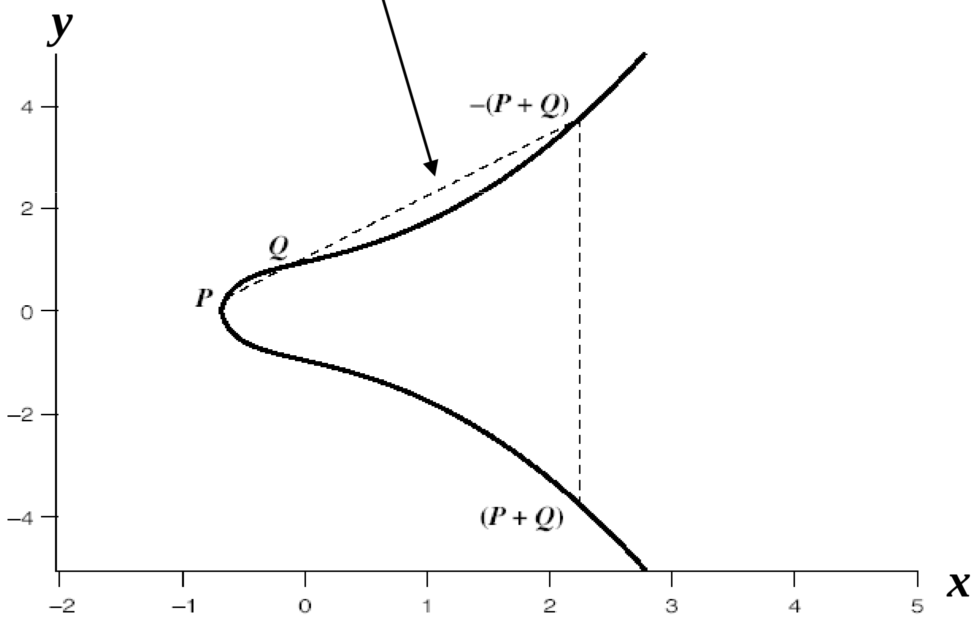
  $P_3 = P_1 + P_2$

  as shown in picture

- Addition is all we need

Addition in Affine Co-ordinates

$y=m(x-x_1)+y_1$



$y^2=x^3+Ax+B$

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

Let, P≠Q,

$$m=\frac{y_2-y_1}{x_2-x_1};$$

To find the intersection with E. we get

$$(m(x-x_1)+y_1)^2=x^3+Ax+B$$
$$or,0=x^3-m^2x^2+\ldots$$
$$So,x_3=m^2-x_1-x_2$$
$$\Rightarrow y_3=m(x_1-x_2)-y_1$$

Doubling of a point

- Let, P=Q

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

$$\Rightarrow m = \frac{dy}{dx} = \frac{3x_1^2 + A}{2y_1}$$

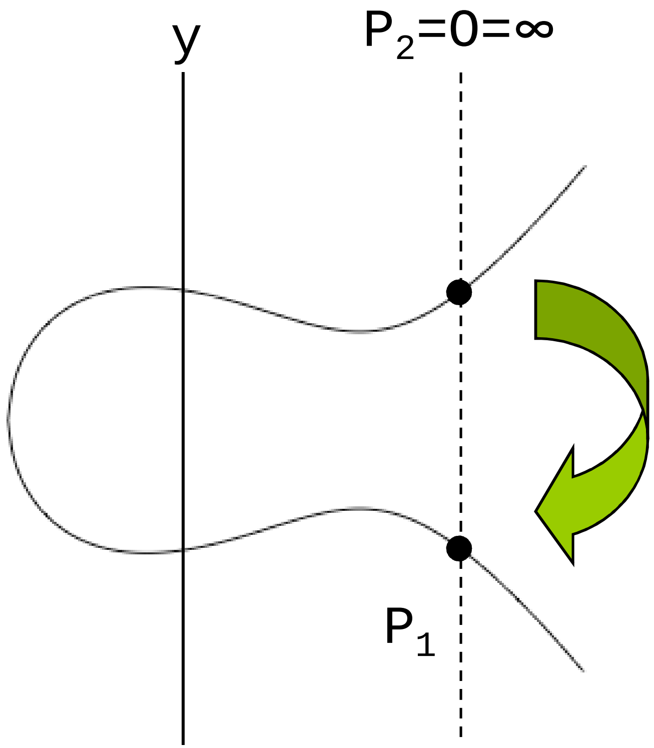
$$If\ , y_1 \neq 0 \text{ (since then } \mathrm{P_1+P_2=\infty}\text{):}$$

$$\therefore 0 = x^3 - m^2x^2 + \ldots$$

$$\Rightarrow x_3 = m^2 - 2x_1, y_3 = m(x_1 - x_3) - y_1$$

- What happens when $P_2=\infty$?

Why do we need the reflection?



$P_1 = P_1 + O = P_1$

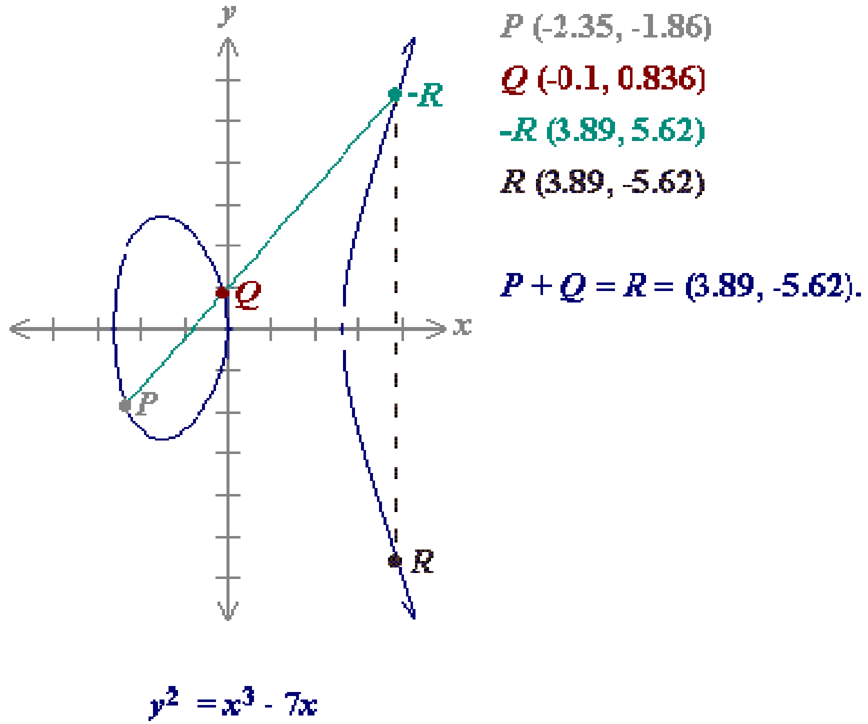
Sum of two points

Define for two points ***P* (x_1,y_1)** and **Q (x_2,y_2)** in the Elliptic curve

$$\lambda = \begin{cases} \dfrac{y_2 - y_1}{x_2 - x_1} & for\_x_1 \neq x_2 \\ \dfrac{3x_1^2 + a}{2y_1} & for\_x_1 = x_2 \end{cases}$$

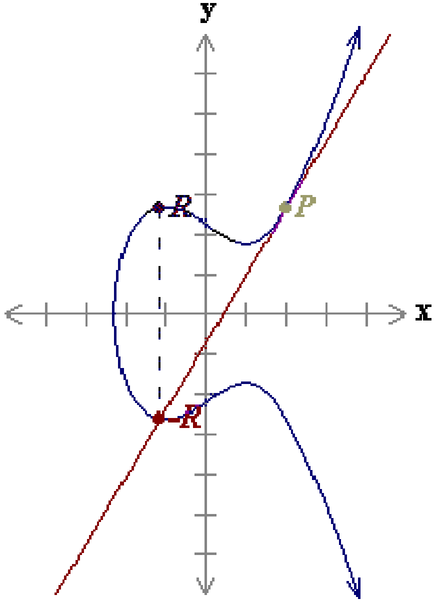
Then ***P+Q*** is given by ***R*(x_3,y_3)** :

$$\boxed{\begin{aligned} x_3 &= \lambda - x_1 - x_2 \\ y_3 &= \lambda(x_3 - x_1) + y_1 \end{aligned}}$$



Point at infinity *O*

P+P = 2P



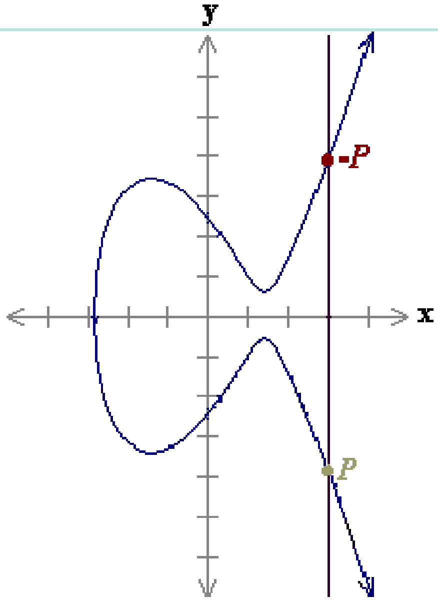
$P\ (2, 2.65)$

$-R\ (-1.11, -2.64)$

$R\ (-1.11, 2.64)$

$2P = R = (-1.11, 2.64).$

$y^2 = x^3 - 3x + 5$



$P + (-P) = O$

$y^2 = x^3 - 6x + 6$

As a result of the above case ***P=O+P***

***O* is called the additive identity of the elliptic curve group.**

Hence all elliptic curves have an additive identity ***O***.

Projective Co-ordinates

- Two-dimensional projective space P_K^2 over *K* is given by the equivalence classes of triples (x,y,z) with x,y z in K and at least one of x, y, z nonzero.
- Two triples (x_1,y_1,z_1) and (x_2,y_2,z_2) are said to be equivalent if there exists a non-zero element λ in K, st:
  - $(x_1,y_1,z_1) = (\lambda x_2, \lambda y_2, \lambda z_2)$
  - The equivalence class depends only the ratios and hence is denoted by (x:y:z)

Projective Co-ordinates

- If z≠0, (x:y:z)=(x/z:y/z:1)
- What is z=0? We obtain the point at infinity.
- The two dimensional affine plane over K:

$$A_K^2 = \{(x, y) \in K \times K\}$$

Hence using,

$$(x, y) \rightarrow (X : Y : 1)$$

$$\Rightarrow A_K^2 = P_K^2$$

There are advantages with projective co-ordinates from the implementation point of view

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

If Characteristics of field is not 3:

$$y^2 = f(x) = x^3 + Ax + B$$

1. **Hence condition for no singularity is $4A^3+27B^2 \neq 0$**
2. **Generally, EC curves have no singularity**

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

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

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

$\therefore$ f has a double root

$$y^2 = x^3 + Ax + B$$

For double roots,

$$x^3 + Ax + B = 3x^2 + A = 0$$

$$\Rightarrow x^2 = -A/3.$$

Also, $x^4 + Ax^2$+Bx=0,

$$\Rightarrow \frac{A^2}{9} - \frac{A^2}{3} + Bx = 0$$

$$\Rightarrow x = \frac{2A^2}{9B}$$

$$\Rightarrow 3(\frac{2A^2}{9B})^2 + A = 0$$

$$\Rightarrow 4A^3 + 27B^2 = 0$$

Elliptic Curves in Characteristic 2

- Generalized Equation:

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

- If a_1 is not 0, this reduces to the form:

$$y^2 + xy = x^3 + Ax^2 + B$$

- If a_1 is 0, the reduced form is:

$$y^2 + Ay = x^3 + Bx + C$$

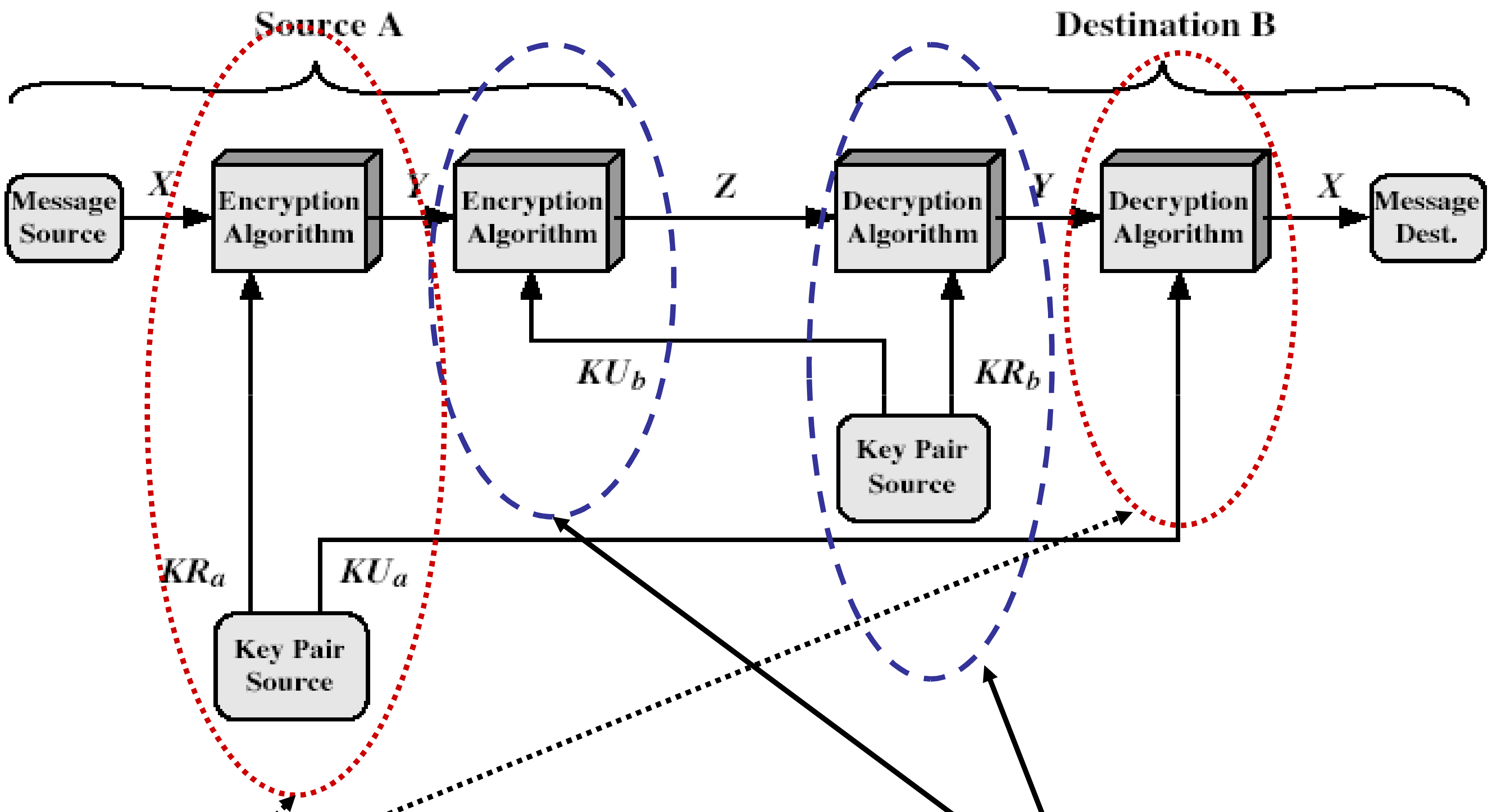
- Note that the form cannot be:

$$y^2 = x^3 + Ax + B$$

Agenda

- Introduction
- Elliptic curve
- Elliptic curve cryptography
- Summary
- Test your understanding
- References

Public-Key Cryptosystems

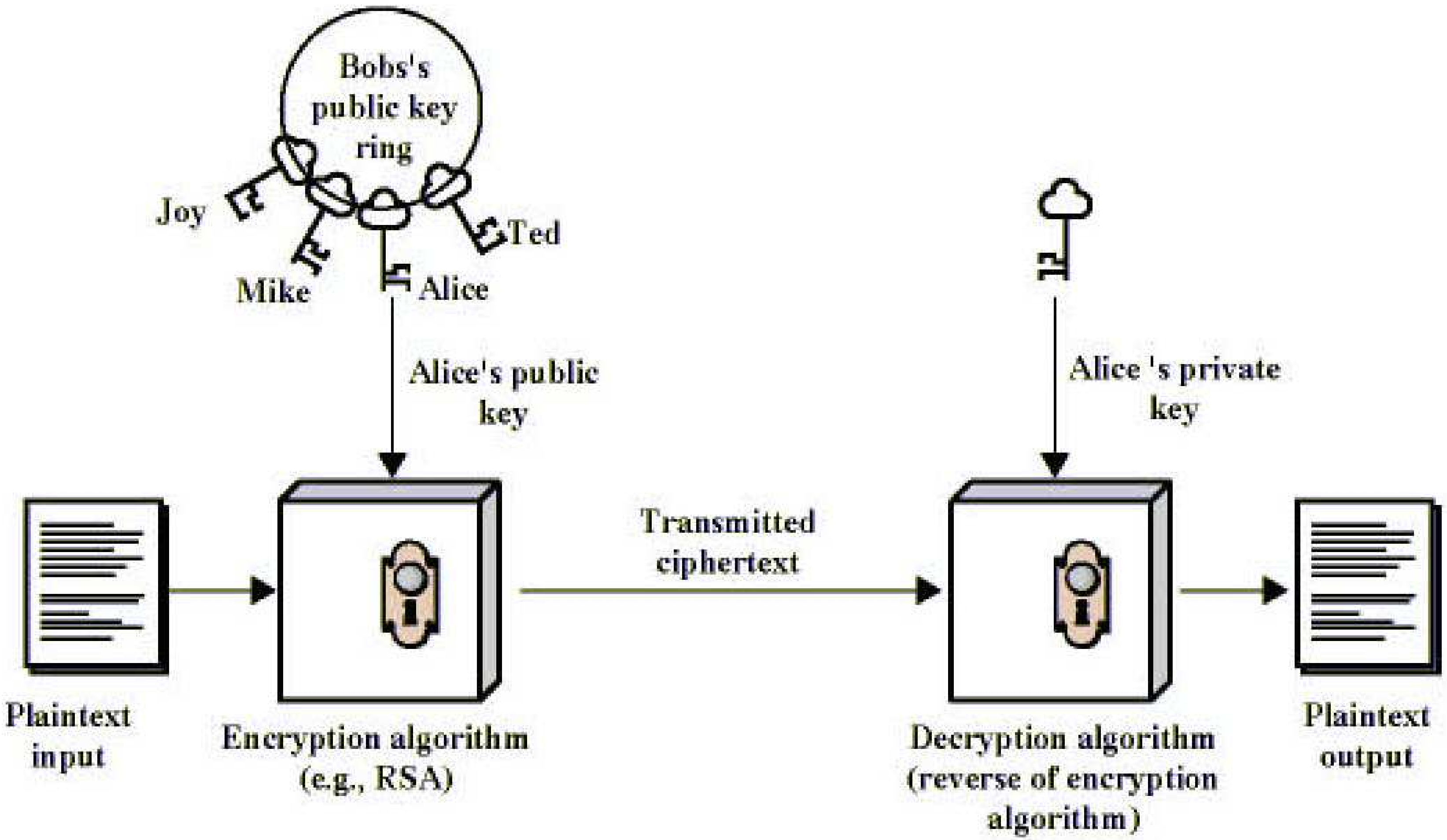


Public-Key Cryptosystem: Secrecy and Authentication

Authentication: Only **A** can generate the encrypted message

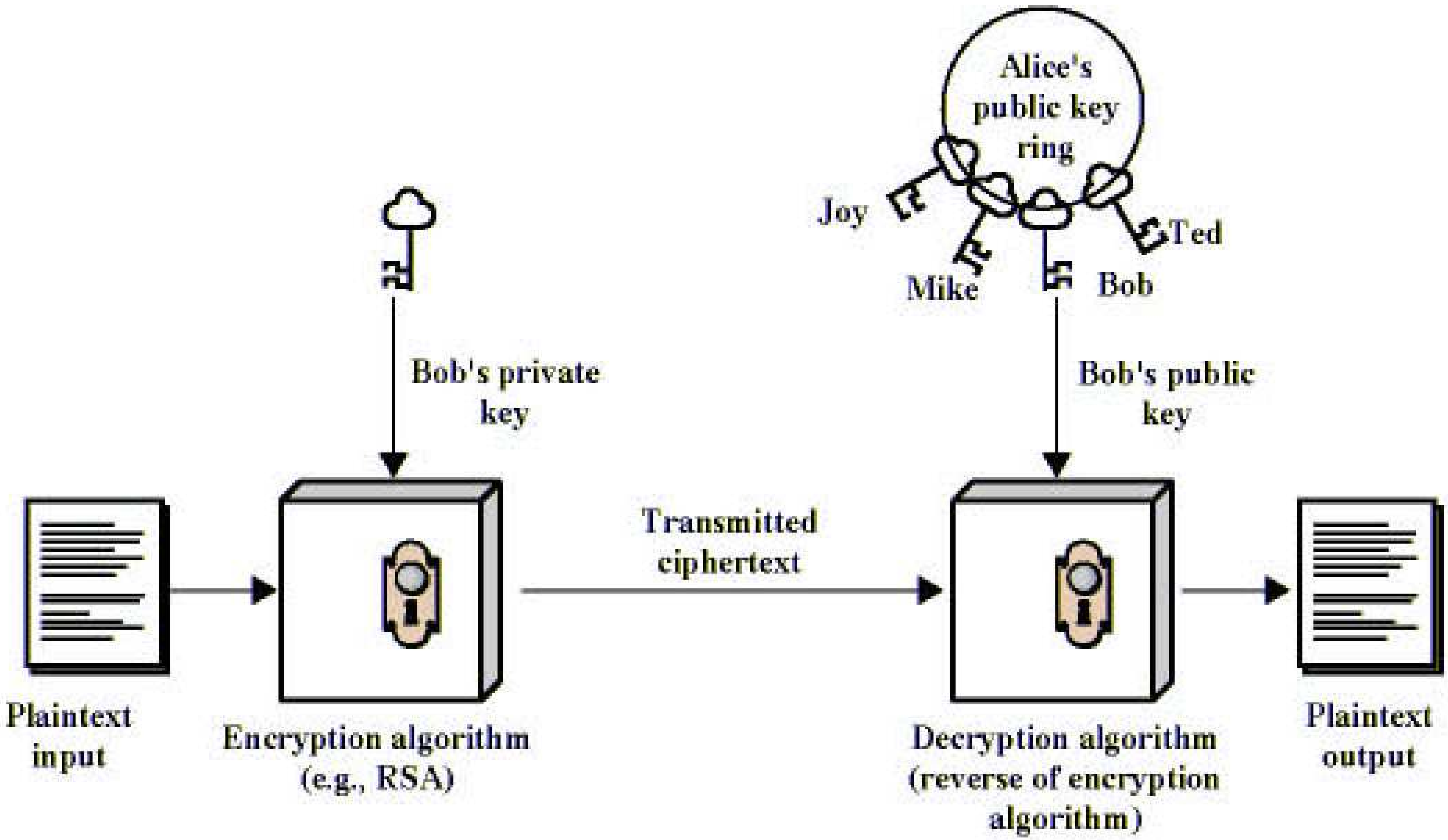
Secrecy: Only **B** can Decrypt the message

Public-Key Cryptography



(a) Encryption

Public-Key Cryptography



(b) Authentication

What Is Elliptic Curve Cryptography (ECC)?

- Elliptic curve cryptography [ECC] is a **public-key** cryptosystem just like RSA, Rabin, and El Gamal.
- Every user has a **public** and a **private** key.
  - Public key is used for encryption/signature verification.
  - Private key is used for decryption/signature generation.
- Elliptic curves are used as an extension to other current cryptosystems.
  - Elliptic Curve Diffie-Hellman Key Exchange
  - Elliptic Curve Digital Signature Algorithm

Using Elliptic Curves In Cryptography

- The central part of any cryptosystem involving elliptic curves is the **elliptic group**.
- All public-key cryptosystems have some underlying mathematical operation.
  - RSA has exponentiation (raising the message or ciphertext to the public or private values)
  - ECC has point multiplication (repeated addition of two points).

Generic Procedures of ECC

- Both parties agree to some publicly-known data items
  - The **elliptic curve equation**
    - values of ***a*** and ***b***
    - prime, ***p***
  - The **elliptic group** computed from the elliptic curve equation
  - A **base point**, B, taken from the elliptic group
    - Similar to the generator used in current cryptosystems
- Each user generates their public/private key pair
  - Private Key = an integer, x, selected from the interval [1, p-1]
  - Public Key = product, Q, of private key and base point
    - (Q = x*B)

Example – Elliptic Curve Cryptosystem Analog to El Gamal

- Suppose Alice wants to send to Bob an encrypted message.
  - Both agree on a base point, B.
  - Alice and Bob create public/private keys.
    - Alice
      - Private Key = a
      - Public Key = $P_A = a * B$
    - Bob
      - Private Key = b
      - Public Key = $P_B = b * B$
  - Alice takes plaintext message, M, and encodes it onto a point, P_M, from the elliptic group

Example – Elliptic Curve Cryptosystem Analog to El Gamal

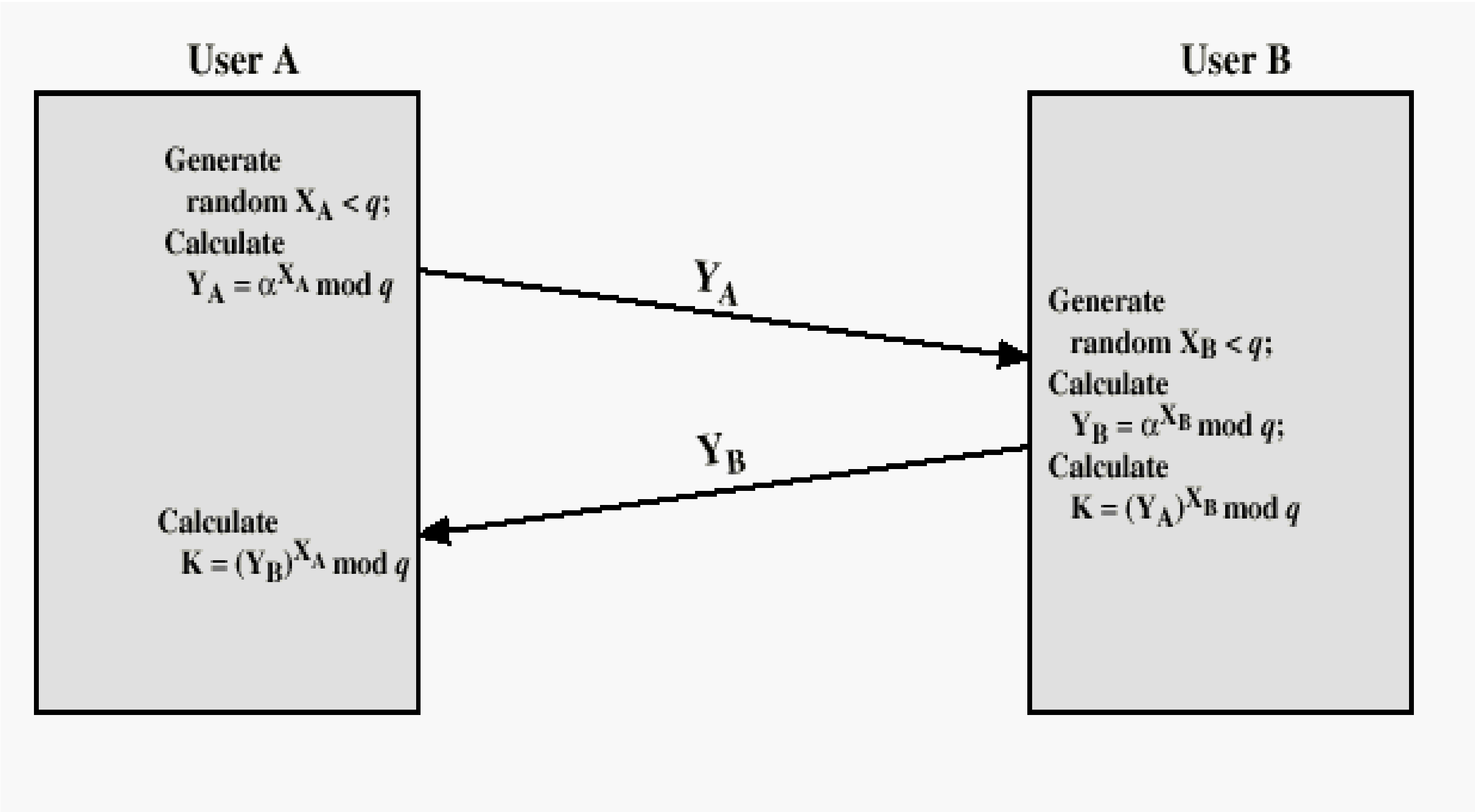
- Alice chooses another random integer, k from the interval [1, p-1]
- The ciphertext is a pair of points
  - **P_C = [(kB), (P_M + kP_B)]**
- To decrypt, Bob computes the product of the first point from P_C and his private key, b
  - **b * (kB)**
- Bob then takes this product and subtracts it from the second point from P_C
  - **(P_M + kP_B) – [b(kB)] = P_M + k(bB) – b(kB) = P_M**
- Bob then decodes P_M to get the message, M.

Example – Compare to El Gamal

- The ciphertext is a pair of points
  - $P_C = [(kB), (P_M + kP_B)]$
- The ciphertext in El Gamal is also a pair.
  - $C = (g^k \bmod p, mP_B{}^k \bmod p)$

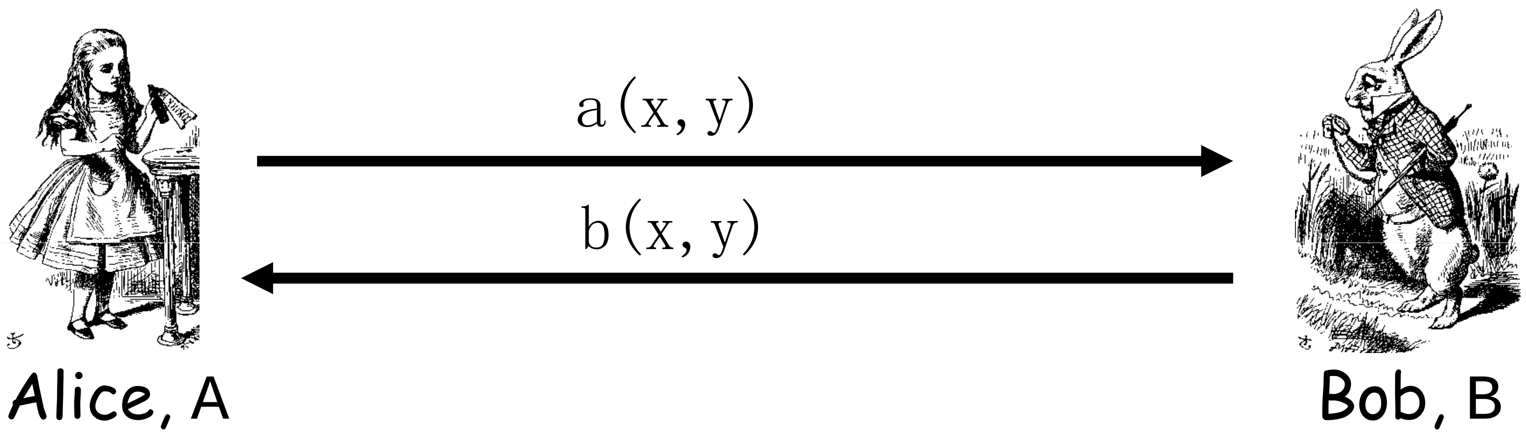
- Bob then takes this product and subtracts it from the second point from P_C
  - $(P_M + kP_B) – [b(kB)] = P_M + k(bB) – b(kB) = P_M$
- In El Gamal, Bob takes the quotient of the second value and the first value raised to Bob's private value
  - $m = mP_B{}^k / (g^k)^b = mg^{k*b} / g^{k*b} = m$

Diffie-Hellman (DH) Key Exchange



ECC Diffie-Hellman

- **Public:** Elliptic curve and point B=(x, y) on curve
- **Secret:** Alice's a and Bob's b



- Alice computes a(b(x, y))
- Bob computes b(a(x, y))
- These are the same since ab = ba

Example – Elliptic Curve Diffie-Hellman Exchange

- Alice and Bob want to agree on a shared key.
  - Alice and Bob compute their public and private keys.
    - Alice
      - » Private Key = a
      - » Public Key = P_A = a * B
    - Bob
      - » Private Key = b
      - » Public Key = P_B = b * B
  - Alice and Bob send each other their public keys.
  - Both take the product of their private key and the other user's public key.
    - Alice → K_{AB} = a(bB)
    - Bob → K_{AB} = b(aB)
    - **Shared Secret Key = K_{AB} = abB**

Why use ECC?

- How do we analyze Cryptosystems?
  - How difficult is the underlying problem that it is based upon
    - RSA – Integer Factorization
    - DH – Discrete Logarithms
    - ECC - Elliptic Curve Discrete Logarithm problem
  - How do we measure difficulty?
    - We examine the algorithms used to solve these problems

Security of ECC

- To **protect** a 128 bit AES key it would take a:
  - RSA Key Size: 3072 bits
  - ECC Key Size: 256 bits
- How do we strengthen RSA?
  - Increase the key length
- **Impractical?**

NIST guidelines for public key sizes for AES

ECC KEY SIZE (Bits)	RSA KEY SIZE (Bits)	KEY SIZE RATIO	AES KEY SIZE (Bits)
163	1024	1 : 6	
256	3072	1 : 12	128
384	7680	1 : 20	192
512	15 360	1 : 30	256

Supplied by NIST to ANSI X9F1

Applications of ECC

- Many devices are small and have limited storage and computational power
- Where can we apply ECC?
  - **Wireless communication devices**
  - Smart cards
  - Web servers that need to handle many encryption sessions
  - **Any application where security is needed but lacks the power, storage and computational power that is necessary for our current cryptosystems**

Benefits of ECC

- Same benefits of the other cryptosystems: confidentiality, integrity, authentication and non-repudiation but…
- Shorter key lengths
  – Encryption, Decryption and Signature Verification speed up
  – Storage and bandwidth savings

Comparable Key Sizes for Equivalent Security

Symmetric scheme (key size in bits)	ECC-based scheme (size of *n* in bits)	RSA/DSA (modulus size in bits)
56	112	512
80	160	1024
112	224	2048
128	256	3072
192	384	7680
256	512	15360

Agenda

- Introduction
- Elliptic curve
- Elliptic curve cryptography
- Summary
- Test your understanding
- References

Summary of ECC

- "**Hard problem**" analogous to discrete log
  - **Q=kP, where Q, P belong to a prime curve**

    given k, P → "easy" to compute Q

    given Q, P → "hard" to find k
  - **known as the elliptic curve logarithm problem**
    - **k must be large enough**
- ECC security relies on elliptic curve logarithm problem
  - compared to factoring, can use much smaller key sizes than with RSA etc

    → for similar security ECC offers significant computational advantages

Agenda

- Introduction
- Elliptic curve
- Elliptic curve cryptography
- Summary
- Test your understanding
- References

Test your understanding

1) What is an elliptic curve?
2) What is the zero point of an elliptic curve?
3) What is the sum of three points on an elliptic curve that lie on a straight line?
4) Does the elliptic curve equation $y^2 = x^3 + 10x + 5$ define a group over Z_{17}?

Agenda

- Introduction
- Elliptic curve
- Elliptic curve cryptography
- Summary
- Test your understanding
- References

References

1. William Stallings, Cryptography and Network Security, 6th Edition, Pearson Education, March 2013.
2. Charlie Kaufman, Radia Perlman and Mike Speciner, “Network Security”, Prentice Hall of India, 2002.