Assignment Topics

Topic 1 - **ONLINE VOTING SYSTEM**

- In this system people who have citizenship of India and whose age is above 18 years and any sex can **cast their vote online** without going to any physical polling station.

- There is a database which is maintained by the Independent Electoral Commission of India (IEBC) in which all the necessary information is stored.

- Design a secure framework for the **online authentication**

  - Suggest possible attacks for the chosen scenario.
  - Choose one of the attacks and recommend a service and suitable techniques to implement.
  - Formulate a security framework defining appropriate algorithms and their crypt analysis.
  - Highlight your contribution

Topic 2 - **ONLINE VOTING SYSTEM**

- In this system people who have citizenship of India and whose age is above 18 years and any sex can cast their vote online without going to any physical polling station. Voter can vote only once. There is a database which is maintained by the Independent Electoral Commission of India in which all the necessary information is stored.

- **Design A FRAME WORK to achieve the Privacy of the voting**
  - Vote can be known only by voter and tallying officer in ECI.
    - Suggest possible attacks for the chosen scenario.
    - Choose one of the attacks and recommend a service and suitable techniques to implement.
    - Formulate a security framework defining appropriate algorithms and their crypt analysis.
    - **Highlight your contribution**

TOPIC 3 - Secure banking system

- Bank accounts will be accessible to all users who have a valid user Id and password.
- A customer can access his account from anywhere.
- A customer can request details of last n number of transaction he has performed on any account.
- A customer can make a fund transfer to another account in the same bank.
- A customer can view his monthly statements.
  - **Suggest possible attacks for the chosen scenario.**
  - **Choose one of the attacks and recommend a service and suitable techniques to implement.**
  - **Formulate a security framework defining appropriate algorithms and their crypt analysis.**
  - **Highlight your contribution**

Topic 4 - Doctor's office

- Describe the **business threats** posed by each of the following situations and explain what its effect may be if a Web application is compromised:

- A local doctor's office that keeps all patient information in the private cloud

- Identify the specific attacks, possible for the chosen scenario
- Choose one of the attacks and recommend a service and suitable techniques to implement.
- Formulate a security framework defining appropriate algorithms and their cryptanalysis.
- Highlight your contributions

Topic 5 – A Private law firm

- Describe the business threats posed by each of the following situations and explain what its effect may be if a Web application is compromised

- A small, private law firm's website with forms for potential clients to complete, including name, address, contact number, and reason for scheduling an appointment, including the reason for scheduling appointment, in the event of a web breach customers' legal or other personal information could be leaked.

  - Identify the specific attacks, possible for the chosen scenario
  - Choose one of the attacks and recommend a service and suitable techniques to implement.
  - Formulate a security framework defining appropriate algorithms and their crypt analysis.
  - Highlight your contributions

Topic 6 – Online parking/ Toll pass payment

- Describe the business threats posed by each of the following situations and explain what its effect may be if a Web application is compromised:
- A city government that allows people with parking tickets and toll pass to pay the fees and fines online using a credit card or online check.
- Financial fraud or identity theft; customer information could be compromised including personal payment information. False payments could be made online.
  - Identify the specific attacks, possible for the chosen scenario
  - Choose one of the attacks and recommend a service and suitable techniques to implement.
  - Formulate a security framework defining appropriate algorithms and their crypt analysis.
  - Highlight your contributions

Topic 7 Fine-grained access control in cloud

- Design goal is to help the data owner **achieve fine-grained access control on files stored by Cloud Servers.**

- Specifically, we want to enable the data owner to enforce a unique access structure on each user, which precisely designates the set of files that the user is allowed to access.

- We also want to prevent Cloud Servers from being able to learn both the data file contents and user access privilege information.

  - Identify the specific attacks, possible for the chosen scenario
  - Choose one of the attacks and recommend a service and suitable techniques to implement.
  - Formulate a security framework defining appropriate algorithms and their crypt analysis.
  - Highlight your contributions

Elliptic Curve Cryptography

What's wrong with RSA?

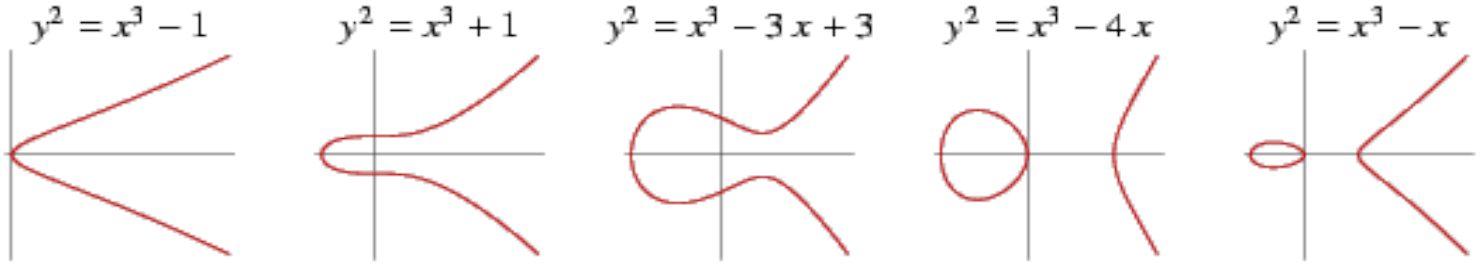
- RSA is based upon the 'belief' that factoring is 'difficult' – never been proven
- Prime numbers are getting too large
- Amount of research currently devoted to factoring algorithms
- Quantum computing will make RSA obsolete overnight

General form of a EC

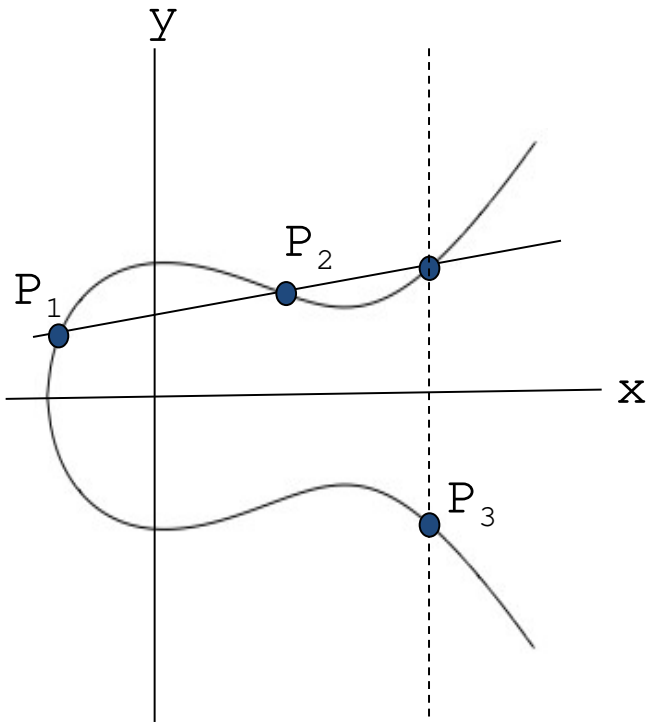
- An *elliptic curve* is a plane curve defined by an equation of the form

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

Examples



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

Sum of two points

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

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

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

$$x_3 = \lambda^2 - x_1 - x_2$$

$$y_3 = \lambda(x_3 - x_1) + y_1$$

Information on Elliptic Curves and Groups

- Elliptic curves are algebraic/geometric entities that have been studied extensively for the past 150 years.
- Has emerged a rich and deep theory.
- Cryptosystems often require the use of **algebraic groups**.
- A group is a **set of elements** with **custom-defined arithmetic operations** on those elements.
- Elliptic curves may be used to form **elliptic curve groups.**
- For elliptic curve groups, these specific operations are defined **geometrically**.
- Introducing more **stringent properties** to the elements of a group,
  - Eg. **limiting the number of points** on such a curve, creates an underlying **field for an elliptic curve group.**

Group

A group is an algebric system consisting of a set G together with a binary operation * defined on G satisfying the following axioms :

1. Closure : for all x,y in G we have $x * y \in G$
2. Associativity : for all x,y and z in G we have
   $(x * y) * z = x * (y * z)$
3. Identity : there exists an e in G such that $x * e = e * x = x$

   for all x
4. Inverse : for all x in G there exists y in G such that

   $x * y = y * x = e$

In addition if for x, y in G we have x * y = y * x then we say that group G is **abelian**.

An elliptic curve over real numbers

- It is defined as the set of points (x,y) which satisfy an elliptic curve equation of the form:

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

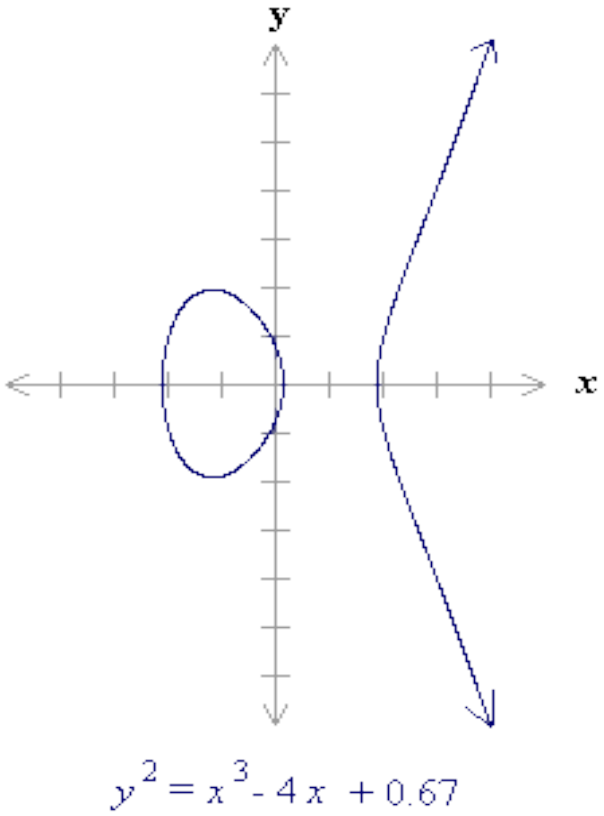
where x, y, a and b are real numbers.

- Each choice of the numbers a and b yields a different elliptic curve.

- For example, a = -4 and b = 0.67 gives the elliptic curve with equation

$$y^2 = x^3 - 4x + 0.67;$$

the graph of this curve is shown.



An EC over real numbers – cont'd

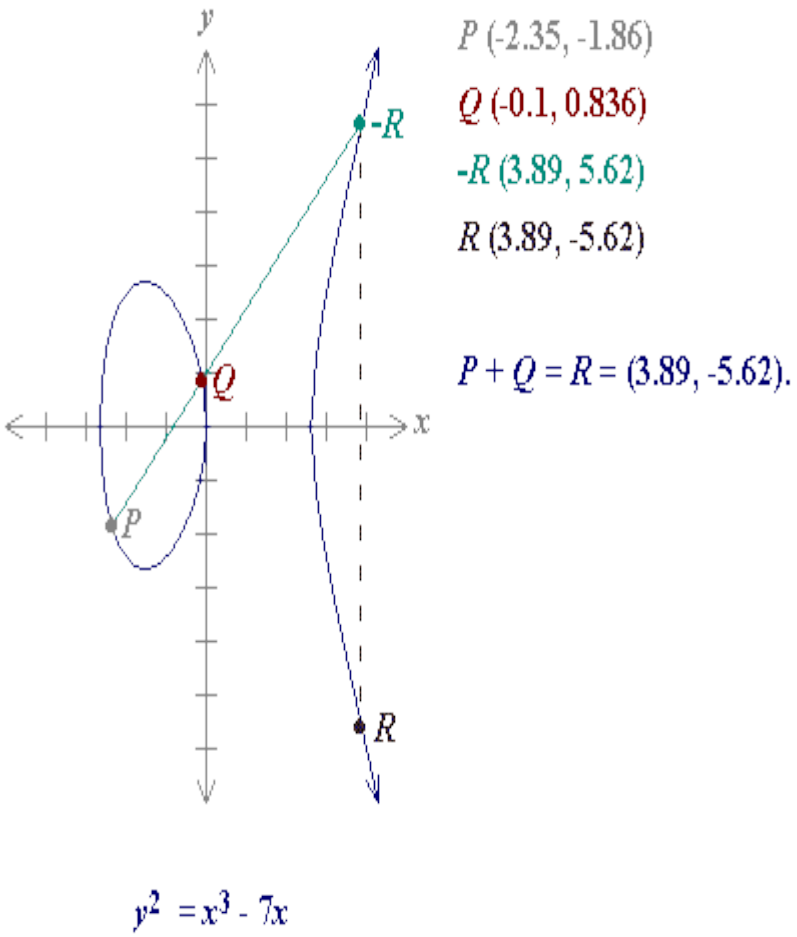
- If $x^3 + ax + b$ contains no repeated factors, or
- Equivalently if $4a^3 + 27b^2$ is not 0,
- then the elliptic curve $y^2 = x^3 + ax + b$ can be used to form a group.
- An elliptic curve group over real numbers consists of the points on the corresponding elliptic curve, together with a special point O called the point at infinity.

Elliptic curve groups are additive groups

- Elliptic curve groups are additive groups;
- That is, their basic function is addition.
- The addition of two points in an elliptic curve is defined **geometrically**.
- The negative of a point P = (xP,yP) is its reflection in the x-axis: the point -P is (xP,-yP).
- Notice that for each point P on an elliptic curve, the point -P is also on the curve

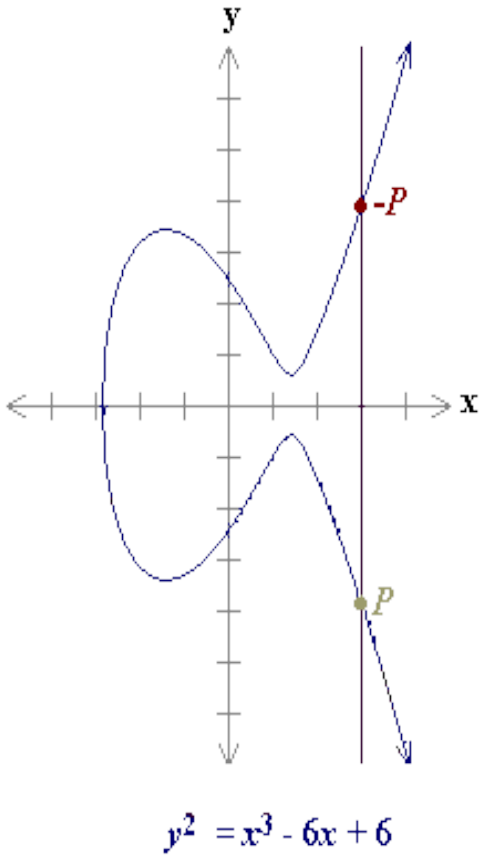
Adding distinct points P and Q

- Suppose that P and Q are two distinct points on an elliptic curve, and the P is not -Q.
- To add the points P and Q, a line is drawn through the two points.
- This line will intersect the elliptic curve in exactly one more point, call -R.
- The point -R is reflected in the x-axis to the point R.
- The law for addition in an elliptic curve group is P + Q = R. For example



ECC

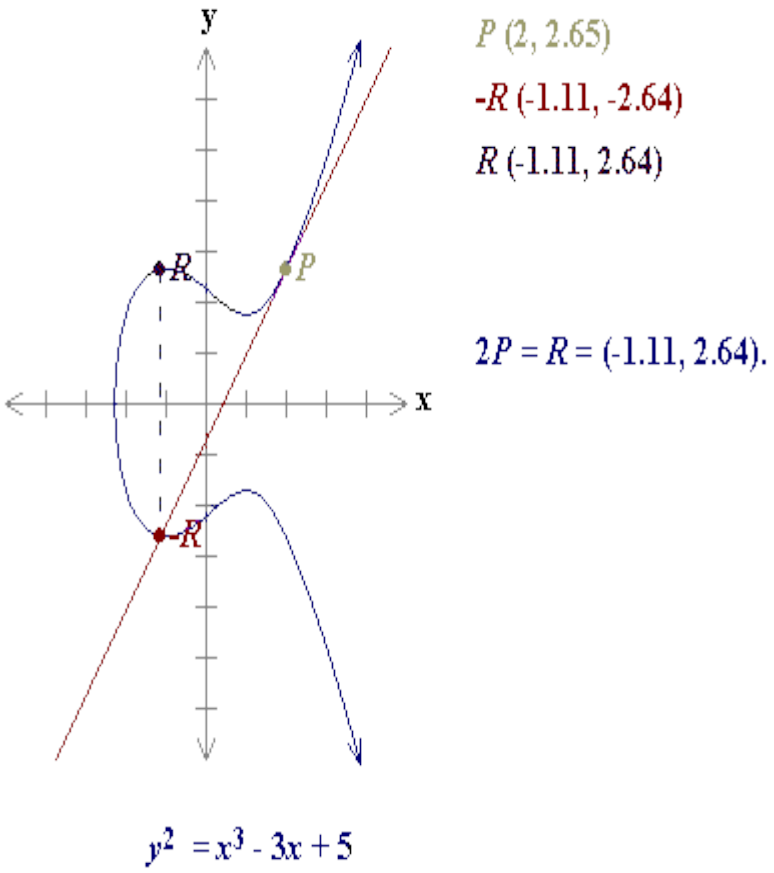
- **The line through P and -P is a vertical line which does not intersect the elliptic curve at a third point;**
- **Thus the points P and -P cannot be added as previously.**
- **It is for this reason that the elliptic curve group includes the point at infinity O.**
- **By definition, P + (-P) = O. As a result of this equation, P + O = P in the elliptic curve group .**
- **O is called the additive identity of the elliptic curve group; all elliptic curves have an additive identity**



ECC

- To add a point P to itself, a tangent line to the curve is drawn at the point P.
- If yP is not 0, then the tangent line intersects the elliptic curve at exactly one other point, -R.
- -R is reflected in the x-axis to R.
- This operation is called doubling the point P;
- the law for doubling a point on an elliptic curve group is defined by:

P + P = 2P = R.



P + P = 2P = R.

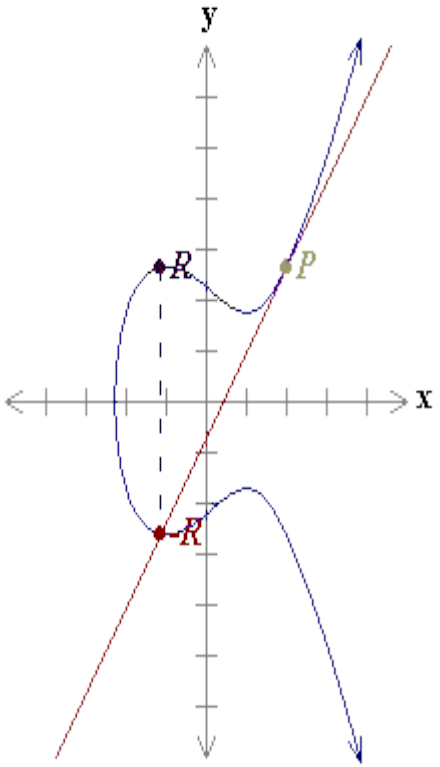
$y = s \cdot x - y_0$

$$y_0 = y_P - s \cdot x_P$$

Coordinates of point R

$$x_R = s^2 - x_P - x_Q$$

$$y_R = -(s \cdot x_R + y_0)$$



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

P (2, 2.65)

$-R$ (-1.11, -2.64)

R (-1.11, 2.64)

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

Try the following experiments:

1. Change the variables a and b to see the resulting shape and the elliptic curve.
2. Select a point P on the curve, and then select a point Q on the curve. Add them together.
3. Select a point P on the curve and then double it.
4. Try selecting a = -3 and b = 2

Solve

$y^2=x^3+x+1$ over Z_{23}.

1. Let $P=(3,10)$ and $Q=(9,7)$. Then $P+Q=(x_3,y_3)$

2. Let $P=(3,10)$. Then $2P=P+P=(x_3,y_3)$

Figure 3: Examples of elliptic curve addition on the curve $y^2=x^3+x+1$ over Z_{23}.

1. Let $P=(3,10)$ and $Q=(9,7)$. Then $P+Q=(x_3,y_3)$ is computed as:

$$\lambda = \frac{7-10}{9-3} = \frac{-3}{6} = \frac{-1}{2} = 11 \in \mathbb{Z}_{23},$$

$$x_3 = 11^2-3-9 = 6-3-9 = -6 \equiv 17 \pmod{23}, \text{ and}$$

$$y_3 = 11(3-(-6))-10 = 11(9)-10 = 89 \equiv 20 \pmod{23}.$$

Hence $P+Q=(17,20)$.

2. Let $P=(3,10)$. Then $2P=P+P=(x_3,y_3)$ is computed as follows:

$$\lambda = \frac{3(3^2)+1}{20} = \frac{5}{20} = \frac{1}{4} = 6 \in \mathbb{Z}_{23},$$

$$x_3 = 6^2-6 = 30 \equiv 7 \pmod{23}, \text{ and}$$

$$y_3 = 6(3-7)-10 = -24-10 = -11 \equiv 12 \pmod{23}.$$

Hence $2P=(7,12)$.

Quiz 1

1. Does the elliptic curve equation $y^2 = x^3 - 7x - 6$ over real numbers define a group?

2. What is the additive identity of regular integers?

3. Is (4,7) a point on the elliptic curve $y^2 = x^3 - 5x + 5$ over real numbers?

Quiz 1

4. In the elliptic curve group defined by $y^2 = x^3 - 17x + 16$ over real numbers, what is P + Q if P = (0,-4) and Q = (1,0)?
5. In the elliptic curve group defined by $y^2 = x^3 - 17x + 16$ over real numbers, what is 2P if P = (4, 3.464)?

Discrete Logarithm Problem

- The security of ECC depends on the difficulty of Elliptic Curve Discrete Logarithm Problem.

- Let **P** and **Q** be two points on an elliptic curve such that **kP = Q**, where k is a scalar.

- **Given P and Q, it is computationally infeasible to obtain k**, if k is sufficiently large.

- **k is the discrete logarithm of Q to the base P.**

- Hence the main operation involved in ECC is point multiplication. i.e. multiplication of a scalar k with any point P on the curve to obtain another point Q on the curve.

What Is ECC ?

- Elliptic curve cryptography [ECC] is a **public-key** cryptosystem just like RSA.
- 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.

Extension

- 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).

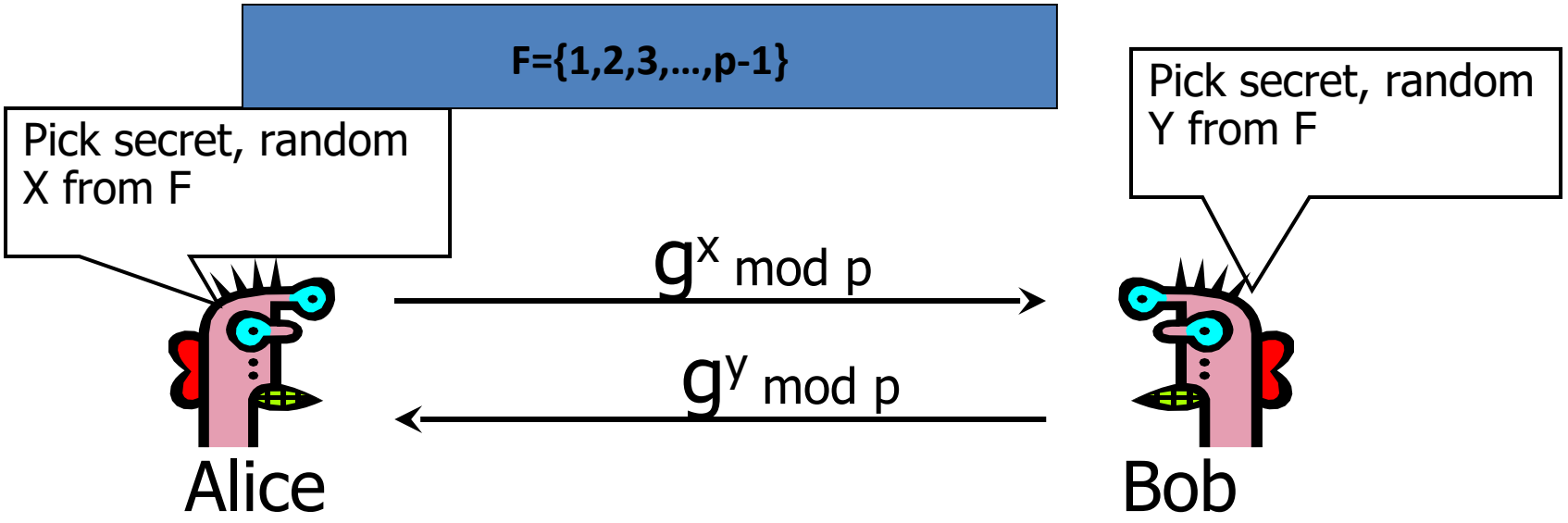
- Suppose Alice wants to send to Bob an encrypted message.
  - Both agree on a base point, B.
  - Alice and Bob create public/private keys.
    - **Alice**
      - Private Key = a
      - Public Key = $P_A = a * B$
    - **Bob**
      - Private Key = b
      - Public Key = $P_B = b * B$
  - Alice takes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

- 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
  - **$(P_M + kP_B) - [b(kB)] = P_M + k(bB) - b(kB) = P_M$**

  (BECAUSE $P_B = b * B$)
- Bob then decodes P_M to get the message, M.

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

ECC Diffie-Hellman

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

a(x,y)

b(x,y)

Alice, A

Bob, B

- Alice computes a(b)
- Bob computes b(a)
- 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

1. Does the elliptic curve equation $y^2 = x^3 - 7x - 6$ over real numbers define a group?

Yes, since

$4a^3 + 27b^2 = 4(-7)^3 + 27(-6)^2 = -400$

The equation $y^2 = x^3 - 7x - 6$ does define an elliptic curve group because $4a^3 + 27b^2$ is not 0.

2. What is the additive identity of regular integers?

The additive identity of regular integers is 0,

since $x + 0 = x$ for all integers.

3. Is (4,7) a point on the elliptic curve $y^2 = x^3 - 5x + 5$ over real numbers?

Yes, since the equation holds true for x = 4 and y = 7:

$(7)^2 = (4)^3 - 5(4) + 5$

$49 = 64 - 20 + 5$

$49 = 49$

4. In the elliptic curve group defined by $y^2 = x^3 - 17x + 16$ over real numbers, what is P + Q if P = (0,-4) and Q = (1,0)?

From the Addition formulae:

$$s = (y_P - y_Q) / (x_P - x_Q) = (-4 - 0) / (0 - 1) = 4$$

$$x_R = s^2 - x_P - x_Q = 16 - 0 - 1 = 15$$

and

$$y_R = -y_P + s(x_P - x_R) = 4 + 4(0 - 15) = -56$$

Thus P + Q = (15, -56)

5. In the elliptic curve group defined by $y^2 = x^3 - 17x + 16$ over real numbers, what is 2P if P = (4, 3.464)?

From the Doubling formulae:

$$s = (3x_P^2 + a) / (2y_P)$$

$$= (3*(4)^2 + (-17)) / 2*(3.464) = 31 / 6.928 = 4.475$$

$$x_R = s^2 - 2x_P$$

$$= (4.475)^2 - 2(4)$$

$$= 20.022 - 8 = 12.022 \quad \text{and}$$

$$y_R = -y_P + s(x_P - x_R)$$

$$= -3.464 + 4.475(4 - 12.022)$$

$$= -3.464 - 35.898 = -39.362$$

Thus 2P = (12.022, -39.362)

- In the elliptic curve group defined by $y2=x3+9x+17$over F23,
- what is the discrete logarithm k of $Q=(4,5)$ to the base $P=(16,5)$?

- One (naïve) way to find k is to compute multiples of *P* until *Q* is found. The first few multiples of *P*are:
- P=(16,5) $2P$=(20,20) $3P$=(14,14),
- $4P$=(19,20) $5P$=(13,10) $6P$=(7,3),
- $7P$=(8,7) $8P$=(12,17) $9P$=(4,5)
- Since $9P$=(4,5)=Q , the discrete logarithm of Q to the base P is k=9

Public-Key Cryptosystem Comparison (RSA vs ECC)

Time to break in MIPS years	*RSA/DSA key size*	*ECC key size*	*RSA/ECC key size ratio*
10^4	512	106	5 : 1
10^8	768	132	6 : 1
10^{11}	1,024	160	7 : 1
10^{20}	2,048	210	10 : 1
10^{78}	21,000	600	35 : 1

A MIPS year represents a computing time of one year on a machine capable of performing one million instructions per second.

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:

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

$$x_3 = \lambda^2 - x_1 - x_2$$

$$y_3 = \lambda(x_1 - x_3) - y_1, \text{ and}$$

$$\lambda = (3x_1^2 + a) / 2y_1$$