Elliptic Curve Cryptography

What’s wrong with RSA?

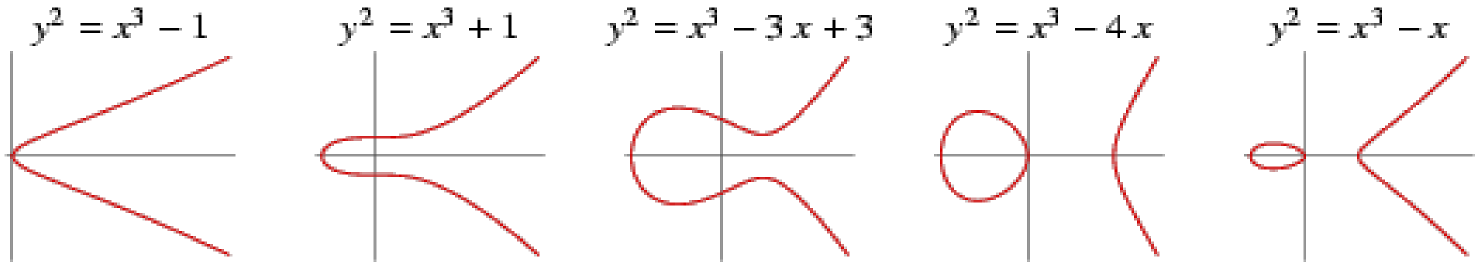
- RSA is based upon the ‘belief’ that factoring is ‘difficult’ – never been proven
- Prime numbers are getting too large
- Amount of research currently devoted to factoring algorithms
- Quantum computing will make RSA obsolete overnight

General form of a EC

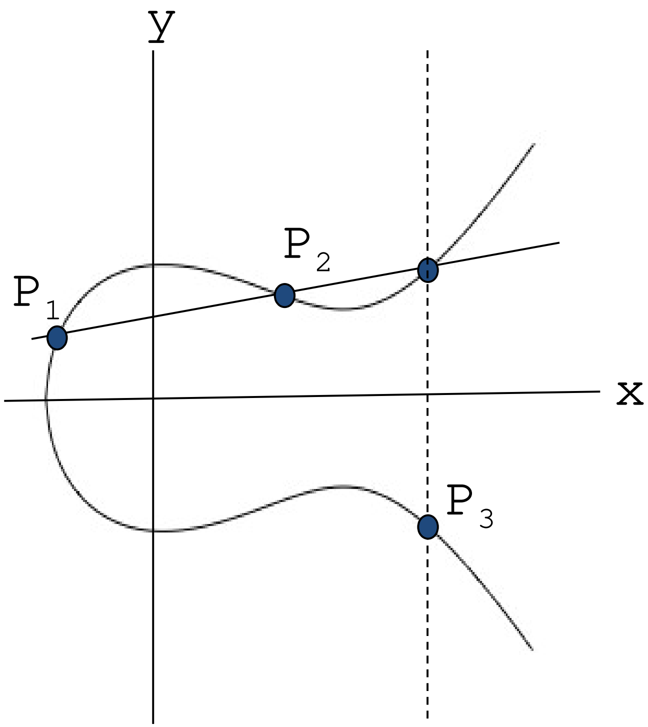
- An *elliptic curve* is a plane curve defined by an equation of the form

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

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 (x₁,y₁)*** and ***Q (x₂,y₂)*** 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(x₃,y₃)*** :

$$\boxed{\begin{aligned} x_3 &= \lambda^2 - x_1 - x_2 \\ y_3 &= \lambda(x_3 - x_1) + y_1 \end{aligned}}$$

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:

$$\underline{\mathbf{y^2 = x^3 + ax + b,}}$$

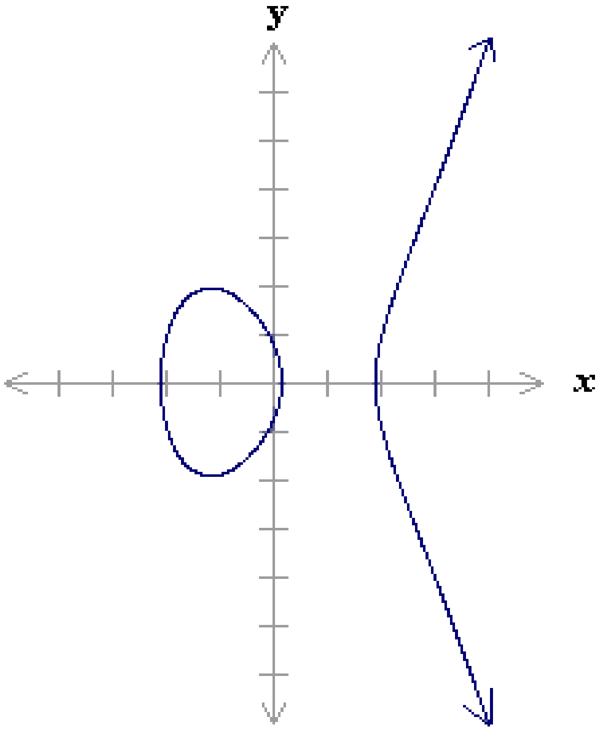
where x, y, a and b are <u>real numbers</u>.

- 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

$$\underline{\mathbf{y^2 = x^3 - 4x + 0.67;}}$$

the graph of this curve is shown.



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

An EC over real numbers – cont'd

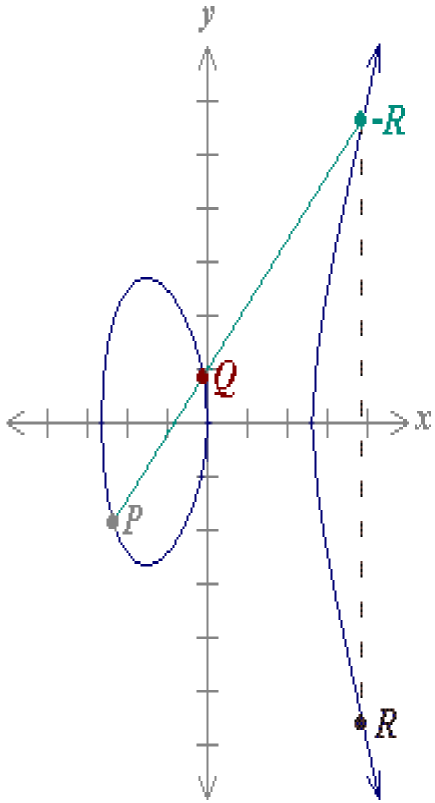
- If $x^3 + ax + b$ contains no repeated factors, or
- Equivalently if $4a^3 + 27b^2$ is not 0,
- then the elliptic curve $y^2 = x^3 + ax + b$ can be used to form a group.
- An elliptic curve group over real numbers consists of the points on the corresponding elliptic curve, together with a special point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



P (-2.35, -1.86)

Q (-0.1, 0.836)

$-R$ (3.89, 5.62)

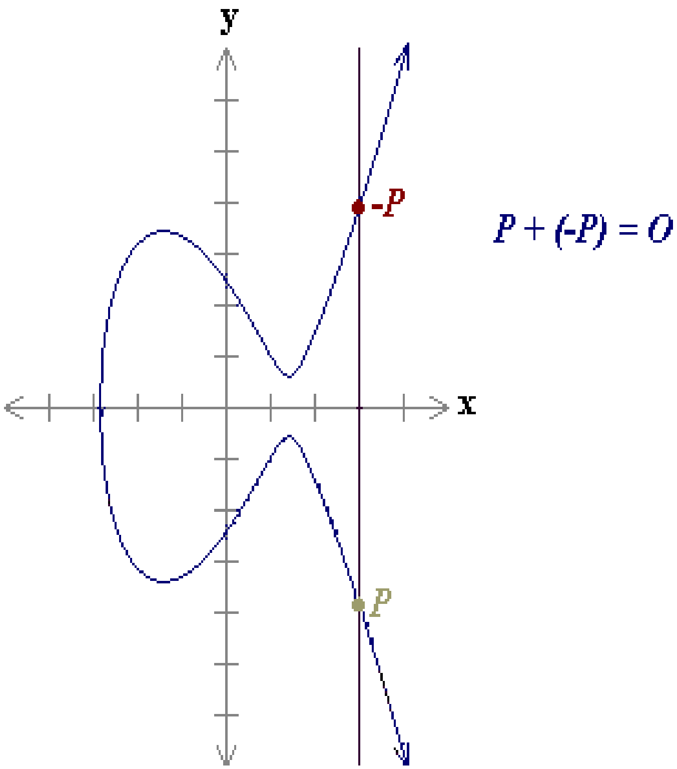
R (3.89, -5.62)

$P + Q = R =$ (3.89, -5.62).

$y^2 = x^3 - 7x$

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



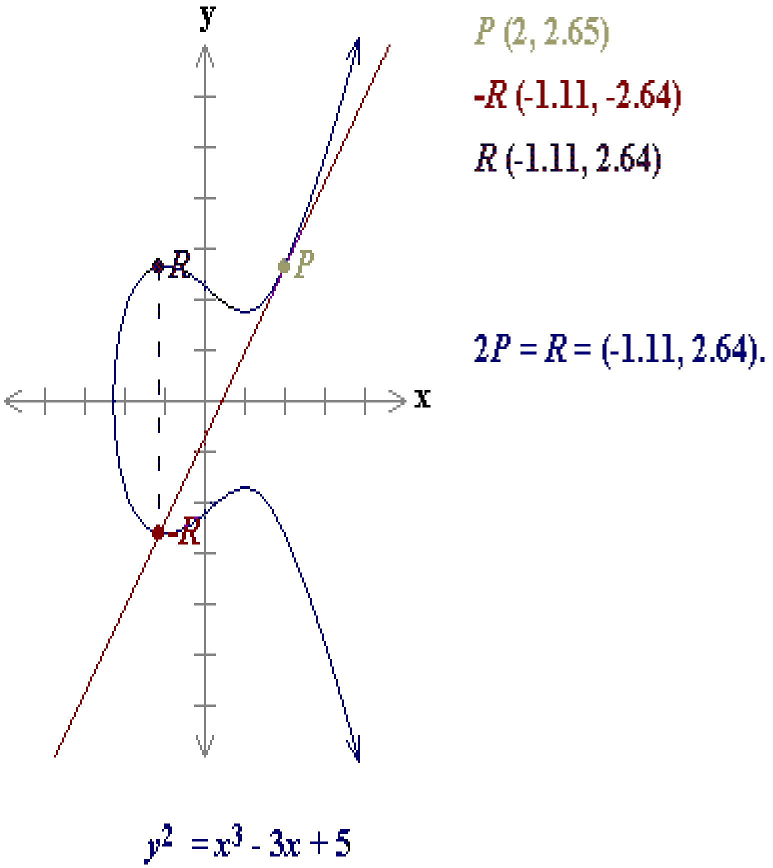
$P + (-P) = O$

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

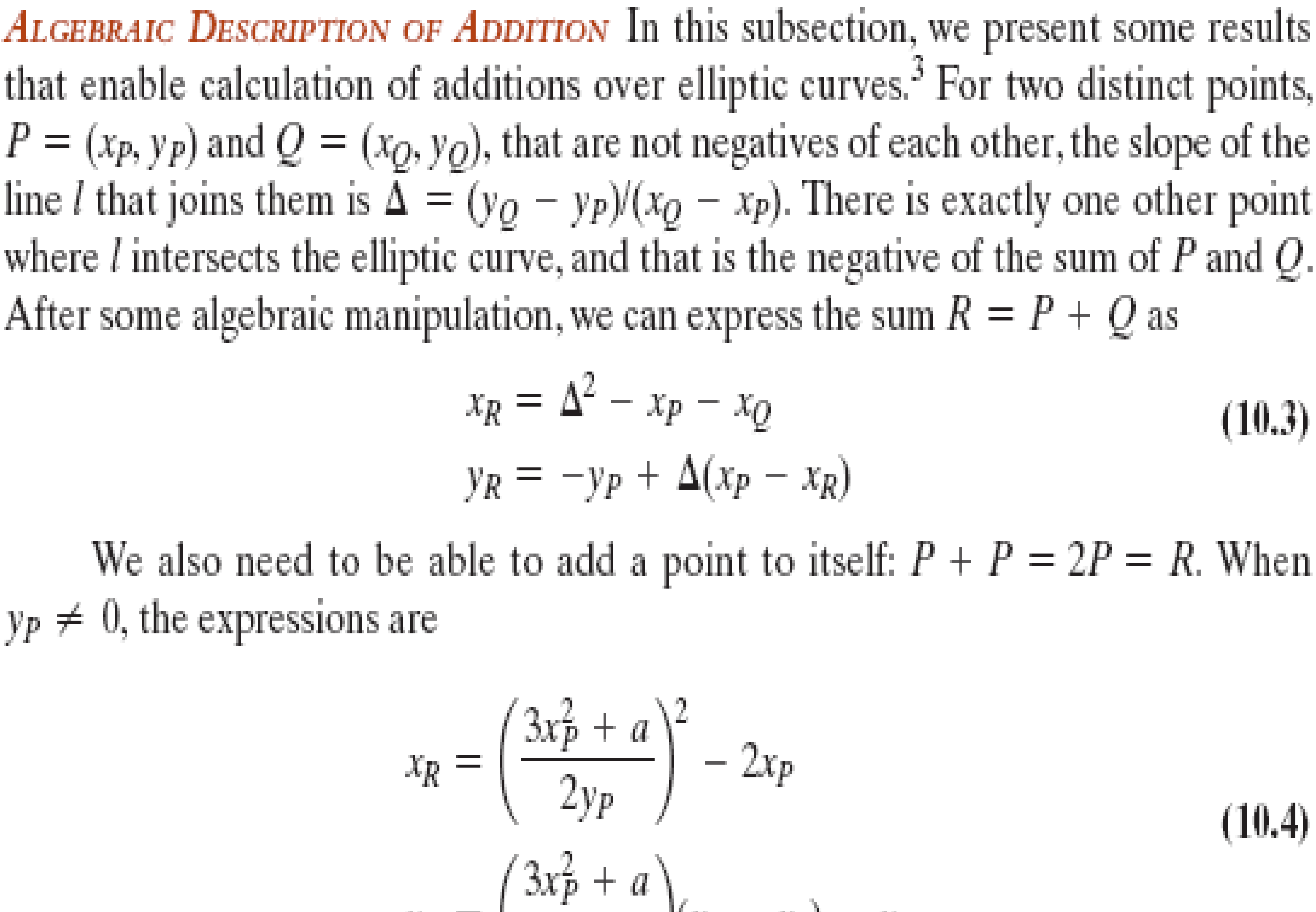
ECC

- 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:

$$P + P = 2P = R.$$



Elliptic Curves over Real Numbers



ALGEBRAIC DESCRIPTION OF ADDITION In this subsection, we present some results that enable calculation of additions over elliptic curves.[3] For two distinct points, $P = (x_P, y_P)$ and $Q = (x_Q, y_Q)$, that are not negatives of each other, the slope of the line l that joins them is $\Delta = (y_Q - y_P)/(x_Q - x_P)$. There is exactly one other point where l intersects the elliptic curve, and that is the negative of the sum of P and Q. After some algebraic manipulation, we can express the sum $R = P + Q$ as

$$x_R = \Delta^2 - x_P - x_Q \qquad (10.3)$$

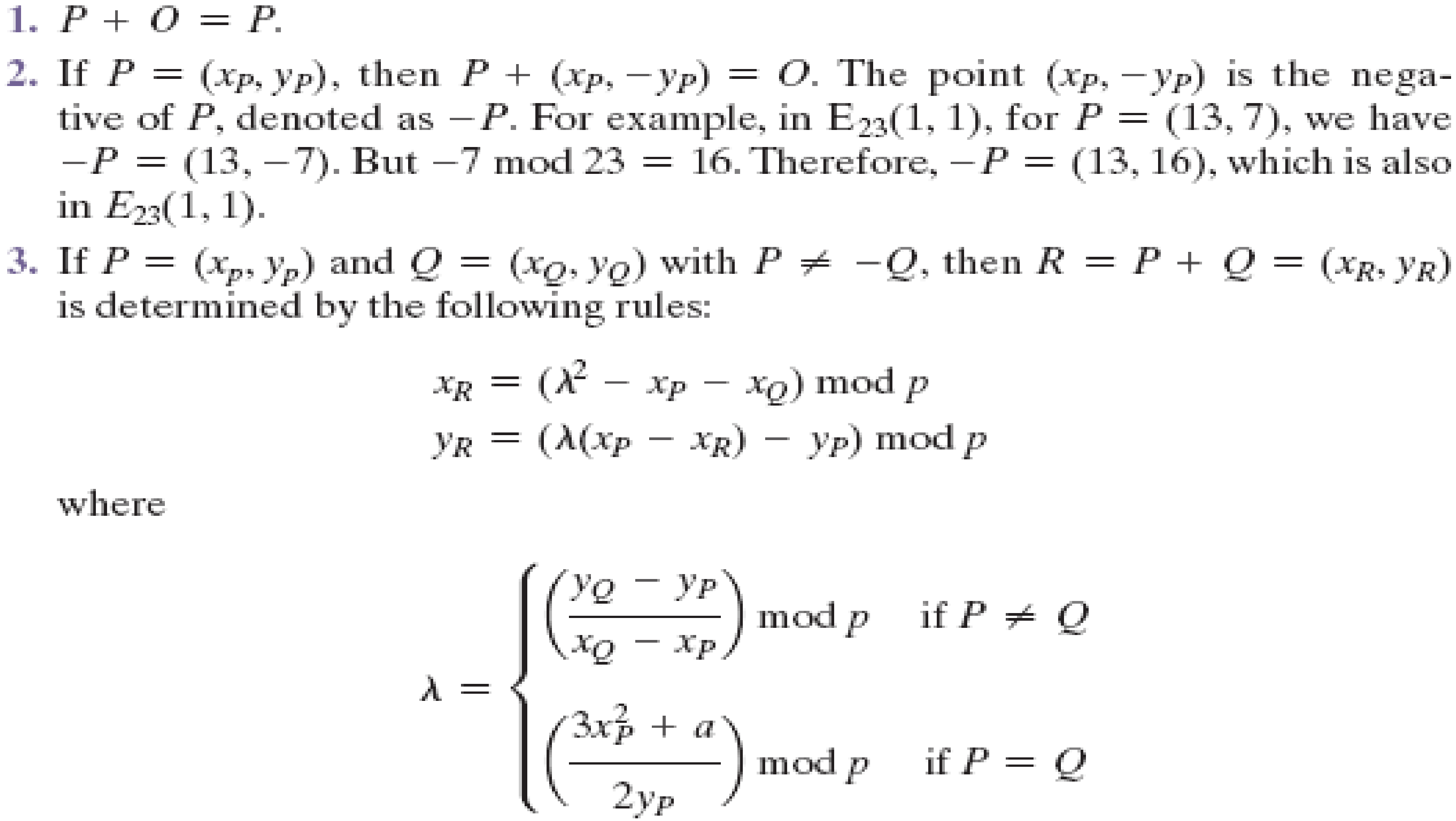
$$y_R = -y_P + \Delta(x_P - x_R)$$

We also need to be able to add a point to itself: $P + P = 2P = R$. When $y_P \neq 0$, the expressions are

$$x_R = \left(\frac{3x_P^2 + a}{2y_P}\right)^2 - 2x_P \qquad (10.4)$$

$$\left(3x_P^2 + a\right)$$

Elliptic Curves over *Zp*



1. $P + O = P$.
2. If $P = (x_P, y_P)$, then $P + (x_P, -y_P) = O$. The point $(x_P, -y_P)$ is the negative of P, denoted as $-P$. For example, in E$_{23}$(1, 1), for $P = (13, 7)$, we have $-P = (13, -7)$. But $-7 \bmod 23 = 16$. Therefore, $-P = (13, 16)$, which is also in $E_{23}(1, 1)$.
3. If $P = (x_p, y_p)$ and $Q = (x_Q, y_Q)$ with $P \neq -Q$, then $R = P + Q = (x_R, y_R)$ is determined by the following rules:

$$x_R = (\lambda^2 - x_P - x_Q) \bmod p$$
$$y_R = (\lambda(x_P - x_R) - y_P) \bmod p$$

where

$$\lambda = \begin{cases} \left(\dfrac{y_Q - y_P}{x_Q - x_P}\right) \bmod p & \text{if } P \neq Q \\ \left(\dfrac{3x_P^2 + a}{2y_P}\right) \bmod p & \text{if } P = Q \end{cases}$$

4. Multiplication is defined as repeated addition; for example, $4P = P + P + P + P$.

For example, let $P = (3, 10)$ and $Q = (9, 7)$ in $E_{23}(1, 1)$. Then

$$\lambda = \left(\frac{7 - 10}{9 - 3}\right) \bmod 23 = \left(\frac{-3}{6}\right) \bmod 23 = \left(\frac{-1}{2}\right) \bmod 23 = 11$$

$$x_R = (11^2 - 3 - 9) \bmod 23 = 109 \bmod 23 = 17$$

$$y_R = (11(3 - 17) - 10) \bmod 23 = -164 \bmod 23 = 20$$

So $P + Q = (17, 20)$. To find $2P$,

$$\lambda = \left(\frac{3(3^2) + 1}{2 \times 10}\right) \bmod 23 = \left(\frac{5}{20}\right) \bmod 23 = \left(\frac{1}{4}\right) \bmod 23 = 6$$

The last step in the preceding equation involves taking the multiplicative inverse of 4 in Z_{23}. This can be done using the extended Euclidean algorithm defined in Section 2.2. To confirm, note that $(6 \times 4) \bmod 23 = 24 \bmod 23 = 1$.

$$x_R = (6^2 - 3 - 3) \bmod 23 = 30 \bmod 23 = 7$$

$$y_R = (6(3 - 7) - 10) \bmod 23 = (-34) \bmod 23 = 12$$

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

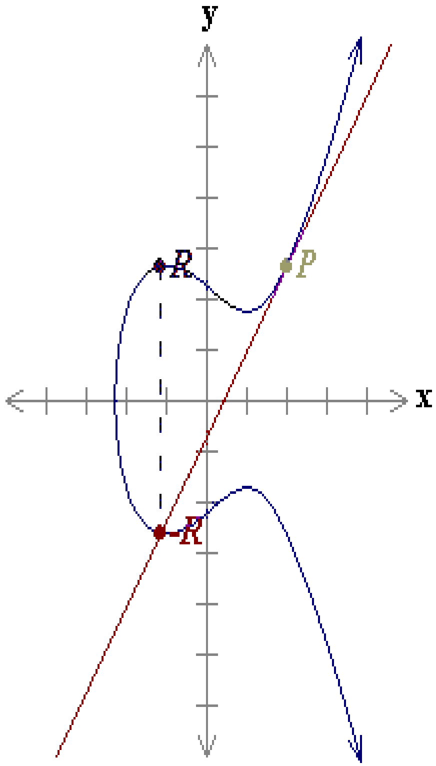
P + P = 2P = R.

$$y = s \cdot x - y_0$$

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

Coordinates of point R

$$x_R = s^2 - x_P - x_Q$$
$$y_R = -(s \cdot x_R + y_0)$$



P (2, 2.65)

-*R* (-1.11, -2.64)

R (-1.11, 2.64)

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

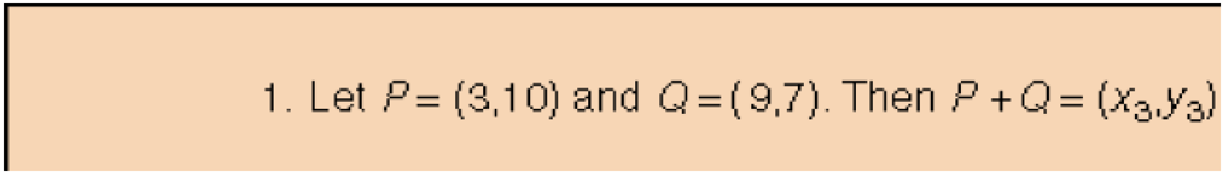
$$y^2 = x^3 - 3x + 5$$

Try the following experiments:

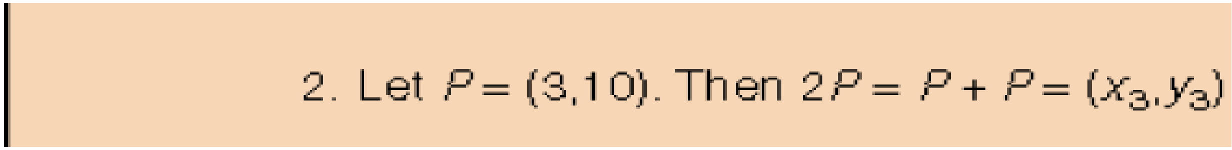
1. Change the variables a and b to see the resulting shape and the elliptic curve.
2. Select a point P on the curve, and then select a point Q on the curve. Add them together.
3. Select a point P on the curve and then double it.
4. Try selecting a = -3 and b = 2

Solve

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

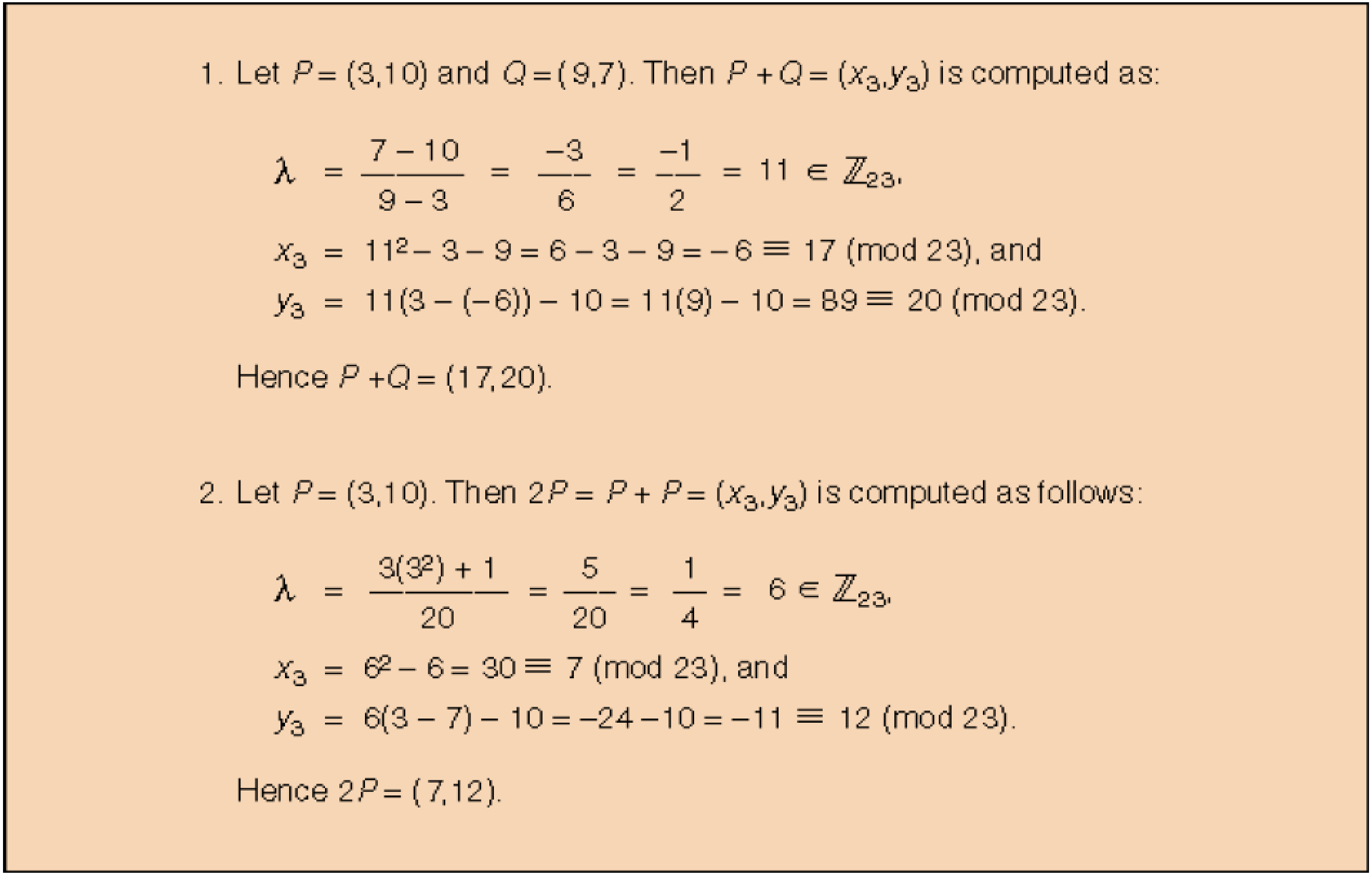


1. Let $P=(3,10)$ and $Q=(9,7)$. Then $P+Q=(x_3,y_3)$



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

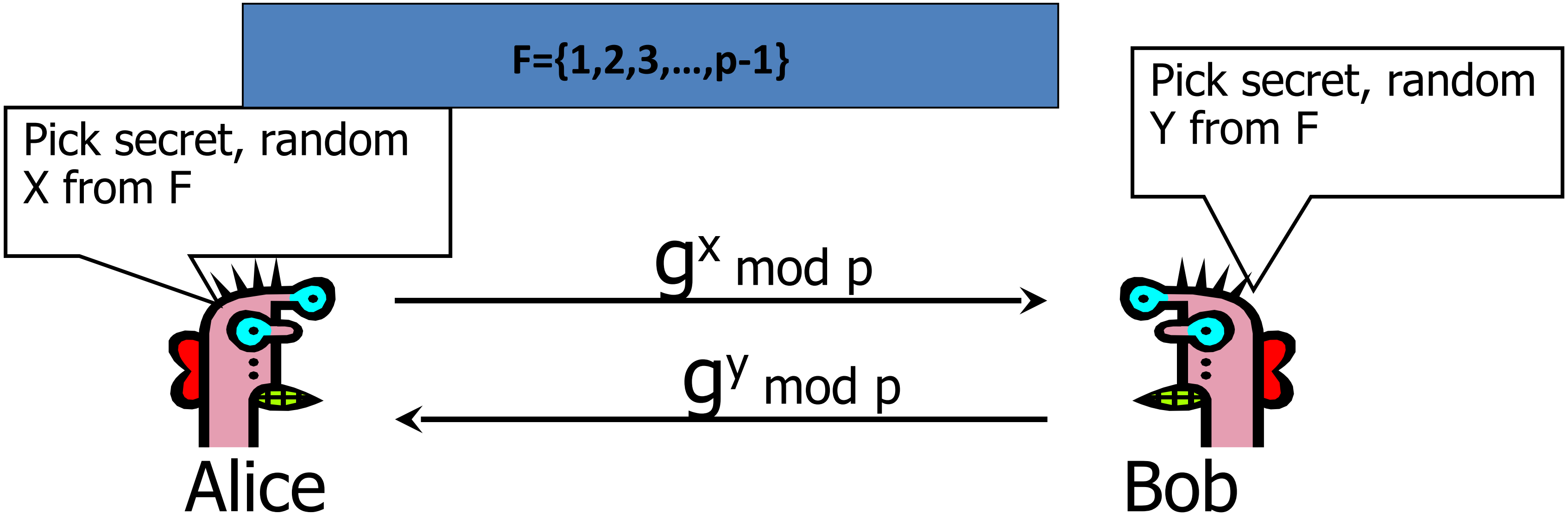
- Alice chooses another random integer, k from the interval [1, p-1]
- The ciphertext is a pair of points
  - **$P_C = [\ (kB), (P_M + kP_B)\ ]$**

- 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



F={1,2,3,…,p-1}

Pick secret, random X from F

Pick secret, random Y from F

$g^x \bmod p$

$g^y \bmod p$

Alice

Bob

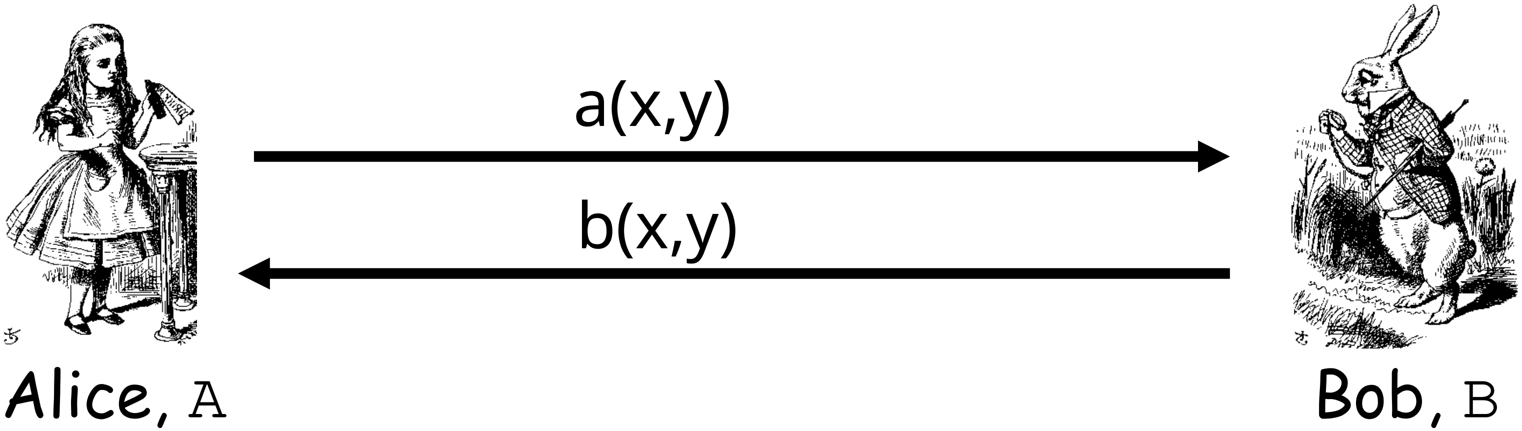
Compute $k=(g^y)^x=g^{xy} \bmod p$

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

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

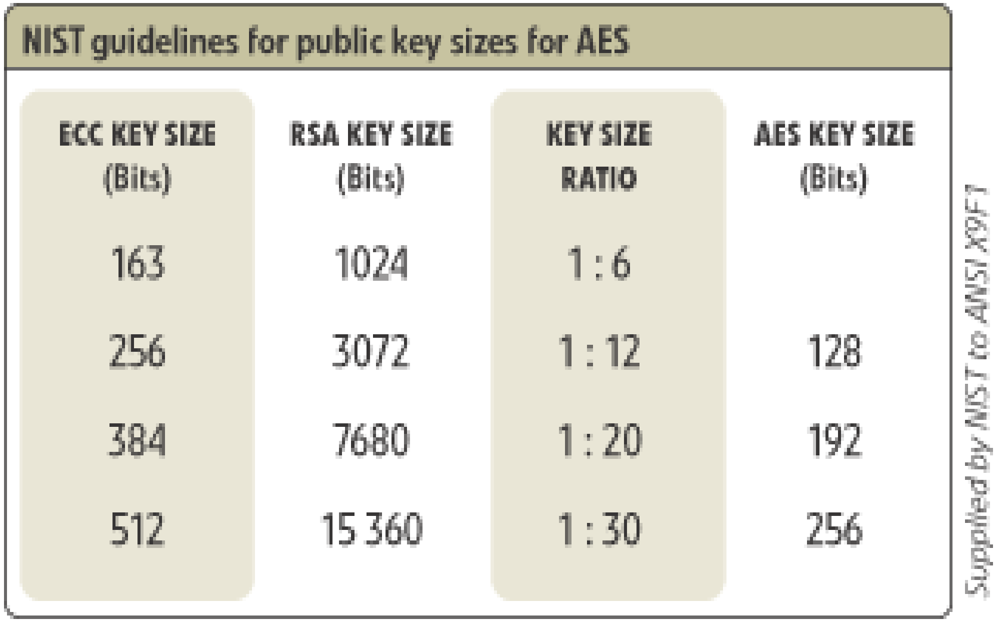
- Alice and Bob want to agree on a shared key.
  - Alice and Bob compute their public and private keys.
    - Alice
      - » Private Key = a
      - » Public Key = $P_A = a * B$
    - Bob
      - » Private Key = b
      - » Public Key = $P_B = b * B$
  - Alice and Bob send each other their public keys.
  - 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:

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

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

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

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

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

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

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

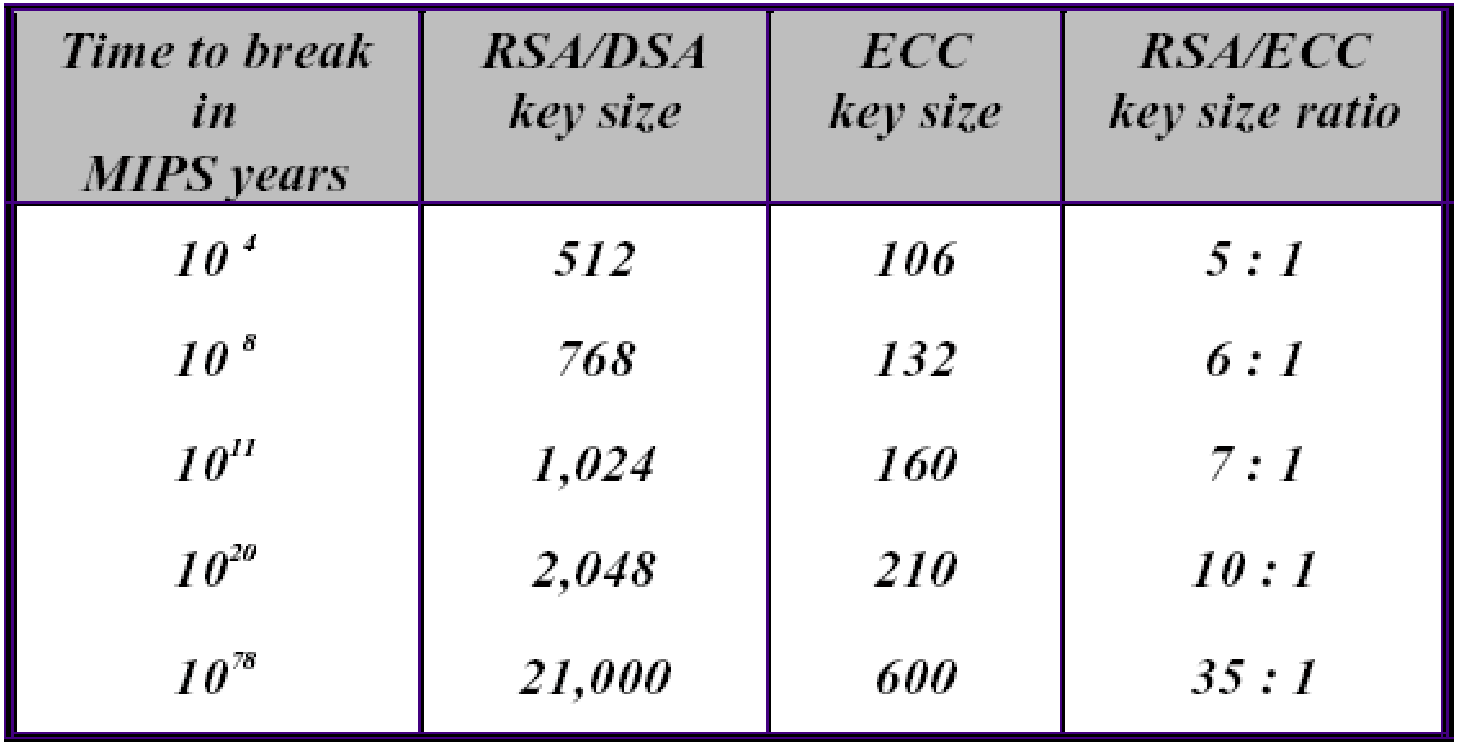
$$= - 3.464 - 35.898 = -39.362$$

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) 2*P*=(20,20) 3*P*=(14,14),
- 4*P*=(19,20) 5*P*=(13,10) 6*P*=(7,3),
- 7*P*=(8,7) 8*P*=(12,17) 9*P*=(4,5)
- Since 9*P*=(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

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

$y_3 = \lambda(x_1 – x_3) - y_1$, and

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