# UNIT III
# PUBLIC KEY CRYPTOGRAPHY

# UNIT III PUBLIC KEY CRYPTOGRAPHY

Introduction to Number Theory: Prime Numbers, Fermat’s and Euler’s Theorem, Testing for Primality. Public key ciphers - RSA cryptosystem, Elliptic Curve Cryptography, Key Management

# Primes & Factorization

- An integer $p>1$ is a prime number if and only if its only divisors are $\pm 1$ and $\pm p$.
- Any integer a>1 can be factored in a unique way as
- $a = p_1^{a1} * p_2^{a2} * \ldots\ldots * p_t^{at}$ where $p_1<p_2<\ldots\ldots<p_t$ are prime numbers and where each $a_i$ is a positive integer.
- $a=\prod_{p\in P} p^{ap}$ where $a_p>=0$

$$24 = 8 * 3 = 3^1 * 2^3$$

$p_1=3;a1=1$

$p_2=2;a2=3$

# Primality Testing

- Miller and rabin algorithm is used to test a large number for primality.
- If p is prime and a is a positive integer less than p, then $a^2$ mod p = 1 if and only if either

$$a \bmod p = 1 \text{ or } a \bmod p = -1 \bmod p = p - 1.$$

# Euler‘s totient function

- Euler’s totient function is represented as $\Phi(n)=n-1$, $\Phi(pq)= (p-1)(q-1)$
- It is defined as the number of positive integers less than n and relatively prime to n.

$\Phi(1) = 1$

$\Phi(5) = 1, 2, 3, 4 = 4$

$\Phi(4) = 1, 3 =2$

$\Phi(20) =1, 3, 7, 9, 11, 13, 17, 19 = 8$

$= \Phi(5) * \Phi(4)$

$= 4 * 2 = 8$

# Fermat‘s Theorem

- If p is prime and a is a positive integer not divisible by p, then

$$a^{p-1} \equiv 1 \pmod{p}$$

$$a^{p-1} \bmod p = 1$$

p = 5 (prime); a=2

$$2^{5-1} \bmod 5 = 1$$

$$2^{4} \bmod 5 = 1$$

$$16 \bmod 5 = 1$$

$$1 = 1$$

# Euler‘s Theorem

- Euler’s theorem states that for every a and n that are relatively prime:

$$a^{\Phi(n)} \equiv 1(\text{mod } n)$$

$$a^{\Phi(n)} \text{ mod } n = 1$$

$\Phi(5) = 1, 2, 3, 4 = 4$

n=5

a=2

$$24 \text{ mod } 5 = 1$$

$$16 \text{ mod } 5 = 1$$

$$1 = 1$$

# TRASH TALKER-12

1. **There are 67 people in a company where they are using secret key encryption and decryption system for privacy purpose. Determine the number of secret keys required for this purpose?**

   a) 887
   b) 6529
   c) 2211
   d) 834

Answer: c

Explanation: Since every two employee have their own secret key encryption and decryption. Both users have to agree on a secret key to communicate using symmetric cryptography. After that, each message is encrypted with that key it is transmitted and decrypted with the same key. Here, key distribution must be secret. For n = 67 we would need $n(n–1)2=67(67–1)2$ = 2211 key

**2. ________ can decrypt traffic to make it available to all other network security functions such as web proxies.**

a) SSL visibility appliances
b) RSA appliances
c) Rodriguez cipher system
d) Standard cipher system

Answer: a
Explanation: In the data loss prevention systems, Web proxies and antivirus network security functions, SSL visibility appliances decrypt traffic to make it available for all networks.

**3. Suppose that there are two primes, $P_1$ = 229 and $p_2$ = 61. Find the value of z and Φ.**

a) 13969, 13680
b) 5853, 23452
c) 7793, 34565
d) 17146, 69262

Answer: a
Explanation: We know that, $z = p_1*p_2 = 229*61 = 13969$ and $\Phi = (p_1 – 1)(p_2 – 1) = (229 – 1)(61 – 1) = 228*60 = 13680$.

**4. Euler’s totient function is determined by**

A. Pq

B. (p-1)(q-1)

C. (p+1)(q+1)

D. p/q

**Ans:B**

**6. Euclid’s algorithm is used for finding ___________**

a) GCD of two numbers
b) GCD of more than three numbers
c) LCM of two numbers
d) LCM of more than two numbers

Answer: a

Explanation: Euclid’s algorithm is basically used to find the GCD of two numbers. It cannot be directly applied to three or more numbers at a time.

**7. Who invented Euclid’s algorithm?**

a) Sieve
b) Euclid
c) Euclid-Sieve
d) Gabriel lame

Answer: b

Explanation: Euclid invented Euclid’s algorithm. Sieve provided an algorithm for finding prime numbers. Gabriel lame proved a theorem in Euclid’s algorithm.

**8. If 4 is the GCD of 16 and 12, What is the GCD of 12 and 4?**
a) 12
b) 6
c) 4
d) 2

Answer: c
Explanation: Euclid’s algorithm states that the GCD of two numbers does not change even if the bigger number is replaced by a difference of two numbers. So, GCD of 16 and 12 and 12 and (16-12)=4 is the same.

**9. Which of the following is not an application of Euclid’s algorithm?**
a) Simplification of fractions
b) Performing divisions in modular arithmetic
c) Solving quadratic equations
d) Solving diophantine equations

Answer: c
Explanation: Solving quadratic equations is not an application of Euclid’s algorithm whereas the rest of the options are mathematical applications of Euclid’s algorithm.

**10. The Euclid’s algorithm runs efficiently if the remainder of two numbers is divided by the minimum of two numbers until the remainder is zero.**

a) True

b) False

Answer: a

Explanation: The Euclid’s algorithm runs efficiently if the remainder of two numbers is divided by the minimum of two numbers until the remainder is zero. This improvement in efficiency was put forth by Gabriel Lame.

# Elliptic curve arithmetic

- Elliptic curve is represented as $E_p(a,b)$. p is a prime number & a and b are restricted to mod p.
- The curve is represented as

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

$$y^2 \text{ mod } p = (x^3+ax+b) \text{ mod } p$$

- ECC can be defined as EC over $Z_p$

# Elliptic curve arithmetic

Find a point in Elliptic curve $E_{11}(1,1)$

$E_p(a,b)$ =>$p = 11$; $a = 1$; $b = 1$

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

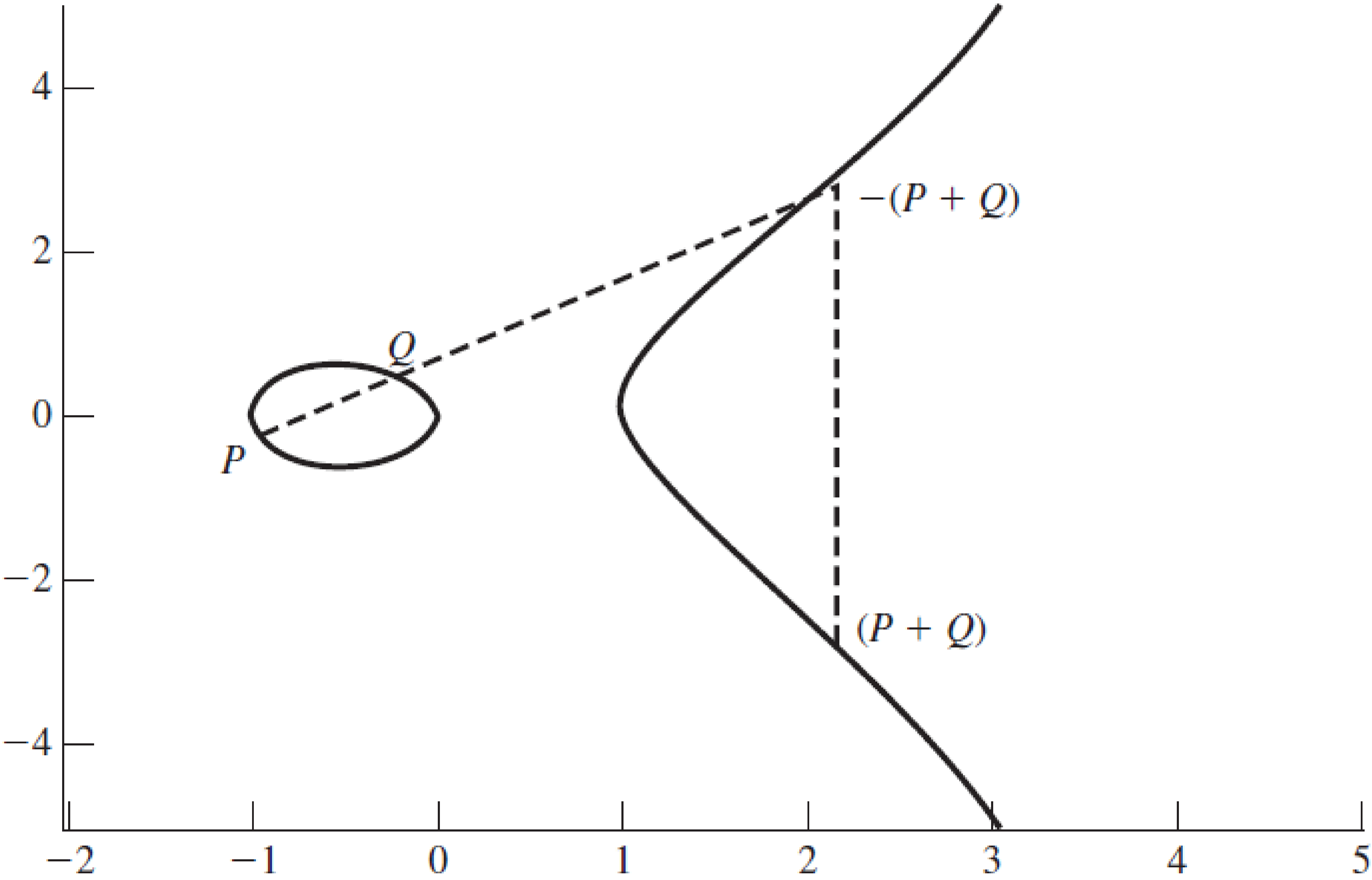
Substituting the values

$$y^2 = x^3+x+1$$

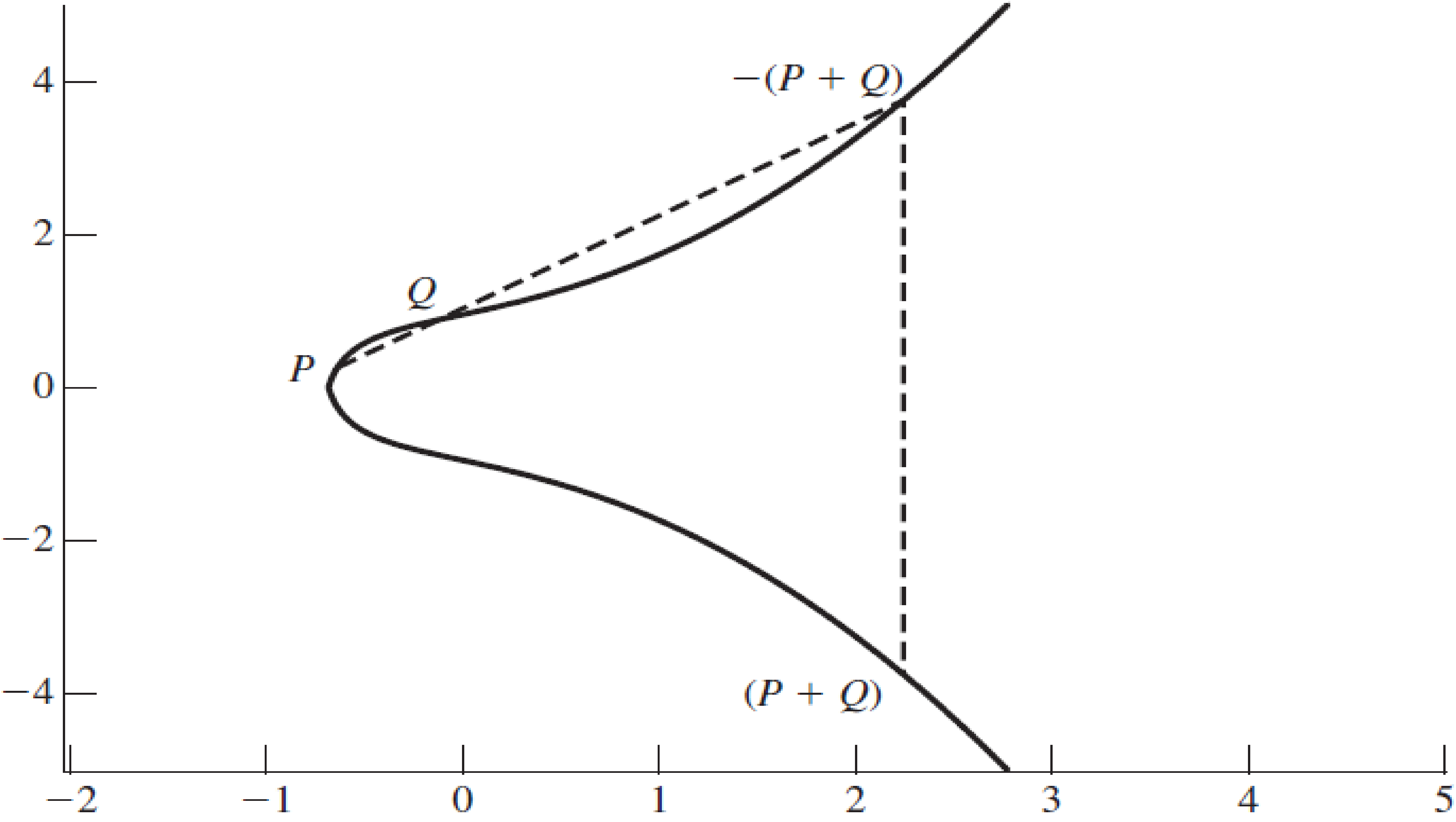
Solving the equations, put $x = 0$

$$y= 1, -1$$

$$x= 0 \quad \Rightarrow \quad (0,1)\ (0,-1)$$



(a) $y^2 = x^3 - x$

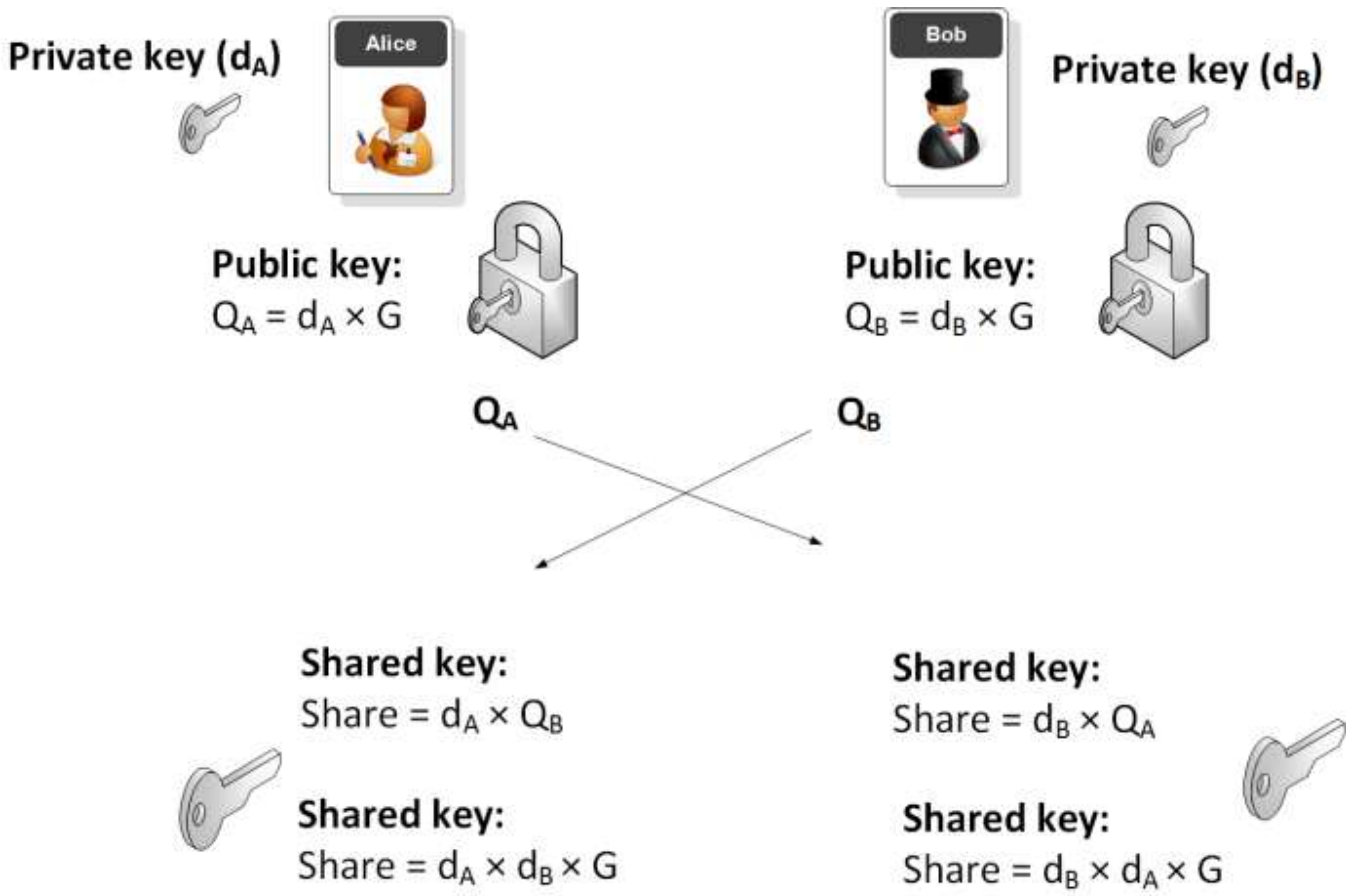


(b) $y^2 = x^3 + x + 1$

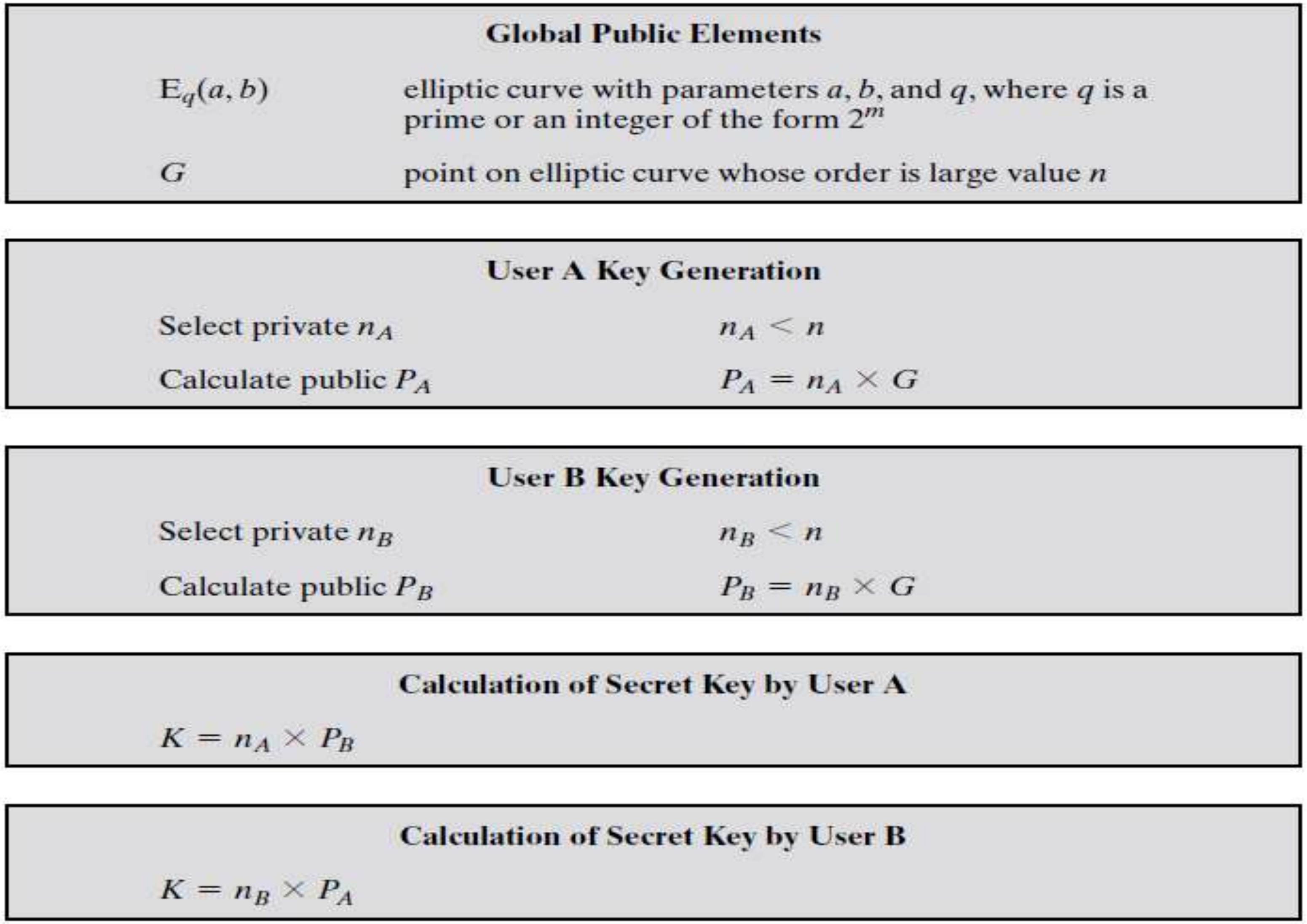
# Elliptic curve cryptography

- Elliptical curve cryptography (ECC) is a public key encryption technique based on elliptic curve theory that can be used to create faster, smaller, and more efficient cryptographic keys.
- ECC generates keys through the properties of the elliptic curve equation instead of the traditional method of generation as the product of very large prime numbers.
- It can be used in conjunction with most public key encryption methods, such as RSA, and Diffie-Hellman.

# Elliptic curve cryptography



# ECC Diffie-Hellman Key Exchange



**Global Public Elements**

| | |
|---|---|
| $E_q(a, b)$ | elliptic curve with parameters $a$, $b$, and $q$, where $q$ is a prime or an integer of the form $2^m$ |
| $G$ | point on elliptic curve whose order is large value $n$ |

**User A Key Generation**

| | |
|---|---|
| Select private $n_A$ | $n_A < n$ |
| Calculate public $P_A$ | $P_A = n_A \times G$ |

**User B Key Generation**

| | |
|---|---|
| Select private $n_B$ | $n_B < n$ |
| Calculate public $P_B$ | $P_B = n_B \times G$ |

**Calculation of Secret Key by User A**

$K = n_A \times P_B$

**Calculation of Secret Key by User B**

$K = n_B \times P_A$

# Security of Elliptic Curve Cryptography

- The security of ECC depends on how difficult it is to determine *k* given *kP* and *P*.
- This is referred to as the elliptic curve logarithm problem.
- The fastest known technique for taking the elliptic curve logarithm is known as the Pollard rho method.

# TRASH TALKER-13

**1. “Elliptic curve cryptography follows the associative property.”**

a) True

b) False

Answer: a

Explanation: ECC does follow associative property.

**2. What is the general equation for elliptic curve systems?**

a) $y^3$+b_1 xy+b_2 y=$x^3$3+a_1 $x^2$+a_2 x+a_3

b) $y^3$+b_1 x+b_2 y=$x^2$+a_1 $x^2$+a_2 x+a_3

c) $y^2$+b_1 xy+b_2 y=$x^3$+a_1 $x^2$+a_2

d) $y^2$+b_1 xy+b_2 y=$x^3$+a_1 $x^2$+a_2 x+a_3

Answer: d

Explanation: The general equations for an elliptic curve system is $y^2$+b_1 xy+b_2 y=$x^3$+a_1 $x^2$+a_2 x+a_3.

**3. In Singular elliptic curve, the equation x^3+ax+b=0 does ____ roots.**

a) does not have three distinct

b) has three distinct

c) has three unique

d) has three distinct unique

Answer: a

Explanation: In Singular elliptic curve, the equation x^3+ax+b=0 does not have three distinct roots.

**4.In the elliptic curve group defined by y2= x3- 17x + 16 over real numbers, what is P + Q if P = (0,-4) and Q = (1, 0)?**

a) (15, -56)

b) (-23, -43)

c) (69, 26)

d) (12, -86)

Answer: a

Explanation: P=(x1, y1)= (0,-4)

Q=(x2, y2)= (1,0)

From the Addition formulae:

λ= (0-(-4)) / (1-0) = 4

x3= = 16 – 0 – 1 = 15 and

y3= 4(0 – 15) –(-4) = -56

Thus R=P + Q = (15, -56).

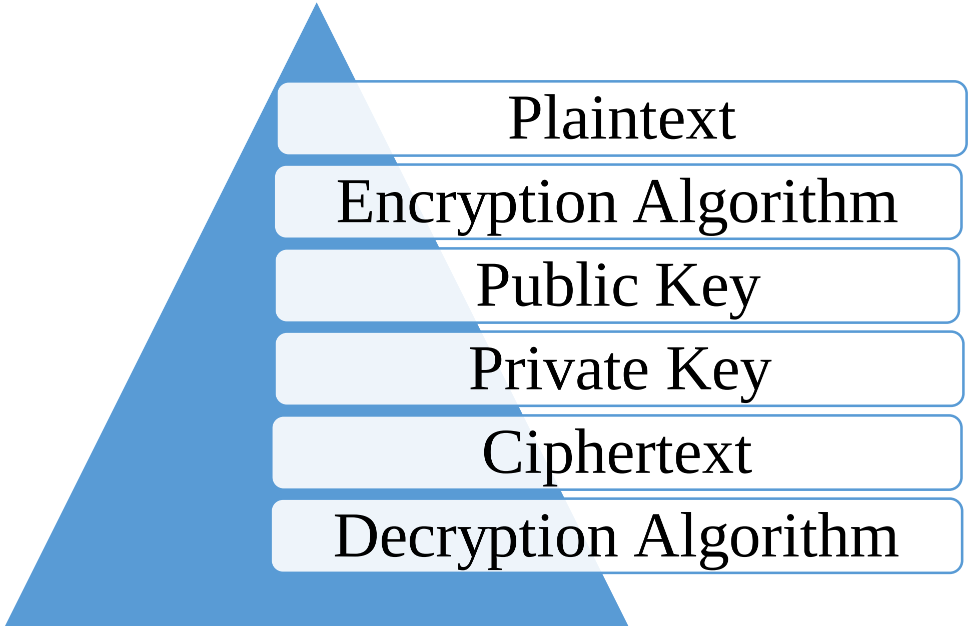
**5.In the elliptic curve group defined by y2= x3- 17x + 16 over real numbers, what is 2P if P = (4, 3.464)?**
a) (12.022, -39.362)
b) (32.022, 42.249)
c) (11.694, -43.723)
d) (43.022, 39.362)

Answer: a

Explanation: From the Doubling formulae:
λ = (3*(4)2+ (-17)) / 2*(3.464) = 31 / 6.928 = 4.475
x3= (4.475)2- 2(4) = 20.022 – 8 = 12.022 and
y3= -3.464 + 4.475(4 – 12.022) = – 3.464 – 35.898 = -39.362
Thus 2P = (12.022, -39.362).

# Public-Key Cryptosystems

- Asymmetric algorithms rely on one key for encryption and a different but related key for decryption.
- A public-key encryption scheme has six ingredients



Plaintext

Encryption Algorithm

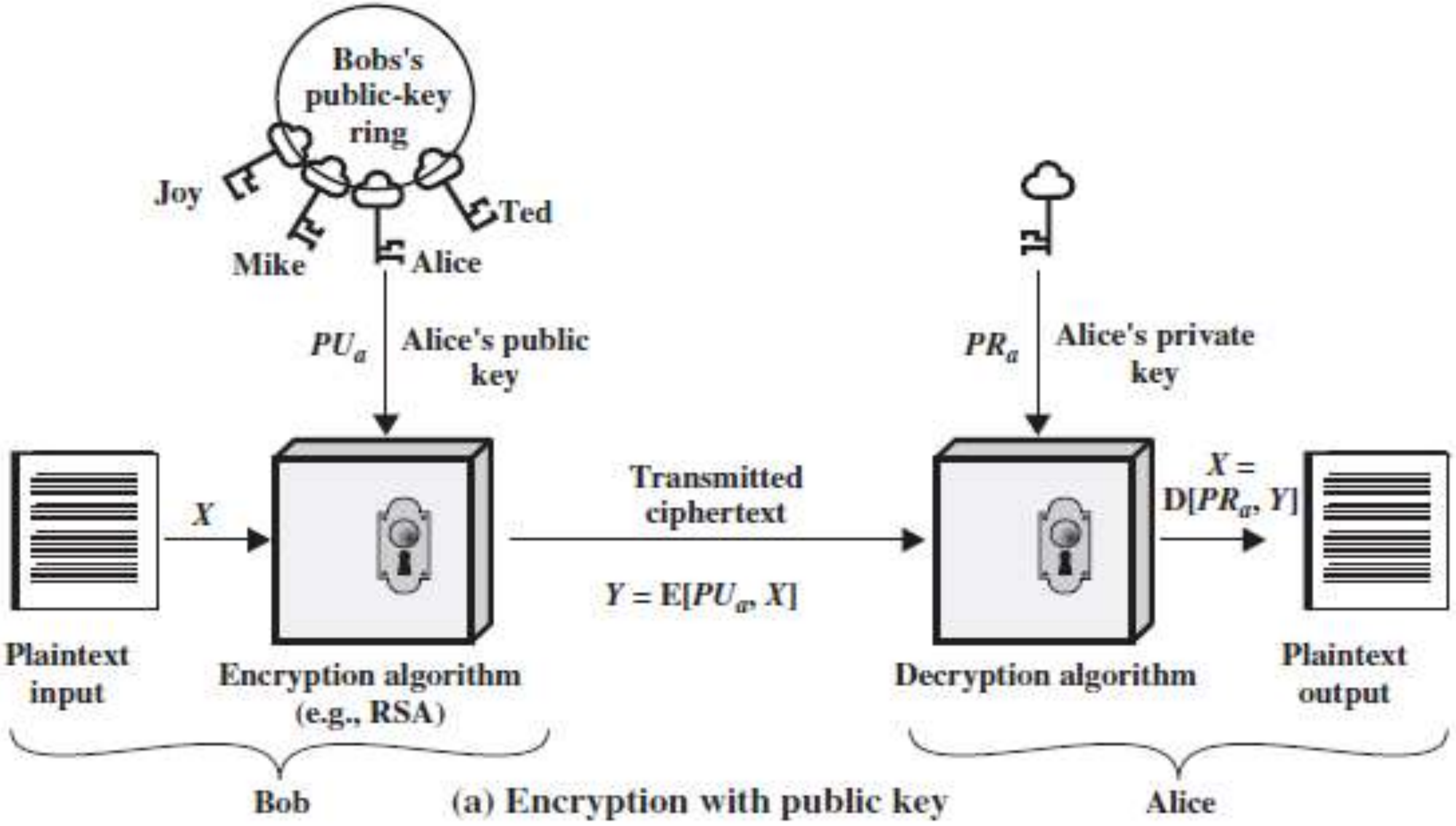
Public Key

Private Key

Ciphertext

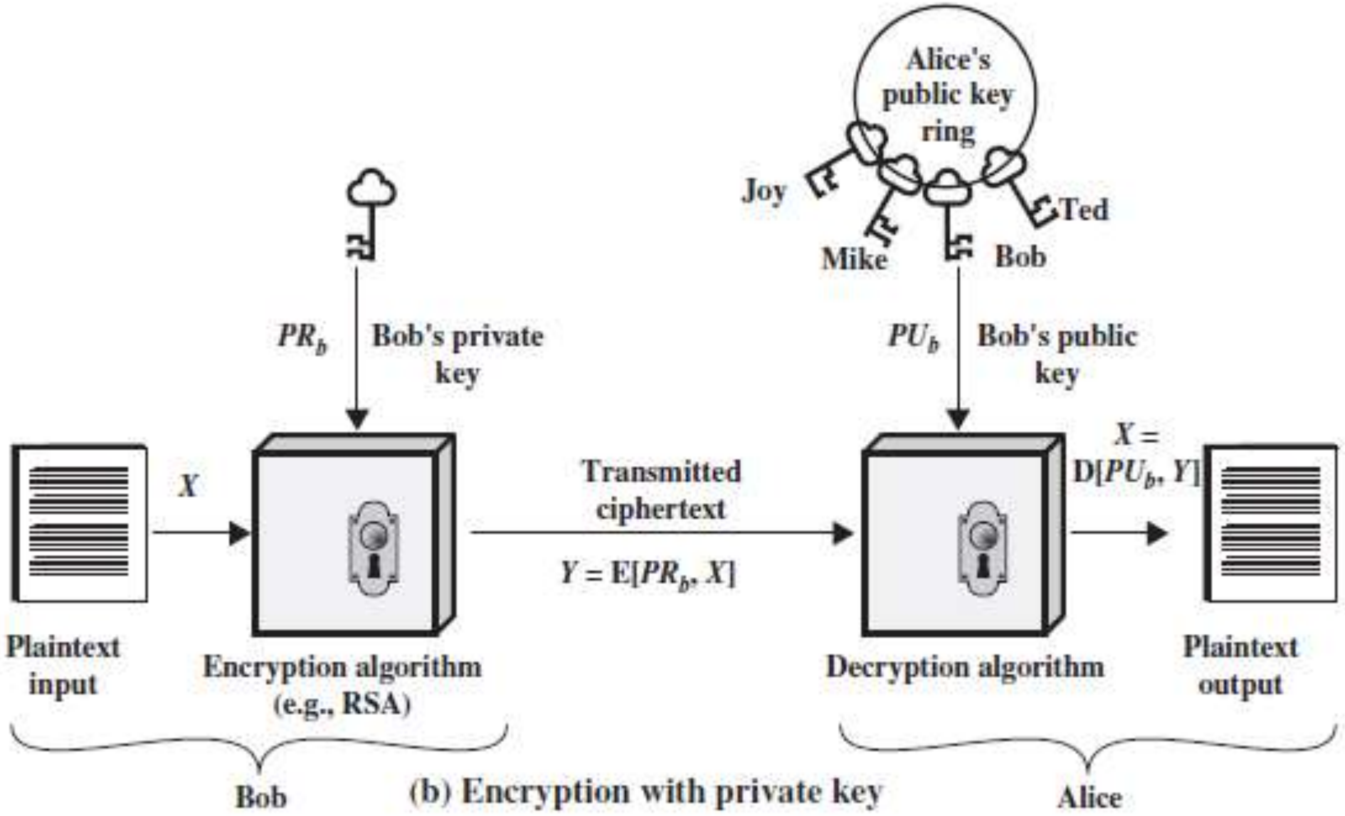
Decryption Algorithm

# Public-Key Cryptosystems



(a) Encryption with public key

# Public-Key Cryptosystems



(b) Encryption with private key

# Applications of Public-Key Cryptosystems

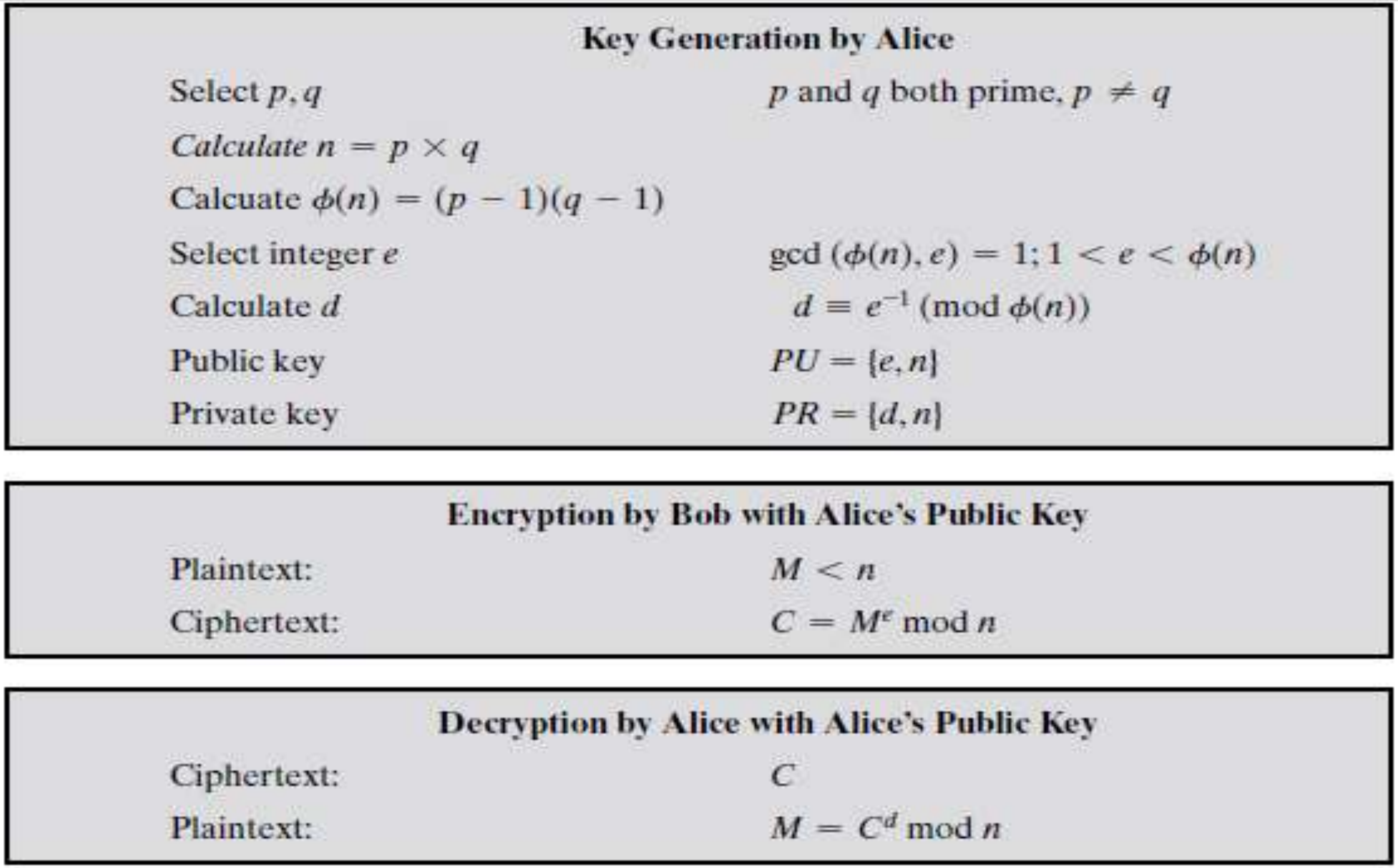
| Algorithm | Encryption/ Decryption | Digital Signature | Key Exchange |
|---|---|---|---|
| RSA | Yes | Yes | Yes |
| Elliptic Curve | Yes | Yes | Yes |
| Diffie-Hellman | No | No | Yes |
| DSS | No | Yes | No |

# RSA cryptosystem

- RSA was developed in 1977 by Ron Rivest, Adi Shamir and Len Adleman at MIT and first published in 1978.
- Algorithm parameters

| | | | |
|---|---|---|---|
| M | => Message | n | => product of p & q |
| C | => Ciphertext | $\Phi(n)$ | => product of p-1 and q-1 |
| d | => Private Key | | |
| e | => Public Key | | |
| p & q | => Prime numbers | | |

# The RSA Algorithm



**Key Generation by Alice**

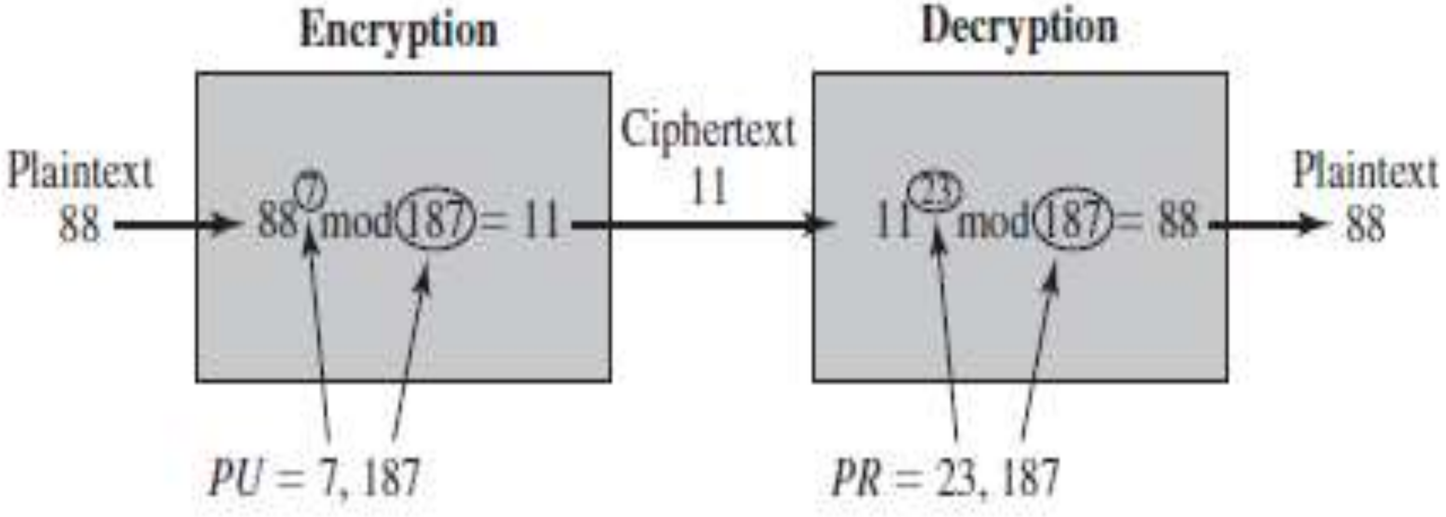
| | |
|---|---|
| Select $p, q$ | $p$ and $q$ both prime, $p \neq q$ |
| *Calculate* $n = p \times q$ | |
| Calcuate $\phi(n) = (p - 1)(q - 1)$ | |
| Select integer $e$ | $\gcd(\phi(n), e) = 1; 1 < e < \phi(n)$ |
| Calculate $d$ | $d \equiv e^{-1} \pmod{\phi(n)}$ |
| Public key | $PU = \{e, n\}$ |
| Private key | $PR = \{d, n\}$ |

**Encryption by Bob with Alice's Public Key**

| | |
|---|---|
| Plaintext: | $M < n$ |
| Ciphertext: | $C = M^e \bmod n$ |

**Decryption by Alice with Alice's Public Key**

| | |
|---|---|
| Ciphertext: | $C$ |
| Plaintext: | $M = C^d \bmod n$ |



Example of RSA Algorithm

# RSA cryptosystem

Encryption & Decryption

p & q = Two prime numbers

n = p * q

Φ(n) = p-1 * q-1

gcd(e,Φ(n)) = 1 => e

e*d mod Φ(n) =1 => d

C = $M^e$ mod n

M = $C^d$ mod n

# RSA cryptosystem

Message = hello

Represent in number

= 8 5 12 12 15

$p = 5$, $q = 7$ (Randomly)

$n = p*q=35$

$\Phi(n) =p-1 * q-1 = 24$

$\gcd(e, \Phi(n) )=1$

$\gcd(e,24)=1$

$e=1, 5, 7, \mathbf{11}, 13, 17, 19, 23 = 11$

$e * d \bmod \Phi(n) = 1$

$11 * d \bmod 24 =1$

$11 * 11 \bmod 24 =1$

$121 \bmod 24 =1$

$d=11$

# RSA cryptosystem

$$
\begin{aligned}
C = M^{e} \bmod n &= 8^{11} \bmod 35 \\
&= 8589934592 \bmod 35 \\
&= 22 \\
&= [8^{4} \bmod 35 * 8^{4} \bmod 35 * 8^{3} \bmod 35] \bmod 35 \\
&= [4096 \bmod 35 * 4096 \bmod 35 * 512 \bmod 35] \bmod 35 \\
&= [1 * 1 * 22] \bmod 35 \\
&= 22 \bmod 35 \\
&= 22
\end{aligned}
$$

# RSA cryptosystem

$M = C^d \bmod n = 22^{11} \bmod 35$

$= 584318301411328 \bmod 35$

$= 8$

$= [22^4 \bmod 35 * 22^4 \bmod 35 * 22^3 \bmod 35] \bmod 35$

$= [234256 \bmod 35 * 234256 \bmod 35 * 10648 \bmod 35] \bmod 35$

$= [1 * 1* 8] \bmod 35$

$= 8$

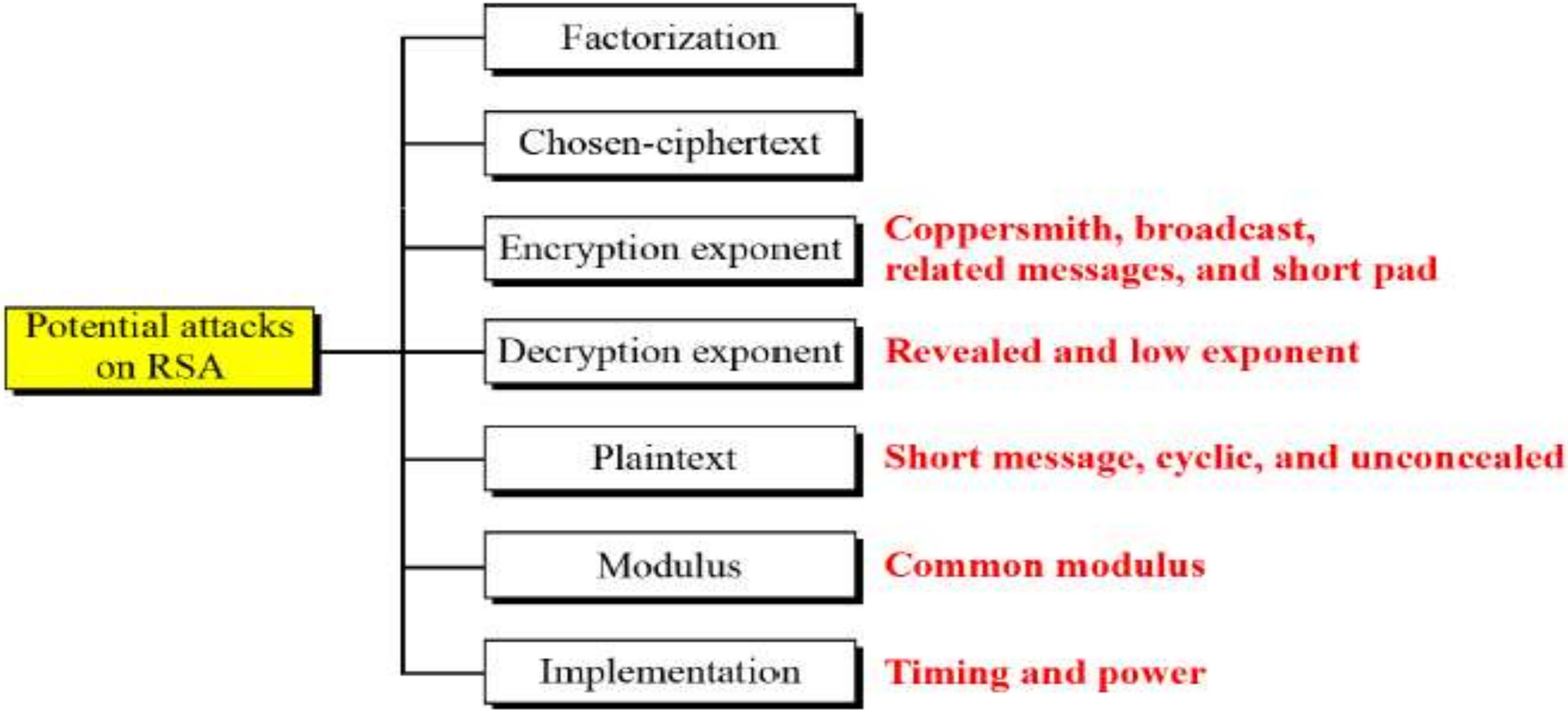
# The Security of RSA

Five possible approaches to attacking the RSA algorithm are

- **Brute force:** This involves trying all possible private keys.
- **Mathematical attacks:** There are several approaches, all equivalent in effort to factoring the product of two primes.
- **Timing attacks:** These depend on the running time of the decryption algorithm.
- **Hardware fault-based attack:** This involves inducing hardware faults in the processor that is generating digital signatures.
- **Chosen ciphertext attacks:** This type of attack exploits properties of the RSA algorithm.

# Attacks on RSA

Taxonomy of potential attacks on RSA



# TRASH TALKER-13

1. RSA is also a stream cipher like Merkel-Hellman.
a) True
b) False

Answer: a
Explanation: RSA is a block cipher system.

2. In the RSA algorithm, we select 2 random large values ‘p’ and ‘q’. Which of the following is the property of ‘p’ and ‘q’?
a) p and q should be divisible by Φ(n)
b) p and q should be co-prime
c) p and q should be prime
d) p/q should give no remainder

Answer: c
Explanation: ‘p’ and ‘q’ should have large random values which are both prime numbers.

3. In RSA, $\Phi(n)$ = ________ in terms of p and q.
a) (p)/(q)
b) (p)(q)
c) (p-1)(q-1)
d) (p+1)(q+1)

Answer: c
Explanation: $\Phi(n) = (p-1)(q-1)$.
4. For p = 11 and q = 19 and choose e=17. Apply RSA algorithm where message=5 and find the cipher text.
a) C=80
b) C=92
c) C=56
d) C=23

Answer: a
Explanation: $n = pq = 11 \times 19 = 209$.

5. In RSA, we select a value ‘e’ such that it lies between 0 and $\Phi(n)$ and it is relatively prime to $\Phi(n)$.
a) True
b) False

Answer: b
Explanation: $\gcd(e, \Phi(n))=1$; and $1 < e < \Phi(n)$.