UNIT-2

PART-A

Mathematics of Asymmetric-key cryptography

1. primes
2. primality Testing.
3. Factorization.

PART-B

Asymmetric key cryptography.

1. RSA cryptosystem
2. Rabin Cryptosystem.
3. ElGamal Cryptosystem.
4. Elliptic curve cryptosystem.

PART-A

Mathematics of Asymmetric-Key cryptography.

(1) primes :

(1) Asymmetric-Key. cryptography uses primes extinsively.
(2) The positive integers can be divided into Three groups, They are Number 1,, primes and composites.

Integer
- Number 1 — exactly 1 divisors
- prime — exactly 2 divisors
- composite — more than 2 divisors.

→ An integer can be Number 1, if it has exactly 1 divisor.
→ An integer can be prime number, if it has exactly 2 divisors. (1 & itself)
→ An integer can be a composite number, if it has more than 2 divisors.

Co-primes :
1) The positive integers 'a' and 'b' are said to be co-primes, if

$$\boxed{\gcd(a,b)=1}$$

2) co-primes are also called Relative primes.
3) If 'p' is a prime then all integers 1 to p-1 are relatively prime

cardinality of primes :
→ Given, a number 'n', the cardinality of primes will result in how many primes are smaller than or equal to 'n'.
ex: The cardinality of 23 is '9'.

Checking for primes :
example-1 : check 97 is a prime or not.
sol: step-1: calculate the floor of $\sqrt{97}$ = 9
step-2: The primes which are less than '9' are considered. (2,3,5,7)
Step-3: We need to see that 97 is divisible by 2,3,5 or 7.

step-4 : Since 97 is not divisible by 2, 3, 5 or 7, Hence, 97 is prime Number.

example-2 : check 301 is a prime number or not.

Step-1 :- calculate the floor of $\sqrt{301} = 17$.

Step-2 :- The primes which are less than 17 are considered (2, 3, 5, 7, 11 & 13)

Step-3 :- we need to see that 301 is divisible by 2, 3, 5, 7, 11 and 13

Step-4 :- The number 301 is divisible by 7, hence 301 is not prime.

→ Eulers phi-function :

(1) Eulers phi-function can also be called as Euler's Totient function.

(2) Eulers phi-function is denoted by $\phi(n)$. which is used to find the number of integers that are both smaller than 'n' and a relatively prime to 'n'.

(3) The function $\phi(n)$ calculates the number of elements in the set which is denoted by Z_n^*.

(4) To find the value of $\phi(n)$, we use the below mentioned rules.

1. $\phi(1) = 0$
2. $\phi(p) = p-1$, if p is prime.
3. $\phi(m \times n) = \phi(m) \times \phi(n)$, if m and n are relatively prime.
4. $\phi(p^e) = p^e - p^{e-1}$, if p is prime.

ex-1 : calculate the value of Eulers phi-function for $\phi(10)$.

$\rightarrow \phi(10)$

$\rightarrow \phi(2 \times 5)$

$\Rightarrow \phi(2) \times \phi(5)$

$\Rightarrow (2-1) \times (5-1)$

$\Rightarrow 1 \times 4 = 4$

ex-2: Calculate the value of $\phi(240)$ using Euler's Totient function.

$\phi(240) = \phi(5 \times 3 \times 2^4)$.

$= \phi(5) \times \phi(3) \times \phi(2^4) = 4 \times 2 \times (2^4 - 2^3)$

$= 8 \times (16-8) = 8 \times 8 = 64$.

→ Fermat's Little Theorem:

(1) The Fermat's little Theorem is of two versions, They are

First version: The First version of Fermat's little Theorem says that if 'p' is a prime and 'a' is an integer such that 'p' does not divide 'a' then

$$\boxed{a^{p-1} \equiv 1 \bmod p} \qquad \boxed{a^{p-1} = 1}$$

$p > 2$

Second version: The second version of Fermat's little theorem removes the condition on 'a', where 'p' is a prime and 'a' is an integer.

Then $$\boxed{a^p \equiv a \bmod p} \qquad \boxed{a^p = a}$$

ex-1: Find the result of 6^{10} mod 11 using Fermat's little theorem.

→ 6^{10} mod $11 \leftarrow p$

⇒ 6^{11-1} mod 11 ($p-1$)

$= 1$ (By using 1st version).

ex-2: Find the result of 3^{12} mod 11 using Fermat's little Theorem.

→ 3^{12} mod 11

⇒ 3^{11+1} mod 11

⇒ $3^{11} . 3^1$ mod 11

⇒ $(3^{11}$ mod $11)(3$ mod $11)$

⇒ $3 \times 3 = 9$

→ Euler's Theorem:

(1) Euler's Theorem is a generalization of Fermat's little Theorem.

(2) The modulus in the Fermat Theorem is a prime whereas the modulus in Euler's Theorem is an integer.

(3) Euler's Theorem has two versions, They are.

First Version: It is similar to the first version of Fermat's little Theorem. If 'a' and 'n' are coprimes then $a^{\phi(n)}$ is linearly congruent to $1 \pmod n$ $\Rightarrow$ $\boxed{a^{\phi(n)} \equiv 1 \pmod n}$

Second version: It is similar to the second version of Fermat's little Theorem which removes the condition that 'a' and 'n' should be coprimes:

If $n = p \times q$, $a < n$ and K is an integer, then

$$\boxed{a^{K \times \phi(n) + 1} \equiv a \pmod n}$$

PART-B

Asymmetric key cryptography.

1. RSA Algorithm:

(1) RSA Algorithm was developed by Ron Rivest, Adi Shamir and Leonard Adleman

(2) RSA is based on Asymmetric key cryptography which uses two keys, They are public key and private key.

(3) RSA is most widely implemented general purpose public key encryption algorithm.

Algorithm:

1. Consider two large prime numbers, denoted by p and q.
2. Calculate n, where $\boxed{n = p * q}$
3. Calculate Eulers Totient function for n which is denoted by $\phi(n)$, where $\boxed{\phi(n) = (p-1) * (q-1)}$
4. Assume a public key, denoted by 'e' where $\boxed{\gcd(e, \phi(n)) = 1}$ such that $1 < e < \phi(n)$
5. Determine private key which is denoted by 'd' such that $\boxed{d \equiv e^{-1} \bmod \phi(n)}$ (or)

$$\boxed{d * e \bmod \phi(n) = 1}$$

6. Hence, The derived keys are

public Key = $\{e, n\}$

private Key = $\{d, n\}$

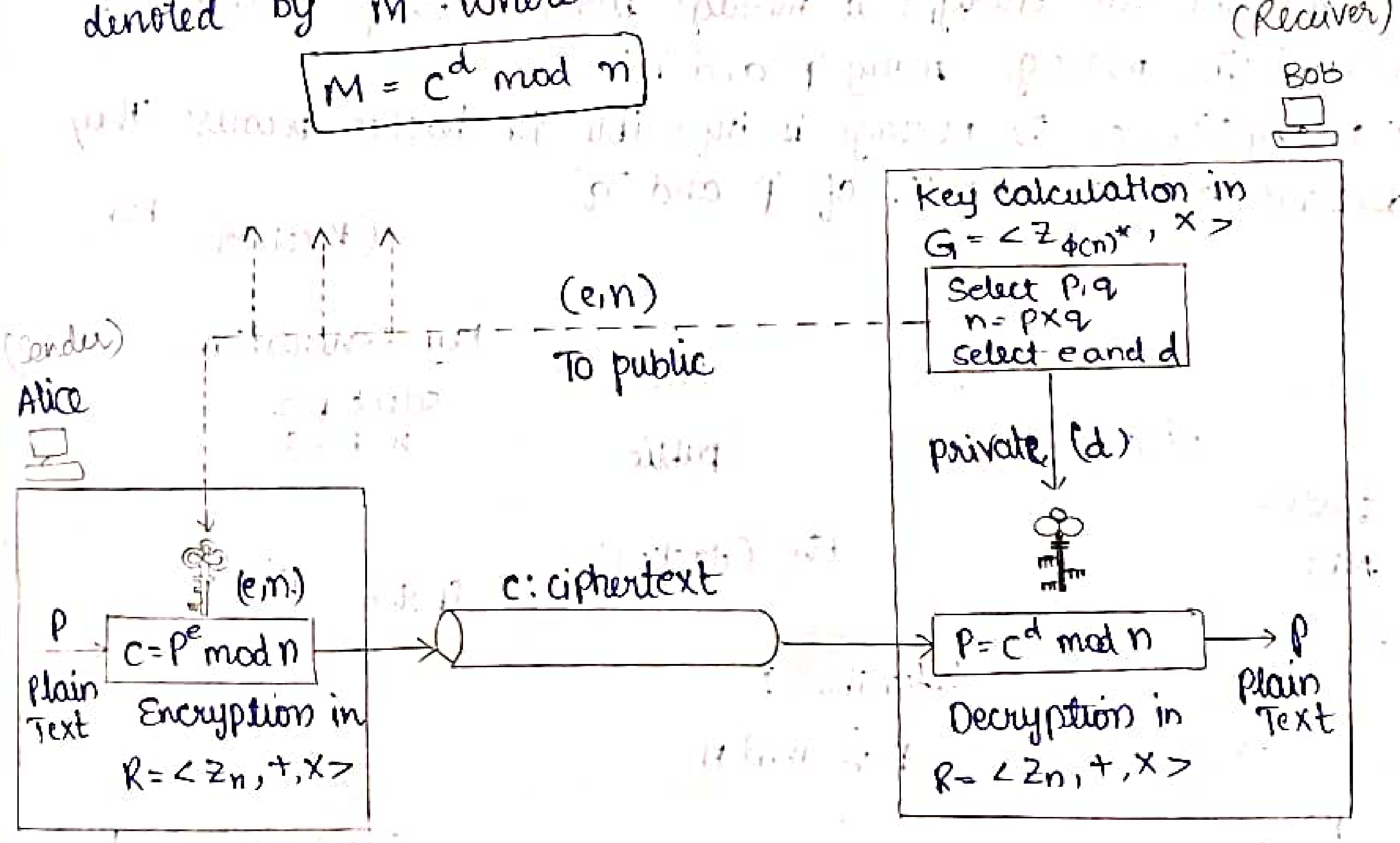
7. Consider a plain text message denoted by 'M' where $M < n$.

8. Encryption: The cipher Text is denoted by 'C' where

$$\boxed{C = M^e \bmod n}$$

9. Decryption: To decrypt the ciphertext, the plain text is denoted by 'M' where

$$\boxed{M = C^d \bmod n}$$



Encryption, decryption and key generation in RSA

2. Rabin Cryptosystem:

(1) The Rabin crypto system, devised by M. Rabin, is a variation of the RSA cryptosystem.

(2) RSA is based on the exponentiation congruence, Rabin is based on a Quadratic congruence.

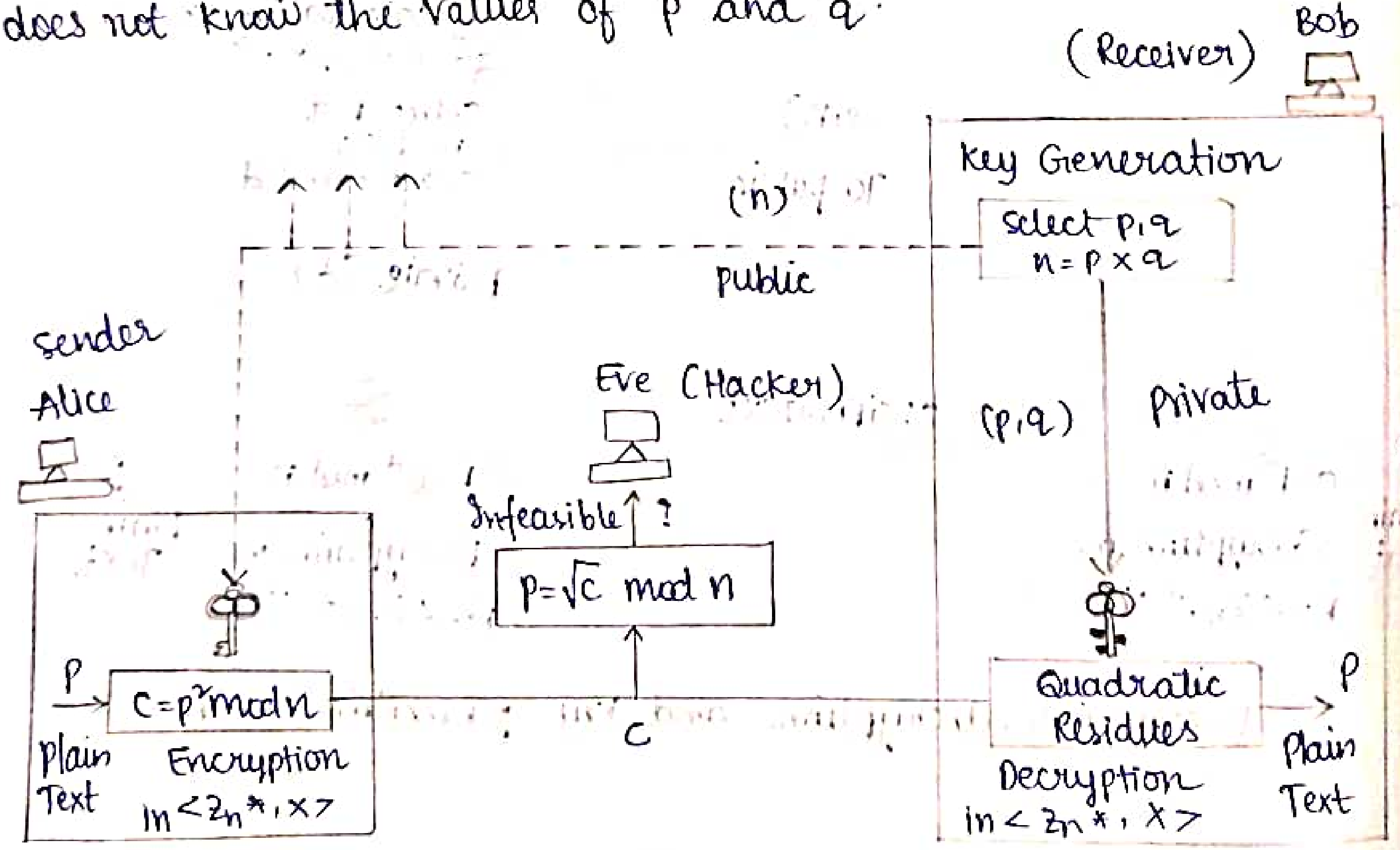
(3) The Rabin cryptosystem can be thought of as an RSA cryptosystem in which the value of 'e' and 'd' are fixed. i.e., $e = 2$ and $d = 1/2$

(4) In other words, the encryption is $C \equiv P^2 \pmod{n}$ and the decryption is $P \equiv C^{1/2} \pmod{n}$

(5) The public key in the Rabin cryptosystem is n, the private key is the tuple (p, q)

(6) Everyone can encrypt a message using 'n', only receiver can decrypt the message using 'p' and 'q'.

(7) Decryption of the message is infeasible for hacker because they does not know the values of 'p' and 'q'.

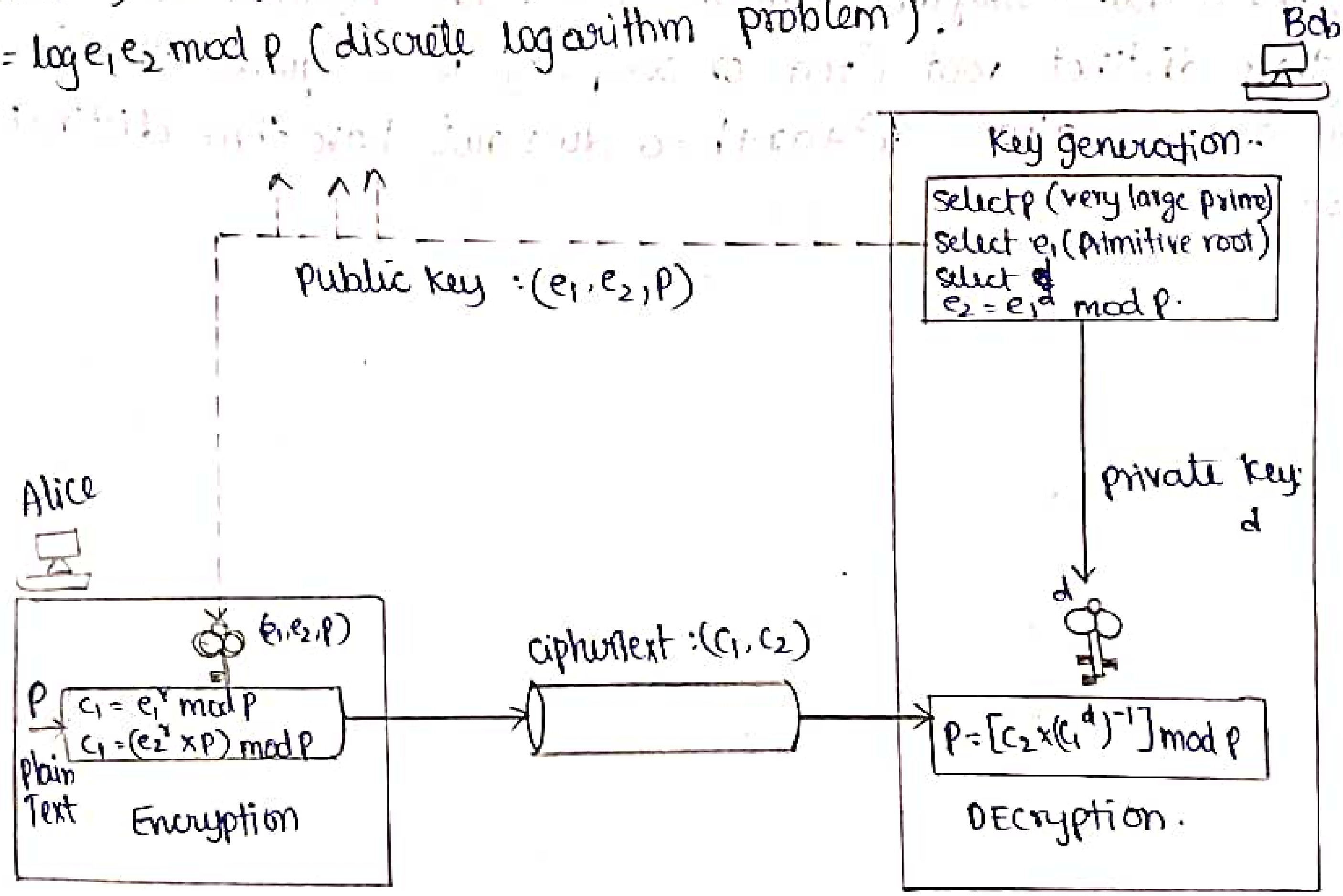


Encryption, decryption and key generation in Rabin Cryptosystem

(3) Elgamal cryptosystem :

Besides RSA and Rabin, another public key cryptosystem is Elgamal, named after its inventor, Taher Elgamal. Elgamal is based on the discrete algorithm problem.

If 'p' is a very large prime, 'e_1' is a primitive root in the group $G = \langle Z_p^*, \times \rangle$ and 'r' is an integer, Then $e_2 = e_1^r \bmod p$. is easy to compute using the fast exponential algorithm (square and multiply method) but given e_2, e_1 and p, it is infeasible to calculate $r = \log_{e_1} e_2 \bmod p$ (discrete logarithm problem).



Key Generation, encryption and decryption in ElGamal.

(4) Elliptic curve cryptosystems :

RSA and Elgamal are secure assymmetric key cryptosystems with large keys. One of the promissing alternatives is the elliptic curve cryptosystem. (ECC). The system is based on the Theory of elliptic curve.

Elliptic curves over Real Numbers

Elliptic curves which are not directly related to ellipses, are cubic equations in two variables That are similar to the equations used to calculate the length of a curve in the circumference of an ellipse. The general equation for an elliptic curve is

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

Elliptic curves over real number are a special class of elliptic curve of the form

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

In the above equation, if $4a^3 + 27b^3 \neq 0$, The equation represents a non-singular elliptic curve, the equation $x^3 + ax + b = 0$ has three distinct roots (real or complex) in singular elliptic curve the equation $x^3 + ax + b = 0$ does not have three distinct roots.