* UNIT IV *

* Assymentric or public key cryptography

public key cryptography is also known as assymentric key cryptography here do diffent keys are use for encryption and description process respectively know other key can decrept the massage given the orignal key and therefore. on key is strictly use for encryption. i.e private key of sender and another key of will only decrept the massage the charactersitic of pkc. is that each communicating entity must have a paired of secreate key i.e private key and public key once a key pair is obtained then they can communicate with another entity

There is simple mathematical basis for this scheme if you have an extemly large number that has exactly two factors (prime numbers then you can gerate the pair of secreate (key)

for ex- consider the number 10

also = 10 has two factors 2 and 5 are prime numbers so we will use 5 for encryption and 2 for decryption purpose also nothing else can decrypt the massage. even 5 can also not decrypt

the massage. hence we can genrate and utilize the secrate key pairs using prime numbers but the prime numbers must be sufficently large. that no one can case it easily

* working of public key cryptography

Let as assume that you want to communicate over computer network in secrate manner so we first need to remember obtained a pair of secrate key this pair of secrate key should not declose to any body private key is kept confidencial always and public key will be published for general public cryptography and may disclose. so that other entities can decrapt your massage (to whom youre really to send the massage)

In this scheme each party on node publish there pubic key using the directory of cryptogra phy that can be constructed where the parties and therefor corresponding pubic keys are mainted someone can concern this cryptography directory and get the public key for decryption of massage the key details to whom the key should be known are as follows

key details	A should know	B should know
A s private key	yes	No
As public key	yes	yes
Bs private key	No	yes
Bs public key	yes	yes

using above table the to parties can comunicate over a channel secrate key

the assymentric key cryptography works as follows

① when user A wants to send a massage to user B. the user A encrypt the massage using pubic key of user B. this is possible beacause user A know the public key of user B.

② user A sends the massage which is encypted with the help of public key of user B.

③ user B can decrypt the massage using private key of user B.

④ so that it is not decrypted by any other party, as well as any other parties massage can not be decrypted by user B. and thus attacker can not hack the massage. beacause these private key is not known to any body.

similarly when user B wants to send the message. exactly use procedure will take reverse process take place