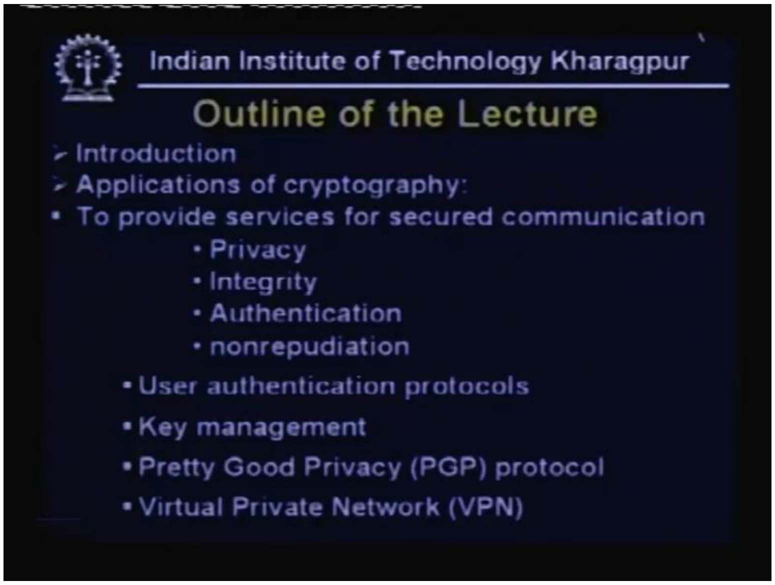
Data Communication
Prof .A.Pal
Dept of Computer Science & Engineering
Indian Institute of Technology, Kharagpur
Lecture - 40
Secured Communication - II

Hello and welcome to today's lecture on secured communication. This is the second lecture on this topic. In the last lecture we have considered various issues on cryptography which has been found to be the panacea to the problem of secured communication. And in this lecture we shall cover various topics essentially which are applications of cryptography. We shall see how cryptography can be used to achieve secured communication particularly before different type of services required in secured communication.

Here is the outline of today's talk. First I shall give a brief introduction then I shall discuss about the applications of cryptography. As I mentioned, particularly this will lead to privacy, integrity, authentication and nonrepudiation. These are the four services to be provided for secured communication.

(Refer Slide Time: 01:38)



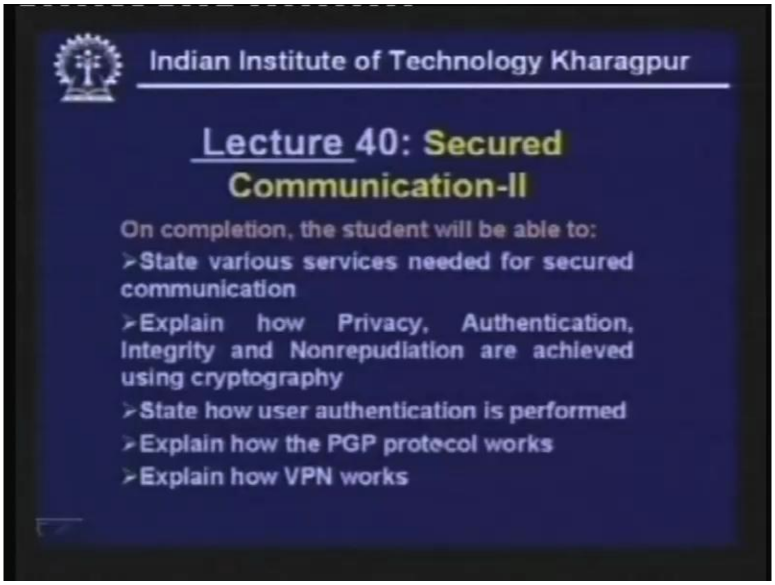
Indian Institute of Technology Kharagpur

Outline of the Lecture

- Introduction
- Applications of cryptography:
- To provide services for secured communication
  - Privacy
  - Integrity
  - Authentication
  - nonrepudiation
- User authentication protocols
- Key management
- Pretty Good Privacy (PGP) protocol
- Virtual Private Network (VPN)

Then apart from message privacy message, integrity message, authentication and nonrepudiation it is necessary to provide user authentication which is important in the context of key management. Then we shall discuss how key management can be done by using suitable techniques then we shall consider application layer protocol pretty good privacy PGP which can be used for secured communication of emails. And I shall conclude my lecture after discussing virtual private network which is essentially a network used for secured communication.

(Refer Slide Time: 02:49)



Indian Institute of Technology Kharagpur

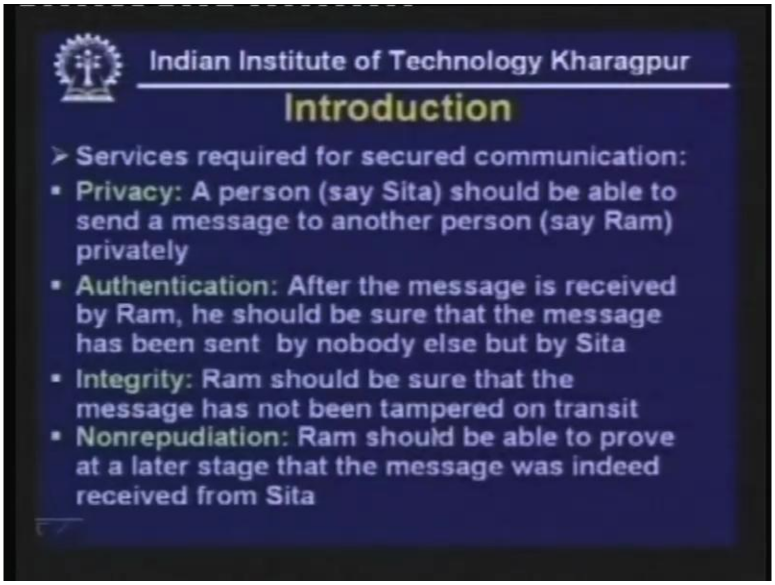
Lecture 40: Secured Communication-II

On completion, the student will be able to:

- State various services needed for secured communication
- Explain how Privacy, Authentication, Integrity and Nonrepudiation are achieved using cryptography
- State how user authentication is performed
- Explain how the PGP protocol works
- Explain how VPN works

And on completion of this lecture the students will be able to state various services needed for secured communication, they will be able to explain how the four services such as privacy, authentication, integrity and nonrepudiation are achieved using cryptography, they will be able to state how user authentication is performed, they will be able to explain how PGP protocol pretty good privacy protocol works and also they will be explain how virtual private network works. So as I mentioned in the last lecture, these are the four important services required for secured communication.

(Refer Slide Time: 03:27)



Indian Institute of Technology Kharagpur

Introduction

- Services required for secured communication:
- Privacy: A person (say Sita) should be able to send a message to another person (say Ram) privately
- Authentication: After the message is received by Ram, he should be sure that the message has been sent by nobody else but by Sita
- Integrity: Ram should be sure that the message has not been tampered on transit
- Nonrepudiation: Ram should be able to prove at a later stage that the message was indeed received from Sita

In cryptography we normally use three characters; the sender, the receiver and the person in the middle sender here we have used the character Sita. The receiver is Ram and the person in the middle who is essentially the intruder or eavesdropper who is trying to impersonate is Ravana. By privacy we mean a person say Sita should be able to send a message to another person called Ram privately. Also, we mean, even if the message is received by other than Ram then it will not be intelligible to him or her so it should be intelligible only to Ram and not by anybody else. That is the basic reason for privacy.

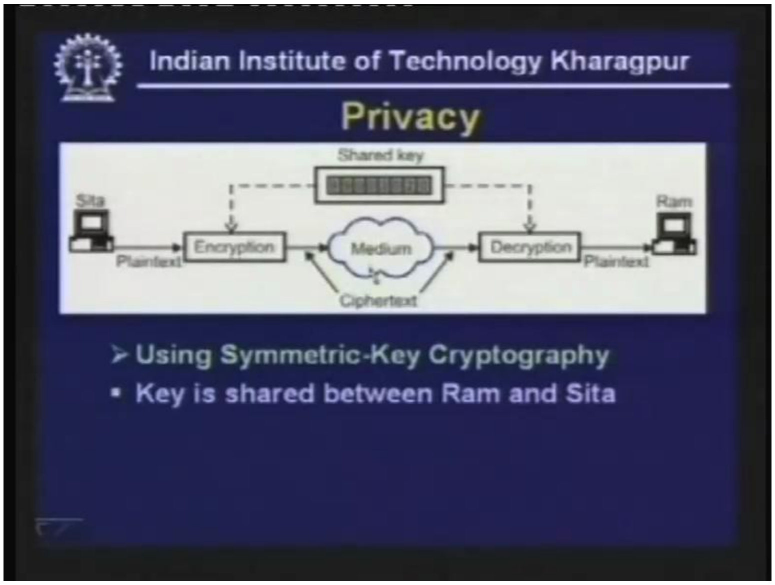
Second is authentication. After the message is received by Ram he should be sure that message has been sent by nobody else but by Sita. That means the authentication of the sender has to be authenticated.

Then we have integrity. Ram should be sure that the message has not been tampered on transit so when the message is passing through an unreliable network it may be tampered by the intruder Ravana. So he will try to modify and to his advantage it may necessarily corrupt it and that should be clear to Ram, Ram should be able to identify if a message is tampered on transit.

Finally is the nonrepudiation. Ram should be able to prove at a later stage that the message was indeed received from Sita so there may be a situation when Sita may say at a later stage that a particular message was not sent by her to Ram so Ram should be able to prove that it was indeed sent by Sita so that is the requirement service requirement in the context of non repudiation.

First we shall focus on privacy, how privacy can be achieved by using cryptography. It can by achieved by cryptography by using shared key or symmetric key approach. Here what can be done Sita can convert the plain text into cipher text by encrypting with the help of a shared key.

(Refer Slide Time: 06:22)



Indian Institute of Technology Kharagpur

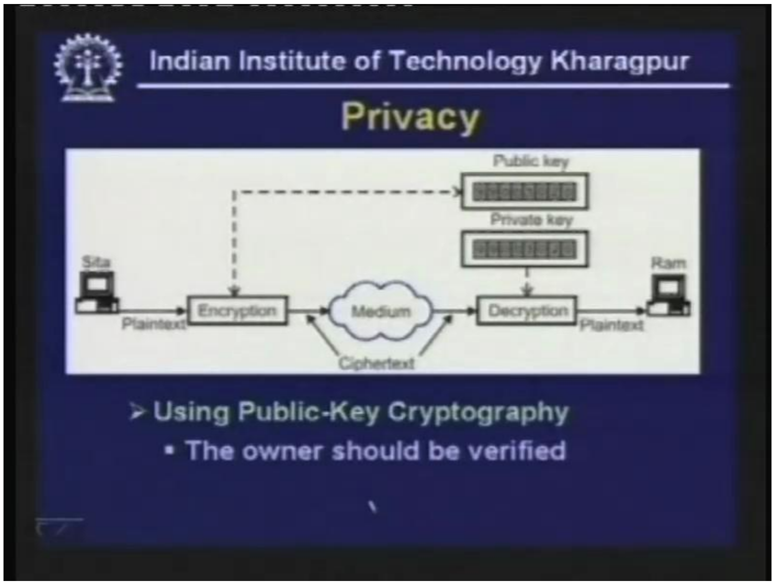
Privacy

- Using Symmetric-Key Cryptography
- Key is shared between Ram and Sita

So encrypted message is now sent through the medium which is not safe. Thus in the middle Ravana may try to get access of it but it will not be intelligible, it will be unintelligible to Ravana. After it reaches Ram he should be able to decrypt it with the help of the same shared key and get back the message so the privacy is satisfied here because even if Ravana gets the message he may not be able to understand the message. So here the basic issue is that key is shared between Ram and Sita and particularly in shared key approach we require a very large number of keys that is one important problem. Later on we shall discuss on how it can be resolved.

Then comes the privacy by using public key cryptography. Here what is being done is Sita performs encryption. That means Sita converts the plain text into cipher text with the help of the public key of Ram.

(Refer Slide Time: 07:37)



Indian Institute of Technology Kharagpur

Privacy

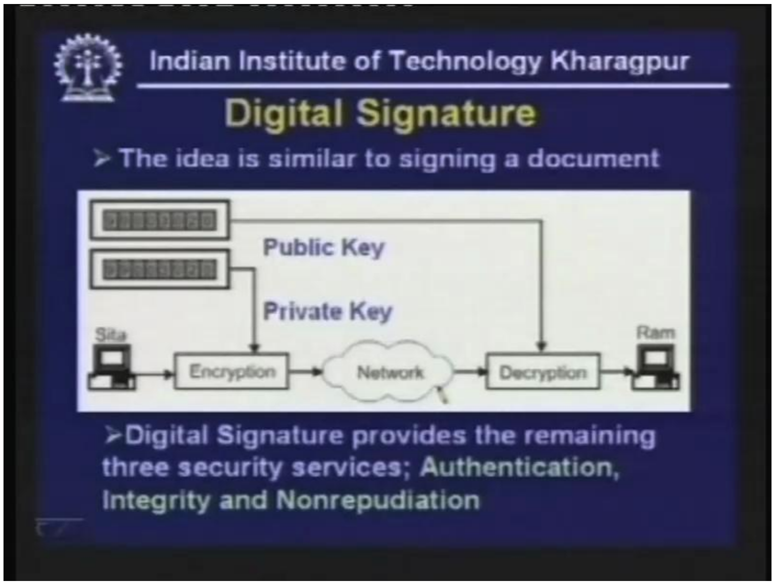
- Using Public-Key Cryptography
  - The owner should be verified

So the public key of Ram is used to do the encryption and the encrypted message traverses through a reliable medium and as it reaches Ram then decryption can be done with the help of the private key of Ram. So Ram can do the decryption by using his private key to get back the plain text from the cipher text. This is how the privacy of the message is preserved by this technique.

In this case the problem is Sita is using the public key of Ram so it is necessary to verify that the public key indeed belongs to Ram and not by some imposter. So, if an imposter sends a public key to Sita and if she uses that public key for sending through the medium then the purpose will be lost. Hence, this has to be verified in the context of public key cryptography when you use public key cryptography.

So you have seen how privacy can be maintained by using shared key cryptography and by public key cryptography. Let us now focus on the other three aspects or services required that is authentication, integrity and nonrepudiation. These three services can be achieved by using a technique known as digital signature. What is digital signature? Let us try to understand. The digital signature is very similar to signing a document.

(Refer Slide Time: 09:28)



Indian Institute of Technology Kharagpur

Digital Signature

- The idea is similar to signing a document

Public Key

Private Key

Sita

Ram

Encryption

Network

Decryption

- Digital Signature provides the remaining three security services; Authentication, Integrity and Nonrepudiation

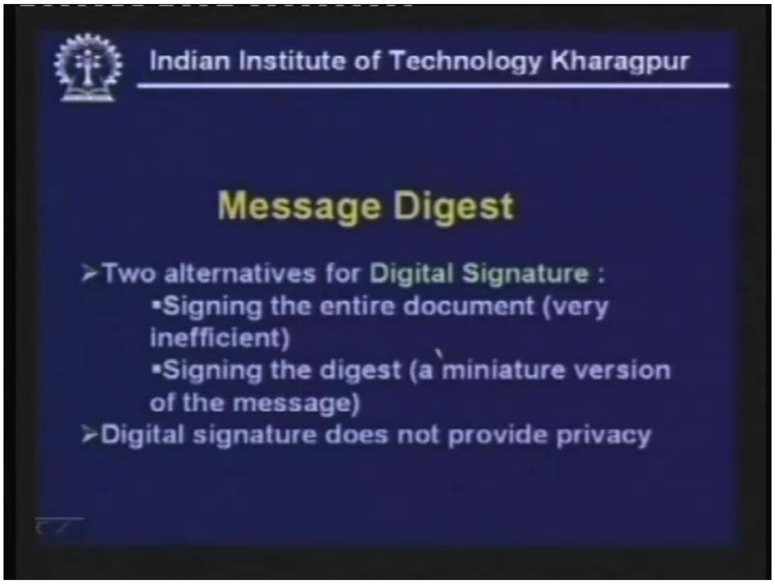
Normally whenever we send a document, and particularly if it is a legal document or something else, on each page signature is given so that signature actually authenticates the document. So a somewhat similar technique is used here. However, here where by signature we mean some kind of encryption is being done. How it is done is explained here by using the public key cryptography.

Here Sita does the encryption by using the private key of Sita. So private key of Sita is being used here for doing the encryption of the plain text and the cipher text passes through the network and as it reaches the receiver Ram he does the decryption by using public key of Sita. So here you see the public key of Sita is used to do the decryption and private key of Sita is being used to do the encryption. By this process Ram is able to achieve all the three services required. For example, authentication is done because here Ram is doing the decryption by using the public key of Sita. That means if it was not received from Sita then obviously the encryption and decryption would not have been possible by using the public key of Sita. So it does authentication and integrity is also verified because the entire message was encrypted. And after decryption it is possible to regenerate the plain text so since it is possible to regenerate the plain text the integrity is maintained. That means if the message was tampered on transit then it is not possible to get back the plain text after decryption so the integrity is also achieved by using this approach.

Finally comes the question of nonrepudiation. Here since the decryption has been done by using the public key of Sita, later on if somebody asks Ram can you prove that the message you received was indeed received from Sita then the plain text that was generated can be encrypted again by the public key or private key of Sita and then decrypted using the public key of Sita to get back the same plain text. That proves that the message was indeed received from Sita because it was possible to do the decryption by the public key of Sita. So, all the three aspects are satisfied by using this digital signature technique.

However, this digital signature can be done by using two approaches. First one is signing the entire document and second one is signing the digest. So, if signing the entire document is done that is possibly better but it is not very efficient because the message can be very large so encryption will take lot of time.

(Refer Slide Time: 12:48)



Indian Institute of Technology Kharagpur

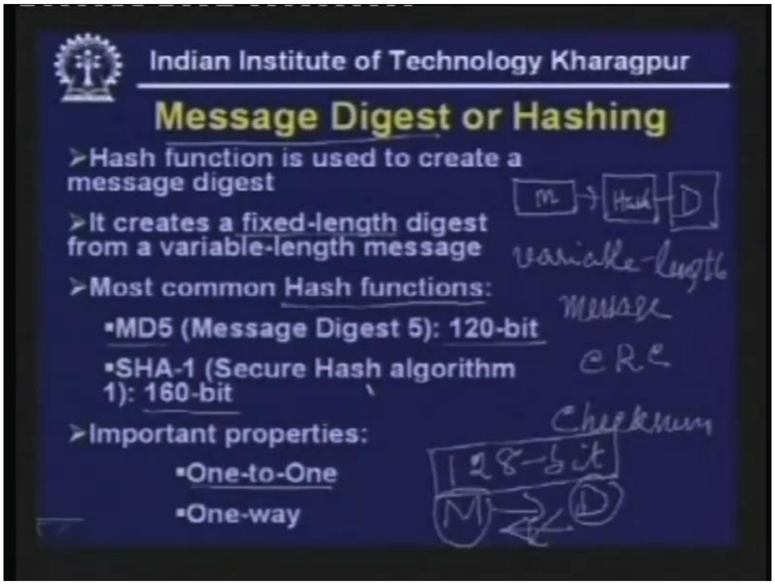
Message Digest

- Two alternatives for Digital Signature :
  - Signing the entire document (very inefficient)
  - Signing the digest (a miniature version of the message)
- Digital signature does not provide privacy

But particularly by using the public key cryptography as you know in public key cryptography the size of the key is quite large more than 256 bits and as a consequence the encryption takes very long time. So if it is done on the entire message it will take very long time so it is not very efficient. That is why another approach can be done which is known as digital signature which is essentially a miniature version of the original message. So a miniature version of the original message is used for the purpose of authentication, integrity and nonrepudiation verification. However, this digital signature will not be able to provide privacy as we shall see.

Now let us see what we really mean by this message digest and how it can be done. That means the message digest can be done by using a technique known as hashing.

(Refer Slide Time: 17:42)



Indian Institute of Technology Kharagpur

Message Digest or Hashing

- ➢Hash function is used to create a message digest
- ➢It creates a fixed-length digest from a variable-length message
- ➢Most common Hash functions:
  - ▪MD5 (Message Digest 5): 120-bit
  - ▪SHA-1 (Secure Hash algorithm 1): 160-bit
- ➢Important properties:
  - ▪One-to-One
  - ▪One-way

What the hashing does is, suppose this is the message (refer Slide Time: so message is applied to a hashing function and to generate a digest this is your digest. What it effectively does is it converts a variable length message into a fixed length as it is written here fixed length digest. So it is somewhat similar to generating CRC or checksum. We have seen that for the purpose of error detection checksum or cycle redundancy codes are used and those checksum and cycle redundancy codes are either 16 bit or 32 bit long and those are generated from a long message. So here also in a somewhat similar technique a fixed length digest is created from the variable length message and some standard techniques have been developed to perform hashing.

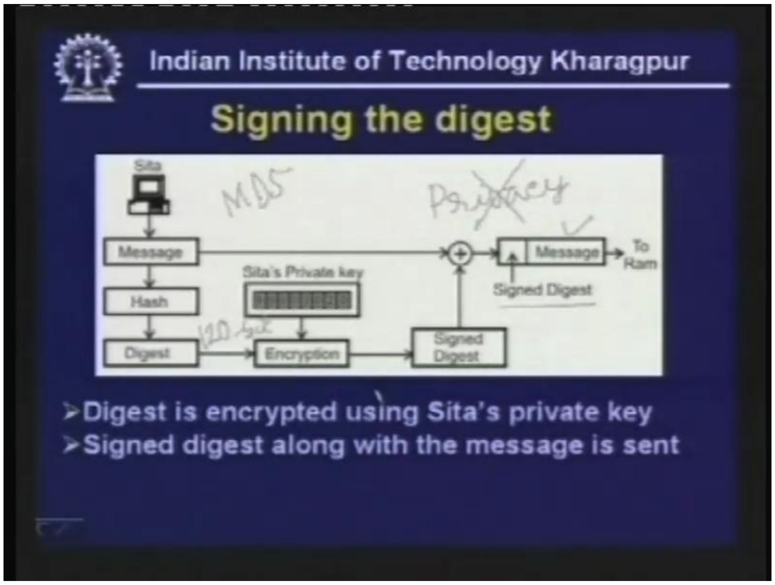
The most common hashing functions are MD5 message digest 5 approach which uses one twenty bit or 128-bit digest that means a fixed length 120 bit digest is generated by using this approach message digest five which is very popular and widely used.

There is another approach secured hash algorithm one SHA-1 which uses 160-bit digest and obviously SHA-1 is much more secure than the MD5 because it uses 160-bit instead of 120-bit. However, SHA-1 is less popular than MD5.

Now you must understand two very important properties of this hashing operation. First of all it is one-to-one. What we really mean by one-to-one? For each message the digest has to be unique. That means the digest that is created has to be unique for a given message and that requirement is satisfied if the digest is about 128-bit. So if it is chosen above 128-bit then that condition is satisfied and 128-bit or more than 128-bit then another condition that has to be that is to be satisfied is it is one way. That means from the message you can generate the digest but you cannot really generate the message from the digest. That means the reverse process is not possible. So a message cannot be generated from the digest and that’s why it is one way. So these two properties are to be satisfied for the message digest to be successful.

Let us see how the signing is done on the digest, signing the digest is performed so here again we are using the private key by public key approach to do the signing on the digest.

(Refer Slide Time: 19:09)



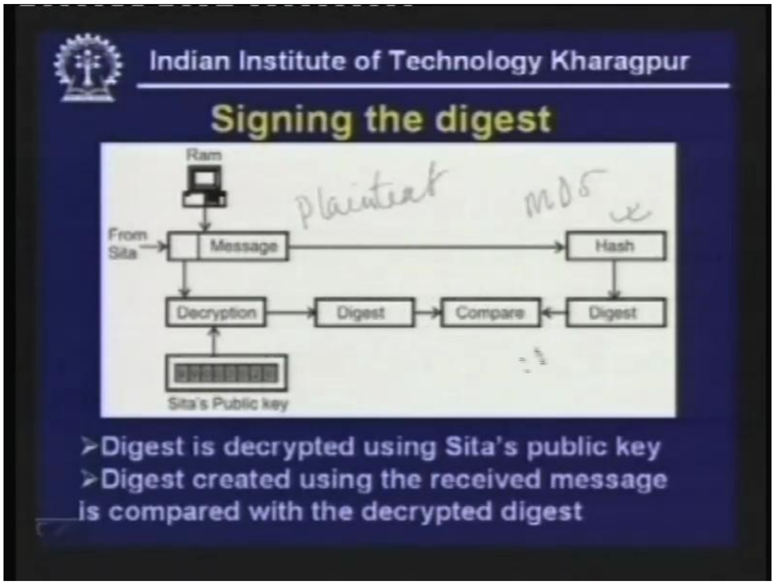
Indian Institute of Technology Kharagpur

Signing the digest

- Digest is encrypted using Sita's private key
- Signed digest along with the message is sent

Here Sita is generating a message then some hashing operation is performed may be MD5. MD5 version five is used to do the hashing to generate 120-bit digest. This 128-bit digest is encrypted by using Sita's private key and then that signed digest is sent along with the message to Ram. So to Ram not only the message is being sent but the signed digest is also sent. Thus, here you see the signed digest is the encrypted version of the digest. On the other hand, the message is not encrypted. As a result it does not give you the privacy. So privacy is not provided by this approach. However, it provides the other three functions that I mentioned namely authentication, integrity and nonrepudiation. Now let us see what is done at the other end.

(Refer Slide Time: 20:18)



Indian Institute of Technology Kharagpur

Signing the digest

- Digest is decrypted using Sita's public key
- Digest created using the received message is compared with the decrypted digest

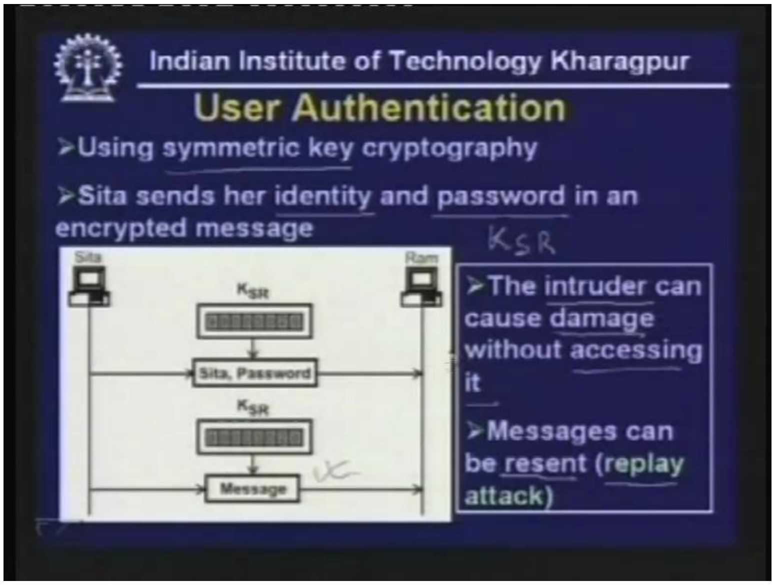
At the other end Ram receives the message along with the signed digest then the signed digest is decrypted by using Sita's public key. Since the encryption was done by using Sita's private key the decryption can also be done by using Sita's public key. So, after doing the decryption the digest is created. Therefore, the message is now received in its original form that is in plain text form.

This plain text form message again is used to generate the digest by using the hashing operation. That is, again the MD5 is used to generate the hashing and the digest is created. And if these two digest are same they are compared.

If they are same then the authentication integrity and non repudiation is satisfied so digest created using the received message is compared with the decrypted digest. In this way the message digest is used to perform the three operations.

Now, apart from this message authentication checking authentication of the integrity of the message it is necessary to do user authentication and this is related to essentially key management and it is necessary how the user authentication can be done is explained here this can be done in various ways.

(Refer Slide Time: 23:15)



Indian Institute of Technology Kharagpur

User Authentication

- Using symmetric key cryptography
- Sita sends her identity and password in an encrypted message

KSR

- The intruder can cause damage without accessing it
- Messages can be resent (replay attack)

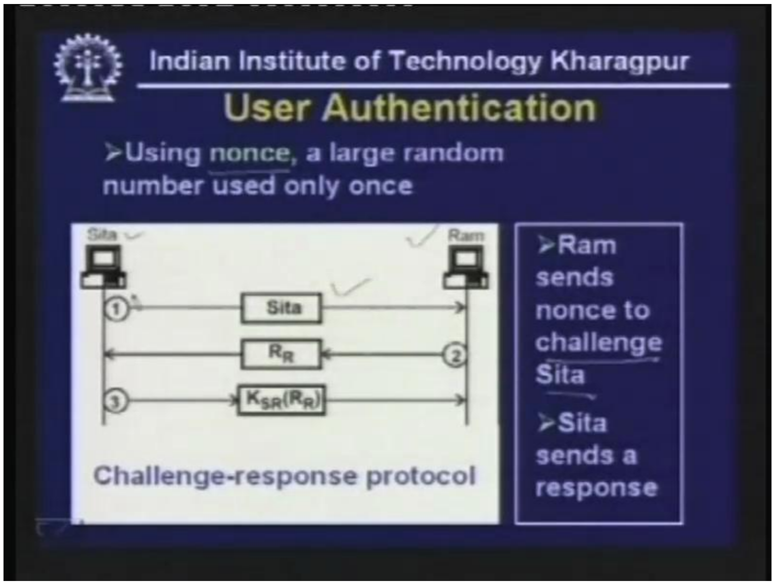
The first approach is based on symmetric key cryptography. Here what is being done is Sita sends her identity and password so identity and password is being sent in an encrypted form by using that shared key KSR. KSR is essentially the shared key between Sita and Ram. SR stands for Sita and Ram so the shared key is being used to do the encryption where the identity of Sita along with password is sent to Ram. Then Ram now knows that the message is indeed coming from Sita so the user authentication is being performed then the message communication takes place.

Sita can send message by using the encryption based on that shared key KSR. Hence, in this way message communication can go on. However, here this particular approach has some problem. First problem is that the intruder can cause damage without accessing it. That means whenever this particular message is going through the network then the intruder or Ravana can get hold of it, can modify it and send it so it can cause damage without accessing it. Therefore in such a case Ram will not be able to authenticate Sita.

Secondly, what the intruder can do is, instead of this a particular message can be replayed, can be generated twice.

Suppose Sita is sending a message to banker ton make some bank payment now one message is sent to pay let’s assume 10000 rupees, another message can be resent by the imposter or intruder and as a consequence two payments are being made. Although Sita has sent only one message for making payment so the banker is making two payments instead of one payment because the same message was resent by the intruder twice. This is known as replay attack. You have to overcome this replay attack. How it can be done is explained later. This problem can be overcome by using an approach known as nonce.

(Refer Slide Time: 25:00)



Indian Institute of Technology Kharagpur

User Authentication

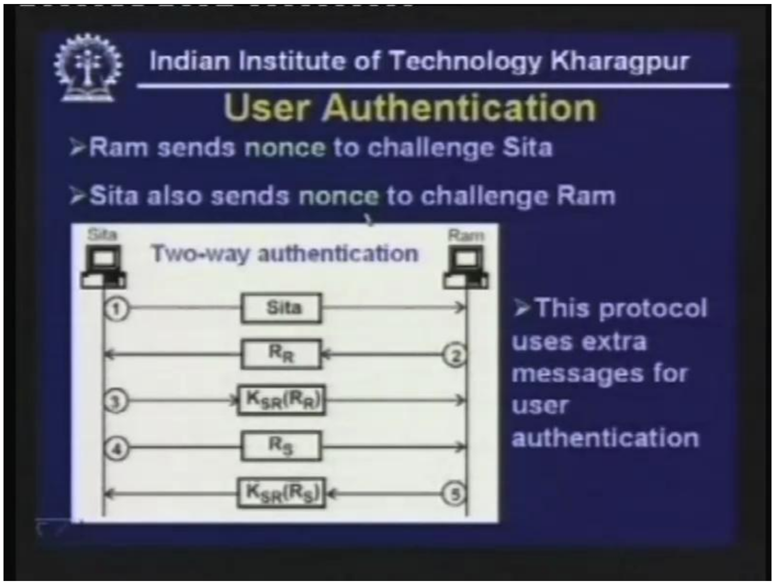
- Using nonce, a large random number used only once

Challenge-response protocol

- Ram sends nonce to challenge Sita
- Sita sends a response

A random number is used only once to challenge to per to do the authentication. What is being done is after Sita sends her identity the Ram receives that identity then Ram sends a nonce. That means one random number our r that means it has been generated by Ram a random number which is being sent to Sita so as a challenge it is being sent to Sita and after Sita receives it she does encryption she responds by sending the encrypted form of this random number R_R and after receiving that Ram is happy because now he is confident that the message is indeed coming from Sita. This particular approach is known as challenge response protocol. By using this challenge response protocol the above problem is verified because after a session is created the resending of message cannot be done twice. However, in this particular situation Ram is able to authenticate the user Sita but Sita is not able to authenticate Ram. So, to do that one can use two-way authentication.

(Refer Slide Time: 26:10)



Indian Institute of Technology Kharagpur

User Authentication

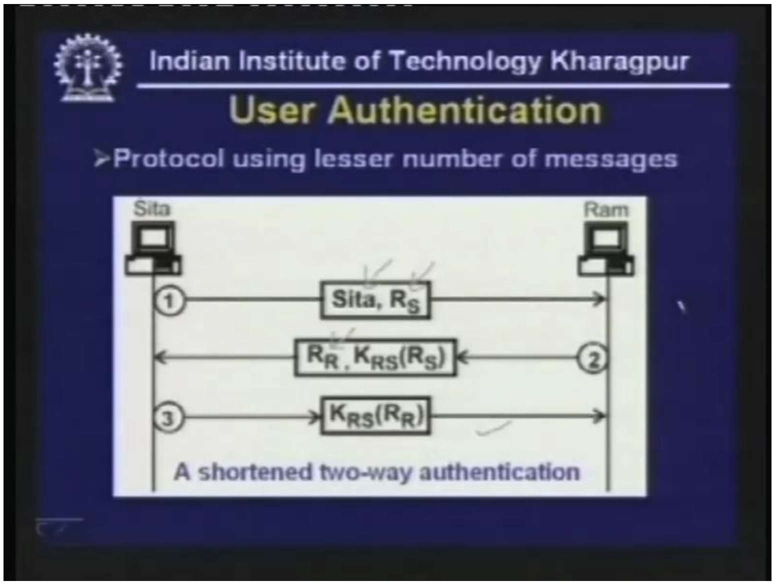
- Ram sends nonce to challenge Sita
- Sita also sends nonce to challenge Ram

- This protocol uses extra messages for user authentication

In this particular case Sita sends her identity to Ram ram sends the challenge by sending our r which is there that random number to Sita Sita sends the encrypted version of rr to Ram

Ram now authenticate is now confident that the message is coming from Sita then Ram also sends one message Ram also sends one message here Sita also sends that another message random number R_S to challenge Ram and after receiving that R_S Ram responds with the encrypted version of R_S by using the symmetric key which is being shared by both of them then they can communicate under the cover of K_{SR}. So in this way two-way verification is done. However, this particular approach requires more number of communications of messages and this can be reduced as it is shown in this approach.

(Refer Slide Time: 27:10)



Indian Institute of Technology Kharagpur

User Authentication

➢Protocol using lesser number of messages

Sita

Ram

1 Sita, R_S

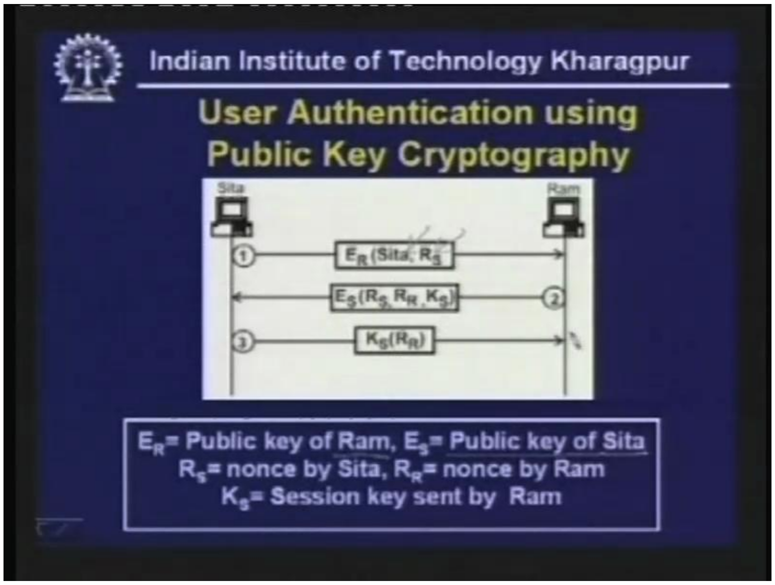
2 R_R, $K_{RS}(R_S)$

3 $K_{RS}(R_R)$

A shortened two-way authentication

Here instead of five messages only three messages can suffice that’s why it is a shortened two-way authentication approach. What is being done here is Sita not only sends her identity but also that random number in a single message to Ram. Ram in turn does the encryption of that random number and sends the encrypted version along with another random number generated by Ram nonce and that is being sent to Sita. Now Sita in turn does the encryption by using that shared key of R_R and sends it to Ram. In this way by sending three messages the two party authentication is being performed. This is how user authentication can be done by using, the symmetric key cryptography, the user authentication can also be done by using public key cryptography in this manner as it is explained here.

(Refer Slide Time: 28:35)



Indian Institute of Technology Kharagpur

User Authentication using Public Key Cryptography

Sita

Ram

1 E_R(Sita, R_S)

$E_S(R_S, R_R, K_S)$ 2

3 $K_S(R_R)$

E_R= Public key of Ram, E_S= Public key of Sita
R_S= nonce by Sita, R_R= nonce by Ram
K_S= Session key sent by Ram

Here again Sita sends a message by sending her identity and the random number R_S and that is being encrypted by using the public key of Ram. Thus encryption is done by using the public key of Ram, it is known to Sita. Now, after receiving that Ram responds to the encrypted version of the $R_{S,}$ R_R and K_S.

Ks is the key generated for that session so a new session key is being generated and that is being sent in encrypted form by using K_S that is the public key of Sita which is known to Ram. So, after messaging that Sita knows that it has been done by Ram and Sita does the decryption by using her private key and gets back R_S, R_R and K_S then she sends R_R in an encrypted form by using the session key K_S to Ram. So in this way by using public key cryptography the user authentication can be done.

Now, as I mentioned in the last class particularly the symmetric key cryptography is not very efficient because of large number of keys to be generated.

(Refer Slide Time: 29:36)

Indian Institute of Technology Kharagpur

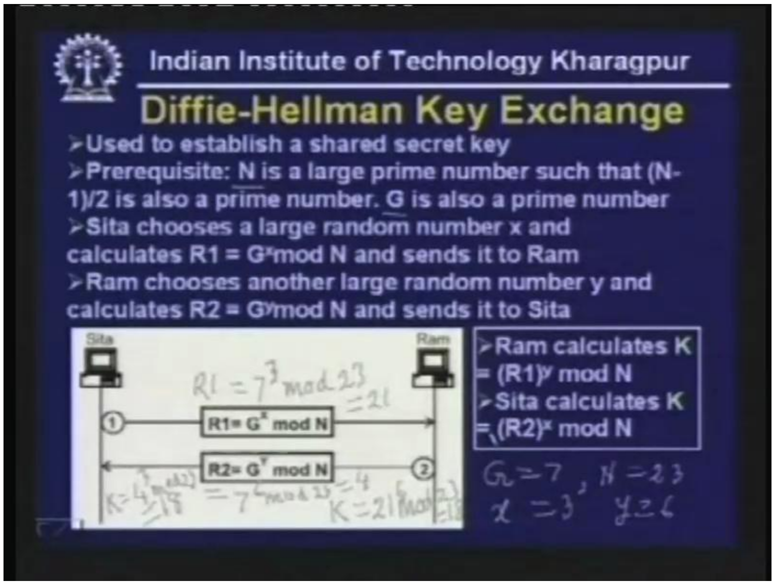
Key Management

One-time session key for two parties

1 million
500 billion

When the numbers of users is large, if there is 1 million people who are interested in communication then you will require 500 billion keys t that has to be generated, that is very difficult to do that’s why a simpler and efficient technique has to be used for the purpose of key management and that can be done by one-time session key for two parties. That means a key is generated only for a particular session is being used by both the parties for that session and again in the next session another new key is generated and that can be done by using a protocol known as Diffie-Hellman key exchange protocol.

(Refer Slide Time: 33:42)



Indian Institute of Technology Kharagpur

Diffie-Hellman Key Exchange

- Used to establish a shared secret key
- Prerequisite: N is a large prime number such that (N-1)/2 is also a prime number. G is also a prime number
- Sita chooses a large random number x and calculates R1 = G^xmod N and sends it to Ram
- Ram chooses another large random number y and calculates R2 = G^ymod N and sends it to Sita

- Ram calculates K = $(R1)^y$ mod N
- Sita calculates K = $(R2)^x$ mod N

This is used to establish a shared secret key per session basis. The prerequisite is in the beginning both the parties should know two large numbers N and G so these two numbers have some properties. First of all N is a large prime number such that N minus 1 by 2 is also a prime number and G is also a prime number. As an example for simplicity let’s assume G is equal to 7 and N is equal to 23.

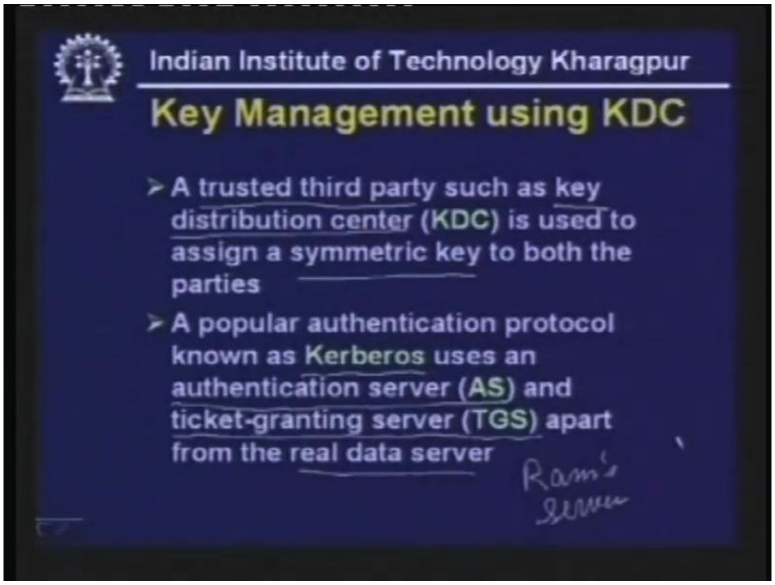
In practice the numbers are much larger. To explain the approach I have taken smaller numbers. After N and G are known to both the parties Sita chooses a large random number x to calculate R1 and R1 is equal to g to the power x mod N. Let’s assume x is equal to 3. So he creates R1 is equal to g to the power x mod N that means R1 is equal to 7 to the power 3 mod N where N is equal to 23 and that is equal to 21 so this 21 is sent to Ram. Now, after receiving this number Ram generates the key by using this 21 to the power 6, 6 is here (Refer Slide Time: 31:51) y is equal to 6 and that number has been used by Ram 2 to the power 6 mod 23 is equal to 18 so 18 is the key. This is how the key is generated at Ram’s end which can be used as a shared key. That means 18 can be used as a shared key. Now let’s see what Ram does.

Ram calculates R2 is equal to g to the power y mod n, so what is g to the power y mod n? As you already know g is equal to 7 to the power 6 which is the value of y and mod 23 is equal to 4, 4 is being sent by Ram to Sita and after receiving 4 what Sita does is she generates the key, key is equal to 4 to the power 3 that means g to the power y and mod g to the power y I means g to the power x and Sita has g to the power x that is (R2) to the power x mod N so mod 23 and again it gets 18.

Therefore both the parties have got the shared secret key. This is essentially working based on number theory. So I have illustrated with small numbers but when large numbers are used it is quite safe, it serves the purpose of generating a shared key per session basis. So this is how key management can be done.

Apart from this approach there are other approaches. Another important approach is based on what is known as key distribution centre (KDC). So key distribution centre is essentially a trusted third party which maintains a database of the keys and the key distribution centre maintains the keys and delivers the keys to different parties so it assigns a symmetric key to both the parties that is the role of the trusted third party KDC.

(Refer Slide Time: 35:20)



Indian Institute of Technology Kharagpur

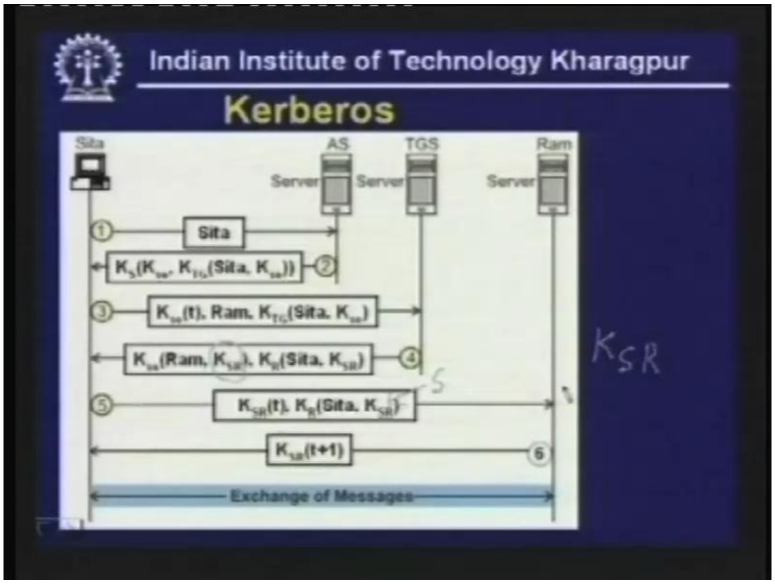
Key Management using KDC

- A trusted third party such as key distribution center (KDC) is used to assign a symmetric key to both the parties
- A popular authentication protocol known as Kerberos uses an authentication server (AS) and ticket-granting server (TGS) apart from the real data server

Ram's server

However, this approach is not full proved and a popular authentication protocol has been developed which is known as Kerberos which uses the concept of key distribution centre but in addition to key distribution centre it does more and it actually uses an authentication server (AS) and a ticket granting server (TGS) apart from the real data server. So it generates three servers where one of them is the authentication server, second one is ticket granting server and third one is real data server essentially this can be Ram's server and by using these three servers the authentication is being done. Let's see how it is being done with the help of this particular diagram.

(Refer Slide Time: 38:40)



Indian Institute of Technology Kharagpur

Kerberos

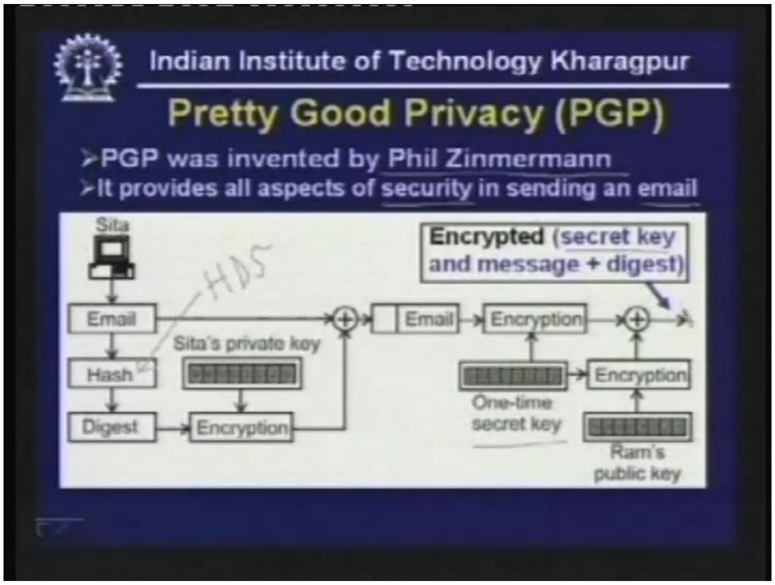
Sita
AS
TGS
Ram
Server
Server
Server
1 Sita
2 $K_S(K_{SA}, K_{TG}(\text{Sita}, K_{SA}))$
3 $K_{SA}(t)$, Ram, $K_{TG}(\text{Sita}, K_{SA})$
4 $K_{SA}(\text{Ram}, K_{SR})$, $K_R(\text{Sita}, K_{SR})$
5 $K_{SR}(t)$, $K_R(\text{Sita}, K_{SR})$
6 $K_{SR}(t+1)$
S
Exchange of Messages
K_{SR}

Here as you can see Sita is sending a message and before the messages are sent a six-way protocol is being performed. Sita sends her name to the authentication server (AS) and after receiving the identity of Sita the authentication server generates a session key that is K_{SC} and a TGS token to be used by Sita. So, using that token I mean after receiving this Sita will simply type her password to get the session key and using that session key she will do the encryption of a timestamp and also inform the ticket granting server with whom she wants to communicate and that is Ram and also she will send the token in an encrypted form which is the shared key between Sita and the ticket granting server so that is KTG. So this is being sent to the ticket granting server and since it is being encrypted by using the shared key between the ticket granting server and Sita it will accept these requests and it will generate two tickets, TGS responds to her creating a session key for Sita to use with Ram so you can see session ks is Ram, K_{SR} is being generated and $K_{SR,}$ $K_{R,}$ Sita, S_R so these two tickets are being generated where K_{SR} is the session key to be used by Sita for the communication with Ram.

These are being sent to Sita and after receiving this Sita sends a message to Ram along with the session key. This is the session key to some ticket (Refer Slide Time: 37:46) encrypted by using session key and also the timestamp. After receiving this Ram will do the encryption by using K_{SR} that is the shared session key to be used by both of them for communication by incrementing the time stamp by one. And after this is performed then both Sita and Ram not only have authenticated their identity but also they have got a shared key to be used by both of them which is this K_{SR}. Thus, under the cover of this K_{SR} this shared symmetric key both of them will exchange messages. This is how Kerberos works and this is very popular nowadays.

Now the security measures can be implemented by using the cryptographic technique at different layers particularly in network layer, transport layer and application layer. Implementing in network layer and transport layer is very difficult because there are many protocols, for each of them you have to develop a suitable protocol for the purpose of security. So it has been found that the protocol for the application layer is most efficient and simple and that is the reason why I shall consider an application layer protocol which has been used for sending emails in secured form.

(Refer Slide Time: 40:45)



Indian Institute of Technology Kharagpur

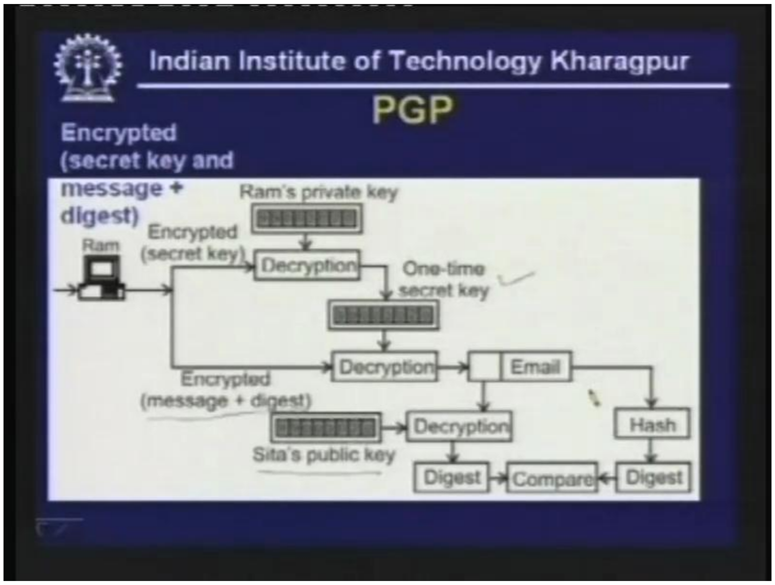
Pretty Good Privacy (PGP)

- PGP was invented by Phil Zinmermann
- It provides all aspects of security in sending an email

It was invented by Phil Zinmermann and it provides all aspects of security that is all the four aspects in sending an email message. I will mention these. Let’s see how it works.

Sita is sending an email. first the hashing is done by using a popular approach may be the HD5 approach and after hashing digest is created, the digest is encrypted by using Sita’s private key and that digest in encrypted form is sent along with this email and again the entire thing is encrypted by using one time secret key that is generated and not only it is encrypted but this one time secret key is also encrypted by using Ram’s public key and all the three are now sent that means the secret key in encrypted form then message and digest in encrypted form. All the three are being sent to Ram at the other end. After receiving the encrypted secret key and message plus digest the decryption is done in this manner.

(Refer Slide Time: 42:28)



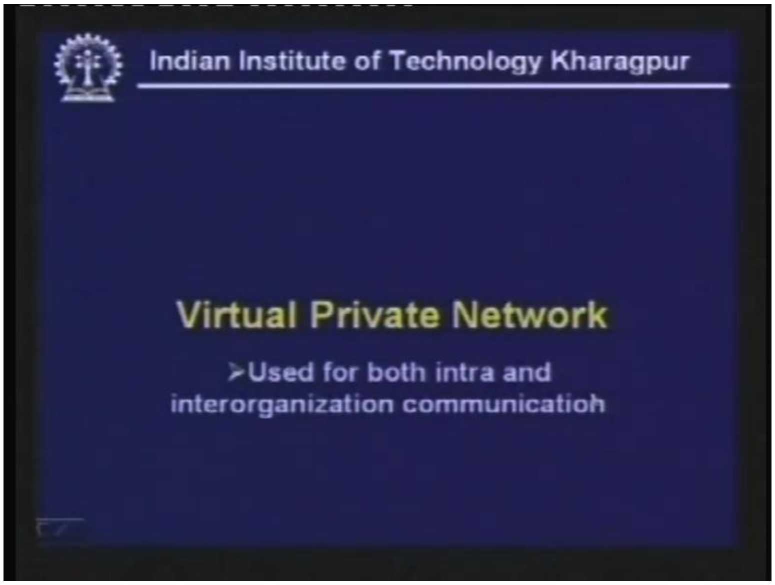
Indian Institute of Technology Kharagpur

PGP

Ram performs decryption. As you can see here the secret key is decrypted by using Ram’s private key because it was encrypted by using Ram’s public key. Since it was encrypted by using ram’s private key it is decrypted by using ram’s private key so the one time secret key is now generated and this message plus digest which was encrypted by using one time secret key which is your symmetric key is being used now for decryption to get back the message digest along with the email. now the message digest was in encrypted form by using Sita’s private key but now it is decrypted by Sita’s public key to get back the digest and email is also passed through a hashing function and digest is created and both the digest are compared to check whether they are same or not and if they are the same then it means that all the three functions are satisfied. That means privacy, authentication, integrity and nonrepudiation are satisfied. That means message is being communicated in secured form, however, if it does not match then there is some problem such as the email message has been modified or corrupted.

Now we shall discuss an approach by which a secured communication network or secured link can be created which is known as virtual private network and that is very popular. Without this our discussion on secured communication cannot be completed.

(Refer Slide Time: 42:36)



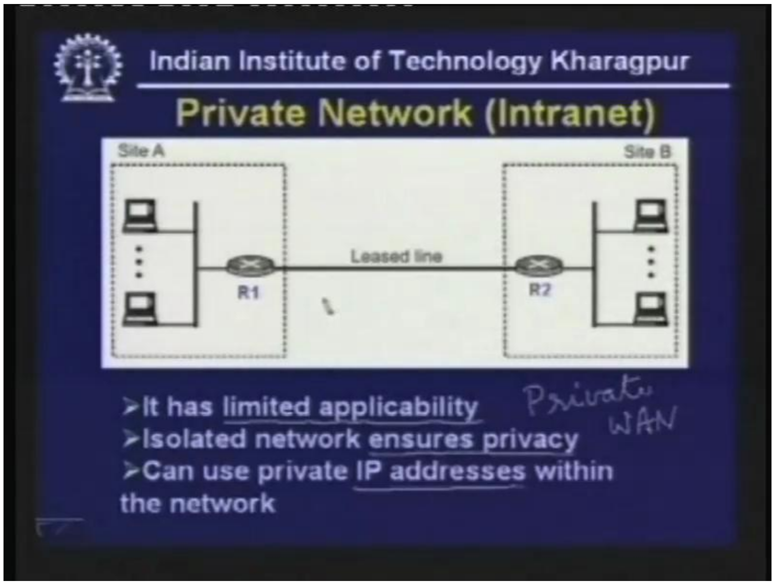
Indian Institute of Technology Kharagpur

Virtual Private Network

- Used for both intra and interorganization communicatioh

One possible approach for realizing private network in communication of interorganization communication messages is to connect various sides by using lease line.

(Refer Slide Time: 44:58)



Indian Institute of Technology Kharagpur

Private Network (Intranet)

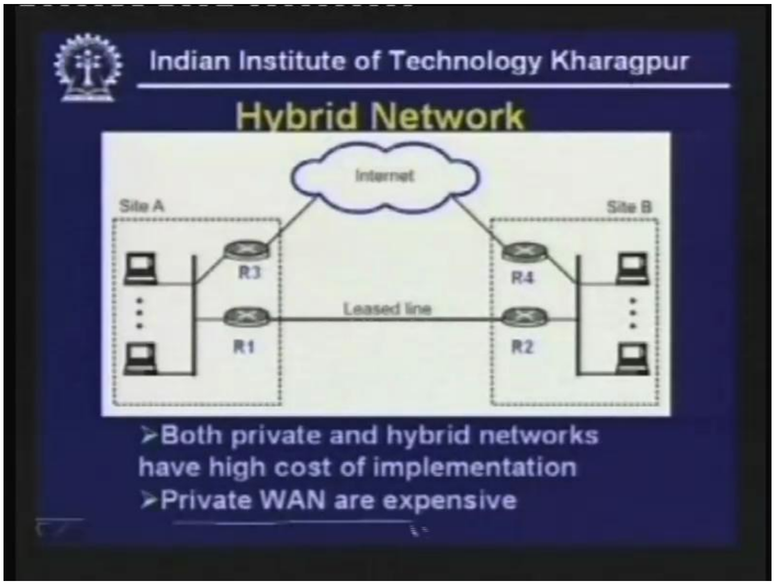
- It has limited applicability
- Isolated network ensures privacy
- Can use private IP addresses within the network

Private WAN

If the organization is located in a single building or in a single campus then there is no problem. A LAN local area network can be created and they can be communicated with each other. But in practice that is not so. Particularly organizations like National Insurance Company, banks such as State Bank of India and other organizations have their offices throughout the country, they may have thousands of offices and in each place they have got a local area network. Now they are connected with the help of lease line for communication of their private messages so only two sites are shown site A and site B but in practice there can be thousands of sites. In this case the intraorganization messages can be communicated through this private wide area network created with the help of these lease lines. This particular approach is simple but it also ensures privacy.

The advantage is here one can use private IP addresses because the IP address used in router R1 and R2 need not be a global IP so there is no need to take permission from the global organization so the organization itself can create their own IPs and use it under this approach. But it has limited applicability because these organizations as I mentioned banks, insurance companies etc have to serve many people and to do that there must be some global communication where they have to communicate through internet. So the second approach can be used by using hybrid network.

(Refer Slide Time: 46:19)



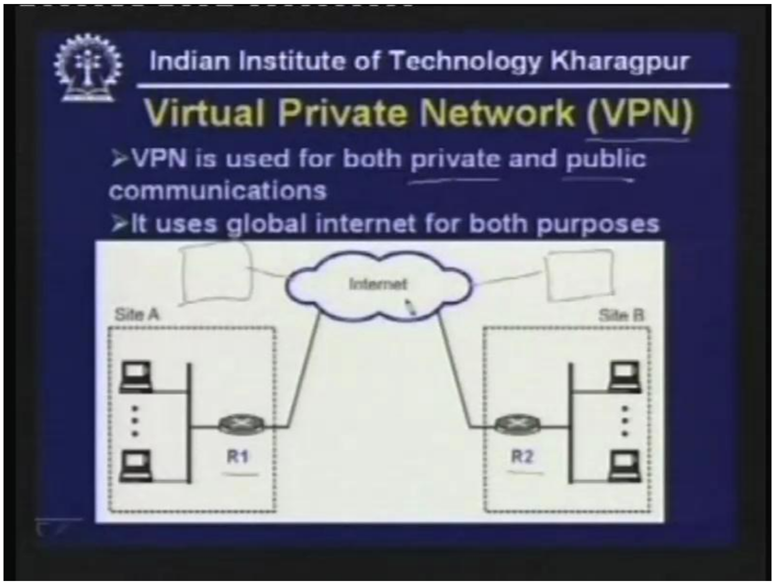
Indian Institute of Technology Kharagpur

Hybrid Network

- Both private and hybrid networks have high cost of implementation
- Private WAN are expensive

In this case what is being done is the intra organization communications are communicated with the help of lease line using the router R1 and R2. On the other hand, the global internet communications are being performed through the internet by using another set of routers R3 and R4 so separate path is there for communication of the global messages. This is hybrid because both private network and public network are being used as shown here (Refer Slide Time: 45:58). But the main problem in this case and as well as the previous case is where private wide area network is created by using lease lines, satellite links and various other communication things which is very costly so these networks are very costly, the private wide area networks are very expensive. To overcome that a technique known as virtual private network can be used.

(Refer Slide Time: 47:24)



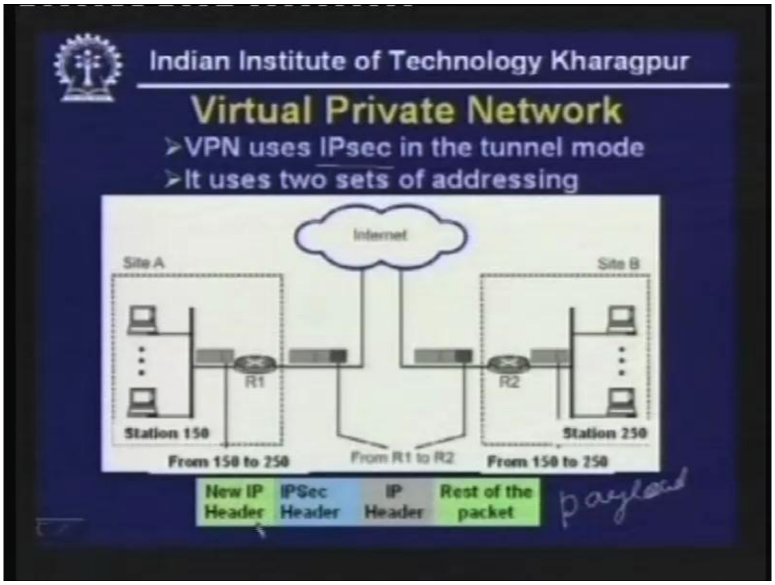
Indian Institute of Technology Kharagpur

Virtual Private Network (VPN)

- VPN is used for both private and public communications
- It uses global internet for both purposes

Virtual private network is used for both private and public communication. Not only private message or data but public communications is also performed by using the internet so a global internet is used for both private and public communications. You may be asking how you are achieving security in this particular case. In this particular case you are using a pair router R1 and R2 between two sides and in fact all these sides are now connected to this global internet so another site is also connected to this internet, then another site is also connected to this internet (Refer Slide Time: 47:10) so there is no need to deploy a public wide area network because this internet is now available throughout the world so each organization has to link it to the internet. However, question arises how security can be achieved. That can be done by using the concept of virtual private network or VPN.

(Refer Slide Time: 48:50)



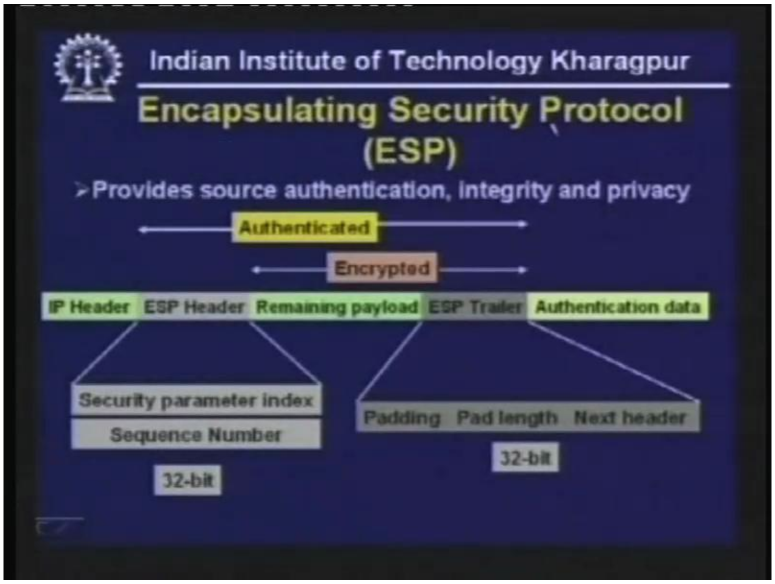
Indian Institute of Technology Kharagpur

Virtual Private Network

- VPN uses IPsec in the tunnel mode
- It uses two sets of addressing

VPN uses IPsec which is a protocol in the network layer known as internet protocol security in the tunnel mode. It uses two sets of addressing. As you can see here this is site one and this is site two, they are connected by using routers so apart from the IP header and the packet that is being used by this station 150 to send the message to station 250 when it is being sent by R1 it adds two more headers first one is IPsec header and in front of that a new IP header is being used for communication between R1 and R2 through the internet and this part is now used as some kind of a payload. So this IP address is not being used but it is sent as payload using these four components or four fields of this message. Here it is given in more detail. Particularly there are two protocols.

(Refer Slide Time: 51:15)



Indian Institute of Technology Kharagpur

Encapsulating Security Protocol (ESP)

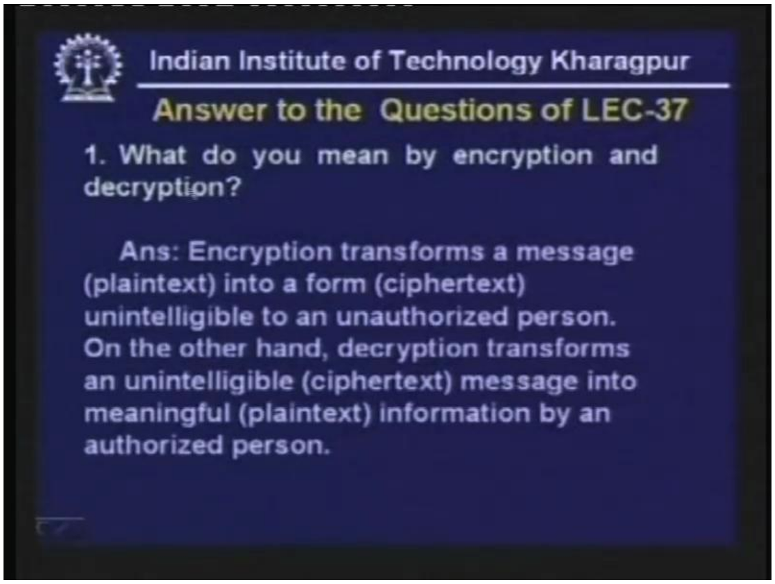
➢ Provides source authentication, integrity and privacy

The second one is known as encapsulating security protocol or ESP. ESP provides you source authentication, integrity and privacy. This is very useful because it provides all the three functionalities or services required and here is the frame format. Here you can see it adds a ESP header and a ESP trailer, this is the remaining payload, this part (Refer Slide Time: 49:44) IP header and the rest of the packet is now being sent as payload and a new IP header is being generated which is being used and this ESP header has got two important components security parameter index and sequence number and ESP trailer has got padding, provides pad length and next header. By using this, a connection oriented service is created.

Here you have the authentication data that means some kind of digest is created which is being sent along with the packet and this is communicated through the internet. So you can see here the packet is in the tunnel mode, the message along with the original IP address is sent as payload and additional fields are used to achieve this authentication, integrity and privacy by using the virtual private network.

It is virtual because you were not really creating a private network but you are achieving the benefits of private network that’s why it is virtual private network. That means by using public network you are creating a virtual private network for secured communication. Now it is time to give you the answer to the questions of lecture 37.

(Refer Slide Time: 51:25)



Indian Institute of Technology Kharagpur

Answer to the Questions of LEC-37

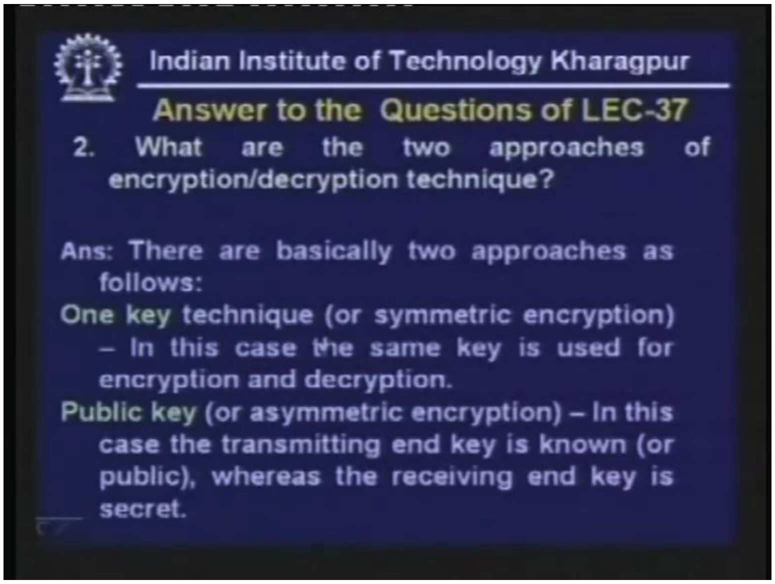
1. What do you mean by encryption and decryption?

Ans: Encryption transforms a message (plaintext) into a form (ciphertext) unintelligible to an unauthorized person. On the other hand, decryption transforms an unintelligible (ciphertext) message into meaningful (plaintext) information by an authorized person.

1) What you mean by encryption and decryption?

As we have already discussed on many occasions, encryption transforms the message that is plain text into a form called cipher text which is unintelligible to an unauthorized person but the authorized person can get back the plain text by doing decryption. So, on the other hand, decryption transforms an unintelligible message into meaningful information by an authorized person by doing the decryption.

(Refer Slide Time: 52:05)



Indian Institute of Technology Kharagpur

Answer to the Questions of LEC-37

2. What are the two approaches of encryption/decryption technique?

Ans: There are basically two approaches as follows:

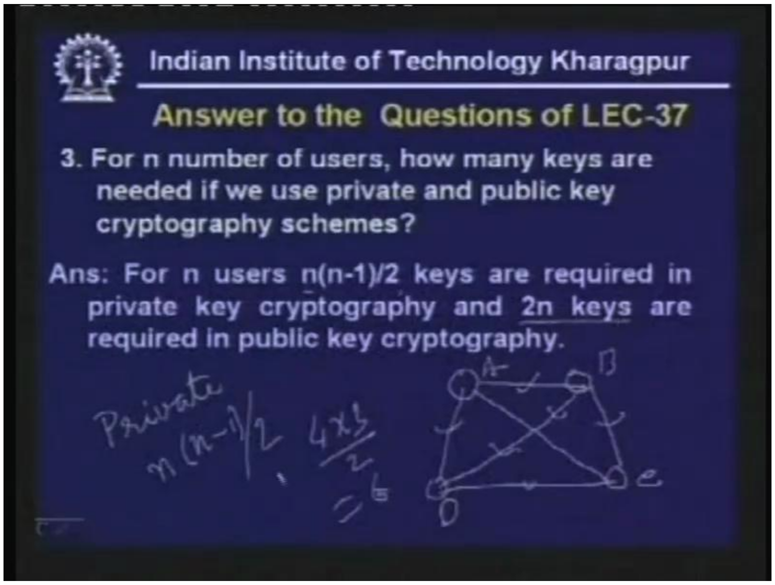
One key technique (or symmetric encryption) – In this case the same key is used for encryption and decryption.

Public key (or asymmetric encryption) – In this case the transmitting end key is known (or public), whereas the receiving end key is secret.

2) What are the two approaches of encryption and decryption technique?

There are basically two approaches as follows. First one is known as one key technique which is also known as symmetric key encryption technique. In this case the same key is being used for encryption as well as decryption and the second approach is known as public key approach which is also known as asymmetric key encryption. In this case the transmitting end key is known as the public key whereas the receiving end key is known as secret key or private key. So we have made use of these two approaches in these lectures as you have seen.

(Refer Slide Time: 54:22)



Indian Institute of Technology Kharagpur

Answer to the Questions of LEC-37

3. For n number of users, how many keys are needed if we use private and public key cryptography schemes?

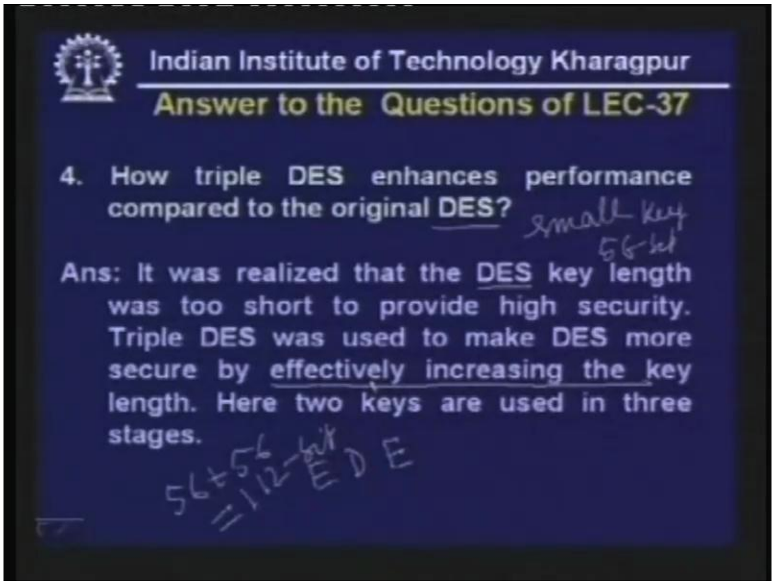
Ans: For n users n(n-1)/2 keys are required in private key cryptography and 2n keys are required in public key cryptography.

3) For n number of users, how many keys are needed if we use private and public key cryptography schemes?

As we have seen for private key cryptography or symmetric key cryptography we require n (n minus 1) by 2 keys. For example, suppose there are four nodes then node 1 will require at least three keys that means three keys are required for communication by node A, then D will require for communication with B C and D, B will require additional two keys for communication and D will require another node. So in this way the number of edges are essentially the number of keys required. So in case of 4 it is 4 by 3 into 2 that is 6 edges. As you can see there are six edges so in this way total number of keys is quite large n (n minus 1) by 2.

On the other hand, in case of public key cryptography or asymmetric key you require only 2n keys. The reason is each user will require one private key and another key for the rest of the world, for all the other users so in this way the total number of keys required is 2n.

(Refer Slide Time: 55:47)



Indian Institute of Technology Kharagpur

Answer to the Questions of LEC-37

4. How triple DES enhances performance compared to the original DES? small key 56-bit

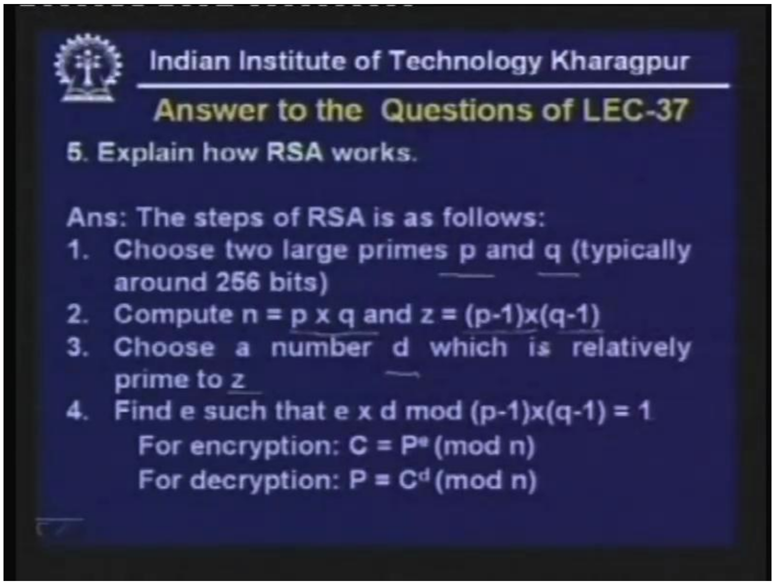
Ans: It was realized that the DES key length was too short to provide high security. Triple DES was used to make DES more secure by effectively increasing the key length. Here two keys are used in three stages.

56+56 =112-bit E D E

4) How triple DES enhances performance compared to the original DES?

One common complaint given is this DES uses a very small. We have seen the key size was 56-bit and obviously with 56-bit key it is not possible to achieve very good security. So we have to see how to improve the security without discarding the DES. That means triple DES was used to make DES more secure. This effectively increases the key length. what is being done is two keys are used to do encryption followed by decryption followed by encryption and by doing that the size of the effectively is 56 plus 56 that is 112 bit and 112 bit is considered to be quite reasonable, secrecy or security. That’s why this triple DES was invented and it is quite popular nowadays.

(Refer Slide Time: 56:35)



Indian Institute of Technology Kharagpur

Answer to the Questions of LEC-37

5. Explain how RSA works.

Ans: The steps of RSA is as follows:

1. Choose two large primes p and q (typically around 256 bits)
2. Compute n = p x q and z = (p-1)x(q-1)
3. Choose a number d which is relatively prime to z
4. Find e such that e x d mod (p-1)x(q-1) = 1

For encryption: C = P^e (mod n)

For decryption: P = C^d (mod n)

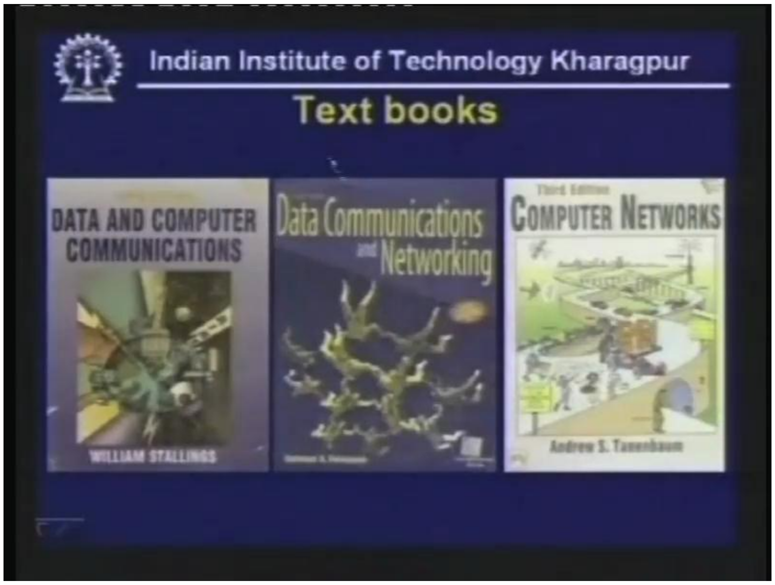
5) Explain how RSA works?

The steps for RSA is as follows:

It chooses two large prime numbers p and q typically around 256 bits.
It computes n is equal to p into q and z is equal to (p minus 1) into (q minus 1)
It chooses a number d which is relatively prime to z that is p minus 1 and q minus 1 and it then finds e and e such that e into d mod p minus 1 into q minus 1 is equal to 1 then for encryption it is p to the power d mod n is used and for decryption to get back the plain text c to the power d mod n is used.

This is how RSA works as I have explained in the last lecture. Now it is time to give you references to the various books that I have used in this lecture.

(Refer Slide Time: 56:43)



Indian Institute of Technology Kharagpur

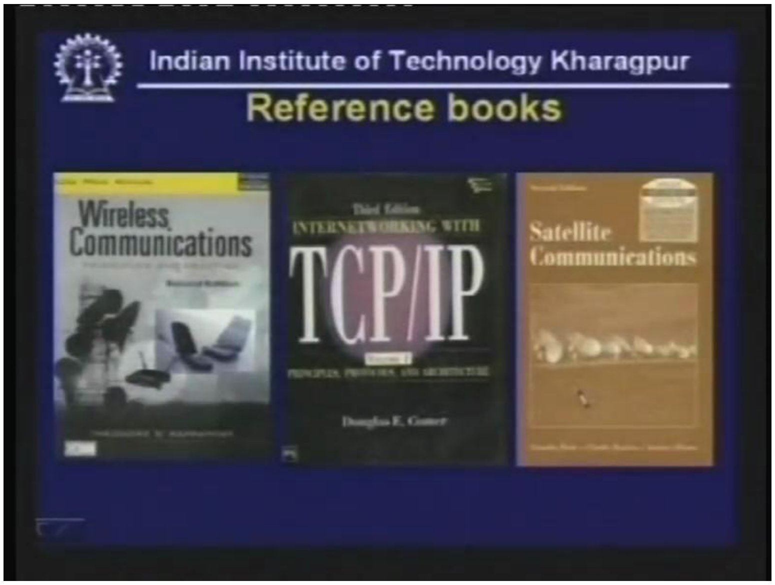
Text books

DATA AND COMPUTER COMMUNICATIONS
WILLIAM STALLINGS
Data Communications and Networking
Third Edition
COMPUTER NETWORKS
Andrew S. Tanenbaum

So far as textbooks are concerned the main textbook that I have used is Data Communications and Networking by Behrouz A Forouzan and apart from these I have used two more books. on the left side is the book by William Stallings, the name of the book is data and computer communications published by Prentice Hall of India, the third book is Computer Networks by Andrew S Tanenbaum again it is published by Prentice hall of India.

Apart from these textbooks I have used several reference books. For example, for TCP when we shall discuss internetworking this book is very useful, TCPIP by Douglas E Comer

(Refer Slide Time: 57:21)

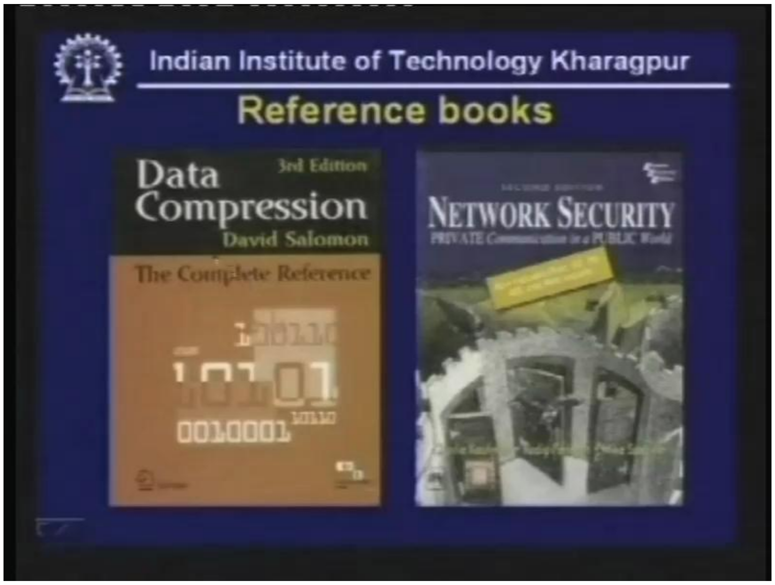


Indian Institute of Technology Kharagpur

Reference books

Then for Wireless Communication there were some lectures. I have used this Wireless Communication Principles and Practices by Theodore S Rappaport and this is actually published by Pearson then you have got a book on Satellite Communication which is published by Wiley and two more reference books that has been used when I discussed Data Compression, this book is by David Solomon and on Network Security the book is by Charlie Kaufman and two more authors.

(Refer Slide Time: 57:56)



Indian Institute of Technology Kharagpur

Reference books

Hence, these are the reference books I have used during my lectures. So with this we have come to the end of not only today's lecture but to the end of forty hour lecture series on data communication.