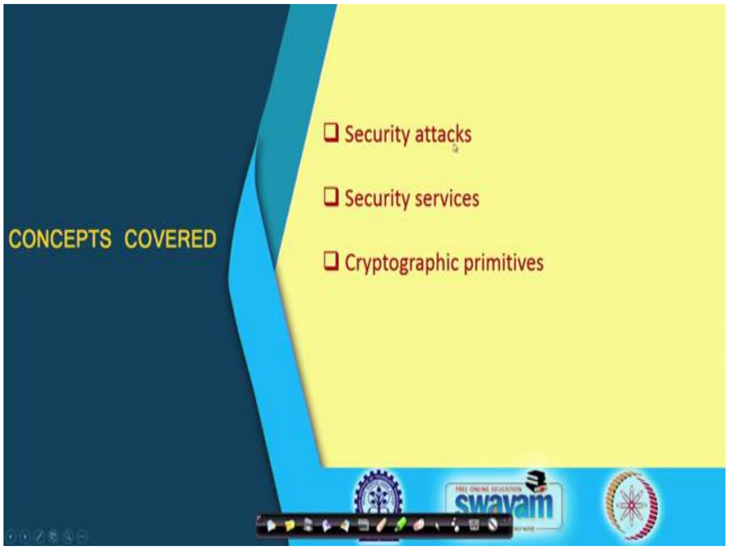
Ethical Hacking
Prof. Indranil Sengupta
Department of Computer Science and Engineering
Indian Institute of Technology, Kharagpur

Lecture - 26
Basic Concepts of Cryptography

Now, when we talk about hacking, breaking into a system, attacking a network what we actually are talking about; we are talking about identifying some vulnerability or weakness in an existing system and try to break into the system or the network or the environment or the organizational infrastructure whatever through that weakest link, weakest point. Now, there are many ways and techniques that are used to try and strengthen the infrastructure so, that the chance of such attacks are minimized.

I would never say that it will be 0, the chance is minimized or reduced. Well, cryptography is one of the most important and useful tools that are used to try and prevent these kind of attacks in a system or in a network. In this lecture here I shall be trying to tell you some Basic Concepts of Cryptography which will help you in understanding and appreciating how many of the network based attacks take place and how you can prevent them, just using some techniques.

(Refer Slide Time: 01:36)



CONCEPTS COVERED

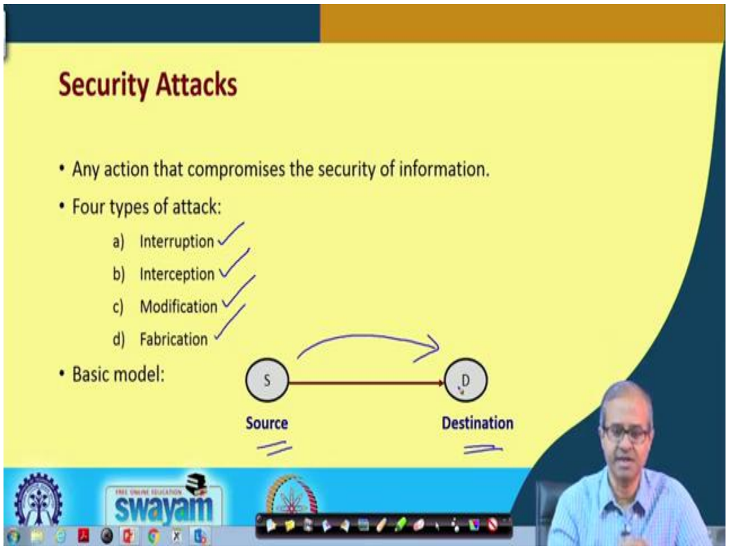
❑ Security attacks

❑ Security services

❑ Cryptographic primitives

So, in this lecture we shall broadly be talking about some of the generic security attacks, some of the security services that are typically provided and some of the cryptographic primitives which are used to provide such security services.

(Refer Slide Time: 01:56)



Security Attacks

- Any action that compromises the security of information.
- Four types of attack:
  - a) Interruption ✓
  - b) Interception ✓
  - c) Modification ✓
  - d) Fabrication ✓
- Basic model:

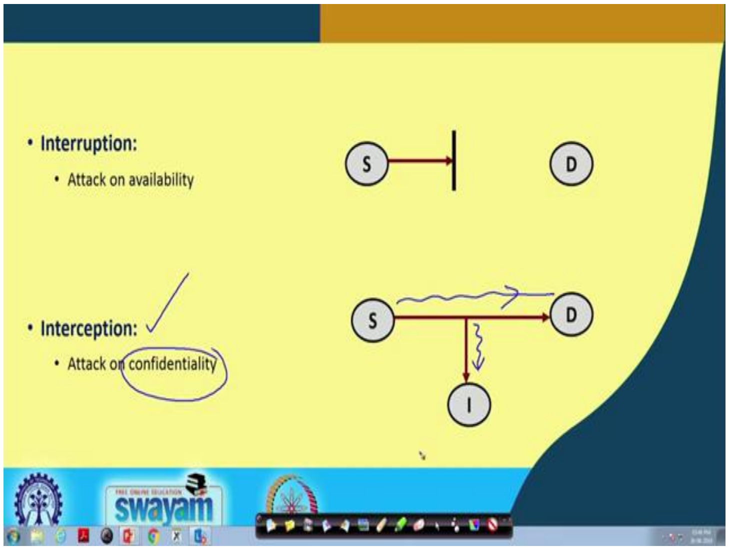
Let us start by a very brief discussion on the security attacks. Now, when we say security attack, we are saying that we have some kind of an infrastructure; I do not know what, that is, it can be anything and there is someone from the outside world who is trying to compromise the security or trying to break into my infrastructure. So, security attack can be, could say anything, it can be of various types. You can say, it can be any action that compromises the security of information.

I am not saying a network or a computer, I am saying information. Ultimately a computer stores an information through a network, some information flows. So, by virtue of some malicious operation which an intruder carries out on such a system or an environment, somehow this information content or information flow might get affected. So, these are something which we refer to as security attacks.

Broadly speaking four kind of attacks you can identify or you can talk about: interruption, interception, modification and fabrication. So, let us try to understand these four things one by one. Our generic model is like this we are assuming that we have something like networking infrastructure, where there is a source, there is a destination. Source is trying to send some message to a destination.

This is the thing which is being done and on this some kinds of attacks are being carried out. Let us see with respect to these four, alright.

(Refer Slide Time: 04:01)



- Interruption:
  - Attack on availability
- Interception:
  - Attack on confidentiality

First let us talk about interruption, interruption conceptually is very simple. This source was sending some data to a destination. Somehow the intruder makes sure that this message never reaches the destination. Well, you may ask how this can be done; now, you think of a typical network, there will be several routers through which the message packets are normally flowing through. You may assume that there are multiple routers on the way, the message that source was sending was flowing through a number of routers and finally, it was reaching a destination. Now, imagine an intruder has hacked a router.

Well, what is a router; router is nothing very sacrosanct, a black box, it cannot be hacked nothing like that. Router is also like a normal computer, it is also a computer, there is a processor, there is memory, there are some IO facilities, input output facilities and it also runs an operating system like Linux or something. So, it is ultimately it is a computer. Now a computer can be hacked as you know.

So, a router if you treat it as a computer there is no reason why it cannot be hacked. There is also some usernames and passwords, would through which some people or administrator can login into a router, can change some configurations and do a number of things.

And, the network ports and connections those are the input/outputs for the router, ok. Now, suppose one of the routers is getting hacked and all packets which are coming into the router, they are either routed to a different direction or all packets are getting discarded.

So, these packets will never reach the destination, this is something called a denial of service attack. You see someone is trying to contact a server, the server is providing a service, but if you somehow can stop that communication from happening; that means, you are not getting a service, it is denial of service ok.

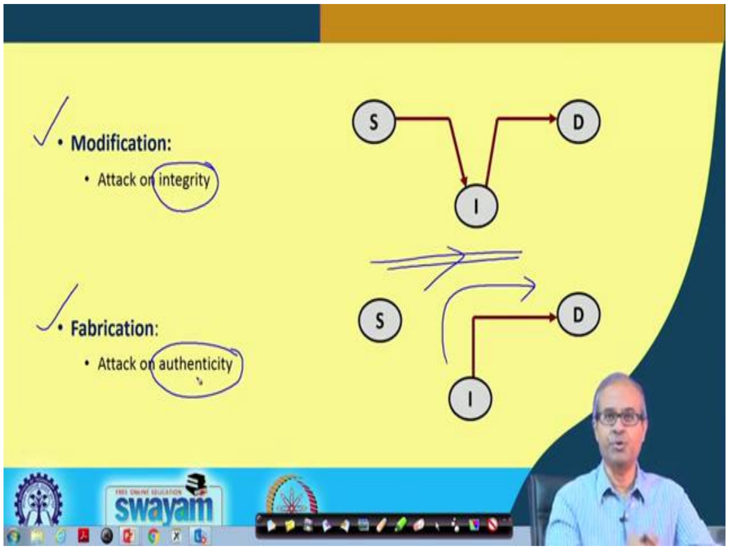
So, interruption is an attack which is attack on availability. So, so that you cannot contact the other side; the server, this server may be providing you with some facility. It can be a web server. It can be a mail server. You are not being able to access it. So, it is an interruption on availability of some service ok.

The second one is interception. Well, interception means that source is sending some data to a destination fine. There is a intruder in the middle, is silently listening to what is going on. So, whatever I am sending to you some messages, some intruder is also reading those messages right.

Now, how it is happening; is it that someone is measuring what signals are going through a cable or an optical fiber. Well, I am not saying that it is not possible, but it is extremely difficult, most common way of interception is again by hacking a router. You hack a router, whatever packet comes, a copy of that packet you forward to some other place that will be the machine of the intruder.

So, intruder can read all the packets, everything will be coming as a copy to the intruder or so. So, interception is an attack on confidentiality; meaning I may be sending you some confidential information like my bank account number or something, but someone in the middle can read the information and can get hold of that confidential information well.

(Refer Slide Time: 08:15)



- Modification:
  - Attack on integrity
- Fabrication:
  - Attack on authenticity

Now, things are getting more complicated. The third one is modification; well you again think of that model that some router in between has been hacked, but now what the intruder has done? Intruder is more intelligent. Intruder is not simply reading out the packets, but whatever packet is coming, the intruder is making some modifications in the packet and then forwarding it.

So, the destination will be receiving the packet alright, but it is not the original packet with some changes or modifications. These are very dangerous, there maybe some critical messages which may be flowing between points; means you think of a scenario during a war.

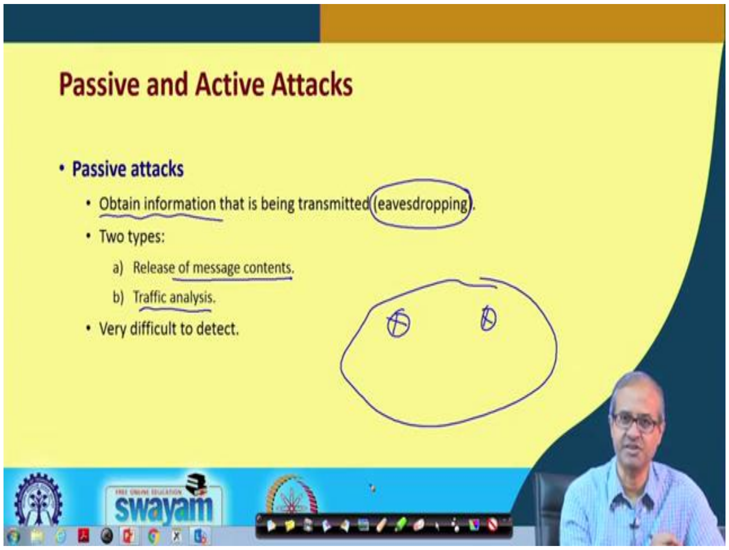
There are some advanced posts to who are exchanging messages which are very critical for taking some strategic decisions. Now, if the enemy can hack into their machines or servers or routers and change the messages then it can be catastrophic right. Modification is something called attack on integrity. I am saying that I was sending you a message. Ihe integrity of the message is lost.

Someone has modified the message in transit that is called integrity of the message right and lastly comes fabrication; fabrication says the source did not send anything at all to the destination, but the intruder artificially fabricated a packet with the source address put as the source address of S and the packet was sent to the destination.

Destination will feel that the packet is actually coming from S, but which is not; the packet was coming from the intruder and this is something called attack on authenticity. You see authentication again becomes a very important issue here, authentication means the destination must be sure of the actual sender of the message or the packet. Who is actually sending, is it S or someone else I is sending it by fabricating a packet ok.

So, these are broadly the security attacks which are very important in a very general context.

(Refer Slide Time: 10:48)



Passive and Active Attacks

- Passive attacks
  - Obtain information that is being transmitted (eavesdropping).
  - Two types:
    - a) Release of message contents.
    - b) Traffic analysis.
  - Very difficult to detect.

Now, there is another way you can classify attacks: passive and active; passive means it does not change anything. Nothing is modified in the network or in the information that is flowing. Passive attacks are those attacks where the intruder is simply obtaining some information. It is reading some information which is flowing in the network. This is sometimes called eavesdropping.

Someone is silently listening. This is the most difficult kind of attacks to detect, because you as a user, as a participant you will have no idea that something wrong is going on. But someone silently is listening everything whatever is flowing through your network, right. This is called passive attacks.

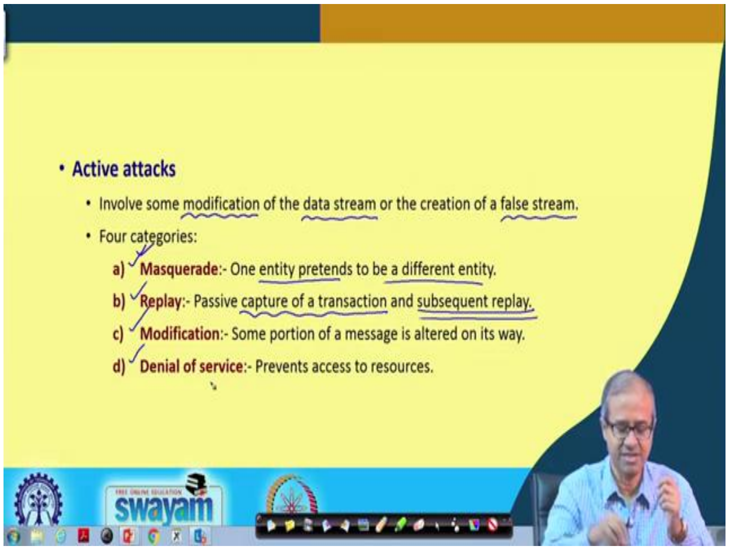
Now, broadly passive attacks again can be of two types: one is messages as I said, I am sending your message. Someone is reading that message. Well, I may say that well I do not care because my messages are anywhere not very confidential, let someone read it. I do not care. But, there are cases where messages may be confidential, may be important and someone reading the message may not be desirable, but something else can also happen, there can be some kind of traffic analysis going on.

Like the intruder is trying to attack a remote a network let us say, but intruder does not have much information about the network. It does not know which is the most important point where I should attack.

So, initially the intruder will try to listen to the packets that are flowing through the network and try to analyze the traffic that which are the computers, which are most heavily used.

So, it can identify one or two such very important or heavily used nodes in the network; they may be your web server, the mail server or something like that. Then the intruder can pointedly try to attack those servers so, that maximum harm can be done to that network. This is how traffic analysis can also be carried out to know some vulnerable points in the network; all right.

(Refer Slide Time: 13:26)



- Active attacks
  - Involve some modification of the data stream or the creation of a false stream.
  - Four categories:
    - a) **Masquerade**:- One entity pretends to be a different entity.
    - b) **Replay**:- Passive capture of a transaction and subsequent replay.
    - c) **Modification**:- Some portion of a message is altered on its way.
    - d) **Denial of service**:- Prevents access to resources.

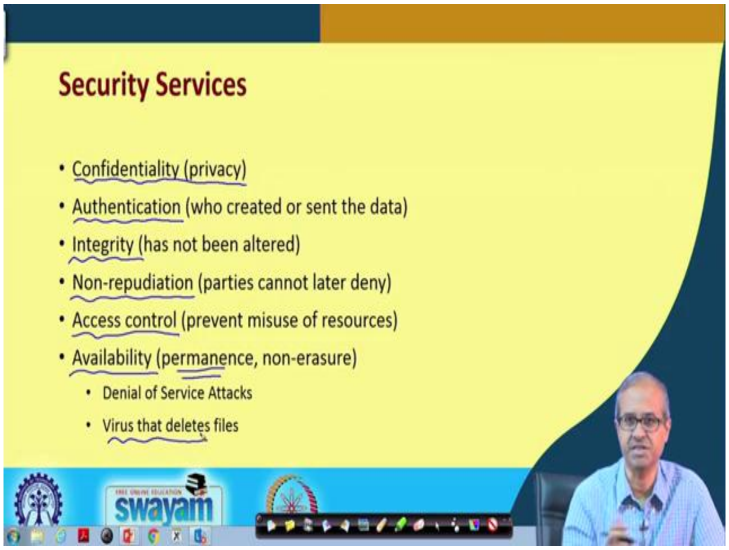
Now, talking about this active attacks, active attacks as it said are those where some kind of changes or modifications are taking place. They involve some kind of modification of the data that are flowing through the network or through fabrication you can also create a false stream of data which was not there. Some new or false data is injected into the network. Now, here again under active attacks you can classify as four types; one is some kind of authentication attack masquerade, means one entity pretends to be a different entity.

Like I am sending a message to you telling that well I am mister x, but I am not mister x that is masquerade; I am masquerading as mister x, ok. Replay; replay means I silently listen to network traffic and see that when someone is logging into a machine, some particular packets are being sent to a server which happens, which allows access. Now, now I silently listen to it, later on I replay those packets, I send those same packets from my machine. So, I would expect that I would also be granted access to that server. So, this is some kind of a replay attack which is called.

So, you are capturing some transactions silently and then try to carry out a subsequent replay of that same transaction, ok. Modification as I have already said, some part of the message you can modify. Now of course, simple modification will not work. You see how means you know that in the IP packet there is also a checksum field. If you modify the message, the checksum field also will have to be updated right.

So, you can do both so, that the receiver will not be able to identify that there is anything wrong ok; and lastly this is exactly not a modification, but by doing something you are preventing someone to access some facility or some service. This is denial of service attack. This is also very common.

(Refer Slide Time: 16:00)



Security Services

- Confidentiality (privacy)
- Authentication (who created or sent the data)
- Integrity (has not been altered)
- Non-repudiation (parties cannot later deny)
- Access control (prevent misuse of resources)
- Availability (permanence, non-erasure)
  - Denial of Service Attacks
  - Virus that deletes files

Now, based on these attacks we can identify some security services which are desirable, ok. It is not that all of the security services must be present in all organizations. In every place, it depends on the kind of place and kind of service you are providing; you may be requiring some of these services, ok.

So, these services some of them are fairly self explanatory. Confidentiality I have already talked about, there can be certain cases where privacy of information is important. Like when you are logging in into a bank, you are typing in your user ID and password, you are carrying out some online transactions. Their utmost confidentiality is important right.

Secondly, authentication so, when someone is registering or trying to do a login; there should be a mechanism that the, that the other side should be able to verify that I am the correct person, that I am the authorized person who is trying to carry out that transaction. Nowadays you know in banking transaction there are so many ways that had been tried out like OTP, One Time Passwords, then similar things multiple levels of a passwords authentication, ok.

These are all means of checking the authenticity of the person, that whether it is a correct person who is trying to carry out the transaction. Integrity means the messages should not be modified; suppose I am sending you some very important information and you should be sure that it is the original information and is not modified by someone else, ok.

Non-repudiation is a parameter which is very important more from the, I mean to say a legal point of view. Non-repudiation means something like this, let us say I had sent to a message, but tomorrow I say that well, I did not send to the message, maybe someone hacked and someone sent the message on my behalf.

This is something called non- repudiation, parties cannot deny later like your security system or the mechanism for sending and receiving messages should be such that such things are never possible; that if you receive a message from me, it will actually be coming only from myself. You can verify that.

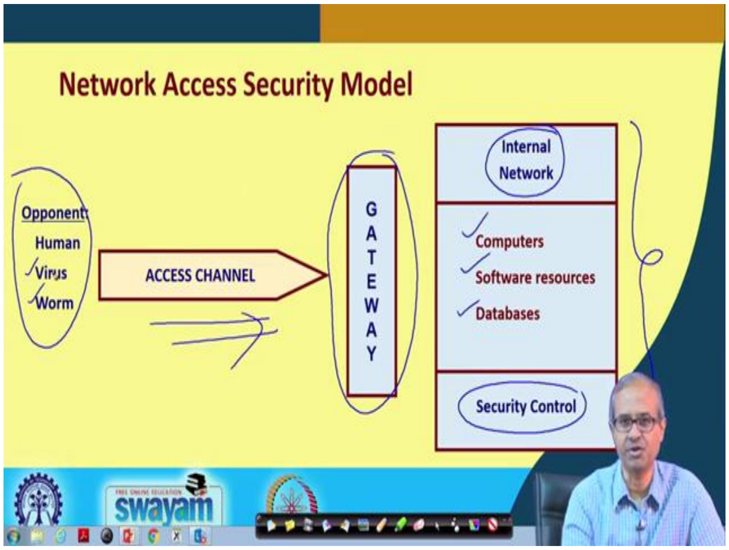
So, I cannot later on say that well that message was not sent by me, this is called non-repudiation, ok. Then access control of course, some services where multiple peoples access or use like cloud services. Let us say when you are accessing cloud, you will be given some right or some access.

So, how much computing resources, how much memory you are just allowed to use or access that kind of access control and availability of resources like we already talked about denial of service that is one kind of availability, like Gmail, we all use Gmail today.

So, well we assume that Gmail is something which is always available, but if we wake up in the morning and we suddenly find that Gmail is not accessible, many of us would be in great trouble, right.

These are something which are some features switch over which we demand some kind of permanence in them, they should not be erased or removed; they should always be there, always be made available. There are services one thing of course, virus also fall under that category, some viruses which can delete some files from your machine, from your computer ok. These are some of the security services which you can think of.

(Refer Slide Time: 20:32)



Network Access Security Model

Now, with respect to your network, this is a general network model or security model you can think of; you see this is some kind of an organizational network you can say. You will have some internal network, internal network will be having some security policies and inside the network there will be several computers.

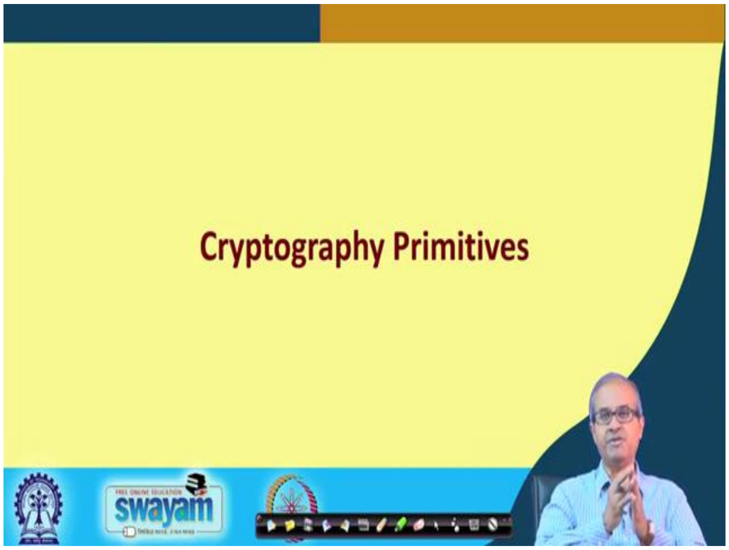
There will be databases, lots of data stored somewhere and there also be lot of software packages and other things available. So, this is your internal network and normally you secure your internal network by using some router, some firewalls and so on.

So, let us say I have some gateways here which is protecting my network from the outside world. There is some opponents which are trying to attack your network via internet, we are calling it the access channel. Now, these opponents can be manual mean human being, but nowadays these attacks have become very sophisticated, they are software generated.

So, some person need not sit on a computer and mount an attack. There will be some viruses or worms or automatic, some software that will be mounting these attacks in an automated way and it will be much faster and much more you can say, lethal in that case.

So, this is the general model of attacking an organizational network that we are talking about.

(Refer Slide Time: 22:17)

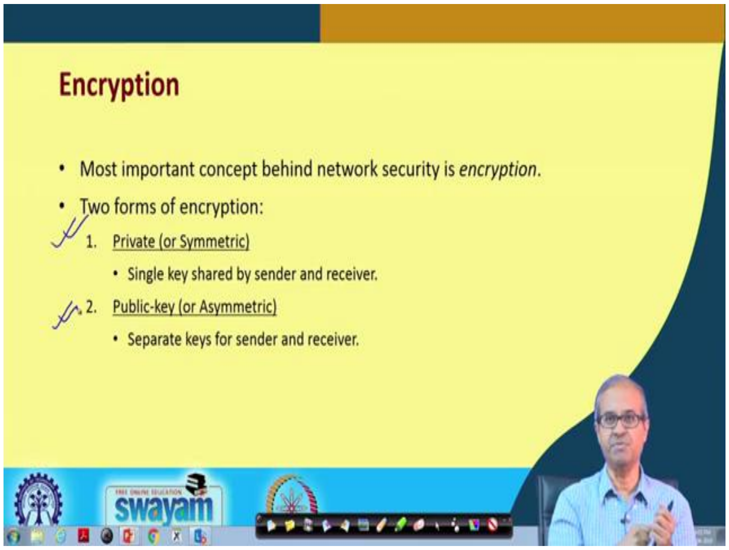


Cryptography Primitives

Now, we talked about the security attacks and security services. We need this, but the question is how do you achieve this; it is fine these are my wish lists, I need, I want that my messages should be secure, they should not tampered with, there will be no; there were no non-repudiation.

But who will ensure all these things? Well, the branch of cryptography gives us some basic tools and techniques with which we can build applications which can ensure most of these security services that you want. So, let us look at some of the most basic cryptographic primitives.

(Refer Slide Time: 23:05)



Encryption

- Most important concept behind network security is *encryption*.
- Two forms of encryption:
  1. Private (or Symmetric)
     - Single key shared by sender and receiver.
  2. Public-key (or Asymmetric)
     - Separate keys for sender and receiver.

The most basic form is something called encryption and decryption. Well, I want my message to be somehow garbled so that if someone captures will not be able to make any head or tail out of it. What it is? This is what is meant by encryption, but there is a catch.

So, I should not garble it in a way that no one can detect it at all; well, I will want that the person whom I am sending this message only that person should be able to decode it back, read it back that is decryption, ok.

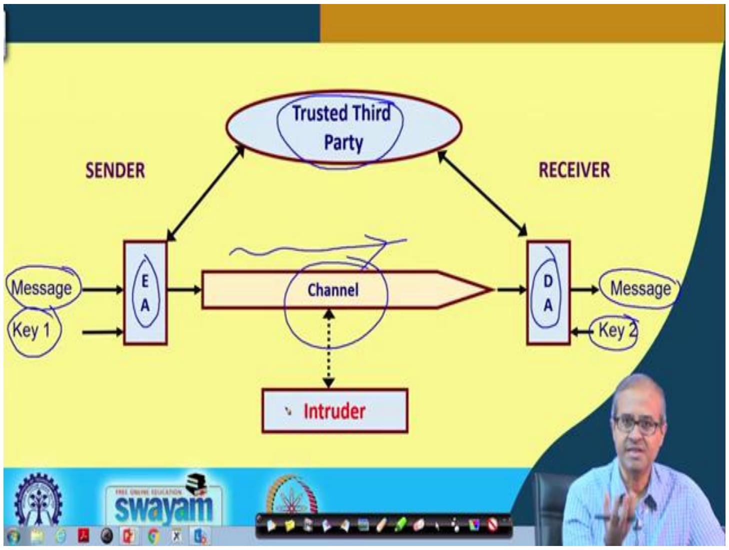
Now, this encryption and decryption are the most important you can say, cryptographic primitives or tools that provide many of these security services. Broadly, speaking there are two kinds of encryption/decryption schemes that are available, we will be talking about these methods. One is called private key, other is called public-key. Private key means whenever I am garbling my message, I am doing it using some secret information that I am calling it a key and I am sharing that secret information with you, the intended recipient, right.

So, when I am sharing this key with you, no one else knows about this key. So, I can encrypt my message using this key, you can decrypt the message using the same key; this is how it works. This is called private or symmetric key encryption, but public-key encryption is something different. Public-key means there will be two keys with me, with one key someone can encrypt a message and send it to me, with the other key I can decrypt.

So now, I can say that anyone can send messages to me that is public; one of the key is public. So, anyone can encrypt and send it to me, but whatever is coming to me, no one else can decode it, only I can decrypt using my, the other key, second key.

There are two keys I told you, one is a public, available to everybody, other is with me, that is private to me, ok. There is separate keys for sender and receiver.

(Refer Slide Time: 25:32)

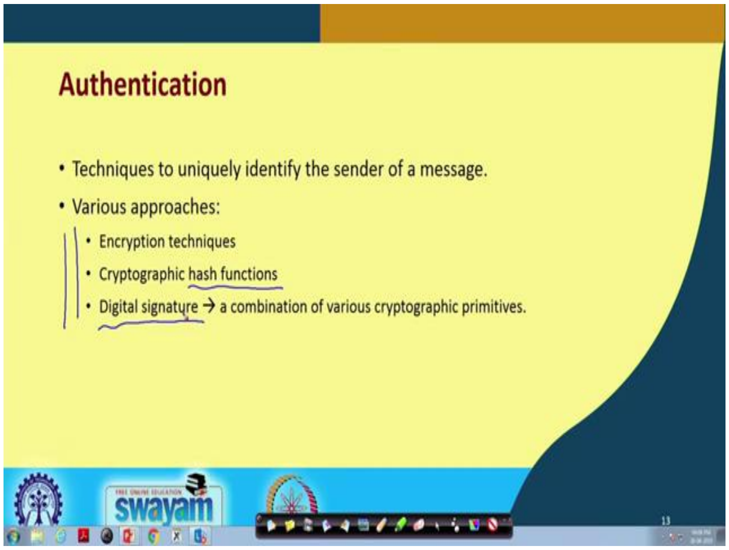


This is the general model of encryption/decryption, as I told you; there will be some encryption algorithm where the message will get encrypted using some secret key and on the other side there will be a decryption algorithm where this message which is coming in encrypted form will get decrypted back into the message using some key. These keys may be the same key, may be different, it will depend whether we are using symmetric key or public key.

And, in many algorithm we rely on a trusted third party, we rely on some other third party to provide us with some kind of help. We will see about these things later and the model of the intruder is that intruder can only tap information that is flowing through in this channel, in an encrypted form.

So, the intruder if he or she tap some information, the information that is obtained will be an encrypted form. So, to get back I mean, any meaningful information he will have to decode that information somehow, that is called cryptanalysis which is extremely difficult.

(Refer Slide Time: 27:01)



Authentication

- Techniques to uniquely identify the sender of a message.
- Various approaches:
  - Encryption techniques
  - Cryptographic hash functions
  - Digital signature → a combination of various cryptographic primitives.

Now, the other thing I told you out, authentication. Here also we will be talking about some techniques in more detail. So, authentication is a very important cryptographic primitive which is again used in many security applications.

This consists of techniques to identify the uniqueness of the sender, the sender of a message, who is the sender, right. There are various approaches that can be used for this kind of authentication. So, you can use encryption techniques also for authentication, you can you, something called cryptographic hash functions, we shall be talking about.

Or you already may be aware of this term digital signature; so, using this kind of digital signature, you can also have some kind of authentication. So, we shall be talking about some of these techniques during the course of this lecture, we will also be seeing some actual demonstrations of some of the attacks and how they are mounted.

So, with this we come to the end of this lecture. In the next few lectures we shall be looking at some more details about the encryption and decryption techniques and I told you authentication, cryptographic hash function, how these actually work and how this can be used to build some security application which can secure my networks, ok.

Thank you.