

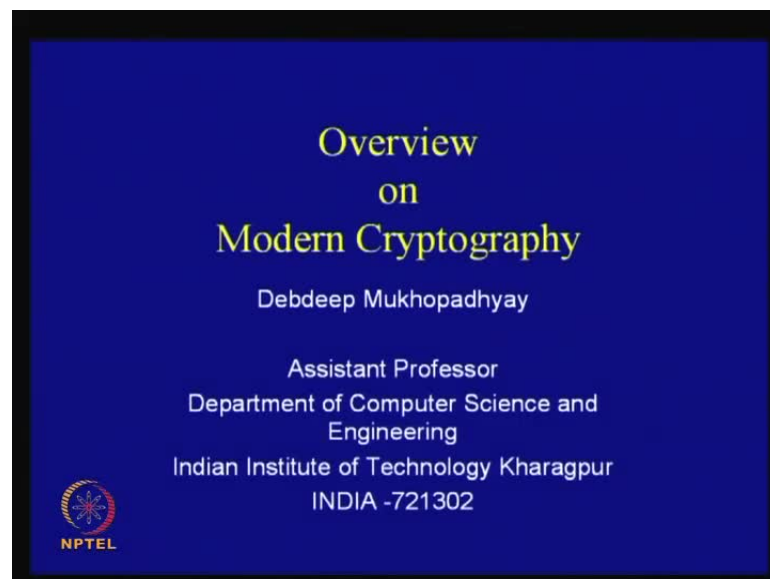
**Cryptography and Network Security**  
**Prof. D. Mukhopadhyay**  
**Department of Computer Science and Engineering**  
**Indian Institute of Technology, Kharagpur**

**Module No. # 01**

**Lecture No. # 02**

**Overview on Modern Cryptography**

(Refer Slide Time: 00:25)



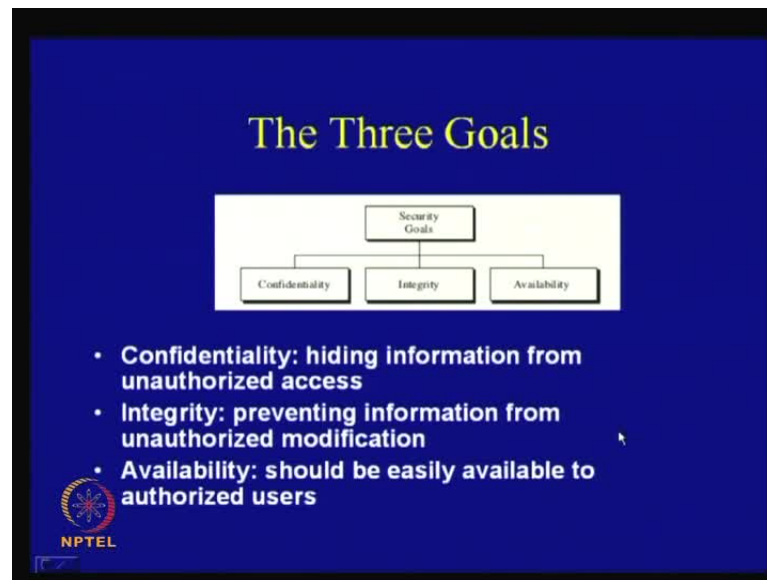
(Refer Slide Time: 00:29)



Welcome to today's lecture. Today, we shall be discussing about an overview on modern cryptography. As we have introduced the topic, today's discussion will be essentially about achieving the following objectives. Like today, we shall try to understand what are the goals of cryptography, what are the security services, which are intended by cryptographers to provide to users? Also, what are the mechanisms which are adopted to realize these services?

Finally, we shall conclude with some comments about the relationships between the services and the mechanisms. Throughout the course, we shall actually go deeper into these topics, but today's lecture essentially shall be trying to understand, or rather obtain an overview on this subject.

(Refer Slide Time: 01:08)



So, first of all, what are the three main goals of cryptography? Essentially, as we say it to CIA, that is – confidentiality, integrity and availability; so the goals are essentially as follows, like hiding the information from unauthorized access, that is - a person or user who is not authorized to use a particular piece of information should not be able to access the information. Integrity of data is important, that is, the information should be prevented from modification, by a person who is not authorized to do so.

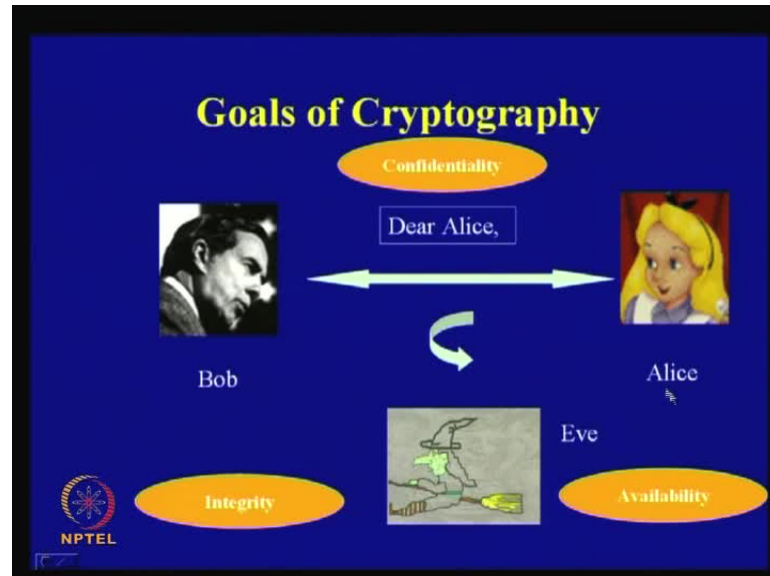
We all know that we always do modification of data. For example, typically, in a bank scenario, where we try to kind of debit an account or credit an account, then we are continuously changing our balances, but imagine like, if instead of me updating my bank account, somebody else does; so that is not proper; so that is an illegal use. So, cryptography also tries to provide the integrity of the information, which is there in my bank account; so, that is what is meant by integrity.

The other important thing is availability; so, therefore, while doing all these or rather while taking measures to achieve the goals of confidentiality and integrity we should not make it so clumsy - like the network should not be nor the communication should not be so clumsy, that the information is not accessible to the authorized user.

So, by saying that it is not accessible or **it is** rather not available easily means that it may become very slow. For example, you are trying to access particular information and imagine that it is so slow that you cannot access it, therefore it is not usable.

So, therefore, the objective of cryptography is to provide confidentiality and integrity of data while maintaining the availability of information to an authorized user.

(Refer Slide Time: 03:03)



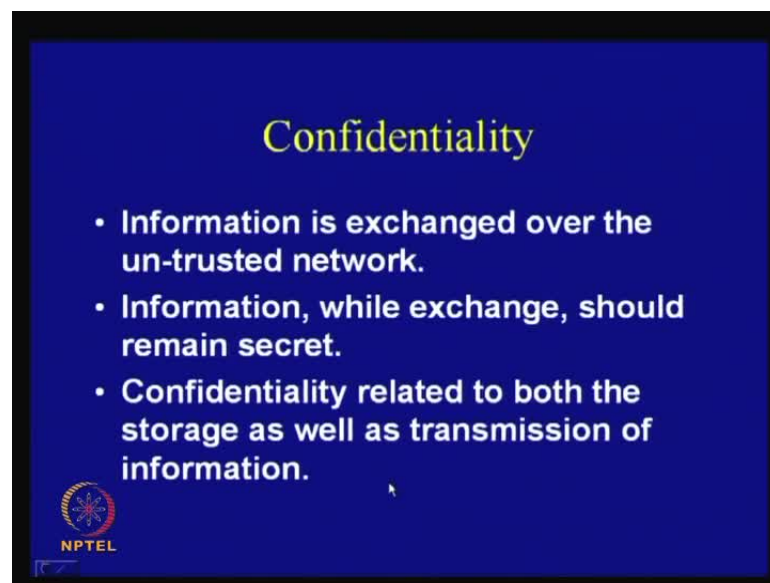
Now, we shall consider the typical scenario of a cryptographic network. So, therefore, there are two users, or as we say, legal users or authorized users. Consider Bob and Alice, as we have discussed in the last class, they are the two most popular characters which are used to describe a cryptographic scenario, and they send information like suppose, Dear Alice. So, there is an eves-dropper who is unauthorized to obtain the information; so the eves-dropper essentially has got an access to the communication channel. And Therefore, what is believed in this set work, or rather, in the setting is that this communication channel is not trusted; so it is an untrusted communication channel through which Bob and Alice tries to communicate a piece of information.

The goals which cryptography tries to provide are, as we have discussed, confidentiality, integrity and availability of information; that means, eve should not have an access to this information, so it should be some sort of unintelligible to the eve, and at the same time it should not be able to modify this piece of information. Like, instead of saying dear Alice, it should not be something else; so that there is a kind of misunderstanding between Bob and Alice. At the same time, Alice should be able to access this piece of information easily. So, it should not be that the network becomes slow or the packet is dropped, in order to prevent it from being accessed by eve, and in the process ending up

in Alice not being able to access the piece of information, so that should not happen; so the piece of information should also be available to Alice.

So, these are the basic three broad goals which cryptography tries to provide to users. We have to see that what are the mechanisms that cryptography or network security or the subject essentially, provides to achieve these goals?

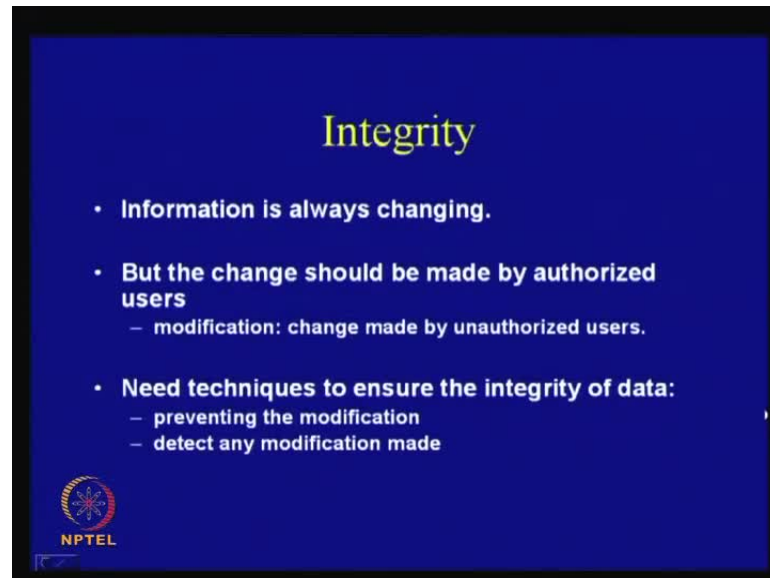
(Refer Slide Time: 04:56)



Now, we shall little bit look more deeply into each of these topics. So, we can see for example, confidentiality; confidentiality is essentially, where the information is exchanged over untrusted network. As we have said just now, that the information is being exchanged over untrusted network and we have to provide confidentiality in such a setting. So, therefore, the information, while in exchange should remain secret.

Therefore, when we are kind of exchanging a piece of information, then it should not be opened up to a person who is not supposed to use this information. At the same time, confidential is related to both the storage as well as transmission of information, which means, that it is not only like, when we are storing a piece of information, but confidentiality has to be provided in transit; that is, when the message is being passed from say, Alice or Bob or over an untrusted network, it should be confidential and it should not be opened up to person like eve, who is not authorized to use the piece of information.

(Refer Slide Time: 05:55)



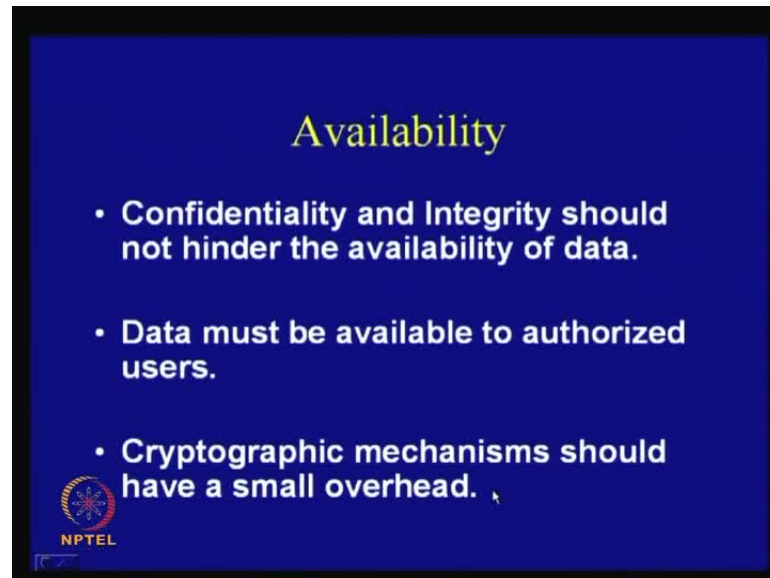
So, then comes the topic of integrity, as we have discussed. We know that information is always changing. The basic objective of having information is one of the objective is like, to kind of, modify this information; so information is always transient, but the thing is, it should be made by only the authorized users.

So, imagine I do a railway booking, or for example, as I said that I have a bank account, and this information should be only changed by the people who are authorized to do so. But what we term in this literature as modification means, that change which is made by unauthorized user. So, therefore, these unauthorized users can be given various names like attackers, it could be hackers, it could be people who are kind of trying to sabotage this piece of information by modifying.

So, for example, I have a bank account and somebody else continuously extracts money out of it; so that is the piece of modification which needs to be stopped. So, therefore, we need techniques to ensure the integrity of data, that encompasses essentially two parts: the unauthorized users should be prevented from modifying this piece of information and also if somebody does any modification, the second line is, I should be at least able to detect that the modification has taken place, and try to identify who has made this modification.


So, these are kind of the two important goals which essentially needs to be satisfied by cryptography and is needed by any form of e-commerce or electronic transactions; so these are very important goals which cryptography needs to satisfy.

(Refer Slide Time: 07:34)



Then as I told you that confidentiality and integrity should not hinder the availability of data; so data must be continuously available to an authorized user. Cryptographic mechanisms will definitely have an overhead; so it is always like you are doing something over, what you are supposed to do for the normal transaction, but the overhead should be as small as possible. So, therefore, cryptography should not be a nuisance so much, that it is kind of bypassed for practical user. So, therefore, we need fast algorithm, faster modification techniques, something which has got a lesser footprint over time and other important parameters.

(Refer Slide Time: 08:08)



**Mechanisms**

- **Cryptographic Algorithms are used to achieve the above goal.**
- **They rely on a secret piece of information, called the key.**
- **The algorithms are published.**
- **Attackers objective is to obtain the key from the communication.**

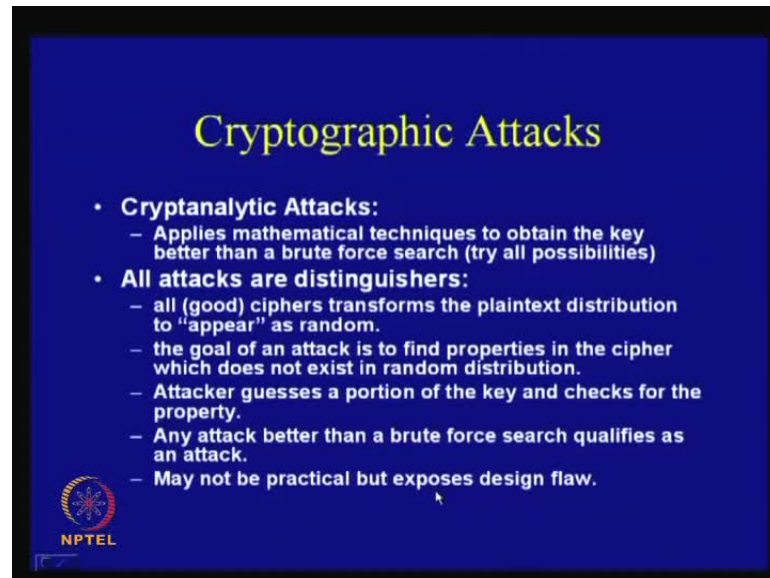
  
NPTEL

So, then we come to the topic I mean, how are these goals achieved; so, therefore, the mechanisms. We see, the cryptographic algorithms needs to be designed to achieve these goals and what we say is that what is very central to cryptography is like, they rely on a piece of information, which is known as the secret key. So, therefore, the idea is as follows that is everybody knows the algorithms, the algorithms are existing in public domain, what does not exist or what is not known to an attacker is the piece of information, which we know as or call as the key.

So, therefore, the objective of any attacker is essentially, to find out the key. So, therefore, if he or she is able to find out the key, he is able to deduce the key by an efficient technique, then the cryptographic algorithm is supposed to be compromised. Then, the various goals which cryptographic algorithms kind of guarantees like confidentiality, integrity and availability - does not hold anymore, because the basic algorithm on which these goals, or rather through which these goals are achieved, are compromised by these attacks.




(Refer Slide Time: 09:12)



**Cryptographic Attacks**

- **Cryptanalytic Attacks:**
  - Applies mathematical techniques to obtain the key better than a brute force search (try all possibilities)
- **All attacks are distinguishers:**
  - all (good) ciphers transforms the plaintext distribution to “appear” as random.
  - the goal of an attack is to find properties in the cipher which does not exist in random distribution.
  - Attacker guesses a portion of the key and checks for the property.
  - Any attack better than a brute force search qualifies as an attack.
  - May not be practical but exposes design flaw.

 NPTEL

So, therefore, we have to consider cryptographic attacks. So, therefore, when we are designing a cryptographic algorithm, then we have to consider the attacks and this is the very fascinating part of the subject. One of the primary reasons is that we do not know what an attacker can do? So, therefore, it is difficult to develop a proper model of an attacker and that makes the subject quite interesting, because you are supposed to develop a cryptographic algorithm, which is secured against an algorithm or a concept, which we call as attacker, who is not properly defined.

So, the first thing which we do is that we try to properly understand, or rather, we can try to conceptualize, what are the possible types of attacks which can take place? So, for example, we can broadly categorize the attacks as two parts as we can say like, one of the parts is called as, what is called as, cryptanalytic attacks. What is cryptanalysis?

As we will be seeing, that this particular discourse or this particular subject has got two important components: one of them is what we call as cryptography, which is the science of making ciphers or cryptographic algorithms, and the other is the science of breaking ciphers and this science, which discusses how to compromise existing ciphers, is technically known as cryptanalysis and together with cryptography and cryptanalysis, the subject is called cryptology.

So, there are some attacks which belong to this category of cryptanalytic attacks, which essentially tries to find out, or rather, applies mathematical techniques to find out the weaknesses of existing cryptographic algorithms.

Now, we have noted that the objectives of cryptanalysis is, when we are doing a study, is not bad; so, the objective is to make our defenses stronger. So, we can make a strong cryptographic algorithm, only if we analyze the cryptographic algorithm quite deeply; so that a third person or an illegal user is not able to find out the weaknesses.

So, we are kind of trying to find out, or rather, we are trying to develop a cryptographic algorithm, through which we can actually guarantee security to end user, but that is quite difficult, but that is the objective or the goal of this subject. So, therefore, we find that in cryptanalytic attacks, we apply mathematical techniques to obtain the key better than a brute force search.

So, consider that in a practical scenario, you may have, say for example, a cryptographic algorithm which has say, a 128 bit key. So, 128 bit key means, you can imagine that it is a 0 1 value and therefore, there are 2 to the power of 128 possible values of the key. So, what we can do or what an attacker can do is, for example, try all these 2 to the power of 128 possibilities - that is something, which we call as a brute force search.

So, it does not take care, or rather, exploit the properties of a cryptographic algorithm, but just searches all the possible keys. But as we know that 2 to the power of 128 is a huge number, it is probably more than the number of particles in this universe. So, therefore, it is not possible for a bounded adversary, or what we say as a practical adversary, or a practical attacker to search for all the possible keys.

But the goal of a cryptographic algorithm is to guarantee that an attack does not exist, which is better than a brute force search. Now, if an attack is developed for example, talking about our 128 bit key, if I develop an attack against a cryptographic algorithm, which requires say 2 to the power of 127 searches.

So, technically speaking, it is still an impractical attack, but we will classify them as an attack, and we will say that a cryptographic algorithm is technically compromised. So, therefore, we will try to develop techniques, so that even such an attack does not exist;

the reason being, that this attack may not be practical today, but it may be exploited to develop further attacks.

So, the objective, rather the principle, which is followed in the subject of designing ciphers is - to develop a cryptographic algorithm, to state the algorithm properly rather formally, then trying to find out various methods through which it can be attacked, and then to guarantee or give proper mathematical arguments, to say that an attack does not exist, which is better than a brute force search; so, that is the objective of the subject which we call as cryptanalysis.

We will see that all attackers, or rather, all attacks are essentially distinguishers; so, what we mean by distinguishers is that all good ciphers, that is, supposedly the ciphers which are good, transform the plaintext distribution to appear as random. So, which means that suppose, we take a normal cryptographic algorithm and apply it over alphabetic text; so, I use English language text, that is what we call as the plaintext, and we apply my cryptographic algorithm to develop something, which I call as cipher or the cipher text. Now, we know that, as we will see in our future classes is that, English language distribution has got a particular distribution. So, we know that for example, e is the popular letter which we use in our normal English literature; so these types of properties exist in the language that I speak.

The objective of a good cipher should make this distribution look random to a person who is just observing the output, that is, what I mean is, take for example a plaintext, and I know that there is a distinct distribution in that plaintext. Now, the objective of a ciphering algorithm should be to make this distribution lost. So, that means, the distribution of the cipher text should look random, but we noted that a ciphering algorithm is a kind of a sequence of mathematical steps, it can never be random; it can at best be something which we call as pseudo random. So, it is hard to distinguish from a random, but it is definitely not random.

The objective of an attacker or a cryptanalytic attacker or cryptanalysis is to find properties; basically, to study the cipher and to find properties, which still exist in the cipher text, which makes it distinguished from a random distribution.

So, the moment I find such a property, then I can exploit that or use that to develop a real life attack. So, what we can do is that once we have this kind of property, we guess a

portion of the key and then we see whether that property exists in the cipher text. The hypothesis is that if the key is wrong, then the property does not exist, but if the key is correct then the property exists and that can give a kind of distinguisher between a wrong key and a correct key.

So, therefore, the objective of a cryptanalytic procedure would be typically, to find out these properties and then to develop a kind of divide and conquer technique, to find out or rather, to kind of distinguish a wrong key from a correct key.

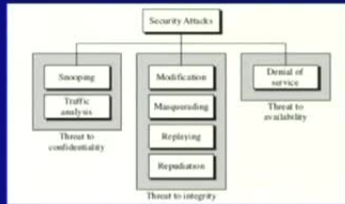
We will see this concept in more detail **from a** when we talk about linear cryptanalysis and differential cryptanalysis. But the message which I want to convey is - all cryptanalytic attacks or all attacks in general, are nothing but distinguishers, they are distinguishers from a random distribution. So, you see that all good ciphers transform the plaintext distribution to appear as random. The goal of an attack is to find properties in the cipher, which does not exist in a random distribution.

So, therefore, the attacker basically checks, guesses the portion of the key and checks whether the property exists. Any attack, which is better than a brute force search, like, if it is greater than  $2^{128}$ , so it could be  $2^{127}$ , even then it qualifies as an attack; so it may not be practical attack, but it definitely exposes a design flaw.

So, it says that the designer of this particular cryptographic algorithm gave me a security of 128 bits, but what it is achieving actually is a security of 127 bits. So, it may be still sufficient for real life scenario, but it definitely exposes a design flaw, which can be exploited with further developments in cryptanalysis; so therefore, it needs to be taken care of.


(Refer Slide Time: 18:13)

## Non-cryptanalytic Attacks



```
graph TD; SA[Security Attacks] --> T1[Threat to confidentiality]; SA --> T2[Threat to integrity]; SA --> T3[Threat to availability]; T1 --> S[Snooping]; T1 --> TA[Traffic analysis]; T2 --> M[Modification]; T2 --> MAS[Masquerading]; T2 --> R[Replaying]; T2 --> REP[Repudiation]; T3 --> DOS[Denial of service];
```

- Do not exploit the mathematical weakness of the cryptographic algorithms.




Then there are arrays of non-cryptanalytic attacks. So, they do not expose the mathematical weaknesses of the cryptographic algorithms, but they attack or rather threaten the way of the protocols, which are adopted in a typical network kind of scenario; so, they are also threat to confidentiality, integrity, and availability. As we see that in under security attacks, there are two kinds of attacks, which are known as snooping attacks and traffic analysis. Then we have got modification, masquerading, replying, repudiation and denial of service; I will come to these topics gradually.

(Refer Slide Time: 18:53)

## Threat to Confidentiality

- **Snooping:** Refers to unauthorized access or interception of information. Encryption is used to make information non-intelligible to the snooper.
- **Traffic Analysis:** Even an encrypted message can be analyzed to obtain some information, like say the identity of the sender and the recipient, the nature of information (like text or image files).



So, therefore, If I concentrate on the threat to confidentiality part, there are two types of attacks - one is called snooping and the other one is called traffic analysis. Snooping refers to unauthorized access or interception of information. So, if you just think of Bob and Alice kind of scenario, when Bob was transferring a message over to Alice and if eve obtains this information of dear Alice, that is, the information which was being passed over the communication channel, then we say that eve is snooping over the communication channel.


So, what is normally done is that this message of dear Alice is encrypted; therefore, it is made unintelligible, so that even if eve has an access to this network, he or she does not understand the content of the information. So, therefore, encryption is used to make information non-intelligible to the snooper and it does not have an idea about what is the actual content, which is being transferred.

The other thing is, even if cryptographic algorithms like encryption is being adopted and is made unintelligible to eve, eve can get certain information from the message that is being passed, by doing kind of traffic analysis. For example, it can obtain the identity of the receiver and the sender, he can also understand whether, say, if a message file is, or a text file is being encrypted, or whether an image file is being encrypted, or say a music file is being encrypted. So, it can get the nature of the content which is been transferred by studying the header, or doing mode analysis on the packets which are being transferred; so, that is what is called as the traffic analysis.

(Refer Slide Time: 20:37)

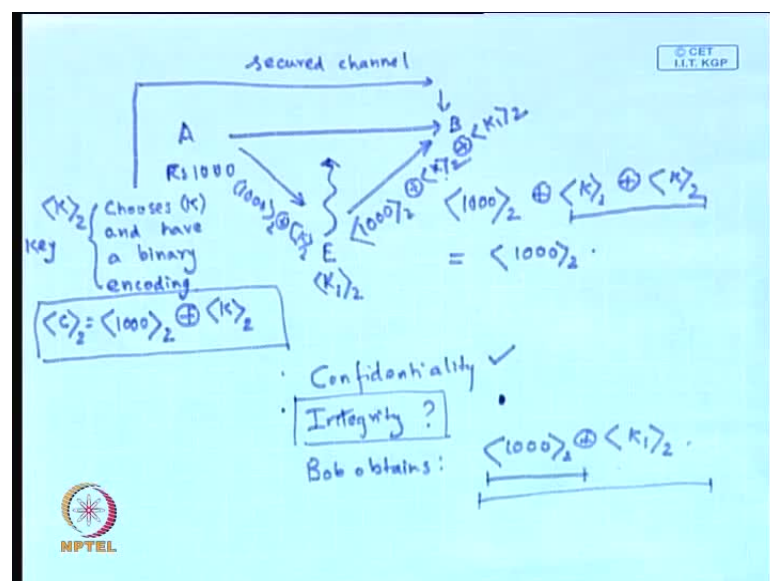
## Threat to Integrity

- **Modification:** An attacker can modify the transmitted information, without needing to know the actual content. It could delay or change the content to foil the objective of a transaction.
- **Masquerading:** An attacker can modify the communication data to pretend (spoof) as a legal sender or receiver to obtain the information to which it does not have access.



And, then we have got the threat to integrity; so therefore, under the threat to integrity, we have the topic of, or rather, we have got the threat of modification. As I told you previously, modification means that essentially the content is being kind of changed or being updated by a person who is not authorized to do so; so, therefore, an attacker can modify the transmitted information without actually changing the content or without actually needing to know the actual content.

(Refer Slide Time: 21:19)



So, therefore, I can give you one example. For example, imagine that there is Alice and there is Bob, who are communicating, and suppose, Alice wants to send to Bob a transaction of say Rupees 1000. So, what may happen in between is that eve is also obtaining this information, and Alice or Bob does not want that eve should understand the amount of the transaction.

So, what Alice does is that Alice chooses a random number, so, Alice chooses  $K$  randomly and encodes that in a binary format, therefore, I have a binary encoding, I call that to be something like, I denote that to be  $K$ . So, this is actually nothing but a key which Alice generates and somehow communicates this key to Bob through a secured channel. So, therefore, imagine that there is secured channel through which Alice communicates this information to Bob, and that is used only once in a transaction, that is, when the transaction starts Alice communicates this piece of information to Bob.

Now, what Alice does is that Alice takes this 1000 number I mean that is also encoded in a binary format - and XOR's that with the binary encoding of the key, and I denote this as the binary encoding; so, it obtains this information and just XOR's that with the key, so this could be some piece of information. So, 1000, then XORed with a key and I call that some information, which is encoded in the binary format; so eve has an access to this piece of information. So, Bob since, it knows the value of this key, what Bob can do when it receive this packet is, it can modify this, or rather, take this 1000 binary encoded with key, and XOR that with the binary encoding of key. Since, we know that if I do an XOR of two same numbers, then I essentially get zero, and therefore, what Bob obtains back is the binary encoding of 1000, and therefore, it knows the amount of the transaction.

But you see, the information which eve has an access to is this - 1000 XORed with this key, but if this key is randomly chosen, then eve does not have knowledge about what is this key; so, it cannot actually extract this information from this information. (Refer Slide Time: 24:20)

So, therefore, we say that confidentiality is definitely maintained; so, confidentiality is maintained if the key is randomly chosen, then confidentiality is obtained using this kind of technique.



But what about integrity? You see, if I take this information like, 1000 XORed key, and what eve can do is that eve can obtain this information, and instead of relaying back the same information, what it can do is that, it can randomly generate another string  $K_1$  I suppose, and just XOR this information, it just takes this, so it has got this information. So, it has got 1000 binary encoded XORed with  $K$ , it just takes this and XORs this with the  $K_1$  it has generated and passes this to the Bob. So, eve has not bothered to obtain the actual information, but it has modified the cipher text in this fashion.

So, now, when Bob does the decryption, Bob XORs it with this key value and therefore, what Bob obtains is (Refer Slide Time: 26:00). So, now you see that what Bob is supposed to obtain is that a transaction of Rupees 1000 has taken place, but instead Bob understands that a transaction of 1000 XORed with some non-zero number, which has taken place. So, therefore, the objective of Alice and Bob is kind of sabotaged; therefore, the integrity of the information is not really provided by the strategy, which Alice and Bob has taken.

So, therefore, we see that for integrity, you have to take or adopt some other mechanisms, which we will be seeing in our class when we go ahead. So, therefore, this particular example kind of motivates us that confidentiality and integrity are two different aspects of cryptography and needs to be tackled quite independently.

This essentially means that, for example, an attacker who can actually modify the transmitted information, without actually needing to know the actual content. So, therefore, here also, eve did not know the actual content, but it was able to modify the piece of transmitted information; so it could delay or change the content to foil the objective of a transaction; therefore, it needs to be taken safeguard.

So, the other thing could be like, masquerading; therefore, an attacker, for example, can modify the communication data to pretend of something which I call as the spoof, as a legal sender or a receiver, to obtain the information to which it does not have an access. For example, imagine that I am doing a transaction with a bank and when I am accessing the bank account, it may happen that there may be a fake kind of website, which pretends to me as my bank account and does the transaction with me; so this could be a dangerous example of masquerading. So, therefore, we need to adopt mechanisms to prevent such kind of attacks - security attacks.

(Refer Slide Time: 28:15)



The slide has a dark blue background with yellow text. The title 'Threat to Integrity' is centered at the top. Below it are two bullet points. The first bullet point is 'Replaying: An attacker copies a message sent by a different user and replays later.' The second bullet point is 'Repudiation: Sender of a message may later deny that it has sent it. Example, a user may deny a third party payment request.' Below the second bullet point is a paragraph: 'A receiver of a data may also refuse the receipt. Example, a merchant may refuse the receipt of a credit card payment. It is obvious, that cryptography should guarantee non-repudiation in these applications.' In the bottom left corner, there is a small circular logo with a globe and the text 'NPTEL' below it.

## Threat to Integrity

- **Replaying:** An attacker copies a message sent by a different user and replays later.
- **Repudiation:** Sender of a message may later deny that it has sent it. Example, a user may deny a third party payment request.

A receiver of a data may also refuse the receipt. Example, a merchant may refuse the receipt of a credit card payment. It is obvious, that cryptography should guarantee non-repudiation in these applications.

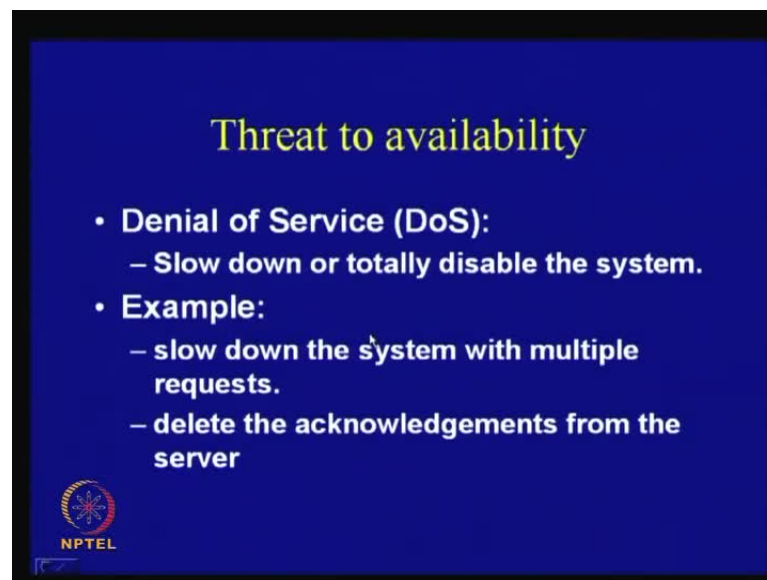
NPTEL

Then, we have got the attacks of replaying. In this case, an attacker copies a message sent by a different user and replays later. For example, in a network kind of scenario, there is not one particular protocol which is taking place at one time, but there are multiple protocols taking place; so, in one case I am the sender and in one case I am the receiver. So, what can happen in a typical replay attack kind of scenario is that I obtain a piece of information and suppose, I am doing a transaction one, consider that I am taking part in two transactions, transaction  $t_1$  and transaction  $t_2$ . So, suppose, I obtain the information in a transaction  $t_1$ , and I use this piece of information to reply a particular channel in a transaction  $t_2$  that can essentially lead to potential vulnerabilities in several attacks that we have seen and this also needs to be protected; therefore, we need to develop strategies to prevent something which is called replay. What is commonly adopted is, like the concept of timestamps or **evinces** or sequence numbers, to protect against this class of attacks.

Then we have got the important concept of repudiation; so, what repudiation means? That a sender of a message may later deny that it has actually sent it; now this could be a dangerous thing. Because, for example, imagine that a user may deny a third party payment request. For example, I do a third party payment request and after that transaction is done, I may deny completely that I have done this transaction.


So, there should be some way of proving to me later on, if I take up an objection, that yes, you have actually requested this and then payment has been done as per as your request. The other scenario could be like, a receiver of a data may also refuse the receipt, that it could refuse simply like it has never got this particular payment. So, for example, I do a credit card transaction and after I have transferred the money to the merchant, it may be that the merchant may refuse the receipt of the payment. Therefore, it is obvious that cryptography should guarantee that, such kind of scenario should not take place, or what we say, that it should guarantee non-repudiation in these kinds of applications. And therefore, we have to see how to, or rather, what are all the security mechanisms, or what are the cryptographic mechanisms which provides us these concepts of repudiation or non-repudiation?

(Refer Slide Time: 30:37)



**Threat to availability**

- **Denial of Service (DoS):**
  - Slow down or totally disable the system.
- **Example:**
  - slow down the system with multiple requests.
  - delete the acknowledgements from the server

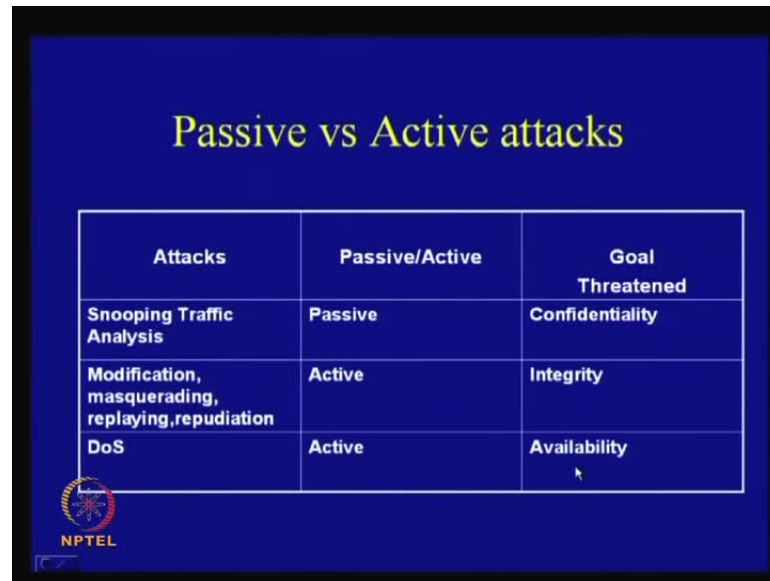
  
NPTEL

Then, we have got the threat to availability; therefore, as I told you, that data must be available to legal users. There are some classes of attacks, like denial of service is a very popularly known term. So, it could be like, the system is so much slowed down or it is totally disabled, that a legal user is not able to access.

So, for example, an attacker could slow down the system with multiple requests **and it could also like**, suppose, consider a sender and a receiver kind of scenario, where the sender sends requests and does not receive the acknowledgements. So, the sender again sends the request, which could be like an attacker who is actually sitting in between the

network, just simply deletes the acknowledgements and therefore, the sender thinks that he is actually not receiving the acknowledgements, he is again sending the requests. This could potentially crowd the network so much, that the entire system is slowed down or may be completely disabled; therefore, these kinds of scenarios also need to be tackled by various mechanisms; therefore, these also need to be found out.

(Refer Slide Time: 31:52)



Attacks	Passive/Active	Goal Threatened
Snooping Traffic Analysis	Passive	Confidentiality
Modification, masquerading, replaying, repudiation	Active	Integrity
DoS	Active	Availability

The slide features a blue background with the title 'Passive vs Active attacks' in yellow text. Below the title is a white-bordered table with three columns: 'Attacks', 'Passive/Active', and 'Goal Threatened'. The table lists three types of attacks: 'Snooping Traffic Analysis' (Passive, Confidentiality), 'Modification, masquerading, replaying, repudiation' (Active, Integrity), and 'DoS' (Active, Availability). An NPTEL logo is visible in the bottom left corner of the slide.

There is another taxonomy of attacks, what we say as, passive and active attacks. So, we do a classification, we again revisit these attacks and try to classify them as passive attacks or active attacks. So, passive attack means, it is a benign kind of attack, that means, that the eavesdropper or the attacker does not modify or delete the information, but just receives the information and observes the content; while in active attack scenario, the attacker actually modifies or deletes or inserts information, therefore, it is a potentially more harmful kind of attack modeling.

We shall also consider the goals, which are threatened. Consider snooping and traffic analysis, this falls into the class of passive attacks and the goal which it threatened is essentially, confidentiality. Just imagine that in Alice and Bob kind of scenario, there is a person eavesdropper, who obtains this information and tries to see what is actually going on. So, therefore, it tries to observe the piece of the information which is being transferred, it does not do any malice by modifying or deleting or inserting the

information, but just observes the content which is being transferred; so this is a typical passive attack and it threatens the goal of confidentiality.

So, we have got modification, masquerading, replaying and repudiation; we have seen what are these attacks, and these attacks, essentially, fall under the class of active attacks because they modify. Even in masquerading, you are also modifying the input packets, because we need to pretend as a sender or the receiver, so we also need to modify the packets by may be, planting - in place of my own identifier, I am planting the identifier of another person who is legal to use the information. So, that also falls under the class of active attacks because you are modifying the packet, you are inserting some other information into the packet, which you are not supposed to do.

Then comes the topic of replaying and repudiation, which are obvious examples of active attacks. So, these goals, or rather, these attacks threaten the goal of integrity because as we have seen, that the integrity or data integrity is compromised by these attacks.

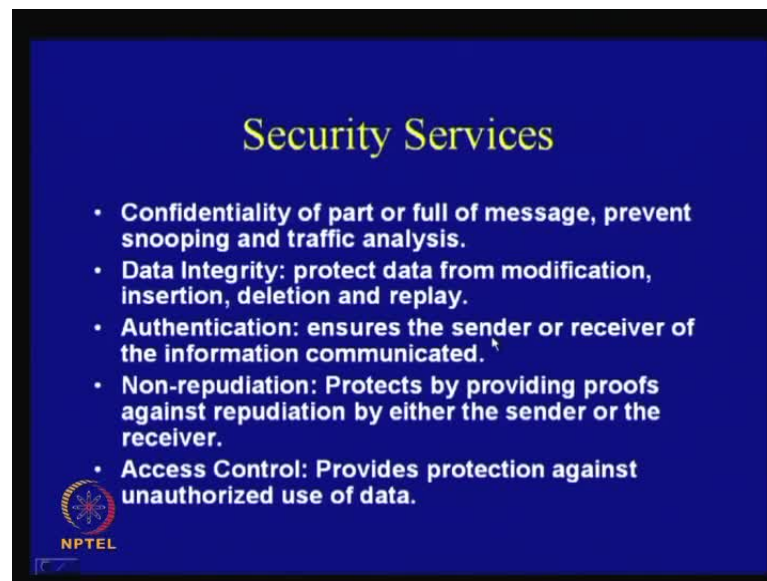
The denial of service attacks that we have seen, is also an active attack because again, you are deleting information by - say, deleting the acknowledgements or you are inserting large number of requests; therefore, you are also actively attacking the network and the goal which you are threatening is availability, because under the denial of service attack, information may not be available to even a user who is authorized to use this piece of information; so these are the basic attacks that we have seen.

(Refer Slide Time: 34:54)



Now, comes the most interesting part, like, how do we achieve these goals? What are the security services through which we essentially obtain, rather, what are the security services? We will see the various kinds of security services, one of them is data confidentiality, the other one is data integrity, authentication, non-repudiation, and access control.

(Refer Slide Time: 35:51)



Now, International Telecommunication Union-Telecommunication Standardization Sector, which is called commonly called as ITU-T, provides some security mechanisms to achieve these security services. We have seen the goals of data confidentiality and integrity also. So, the three new kind of security services that we have seen in this case is authentication, non-repudiation is also something which we have seen and also access control. So, I will go through this slowly one by one and therefore, we see that what the ITU-T guarantees is confidentiality of part or full of the message, that is essentially to prevent snooping and traffic analysis. So, these are the goals, or rather, the objective of ITU-T, and also it should provide data integrity, which means it should protect data from modification, insertion, deletion and also replay; so, therefore, integrity also should be provided.

Then you have got the service of authentication, which means that it ensures that the sender or the receiver of the information communicate, which means that the sender and the receiver are supposed to communicate some messages between each other and should

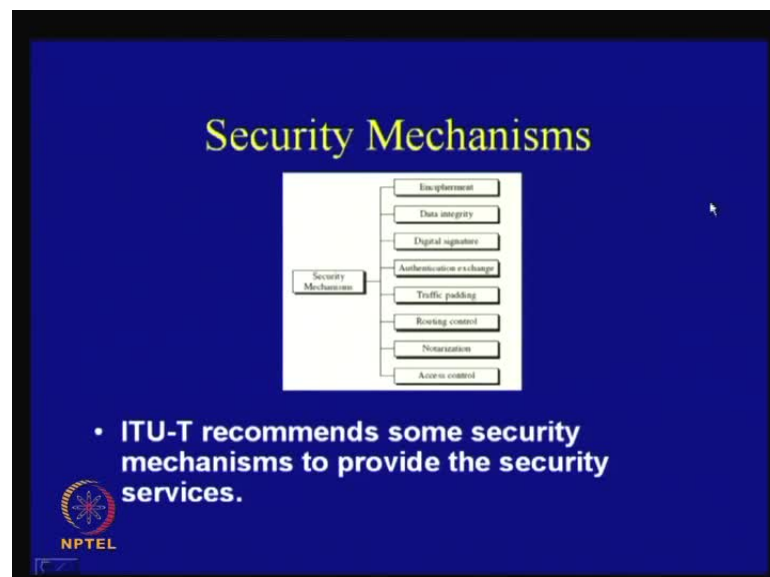
kind of guarantee, rather, build up the trust among each other that they are the person who are communicating and not being masqueraded by someone else.

So, therefore, you need to make your protocol or make your communication in a fashion, that it is authenticated like the sender and the receiver are authenticated to each other. So, the sender has a trust that it is really communicating to the intended receiver and the receiver is also convinced that it is actually receiving the information from the sender who is supposed, or rather, who is authorized to communicate with it.

So, this is quite an interesting field of the subject as well. Then, you have got non-repudiation, which means that it protects by providing proofs against repudiation by either the sender or the receiver; we have seen what is meant by repudiation.

Then you have got the topic of service or access control, it basically provides protection against unauthorized use of data. The common ways of providing access control is by the passwords or by the pin codes, or rather, pin numbers which you have. So, you know that all of your ATMs you have got a pin number, so basically, that gives you an access control mechanism.

(Refer Slide Time: 37:57)

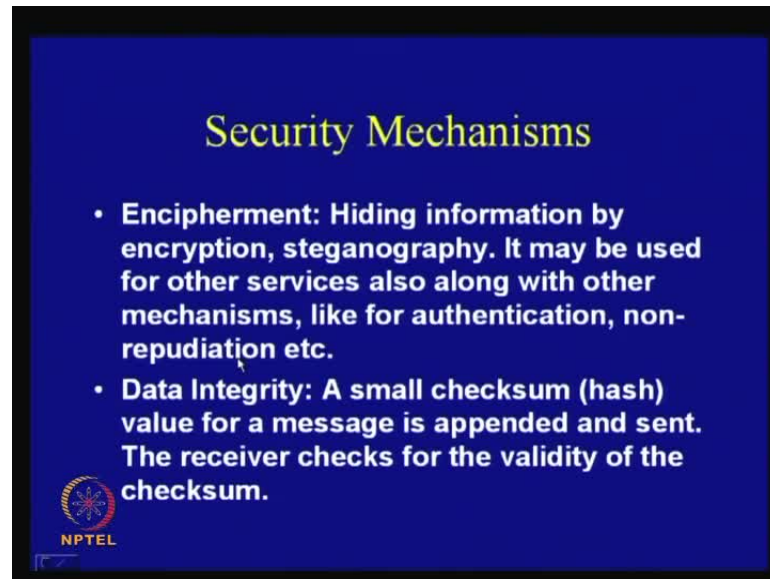


The basic mechanisms through which to obtain these security services or security goals, ITU-T recommends some security mechanisms to provide the security services. Therefore, what we see is that you have to consider the various mechanisms. The

mechanisms are as following: it is encipherment, data integrity, digital signature, authentication exchange, traffic padding, routing control, notarization and access control.

So, these are various mechanisms through which these services are supposed to be provided to the user; we shall consider each of these mechanisms one by one.

(Refer Slide Time: 38:37)



First comes the topic of encipherment; so this is one of the significant portions of this particular course; we shall be considering the mechanisms of doing encipherment. Encipherment means, broadly, hiding information by encryption, or by something which we call as steganography; so, steganography is a different thing and what we will be essentially studying in this course is cryptography, but I will just give you a hint of what is meant by steganography. It may be used for other services also along with other mechanisms, like for authentication and non-repudiation.

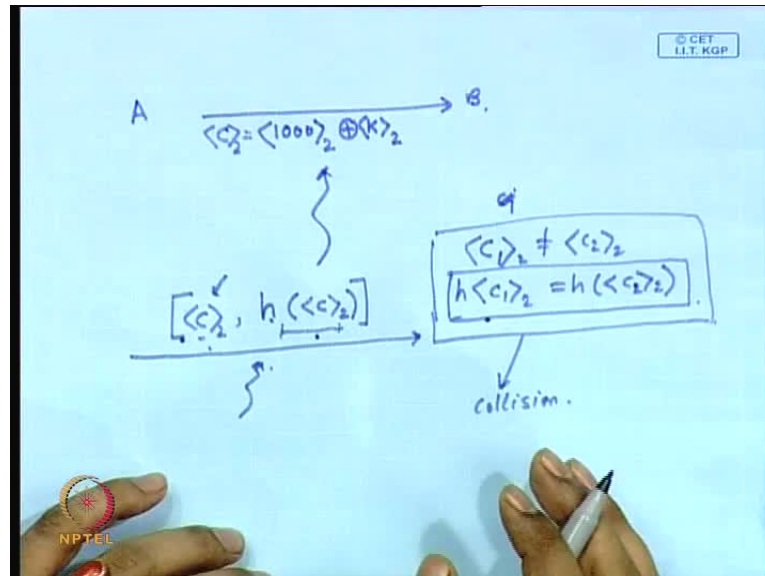
So, the objective of encipherment, as we will be seeing in our course, is mainly to provide confidentiality on information, but also with other mechanisms, it also sometimes provides authentication or non-repudiation; it also helps us in achieving the goals of authentication or non-repudiation.

Then we have got data integrity; in data integrity something which has been used commonly is a small checksum value for a message which is appended and sent. The



receiver checks for the validity of the checksum and that gives us a mechanism of obtaining data integrity; so this we shall also study in our course.

(Refer Slide Time: 39:58)



Imagine that Alice is sending information to Bob; it is sending the encrypted output of, say, 1000, as we have seen in the previous example. So, it is for example, sending this 1000 XORed with the binary value of a key and as we have seen that this particular mechanism alone, although it is an encryption and provides confidentiality, does not give, or rather, does not achieve the goal of integrity; therefore, eve can come in between and can modify this piece of information.

So, **what is commonly done is**, therefore, if I call this as the message which is being transferred, so this particular message is appended with a piece of information which is the output of a hash function. So, this is a specially designed hash function, which we call as the cryptographic hash function, which satisfies some properties. So, therefore, you take this  $h$  and you apply it over the binary encoding of  $c$  and you append it and send it along with the cipher text. So, this is the actual information which has been transferred.

Now, imagine, if eve comes in between and modifies this information, then Bob will easily be able to detect. Because, suppose this information is being modified, then when Bob receives this information, Bob can apply the hash function  $h$  on this particular component of the text and can check whether it matches with this checksum. If it does

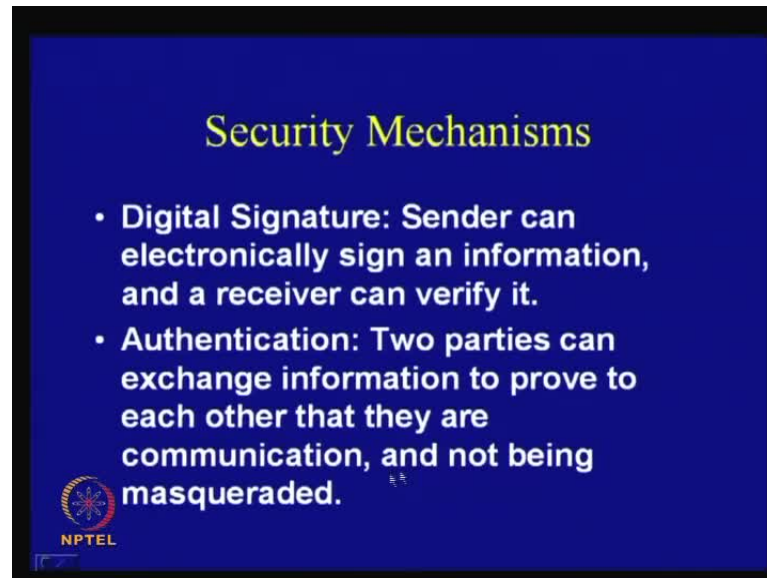
not match, then Bob understands that there has been a sabotage of integrity done by an eavesdropper, by an attacker, and therefore obviously, you understand or probably, you have started to think that this hash function should definitely satisfy some properties - some cryptographic properties which are also been postulated.

For example, one thing probably which can come to your mind is that it should not be easy to find out two values like this, which hash to the same value. So, therefore, what I mean is, it should not be easy to find out two  $c_1$  and  $c_2$  values which are not equal to each other and the hash of  $h(c_1)$  is same as the hash of  $h(c_2)$ . Because if this takes place, if it is easy to find out such a piece of information, then the integrity of this is not really provided by this hash function; so, the hash function should not essentially expose such kind of collision points. So, this is something which is called collision and therefore, the hash function should be something, as we say, as collision resistance.

I will come to these properties which the hash function should satisfy, but this is the basic scenario or basic objective for which these mechanisms are being developed. Although, it is not kind of so much well-defined, but we can say that encryption alone is helpful to provide us confidentiality of information, but not necessarily integrity.

Integrity has to be taken, or rather, tackled independently and the mechanism of cryptography which gives us, or rather, satisfies or achieves the goal of integrity, is something which is known as, cryptographic hash functions. So, we shall study in our course how to design these, or rather, achieve these mechanisms.

(Refer Slide Time: 43:31)



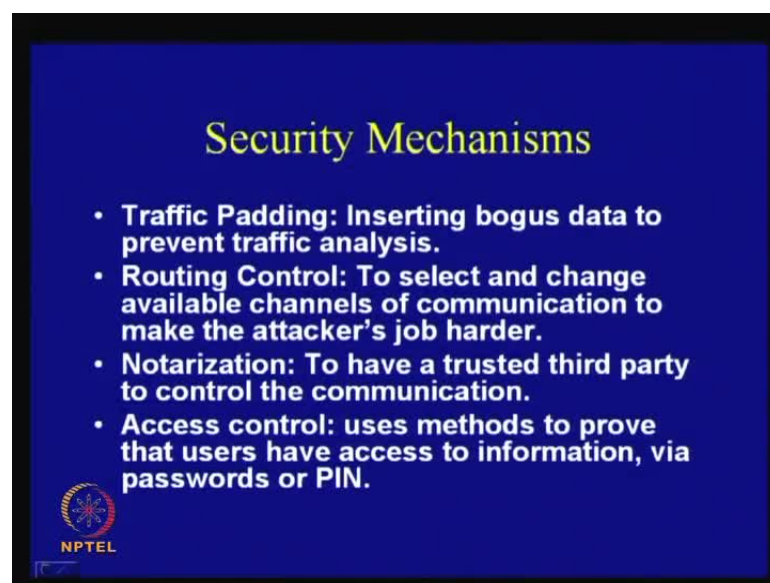
Then comes the important topic of digital signature. As we know that in our normal life, we know that if we have made a will or made a document, and we make a signature, the signature carries my bearance that it is - say for example, I have a cheque and I sign over - that it is a kind of authorization; that it is my signature, that I am granting this transaction, I have knowledge of this transaction.

But in the digital world, when you have got large number of information being transferred over digitally, then also it would be quite nice, if we can develop techniques which will help us to digitally sign a piece of information. Therefore, we shall study in our course how to develop, or rather, how to electronically sign a piece of information, so that I can also sign and the receiver can verify that it has really been signed by me. So, that also helps us in providing, rather, achieving the goals of integrity of information because it gives us authentication that this piece of information has got - if I am doing this transaction, my information which is being exchanged also carries this information - that I have knowledge of this transaction, it is not like, it is taking place without my knowledge.

Then, we also have, as I told you, the authentication; therefore, two parties can exchange information to prove to each other that they are communicating, that they are communicating among each other and not being masqueraded.

This is to stop masquerading and therefore, authentication is also a very important goal. Often, digital signatures are used to obtain the goals of authentication; therefore, these are the broad mechanisms and underlying these broad mechanisms, we have called cryptographic modules. So, various kinds of things are working underneath these broad mechanisms and the fascinating part of subject is how to develop, or rather, how to design these mechanisms. We shall see that lot of mathematics and mathematical properties are also being used to develop these mechanisms and that makes the subject quite interesting.

(Refer Slide Time: 45:50)



Then we have got techniques like traffic padding, where we insert bogus data to prevent traffic analysis. Therefore it could be like, I just implant in bogus data, so that the traffic analysis or statistical analysis does not take place; so, typical example could be like for example, there are some attacks which take care of the timing information.

So, it could be like, there is a sender and there is a receiver and what the attacker does is, the attacker tries to obtain the time of information, whether it is taking a longer time or it is taking a lesser time; that often, or rather, sometimes it has been found out, leaks the information about the secret.

Therefore, you can do analysis to ascertain the knowledge of the secret key. As a defense strategy what you can do is, do some bogus operation, or rather, you send some kind of garbage data over the traffic, so that the time of the transaction is always a constant.

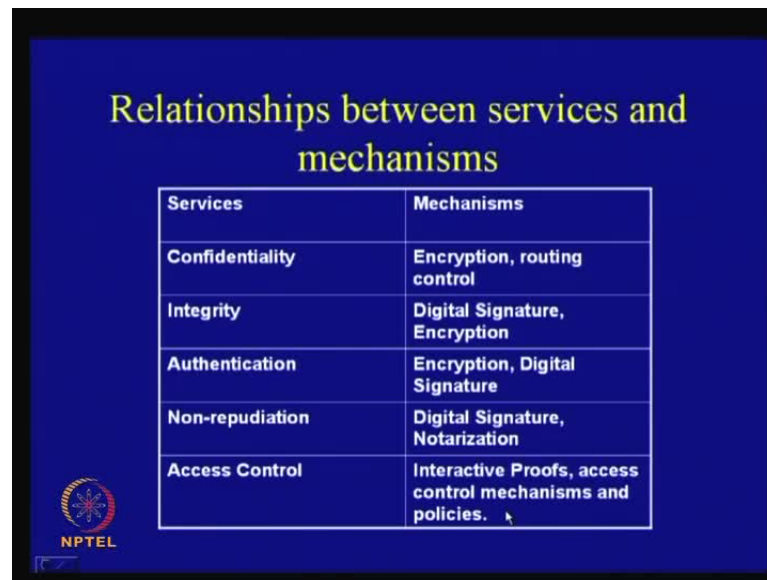
Therefore, you cannot actually adopt these techniques to find out, or rather, the timing techniques to adopt the key; therefore, this is very simple and on a broad level, very simplistic example to show you. So, you can actually plant in bogus data, prevent the traffic analysis of information.

Then, you have got routing control. Routing control means that there is a sender and a receiver and there may be various channels through which you can actually pass information from the sender to the receiver; so, you could actually use all the information rather than sending through only one channel, which can be eavesdropped. You can actually use, rather, switch and send the message over various channels; therefore, the task of the attacker will become harder because the attacker now, needs to monitor large number of channels. Therefore, you can actually have practical security in a network kind of scenario.

Then, there is a concept of notarization. Notarization means that you essentially have a trusted third party to control the communication. So, it could be like, when a sender, say, Alice and Bob are communicating among each other, they have a trusted third party from where you obtain the tickets, where you obtain the keys and other things. You can actually have, for example, if you would like to obtain the goal of non-repudiation, then what the trusted third party can do is that the trusted third party always stores all the information which is being passed by, say, Alice. Later on, when Alice denies, rather Bob denies a particular transaction, then the trusted third party can say no, see that I have noted down these transactions and these transactions prove that you have actually previously requested these transaction. So, therefore, now, you cannot refuse that you have not requested this transaction. Therefore, you can actually obtain non-repudiation by having a trusted third party, but, of course, that also adds to the cost of your communication.

Then you have got access control. As I told you that various ways of obtaining this access controls, there are various mechanisms through which access controls are obtained and there are various password-based schemes, there are various PIN-based schemes through which access control is maintained or obtained in networks. So, these are the various broad mechanisms.

(Refer Slide Time: 49:08)



Services	Mechanisms
Confidentiality	Encryption, routing control
Integrity	Digital Signature, Encryption
Authentication	Encryption, Digital Signature
Non-repudiation	Digital Signature, Notarization
Access Control	Interactive Proofs, access control mechanisms and policies. ↵

The relationship between the services and the mechanisms are also interesting and I believe that it is not so well defined, but we can actually have a fair amount of idea if we study this. As we have shown in this particular slide, for example, how do you obtain the service of confidentiality, may be, through the mechanisms like encryption and also, may be through routing control. Like, you keep on changing your routing so fast or so frequently that confidentiality is maintained, but what is more popular is, of course, encryption, that is, you make the piece of information unintelligible by using a piece of algorithm and a piece of secret key and make the information unintelligible to a person who is not authorized to have an access to the information.

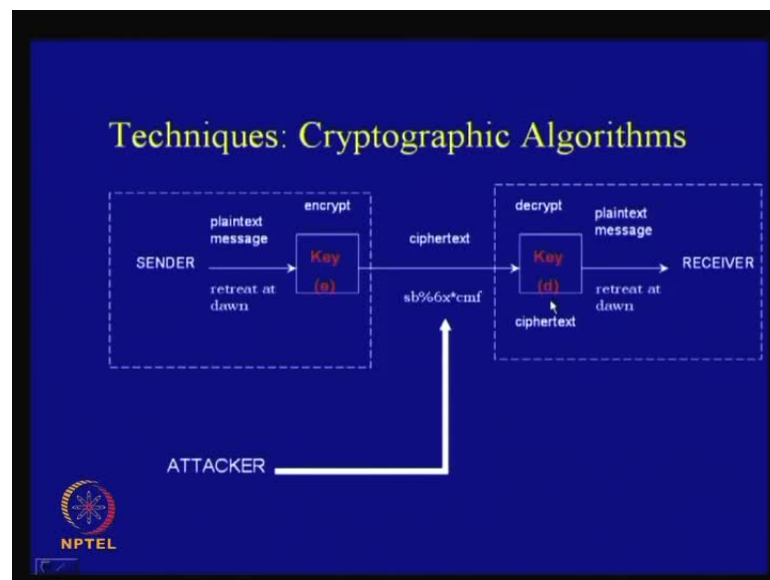
As we have seen, the other important service is integrity; integrity is obtained by digital signature and may be, again, encryption because encryption used along with other mechanisms, sometimes also provides, or rather, achieves the service of integrity and provide service of the integrity; therefore, it is also commonly used. The other important service is that of authentication, which is achieved using encryption and digital signature; so as we have seen, the digital signatures are used for integrity, it may be also be used for authentication as well.

The other service is non-repudiation, which is obtained using digital signatures, again and also by notarization. As I have just told you, how you can obtain that, because trusted third party can just keep on saving all the piece of information, storing the piece

of information which has been transacted and a denial later on can be detected by the trusted third party.

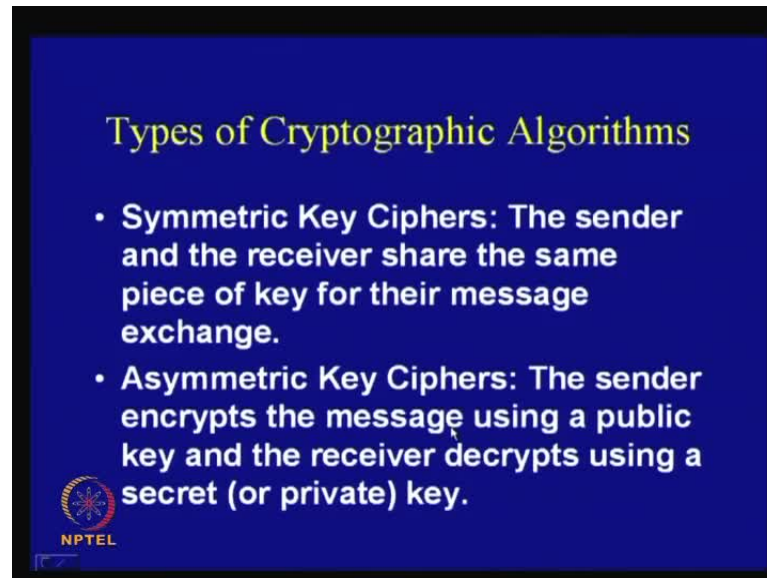
Then, you have got access control and this access control is achieved through something, which is called as interactive proofs. There are various access control mechanisms which are also being adopted and also policies, by laying out proper policies in the company or in the industry, you can also obtain access controls and there is various works in these lines as well.

(Refer Slide Time: 51:12)




So, what are the cryptographic algorithms? You have got a sender and you have got a receiver and as we have seen, we have got a plaintext message. For example, the plaintext here is, retreat at dawn, and there is an encryption algorithm and there is a secret piece of information which encrypts this information and makes it something like this. Now, this is kind of unintelligible to an attacker who sees this, but really does not understand what is the piece of information? Then in the receiver end, what it does is that this is decrypted and is decrypted by a piece of information, and obtains the plaintext and then receives back, or rather, extracts that information.

(Refer Slide Time: 52:08)



**Types of Cryptographic Algorithms**

- **Symmetric Key Ciphers:** The sender and the receiver share the same piece of key for their message exchange.
- **Asymmetric Key Ciphers:** The sender encrypts the message using a public key and the receiver decrypts using a secret (or private) key.

 NPTEL

Now, the question is, what are the types of cryptographic algorithms which are existing? There are broadly two types of cryptographic algorithms: one of them is called symmetric key ciphers and another one is called asymmetric key ciphers; we shall be studying these in depth in our course.

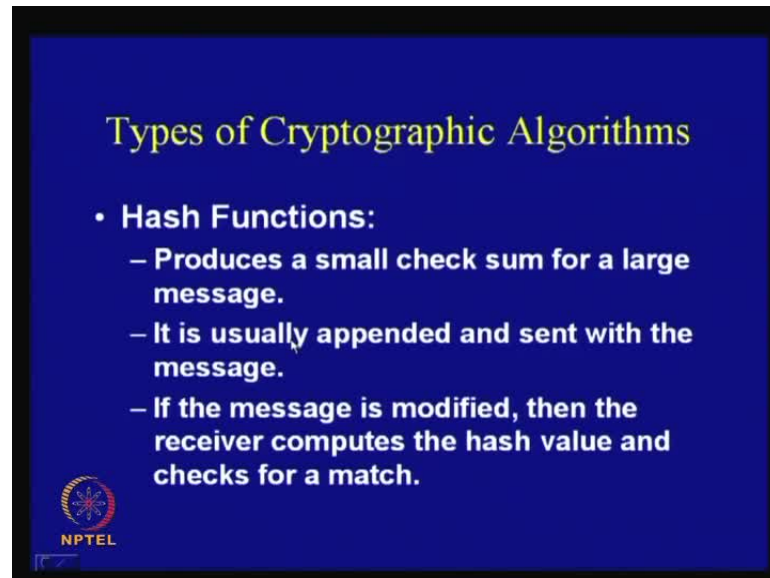
In symmetric key ciphers, the sender and the receiver share the same piece of key for their message exchange, that is, when the sender is communicating with the receiver, as we have seen, there is an encryption key denoted by  $e$  and that is the decryption key denoted by  $d$ , the encryption key and the decryption key are same; therefore, in a symmetric key environment  $e$  and  $d$  are same.

But there is something which is called as asymmetric key ciphers and in this case, the sender encrypts the message using a public key and that is public, means that this key is known to everyone; therefore, this key  $e$  is known to everyone, so it exist in a public domain. But for decryption, we have got a secret key, so it is called the private key and therefore, using this private key we recover back the plaintext. So, therefore, that concept means, that in order to decrypt, you need that secret piece of information but anybody can encrypt.

So, this is a very fascinating field of these cryptographic algorithms, which says that how you can actually do this asymmetric key ciphering and it relies on various numbers, theoretic and difficult problem, which exists or rather, which are believed to exist.




(Refer Slide Time: 53:31)



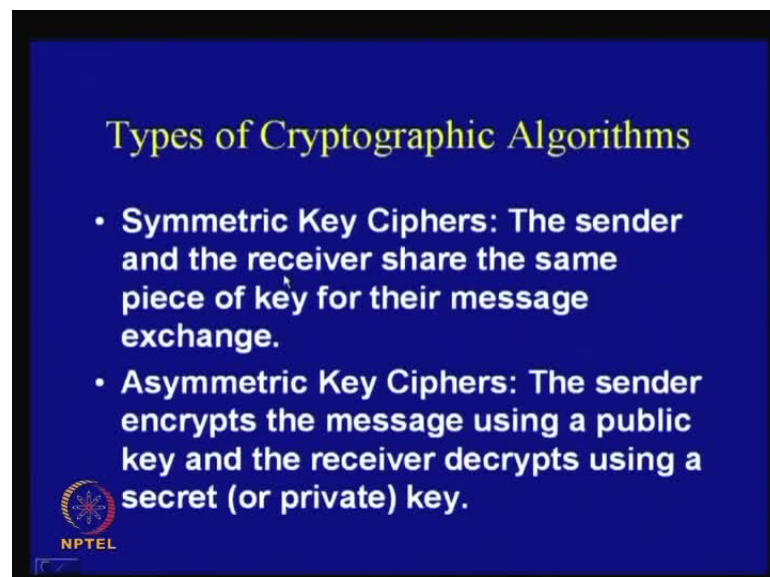
**Types of Cryptographic Algorithms**

- **Hash Functions:**
  - Produces a small check sum for a large message.
  - It is usually appended and sent with the message.
  - If the message is modified, then the receiver computes the hash value and checks for a match.

  
NPTEL


Then we have got hash function that I have told you. So, it produces a small checksum for a large message, it is usually appended and sent with the message, and if the message is modified, then the receiver computes the hash value and checks for a match.

(Refer Slide Time: 53:51)

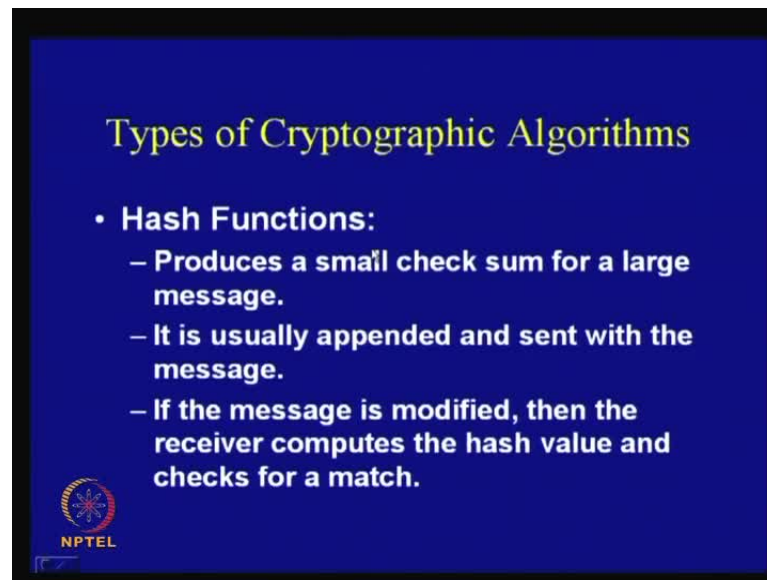


**Types of Cryptographic Algorithms**

- **Symmetric Key Ciphers:** The sender and the receiver share the same piece of key for their message exchange.
- **Asymmetric Key Ciphers:** The sender encrypts the message using a public key and the receiver decrypts using a secret (or private) key.

  
NPTEL

(Refer Slide Time: 54:23)



The slide has a dark blue background with yellow text. The title 'Types of Cryptographic Algorithms' is centered at the top. Below it, a bullet point '• Hash Functions:' is followed by three sub-bullets. In the bottom left corner, there is a circular logo with a star-like pattern and the text 'NPTEL' below it.

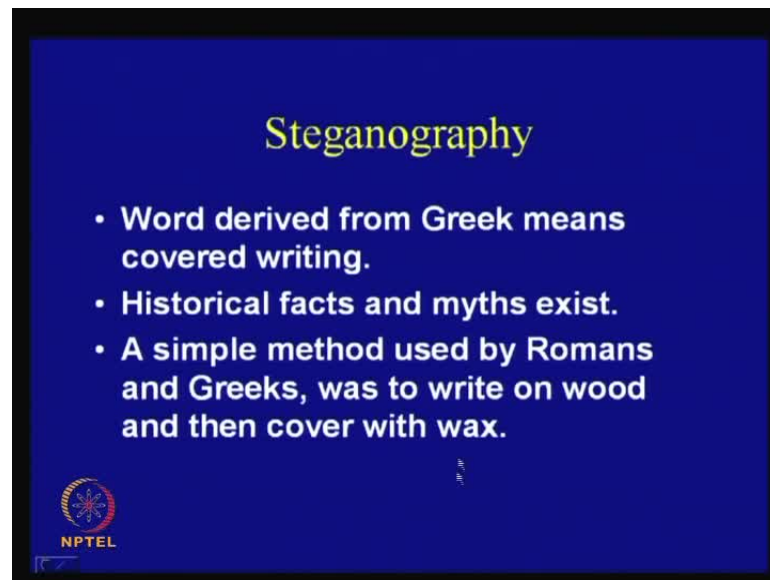
### Types of Cryptographic Algorithms

- **Hash Functions:**
  - Produces a small check sum for a large message.
  - It is usually appended and sent with the message.
  - If the message is modified, then the receiver computes the hash value and checks for a match.

NPTEL


This is again the topic of hash function. There are various cryptographic algorithms, which are being developed by cryptographers. Like under the category of symmetric key ciphers, we have got popular key terms like DES AES and other **blow fish** and so on, and there are stream ciphers and block ciphers; so, we will see these categories as we proceed in our course. Under the category of asymmetric ciphers, we have got RSA algorithm which are based on something which we call as ElGamal cryptographic system; they assist the algorithm like Elliptic curve cryptosystems, which forms the standards under these asymmetric key ciphers. Under the category of hash functions, you have got large array of hash functions; some of the popularly known hash functions are **MD**-family hash functions and then you have got the **Sha** hash functions and so on.

(Refer Slide Time: 54:36)

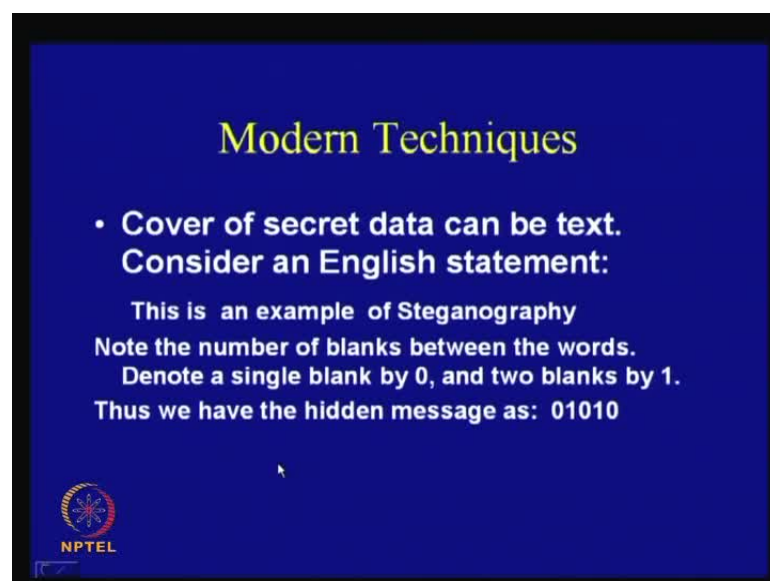


**Steganography**

- **Word derived from Greek means covered writing.**
- **Historical facts and myths exist.**
- **A simple method used by Romans and Greeks, was to write on wood and then cover with wax.**


 NPTEL

(Refer Slide Time: 55:03)



**Modern Techniques**

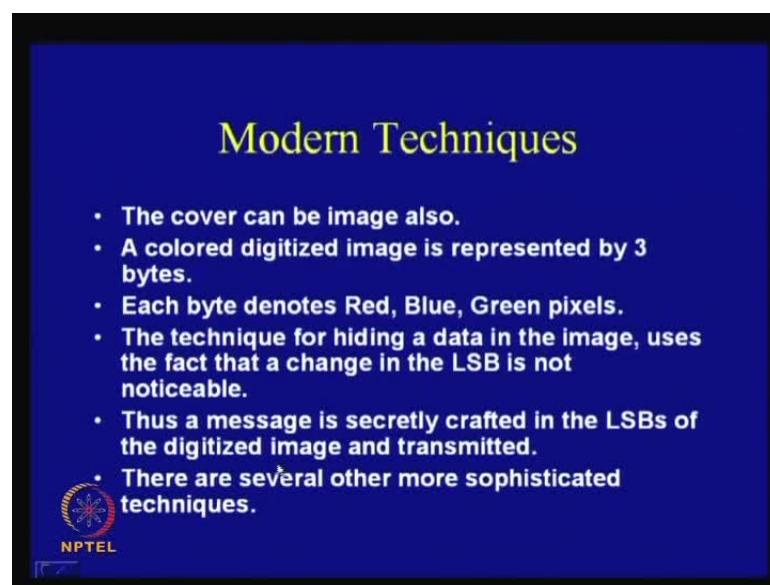
- **Cover of secret data can be text. Consider an English statement:**  
This is an example of Steganography  
Note the number of blanks between the words.  
Denote a single blank by 0, and two blanks by 1.  
Thus we have the hidden message as: 01010

 NPTEL

Now, we shall conclude our talk with something which is called steganography because we will not really cover this in our course. Steganography is an interesting field, which is like, this word is derived from Greek, which means covered writing. The historical facts and myths exist about this study and it is a simple method used by Romans and Greeks. For example, to write on wood and then cover them with wax, this is a very primitive way of doing steganography. Some of the modern techniques could be like this - you could actually cover up a secret data, could be a text; therefore, you can just consider this English statement like this is an example of steganography.

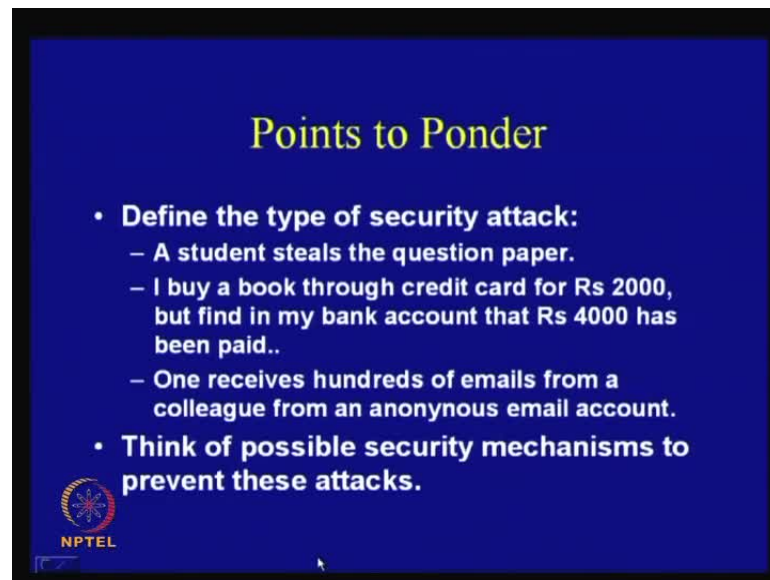
This is seemingly quite a simple English statement, but if you observe carefully, you will find that the gaps between two words are not exactly the same. For example, here there is 1 single blank, but here there are 2 blanks, but here there is again 1 blank here, there are 2 blanks here, there are 1 blank. Now, if you denote a single blank by 0 and the 2 blanks by 1, then you can actually say that the hidden message in this simple benignly looking text, it could be like 01010. Therefore, when communicating, this is an example of steganography, but actually what we are trying to communicate is this piece of information; therefore, this is the quite interesting way of obtaining confidentiality.

(Refer Slide Time: 56:01)




So, another modern technique could be like this, which is also quite interesting. The cover can be an image also, like a colored digitized image is represented by 3 bytes and each byte denotes red, blue, green pixels; therefore, you can have red, blue, green pixels. The techniques for hiding a data in this image, it uses the fact that if you change the LSB, then it is not noticeable; therefore, if we take a digitized image and just change the LSB, then it is not noticeable. Therefore, what you can do, you can have a secret message and secretly you can craft this message by modifying the LSB of the digitized image and then transmit that. Since, you are changing the LSB, probably, you cannot detect this change, but you can actually convey this message quite secretly.

(Refer Slide Time: 57:02)



**Points to Ponder**

- **Define the type of security attack:**
  - A student steals the question paper.
  - I buy a book through credit card for Rs 2000, but find in my bank account that Rs 4000 has been paid..
  - One receives hundreds of emails from a colleague from an anonymous email account.
- **Think of possible security mechanisms to prevent these attacks.**

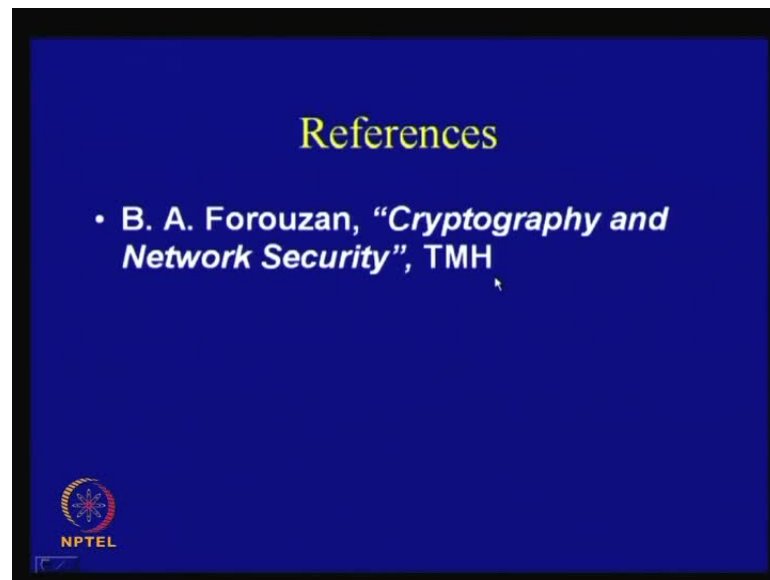
  
NPTEL

So, there are several other more sophisticated techniques, but we shall not go into them, but just wanted to hint that there is also an interesting topic of work, which is called as steganography.

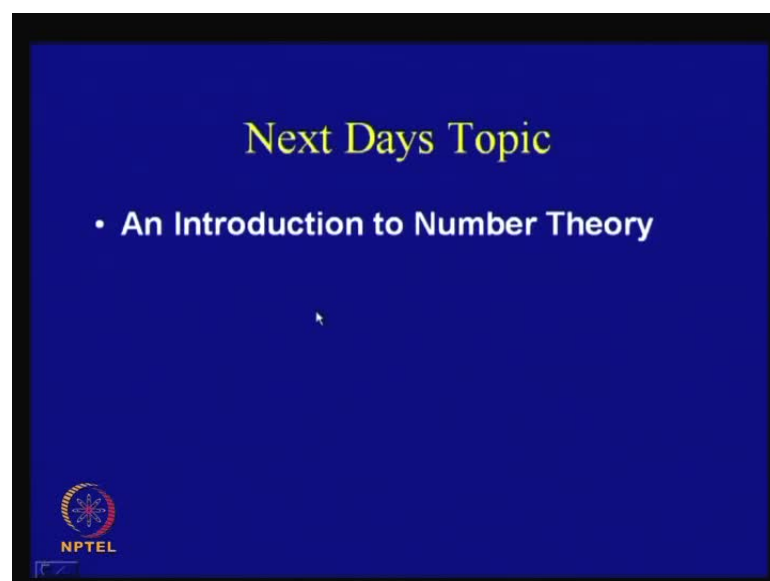
I shall give you some points to ponder, like points to think on. There are some examples which I have shown here, like - you are supposed to define the type of security attack, like, a student steals the question paper and another scenario could be, I buy a book through credit card for Rupees 2000, but find that in my bank account Rupees 4000 has been paid; so, you have to just classify the type of security attack.

The other scenario could be, like, one receives hundreds of emails from a colleague from an anonymous email account, so it is also interesting to think of possible security mechanisms to prevent these kinds of attacks; so, you can just think on what kind of mechanisms would you adopt to prevent these kinds of security threats.

(Refer Slide Time: 57:50)



(Refer Slide Time: 57:59)



So, I conclude here and the reference that I have used quite extensively is this book Cryptography and Network Security by Forouzan of Tata McGraw Hills. The next day's topic shall be on An Introduction to Number Theory.

Thank You.