

Data Communication
Prof. A. Pal
Department of Computer Science & Engineering
Indian Institute of Technology, Kharagpur
Lecture - 39
Secured Communication - I

Hello and welcome to today's lecture on secured communication. Nowadays **computer come network** or internet is used for many sensitive applications such as shopping, banking, reservation of railway and airline tickets and in general for ecommerce. And as a consequence communication of data securely over the network is glooming large on the horizon as a massive problem.

In this lecture I shall try to discuss how secure communication can be achieved. Obviously the subject is very vast. Usually a full course can be covered on secured communication. But I shall try to give an overview of various aspects of secured communication in two lectures. Here is the outline of today's talk. I shall give a brief introduction where I shall explain the need for secured communication.

(Refer Slide Time: 01:57)

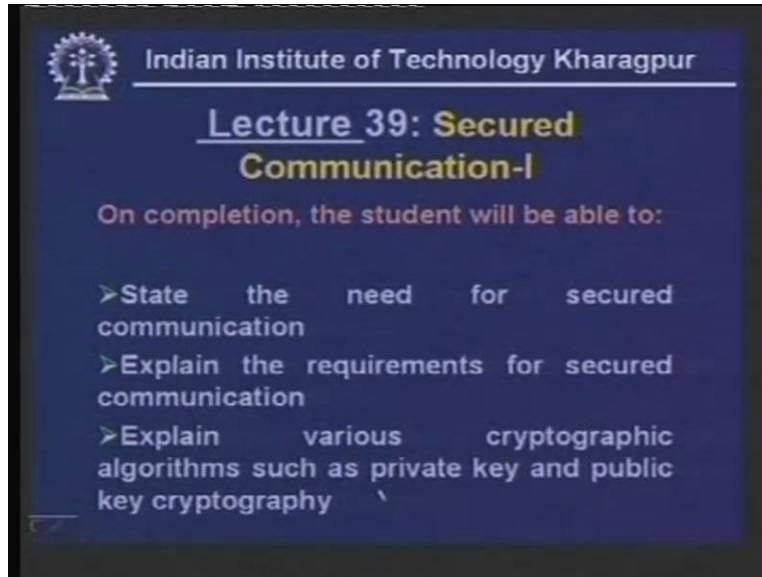


What is really meant by secured communication?

As we shall see cryptography will play a very important role in secured communication. In fact cryptography can be considered as a panacea to this problem. We shall see there are several cryptographic approaches. Basically it can be divided into two broad categories. One is known as symmetric-key cryptography where there are several variations like traditional ciphers using monoalphabetic substitution, polyalphabetic substitution and transpositional cipher. Then there are block ciphers where different transformations are used. We shall explain the different transformations and explain one

important cryptographic technique known as Data Encryption Standard DES which is widely used. Then we shall discuss about another cryptography technique known as public-key cryptography. We shall also see one application of public-key cryptography that is the RSA algorithm.

(Refer Slide Time: 03:20)



Indian Institute of Technology Kharagpur

Lecture 39: Secured Communication-I

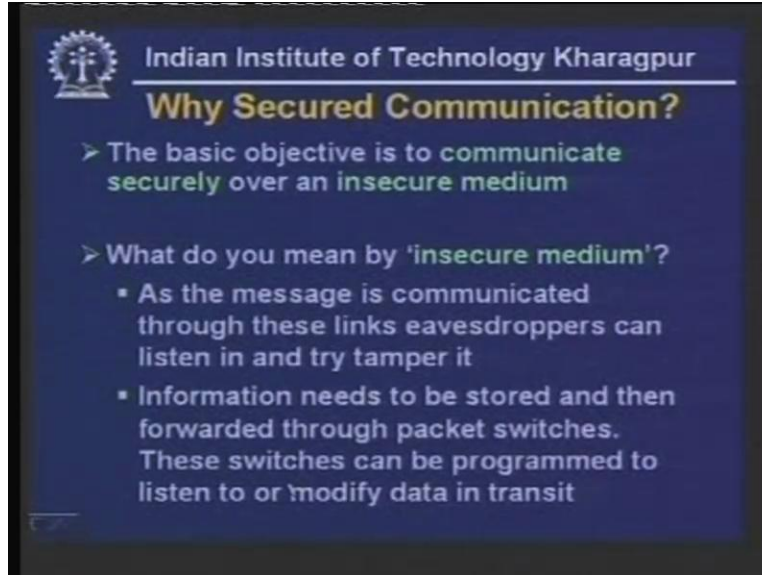
On completion, the student will be able to:

- > State the need for secured communication
- > Explain the requirements for secured communication
- > Explain various cryptographic algorithms such as private key and public key cryptography

On completion the student will be able to state the need for secured communication, they will be able to explain the requirement for secured communication and they will explain various cryptographic algorithm such as private-key and public-key cryptography.

Now let us focus on why you need secured communication for applications like ecommerce. The basic objective is to communicate securely over an insecure medium.

(Refer Slide Time: 03:41)

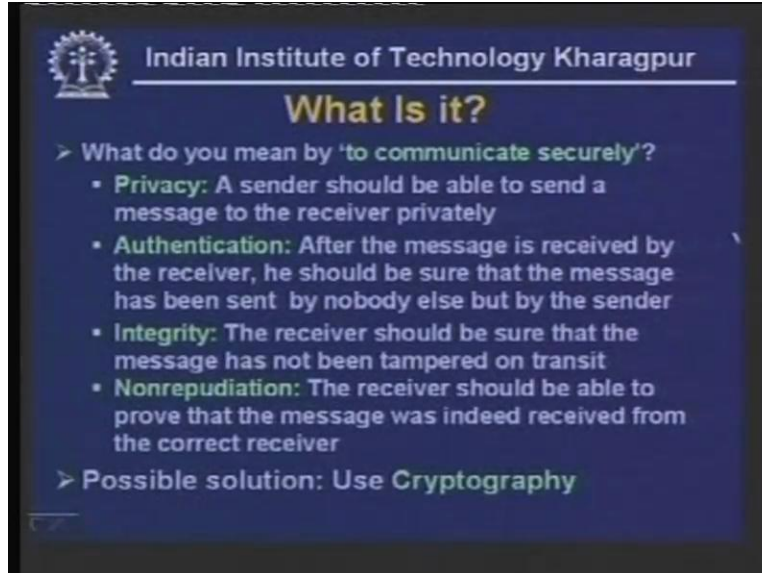


Essentially what we are trying to do is to communicate privately over public network. So whenever we use public network we encounter what is known as insecure medium. What do we really mean by insecure medium?

As the message is communicated through these links or communication media eavesdropper can listen in and try to tamper it so there are some people who can try to get hold of the message or make use them for their own benefit or tamper them.

Moreover, as we have seen in public communication network the information has to be stored in switches and routers before forwarding to the next node and in such cases information needs to be stored and then forwarded through packet switches. These switches can be programmed to listen to and modify data in transit. So these are the two problems that we encounter while communicating through public medium. So we have to find out the solution and solution is we have to develop techniques so that we can communicate securely over insecure medium. It involves four different aspects or four different components.

(Refer Slide Time: 05:17)



The slide is a presentation slide from the Indian Institute of Technology Kharagpur. It has a dark blue background with white and yellow text. At the top left is the IIT Kharagpur logo. The title 'What Is it?' is in yellow. Below it, a question 'What do you mean by 'to communicate securely'?' is followed by four bullet points: Privacy, Authentication, Integrity, and Nonrepudiation. A final point suggests 'Possible solution: Use Cryptography'.

Indian Institute of Technology Kharagpur

What Is it?

- What do you mean by 'to communicate securely'?
- **Privacy:** A sender should be able to send a message to the receiver privately
- **Authentication:** After the message is received by the receiver, he should be sure that the message has been sent by nobody else but by the sender
- **Integrity:** The receiver should be sure that the message has not been tampered on transit
- **Nonrepudiation:** The receiver should be able to prove that the message was indeed received from the correct receiver
- Possible solution: Use **Cryptography**

First one is privacy. A sender should be able to send a message to the receiver privately. What do you really mean by privately? By that we mean obviously this message will be exposed to other people but they will not be able to understand it. So it should be **intelligible un-intelligible** to others but it should be intelligible only to the person to which it is being sent.

Second is authentication. After the message is received by the receiver he should be sure that the message has been sent by nobody else but by the sender. So by authentication we mean that information message is coming from the intended sender and not from somebody else we do not know. This is known as authentication. So the security service has to provide this privacy and authentication.

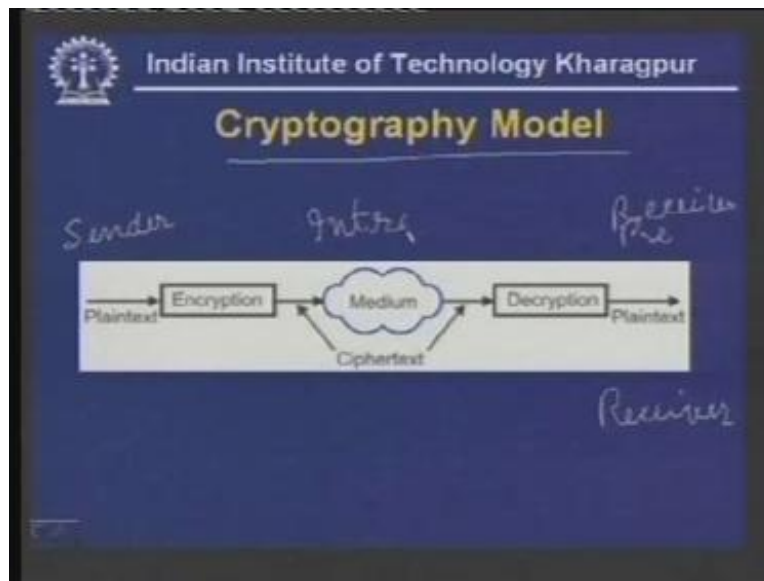
The third parameter or third component is integrity. The receiver should be sure that the message has been not tampered on transit. So by looking at the received message the receiver should be able to **sure** that message has not been modified or tampered on transit.

Finally the fourth important component is non repudiation. The receiver should be able to prove that the message was indeed received from the correct receiver. That means suppose a subscriber tells a bank to pay some money to a particular customer now over phone or over electronic medium after sometime he may come to the bank and say no I did not send it then it is the responsibility of the bank to prove that the person actually gave the instruction to pay. So, that is the function of non repudiation, these are the services to be provided by the secured communication network. And as we shall see possible solution is to use cryptography.

To achieve all these services we have to use cryptography. So in this lecture I shall try to give an overview of the various techniques used in cryptography.

First let us have a look at the cryptography model. In cryptography we require three characters. Actually to tell the story of cryptography we require three characters; one is the sender, another is the receiver. So here is the receiver and in between there may be an intruder

(Refer Slide Time: 8:45)



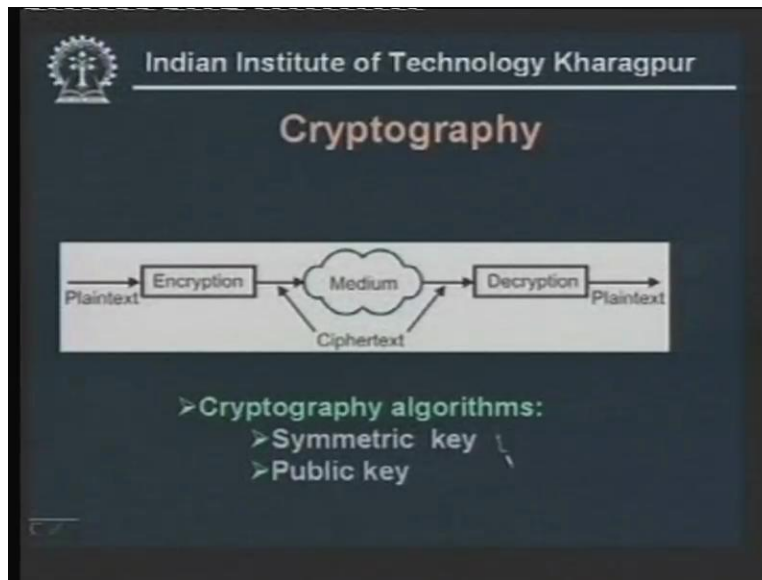
Usually we give three names. If you look at some textbook you will find Alice, Bob and Eve, these kinds of names from Europe is taken. But I shall borrow the characters from Ramayana. We shall consider the sender to be Sita, the receiver is Ram and on the other hand the intruder we shall consider as Ravana. So we shall use three characters Sita, Ram and Ravana to tell the story of cryptography.

Now a message is sent by the sender Sita known as plain text, usually that message is known as plain text and that is being encrypted and for encryption purpose a key is being used which is secret which is not known to Ravana or the intruder or the imposter which is in between. With the help of that key encryption is being performed and to do the encryption we have different algorithms. Actually the encryption can be done either by hardware or by software or a combination of both. And after doing the encryption, suppose this is the message (Refer Slide Time: 10:30) and encryption is done by Sita or you can say this is the key, we can say that the key that is being used generates a message modified message C is equal to encrypted by key and this is the plain text P .

So a plain text P which is the message is being encrypted to produce a modified message known as cipher text. So cipher text is being transmitted through the media which reaches the other end. And at the other end the receiver or Ram performs the decryption with the help of the same key or a different key so another key is being used for decryption so

decryption is being performed on C to get back P so C is decrypted to get key P. This is how the entire cryptography works. So a plain text generated by the sender or Sita is encrypted with the help of a key and after encryption the message is known as cipher text that is communicated through the insecure medium which reaches the other end and which is decrypted with the help of another key to get the plain text, this is the model for cryptography.

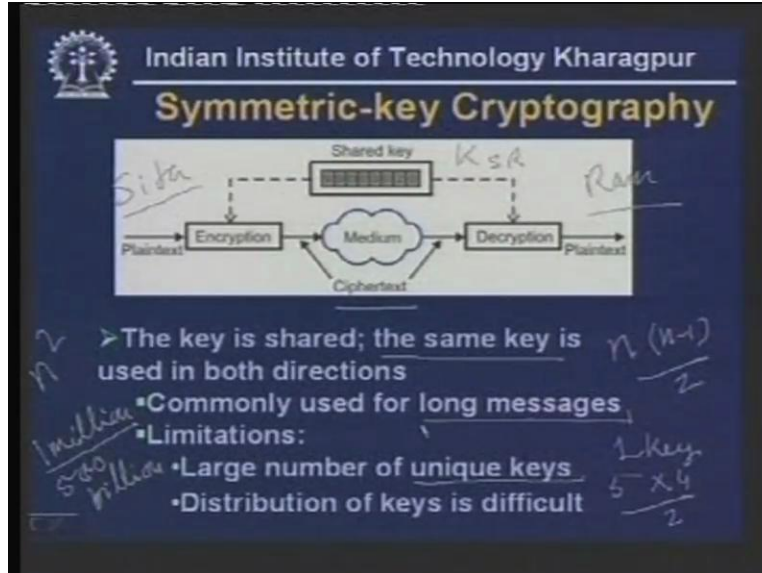
(Refer Slide Time: 12:15)



Now let us see what the various alternatives are. There are two basic approaches. One is known as symmetric key cryptography and the other is public key cryptography. There are two basic approaches we shall consider one after the other in detail.

In case of symmetric key cryptography a single key which is known as shared key is being used by both the parties. That means both Sita and Ram which are at the two ends they use the same secret key, let us name it SR being used by both Sita and Ram.

(Refer Slide Time: 15:36)



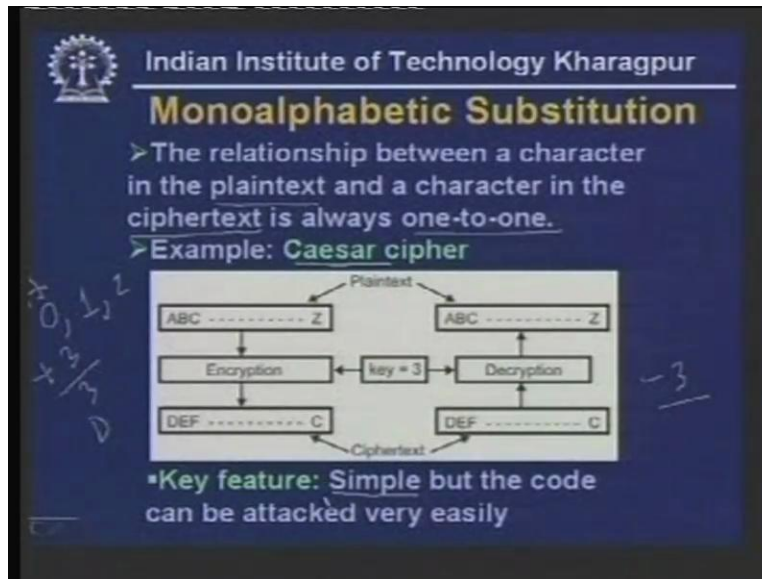
This particular key is known only to Ram and Sita and not by anybody else. And after doing the encryption by using this key K_{SR} this is being transmitted through the medium in the form of cipher text and as it reaches the other end the same key is being used for decryption to generate the plain text by Ram. So this is how the symmetric key cryptography works and as I have told it uses the same key in both directions. This is commonly used for long messages. When we have to use a long message say some text of few pages or some thing like that we can use this symmetric key cryptography.

It has got several problems. First of all it has got it will require a large number of unique keys. For example, if you have got two users you will require one key. So if you have 5 users how many keys will be required? It is 5 into 4/2 so you will require 10 keys and in general if you have got n users you will require **n into n minus by two** keys. That means if you have got say one million users then you will require 500 billion keys so that is the problem of this symmetric key cryptography. The total number of key is very, very large. Particularly when the number of user increases the number of keys also increase, this is known as n square problem.

Moreover, another problem is distribution of the keys you have to distribute so many keys secretly to all the users. That means this key K_{SR} should be known only to Sita and Ram but nobody else. So n square keys n into n minus 1/2 actually are to be known only to a pair of users, each will be known to a pair of users so this makes the distribution of keys very difficult. Moreover, each user has to store the key in the storage medium. for example, when you have got one million users you will require about one million storage space for each user to store the keys, actually it is one million minus 1 so one million minus 1 keys are to be stored by each user to store the keys if he wants to communicate will all the people. These are the problems we have to tackle. In the next lecture we shall discuss how it can be done.

First I shall discuss the traditional ciphers where the characters are used as the unit for encryption and decryption. as you know an ASCII character can be represented by 7-bit and of course if you use one bit parity so that makes it 8-bit so each character is of 8-bit and traditional ciphers performs the encryption character by character so the unit of encryption and decryption is in terms of character.

(Refer Slide Time: 19:10)



The unit of encryption and decryption is in terms of characters. The first one is monoalphabetic substitution. Here the relationship between characters in the plain text and a character in the cipher text is always one-to-one. That means for each character there is a unique character in the cipher text. For example, here the key that is used is 3, key is equal to 3. By that we mean in place of 'a' we shall use a character which is three characters away from 'a' that is 'd' and this was used by Julius Caesar that's why it is known as Caesar cipher. So Julius Caesar was not only a good soldier good fighter but he developed the cryptographic technique for secret communication and this was the technique that was being used.

So, if you are sending 'a' in place of 'a' 'd' will be used, in place of 'b' 'e' will be used, in place of 'c' 'f' will be used and so on so in this way when you use key it has to be done in this manner. Usually the characters can be represented by numbers. For example 'a' can be represented by numbers. For example, 'a' can be represented by 0, 'b' can be represented by 1, 'c' can be represented by 2 and so on. Now if you add 3 to it to the number that means 0 plus 3 will make it 3 so in place of 3 we shall be using 'b' in place of 'a'. Similarly when we do the decryption then you have to subtract 3. So we find that in case of this monoalphabetic substitution the encryption and decryption operation are just the opposite.

If we use addition for encryption we shall use subtraction for decryption, if we use multiplication for encryption we shall use division for decryption. So, for encryption plus

three is added to generate the cipher text and minus three is added with the cipher text to get the plain text. This is how the encryption and decryption is done. Obviously this is a very simple technique but the code can be attacked very easily because from the linguistic point of view each and every character appears with certain frequencies so frequency of appearance varies from character to character. For example, characters like 'e' 't' 'o' and 'a' appear more frequently than other characters. So based on that it can be easily found out, that's why it is not very popular.

Another approach that can be used is known as polyalphabetic substitution. In this particular case the relationship between a character in a plain text and a character in cipher text is always one to many not one-to-one.

(Refer Slide Time: 21:38)

Indian Institute of Technology Kharagpur

Polyalphabetic Substitution

- > The relationship between a character in the plaintext and a character in the ciphertext is always one-to-many.
- > Example: Vigenere cipher

Character in plaintext	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	W	R	K	D	O	V	C	A	S	B	Y	Q	M	L	H	I	T	U	F	E	Z	N	G	J	P	X
1	H	Q	B	G	W	E	R	K	F	C	O	A	Z	J	M	S	L	V	N	I	P	U	D	T	X	Y
2	P	I	D	Z	X	V	S	T	O	C	M	J	N	L	B	Q	R	U	W	K	H	G	E	F	A	Y
...
25	M	C	I	D	A	X	V	S	T	O	N	L	K	U	R	E	W	Z	H	F	P	G	Y	J	B	Q
Character in ciphertext																										

•Key feature: More complex and the code is harder to attack successfully

Mod 10
0
Mod 10
1
2

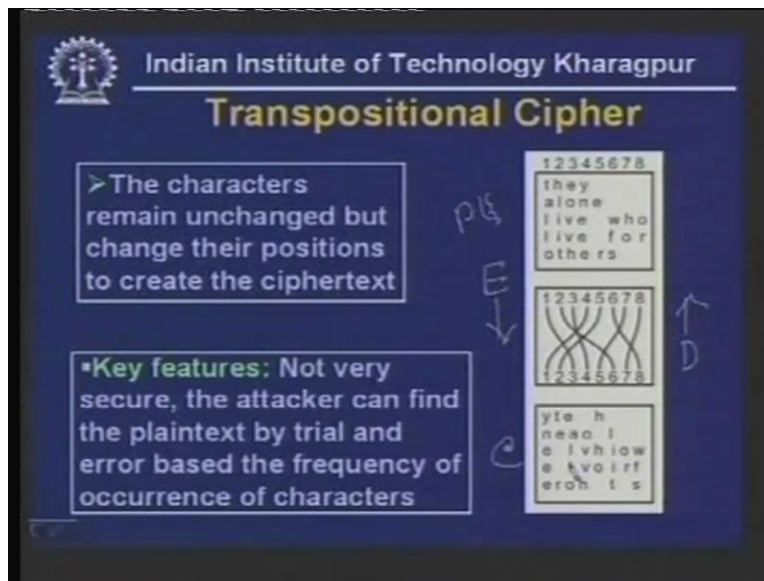
For example, in Vigenere cipher this polyalphabetic substitution is used. So as you can see here you can use a matrix and this matrix provides you information for performing the encryption. So the character 'a' is replaced by 'w' if it appears in the first row, character 'b' is replaced by 'r' if it appears in the first row, on the other hand if 'a' appears in the second row it is replaced by 'h' or if it appears in the third row it is replaced by 'p' or it can be represented mathematically. suppose you perform mod operation on the number, suppose you perform mod ten let's assume then the first character says 'a' is zero mod zero is zero so in the first row all the characters remain as it is, in the second row it is mod ten of one so it is one so 'a' is replaced by 'b', 'b' is replaced by 'c', 'c' is replaced by 'd' and so on so in this way up to ten rows it goes that means in the tenth row it will be added with mod 9.

Finally when it is row eleven then it will again added with one and then it will be substituted. So in this way we can perform poly alphabetic substitution that means each character is represented by different characters based on the appearance in different rows.

Obviously it is more complex than the Caesar cipher and the code is harder to attack successfully. Therefore, this gives you a better security compared to Caesar cipher.

Another approach that can be used is known as transpositional cipher. In this case the characters remain unchanged but change their position to create the cipher text.

(Refer Slide Time: 24:10)



In the previous case we have seen that the text was Sita and the letters s i t a are replaced by some other characters either in polyalphabetic or monoalphabetic substitution. On the other hand, in case of this transpositional cipher the same characters are used however their positions are changed. This is explained here.

For example, here this is the plain text, this is the plain text P and this has to be encrypted and the key is represented by this box which performs the transposition. So you can see here that if the character in column one is now placed in position three in the cipher text, the character in position two is placed in position six in cipher text and so on so this particular diagram represents that one is in position 3, 2 to 6, 3 to 4 and so on. This plain text (they alone live who live for others) gets transformed into this y t e h n e a o i l and so on. as you can see here t h u i they are present here but their position has changed so you are doing encryption by using this by changing the position and you can do the decryption by repositioning in the opposite manner and you'll get back this frame text. So here you get the cipher text from this plain text by using this transpositional cipher and you can get back the cipher text. So you can see it is not very secure, the attacker can find the plain text by trail and error based on frequency of occurrence of characters. So the positions can be altered by trail and error and it can be deciphered that's why it is not very popular.

Now we shall focus on block ciphers. So far we have seen in traditional cipher characters were used as the unit for encryption or decryption. Instead of that in block ciphers a block

of bits as unit of encryption is being used. The block of bits can be 64-bit or it can be 128-bit or it can be 256-bit that can be different for different encryption techniques but usually it is in terms of blocks of bits.

(Refer Slide Time: 26:05)

Indian Institute of Technology Kharagpur

Block cipher

- > Uses a block of bits as the unit of encryption and decryption *128-bit 64-bit 256-bit*
- > To encrypt a 64-bit block one has to take each of the 2^{64} input values and map it to one of the 2^{64} output values.
- > The mapping should be one-to-one

Diagram illustrating the encryption and decryption process:

Plain text (P): 01 — 1011 — 10

Key: [XXXXXXXX]

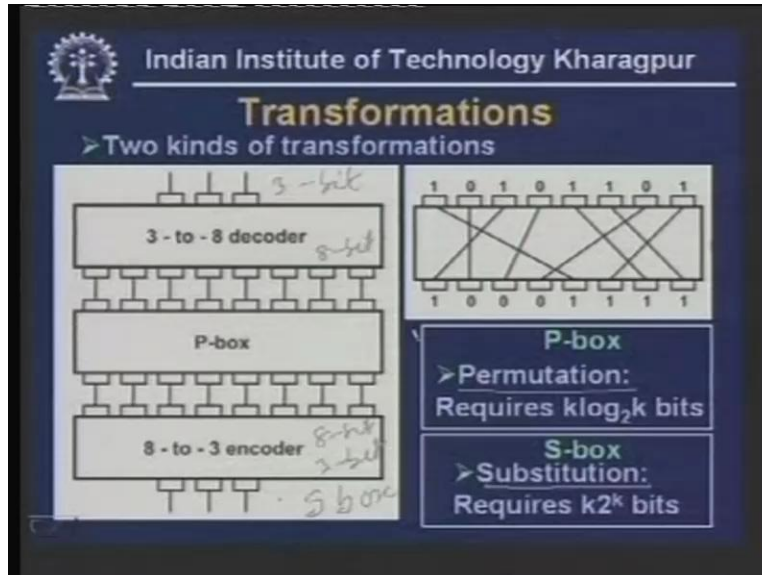
Encryption process: Plain text (P) is encrypted using the key to produce Cipher text (C): 10 — 0100 — 10

Decryption process: Cipher text (C) is decrypted using the key to retrieve the Plain text (P): 01 — 1011 — 10

So to encrypt a 64-bit block one has to take each of the 2 to the power 64 input values and map it on to 2 to the power 64 output values so here the mapping should be one-to-one as it is shown here. This is the plain text P which is encrypted by this key to get this cipher text C. Now you may be asking what is really meant by a key. What is a key? Key is essentially a number which is secret and it is known only to the sender and receiver or Ram and Sita in case of this symmetric-key cryptography.

So, by using this secret number encryption is done to generate this cipher text. This cipher text can be decrypted with the using the same key to get back the original plain text. Thus, the mapping from here to here has to be one to one and this mapping can be done by two transformations. One is known as permutation which can be performed with the help of either by hardware or software which is represented by P-Box.

(Refer Slide Time: 28:15)

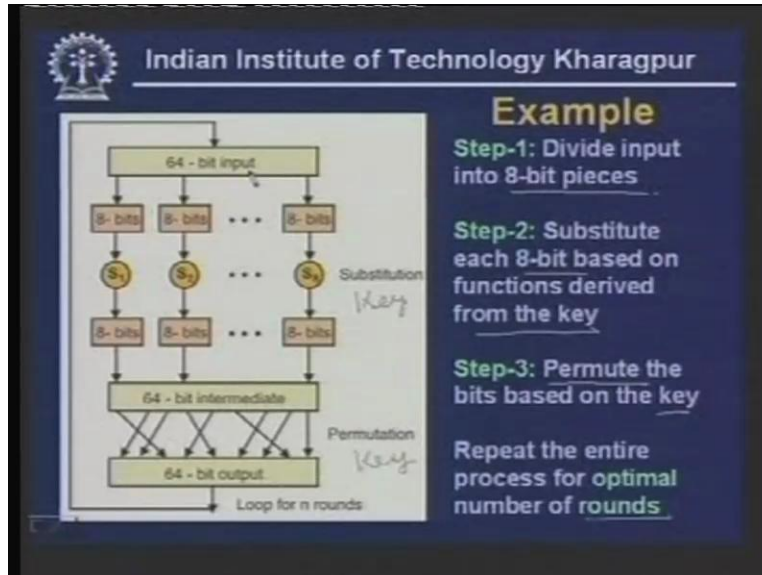


As you can see here this is the 8-bit input and this 8-bit input positions are permuted to generate a different number. So 1 0 1 0 1 1 0 1 gets transformed into 1 0 0 0 1 1 1 1 in the cipher text when it passes through the permutation box. And to represent this permutation operation you require $k \log_2 k$ bits. If you have got k bits and for each position you will require $\log_2 k$ bits to represent the position so you require total number of $k \log_2 k$ bits to represent this permutation operation. On the other hand, another transformation can be done which is known as substitution which can be done with the help of S box as shown here.

here this is the s box so here what is being done is, first with the help of a decoder it is converted into another number for example here you have got three bit input that three bit input is applied to a 3 to 8 decoder and it has got 8 outputs then this output is applied to a P box and this P box does the permutation and then it is applied to a 8 to 3 encoder which performs the reverse operation to get back three bits. Here you have got 8-bit input and 3-bit output (Refer Slide Time: 27:57). So here obviously the number is completely different and the substitution operations require k^{2^k} bits to represent the substitution operation on k bits.

So by using these two transformations you can encryption. I shall explain how it can implement an cryptography technique with the help of this permutation and substitution. Here we see how it has been done for a 64-bit input.

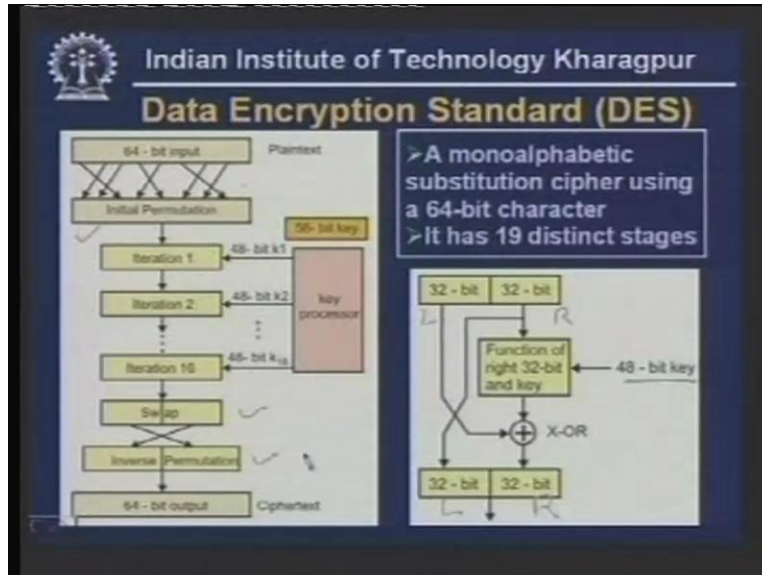
(Refer Slide Time: 30:12)



First it has been divided into 8-bit pieces. Hence, in step one the number is divided into 8-bit pieces. So in 64-bit you have got 8-bit pieces. Now substitute each 8-bit based on the functions derived from the key. So here you perform substitution based on a key and obviously here you get a different 8-bit number for each of these 8-bits. After this is being done you get 64-bit intermediate data, here eight 8-bits numbers are combined to get 64-bit intermediate data and this is being permuted with the help based on another key so permutation is performed again with the help of a key to get 64-bit output. Now you can perform several rounds of looping to improve the encryption technique, to increase the security of encryption.

Obviously the question arises how many rounds you will do. It has been found that as the number of rounds increase, the effectiveness of encryption increases however it should not be too large so you have to find out an optimal number of looping to do the encryption. Let us see a standard technique that is being used which is known as Data Encryption Standard or DES

(Refer Slide Time: 33:10)

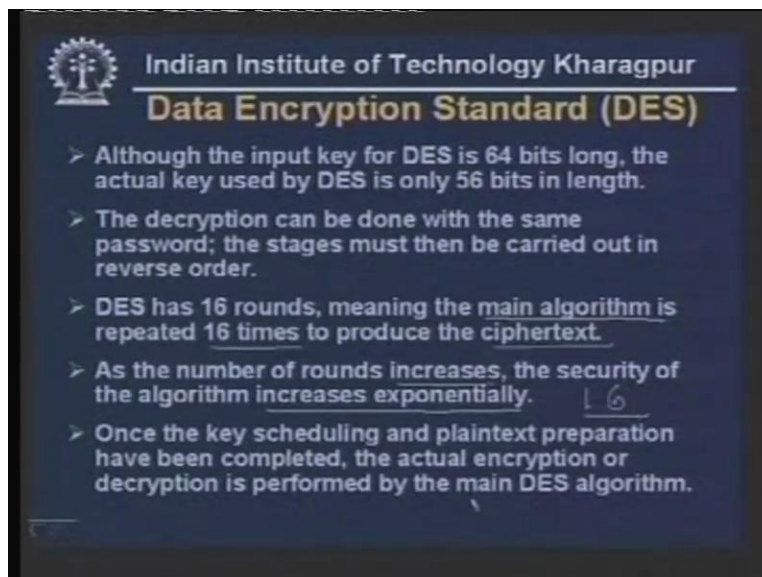


This was developed by IBM and subsequently it was adopted by the US government for use in encryption of non-classified data. How it works is explained here with the help of this diagram.

This is again a monoalphabetic substitution cipher using 64-bit character. So, input is a 64-bit character, this is the plain text (Refer Slide Time: 30:51) and first step is permutation. As you can see initial permutation is performed on this 64-bit input.

Here it is explained how it is being done.

(Refer Slide Time: 31:10)

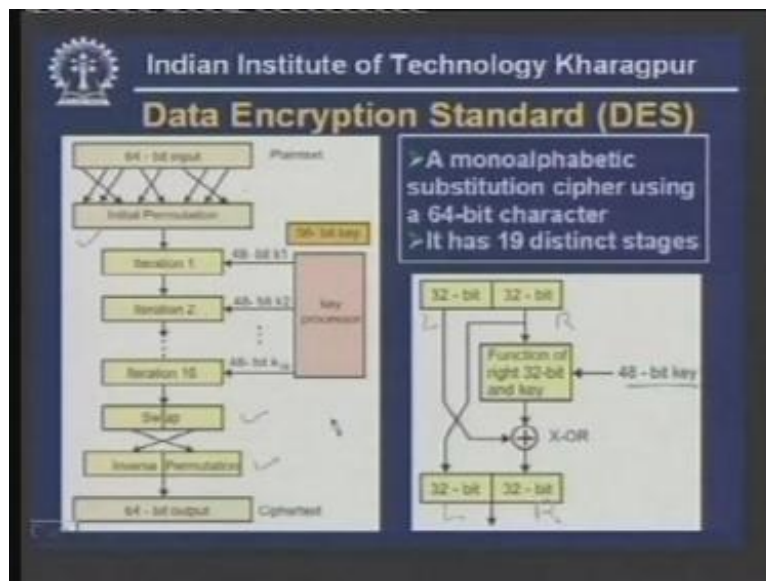


It has got sixteen rounds and the sixteen iterations are performed in this way. Although it has got 56-bit key actually a subset of bits are used as key one, key two and key sixteen to generate keys in different iterations. So with the help of a key processor this k1 to k16 are generated as the information passes through each iteration and in each iteration the operation performed is explained here.

Here (Refer Slide Time: 31:54) the 64-bit is divided into two parts say this is your left part and this is your right part so right part is swapped to the left part and as you can see the right part is encrypted with the help of that 48-bit key so this is the function of this right 32-bit and the key and this is being exclusive OR with the left 32-bit so we get the right 32-bit so we get right 32-bit and left 32-bit and this goes to the next iteration process and again the same operation is done but with a different key. So in this way after passing through sixteen such iterations the 32-bit, 32-bit are swapped and the inverse permutation which is opposite of this initial permutation is performed. So altogether as you can see it has got nineteen distinct stages starting with this initial permutation, sixteen different iterations and then swap and then inverse permutation so altogether nineteen distinct stages are there to generate the cipher text.

These are the typical features of this data encryption standard.

(Refer Slide Time: 33:18)



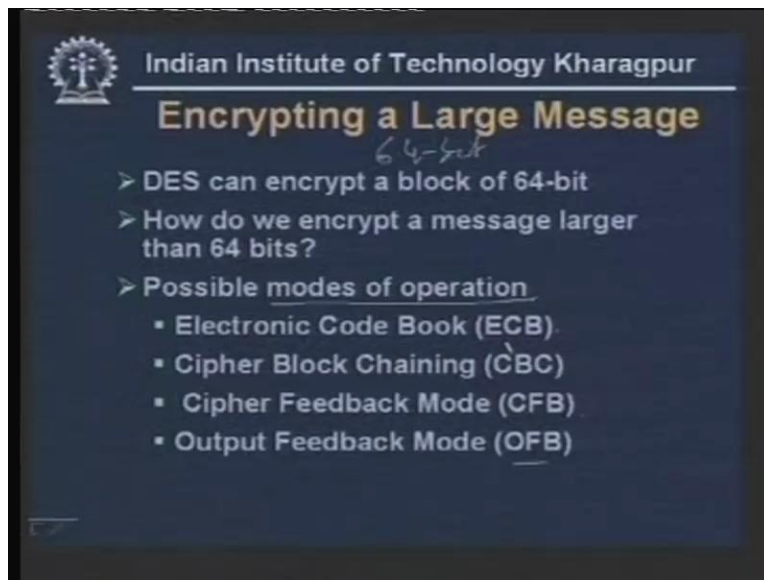
Although the input for data encryption standard is 64-bit long the actual key used by DES is only 56-bit and the other bits are parity bits. So parity bits are essentially used for error checking, they do not take part in generating the keys. The decryption can be done with the same password and the stages must then be carried out in reverse order. So, to perform the decryption operation you have to just do the reverse operation. So here inverse permutation has to be done (Refer Slide Time: 34:01) then swapping then it is

passed through the reverse process by using the same set of keys to get back the plain text.

DES has sixteen rounds meaning the main algorithm is repeated sixteen times to produce the cipher text. As the number of rounds increase the security of the algorithm increases exponentially. As you increase the round more and more security increases but there is some optimal number and in case of DES the optimal number selected was 16. Once key scheduling and the plain text preparation have been completed the actual encryption and decryption is performed by the main DES algorithm.

Although DES works for only 64-bit blocks of data there is need for encrypting large messages or sometimes small messages, how it can be done by using DES?

(Refer Slide Time: 35:45)



That can be done by using different modes of operation of DES. First one is known as;

- Electronic Code Book ECB
- Cipher Block Chaining CBC
- cipher feedback mode CFB and
- output feedback mode OFB

Let me discuss these four different modes of operation of DES. First one is known as Electronic Code Book ECB. This is the regular DES algorithm. Data is divided into 64-bit blocks. Since your message is long it is being divided into 64-bit blocks and each block is encrypted one at a time and separate encryptions with different block are totally independent of each other as it is shown in this diagram.

(Refer Slide Time: 37:37)

Indian Institute of Technology Kharagpur
Electronic Code Book (ECB)

➤ This is the regular DES algorithm. Data is divided into 64-bit blocks and each block is encrypted one at a time. Separate encryptions with different blocks are totally independent of each other.

P_1 64-bit P_1 : Plaintext block i P_2 ... P_n $P_i = P_j$

Encryption Encryption ... Encryption

C_1 C_2 ... C_n $C_i = C_j$

C_i : Ciphertext block i

Encrypt with secret key

So each plain text is 64-bit which generates a cipher text which is also 64-bit. Thus, here you perform some kind of mono alphabetic substitution, 64-bits number is encrypted to get another 64-bit number. As you can see for P_1 we get C_1 , for P_2 you get C_2 and for P_n you get C_n so here you have got n 64-bit inputs and we get n 64-bits output which is the cipher text block.

Here as you can see if P_i is same as P_j then C_i will be same as C_j , this is the drawback of this approach. For example, this may give a clue to the intruder or the Ravana. For example, there are ten persons who are getting the same salary so the intruder can find out those ten persons by looking at the cipher text because the cipher text also will be the same for those ten persons; the salary part will be the same.

In other words it can provide some information to the eavesdropper or intruder. So the message contains two identical blocks of 64-bit and the cipher text corresponding to this block also will be identical. This is not a very good approach.

(Refer Slide Time: 38:55)

Indian Institute of Technology Kharagpur

Disadvantages of ECB

- > If a message contains two identical blocks of 64-bits, the ciphertext corresponding to these blocks are identical. This may give some information to the eavesdropper
- > Someone can modify or rearrange blocks to his own advantage
- > Because of these flaws, ECB is rarely used

Another problem is someone can modify or rearrange blocks to his own advantage. For example, here these two in the cipher text, since they are independent C_2 and C_3 can be interchanged or C_4 and C_5 can be interchanged and at the other end the receiver will not know that this has been done but this can be used for different purposes. Suppose if somebody wants to increase his salary may be it was 16000 he can make it 61000 so this kind of thing can be done and as a result this ECB or Electronic Code Book method is not very safe and as a consequence because of these flaws ECB is rarely used. Thus, to overcome this problem the second approach can be used which is known as Cipher Block Chaining CBC.

(Refer Slide Time: 41:25)

Indian Institute of Technology Kharagpur

Cipher Block Chaining (CBC)

> In this mode of operation, each block of ECB encrypted ciphertext is XORed with the next plaintext block to be encrypted, thus making all the blocks dependent on all the previous blocks. The IV is sent along with data.

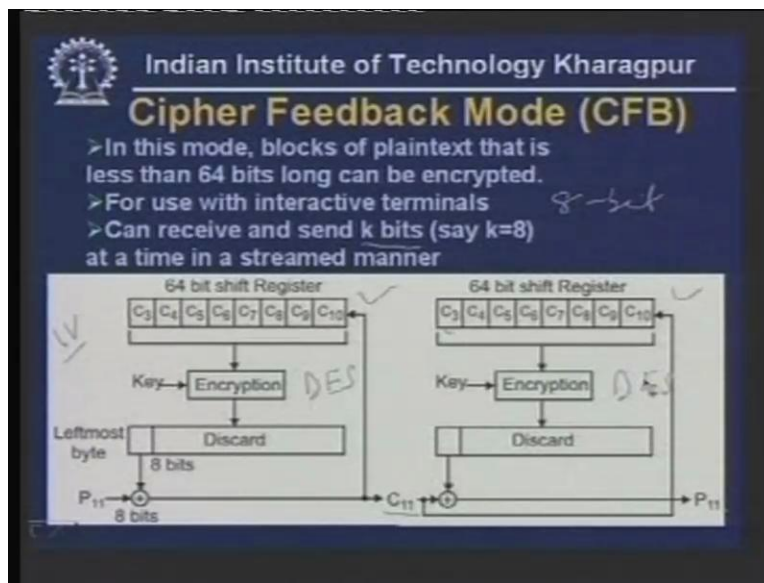
```
graph TD
    IV[Initialization vector] --> X1((+))
    P1[P1] --> X1
    X1 --> E1[Encryption]
    E1 --> C1[C1]
    C1 --> X2((+))
    P2[P2] --> X2
    X2 --> E2[Encryption]
    E2 --> C2[C2]
    C2 --> X3((+))
    Pn[Pn] --> X3
    X3 --> En[Encryption]
    En --> Cn[Cn]
```

In this mode of operation each block of ECB encrypted ciphertext is XORed with the next plain text block to be encrypted. For example, here initially a random number is chosen which is initialization vector or IV. So, that IV is generated randomly a 64-bit number is generated and that is XORed with P_1 and then that number is encrypted to get C_1 then C_1 is XORed with P_2 to get a number which is encrypted to get C_2 . So here depending on the initialization vector C_1 will be different for different cases and also C_1 is exclusive OR with P_2 and then encrypted by using the data encryption standard. So by using DES the encryption is being done and C_2 is used to perform exclusive OR with P_3 and so on. Thus P_n is encrypted with C_{n-1} and then exclusive ORed to do the encryption to generate C_n .

In this case suppose if P_i and P_j are same C_i and C_j will not be same they will be different and as a consequence the problem that we encountered in the previous case the ECB Electronic Code Book does not appear in case of this Cipher Block Chaining CBC method. So here (Refer Slide Time: 40:54) this makes all the blocks dependent on the previous blocks and the only extra thing that has to be done is the initialization vector has to be sent along with data. That means apart from sending the cipher text C_1, C_2 and C_n you have to send the IV initialization vector to the receiving end so that the decryption can be done by using the same initialization vector which is a random number. New numbers are generated for different situations.

There are situations where the size of the plain text is smaller than 64-bit. In the previous two cases we have seen we cannot do encryption unless each of these plain text block is of 64-bit.

(Refer Slide Time: 44:18)



Now suppose from an interactive terminal data is coming out at the rate of one character or 8-bit in such a case how do you use DES that can be done by using this Cipher

Feedback Mode or CFB. So it can receive and send 8-bits say k is equal to 8 at a time in a streamed manner so $8/8$ can be generated. How it works? Again in this case also we use an initialization vector, that initialization vector is loaded in a 64-bit shift register and that is being used initially to do the encryption by using DES and after encryption and only the left most byte of the cipher text we get is used to perform exclusive OR with the character or at that moment.

Therefore, here as you see that is being Exclusive ORed to get the cipher text. So in this way character by character it is being done and then this number is loaded in the shift register so as you can see here after ten such characters have been encrypted this is the snapshot (Refer Slide Time: 43:14) so $C_3, C_4, C_5, C_6, C_7, C_8, C_9$ and C_{10} are already there and this 16-bit number is used as for encryption with the key and this is being encrypted and the left most 8 byte of the resultant number is used to get the cipher text by using exclusive OR with the plain text. So this is how it is being done.

On the other hand, at the receiving end, this is the receiving end (Refer Slide Time: 43:45) so in the receiving end the exclusive OR is being performed to get the cipher text and of course as long as this number and this number is same you will get back the plain text P_{11} . This is also a snapshot after decrypting ten characters. When the eleventh character is getting decrypted this is the situation. So, in a streamed manner character by character encryption can be done again by using DES.

Now let us consider the output feed back mode. This is also a stream cipher and encryption is performed by XORing the message with the one time pad.

(Refer Slide Time: 46:08)

Indian Institute of Technology Kharagpur

Output Feedback Mode (OFB)

- > OFB is also a stream cipher
- > Encryption is performed by XORing the message with the one-time pad

- > One-time pad can be generated in advance
- > If some bits of the ciphertext get garbled, only those bits of plaintext get garbled
- > The message can be of any arbitrary size
- > Less secure than other modes

64 bit shift Register

Key → Encryption

Discard

8 bits

m_i ⊕ c_i

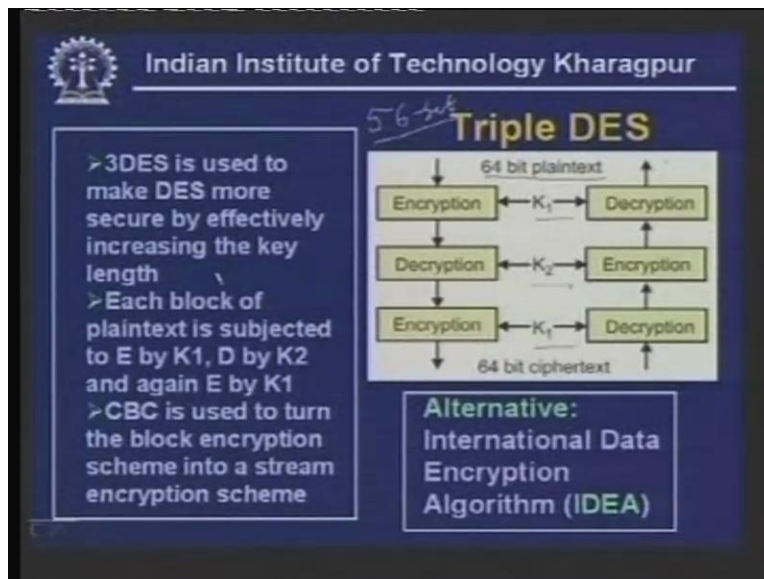
Here the entire process is somewhat similar to the previous case. However, here as you can see after encrypting the left most 8-bit is exclusive ORed with the plain text to get the cipher text and instead of the cipher text the output of this encrypted 8-bit data is applied

to the shift register. As a consequence it is not dependent on the plain text. that means this one time pad can be generated before hand and then exclusive OR can be performed as the bits are received bit by bit to generate the data. So bit by bit exclusive OR operation can be done with the plain text.

In this particular case if some bits of this cipher text get garbled only those bits of the plain text get garbled because here bit by bit operation is being performed. And in this case another advantage is the message can be of arbitrary length, it need not be even multiples of 8-bit but it can be 6-bit, 7-bit, 2-bit or any number because here you are performing bit by bit operation. And at the receiving end also one time pad can be generated then exclusive OR operation can be performed with the cipher text to get back the plain text. However, this is a less secure method than the other modes of operation that we have discussed. As a consequence this output feedback mode is rarely used unless it is absolutely necessary.

One limitation of this Data Encryption Standard is the small size of the key. We have seen the key size is only 56-bit and as a consequence it is not very secure, that was the limitation pointed out by the critics of Data Encryption Standard.

(Refer Slide Time: 48:05)



So what was done was to improve the effectiveness of this encryption the key length was increased not directly increasing the key length or changing the size of the plain text but the triple DES, 3DES technique was developed. What is being done here is each block of plain text is subjected to encryption followed by decryption followed by encryption by using two keys K1 and K2 and again K1. So this effectively increases the size of the key. You can say that 56 into 3 is the size of the key although you are changing the basic algorithm that is being used by data encryption standard so you are performing the standard DES algorithm which operates on 64-bit plain text and the keys are of 56-bit but

you do it in chain one after other that means encryption decryption encryption to generate the 64-bit cipher text.

Then again decryption can be done in the reverse order; decryption encryption decryption to get back the plain text. So this particular approach gives you much better security. There is no known method for breaking this code. You can use CBC Cipher Block Chaining whenever the size of the data is long. So CBC is used to turn the block encryption scheme into stream encryption scheme when you have got messages of 64-bits.

We have discussed the symmetric-key encryption technique of cryptography technique where we have seen for a pair of users you require a single key and we have large number of users. To overcome this problem there is a more recent method known as public-key cryptography.

In this particular case two keys are used for encryption and decryption. The two keys are known as public-key and private-key. Here for example Sita is trying to send a plain text so C does encryption with the help of the public key of the Ram, this is the receiver Ram (Refer Slide Time: 49:30) so by using the public key of Ram encryption is being performed to generate the cipher text then it is sent over the medium to the other end and Ram receives it and does the decryption by using the private key.

(Refer Slide Time: 52:18)



As you can see in this particular case this public key is for the rest of the world and private is the secret key that is being used by the receiver. So here we can see the pair of keys is used with any other entity. That means instead of Sita if somebody else wants to send another message they can use the same public key to perform encryption and send it to Ram. As long as the private key is not disclosed and it is known to Ram, Ram can decrypt the entity or message sent by any other person apart from Sita when it is

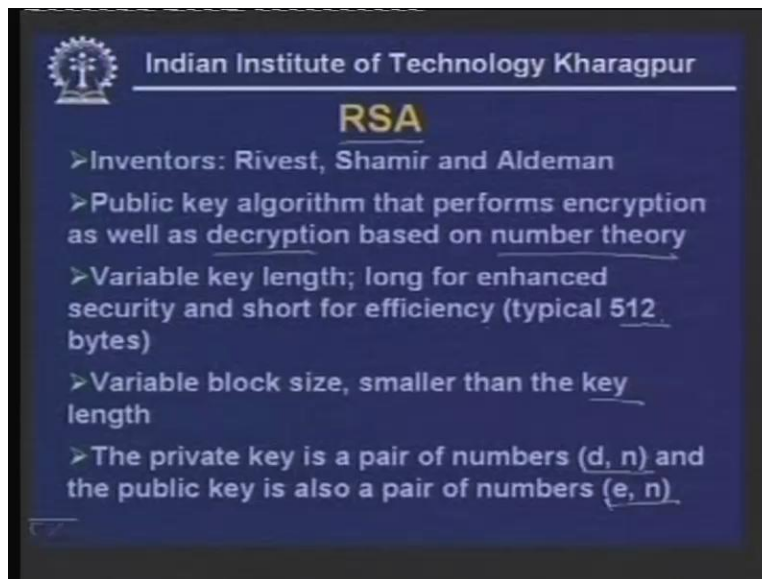
encrypted by the public key of Ram. So in this particular case the number of keys required is very small. Suppose you have got n users you require only two n keys. So, if you have got one million users you will require two million keys in case of this public key cryptography.

The main difference as we can notice here is instead of using the same key for encryption and decryption you are using two different keys; one is public key and another is private key for encryption and decryption. That is the basic difference between the public key cryptography and symmetric key cryptography.

Now question arises what is disadvantage or advantage of this technique. Advantage as you have noticed is the number of keys required is small and the main disadvantage is that it is not efficient for long messages because the encryption technique is quite complicated. However, another problem present here is the association between an entity and its public key has to be verified. That means this public key is received may be through network. So the public key whether it is coming from Ram or somebody else that is the imposter has to be verified. Otherwise this will fail that means in this particular case this verification of this public key has to be performed before using it for encryption.

One popular approach for public key public key cryptography is RSA technique. It was invented by Rivest, Shamir and Aldeman. This public key algorithm that performs encryption as well as decryption is based on number theory.

(Refer Slide Time: 53:30)

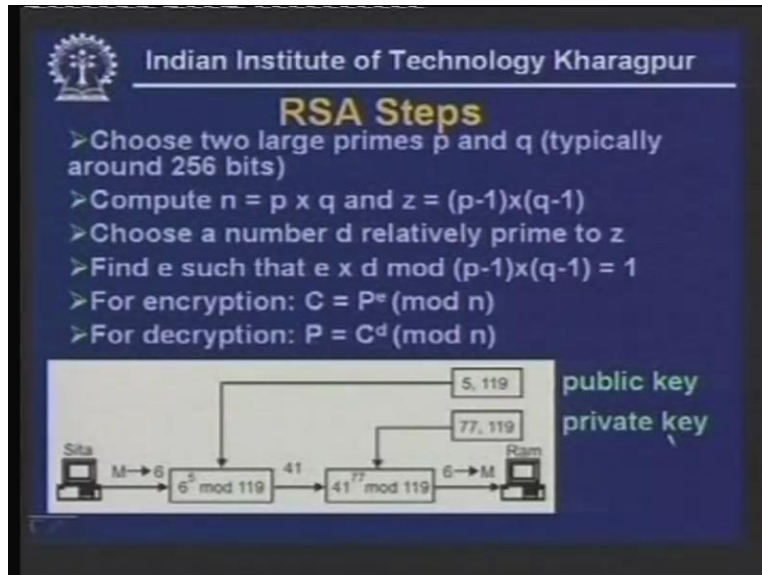


This RSA algorithm is based on number theory and it can perform variable key length; long for enhanced security and short for efficiency. That means the size of the key is not fixed here it can be long or small depending on the security level that you want or the size of the message. And typically the size of key is 512 bytes and variable block size can be used. However, it has to be smaller than the key length. So if it is 512 bytes the key

length has to be smaller than that. The private key is a pair of numbers (d, n) and the public key is also a pair of numbers (e, n).

So using this (d, n) encryption is done and decryption can be done by using (e, n). So here it chooses two large primes p and q typically around 256 bits then compute n is equal to p into q and z is equal to p minus 1 into q minus 1 and third step is choose a number d which is relatively prime to z which is p minus 1 into q minus 1.

(Refer Slide Time: 55:25)

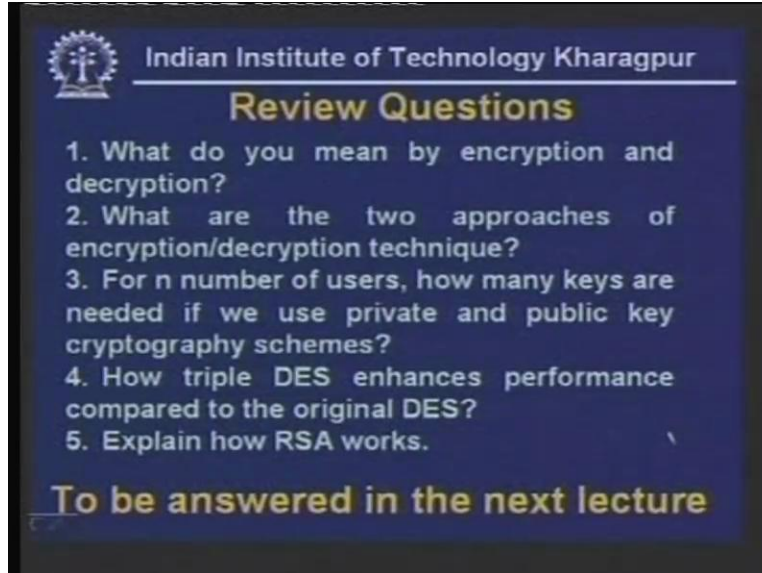


Find e another number such that e into d mod p minus 1 into q minus 1 is equal to 1. Then for encryption you should use c is equal to p to the power e mod n and for decryption one can use p is equal to c to the power d and mod n. this is illustrated with an example.

As you can see 5 and 199 is the public key that is being used for encryption so the message or the plain text sent by Sita is 6 so 6 to the power e is 5 here mod one mod one 119 is 41 that is the cipher text C and C is sent to Ram and the decryption is performed by using c to the power d so 41 to the power 77 because here d is 77, mod is 119 and to get back the plain text 6, this is the message received by Ram. This is how encryption and decryption can be done and here you can see (Refer Slide Time: 55:02) the advantage is the keys can be generated both d and e and d n e these are all known but in spite of that it cannot be broken **by the Ravana**s.

Now it is time to give you the review questions.

(Refer Slide Time: 55:28)



Indian Institute of Technology Kharagpur

Review Questions

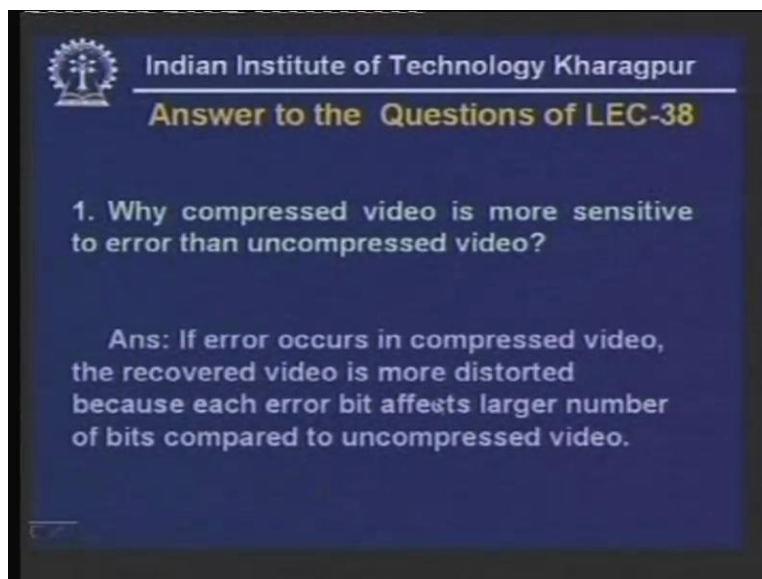
1. What do you mean by encryption and decryption?
2. What are the two approaches of encryption/decryption technique?
3. For n number of users, how many keys are needed if we use private and public key cryptography schemes?
4. How triple DES enhances performance compared to the original DES?
5. Explain how RSA works.

To be answered in the next lecture

- 1) What do you mean by encryption and decryption?
- 2) What are the two approaches of encryption decryption technique?
- 3) For n number of users how many keys are needed if we use private and public key cryptography schemes?
- 4) How triple DES enhances performance compared to the original DES
- 5) Explain how RSA works.

Here are the answers to the question of lecture minus 38.

(Refer Slide Time: 56:02)



Indian Institute of Technology Kharagpur

Answer to the Questions of LEC-38

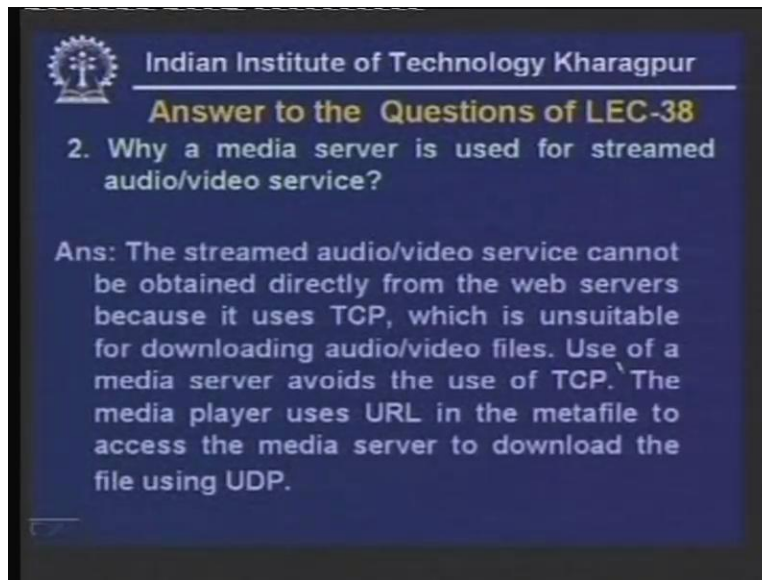
1. Why compressed video is more sensitive to error than uncompressed video?

Ans: If error occurs in compressed video, the recovered video is more distorted because each error bit affects larger number of bits compared to uncompressed video.

1) Why compressed video is more sensitive to error than uncompressed video?

The main reason is if error occurs in compressed video the recovered video is more distorted because each error bit affects larger number of bits compared to the uncompressed video. That means if smaller number of bits affect larger number of bits after recovering that that's why it is more sensitive.

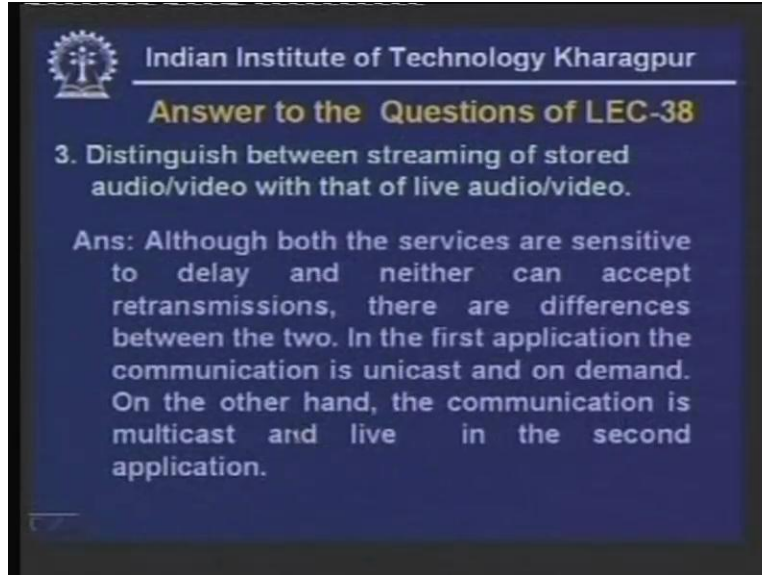
(Refer Slide Time: 56:35)



2) Why a media server is used for streamed audio/video service?

We have seen that the streamed audio/video service cannot be obtained directly from the web servers which use TCP and TCP cannot be used because the error control techniques used in TCP is unsuitable for downloading audio/video files so the use of media server avoids the use of TCP. However, the media player uses the URL in the metafile to access the media server to download in the UDP so UDP does not use the error control and other things and as a consequence it is very suitable for streamed audio/video service. That is why a media server is needed which does not use TCP instead of that it uses UDP.

(Refer Slide Time: 57:31)

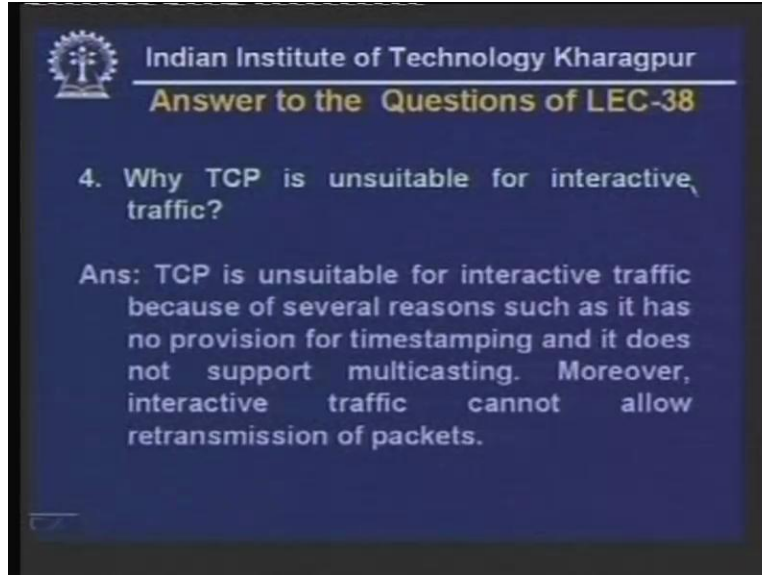


3) Distinguish between streaming of stored audio/video with that of live audio/video.

We have seen that although both the services are sensitive to delay and neither can accept retransmissions. There are differences between the two. In the first application the communication is unicast and on demand. That means whenever you are streaming of stored audio and video usually it is unicast.

A person is requesting for some service and as a consequence it is unicast and usually on demand. On the other hand, when are performing live audio/video transmission streaming of live audio/video it is multicast in nature and it is live in the second application. So these are the key differences between the two although both are sensitive to delay.

(Refer Slide Time: 58:28)

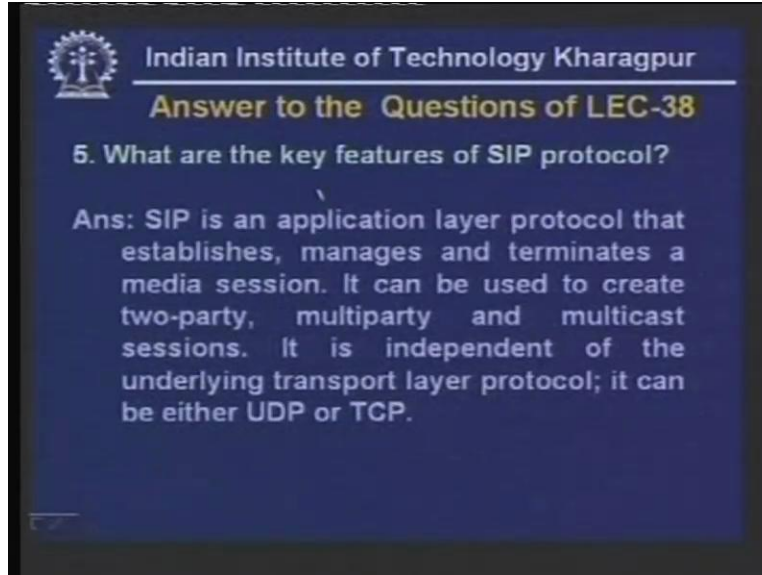


4) Why TCP is unsuitable for interactive traffic?

TCP is unsuitable for interactive traffic because of several reasons such as it has no provision for timestamping and it does not support multicasting. These are the limitations of TCP. On the other hand, for interactive traffic these are the two services needed. Moreover, interactive traffic cannot allow retransmission of packets which is used in TCP in case of error.

As we know whenever error occurs it does retransmission that cannot be done in case of interactive traffic that's why TCP is unsuitable for interactive traffic.

(Refer Slide Time: 59:10)



5) What are the key features of SIP protocol?

SIP is an application layer protocol that establishes, manages and terminates a media session. It can be used to create two-party, multiparty and multicast sessions. It is independent of the underlying transport layer protocol; it can be either UDP or TCP.

In this lecture we have discussed the cryptographic techniques. In the next lecture we shall discuss how these techniques can be used to provide the four services I have mentioned.

Thank you.