

Internet Technology
Prof. Indranil Sengupta
Department of Computer Science and Engineering
Indian Institute of Technology, Kharagpur
Lecture No #32
Basic Cryptographic Concepts – Part 1

In this lecture we shall be continuing with our discussion on network security. If you recall in our earlier lecture we had talked about intranets extranets and firewalls. Now today in this lecture first we shall talk about some of the general network security threats that we typically encounter followed by some discussion on some basic cryptographic techniques.

(Refer Slide Time: 01:24)



So let us start by some of the basic concepts in network security.

(Refer Slide Time: 01:34)

The slide is titled "Security Attacks" and features a logo in the top left corner. The content is as follows:

- Any action that compromises the security of information.
- Four types of attack:
 - Interruption
 - Interception
 - Modification
 - Fabrication
- Basic model:

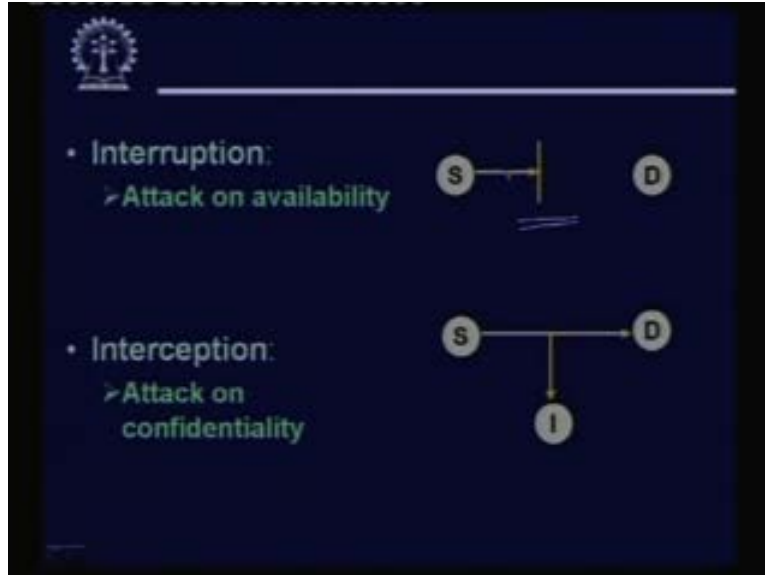
```
graph LR; S((S)) --- D((D));
```

Source Destination

We start with the different kind of generic security attacks that we typically encounter in a network or in a computer system. Now a security attack can be defined rather loosely by any action that compromises the security of information. Now when you say security of information we are not specifically telling where the information is located. And also when we talk about the security of information we also do not specify what kind of security it encompasses the entire range. It can be something related to security or secrecy of information. Security and secrecy are not always the same.

So some time we may want to hide some information; sometime we may want to know who is sending the information or sometime due to some security attack we may be denied our right to access some information. So, all these issues collectively fall under the area of security threats. So talking about attacks we can classify attacks into four types; interruption, interception, modification and fabrication. Let us try to explain these four kinds of attacks with the help of a basic model where we have a source S and a destination D. S wants to send some information to D. So on this model let us try to explain these four kinds of attacks.

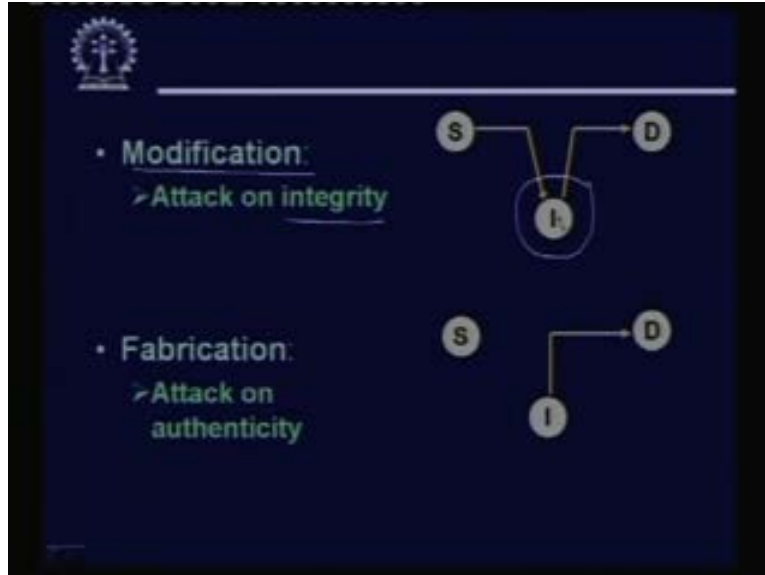
(Refer Slide Time: 03:15)



Interruption means somehow the source is not allowed to access or send the information to the destination D. This can be information; this can be a request for information also. So we really do not classify you are really not distinguish what kind of data is being transmitted. It can be the actual information or request for some information. So interruption means this is some kind of an attack on availability. Some information or resource may be available on D and S wants to access due to some interruption activity, due to some interruption activities. Somehow the sender or the source is unable to make that access to complete that request. Now this kind of attacks have taken place in networks where a group of hackers, if they coordinate among themselves they can possibly bombard a particular website with junk packets.

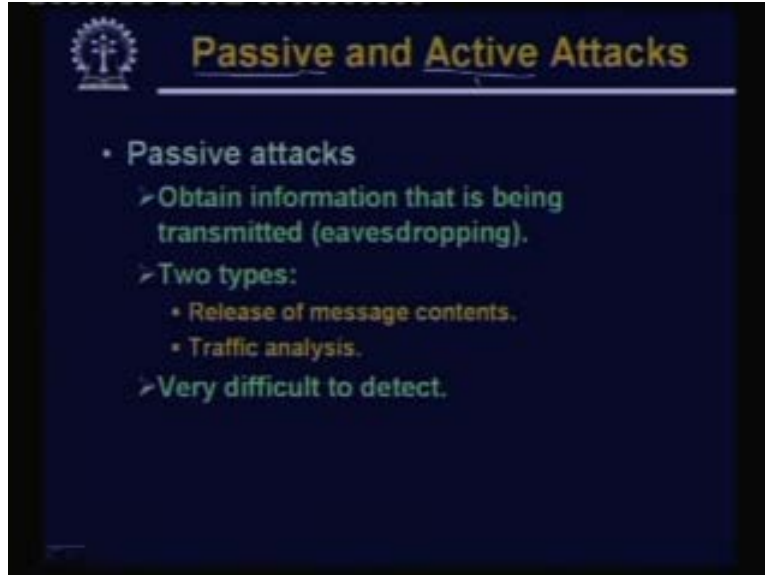
So actually what will be happening is that the website the http server software will be busy handling these junk packets. Suppose I am a legitimate, user I am trying to send a request for some information. So my request will get queued up at the back of a long queue of junk packets and effectively I am unable to access the information. So this is the attack on availability. Then we can have interception. Interception means source is sending. But some intruder sitting out here is also reading out the information that is being transmitted. This is attack on confidentiality. This kind of attack is impossible if the intruder gets access to some intermediate network points like router say. So all packets has to flow through the router. So if the router is hacked, so all information content of the packets will get disposed.

(Refer Slide Time: 05:25)



The third type is modification. This is an attack on integrity say. Here again I am assuming that the intruder has access to some intermediate network node like the router. But here the intruder is doing something more than just passively listening to the packets. The intruder is reading out the packets making some modifications, then sending it forward to D. So the content of a packet is getting modified on its way. And the last kind of attack we are calling fabrication. This is attack on authenticity. Here the intruder was possibly watching the communication S and D were making. After looking at or analyzing a number of such communications what I can possibly do now is, I can fabricate a new packet and can send it do D. In a way D will made to believe that the packet is actually coming from S. So this is an authenticity problem, the destination has to somehow verify that actually from whom the packet is coming. If authentication is not good then the destination may be misguided.

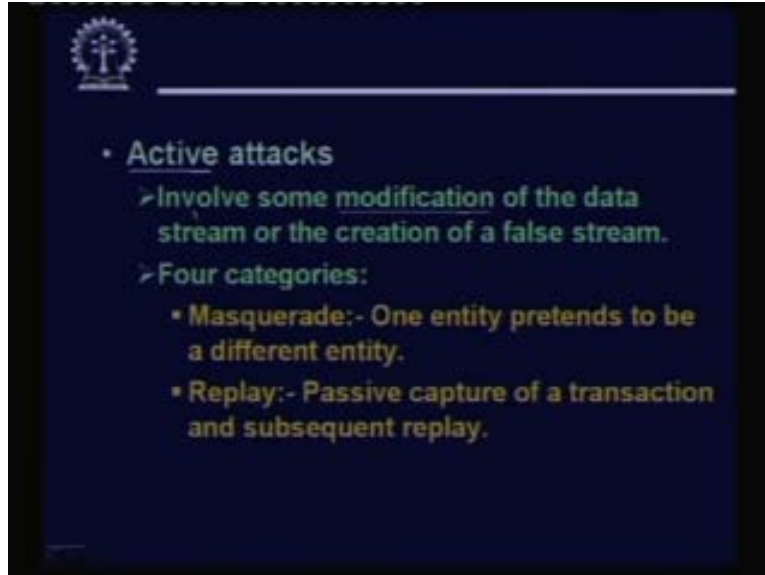
(Refer Slide Time: 06:51)



So these are all the different kinds of attacks. Now attacks can also be classified as whether they are passive or active. Now this is a different kind of classification. Say earlier the four types of attacks that we talked about that is, just the four kinds of attacks. But in terms of the way information is modified or accessed we can classify them as passive or active. Now passive attacks as the name implies they do not make any changes. They passively listen to something obtain information that is being transmitted. Now here the intruder is simply looking at the contents of the packets that are flowing from one point to the other. Now there are two kinds of information. The intruder might be able to reveal out of these packets or the contents of these packets. One is of course what the body of the packets contains. This is so called release of message contents.

Second one is also equally important. This is called traffic analysis. Like an intruder somehow has gained access to my network just by passively looking at the packets flowing. The intruder tries to understand or tries to know that which server in my network is the most frequently used. Now in this way the intruder can identify the so called vulnerable points in my network if it can identify that. These are the three servers or computers which are most widely used. So if someone I can bring them down the damage I can make to the network as a whole will be the maximum. So traffic analysis is also a very valuable you can say tool or information to the intruder. And since here no modification is being made anywhere. These kinds of attacks are very difficult to detect.

(Refer Slide Time: 09:08)



Now in contrast we can have active attacks where some kind of modification takes place in the data packets. Now under active attacks, some of this we have already seen. We can classify these attacks into again a number of categories. First one is that authentication attack masquerade, one entity pretends to be a different entity. So in this way the entity makes some modification to the packet or fabricates a packet out of here so that the destination is made to be believed that the packet is actually coming from a legitimate center. Replay attack is also quite dangerous. The intruder can passively capture a set of packets which can constitute a transaction and can subsequently replay them to the server. Now for example while I am logging into a server I am typing in my password or some other authentication information. If some intruder was passively listening to all the packets during this time, then later on the intruder can also try to gain access to this server by supplying the same packets, that I was sending the login information and other details. This is the so called replay attack.

(Refer Slide Time: 10:35)



Modification is of course some changes are made to the packet. And denial of service is also considered to be an active kind of attack because we are logically making some active change in the performance of the network. Some data are being stopped to flow beyond a point or such things.

(Refer Slide Time: 11:02)

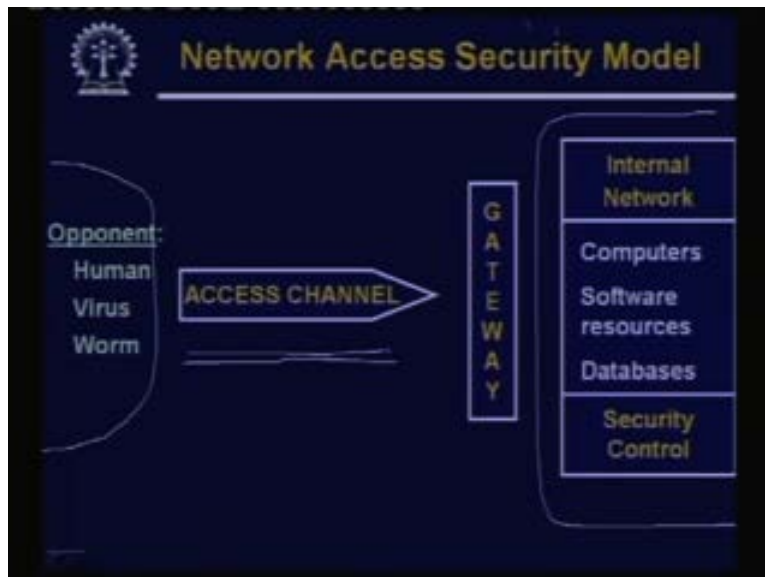


Now looking from the point of security service. Actually from users point of view. What are the different kinds of services I require? So here we can talk of several things. One is confidentiality or privacy there may be requirement that whatever I am sending I do not want an intruder to gain access to that. Second is authentication the receiver wants to

verify that who actually created or has transmitted the data. Third one is integrity suppose I am downloading a program code from somewhere I would like to verify whether or not. This is the original version or someone has modified this. So as to include a virus program code inside it. This is the integrity problem to verify whether the message has not been altered. Non repudiation is a service which says, suppose using some security mechanism. I put my signature digitally on some document. Later on I cannot deny that will that is not my signature.

So non repudiation means the system is such that once someone signs on a document by digital signature or some thing equivalent the system should be so robust and safe that he or she cannot deny it later. It is not possible for someone else to forge that signature. Of course access control is one service I want to prevent misuse of resources. I want to have a tag of who are the users of this system and of course availability is service. One of them I have already mentioned, denial of service attack or virus programs that can delete files make some folders inaccessible. These are all different kinds of security services that we may want. Now depending on the kind of application you may decide that among them which are the security services that are important to your organization or to individuals who are there on the network and you can accordingly set and implement the security policies.

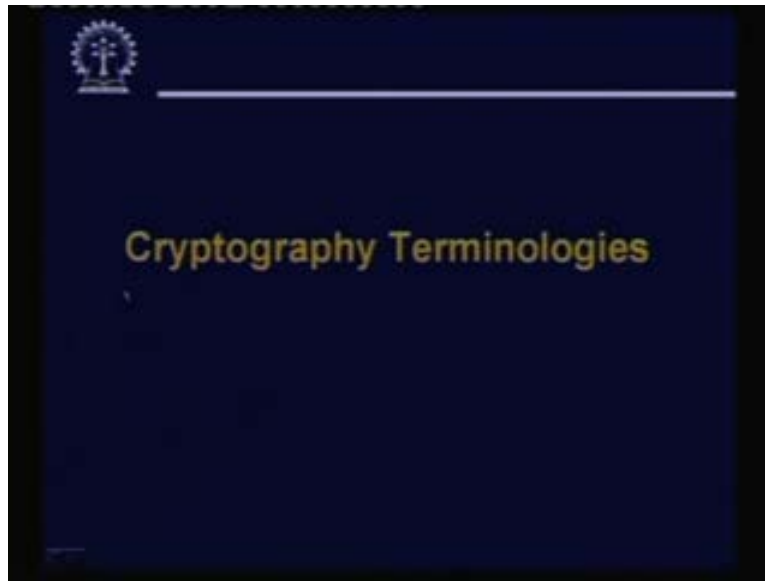
(Refer Slide Time: 13:30)



Here we will look at a generic network access security model. Now this model is like this. On this side we have our internal organizational network. This is the outside world. Here we have the channel through which the data is flowing and gateway is like a firewall that is protecting our organization network. Now this model shows the different components of the system. Like the access channel is of course the medium through which the packets or the information is flowing. Gateway is an entity which is trying to filter the contents as they flow, internal network they consists of computers, software resources, databases. They may all be guided by some security control mechanisms and I

am assuming that from the outside world they are all opponents who are trying to break into our system or to access our resources in a way which we do not want. Now these opponents can be human hackers they can be automated systems like viruses or worms. So we should be careful against all this different kinds of opponents like a human hacker can mount actual attacks on our network by trying and transmitting packets. Now a worm or a virus might get into a system if we download an email attachment which contains some malicious code. So we should be very careful about what we are downloading and what we are opening on our machines.

(Refer Slide Time: 15:24)



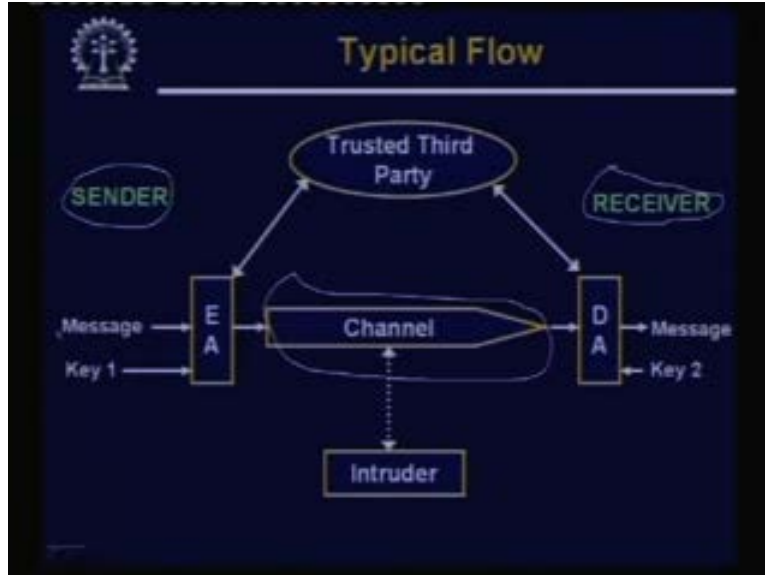
So now let us first look at some of the basic cryptography terminologies. At the bottom level you have to use or implement or utilize some of the basic cryptography primitive operations. So we have to have some idea about the cryptographic terminologies.

(Refer Slide Time: 15:50)



Most important concept behind any network security mechanism is encryption. Encryption means you are trying to hide some information from the intruder I am transforming or modifying or encrypting the information in such a way that it cannot be read in a meaningful way by the intruder. So there are number of ways for doing this. Broadly speaking the methods can be classified as either private or public key. They are also called symmetric or asymmetric. In the private or symmetric key encryption methods there is a single secrete key shared by the sender and receiver. The concept of a key will be explained. Key is something like the key to a lock I am encrypting a message using a key. So unless I have the key for decryption I will not be able to decrypt. Now in case of symmetric or private key system there is the same key available by both available to both the senders and the receivers. Same key is used for encryption. The same key is used for decryption. But for a public key or asymmetric system there are two separate keys lying with the sender and receiver. One for encryption other for decryption.

(Refer Slide Time: 17:17)



Now this is a diagram that shows a typical information flow in a system that utilizes encryption and decryption techniques. This diagram again shows the different important entities in this whole system. First is the channel through which the data flows. We have the sender, we are sending something; receiver who wants to receive. Now sender wants to send some message. Here we have an encryption algorithm EA. Sender encrypts the message with the help of some key. Let us call it key 1 and whatever is actually transmitted over the channel is the encrypted version of the message. Even if an intruder sitting out here listens to whatever is going on in the channel, not much can be made out of it. Similarly on the other side whenever you talk of the receiver, receiver is running some kind of a decryption algorithm which again will be taking the help of a key.

Let us call it key two to convert this encrypted message into the original message. So here we get back the original message. Now in an actual implementation of such a system we may need a trusted third party which sometimes be called as a certifying authority who may be responsible for distributing the keys to be used by the sender and the receiver. Or otherwise how do the sender and the receiver agree upon the key? If I make you a telephone call and listen anyone can tap the telephone and know what I am telling what. What key I am using? So it should be a very secure way of transmitting and exchanging and managing the keys. Because in the system the secrecy of the keys is at the most important and crucial.

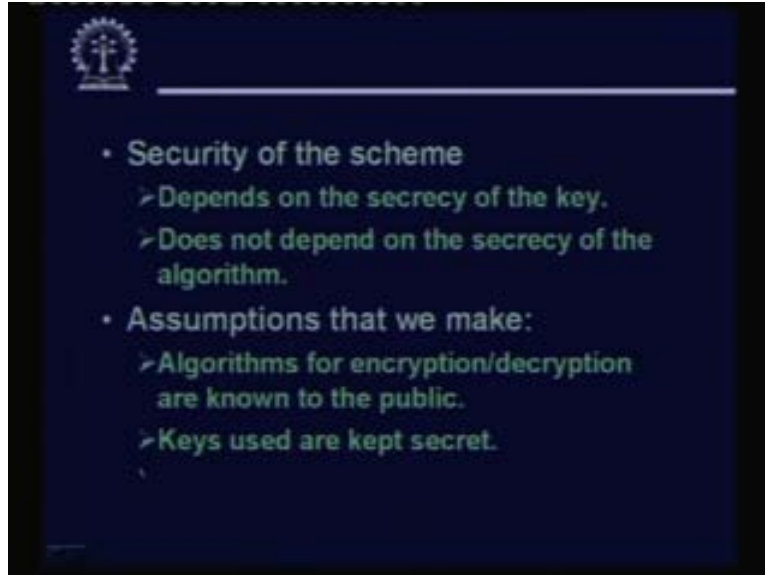
(Refer Slide Time: 19:27)



Let us first talk about symmetric key cryptography. Now in a symmetric key cryptography, there are a few terminologies which let us introduce first. The message that you want to transmit original message this is called the plain text denoted by P. Here in symmetrical cryptography there is a single secret key shared by the two parties. Secret key we denote it by K. Now after encryption whatever you get that we call as the ciphertext C. Encryption is done using the encryption algorithm which takes as input the original message or plain text and the key. On the other side you get back the message by using a decryption algorithm where we use the ciphertext C and the key K again.

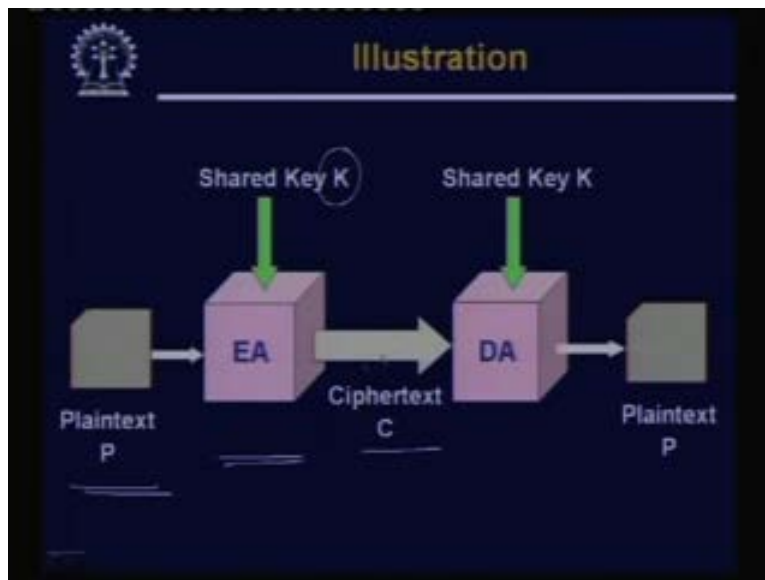
Now one thing is important here. The security of this kind of a system is considered to depend on the secrecy of the key. This does not depend on the secrecy of the algorithm. Some people do think that if I keep my algorithm secret, then my system will also be foolproof it is absolutely wrong. If you keep your algorithm secret then some possible vulnerability in your algorithm will not be disclosed or will not be known fast enough. A cryptographic algorithm is known to be good, is said to be good if you make the algorithm public. But the key you keep secret, the total strength of a system will depend only on the secrecy of the key and not on the secrecy of the algorithm.

(Refer Slide Time: 21:25)



So just as a corollary to what you have said, the assumptions we make is algorithms for encryption or decryption are known to the public. It is only the keys that we have to keep secret.

(Refer Slide Time: 21:41)



This diagram illustrates the symmetric encryption key. So we have the plaintext, at the sender end we use the encryption algorithm to convert the plaintext into a ciphertext using the shared key K . So over the transmission channel the ciphertext C is transmitted. At the receiver end, again we use the decryption algorithm with the same key K to convert this ciphertext C back to the plaintext. So this is how this system works in

general. Let us see now some examples. Before that let us look at an issue regarding the key distribution. Now in a symmetric system for every pair of parties we need a secret key. So if in general there are n number of parties communicating for secrecy and safety every pair of parties must have a different key to enable pair wise secure communication.

(Refer Slide Time: 22:52)

Some Points to Observe

- **Key distribution problem of secret key systems:**
 - Establish key before communication.
 - Need $n(n-1)/2$ keys with n different parties.

The diagram shows a complete graph with five nodes labeled A, B, C, D, and E. Node A is at the top, B and E are on the left and right respectively, and C and D are at the bottom. Every node is connected to every other node by a straight line edge, representing a key for communication between that pair of parties.

So you can say that if there are n numbers of parties, then the number of keys required will be $n C 2$ or n into n minus 1 by 2. For example, in this diagram there are five parties, the number of keys which are represented by the edges in this graph. There are 10 edges in this graph. So there will be 10 keys that will be required.

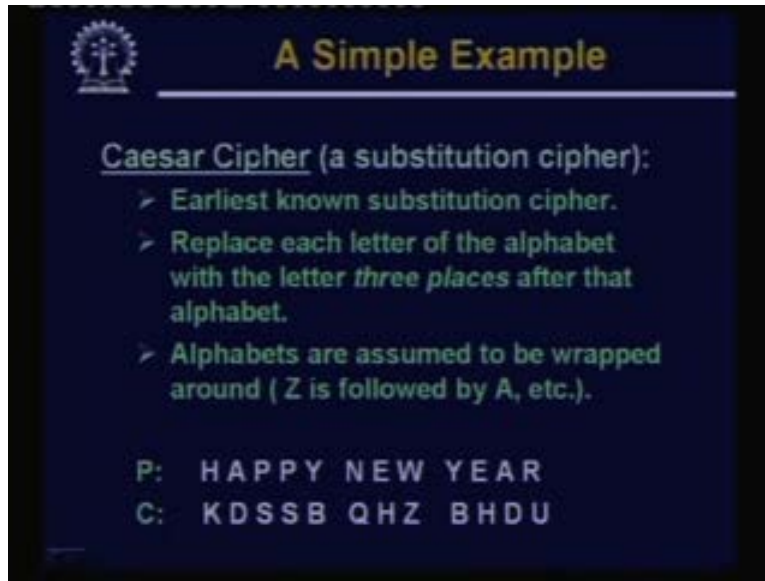
(Refer Slide Time: 23:27)

Classical Techniques

- Broadly falls under two categories:
 1. Substitution ciphers
 - Each letter or group of letters of the plaintext are replaced by some other letter or group of letters, to obtain the ciphertext.
 2. Transposition ciphers
 - Letters of the plaintext are permuted in some form.

Let us now look at some of the classical techniques for symmetry key and encryption decryption. The classical techniques broadly fall under two categories. One is called substitution ciphers other group is called transposition ciphers. Now substitution ciphers as the name implies, here some letters or group of letters of the original assuming that the original message is a text. So we are talking about letters and group of letters. So each such group is replaced by some other letter or group of letter. So suppose I have A I replace A by D, I replace X by P or something like that. So there is some kind of a replacement that we are doing, that replacement method should be kept secret and in the transposition cipher we are not replacing anything. But we are permuting the letters like good g o o d. I can change it to, o g d o. I am just permuting the letters in any arbitrary order to get the permuted text.

(Refer Slide Time: 24:36)



A Simple Example

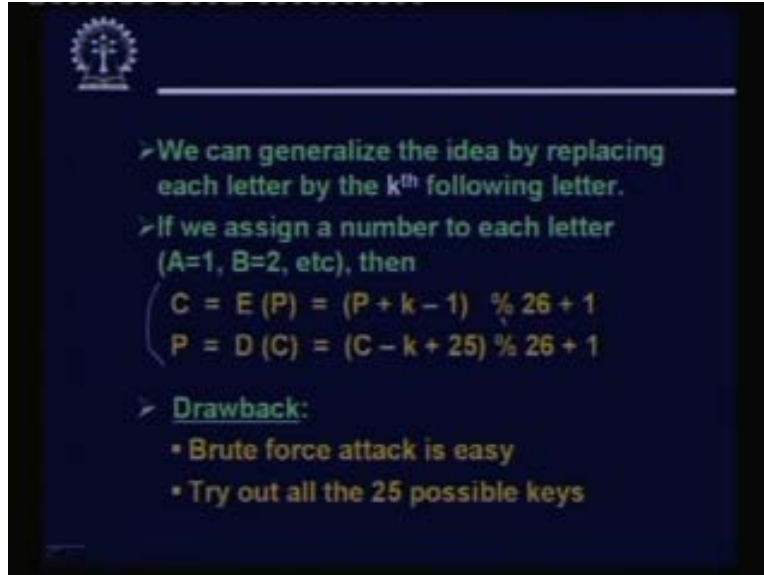
Caesar Cipher (a substitution cipher):

- Earliest known substitution cipher.
- Replace each letter of the alphabet with the letter *three places* after that alphabet.
- Alphabets are assumed to be wrapped around (Z is followed by A, etc.).

P: HAPPY NEW YEAR
C: KDSSB QHZ BH DU

Let us look at some of the ciphers that are initially proposed. These are examples of substitution ciphers. This is perhaps the earliest known cipher, may be you have the cipher possibly you are also familiar with because we usually play with the cipher when we are kids. Now the method is very simple. Say here for the sake of illustration what we take is that we have a message to encrypt like say happy new year. We replace each letter of this text each letter with the letter three places after that. Like we replace H by I, J, K three letters after each we replace A by B, C, D; P by Q, R, S. So all are moving three letters ahead. But for Y we assume that the alphabets are wrapped around circular way. So after Z comes A. So if it is Y next letter is Z, next to Z is A, again next to A is B. So Y is replaced by B. So in this way you can encrypt a message to get this ciphertext and the receiver can carry out the reverse operation. Now this is a fixed kind of a transmission where you are always replacing three the letter by another letter three places ahead in the alphabet.

(Refer Slide Time: 26:07)



➤ We can generalize the idea by replacing each letter by the k^{th} following letter.

➤ If we assign a number to each letter (A=1, B=2, etc), then

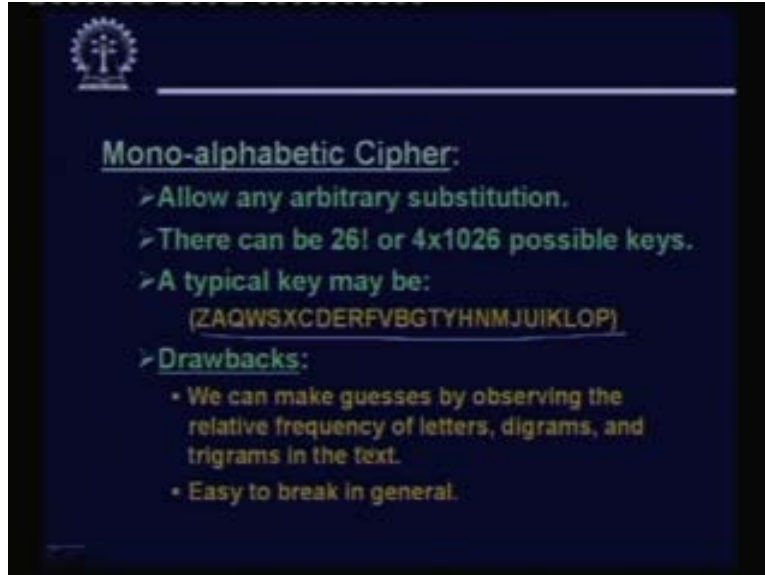
$$\begin{cases} C = E(P) = (P + k - 1) \% 26 + 1 \\ P = D(C) = (C - k + 25) \% 26 + 1 \end{cases}$$

➤ Drawback:

- Brute force attack is easy
- Try out all the 25 possible keys

But you can generalize the idea by replacing instead of three you can make it k . Only the sender and receiver know the value of k , k can be 1, 2, 3, it can be 10, 15, 20, whatever each letter is replaced by the k^{th} next letter. This k is considered to be the secret key, k is known to the sender and receiver and to no one else. So it is easy to formulate some expressions which will actually give you that how to make these transformations. So if we assume that each letter in the alphabet corresponds to a number A is 1, B is 2 up to Z is 26. Then the transformation the encryption algorithm will look like this P plus k minus 1 modulo 26 plus 1. Similarly decryption will be C minus k plus 25 modulo 26 plus 1. You can actually verify with some examples that these expressions are correct. Now the problem with this simple kind of a cipher is that although we are keeping k secret. But there are only 26 possible values of k . So even by brute force attack some intruder can try out all possible combinations and can decode back the result. But this is actually a way of illustrating that practical ciphers are much more complex and it takes much greater effort to break that.

(Refer Slide Time: 27:43)



Now one way you can increase the complexity of Caesar cipher is to allow something called mono alphabetic substitution. Like in Caesar cipher, the displacement is always fixed.

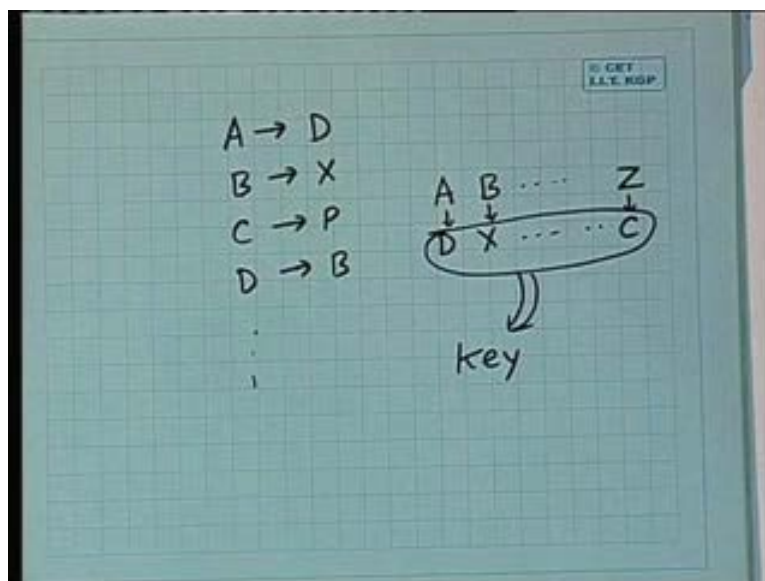
A will be replaced by D;

B will be replaced by E;

C will be replaced by F and so on.

But here when I am saying the combination we are making arbitrary. Like for example I can say that,

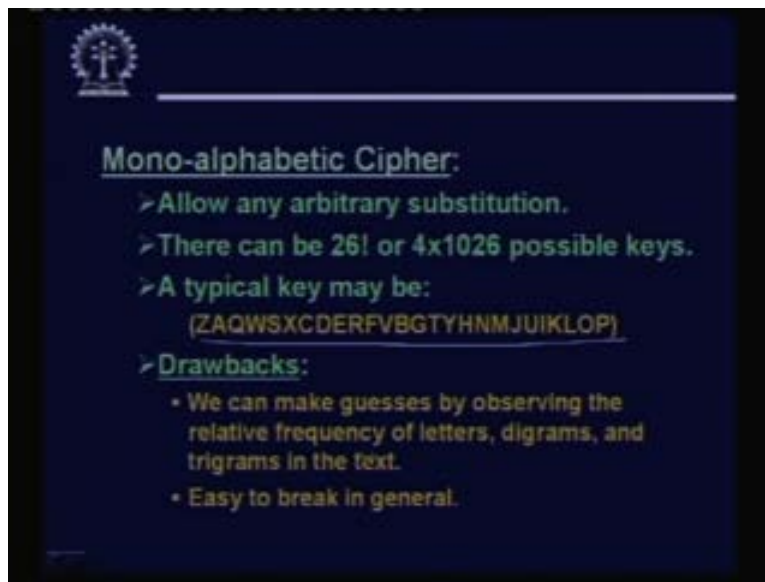
(Refer Slide Time: 28:10)



A will be replaced by D;
B will be replaced by X;
C will be replaced by P;
D will be replaced by B and so on.

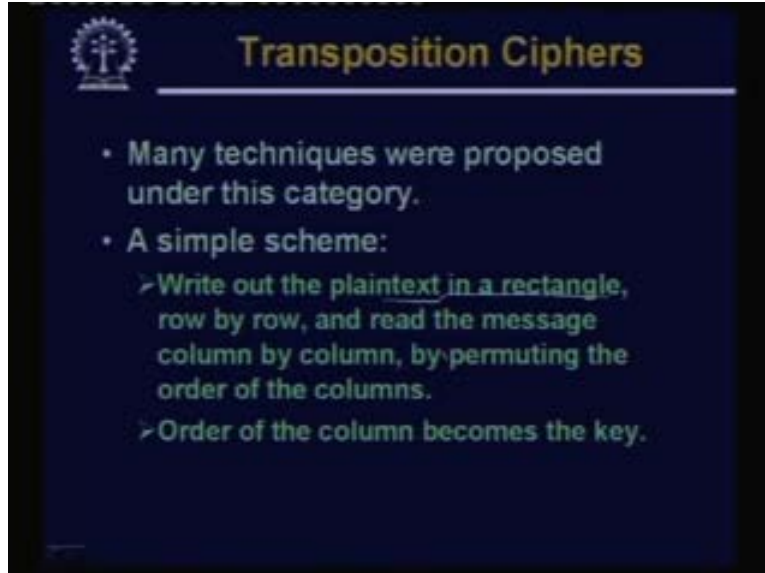
So actually you will be getting for the 26 letters, you will be getting another 26 letters which will be telling you which letter to replace by which. So this new combination of letters, this will be regarded as the key. This is the basic idea behind mono alphabetic cipher.

(Refer Slide Time: 28:57)



As I said a typical key will look like this. Any combination of the 26 alphabets. Drawbacks in this method are we can make guesses by observing the relative frequency of letters. See we can make substitution. We can substitute one letter by another. But we are not able to hide the natural statistics that is present in English language. Like for example, statistics might say that S is the most frequent word A is the next frequent. So I can just count the number of occurrences of the different letters. The most frequent letter I find it is K. I substitute K by S. So I make a guess that most probably K is equivalent of S. So in this way I can make guesses based on single letters based on pairs of letters called digrams. Three letter combinations called trigrams and so on, and you can very easily break the message. This is also quite easy to break depending on the statistical properties as I said. But one thing brute force attack as such will be difficult here because the number of possible keys will be 26 factorial or 4 into 1026. So brute force attack is possible, but you will need a computer for the purpose you cannot possibly very easily do it by hand.

(Refer Slide Time: 31:30)



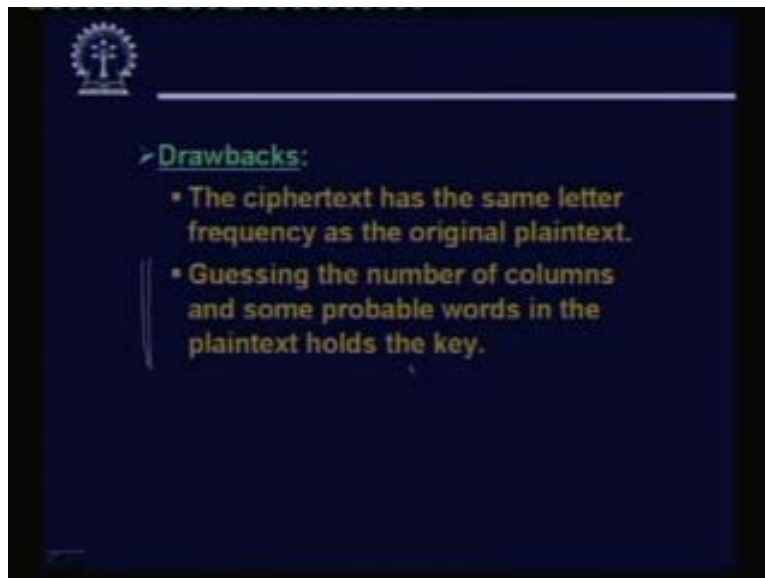
Transposition cipher. Let us look at one example of this. Here we have said that we are trying to permute or change the order of appearance of the letters. Now the method or the scheme we talk about here is very simple to what we say is that we write the plaintext in a rectangular form. We will just illustrate it with a help of for example. The rectangular form. We were writing in a row by row form and we were reading out the characters column by column by permuting the order of the columns. This lets explain with the help of an example and here the key is the order of the column and the size number of columns. Let us explain this with the help of an example.

(Refer Slide Time: 31:29)



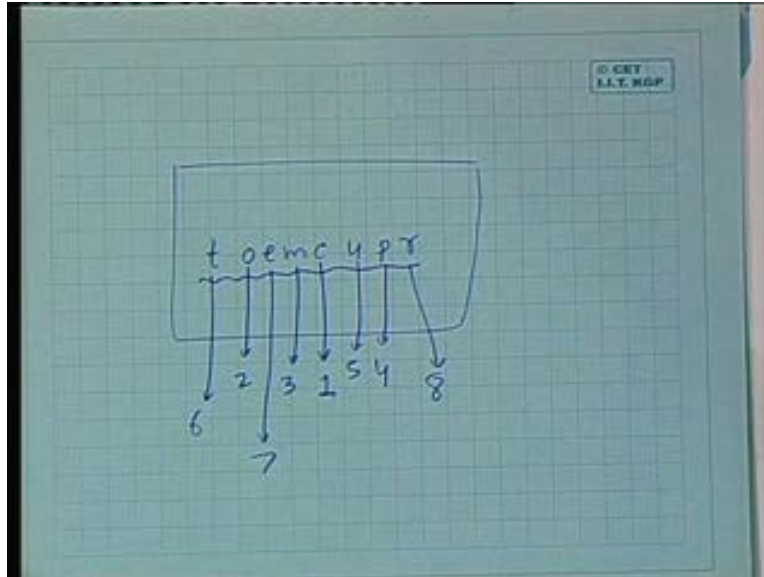
Suppose our plaintext is this. We are attending one conference at IIT Kharagpur. So at the first step we select that the number of letters in the key will be 7. So we create a matrix with 7 numbers of columns and we simply go on writing this text like this. We are a t t e n attending one conference at IIT Kharagpur, the last one is gap. Well in this example I am ignoring blank spaces. But in practice blank spaces will also be there. So we write the text just like this in the form of matrix. Then we define an order of the key not the key order of the columns. In fact, say for an example I say that the third column is marked as one, fourth column as two, second column as three. This one as 4, then 5, then 6, then 7. So this particular combination now becomes the key because when you are converting this plain text to cipher text. What to do? We now read column wise. But which column first? We first read the column numbered as one. So a, n, e, e, I g. So a, n, e, e, I, g, then you read out column 2; r, d, c, n, T, p; r, d, c, n, T, p; then column 3; e, e, n, r, I, a and so on and in this way you go on reading it column wise. So understand in order to break or decode this kind of a cipher text we need to know two things. We need to guess the size of the matrix in terms of the number of columns and then the order of the columns. So this code is again is not very difficult to break as number one.

(Refer Slide Time: 33:29)



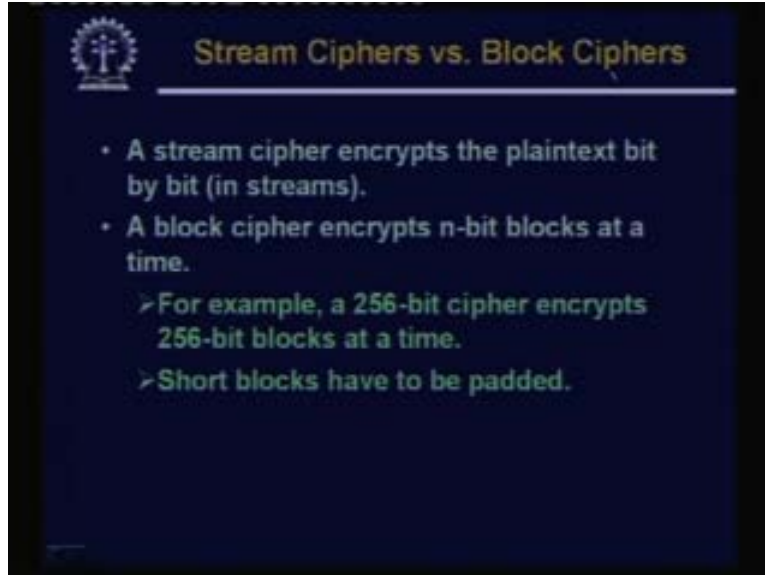
The ciphertext has the same letter frequency as the original plaintext. We are not modifying any letter by any other letter. So the most important part here will be to make a guess regarding the number of columns and some probable words in the text which usually we can guess. Like for example if you have made the guess correctly in terms of the number of columns, you try to arrange the ciphertext in that many columns.

(Refer Slide Time: 34:16)



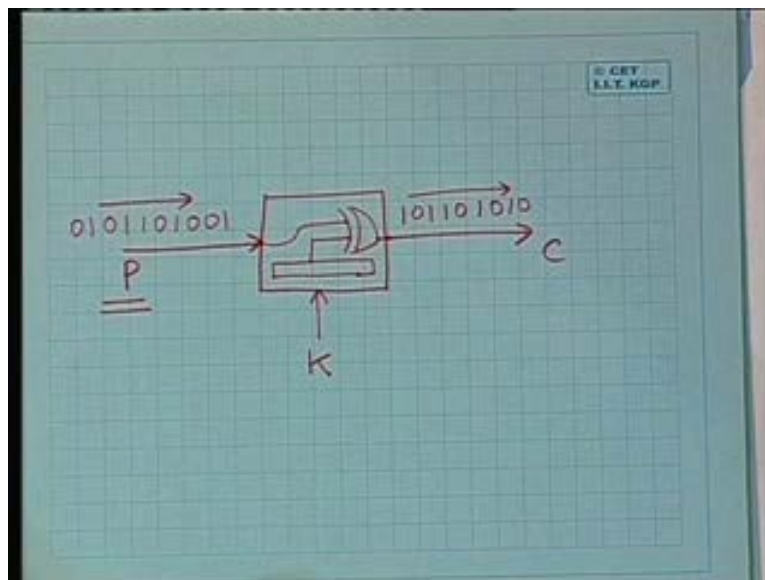
Now you consider that computer is a possible keyword. So you try to search and find out where computer this 8 letters are appearing in a jumbled of form. Like for instance you may find that in the matrix somewhere we have seen you have something like this. You find that there is a jumbled version of computer existing somewhere. So you immediately tell this will be your column number one. This will be your column number 2, this will be your column number 3 and so on. This will be 4, this will be 5, this will be 6, this will be 7 and this will be 8. So once you have found this out, you can easily read out the matrix in the order of this column and you get back the original plaintext. So these methods are interesting in the sense that you can play around with it but in terms of the in terms of breaking complexity. These are not good at all. So in practice people use more complicated kind of ciphers. Some of them we will have looked at.

(Refer Slide Time: 35:16)



Now let us look at one thing before actually going into some practical algorithm. Let us look at two different kinds of ciphers we talk about stream ciphers, block ciphers. Now a stream cipher encrypts the plaintext bit by bit in streams the idea is like this.

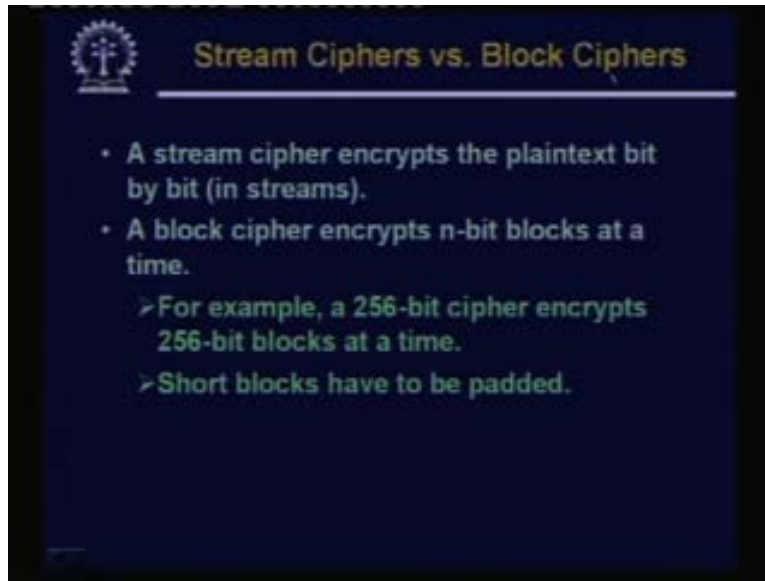
(Refer Slide Time: 35:41)



Suppose I have a stream cipher generating block. Here, my plaintext is coming. Here my ciphertext is being generated here. And I am driving this block by this secret key. Now the idea is that this plaintext is considered to be a stream of zeroes and ones typically. That is why it is called as stream and similarly a stream of encrypted bit stream will be generated on the other side. So a stream cipher continuously converts the incoming bit

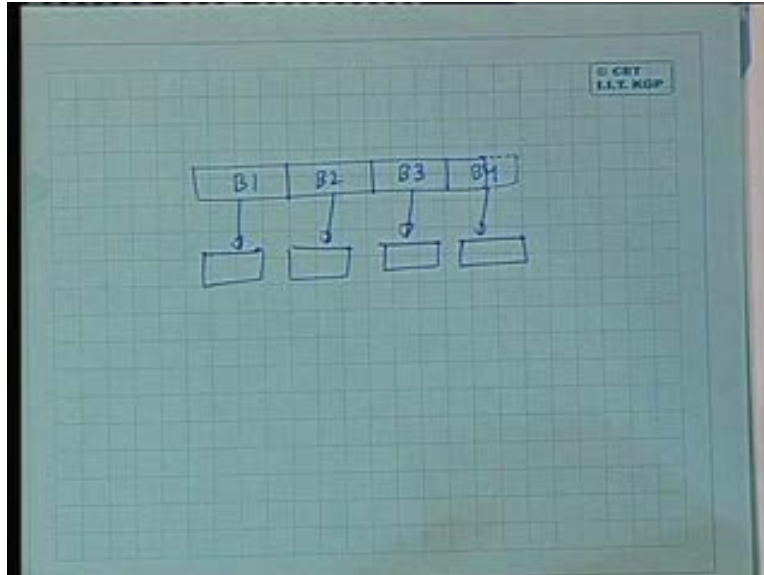
stream into the outgoing bit stream see most of this stream ciphers actually have some kind of a pseudorandom generator block then there is an exclusive or gate which takes the input bit stream the pseudorandom bits generated and then it generates the output bit stream. There are additions to this, of course but there are applications where this kind of stream ciphers are desirable. Number one stream ciphers are much faster because they can be very easily implemented by hardware and the amount of hardware required is also pretty less. Secondly there are applications like speech you are sending speech information over say it can be mobile phone, it can be over satellite, whatever. But you want to do some kind of some encryption while you are sending. Now speech is continuous. Your speech the data you are encoding into digital that is coming continuously. So under this circumstances stream cipher may prove to be more advantageous.

(Refer Slide Time: 37:25)



Now a block cipher in contrast, takes the input plaintext block by block. It takes an n bit block at a time and it will convert it into a ciphertext. For example a 256 bit cipher will encrypt 256 blocks at a time. Like again, let us take an example.

(Refer Slide Time: 37:56)



Suppose we have an input message where I am dividing here into equal size blocks. This is your block 1, block 2 and block 3. Typically these blocks will be having certain sizes. If the last block is smaller you can add some pads to make it equal to that minimum size. Now you can convert or encrypt each of these blocks separately to generate the cipher text blocks. This is the essential idea behind block cipher. So here encryption is taking place in terms of blocks of bits. Decryption will also take place in terms of blocks of bits. So encryption and decryption are not bit by bit continuous; that is block by block.

(Refer Slide Time: 38:39)

Practical Algorithms

- **Data Encryption Standard (DES)**
 - Block size is 64 bits.
 - Key is 56 bits.
- **IDEA**
 - Block size is 64 bits.
 - Key size is 128 bits.
- **Advanced Encryption Standard (AES)**
 - Also known as Rijndael cryptosystem.
 - Block size can be 128, 192, or 256 bits.
 - Key size can be 128, 192, or 256 bits.

Let us now look at some of the practical algorithms that people use in stream ciphers.

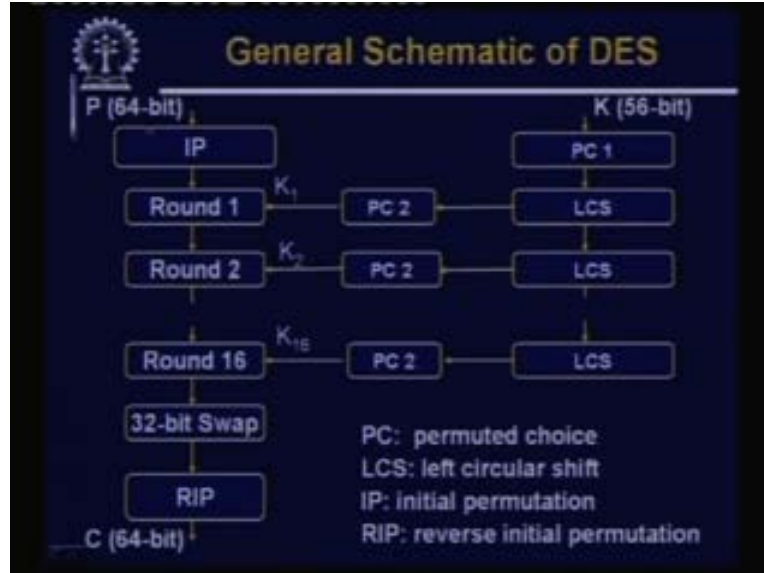
Data Encryption Standard is one of the oldest and one of the most widely used algorithms till very recently. This was developed by the US government department of defense. Here the block size is 64 bits. The secret key is 56 bits. So we will be looking into this algorithm in some detail. There is another method called IDEA. It is an acronym I D E A. Here block size is 64 bits again. But key size is longer. This advanced encryption standard is the most recently proposed algorithm. This is considered to be the standard which is to be adapted and used at least in the near future. This is also known as Rijndael cryptosystem. This name has come from the person who has made this proposal. Here the block size and key size may vary. They can be 128, 192 or 256 bits.

(Refer Slide Time: 40:02)



Let us now look into some detail about the data encryption standard or DES. DES is the most widely used encryption scheme. As I said, till very recently, now people have started to use other methods because, people have started to suspect that the security that is offered by DES may not be sufficient for many applications. I need some algorithm which is better than DES. DES is also sometimes known as Data encryption algorithm. Or DEA as I said this is a block cipher. It takes 64 bit block which means the plaintext is 64 bits in length and for the purpose of encryption the key that is used is 56 bits. So if you have longer plaintexts, then it will be broken up into 64 bit blocks and processed block by block.

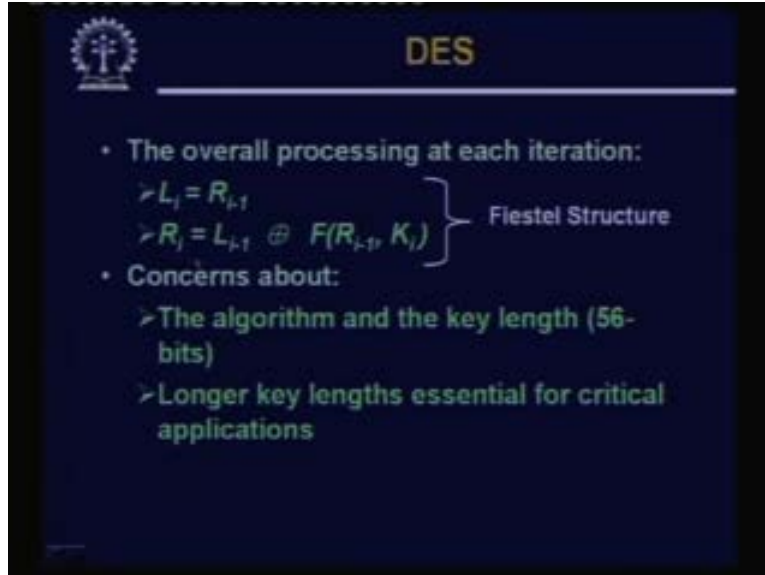
(Refer Slide Time: 41:09)



Now the next diagram gives you some kind of an overall block diagram of the DES algorithm. Here to start with the 64 bit plain text is taken. So the 64 bit plaintext first goes through an initial permutation. Initial permutation means you jumble out the bits in some defined order. Then you carry out 16 rounds of identical looking operations. We will be coming to this little later. So after you have completed these 16 rounds, you make a 30 bit swap. 30 bit swap means you have a 64 bit number that is coming divided into two halves; 32 and 32. Swap the two the second half. You bring it first, the first half you bring it later. So this is 32 bit swap and finally you pass it through a reverse initial permutation block to get back this cipher text. Now reverse initial permutation means whatever permutation you did initially like your first bit when to bit number 3. Now in their RIP the third bit will go back to bit number one.

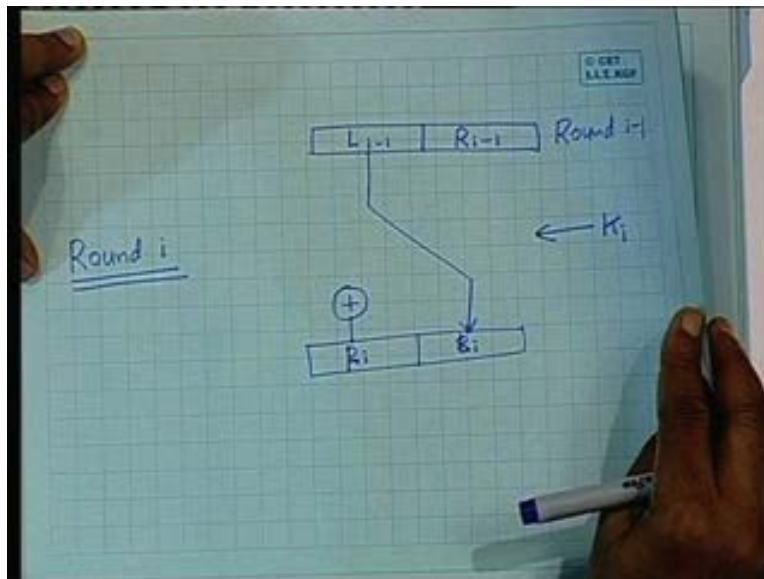
So these permutations are actually used to increase the complexity from the point of intruder and regarding the rounds you see the key is coming here. This is a 56 bit key. PC is a permuted choice initially you make a permutation of the key. Then in every round you make a left circular shift of the residual keys. So you will be getting different key values in the different rounds and in each of the rounds you pass it through some other permutation block PC2. Now here what is happening is the key is a 56 bit quantity. This is also an expansion block 56 bit quantity. Here is expanded into a 64 bit quantity here. So this creates a permutation also replicates some of the bits to make it 64. So as the round number goes the generated round keys k_1, k_2, k_{16} are generated by this portion of the circuit and this round blocks are executed one after the other. Now exactly what kind of operation is carried out in the rounds. Let us see this.

(Refer Slide Time: 43:56)



The overall processing looks like this $L_i = R_{i-1}$, $R_i = L_{i-1} \oplus F(R_{i-1}, K_i)$. I am trying to explain this.

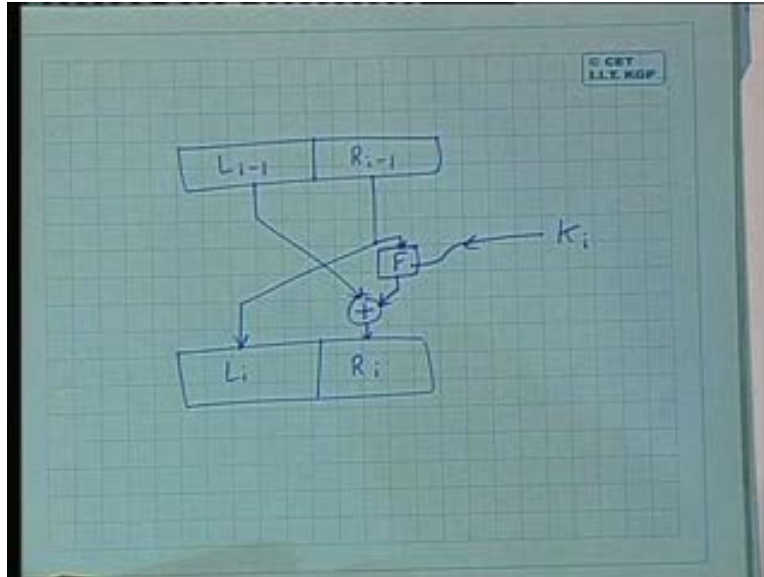
(Refer Slide Time: 44:11)



See we illustrate round number i . Let us say, this is the data which has come from round i minus 1 from the previous round. We are dividing this 64 bit data into two halves. The right half we are calling R_{i-1} , left half we are calling L_{i-1} . Now our objective of round i , is starting from, this we want to generate another 64 bit quantity. It will be L_i and R_i . So we will have to calculate L_i and R_i . From these somehow and another thing is available to us. The key for the i th round K_i . So the way we do it is as

follows. The left half from the 64 bit data of the previous round gets copied into the right half of the next round and for the remaining part for computing the other. This is L_i and this is R_i . For calculating R_i we have an exclusive OR function. Exclusive OR function will take L_{i-1} . This diagram I am straightly redrawing.

(Refer Slide Time: 45:43)



So I make it neater L_{i-1} R_{i-1} , L_i R_i and from here K_i is coming. First thing is L_i is equal to R_{i-1} . I have drawn it reverse. So it will be like this and R_i will be an exclusive OR function of L_{i-1} and some function some complex function of K_i and R_{i-1} . So this function F is a complex function there is some so called non-linear operations in the function. It is sometimes also called an s box. So this is roughly how the rounds are completed and we have 16 such rounds going on. So as you can understand the final ciphertext, what is what you are obtaining it is not very easy to break that by any of the brute force technique. Even if you try brute force techniques a 56 bit key would demand searching of a two to the power 56 size space which is typically infeasible.

(Refer Slide Time: 47:20)

Triple DES

- Use three keys and three executions of the DES algorithm (encrypt-decrypt-encrypt).

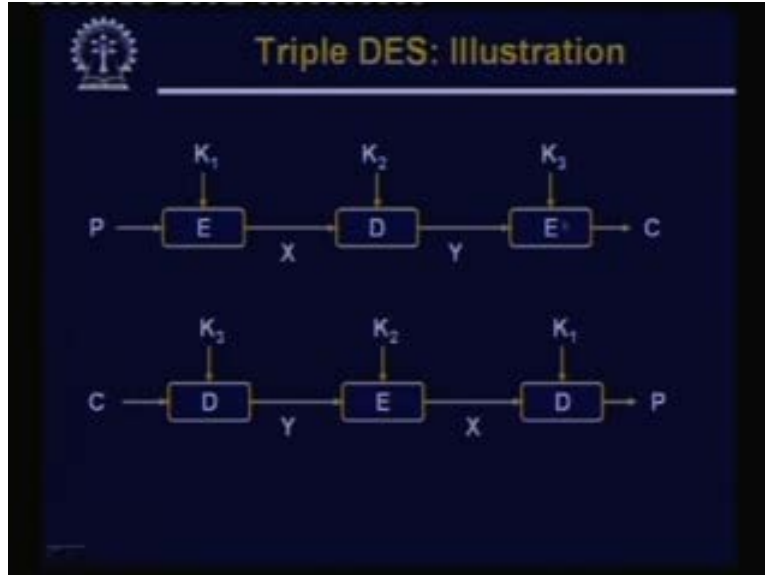
$$C = E_{K3} [D_{K2} [E_{K1} [P]]]$$

C = ciphertext
P = Plaintext
 $E_K[X]$ = encryption of X using key K
 $D_K[Y]$ = decryption of Y using key K

- Effective key length of 168 bits.

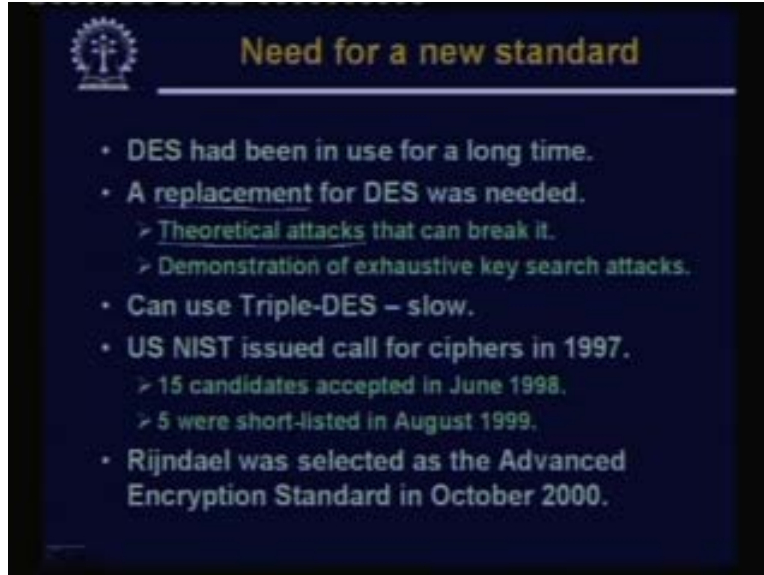
So there is some concern about DES is that with the fastest computers that are available with the intruders or the hackers 56 bit key although it was considered to be sufficient earlier. But today's high security application where you carry out financial transactions electronically 56 bit key is not considered to be sufficient. So longer key lengths should be used for that purpose. Now triple DES was one modification of the DES algorithm which was suggested and in fact this is still used many applications. What the basic idea is that the basic DES algorithm uses a 56 bit key DES says you run DES. Triple DES says you run DES three times possibly on two or three different key values. So your effective's key size will increase. So generally you can have something like this. You can first encrypt P using K 1, then possibly you can decrypt using K 2, again encrypt using K 3. You can use any combination. So when you are decrypting, you will first be decrypting using K 3, encrypting using K 2, decrypting using K 1. You will get back the original plain text. So here if you use three runs but effective key length will become three times.

(Refer Slide Time: 48:50)



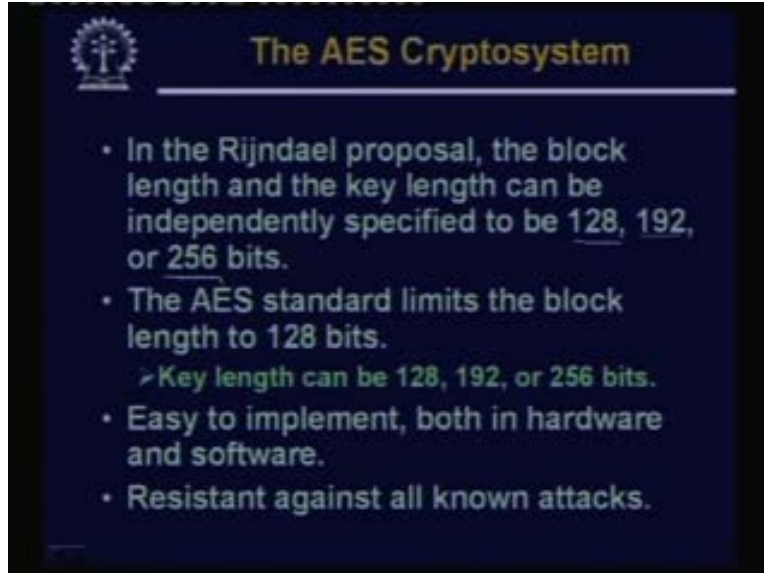
So this is the order. So when you are encrypting see E D E is not mandatory you can have also E E E and the next step D D D. This is just to jumble up thing even further K1, K2, K3 when you decrypting it will be reverse way round. Last time you used K3, so here you would have to use K3 first, then K 2 and then K 1 and this E and D would be reversed. This was E and this will be D. So by suitably using this key and by suitably using the encryption and decryption functions of DES you can have an effective system which will be having a much longer key value. One thing I did not mention in the DES algorithm. You have 16 rounds. Now when you are decrypting, the same hardware can or the same block can carry out decryption if you just run in the reverse order. So it is also felt easy to have a decryption algorithm by slightly configuring the encryption algorithm. So encryption and decryption of DES are also available as hardware implementations in the form of chips. So they are pretty easy to implement.

(Refer Slide Time: 50:12)



Now as said DES had been in use for a long time because it is considered to be secure. But now we need a replacement because a lot of analysis on attacks on theoretical methods are breaking such codes have been analyzed so that the cracking complexity of DES has been made much less than 2^{56} . So it is now feasible to break on a big computer in a reasonable amount of time. People have demonstrated exhaustive key search attacks that DES can be broken. You can use triple DES of course but this would be slow because effectively you have to run 48 rounds every time; 3 runs of DES. So this is not a very good solution. So in 1997, NIST an organization they sent out an open call for proposals. For new ciphers 15 such candidate applications were accepted in June 1985 were shortlisted later. Finally the Rijandael cryptosystem was selected in October 2000 as the so called advanced encryption standard. So sometimes people interchangeably use this AES and Rijandael to mean the same thing. Technically there is a small difference but people use these terms interchangeably.

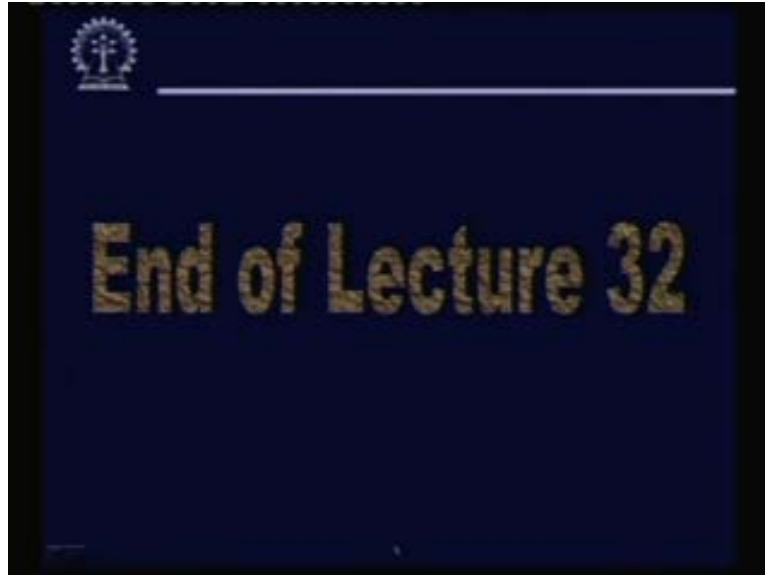
(Refer Slide Time: 51:46)



Just a very brief look at the AES cryptosystem. As I said for AES block size and key size both can be varied between 128, 192 or 256 bits. But however in the AES standard block length is made 128 although the original Rijandael proposal allows all 3. So here is a small difference I just talked about. So when you are talking about the AES standard the block size is fixed. However the key length can be varied, depending on the level of security unit. AES looks somewhat simpler to DES but similar to DES but the operations are slightly different. AES is also easy to implement both in hardware and also in software and this is also resistant against all known kind of attacks. In this context let me tell you that why do we talk about attacks on cryptosystems. This attack on cryptosystems is by itself a separate topic. This is called crypt analysis. So there are many methods or schemes that are being utilized that have been proposed and used for carrying out this sort of crypt analysis and this AES cryptosystem. It has been theoretically proved that no amount of crypt analysis can break this system with in a reasonable amount of time.

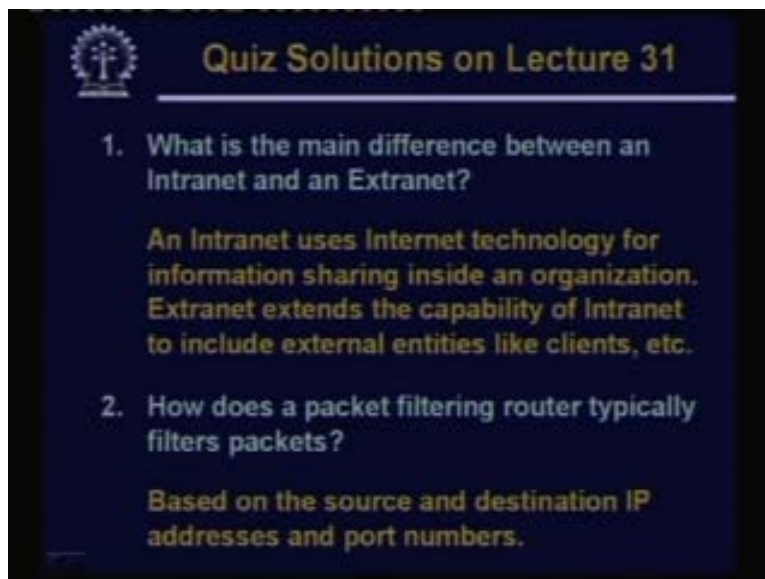
Of course we do not know of the future may be tomorrow some one may come up with a scheme with which we can possibly have a better attack. But what I am trying to say that there are other non conventional attacks like these are called side channel attacks. Like you can measure the electromagnetic radiation emitted by a device during encryption. You can measure the current flowing during encryption process. There will be some small variations. Analyzing the variations you can get a lot of insight about the operation of the device. So unless your implementation is done in a proper way this kind of side channel attack can reveal lot of sensitive information about the key you are using or some other secret things. So with this so we come to the end of today's lecture.

(Refer Slide Time: 54:22)



In the next lecture we shall be continuing with this we shall be looking at the public key cryptosystem first. Then we shall be looking at some issues of authentication. So here first let us quickly look at the solutions to the quiz questions of the last lecture. The questions were as follows.

(Refer Slide Time: 54:50)

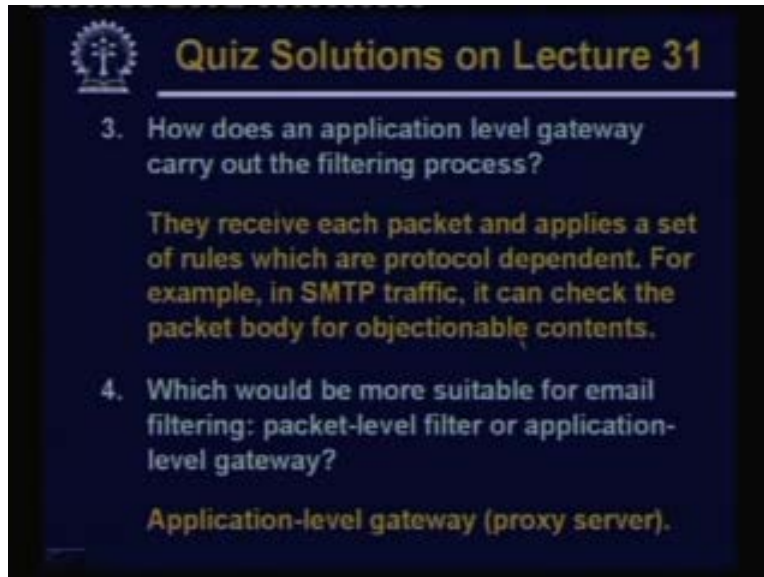


What is the main difference between an intranet and an extranet?

So as I said an intranet uses internet technology for information sharing inside an organization only. Extranet basically extends the capability of intranet to include some entities like clients, customers, etcetera.

How does a packet filtering router typically filter packets?
Based on the source and destination IP addresses and port numbers.

(Refer Slide Time: 55:24)



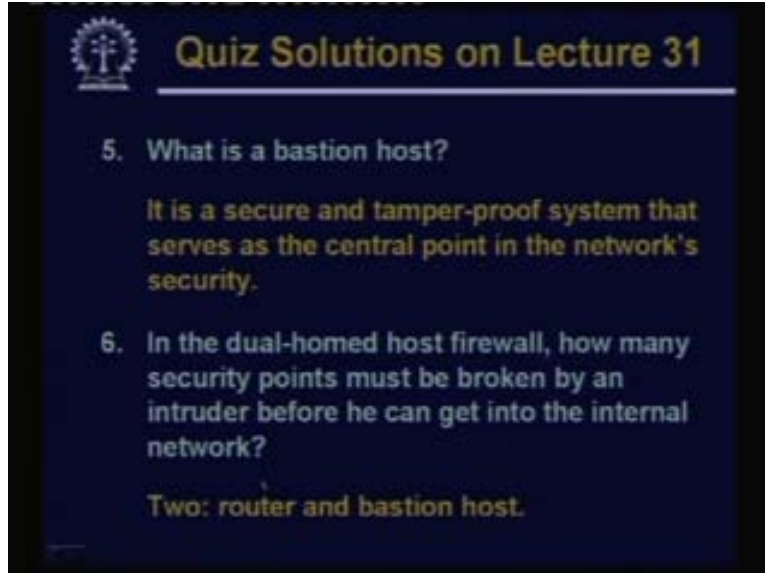
How does an application level gateway carry out filtering process?

They receive each packet and apply a set of rules which are protocol dependent. For example in SMTP traffic it can check the packet body for objectionable contents or viruses etcetera.

Which would be more suitable for email filtering packet level filter or application level gateway?

See as I mentioned, just now for email filtering application level gateway is more suitable because protocol specific checks can be made here at the at the packet filtering level. You can only monitor the IP addresses and port numbers.

(Refer Slide Time: 56:05)



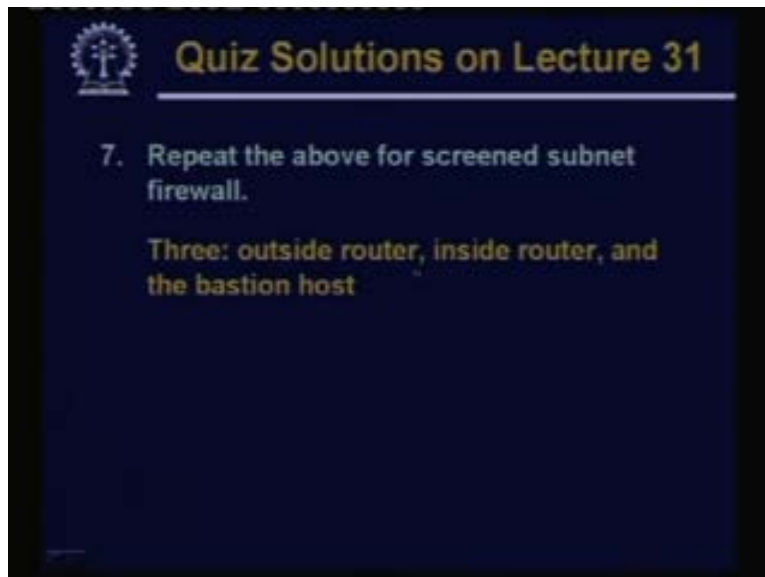
What is a bastion host?

It is a secure and tamper proof that serves as a central point in the networks security.

In the dual homed host firewall how many security points must be broken by an intruder before you can get into the internal network?

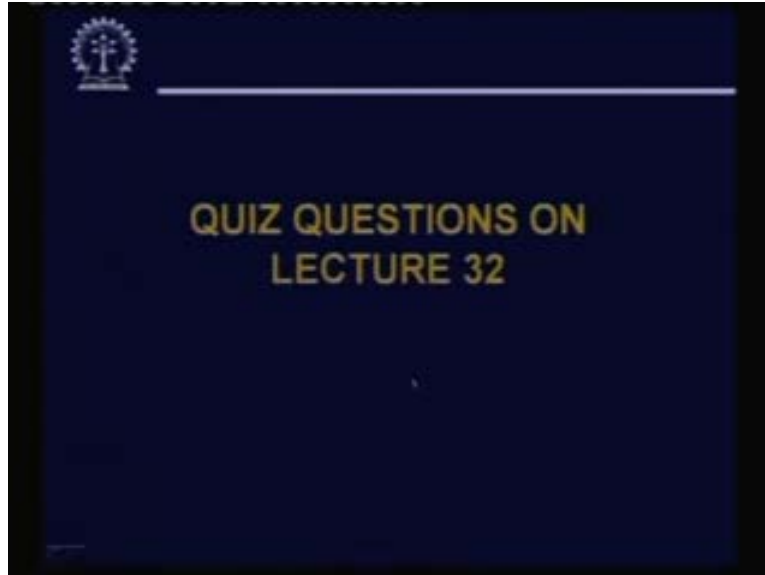
Here it is two the router and the bastion host.

(Refer Slide Time: 56:26)



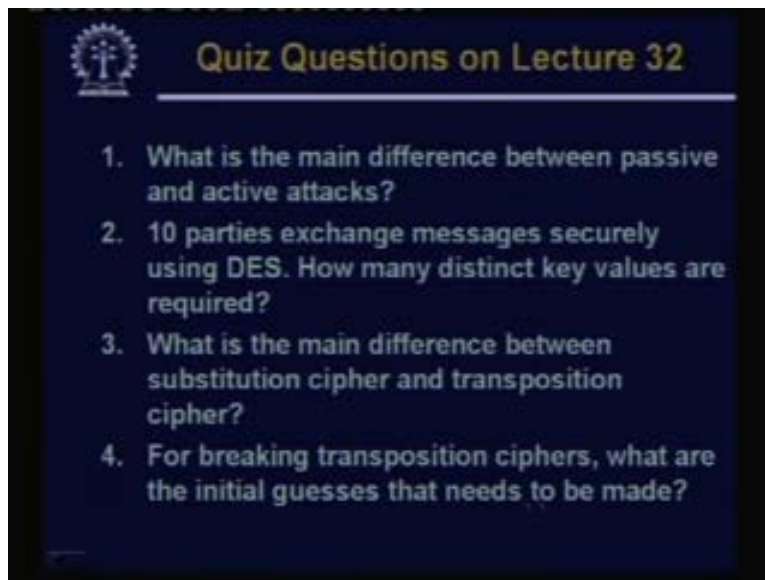
However for the screened subnet firewall with three because not only the outside router and the bastion host also the inside router has to be broken.

(Refer Slide Time: 56:39)



So now questions from today's lecture.

(Refer Slide Time: 56:41)



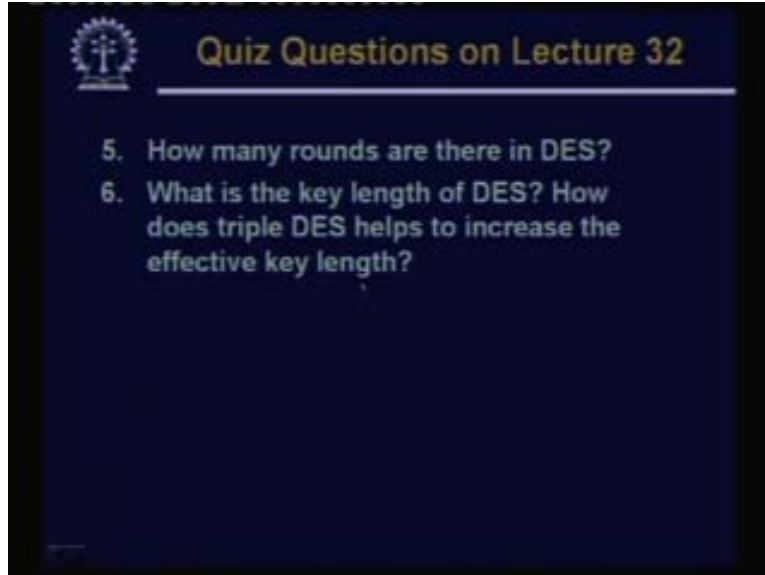
What is the main difference between passive and active attacks?

10 parties exchange messages securely using DES how many distinct key values will be required?

What is the main difference between substitution cipher and transposition cipher?

For breaking transposition ciphers, what are the initial guesses that need to be made?

(Refer Slide Time: 57:10)



How many rounds are there in DES?

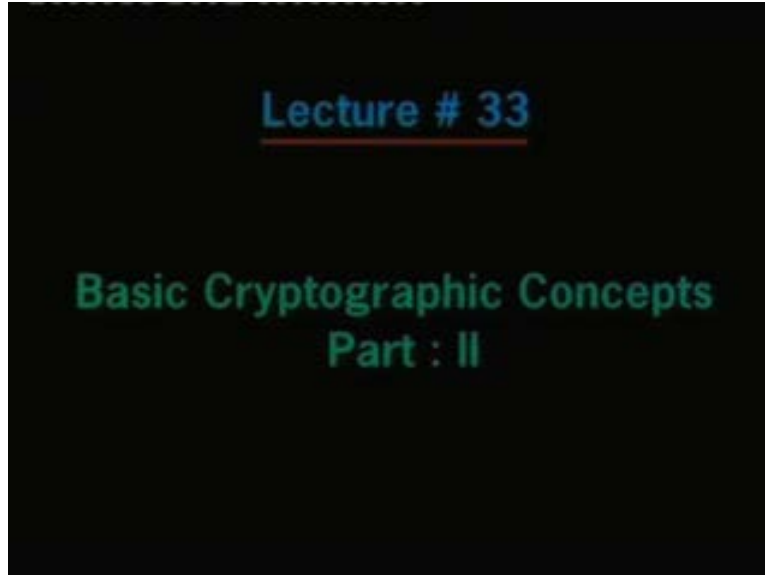
What is the key length of DES how does triple DES help to increase the effective key length?

So with this we come to the end of today's lecture. Thank you.

(Refer Slide Time: 57:29)



(Refer Slide Time: 57:34)



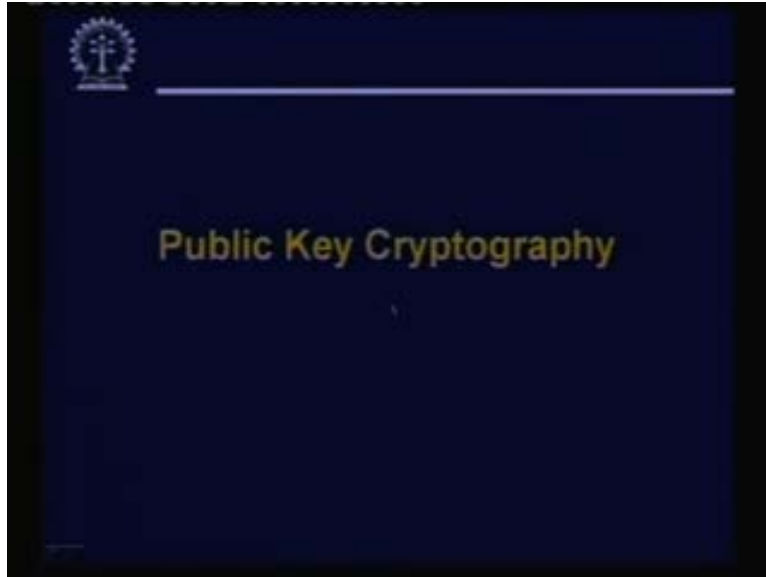
In your last lecture we were talking about some of the network security issues and some of the cryptographic concepts. In particular we talked about the symmetric key encryption decryption techniques. We looked at some of the classical algorithms like Caesar cipher, mono alphabetic cipher, transposition cipher and you also looked at some of the practical schemes that people like DES, triple DES. And you also mentioned about the standard which people use nowadays AES. So continue with the discussion.

(Refer Slide Time: 58:30)



Today we shall be first looking at public key cryptography.

(Refer Slide Time: 58:35)



Let us first try to understand the motivation before trying to explain public key cryptography is. See symmetry key cryptography methods like DES triple DES AES all are fine. They are pretty strong algorithms.