Computer Networks
Prof. S. Ghosh
Department of Computer Science and Engineering
Indian Institute of Technology, Kharagpur
Lecture # 38
Security

Good day, so the topic for today is network security. As the network is becoming ubiquitous, many people have started giving services through network. These services are crucially dependent on security. For example, if you want to do a bank transaction through the network so that from anywhere you can log on to the network and do your banking. This banking service of course is very sensitive so that if security is breached then the whole thing falls down. Therefore security once again is a very big topic, so let us discuss about the overview of security features in network.

(Refer Slide Time: 01.31 - 01.32)

So what is network security? What is the purpose of a network? It moves bit from A to B. And we want this movement to take place securely.

(Refer Slide Time: 01.33 - 01.50)

(Refer Slide Time: 01.51 - 03.32)

And what exactly we mean by securely? Of course, the bits from A must reach B but we also want confidentiality in the sense that only A and B see the bits. That means, if there is somebody in between then he cannot find out the content of the communication from A to B because A may be a client and B may be a bank. Therefore this has to be secured.

Integrity: The message must reach from A to B intact which means without any modification on the way. This is again very important for many kinds of services. Of course sitting at B you are getting some message down the network but may be you want to make sure that this is really from A and whether the messages are coming in order.

These are integrity issues and then finally the availability that B gets it in time. When B wants something from A it is able to get it. Even if all other lower layers are working perfectly B may not get the service from A or vice versa if network security is breached. So these are the three main issues: Confidentiality, integrity and availability. Let us look into these and how they are handled.

(Refer Slide Time: 03.33 - 04.56)

Network security: There is a lot of work on security and it is a very active research area at present. People have come up with lots of solutions but as solutions come up new problems also get generated as we will see. The confidentiality can be handled through encryption. Instead of sending the message as it is, you encrypt it in some fashion so that even if somebody intercepts this message and gets a copy of that he will not be able to decrypt it. We will see various encryption techniques. Encryption basically is the fundamental way in which we handle confidentiality. Integrity may be handled through what is known as the digital signatures. And retransmission and getting the messages in order is a part of the TCP protocol. Then comes availability which is something to do with the quality of service.

(Refer Slide Time: 04.57 - 05.57)

Security environment: this is closely linked not only with the network nodes but also with the operating systems of the systems. Mostly in the application layer although security has become more important that nowadays there are some network nodes also like routers which can encrypt messages almost at a good speed. But a lot of these security issues are handled near the application layer where the operating systems have a role to play.

Goals: Someone attempts to subvert the goals, it may be for fun, it may be for commercial gain, it may be with some malicious intent so

(Refer Slide Time: 05.58 - 06.27)

It is the exposure of data. If you just make a matrix of Goals vs. Threats then for goals it is the data confidentiality and for threats it is the exposure of data. For data integrity in goals it is the tampering with data as the threat. For System availability there may be a denial of service kind of an attack by some malicious people or either for fun that serves as a threat to the systems availability.

(Refer Slide Time: 06.27 - 08.24)

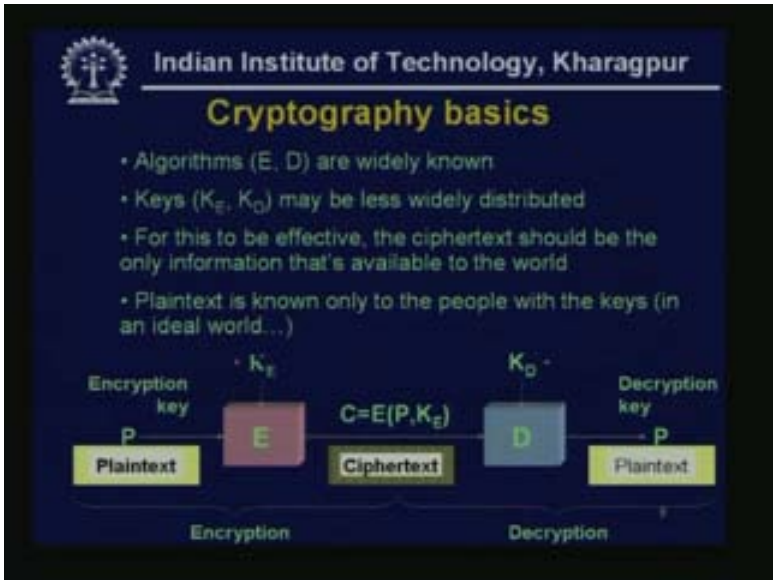
Now what kinds of intruders are there? There may be casual prying by non technical users out of curiosity. There may be snooping by insiders often motivated by curiosity or money. As a matter of fact it has been estimated that for most of the serious security breaches some insider is involved in majority of the cases. And when that happens it becomes more difficult to handle it. Determined attempt to make money may not even be an insider; it could be an insider or someone who wants to just make money. Then there is the commercial and military espionage. This of course is a very big business.

Military communication of course traditionally has been confidential so they were encrypted. So encryption basically derives its history for the military purpose. And now-a-days in the age of information the information technology is a very core part of the military machine of any country. So, security breach in these cases is of course a very serious issue and since most of the large commercial houses are now networked and as they have networked on one hand of course you deal with your business process in a much more efficient manner but at the same time you expose yourself to this kind of new threats which needs to be handled.

(Refer Slide Time: 08.25 - 10.07)

As I mentioned, for confidentiality cryptography is a time honored technique. Now it has become more and more sophisticated. Now-a-days with the help of computers if you are using the older techniques it is possible to crack those encrypted messages so now people have come up with better encryption algorithms and better encryption techniques. The goal is to keep information away from those who are not supposed to see it. You can do it by scrambling the data and use a well known algorithm to scramble data. The algorithm usually has two inputs; the data and key. Key is known only to authorized users. Now, relying upon the secrecy of the algorithm is a very bad idea. If you just have an algorithm and if you think that it is a secret algorithm then it becomes very vulnerable because all your communication is going to use that same algorithm so it becomes very difficult to ensure that the algorithm will indeed remain secret. So the modern cryptography depends on the secrecy of the key as its mainstay. Cracking codes is very difficult, with the modern encryption techniques as we will see.

(Refer Slide Time: 10.08 - 12.53)

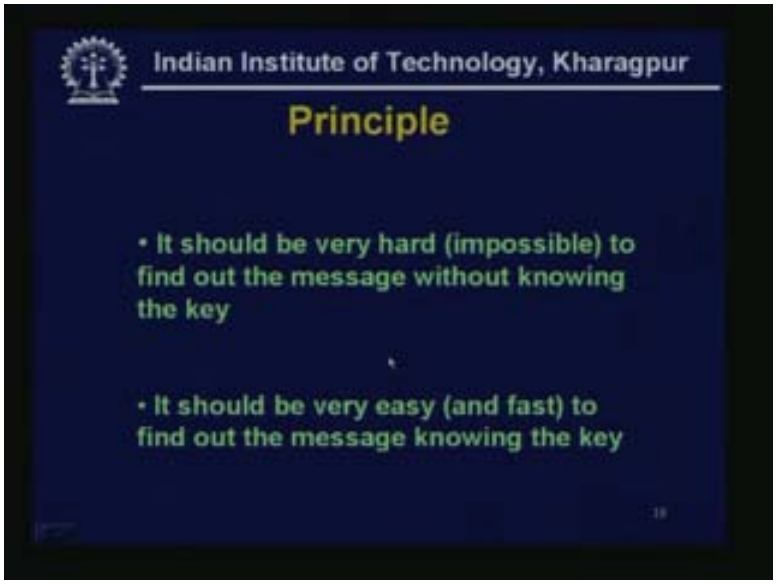


First let us see some basics of cryptography. Actually we have two algorithms in general. You have two algorithms E and D. We will assume that E and D are known. This means they are not only known to the sender and the receiver but whoever wants to hack into it or whoever wants to intercept it may also know E and D. Let us assume that E and D are known to everybody. There are two keys k_e and k_d, these are kept secret. So keeping these keys a secret is a very important part of any crypto system and so how to distribute the keys by themselves is the topic for our discussion.

Let us assume that these keys k_e and k_d, k_e is for encrypting the message and k_d is used for decrypting the message. In general k_e and k_d may be different. In some cases they are same but in some cases they are different. For this to be effective the cipher text should be the only information that is available to the world and the plain text is known only to the people with keys. In an ideal world, this is what happens.

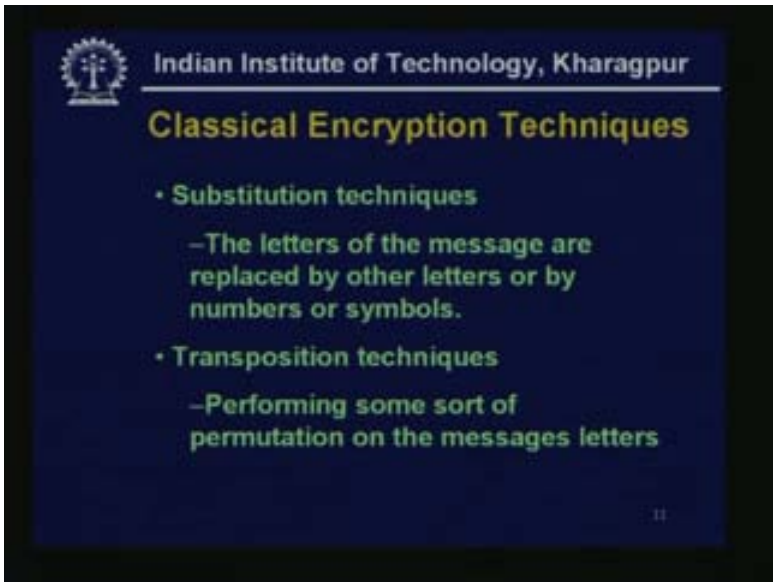
For example, we have got some plain text here which we want to send in a very secret fashion over the network. What we do is, first with the encryption key k_e and the encryption algorithm E we encrypt this. So, as we encrypt the plain text we get what is known as the cipher text c, so c is equal to E(p, k_e) that is the encryption algorithm and then the cipher text is sent. The idea is that, even if somebody intercepts the cipher text since he would not be having k_e it will not be possible for him to produce P or it will be very difficult for him to produce P. And on the other side there is a decryption key k_d and using the algorithm D and k_d we decrypt the cipher text to get the plain text back.

(Refer Slide Time: 12.54 - 13.05)



Therefore this is the encryption part and this is the decryption part. It should be very hard or impossible to find out the message without knowing the key and it should be very easy and fast to find out the message knowing the key. It is also difficult to find out the message even if you know the key or if it takes long time then it becomes very inefficient. So, in order to handle efficiency this should be fast if the key is known.

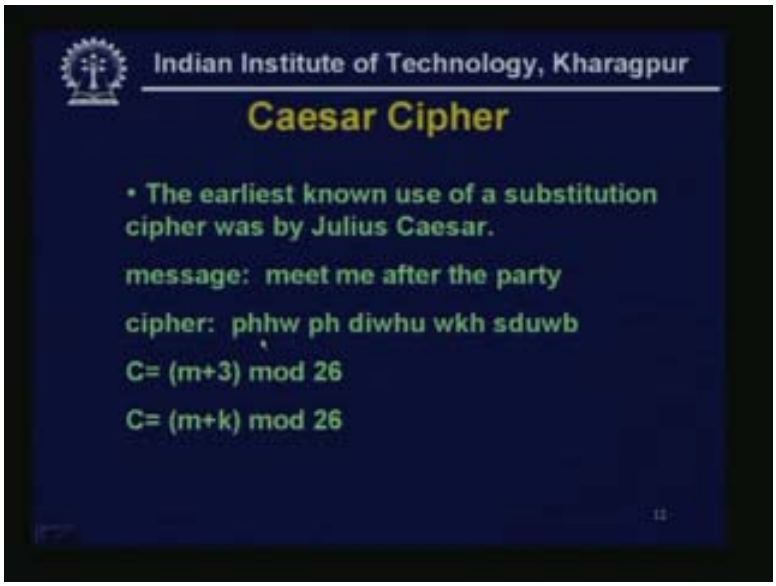
(Refer Slide Time: 13.23 - 13.58)



Before looking at modern encryption techniques let us look at some classical encryption techniques. There are actually two approaches; one is the substitution techniques. The letters of the message are replaced by other letters or by numbers or symbols. And

transposition techniques that performs some sort of permutation on the message letters. These two of course are very basic techniques and they are still used today but in a much more sophisticated fashion.

(Refer Slide Time: 13.59 - 15.09)



You may have come across this kind of encryption in some detective stories, at least in some of the classical detective stories where a message may have been encrypted in this fashion. One of the earliest known uses of the substitution cipher was by Julius Caesar; this is known as Caesar cipher. Suppose the message is ‘meet me after the party’ and your c is equal to m+3 mod 26 in this particular case then m becomes m n o p, e becomes h so ‘meet me after the party’ becomes phhw ph diwhu etc which looks absolutely gibberish to anybody. But of course with the help of modern computers trying out various possibilities it is very easy to crack this code. This is of course no longer used so it is just a kind of history.

(Refer Slide Time: 15.10 - 17.44)

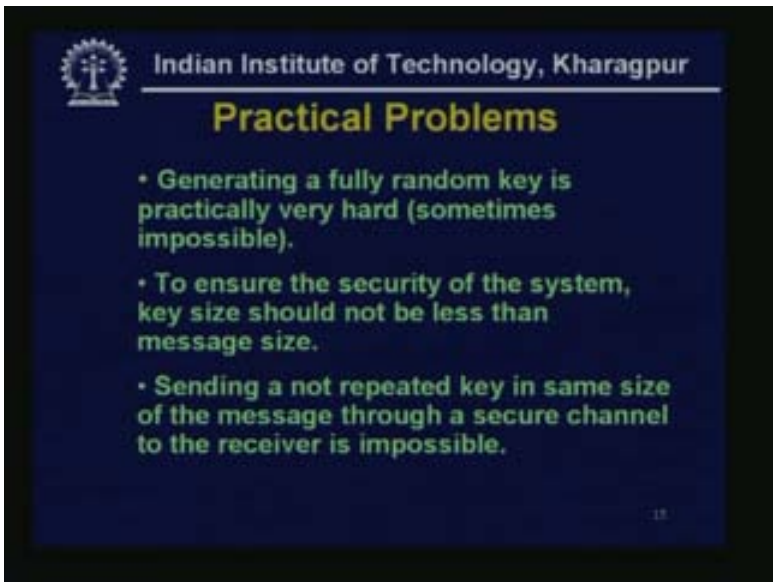
The other is, use any permutation of the 26 alphabetic characters. Caesar's cipher all of them are being displaced by the same amount by three letters. In mono alphabetic cipher this may not be so but you have basically a b c d e f g h etc and it may be any permutation of the same set of letters. Now, for encryption as well as decryption you must have this mapping from a to q b to e c to r and etc. Now under attack u becomes c, n becomes w, d becomes y so c w y u l q etc becomes something like this. You may have noted that we have not considered the blank over here and all of them and that is why it has come as just one string. If you get the reverse mapping then using a dictionary breaking up with these blanks is not difficult. This is mono alphabetic cipher.

Once again it is not difficult to break this, for example, if you have done something like this and if you have got a fairly long text there is a statistical table which is available on the internet also about the frequency of occurrences of different letters, for example, e, a, etc, there are some letters like this which occur many times more than letters like j, q, etc so this is available. So using this kind of a table you may even have a mono alphabetic cipher like this. Using this distribution it is quite possible especially with the help of computers, in those detective stories it was done by detectives but now-a-days a computer will do it. It is possible to guess some of the letters and as you guess more and more it becomes faster and finally you crack the message. This is also not such a great way of encrypting things. Once again we will look at this for historical purpose.

(Refer Slide Time: 17.45 - 18.33)

The other approach to encryption is transposition. It is performing a sort of permutation on the message letters. For example, if the message says 'meet me after the yoga party', then let us say the algorithm is simply this M e then et M e e t, the point is that alternately you write them in one line or in the other line and then you read the top line first M e M a t r etc and then followed by the bottom line e t e f etc. Once again this is quite easy to decipher.

(Refer Slide Time: 18.34 - 19.23)



Apart from this there are certain practical problems which you have to consider. One is generating a fully random key is practically very hard, sometimes impossible. And more

over to ensure the security of the system the key size should not be less than the message size. And sending a not repeated key in the same size of the message through a secured channel to the receiver is impossible, things like how to distribute this key amongst the potential senders and receivers needs to be understood. The previous one's possibly if we have a very long key with a length which is comparable to the length of the message then you can have more and more secured communication but having such long key which is almost equal to the size of the message then distributing is a problem.

(Refer Slide Time: 19.43 - 20.34)

Today let us see what we mean by computational security. An encryption scheme is secure if it takes very long time to break the cipher text. If you are using brute force may be you can break all text but then breaking the cipher text takes a very long time then it becomes infeasible. Lifetime is defined in each application. For example, military orders may be one hour to three years, check transaction may be it is for only one year, business agreement 10 to 15 years. So, if decrypting a cipher text takes longer than this kind of time then may be you are doing fine.

(Refer Slide Time: 20.35 - 21.00)

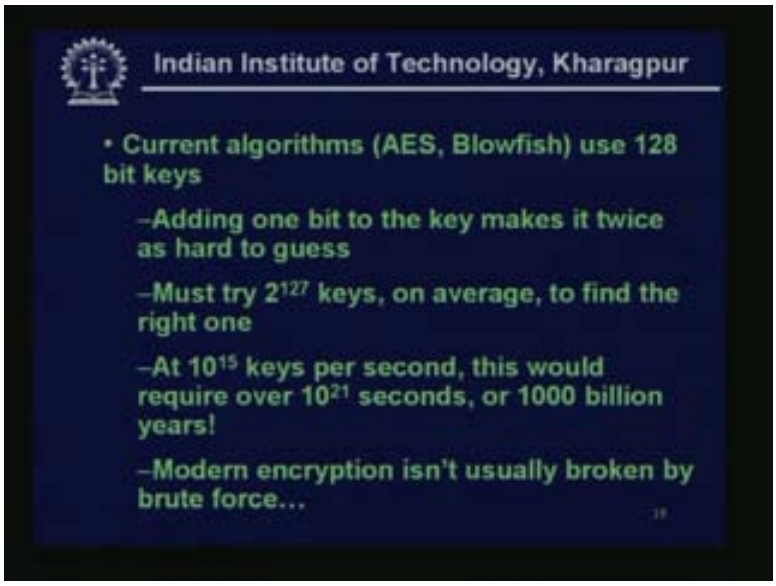
So the bottom line is that if somebody does not know anything about the key it must take more than several years to decrypt a message. With enough number of substitution and transposition modules we can make a strong encryption scheme and this is an algorithm called DES or Data Encryption Standard.

(Refer Slide Time: 21.01 - 22.11)

The basic DES module uses a 56 bit keys. The same key is used to encrypt and decrypt. Keys used to be difficult to guess, needed to try 2 power 55 on average, so modern computers can try millions of keys per second with special hardware. Actually you can make a very special machine which can break DES. But it is not easy as you can see that

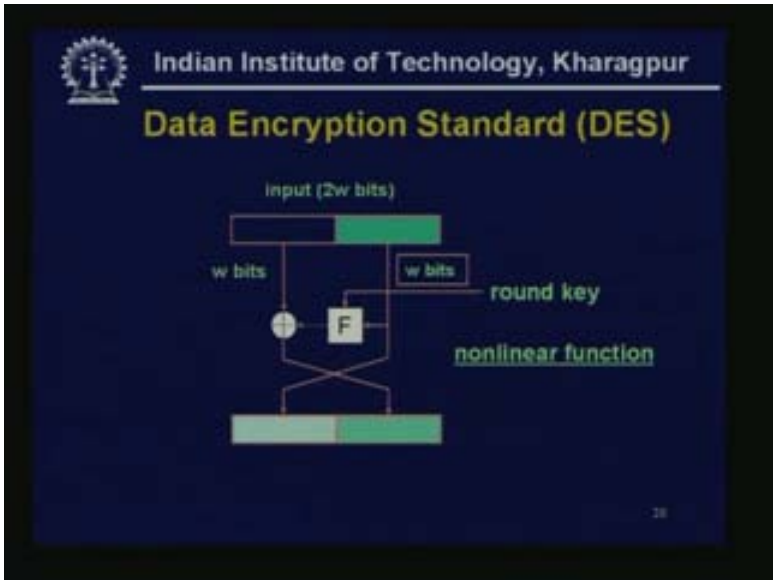
you have to make a very special hardware for trying out millions or even billions keys per second and then it is possible to break this and put a number of machines working in parallel etc. It is possible to break it in some time frame but even then DES is a very good encryption technique and the modern and much more difficult encryption techniques are based on DES.

(Refer Slide Time: 22.12 - 22.56)



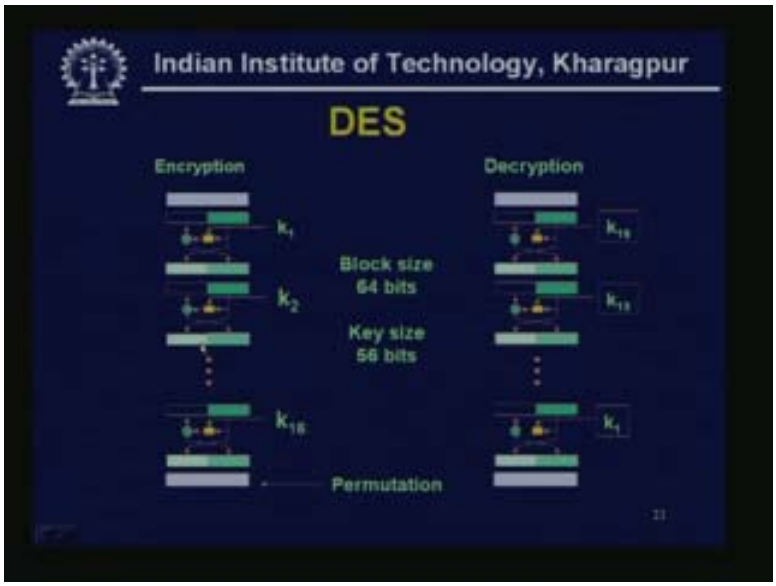
Let us just take a quick look on DES. The current algorithm is Advanced Encryption Standard AES which uses 128 bit keys. Adding one bit to the key makes it twice as hard to guess so must try 2 power 127 keys on an average to find the right one. At 10 power 15 keys per second this would require 10 power 21 seconds or may be thousand billion years. This of course is very good and modern encryption technique. It is not usually broken by brute force so what people try to do is they try to get more information. We will not get into attack crypt analysis but discuss just a part of it because we do not have time.

(Refer Slide Time: 22.57 - 23.44)



This is a basic DES scheme suppose, the input is 2w bits, you divide it into two parts, these w bits you do an xor with the output of this function and this function takes other w bits and a key for this round and these two feed into a non linear function which produces an output. And this output is xor with the first w bits. Now this xor is transposed to the second half and this part comes to the first half. So this is one round of DES.

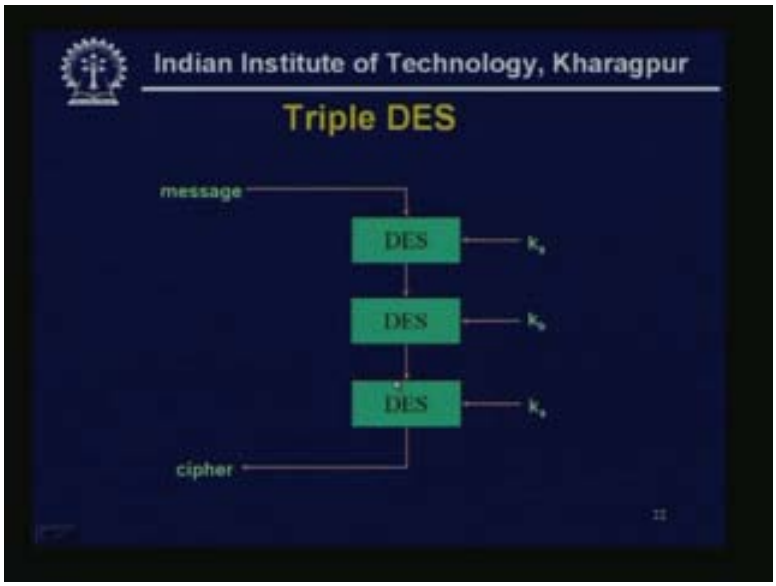
(Refer Slide Time: 23.45 - 24.29)



Actually DES goes in various rounds so for each round there are keys. Actually this is generated from 156 bit am not going into the details and each time you go through this kind of operation with that particular round key from k1 to k16 in 16rounds then in 16

rounds you get the final encrypted text. The decryption also uses the same set of keys only in the reverse order and if you do that you will finally get the plain text. So the original key size is 56 bits from which all these keys are generated.

(Refer Slide Time: 24.30 - 25.13)



Now-a-days as I mentioned, since DES can be broken sometimes these days people use triple DES. Triple DES is a modern encryption standard which is very difficult to break so you require three keys or sometimes only two keys are used; k_a, k_b and k_a once again. So you take the message, make it go through the first DES block k_a then this encrypted message you encrypt again using k_b and this encrypted message you encrypt again using k_a and this gives you the cipher text. So like AES this is also very difficult to break.

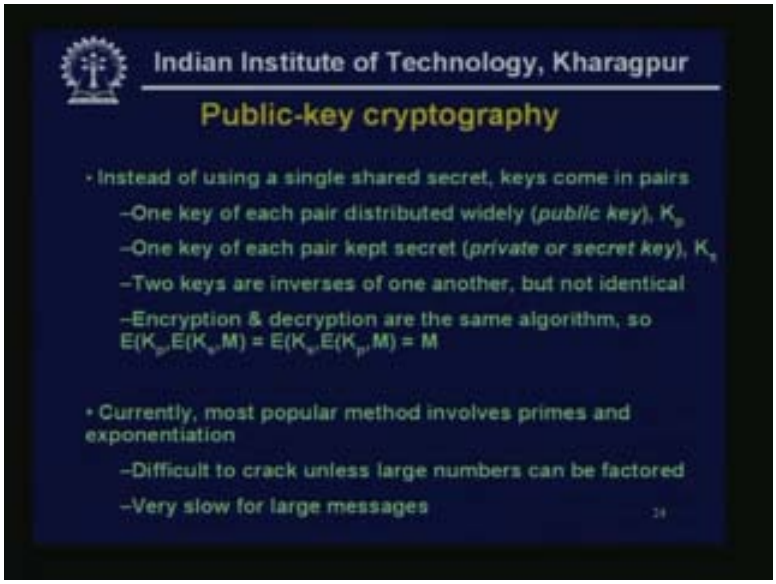
(Refer Slide Time: 25.14 - 27.42)

Another very important kind of cryptographic technique is the public key cryptography, this is asymmetric key. Till now we have been talking about the symmetric key cryptography. In symmetric key for the encryption and decryption you use the same key. So, if you use the same key, if you are doing the same something like a mono alphabetic substitution that table is available to both the parties, it is the same table so that is the same key basically.

Similarly, in DES or triple DES you use the same key or sets of keys in both the cases for both encryption purposes as well as for decryption purpose. Now, in the public key cryptography, this is another class of algorithms where the key that is used for encryption is not the key which is used for decryption. And knowing the key for decryption it is impossible to guess the key which was used for encryption. So this is the so called asymmetric key or public key cryptography. It uses two keys; one is known as the public key mainly for encryption and private key which is for decryption. Now these keys come in pairs.

Suppose A wants to send some message to B, now what will be available to A will be the public key of B. So what it is going to do is that it will encrypt it or and of course it will have his own private key. So you can do it either way. You can encrypt using your own private key and then send it. But then that can be decrypted with your public key. If somebody else sends it using your public key then I can decipher it using my private key. And since my private key is not known to anybody then nobody else can decipher it, and this is the basic idea. Another kind of function which is used is a trap door or the one way function.

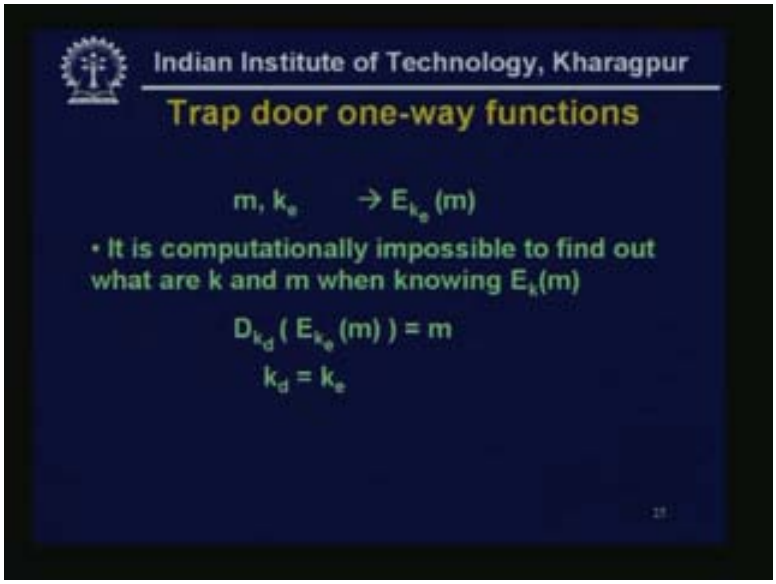
(Refer Slide Time: 27.43 - 29.17)



Let us look at public key cryptography quickly.

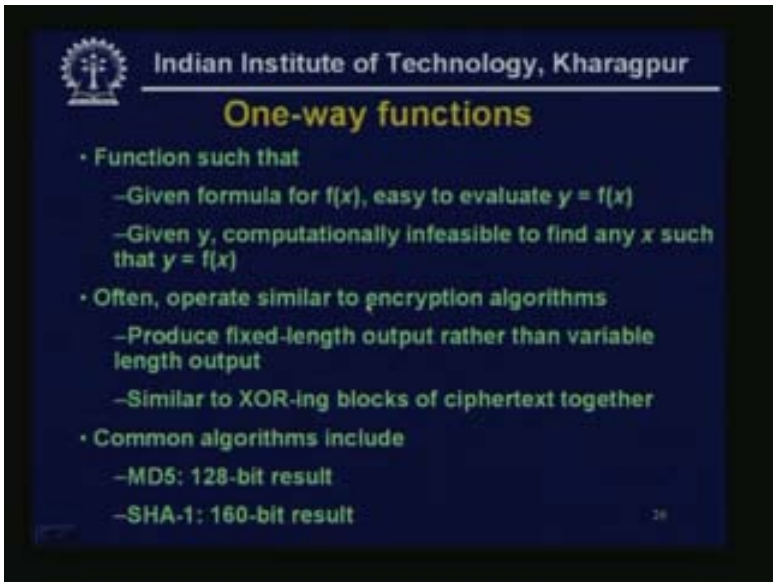
Public-key cryptography: instead of using a single shared secret, keys come in pairs. One key of each pair distributed widely which is called the public key and one key of each pair kept secret, i.e. private or secret. Two keys are inverses of one another but not identical. Encryption and decryption are the same algorithm. If you encrypt a message M using the secret key then using the public key if you run the same algorithm then you will get the deciphered message M. Similarly, if you encrypt using the public key and then decipher it that means run the same algorithm again with the secret key then once again you get M. So, currently the most popular method involves primes and exponentiation. This basically is based on the fact that this is difficult to crack the encryption unless large numbers can be factored easily and there is no known method for factoring very large numbers. Large number means numbers or integers with large number of places. The difficultly with public key cryptography is that it is very slow for large messages.

(Refer Slide Time: 29.18 - 30.00)



Trap door one-way functions: It is computationally impossible to find out what are K and M when knowing the E_k (M). So knowing M you can of course use the trap door function with this k_e to give E_ke(M). Therefore you can go in only one direction but from this side it is impossible to come on the other side. This is also sometimes used for authentication in digital signature as we will see.

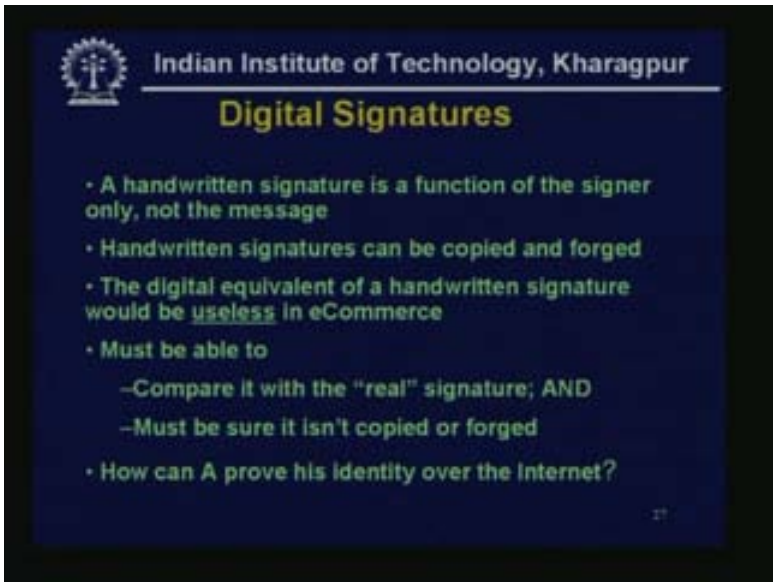
(Refer Slide Time: 30.01 - 30.41)



So one way functions are functions which given a formula for f(x) it is easy to evaluate y is equal to f(x). Given y computationally infeasible to find any x such that y is equal to f(x). Often operate similar to encryption algorithms; it produces fixed length output rather

than variable length output. It is similar to xor in blocks of cipher text together. Common algorithms include MD5, so 128 bit result or SHA 1 which gives you a 160 bit result from a text.

(Refer Slide Time: 30.42 - 32.11)

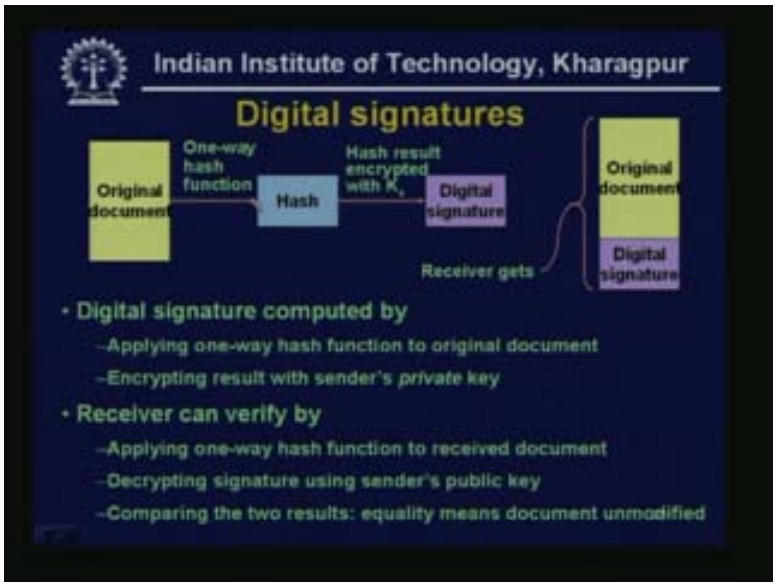


Now let us see one important application of all these; public key and one-way functions etc which is in digital signatures. A hand written signature is a function of the signer only and not the message. That means suppose I sign some document I can sign any number of documents, my signature will remain the same and it is very characteristic of my way of signing, my handwriting etc so it is difficult for ordinary people to replicate that although there are good forgers who can replicate many signatures. Now, the digital equivalent of handwritten signatures would be useless in ecommerce. So we must be able to compare it with the real signature and must be sure it is not copied or forged. Now how can A prove his identity over the internet that is the basic idea? When I sign a document I am basically saying that it is me alone who has sort of written this so that is why I signed the document or agreed to do this. Now how can I do this over a network?

(Refer Slide Time: 32.12 - 33.09)

This is the basic scheme of a digital signature. Digital signature is a function of both the signer and the message. A digital signature is a digest of the message encrypted with the signer's private key. So, we have a message M and it may be a very long message so use some secure hash algorithm to produce hash that is the message digest. That means you make it run through some hashing function which produces an output of its length which is a product of this particular message. Now you encrypt this hash using the signer's private key and this produces the digital signature. Now this is the digital signature of Mr. A on message M.

(Refer Slide Time: 33.10 - 35.16)

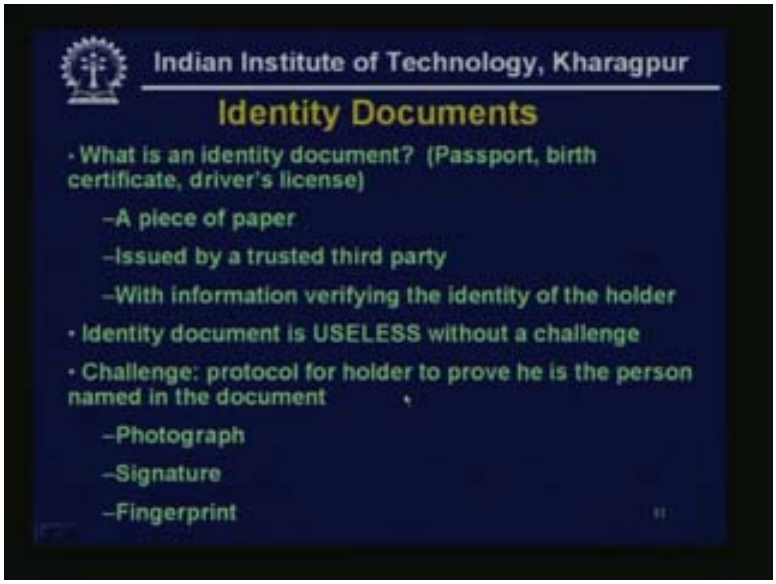


You have the original document, you use a one-way function or a hash function and the hash result is encrypted with a secret key or the private key of the signer and this gives the digital signature, now, the receiver should get the original document plus the digital signature. Of course, if you want to ensure that the original document also should not be seen by anybody then this entire thing that is the original document plus the digital signature you can now encrypt using the public key of the receiver. What the receiver will do is that the receiver will decrypt it using his own private key so that he gets back this. Since public key may be public so anybody could have sent this document, how do I know that this actually came from whomever it purports to be and this is where the digital signature part come in. So the receiver can verify by applying one way hash function to the received document so he will apply the same hash function to this document therefore he is supposed to get back whatever was here. Now he will decrypt the signature using the sender's public key. He has the sender's public key with him and since it was encrypted with the sender's private key now I can use the private key of the sender to get back the same message. So comparing the two results equality means document is unmodified because this digital signature could not have been produced by somebody else because this is a product of this document as well as the secret key of the sender and it is visually known only to him.

(Refer Slide Time: 35.17 - 35.25)

Therefore if the two hashes are equal then the message is authentic.

(Refer Slide Time: 35.26 - 36.42)



This does not solve the entire problem because sometimes you require some identity documents. What is an identity document? Identity documents are passport, birth certificate, driver's license, etc. This is basically a piece of paper issued by a trusted third party with information verifying the identity of the holder. Now, this has to do with the following: For example, even if you have a digital signature, the digital signature will only tell you that it will verify that this message has been sent by somebody who has this particular secret key. That means secret key corresponding to the public key that the receiver is holding. Now how do you absolutely guarantee that the secret key is held by the right person? That is where the identification comes in. So, a challenge is a protocol for holder to prove he is the person named in the document. In the non electronic world we do it with photograph, signature, fingerprint, etc.

(Refer Slide Time: 36.43 - 37.15)

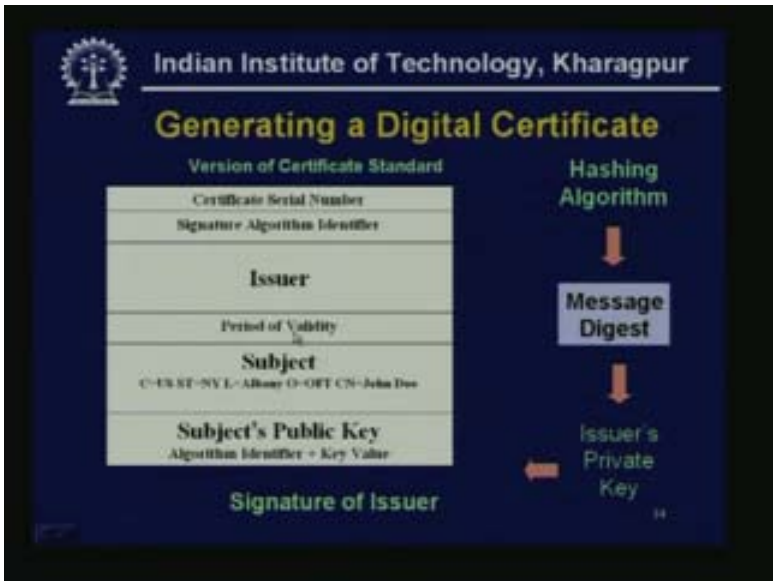
A digital certificate is a digital identity document binding a public private key pair to a specific person or organization. Verifying a digital signature only proves that the signer had the private key corresponding to the public key used to decrypt the signature. It does not prove that the public private key pair belonged to the claimed individual. We need an independent third party to verify the person's identity through non-electronic means and issue a digital certificate.

(Refer Slide Time: 37.16 - 38.54)

And a digital certificate contains all these things; the serial number, name of the holder etc. This has the public key of the holder, name of the trusted third party, then the digital

signature of a certificate authority. Data on which hash and public key algorithms have been used and other business or personal information. The point is that, the digital signature of the certificate authority since the certificate authority is the third party who is trusted. This means, if his digital signature is there, because since the public key of certificate authority is known then his digital signature can be verified. And in this particular case this authority is trusted. That means we know that something bearing the digital signature is indeed coming from that physical trusted authority. And now this trusted authority is basically certifying that the name of the holder is the holder of this particular public key. Of course the holder has his own private key. This private key would not be known to anybody else but then he is the holder of this public key.

(Refer Slide Time: 38.55 - 39.29)



We have a version of certificate standard. So these digital certificates can be checked by a machine that is the whole idea. You have a hash algorithm and then the message digest, issuer's private key and then put the signature of the issuer. The subject's public key is what is being certified. So, it is this algorithm plus the public key value. Then there is period of validity for this.

(Refer Slide Time: 39.30 - 40.26)

This public key cryptography is quite an elegant system. The only trouble is that, this is rather a computationally expensive process, it is quite slow. Pretty good privacy: It uses both public and private key to chart a middle course. It uses public key encryption to facilitate key distribution. It allows messages to be sent encrypted to a person that is encrypting with persons public key. It allows person to send message that must have come from her. That is, encrypt with persons private key.

(Refer Slide Time: 40.27 - 41.31)

The problem is, public key encryption is very slow. The solution is to use public key encryption to exchange a shared key. A shared key is relatively short which is about 128

bits or so. Therefore message is encrypted using the symmetric key encryption. Now what you do is that in the first phase you use the public key cryptography system to exchange just the shared key. This key may be shared just for this very session and then it may go. This is shared for particular session. Since this is 128 bit you can do it once even though it is expensive or this is a bit inefficient. And then, once both the parties are sharing the same key, this is the symmetric key, so this works much faster and the message is encrypted using symmetric key encryption. PGP can also be used to authenticate sender, use digital signature and send message as plaintext. There are various ways in which PGP can be used.

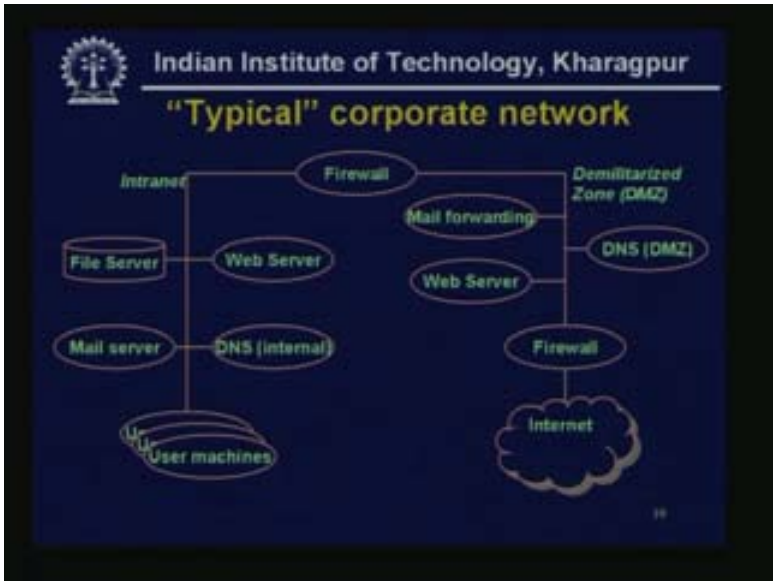
(Refer Slide Time: 41.32 - 43.32)

With this we come to the end of our discussion about some security issues which are very general and with which most of the service organizations are very much concerned. Security is the foundation on which all these so called e activities dependant upon. Now we will focus more on the network technology part of it that what we mean by the security of a network. This is security of messages in the network and now I am talking about security of the network itself. Some terms are quite commonly used here and one such device commonly used is the firewall. It solves poor internal security measures using the network. Now all these have to do with securing the functioning of the network. The other is an intrusion detection system. Sometimes an intrusion detection or intrusion prevention system is integrated with a firewall and sometimes they are two different boxes. So intrusion detection is that, I want to detect whether any unwanted or unauthorized person has some how intruded into my secured zone and once he intrudes into my zone he will have access to data and messages from my network which I do not want. It detects non network security breaches accomplished via the network. Therefore firewalls and intrusion detection, stock prevention are all very important and most of the network vendors have got separate boxes for doing this.

(Refer Slide Time: 43.33 - 43.58)

Therefore here let us see how they are being used. By the way there is also a question of authentication of users and what is used. Sometimes you may use distributed authentication, a centralized authentication, LDAP or AAA server for that authentication and you can do a distributed co-operation also.

(Refer Slide Time: 43.59 - 48.23)



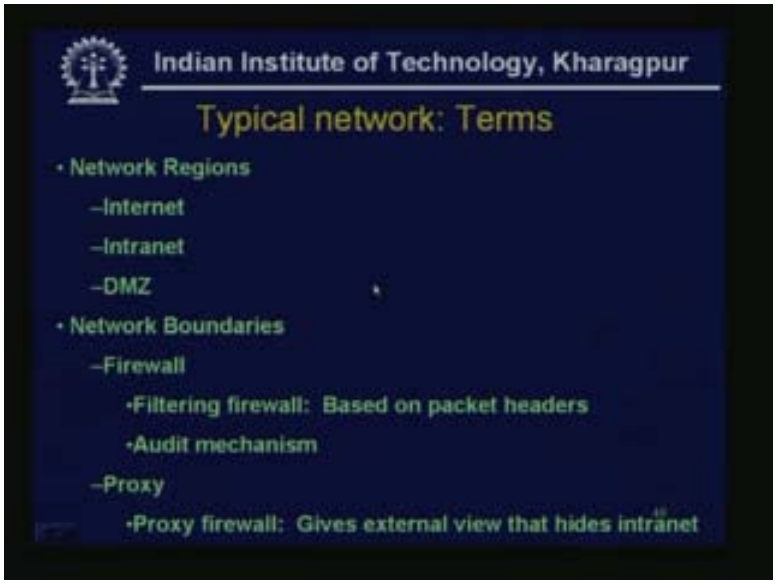
This is a typical corporate network. A typical corporate network is meant to be very secure. We start from the left hand corner. Suppose these are the user machines and then we have an internal domain name server or internal mail server, internal web server, internal file server, etc. This is the private network of the corporation, i.e. the intranet of

the corporation. This term intranet really means that we use the same technology which we use in internet and which you use in your internal network also. So you are using things like web browser, DNS, mail server, etc which work in the internet, the technology being deployed only for private purpose. So, this left hand part is only for the private purpose and only these authentic users should be able to use this intranet. This is connected to the internet as you can see here on the right hand corner. Although this is connected to the internet other people will generally not have access to this part. So what we do is, we try to make this internal network secure using a firewall and this is an internal firewall.

Then we have other machines also belonging to the same corporation like this web server which is used for helping people by providing servicing in the internet, we have mail forwarding and DNS etc. These are put in a zone which is known as demilitarized zone. Then this connects to the external firewall and then the external firewall finally connects to the internet. Actually what happens is that, what a firewall will do is that, a firewall basically inspects the packets and decides on whether these packets are ok and secured or not. It follows a set of rules. Depending on how you configure it is possible to have different levels of security at various ports of the firewall. A firewall may have 2 3 4 5 ports.

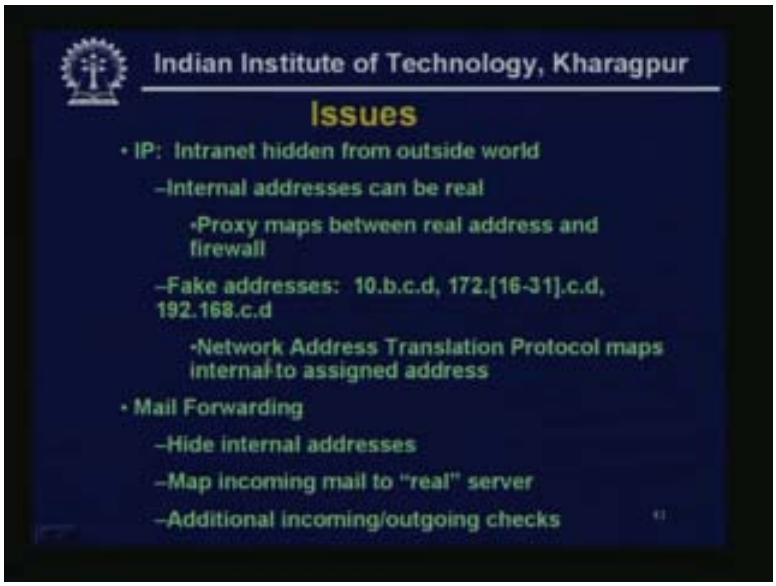
Suppose it has got 4 ports, it is possible to port-wise configure the security level of each of the port. Now what you want to do is that, you want to make your internal network absolutely secure. So somebody who wants to access through this firewall into something which is staying in the highly secured zone, that is absolutely the internal code network then he has to go through lot of checks, so that is a high security zone. But again what may happen is that you also have some machine like web server which you want to be open to the public. Similarly your DNS or your mail machine etc have to have a public dealing, a public face. So we want to keep some kind of medium level security for these kinds of machines. So they are put in a network area which is known as the demilitarized zone DMZ and then a firewall may connect directly to the internet also so that leg of the firewall would be of very low security termed as the low security zone. This may be one way of using two firewalls. Sometimes people will use only one firewall but this is a deployment using two firewalls such as one internal firewall and one external firewall.

(Refer Slide Time: 48.24 - 48.59)



Network regions are these internet that is not secure at all, intranet which is highly secure and DMZ which is the middle level security. And the network boundaries for all these different regions are at the firewall. So there may be filtering firewall based on packet headers, there may be audit mechanisms. A proxy may also be used as some kind of a security device.

(Refer Slide Time: 49.00 - 51.42)

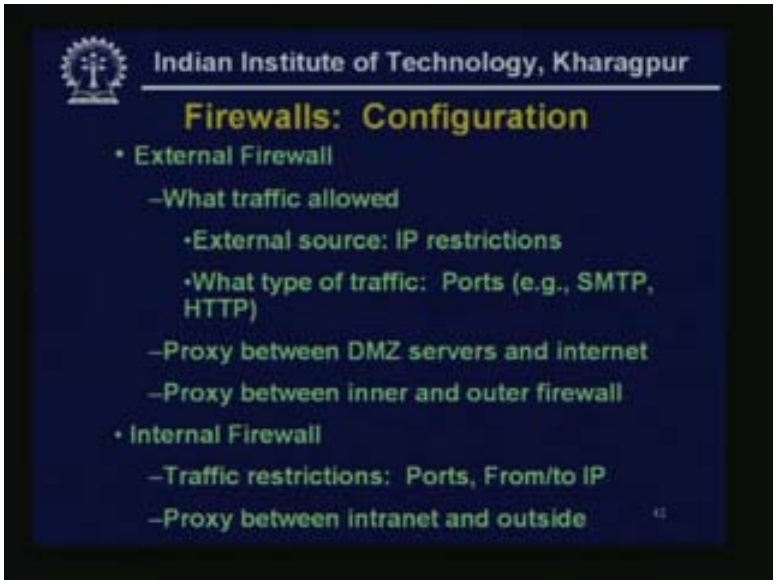


For example, you can use IP addresses for some low level of security. The network address translation came up as the IPv4 addresses have virtually disappeared and only some class C addresses are available. So, in order to obviate that what we did was that in

a internal network we used some private IP addresses and when we use a private IP address in my network, and in order to communicate we have to go through a proxy and the proxy will remember that a machine with this private address is wanting to communicate with the outside world, so it puts a valid IP address from a pool in place of the private address which is not really valid outside and then sends out the request gets the message and then sends it to this private IP. It is conventional to number the private IP addresses starting with 10 which is 10.x.x.x so that is one full class A address which is a huge address space for one organization. And the point is, the routers outside, are usually not going to route any address which starts with 10. because it knows that 10. is used for private IP. So if you use private IP addresses it is difficult for outsiders from the internet to log on to your machine unless he/she is going through some proxy and getting into your network in the first place. Therefore network address translation protocol maps internal to assigned address.

Mail forwarding: Hide internal addresses, map incoming mail to real server, and additional incoming and outgoing checks may be performed. Therefore all these are different things you can do to enhance the security of your network. It is not possible to make your network hundred percent safe but you can increase the level of safety through various measures, this is one kind of such measure apart from any firewall that you might have put.

(Refer Slide Time: 51.43 - 53.24)



For firewall configuration, in the external firewall, what you can configure is, find out what traffic is allowed. External source: You may put IP restriction so external source may only be from this or from these IP addresses, we will specify that. What type of traffic: Ports for example SMTP for mail or http for web etc, what kind of traffic I will allow and what kind of traffic I will not allow. May be I will not allow telnet in the secured zone at all from the outside.

Proxy between DMZ servers and internet and proxy between inner and outer firewall are the things which you can configure in an external firewall. the network has become such a burning issue these days, so more and more development is taking place in this region and especially in firewall design etc so in modern firewall it not only works very fast but it can look at lots of things. It can counter peer to peer messages and all kind of things it can handle.. For internal firewall you can put traffic restrictions on ports from or to IP address and you can proxy between intranet and outside. These are the things which do with the firewall.

(Refer Slide Time: 53.25 - 54.00)

For DMZ administration whether a direct console access is required? If a direct console access is required then naturally this is another place, this is somewhat troublesome. Or you can use special access using SSH Secured Shell Connections allowed from internal to DMZ administration connections or only from some specific internal IPs or only through internal firewall etc you can administer the DMZ. This reduces the security risk to only one or a few machines.

(Refer Slide Time: 54.01 - 54.23)

You can authenticate in various ways. One question always comes up is that whether your authentication will scale? You can repeat the authentication, have multiple administration, but if you have distributed authentication scheme then that is always good.

(Refer Slide Time: 54.25 - 54.26)

(Refer Slide Time: 54.27 - 54.40)

Let us look at some attacks and defenses. One kind of attack which is common is denial of service attack, routing attack, spoofing attack and may be there are other kinds of attacks people are thinking about.

(Refer Slide Time: 54.41 - 55.10)

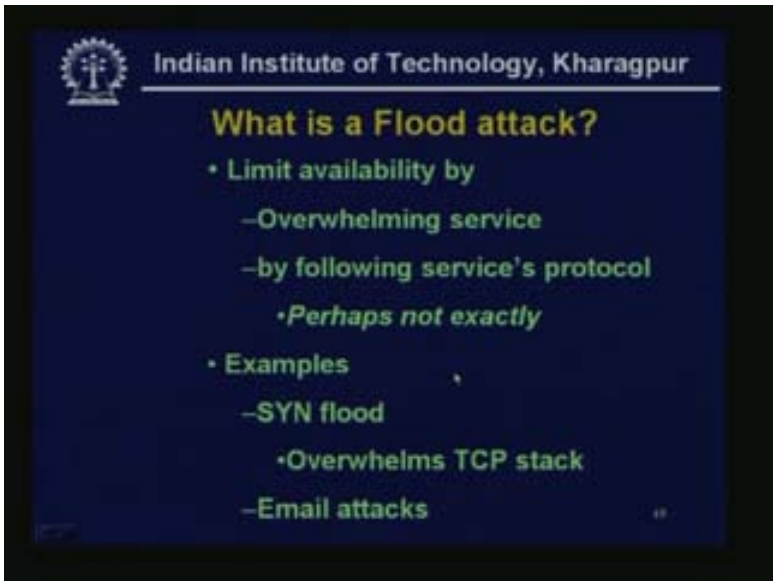
As people are thinking in a more secured way, the hackers and all other peoples are also thinking of many ways of compromising security. Confidentiality on the network is manageable such as encryption to protect transmission, public key cryptography, key management, etc. Integrity is reducible to single system: digital signatures verify source

and commit protocols handle network failure. What about availability? This is where the attacks on the network come into picture.

(Refer Slide Time: 55.11 - 55.40)

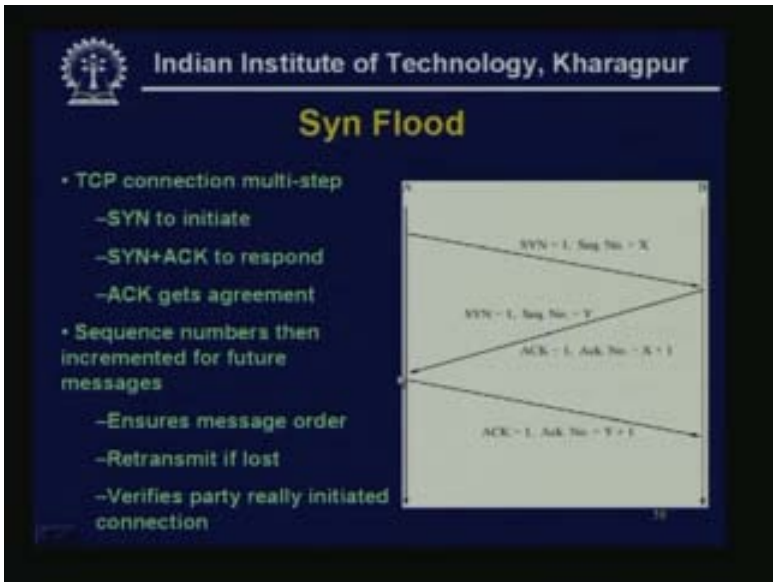
One is flooding: this is a denial of service kind of attack. That means overwhelm TCP stack on target machine which prevents legitimate connections. Routing attack is misdirecting traffic. Spoofing: when somebody is entering your network claiming to be a false identity then spoofing imitates a legitimate source.

(Refer Slide Time: 55.41 - 56.02)



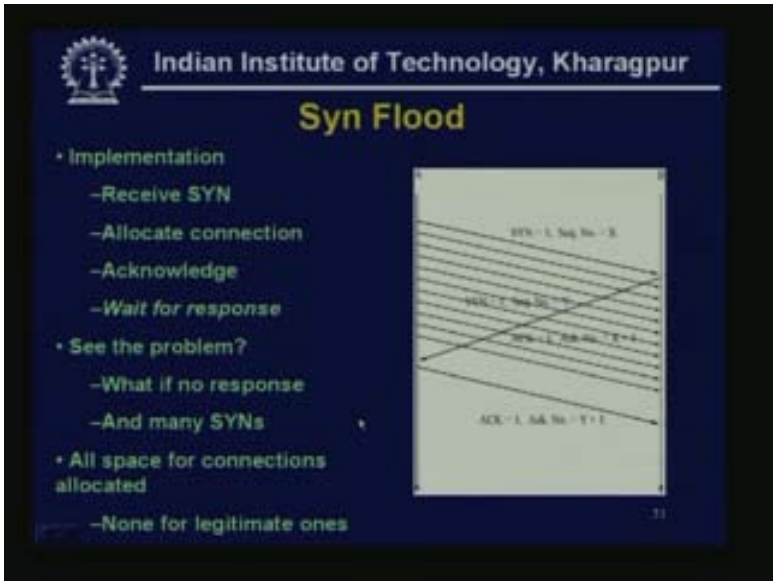
What is a flood attack? Limit the availability by overwhelming service by following service's protocol to an extent. Example is a SYN flood; it overwhelms the TCP stack or may be a large number of emails being generated by a script.

(Refer Slide Time: 56.03 - 56.39)



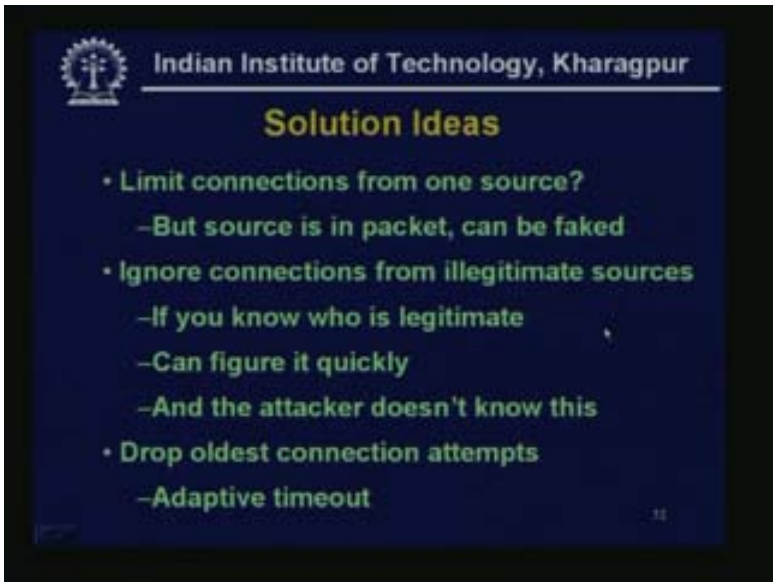
Let us look at SYN flood. In TCP protocol when a client initiates a SYN then it waits and then the server will acknowledge it and send a sequence number. The server will also send the SYN and then it will wait for an acknowledgement from the client. This is a multi-step process. Sequence numbers are incremented for a future message. It ensures message order and retransmits if lost.

(Refer Slide Time: 56.40 - 57.35)



What some malicious person might do is that receive the SYN, the server receives the SYN, allocates connection, acknowledges and waits for response from the other side, waits for this response. So what this is doing is that it is sending one SYN after the other in rapid succession. So, on the server side you will be opening so many connections and you will send acknowledgements and wait. Therefore what will happen is that the entire space for connections becomes allocated. And this is of course is done by a malicious user but a legitimate user can no longer get any access to this server because the server has become absolutely overwhelmed. Hence this is a denial of service.

(Refer Slide Time: 57.36 - 58.04)

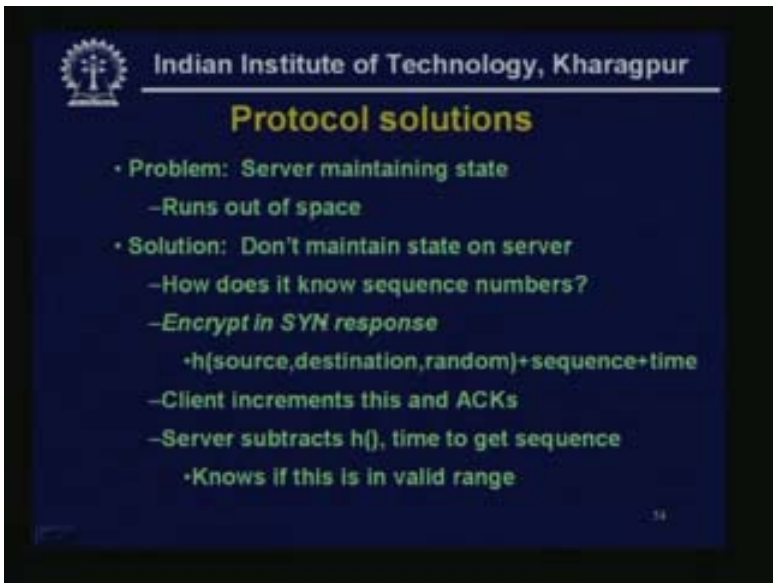


So you can limit connections from one source, ignore connections from illegitimate sources, drop oldest connection attempts etc. What the firewall will do is, the intrusion detection system will also try to detect that and block all the flood of SYNs etc which is coming from one source. But that does not solve the distributed denial of service attack which is coming from many sources.

(Refer Slide Time: 58.05 - 58.29)

Network solutions: TCP intercept: Router establishes connection to client, when connected establishes with server. So router comes in between server and the client.
SYNkill: Monitor machine as a firewall, good addresses: allows history of successful connections otherwise kills it. These are the intrusion prevention kind of situation.

(Refer Slide Time: 58.40 - 58.47)



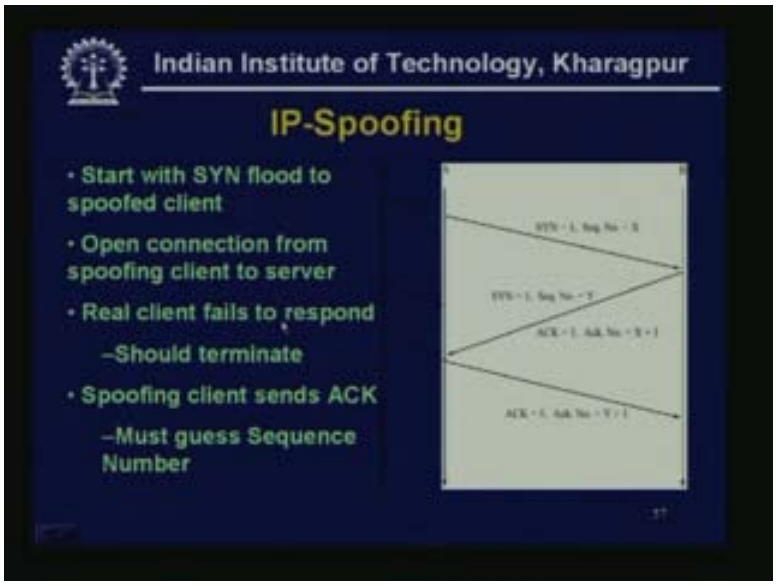
You can try to encrypt your SYN or make changes in protocol also but that is usually more difficult and cumbersome to implement unless absolutely it is your own and private network.

(Refer Slide Time: 58.48 - 59.12)

Service-Level Flooding: Overload the server: Looks into its processing, storage, etc. Typically garbage requests using legitimate protocol: Large emails to victim, many http connections, Heavy use of scripts. These overwhelm the server in some other way so that it cannot give legitimate service.

(Refer Slide Time: 59.13 - 59.15)

(Refer Slide Time: 59.16 - 59.18)



IP Spoofing: What somebody can do is that, instead of overwhelming server he can overwhelm the client and then take on the role of the client. So, there are various ways in which these network attacks are coming and there are ways to handle this. This is a developing and important field. I have just given an overview today, thank you.