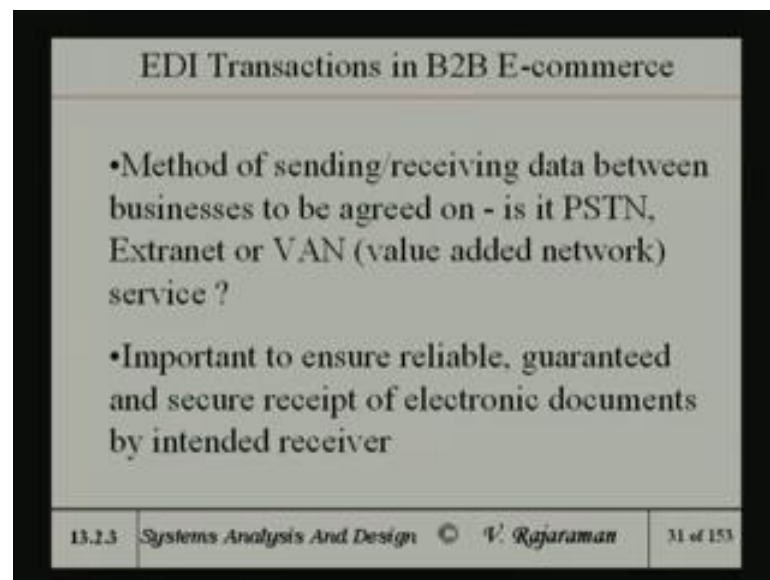


Systems Analysis and Design
Prof. V Rajaraman
Department of Super Computer Education and Research
Indian Institute of Science, Bangalore

Lecture - 34

EDI and EDI transactions - EDI stands for Electronic Data Interchange. And it is an essential formats and standards required for two businesses or multiple businesses, transact business in E-commerce. To this avoids having to keep various data again and again. So, whenever say for instance a purchase order comes, if it is in standard EDI format it can be interpreted automatically.

(Refer Slide Time: 01:50)



And the actual data, namely the purchase order, the actual acceptance of the order, the dispatch or delivery note and so on. All of them had been sent through a network connecting the two business. As I pointed out, these networks can be either a private network. That means, there is a dedicated line between the two or it can be a public network, there is internet infrastructure using the public switch telephone network.

Or there is something called value added networks, which are actually maintained by service providers, which are semi private. In other words a value added networks are essentially provided. So, that it is not open to the public, it is open to only a certain number of limited companies. So, security is definitely better than internet. But, you cannot have absolute security. But then, they go ensure some encryption and so on.

And separate out the various companies in within that plan. So, each one is separately encrypted in possibility of one being able to read the others data and so on is not there. A recent introduction which runs on the internet. But, does provide more security than internet is called the virtual private network. Virtual private network is something which is not a private network, like a dedicated line.

But, it gives you higher security, than the internet. Primarily by using encryption and so called security services in the which are provided by the internet protocol. So, I will not get into the detail of the virtual private networks. Because, you actually learned about them in your network course. But, it is sufficient for me to say, that the acronym which is used is SSL, VPN.

That is Secured Socket Layer in the IP traffic internet traffic, Virtual Private Network. So, they call it SSL VPN. And SSL, VPN is provided by many vendors like Cisco which is vendor of routers and so on. Also provide they also provide some of the IISP's like. For instance, in India sify provides an SSL, VPN service for clients which does provide higher security levels.

Because, SSL VPN effectively you might say, reserves or tunnels through internet in a certain path which is kept secure and which is not easily, you might say intruded by the hackers and so on. So, it provides a better definitely better security than internet. So, the question which company has to decide is what do they want to follow. Do they want to have a private network, dedicated network which is very, very expensive. Or they want to use a value added networks or the VPN.

Today, the trend is towards VPN. Because, it is a cheaper than dedicated line. It is also cheaper than the value added networks. In fact, value added networks they are not too many of them. Now, existing in our country I mean it is to be provided by large companies like IBM and so on. So, primarily all these come because it is important to ensure reliable guaranteed and secured electronic documents by the intended receiver from a sender.

(Refer Slide Time: 06:32)

EDI Using Value Added Network Service

- VAN provides post box for all subscribers
- Guarantees delivery
- Open 24 hours, 7 days a week
- Provides security, acknowledgement, audit trails for transactions, non repudiation by users

13.2.4 Systems Analysis And Design © V. Rajaraman 32 of 153

The value added networks normally provide close boxes for all the subscribers. Now, what the value added network is a private network. And but then as a same shared private network and at guarantee is delivery. It is open 24 by 7 and provides security acknowledgment or a trace route at what time and so on. And no repudiation is possible by users. Because, third party is actually keeping an audit trial.

(Refer Slide Time: 07:05)

EDI Using Value Added Network Service

- Some VAN'S provide conversion of EDI forms to application format
- Disadvantage high cost. Used by large businesses - may not be cost-effective for smaller businesses

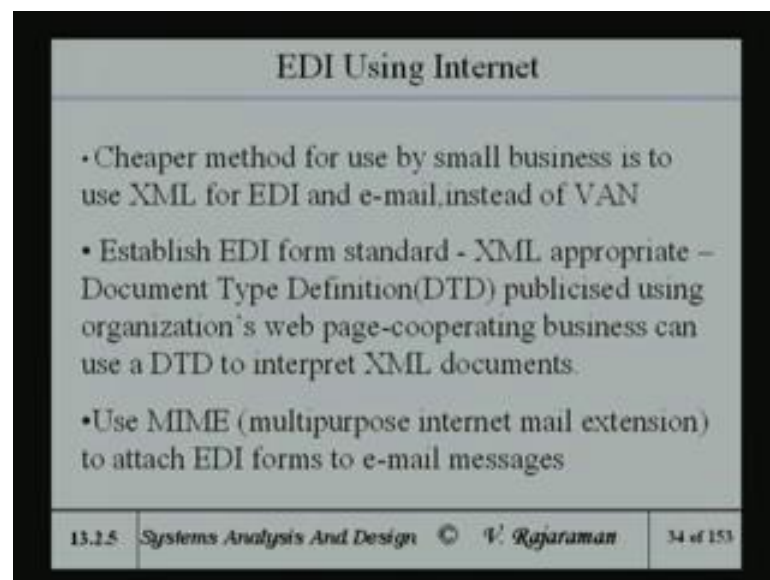
13.2.4 Systems Analysis And Design © V. Rajaraman

Some VANs also provides a conversion from the electronic data interchange format to application format, which a company may use earlier. So, that they stay there in other

words translation from the standard EDI to the internal structure is the service that provide, which allows you without I am to disturb your current method of working with documents to still as you have to EDI standard.

Of course, this is the disadvantage compared to using a say a SSL, VPN or the internet is its cost is high. And so it is used only by large businesses and not by smaller businesses.

(Refer Slide Time: 07:57)



The slide is titled "EDI Using Internet" and contains three bullet points. The footer includes the text "13.1.5 Systems Analysis And Design © V. Rajaraman 34 of 153".

- Cheaper method for use by small business is to use XML for EDI and e-mail, instead of VAN
- Establish EDI form standard - XML appropriate – Document Type Definition (DTD) publicised using organization's web page-cooperating business can use a DTD to interpret XML documents.
- Use MIME (multipurpose internet mail extension) to attach EDI forms to e-mail messages

13.1.5 Systems Analysis And Design © V. Rajaraman 34 of 153

So, to use the internet with EDI as I pointed out XML is becoming a better standard. Because, XML along with the document type definition publicized by the various participants in E-commerce provides a way of essentially having a method of communicating. Because, you can have a agreed upon format and both parties can use XML and use the same format.

And of course, it is better to kind of adhere to EDI like format. Because, that is universally used by many, many companies. But, you can still adapt EDI and use XML as a method of communication on the internet or VPNs. And along with XML one uses what is known as multipurpose internet mail extension to attach EDI forms to e-mail messages. This is part of the internet infrastructure.

(Refer Slide Time: 09:29)

EDI Using Internet

- Can use Simple Mail Transfer Protocol (SMTP) of internet
- If secure transmission needed use S/MIME (Security enhanced MIME) which uses encryption and digital signature –(We will describe encryption and digital signature later in this module)
- If very long document or many documents are to be sent together File Transfer Protocol (FTP) may be more appropriate.

13.2.6 Systems Analysis And Design © V. Rajaraman 35 of 153

And as call a simple I can use simple mail transfer protocol on internet to transmit this documents. If secure transmission is needed something called security enhanced mime is used, which uses encryption and digital signature. And I will talk about encryption and digital signature a greater length later on. And a very long documents or many documents are to be sent together.

If we send it as e-mail I may bind some all together and send using an FTP or a File Transfer Protocol again that of internet.

(Refer Slide Time: 10:01)

EDI Standard

- Defines several hundred transaction sets corresponding to each type of business document such as invoice, purchase order etc.
- Defines data segments - corresponding to groups of data elements such as purchase order line
- Defines data elements - which are individual fields such as price, quantity etc

13.2.7 Systems Analysis And Design © V. Rajaraman 36 of 153

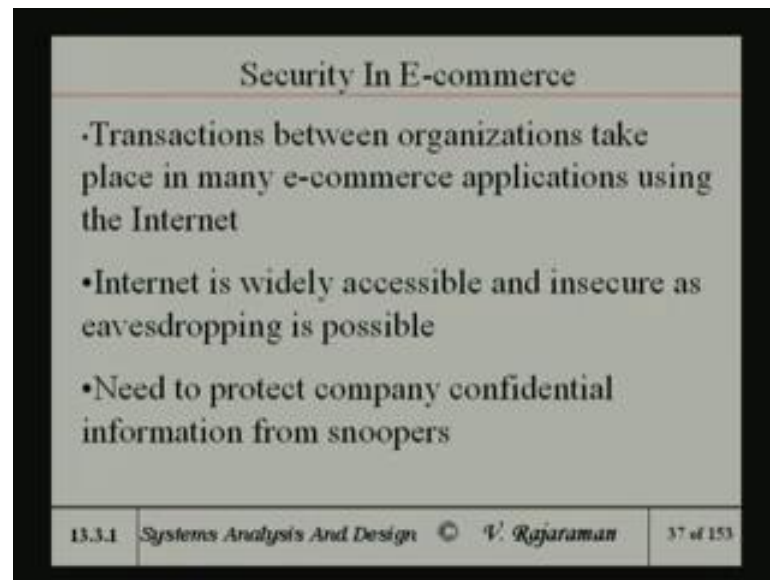
And again, you know just repeat the standard EDI defines several hundred transactions. Defines data segments, corresponding to groups of data elements. And defines data elements with individual fields, such as price, quality etcetera. This is just to reiterate the fact that it is necessary to have an EDI standard document format to facilitate the interpretation of documents. And to facilitate the working of many different companies together.

Now, as I pointed out, if we use internet at even few days before public. Now a day's particularly if you public switch telephone network. It becomes extremely important to ensure security. If you say pure private network even then that private network one or expect no body can intrude. But, some even there certain amount of security concerns are necessary.

And one should be aware of it, even though the level of awareness may not be as much as level of awareness about the internet. But of course, as I pointed out again, the private interconnection is becoming more and more rare, because of it is expensive. And most companies are really going towards the using the internet as the public infrastructure. Because, a lot of work has gone in security to be able companies to work together on the internet, without comprising on security.

So, primarily in succeeding a part of lecture may be part of next lecture I will be concerned about how to ensure security for electronic transactions carried out over the internet. So, we assume that the infrastructure is internet, we assume the transactions are carried out between multiple parties. And we would like to see how to ensure security.

(Refer Slide Time: 12:25)

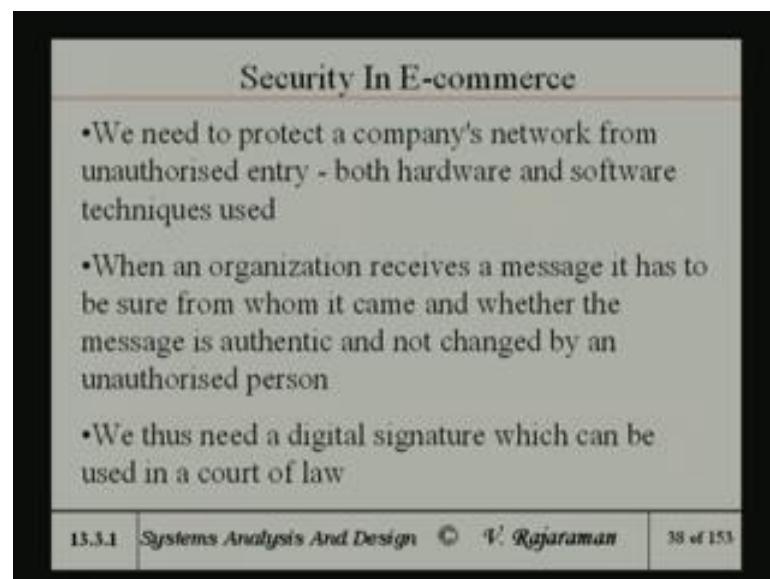


The slide is titled "Security In E-commerce" and lists three bullet points. The footer contains the text "13.3.1 Systems Analysis And Design © V. Rajaraman" and "37 of 153".

| Security In E-commerce | | |
|---|--|-----------|
| <ul style="list-style-type: none">• Transactions between organizations take place in many e-commerce applications using the Internet• Internet is widely accessible and insecure as eavesdropping is possible• Need to protect company confidential information from snoopers | | |
| 13.3.1 | Systems Analysis And Design © V. Rajaraman | 37 of 153 |

So, as I because internet is insecure and eavesdropping is possible by intruders and so on. It is necessary to protect company confidential information from snoopers. That is, hackers, people who get into system and so on.

(Refer Slide Time: 12:44)



The slide is titled "Security In E-commerce" and lists three bullet points. The footer contains the text "13.3.1 Systems Analysis And Design © V. Rajaraman" and "38 of 153".

| Security In E-commerce | | |
|---|--|-----------|
| <ul style="list-style-type: none">• We need to protect a company's network from unauthorised entry - both hardware and software techniques used• When an organization receives a message it has to be sure from whom it came and whether the message is authentic and not changed by an unauthorised person• We thus need a digital signature which can be used in a court of law | | |
| 13.3.1 | Systems Analysis And Design © V. Rajaraman | 38 of 153 |

So, we also need to protect a company's network with unauthorized entry. Though if the companies intranet is connected to internet. In theory every computer in that organization becomes accessible to an outsider, through the internet using the IP address of all the

individuals in the company, this can be very dangerous. Because, several people may work in confidential information.

And they won't allow unauthorized hacking of confidential information, which may be used by different people in the organization. So, it is very necessary to make sure that the company's intranet is protected in some sense or insulated from hackers, from other intruders, who may come on internet. Now, there are two methods which many companies use.

One method, which many companies use which I know is that they have a private intranet, within the company which is highly secure, which is not connected to the internet at all. So, in other words it is completely isolated or insulated from the internet. And there are only few machines, which interact to the outside world. And those machines only transact business between companies.

And so one cannot get into the local intranet. That is of course, complete physical separation of the company's intranet, that confidential work is going on. And then of course, it cannot be isolated you cannot even remove it at all, completely from the external world. So, some machines are connected to the internet, that is one way.

The other way is to use certain kind of machines at the boundary, they are called firewalls to prevent entry by outsiders into the internet. So, I am going to talk a little bit about these issues. So, when an organization receives a message, it has to be sure from whom the messages come and whether the message is authentic and has not been changed by unauthorized person.

So, we need also something called a digital signature, which can be used in a court of law. Let me explain a little bit what I mean by this. When you get a purchase order from somebody, say from a company normally in a manual system. The purchase order is a print is kind of typed or printed. And at the bottom that is a signature of the individual who has ordered. And normally some kind of a company seal also.

So, the company seal and the signature roll on the order is a paper document, which authenticates the fact, that the entire document has been sealed as the person who is signing and the signing person is responsible. Tomorrow say later on, if the company relieves. Now, that they say I never place purchase order. Then, you can take the

company to court by producing this purchase order. And say that, they did send up an order.

And then, I sent material based on the order. So, it is very difficult for the company to kind of say for I did not do that. Because, there is a signature there. So, this has been used for a long time to authenticate document. Signature is an authentication method. In fact, many important documents or contracts and so on, which may be multiple pages, every pages signed physically by somebody.

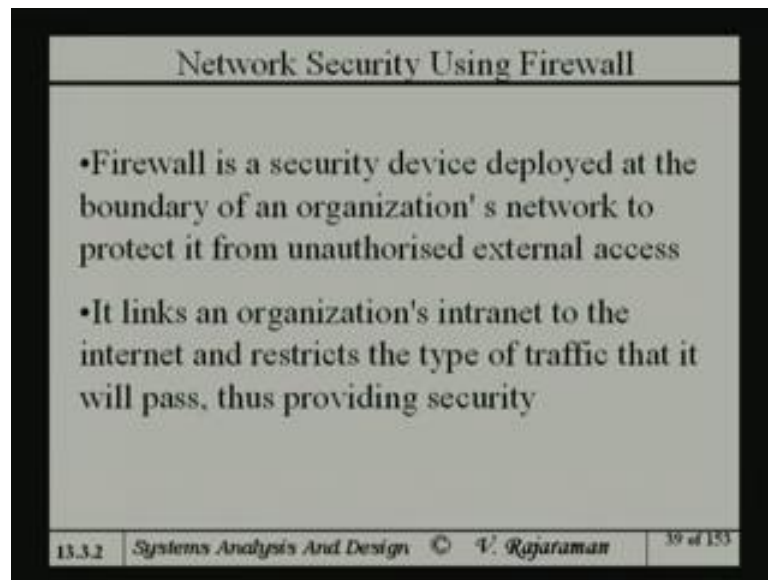
And even, if corrections are made in the text. And the corrections are made, there at the bottom they say so many corrections are made in this page. And on the side where the corrections are made, there is a signature. So, signature physical signature kind of authenticates a document and ties up the document to the person who actually create the document.

So, in the electronic world when some document comes. Somebody can masquerade and send the document. And you may be like to believe that came from some company. But, it may have come by it may have been a fake. So, there is need for authentication. So, there should be an equivalent of the physical signature in the electronic form and it is called digital signature.

And digital signature must be such that, just like a physical signature. Signature should be tied to the document. And the signature along the document has got to be authenticated. And can stand up in a court of law for scrutiny. So, this is important, so we will also talk about digital signature. Now, as we said that to insulate a company's local intranet from hackers and so on.

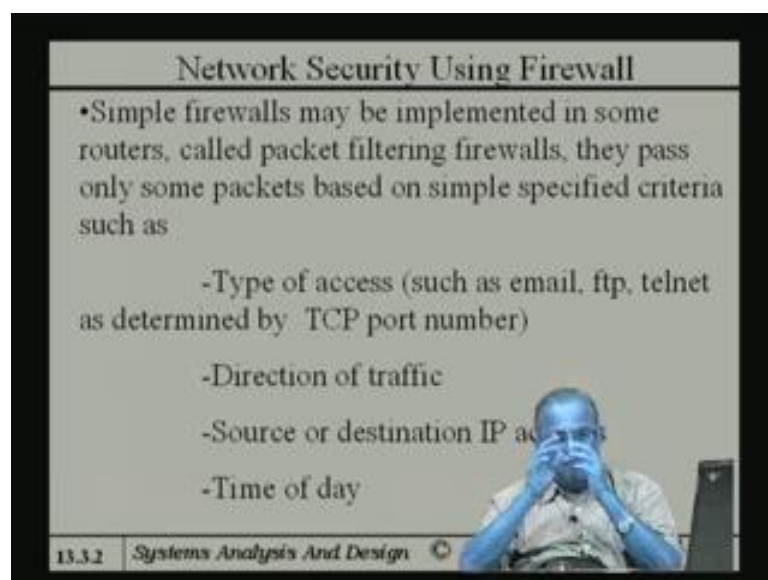
You provide at the boundary of your intranet some device, which in some sense provides a protective wall between your internal network. And the universal internet is called a firewall. So, where is deployed the boundary of the network.

(Refer Slide Time: 19:33)



It could be either a hardware device or it could be some software running on a particular server. Depends upon the level of security you require. And the amount of money you are willing to invest. It the firewalls function is to links the organizations intranet to the internet. And restrict the type of traffic, that will pass in and out of the intranet to the intranet to the internet, thus providing security.

(Refer Slide Time: 20:07)



Simplest firewalls may be implemented in some routers. That is every company when the internet at the boundaries of router which routes all the data, which comes out of that

intranet to appropriate IP addresses. So, this is a normally a router is a hardware device sold by some vendors. And some routers are called packet filtering type routers.

So, they add to the firewall they pass only some packets based on simple specified criteria as time of access. Now, they for instance the router may allow only e-mail. They may not allow FTP, Telnet and so on. Telnet allows an external user to login to a machine in your organization. And that can be very, very dangerous only trusted people are allowed to go Telnet, many organizations just do not allow Telnet from outside the organization to the internet of the organization.

So, the router can actually deeply programmed to filter out some of the disallowed facilities. Like, it may disallow large files from going. So, FTP may be disallowed or it may disallow Telnet. It may allow disallow e-mails to send kinds of addresses and so on. It also sometimes the filters the something going out of the organization. And something coming out of the into the organization.

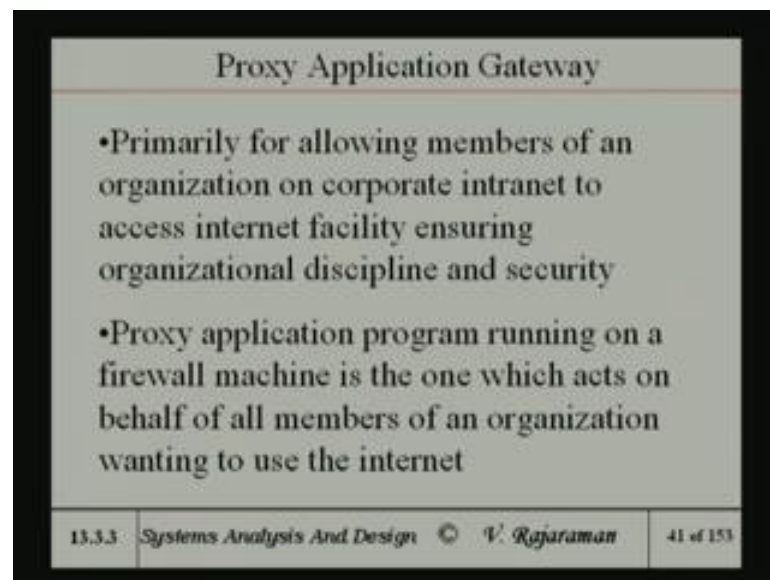
For instance many colleges put a firewall primarily program the router, you might say to disallow the students one looking at certain websites, which are considered harmful, which are not considered useful for the students in the college. So, there may be some sites like, gaming sites, music sites and other sites, which it has no student to have a business to access them.

Because, primarily they can access information from the internet, which are appropriate for the curriculum and further use. But, not things like basic files and video clips and stuff like that. So, those websites which provide all these things. And of course, some companies also ban electronic due to c-commerce from inside the company. So, some built in sites may be also banned.

So, there is a filtering. So, the web's cannot be actually certain web pages cannot be browsed. So, that is based on the source and destination address. Also in other words, some selectively in the company some may be allowed to have high security clearance to be able to unrestrictedly go to any other website. Or they may be allowed to telnet outside or somebody like you know a top person whose got a secure machine may be allowed to telnet, the companies machine when he is traveling.

So, these are decisions which are taken at the highest level of the company and implemented. And also you can program it, that at certain times of the day certain types of traffic are disallowed. And certain times of the day the source traffics are allowed. Because, it depends upon the busy time and the non busy time.

(Refer Slide Time: 24:15)



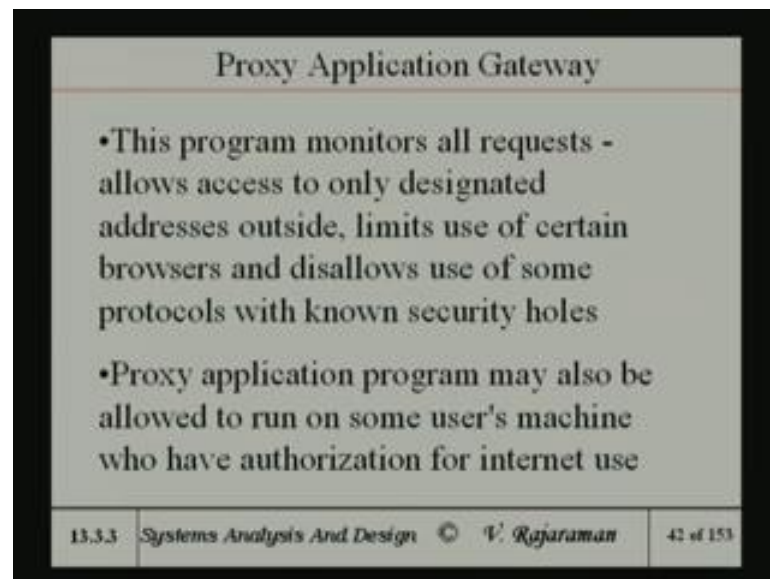
There is something called proxy application gateways. And they primarily for allowing members in an organization on a corporate intranet to access internet facility, ensuring organizational discipline and security. In other words they do not want to completely ban internet. But, you still want to restrict the freedom of the of use.

So, there is something called a proxy machine. Proxy is something which works on your behalf. So, proxy application programs, where in of the firewall machine. So, whether as I said an instead of a router it is actually a computer and this machine one which acts on behalf of all member of organization wanting to use internet.

In other words, it is a some kind of a gate keeper, which acts as proxy or something on your behalf as an intermediary between the internet and yourself. And similarly when some traffic comes in internet that will decide. Whether, it can be actually sent to the person whom it is addressed or not. So, these issues are actually you might say, it is a security or a watchman standing at a gate, who decides and like know the who acts on your behalf.

Like for instance, you may have a some people have the security within a company. So, all types of unnecessary salesperson are not allowed inside the company. And disturb the people working there and only if there is a prior appointment a person is allowed. Similarly, here also there is a certain. In other words that security person is acting on your behalf. And filtering out the visitors who are coming in and so on.

(Refer Slide Time: 26:24)



The proxies main job it monitors all request. Allows access only to designated addresses outside. Limits use of certain browsers and disallows use of some protocols with known security holes. In other words it is effectively a gate keeper which make sure that the people from inside the company. They do not have access free access to anywhere. They also sometimes proxy application programs are run in the users machine, we have to authorize them to use the internet.

Because, if it is a gate way for a firewall, sometimes it may not allow at all internet access for a certain set of IP numbers. And only for certain IP numbers it may allow internet access. And in that case they provide some kind of a proxy for the users machine itself.

(Refer Slide Time: 27:25)

Hardened Firewalls With Proxy Application Gateway

- Any one from inside or outside an organization give their user id, password, service required to the firewall machine which acts as one's proxy (ie. does ones work on his behalf)

13.3.4 Systems Analysis And Design © V. Rajaraman 43 of 153

Anyone from inside or outside an organization given the user id, password, service required, they are given to firewall. So, they once the firewall gets all this information, it acts as a proxy and decides what is to do be done. It works on behalf of the user.

(Refer Slide Time: 27:41)

Hardened Firewalls With Proxy Application Gateway

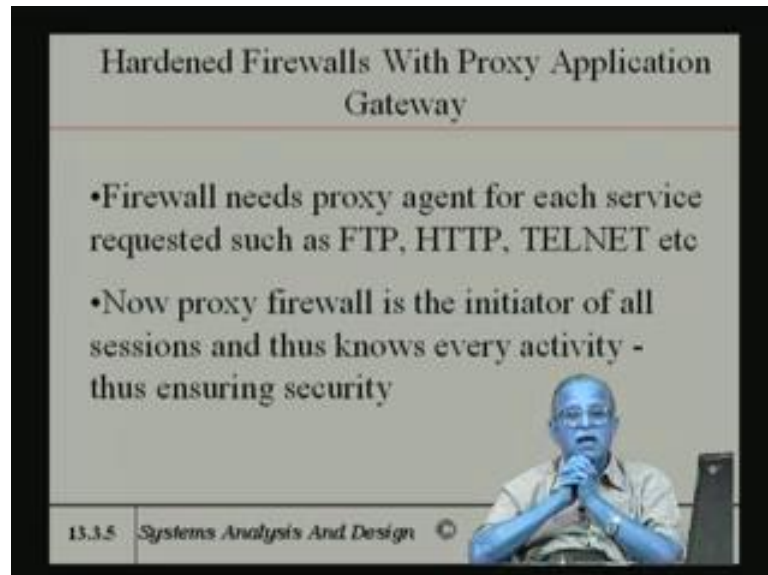
- Proxy firewall is now server to the requestor's desktop PC and also a client to some other requested service acting on requestor's behalf

13.3.4 Systems Analysis And Design © V. Rajaraman

It is actually you might think out proxy is a server to requestors desktop PC. But, it is a client to those requesting service in our absence this guy you know. In other words if a particular service is requested by a person of the company, he sends it to the firewall

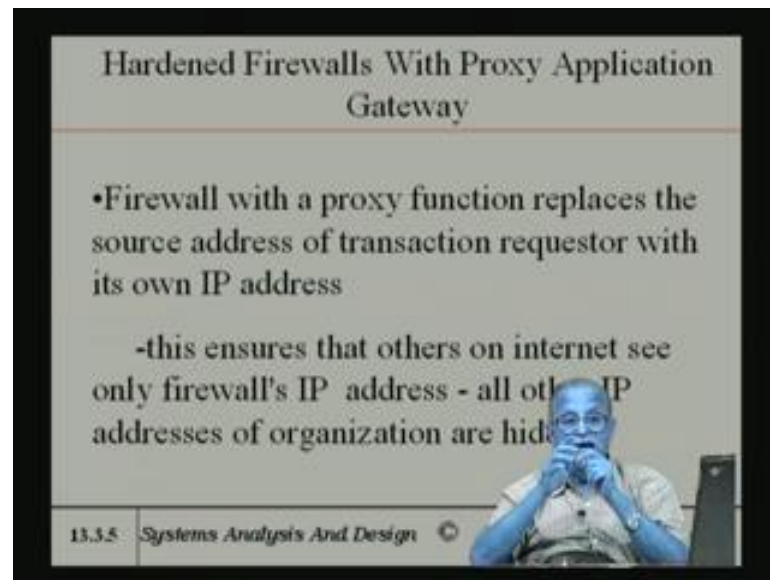
server. But, server itself is a client for service. So, she tries to get it is a kind of a intermediary you might say.

(Refer Slide Time: 28:15)



Firewall needs proxy agents for each service requested. So, in other words you have number of different you might say dimension or agents, which do work on the behalf. Like, FTP, HTTP, TELNET, etcetera. And I said you may ban some may allow some depending upon the IP address of the user. Proxy firewall is a initiator of all sessions and thus knows every activity. So, it is actually a big brother watching what is going on. And ensures security.

(Refer Slide Time: 28:48)



The slide is titled "Hardened Firewalls With Proxy Application Gateway". It contains two bullet points: "•Firewall with a proxy function replaces the source address of transaction requestor with its own IP address" and "-this ensures that others on internet see only firewall's IP address - all other IP addresses of organization are hidden". In the bottom right corner, there is a small video inset of a man speaking. The bottom left corner of the slide has the text "13.3.5 Systems Analysis And Design" followed by a small circular logo.

Hardened Firewalls With Proxy Application Gateway

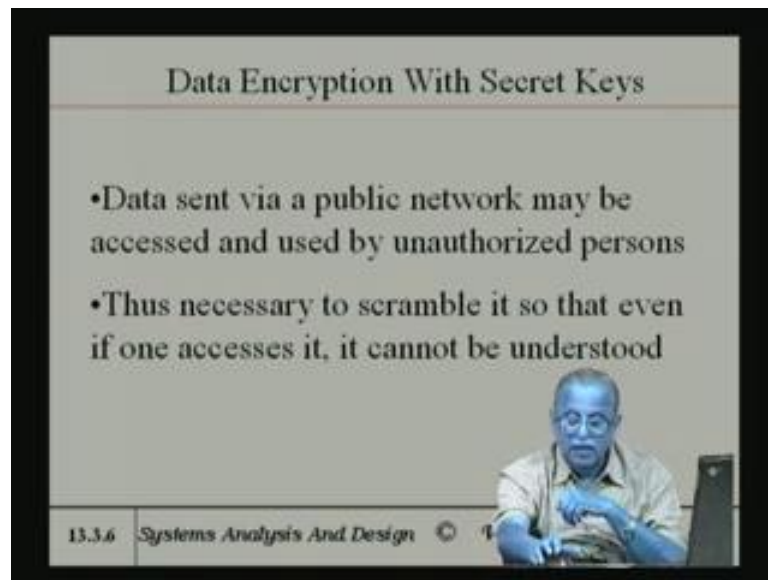
- Firewall with a proxy function replaces the source address of transaction requestor with its own IP address
- this ensures that others on internet see only firewall's IP address - all other IP addresses of organization are hidden

13.3.5 Systems Analysis And Design

Like firewall is a proxy function replaces the source address of transactions requested it is own IP address ((Refer Time: 28:57)) very important. Because, if the IP address of any of the people in the company gets known to outsider. Then, he can use the IP address to get access to a machine. And to proven that, the proxy assert filter out that IP address. And only presents you the IP address, because now it becomes the virtual client asking for the service.

So, the external world only gets access to the IP address proxy. And the proxy is the secure system, secured gateway. It ensure that always an internet, see only firewalls IP address. And all other IP address within the organization are hidden.

(Refer Slide Time: 29:42)



So, the primarily there is a the firewall is something, which kind of controls traffic you might say. And controls the type of traffic between the internet and intranet. And provides some kind of a, you might say a security wall which essentially disallows intrusion. And this is an important function. But, the entire thing is normally some hardware on which some software is running.

Apart from the firewall, there is also a need for some virus protection. Some companies put in the firewall computer itself also a virus protection software, which will filter out, which will take out every mail which is coming in to the company do the virus analysis of that. And anything with viruses it will just filter out. And only send those which have no viruses inside.

Some companies also try to do a virus scanning of mail going from inside the company to outside the company. Because, that way the company will not get a bad name of spreading the virus. And so some virus scanning is also done out going information. There is one more important thing, which is a rare piece of software it is called a spam filter. Lot of unnecessary mail comes to the organizations, trying to sell things and so on, which waste time of people.

Because, when they get you know hundred mail ninety of them may be spam or junk mail, only ten may be useful to them. So, certain programs called spam filters. The spam filters effectively acts on behalf of all the users in within the intranet. And tries to kind of

filter out all known spammers you might say. And this is another function this strictly speaking virus protection and spam filtering are not part of the firewall function.

Firewall primarily is a security enhancing device. But, over and above that there is a large server kind of large firewall. And have software running on it, which also does this over and above that. Or of course, depending upon the company may put, one more machine have to be the firewall to do the filtering business. But, it is up to the companies information, the person who organize the computing facilities or the intranet facilities.

Now, apart from the hardware method like a firewall. And the software running in the firewall and so on. It is also lot of software method which are required and that is called encryption. And I will talk about encryption with rather more the secret keys. As data centre at private network, may be hacked by unauthorized persons will need to be able to protect your messages by garbling that message.

So, even if somebody gets hold of the message. Because, it is in garbled form the difficulty, it is difficult for him to interpret. In fact, coding of messages have a long history, even during roman times and times of our old rajas and maharajas and so on. When messages are being sent from say from the king to be able somebody at the battle front will not be written in plain text.

If you write in plain text, if an enemy agents hold of it. Then, you exactly know what was ordered to the front by the king. So, it is kind of encoded or garbled. And it is garbled using some kind of a system called a encryption system. And how to decrypt that encrypted system is known only to the receiver. And the receiver will be able to decrypt it doing the encryption method. And that is being that is very long history of encryption.

So, in the new era of internet there was of course, taken a greater importance for electronic traffic over the internet. The major difference caused is that, all traffic over the internet is now digital. So, the encryption is all on zeros and ones or digital information. So, the encryption is the scrambling or making the garbling the text or digital text.

The text which is going, as you know all text will be in ASCII. ASCII will be sets of 8 bits per character. So, ultimately they are bit string. So, if the text is garbled even if one access it cannot understand what it contains.

(Refer Slide Time: 36:10)

The slide is titled "Data Encryption With Secret Keys". It contains three bullet points: "•Similarly data stored in data bases accessible via internet should be scrambled", "•Method of scrambling known as encryption", and "•Method of unscrambling known as decryption". In the bottom right corner, there is a small video inset showing a man with glasses speaking. The bottom left corner of the slide has the text "13.3.6 Systems Analysis And Design" followed by a small circular logo.

So, similarly we want to protect data stored in databases, which are accessible by internet if it is scrambled and store it. So, even if somebody gets hold of it will not be able to understand what is there in that disk. So, method of scrambling is known as encryption. And method of unscrambling is known as decryption. As I said if the rajas send some message to the person at to a general at the front. The he decrypts the encrypted messages came from the raja to actually understand what the instructions are.

There are certain types of terminology which is used, when we talk about encryption and decryption by plain text, we mean data in it is natural form.

(Refer Slide Time: 37:16)

Plain Text And Ciphertext

- Plain text is data in its natural form
- Encryption is taking data in any form (Text, Audio, Video etc.) and transforming it to another form which cannot be understood
- Transformed data is known as cryptogram or cipher text

13.3.7 Systems Analysis And Design © V. Rajaraman 49 of 153

Like, ASCII form of a message encryption is taking data, which is essentially string of bits. And transform it into another string of bits, which cannot be understood. Because, we dealing a strings of bits and in digital word. Whereas, textual information or audio information or radio information all of them ultimately become bit strings.

The encryption method we are going to talk about is does not depend upon the type of data it is applicable to multimedia data. Because, the reason why I am saying this is that many companies are trying to sell music over the internet. So, if they have to encrypt that music and the person who has bought the music, he gets a decryption key to be able to decrypt that bit string and actually hear the music. Similarly all the television programs are encrypted.

So, unless you take or listen to that channel and get a decryption key, you cannot actually view that particular television program. Here in satellite radio, like the world space and so on. The radio broadcast is through satellite in a digital form and they encrypt this program. Because, their revenue thus there are not any advertisements.

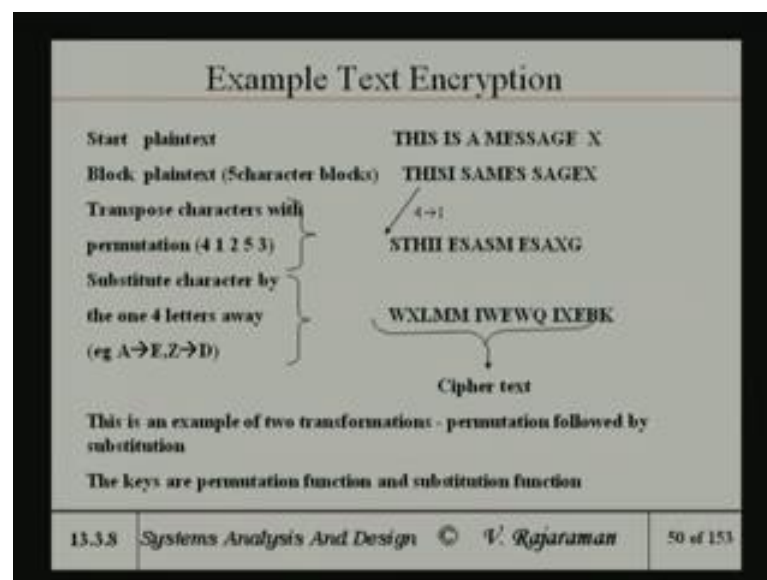
So, the revenue is your subscription. So, that are the subscribers get a decryption key, which is linked the particular radio set you have got. The radio circle has a certain serial number and will be given depending upon the serial number of radio a decryption key. So, when the broadcast you had set up the decryption key on your radio set, only if the

decryption key is properly set. The music which comes on from the satellite will be decrypted by the radio set so for you to be able to hear music or news or whatever it is.

So, most digital services now audio, video and so on which are pay by use you might say do use encryption. And so the method encryption and decryption does not depend upon the type of data. The transformed data is encrypted data. So, you take plain text, when I say plain text does not really mean only textual data, it can be plain text means audio, video or text and whatever it is.

The transformed data, when the plain text is encrypted and transformed. Transformed data is known as cryptogram or a cipher text. Cipher text is the garbled form of the plain text.

(Refer Slide Time: 40:55)



One very simple encryption method for a text I am giving example is that, suppose a plain text say this has a message x. One method encryption, which essentially brings out the principle, which use this encryption. In fact, this principle is used also in some of the digital encryption methods, which I am going to talk about is block the plain text. That is you take say five characters at a time.

So, this is a message you are essentially squeeze out all the blanks first of course, because blanks carry no information. So, squeeze out all the blanks and adopt the text into blocks of five characters, the file is arbitrary I could have cut up into six characters

or seven characters whatever it is. For illustrative purposes I am actually cutting it up into five characters.

And then, once you cut it up. Then, you apply a transformation called a permutation transformation. Permutation transformation is in this case is 41253. It means that the fourth character becomes the first character here. The first character become the second character here. And the second character becomes the third character here. And fifth character becomes the fourth character. And the third character namely becomes the fifth character.

Because, this permutation key is long five digits long and this says position one is now the plain text. Position two is 1, position three is 2, position four is 5, position five is 3 this is called a permutation. So, I permutes so I take five characters permute with this. And similarly I take this five permute and this take this five and permute. So, now I got a permutation, suppose the permuted text.

And after doing the permutation, there is something called a substitution. That is, take a character and replace it by a say replace a leave out B C D and take the fourth character. So, A is replaced by E and you can look at the alphabets as A to Z in the circular way. So, Z will get replaced by leave out A B C, Z will be replaced by D. So, if I take S, S will be replaced by S T U V W. T replaced by T U V W X that way.

So, you take the fourth character from the existing character. In the natural A B C D sequence and get those cipher text. Now, the cipher text, if you see cipher text. And compare with this original text you cannot make head and tail out of this. It looks very, very different from this. So, this is the plain text and this is the encrypted text or cipher text, there is an example of two transformations. One is the permutation transformation followed by a substitution transformation. The key is a permutation function and substitution function.

So, in order to decrypt it I should know the both of them. And I should apply them in the reverse. In another words while I doing the cipher text, now what I would do is W if I know the key. Now, I w replace W by S, because T U V W. So, I go backwards W V U T S, that is the way I go backwards. So, this is way knowing this I can go backwards and get this. And knowing this, I can go and back the permutation again. And this and get back the original text.

So, that is a well idea, so it is the encryption permutation and substitution. And decryption if I know the keys is to do the reverse.

(Refer Slide Time: 45:36)

Symmetric Encryption.

PLAINTEXT (m_1, m_2, \dots, m_n)

CIPHER TEXT $(c_1, c_2, c_3, \dots, c_n)$

Where $c_i = k(T_i(m_i))$ In which T_i is permutation of i^{th} character and k is substitution.

13.3.9 Systems Analysis And Design © V. Rajaraman 51 of 153

So, to make it more you might say abstract a plain text consists of m_1, m_2, m_3 up to m_n , where each one is a block and cipher text is c_1, c_2, c_3 up to c_n , where c_i is the permutation, which T_i is the permutation of i^{th} character. And k is the substitution c_i is the substitution and these two operators. That is the keys which are applied to this.

(Refer Slide Time: 46:01)

Symmetric Encryption.

- Decryption by applying same transformations in reverse on cipher text.
- This method called symmetric key encryption as encryption and decryption performed using same key.
- Normally the encryption/decryption algorithm is publicised. Only key is secret.

13.3.9 Systems Analysis And Design © V. Rajaraman 52 of 153

Now, to decrypt applying the same transformation reserve, as I pointed out. This method is called a symmetric key encryption, it is called symmetric, because knowing the encryption key I use that same encryption key at the receiving end. And apply it in reverse to get back. Normally the method of encryption is made public to the user. In the sense that, you will tell the user that I am going to use a permutation and a substitution, so that is known.

But, actually the permutation key and the substitution key are not made known. Because, I can see that you can see, the permutation key can be randomized again many, many permutation keys. Similarly, substitution can be four characters otherwise five characters the way are one, two characters away anything alright, it is arbitrary. So, both of them are doing arbitrary, unless the person knows the actual key used even though he knows its permutation and substitution. He will not be able to get the actual plain text from the coded text.

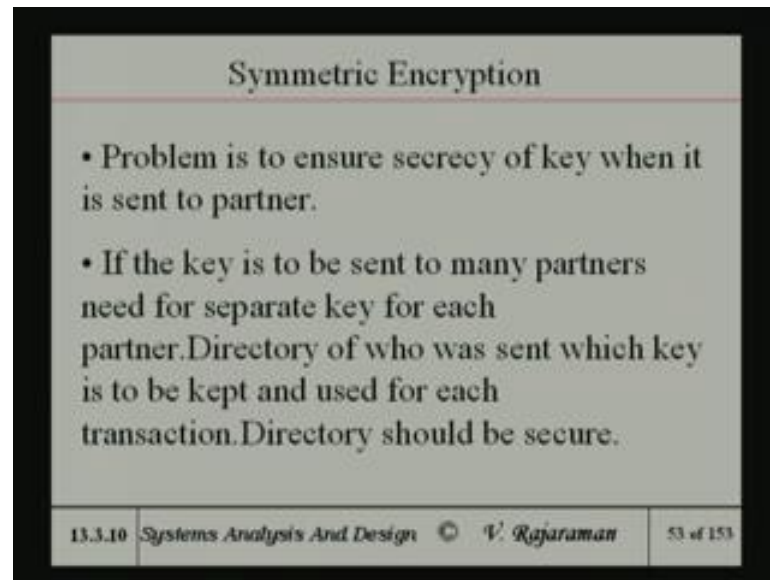
Main problem is the following see. That is, if you do a cipher or you know do a there are two you might say there are two groups of people. One group of people invent these types of methods of garbling messages. That is, they come up with this encryption methods. And they try to make the encryption method as difficult to break as one can, there is something called strength of encryption.

The greater the strength more difficult it is to break. And there is whole lot of other people, who try to get samples of transmitted data. And using those samples try to guess what was used. After all you know it is permutation and substitution. So, if you get a whole lot of samples of text, what you could do is, you can use the computer to try all permutations carry all substitutions.

And you may hit one particular one, where the cipher text decrypted may make sense to you. In other words it is actually English as per the understandable English language. So, then now I say that I would be able to decrypt. So, the ((Refer Time: 49:17)) are being able to break codes. That got a huge sample sets of encrypted data flowing and using those large sample, you try using a computer to try out in a group force fashion, all methods all of the keys and try to guess the right key.

Because, only way to decrypt is that for every message I send, I use a different key. But, that is not always practical. And I can randomize the keys, but when the problem is one of distributing the keys.

(Refer Slide Time: 50:13)



The slide is titled "Symmetric Encryption" and contains two bullet points. The first bullet point states: "• Problem is to ensure secrecy of key when it is sent to partner." The second bullet point states: "• If the key is to be sent to many partners need for separate key for each partner. Directory of who was sent which key is to be kept and used for each transaction. Directory should be secure." The footer of the slide includes the text "13.3.10 Systems Analysis And Design © V. Rajaraman" and "53 of 153".

| Symmetric Encryption | |
|--|-----------|
| • Problem is to ensure secrecy of key when it is sent to partner. | |
| • If the key is to be sent to many partners need for separate key for each partner. Directory of who was sent which key is to be kept and used for each transaction. Directory should be secure. | |
| 13.3.10 Systems Analysis And Design © V. Rajaraman | 53 of 153 |

The other person should be told and the key should be sent to him in some kind of a secured way, same internet cannot be used for sending the key. Secrecy of key is to be ensured and if the key is to be sent to many partners and use the same key for every partner. Then of course, it is no more secret. Because, everybody knows that is the key you are using.

So, for every business partner you have, you must use a different key. And that becomes a verandas thing. You must have a directory of all the different keys into whom you are using this key. And similarly, if you receiver must have a directory saying that, if I talk to a I must have this key, if I talk to b I had to have this key and so on. And go through the entire directory.

And the key distribution problem after distributing the key to all the people and periodically changing the keys, becomes a very difficult book keeping problem. So, if the problem is a symmetric encryption is this. So, key distribution is very difficult.

(Refer Slide Time: 51:22)

The slide is titled "Symmetric Encryption". It contains two bullet points: "• If large number of partners are there key distribution very difficult." and "• Advantage of symmetric key is easy and fast to transform plain text to cipher text." The footer contains the text "13.3.10 Systems Analysis And Design © V. Rajaraman" and "54 of 153".

| Symmetric Encryption | | |
|--|--|-----------|
| <ul style="list-style-type: none">• If large number of partners are there key distribution very difficult.• Advantage of symmetric key is easy and fast to transform plain text to cipher text. | | |
| 13.3.10 | Systems Analysis And Design © V. Rajaraman | 54 of 153 |

Advantage of course, is symmetric key is easy and fast to transform plain text to cipher text. Because, we use a permutation and also substitution, in the range to implement. And so this is a advantage of symmetric encryption.

(Refer Slide Time: 51:39)

The slide is titled "Digital Encryption Standard". It contains the following text: "DES - Proposed by IBM in 1975", "Standardised by US Govt in 1977", "Reasonably secure", "It is a combination of permutation and substitution on blocks of", "64 bits. A message is broken up into 64 bit blocks and each block is separately encrypted." The footer contains the text "13.3.11 Systems Analysis And Design © V. Rajaraman" and "55 of 153".

| Digital Encryption Standard | | |
|--|--|-----------|
| <p>DES - Proposed by IBM in 1975</p> <p>Standardised by US Govt in 1977</p> <p>Reasonably secure</p> <p>It is a combination of permutation and substitution on blocks of</p> <p>64 bits. A message is broken up into 64 bit blocks and each block is separately encrypted.</p> | | |
| 13.3.11 | Systems Analysis And Design © V. Rajaraman | 55 of 153 |

Now, symmetric encryption in spite of this little problem which I pointed out, had been very popular. Because, there are methods which are kind of they are to alleviate the key distribution problem. And try to eliminate the key distribution problem in some sense at

least in the sense of kind of being able to hide the key also in some way alright. So, this I will talk about later.

But, we look at the methods which are being used in practice. And in fact, encryption was people started using very early in the computer era. In 1975, IBM suggested a method, where encryption called digital encryption standard. And which was accepted by US government and standardized in 1977.

It was reasonably secured, what is meant by recently secured is that. If suppose somebody gets hold of some samples of the cipher text, to be able to guess the actual keys from that sample by brute force method using computer. It is actually practically impossible in those days in 77 when computers was slow, one would calculate that if we use brute force, it would take few years to decrypt, the find out the key and decrypt.

But now, as computer as become faster and faster, it turns out with the earlier method, which was used, which I am going to describe is no more secure. Because, machines are so fast that brute force will allow you to guess the keys in a reasonable time, when I mean reasonable time means 2, 3 days. This is a very high speed computer in 2, 3 days I can find out the key. That means, it is just not secure.

So, now DES has been you might say replaced or there are successors to DES then, replace by new methods. But, the new methods still try to use, the advantages which DES had. The greater advantage, which DES had was that it has a simple digital method, which could be implemented using a chip. In other words, you can actually design a VLSI chip or a VLSI chip to be able to do the encryption and decryption.

So, you need not we need not a program. Because, program take notoriously long time. Whereas, chips and hardware will take much shorter time. So, that was the advantage of DES and so the DES has been retained in some sense. But, DES has been modified and DES was being modified to make it easy to again use a VLSI device to be able to do the encryption and decryption.

In the original DES a message is broken up into 64 bit blocks. And each block is separately encrypted, just like a sort of example a five characters blocking and on each 5 characters we applied a permutation and substitution. DES divides up into blocks of 64

bits. And it applies permutation and substitution in again same type of an idea on these set up 64 bits.

(Refer Slide Time: 56:31)

| Digital Encryption Standard | | | |
|---|-----------------------------|----------------|-----------|
| •General idea used in DES | | | |
| M = PLAINTEXT | 01101100 | 11011000 | 11011010 |
| K = KEY | 10101111 | 00101100 | 01011011 |
| E = $M \oplus K$ encryption | 11000011 | 11110100 | 10000001 |
| M = $E \oplus K$ decryption | 01101100 | 11011000 | 11011010 |
| See simplicity of Transformation using Exclusive OR | | | |
| 13.3.12 | Systems Analysis And Design | © V. Rajaraman | 56 of 153 |

In fact, the simplest kind of a method which is used or the major idea used in DES is take the plain text and I am not using 64 bits. Because, it becomes too long on the screen. But, I use the 8 bits know a byte. And then, if I take cut up into bytes, then there is a key, which is again a string of bits and the 8 bits there are so many possible permutations of 8 bits.

So, two to the 8 possibilities are there it is fairly large number. And I do a the one simple encryption can do as ((Refer Time: 57:01)) all these too. And decryption is to take the encrypted text and exclusive OR. So, simplicity to estimate your transformation so simple, that the same transformation applied in reverse gets you back the original function, as you can see from here. But of course, that is not what is used I mean i is just to illustrate.

(Refer Slide Time: 57:21)

Digital Encryption Standard Algorithm

Before applying DES the text is split up into the 64 bit blocks.
DES applied on each 64 bit block.

Encryption method

Step 1: Apply an initial permutation on a block. Result is $B = IP(P)$ where P is the 64 bit block IP Initial Permutation function and B the result.

Step 2: Split B into 32 bit blocks
 L_i = leftmost 32 bits
 R_i = rightmost 32 bits.

Step 3: Pick a 56 bit key. Permute it

Step 4: Left circular shift it by 1 bit giving K_1 .

13.3.13 Systems Analysis And Design © V. Rajaraman 57 of 153

The consider the number of steps and as I said it is split into 64 bit blocks apply an initial permutation on a block. So, the result is a new block it is initial IP over initial permutation function on P , where P is 64 bits and B is a result, split B into 32 bit blocks into left 32 bits and rights 32 bit take a 56 bit key permute it. Left circular shift by one giving a key K_i .

(Refer Slide Time: 58:07)

Digital Encryption Standard Algorithm

Step 5: Perform a complex sequence of operations and obtain $X_1 = F(R_1, K_1)$ (The complex set of operations include table look up and dropping bits).

Step 6: Find $R_2 = L_1 \oplus X_1$

Step 7: Set $L_2 = R_1$

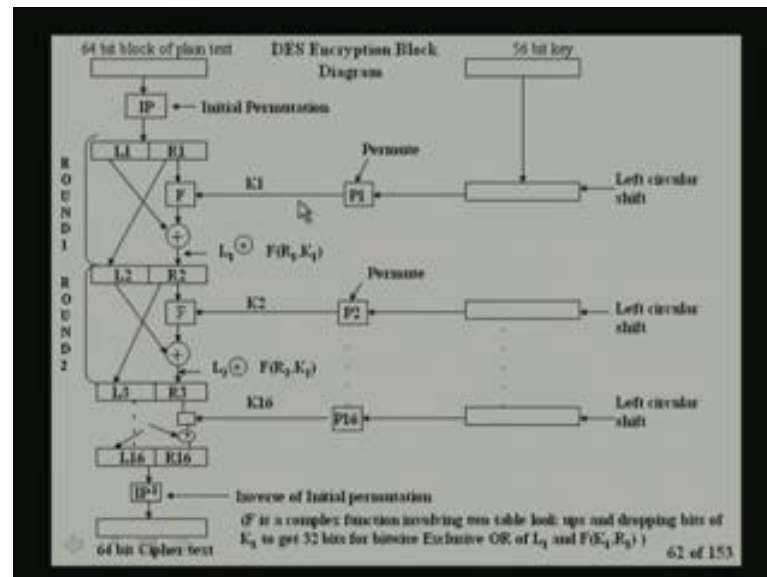
Repeat steps 2 to 7 16 times to get $B_{16} = L_{16}, R_{16}$

Step 8: Apply inverse of initial permutation on B_{16}
The result is the encrypted block

13.3.14 Systems Analysis And Design © V. Rajaraman

And perform a complex sequence of operation to obtain another, you know function of R 1 and K 1 and find the R 2 and L 2. I mean these steps are given, but more since we have to explain the whole thing. I had given a given this picture.

(Refer Slide Time: 58:30)



Picture is really is extremely easy to see what is going on. So, there is a 64 bit plain text and that is the initial permutation. And initial permutation it becomes again 64 bits. And there is a 56 bit key and the key is left circular shifted and then permuted. And after permutation you get a key here K 1 and some bits are dropped. Because, it is a 56 bit key and then, you drop some bits here and then after this you drop some bits here and bring it to actually we want to apply on this 32 bits, this must be a function which operates on 232 bits.

And say at this operation 232 bits and left is taken and function of K 1 R 1 is extremely what to get R 2. And this is again take R 1 is taken directly and becomes R L 2. And this continues like that and I come back to this next time, because I am running out of time. And explain to you, you can see here that the same operation is repeated again and again. It is actually a recurring 16 times in this case.

And the invert DES does the repetitions more, the key is longer and so on to kind of improve the security of the system. But, the general idea remains the same. And so next time what I will do is, I will take this start from this picture and explain this in slightly

greater detail of what essentially DES does. So, we will continue from this point next time.