edi and edi transactions
edi stands for electronic data interchange
and it's an essential format and standards required for two businesses
or multiple businesses transact business in e-commerce
so whenever say for instance a purchase order comes
if it is in standard edi format it can be interpreted automatically
and then the actual data namely the purchase order (refer slide time 01:51)

they have the actual acceptance of the order the dispatch or delivery note and so on
all them 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
um 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 um in within that plan
so each one is separately encrypted in possibility of
one being able to read the others um data and so on is um not there
a recent introduction which is a which runs on the internet
but does provide more security than internet is called the virtual private network
virtual private network is something which um is not a private network
like a dedicated line but um 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 okay
so i will not get into the detail of the um virtual private networks
because you actually learned about them in your network course
but its sufficient for me to say that the um the acronym which is used is um SSL VPN
that is secured socket layer in the um 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
um which is vendor of um routers and so on
also provide they also provide some of the IISP’s like
for instance in India um sify provides an SSL VPN service for clients
which does provide higher security levels because SSL VPN effectively
um you might say reserves or tunnels through internet in a certain path
which is kept secure and which is not easily
um 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 um the trend is towards VPN because it is a cheaper than um dedicated line
its also cheaper than the value added networks
in fact value added networks they are not too many of them
now existing in our in our country i mean it is to be provided by um
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)

the value added networks normally provide close boxes for all the subscribers
now what the value added network is a private network
and um but then as a same shared private network and guarantee is delivery
it is open twenty four by seven 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
some um 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 um 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 ofcourse this is the disadvantage compared to using a say a SSL VPN or the internet is its cost is high and um so its used only by large businesses and not by smaller businesses

(refer slide time 07:59)
so to use the internet with with edi as i pointed out xml is becoming a better standard because xml along with the document type definition publicized by the um the various um participants in ecommerce 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 ofcourse its 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 um as a as a method of communication on the internet okay or um VPNs and along with xml one uses what is known as multipurpose internet mail extension to attach edi forms to email messages this is part of the internet infrastructure and as call a simple i can use simple mail transfer protocol on internet to transmit this documents if secure transmission is needed (refer slide time 09:30)
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 email i may bind some all together and send um send
using an ftp or a file transfer protocol again that of internet
(refer slide time 10:03)

and again 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 um reiterate the fact that the its necessary
to have an edi standard document format to facilitate the interpretation of documents
and to facilitate the working of many different companies together okay
now as i pointed out if we use internet at even few days before publics
nowadays few hours of public switch telephone network
it becomes extremely important to ensure security okay
um if you say pure private network even then that private network um
one or expect no body can intrude
but some even there certain amount of security concerns are necessary okay
and one should be aware of it even though the level of um awareness may not be
as much as level of awareness about the internet
but ofcourse as i pointed out again
the private interconnection is becoming more and more rare because of its expense
and most companies are really going towards the um using the internet
as the public infrastructure because lot of work has gone in security
to be enable 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)
so as i because internet is insecure and eavesdropping is possible by excuse me 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 so we also need to protect a companies network with unauthorized entry okay though if you if the companies internet intranet is connected to internet (refer slide time 12:45)

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 internet
the companies 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 its 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 companies 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 the some machines are connected to the internet that’s 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 little bit about um these 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 a a also something called a digital signature
which can be used in a court of law
let us let me explain little bit what what i mean by this
when you get a purchase order from somebody
say from from a company normally in a manual system
the purchase order is a print is kind of typed or printed
and at the bottom there is a signature of the um 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 um kind of say for i didn’t do that
because there is a signature there okay
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 person who actually create the document
so in the electronic world when some document comes
some body 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 is an there should be an equivalent of the physical signature
in the electronic form and its 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 companies local intranet from hackers and so on
you provide at the boundary of your intranet some device
which um 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 19:35)

![Network Security Using Firewall](image)

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 um 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 20:10)
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 um 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 um email
they may not allow ftp telnet and so on
telnet allows an external um 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 the to filter out some of the disallowed um facilities
like it may disallow large files from going
so ftp may be disallowed
or it may disallow telnet
it may allow disallow emails to send kinds of addresses and so on
it also sometimes be filters the filters something going out of the organization and something coming out of the organization for since many colleges put a firewall um primarily program the router you might say to disallow the students one look 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 um it has no student to have a business to access them because primarily they can access um information from the internet um 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 ofcourse some companies also ban electronic due to still commerce from inside the company so some built in sites may be also banned so there is a filtering so the um um 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 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 okay so these are decisions which are taken at the highest level of the company and implemented okay and um also you can program it that at certain times of the day certain types of traffic are disallowed okay and certain times of the day the source traffics are allowed because it depends upon the busy time and the non busy time there is something called proxy application gateways (refer slide time 24:18)
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 don’t want to completely ban internet
but you still want to restrict the freedom of the use of use
so there is something called a proxy machine
proxy is something which works on your behalf
so proxy application programs where in the firewall machine
so whether as I said an um instead of a router it is actually a computer
and this machine one which acts on behalf of all members of organization
wanting to use internet
in other words it is a some kind of a gate keeper
which um acts as proxy or some thing 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 its addressed or not
so these issues are actually you might say it’s a security to a watchman standing at a gate
who decides and like know the who acts on your behalf
like for instance you may have um some people
have the security within the 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
this proxy um the proxies main job it monitors all request
(refer slide time 26:27)

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 its effectively a gate keeper
which make sure that um people from inside the company
they do not have access free access to any where
they also some times proxy application programs
are run in the users machine
we have to authorize them to use the internet
because the if it’s a gate way for 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 um for the users machine itself
anyone from inside or outside an organization given the user id password service required they are given to firewall (refer slide time 27:26)

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 its actually you might think out (refer slide time 27:43)

proxy is a server to requestors desktop pc but it’s a client to those requesting service
in our absence this guy you know
in other words if a particular service is requested by um
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
okay kind of a intermediary you might say
firewall needs proxy agents for each service requested (refer slide time 28:16)

in other words you have number of different um
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
um proxy firewall initiator of all sessions and thus knows every activity
so its actually a big brother watching what is going on
and ensures security um like firewall is a proxy function replaces the source address
of transactions requested its then the IP address (refer slide time 28:54)
its little more 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 next time i void 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 firewall's IP address and all other IP address with in the organization are hidden so the primarily there is a the firewall is something (refer slide time 29:50)
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 we um which um which essentially um disallows intrusion
and um this is a 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 um spreading the virus
and so some virus scanning is also done out going out going information
there is one more important thing which is a rare piece of software
its called a spam filter
lot of unnecessary mail comes to the organization trying to sell things and so on
which waste time of people 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 the another function this strictly speaking
virus protection and spam filtering are not part of the firewall firewall function
firewall primarily is a security enhancing device but
over and about that there is a large server kind of large firewall
and have software running on it um which also does this okay over and above that
or ofcourse depending upon the company may put
one more one more machine have to be the firewall
to do the filtering business okay
but it its up to the companies information
um 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
its also lot of software method which are required
and that is called encryption
and um i will talk about encryption with rather more the secret keys
as data centre at private network may be hack 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 its 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 um say from the king
to may be somebody at the battle front
will not be written in plain plain text
if you write in plain text if an enemy gets 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 ofcourse taken a greater importance
for electronic tra tra 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 eight bits per character so ultimately they are bit string
so if the text is garbled even if one access it it cannot understand what it contains
(refer slide time 36:12)

so similarly we want to protect data stored in databases
which are accessible by internet if its 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 okay
as i said if the rajas send some message to the
to the person at the to a general at the front
the he decrypts encrypted messages came from the raja to
um to actually understand what the instructions are
there are certain types of terminologies
which is used when we talk about encryption and decryption
by plain text we mean data in its natural form
(refer slide time 37:19)

like ASCII ASCII 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
where as 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 doesn’t depend upon type of data
its 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 programmes are encrypted so unless you take or listen to that channel and get a decryption key you cannot actually view that particular television programme here in satellite radio like the world space and so on the radio broadcast is through satellite in a digital form and um 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 um particular radio set you have got the radio circle have 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 the from the satellite will will be decrypted by the radio set to for you to able to hear the 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 is doesn’t 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 plain 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 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 um block the plain text that is you take say five characters at a time so this is a message you are essentially essentially squeeze out all the blanks first ofcourse because blanks carry no information so squeeze out all the blanks and adopt the um 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 four one two five three 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 um becomes the fourth character
and the third character namely becomes the fifth character because this permutation key is long five five five digits long and this says position one is now the plain text position two is one position three is two position four is five position five is three this is called a permutation so i permute 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 um leave out a b c z will be replaced by d so so if i take s s will be replaced by s t u v w okay 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 cant you cant make head and tail out of this okay it looks very very different from this so this is the plain text and this is the encrypted text or cipher text okay there is an example of two permutations 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 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 w um replace w by s okay because t u v w so i go backwards w um v u t s okay that’s 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 okay
so that is a well idea so its the encryption permutation and substitution
and decryption if i know the keys is to do the reverse okay
so to make it um more you might say abstract
(refer slide time 45:36)

![Symmetric Encryption](image)

a plain text consists of m one m two m three upto m n
where each one is a block and cipher text is c one c two c three upto cn
well ci is the um permutation which ti is the permutation of i’th character
and k is the substitution okay
ci is the substitution and these two operators
that is the keys which are applied to this okay
(refer slide time 46:01)
now to decrypt applying the same transformation this way as i tried it out
this method is called a symmetric key encryption
its 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 um encryption is is made public to we to 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 key 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 um one two characters away anything anything alright
it is 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 um the actual plain text from the coded text
main problem is the following see
that is if you do a cipher or you do a there are two
you might say you might say there are two groups of people
one group of people invent these types of methods of um of garbling messages
that is they come up with this um 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 what was used
after all you know its 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 um one particular one where the decrypted
cipher text decrypted may make sense to you
in other words its actually English okay
as per the understandable English language okay
so then now i say that you would be able to decrypt
so the ((49:18)) are being able to break codes
that got a huge sample sets of n um n 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 okay
and i can randomize the keys but
when the problem is one of distributing the keys
the other person should be told and the key should be sent to him
in some kind of um secured way same internet cannot be used
for sending the key okay
(refer slide time 50:15)
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 ofcourse its no more secret
because everybody knows that’s the key you are using
so for every business partner you have you must use a different key
and that is a 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
advantage ofcourse is symmetric key is easy
(refer slide time 51:23)
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 an advantage of symmetric encryption
now symmetric encryption in spite of this little problem
(refer slide time 51:42)

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 okay
atleast in the sense of um kind of being able to um 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 where people started using
very early in the computer era
in nineteen seventy five ibm suggested a protocol
it was suggested a method where encryption called
digital encryption standard and which was accepted by US government
and standardized in nineteen seventy seven
it was recently secured by the way what is meant by recently secured is that um
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 seventy seven when computers was slow
one would calculate that if we use brute force it would take few years to decrypt
the um 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 brute force will allow you to um guess the keys
in a reasonable time when I mean reasonable time means two three days
this is a very high speed computer in two three days I can find out the key
that means its just not secure so now DES has been you might say replaced
or um there are successors to DES will 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
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
where as 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 sixty four bit blocks and each block is separately encrypted just like a sort of example a five characters blocking and on each five characters we applied a permutation and substitution

DES divides up into blocks of sixteen sixty four character sixty four bits and it applies permutation and substitution in again same type of an idea um on these set up um sixty four bits 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 sixty four bits (refer slide time 56:31)

because it becomes too long on the on the screen but i use the um eight bits um know a byte and then if i take by cut up into bytes then there is a key which is again a string of bits and the eight bits there are so many possible permutations of eight bits okay so two to the eight possibilities are there its fairly large number and i do a the encryption consist one simple encryption
can do and simple we can so all these too
and decryption is to the encrypted text and is to say
simplicity to estimate your transformation say 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 in it
it is just to illustrate okay um the um
(refer slide time 57:23)

if consider the number of steps okay and as i said its split into sixty four bit blocks
apply an initial permutation on a block
so the result is a new block its initial i ip over initial permutation function on p
where p is sixty four bits and b is result
split b into two thirty two bit blocks
into left thirty two bits and rights thirty two bit
take a fifty six bit key permute it
left circular shift by one giving a key ki
and perform a complex sequence of operation
(refer slide time 58:13)
and obtain another um you know function of um r one and k one
and find the um r two and l two
i mean these steps are given but more since we have to explain the whole thing
i had given a given this picture okay
um picture is really is extremely easy to see what is going on okay
(refer slide time 58:35)

so there is a sixty four bit plain text plain text and that is the initial permutation
and initial permutation it becomes again sixty four bits
and there is a fifty six fifty six key um 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 okay
because its a fifty six bit key and then you drop some bits here and then
after this you drop drop some bits here
and bring it to um actually we want to apply on this thirty two bits
this must be a function which operates on two thirty two bits okay
(refer slide time 59:21)

and say at this operation two thirty two bits and um left is taken
and function of $k_1$ one $r_1$ one is extremely what to get $r_2$ two okay
and this is again take $r_1$ one is taken directly and becomes $r_1$ two
and this continues like that okay
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
its actually a recurring sixteen 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 okay
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 okay
so um we will continue from this point um next time