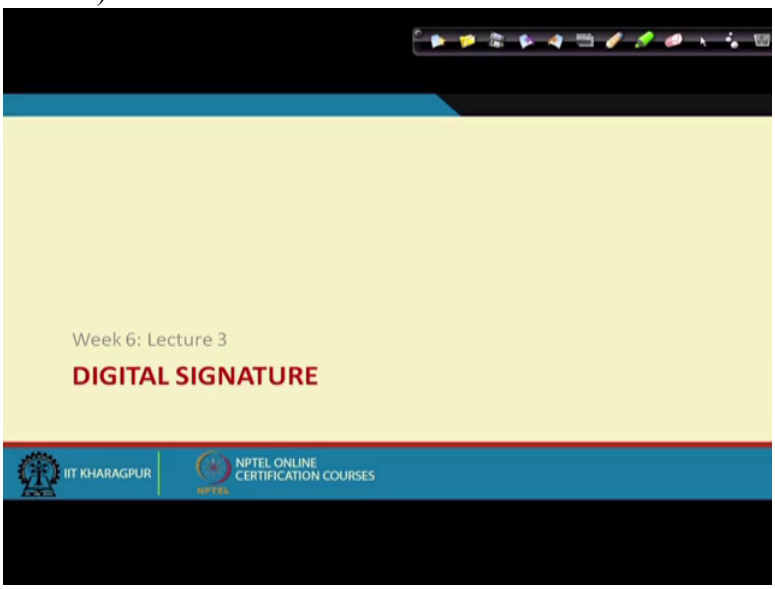
Course on E-Business
Professor Mamata Jenamani
Department of Industrial and Systems Engineering
Indian Institute of Technology, Kharagpur
Module 06
Lecture Number 30
Data Signature

(Refer Slide Time 00:17)

Welcome back. So long we have been talking about various basic principles behind security and various terminologies. Now we are

(Refer Slide Time 00:27)

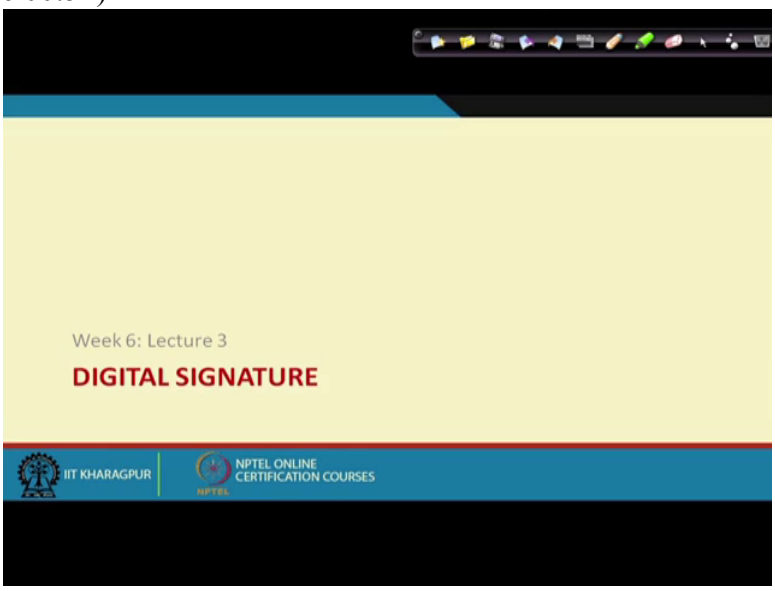


going to see that how they are applied in real

(Refer Slide Time 00:31)

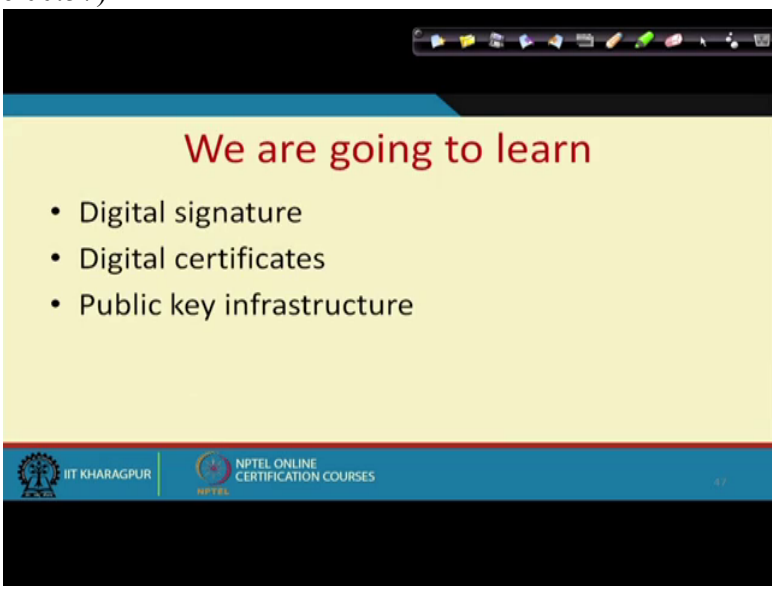
world business transactions. One of the very trendy term which is frequently used in the business world is business is the digital signature, whether a document is digitally signed or not. So today we are going to see what this digital signature is

(Refer Slide Time 00:52)



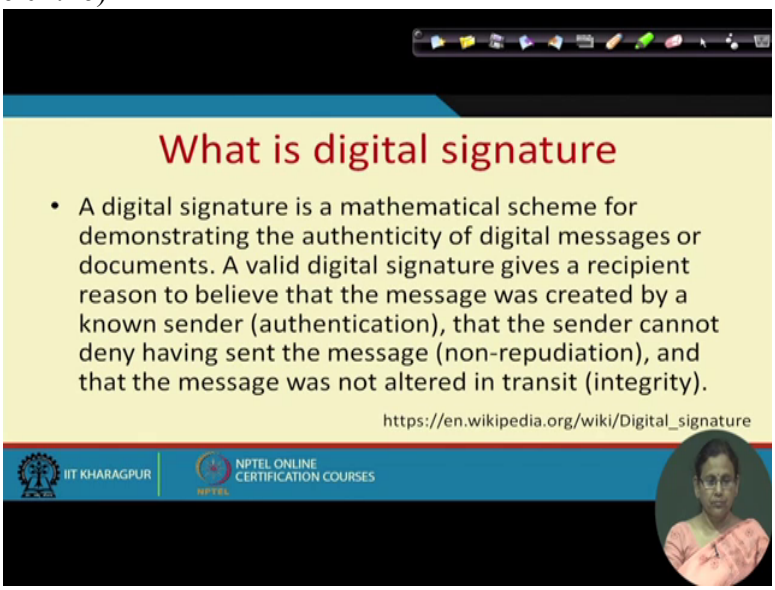
and how it is, and what are its various applications.

(Refer Slide Time 00:57)



In fact to know about the applications, we have to go to few more lectures as well. So let us today understand what a digital signature is, what is digital certificate and what is this public key infrastructure which helps in generating this digital certificate.

(Refer Slide Time 01:16)

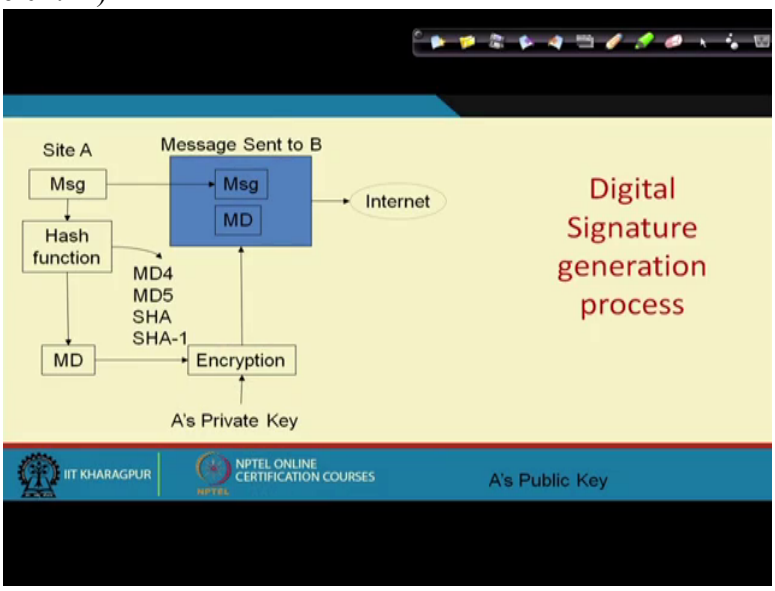


To start with, a digital signature is a mathematical scheme; this whole security stuff is full of mathematical operations starting from your encryption etc, so your digital signature is also a mathematical scheme for demonstrating the authenticity of digital messages or documents. A valid digital signature gives a recipient, gives a recipient reason to believe that the message was created by a known sender which means it authenticates it and that the sender cannot deny having sent the message. So non-repudiation is carried out. And that the message was not altered in the transit. That is integrity. So three

(Refer Slide Time 02:03)

security categories are taken care of by digital signature; their authentication, non-repudiation and integrity. These three digital, three security categories are taken of by digital signature. Look at this.

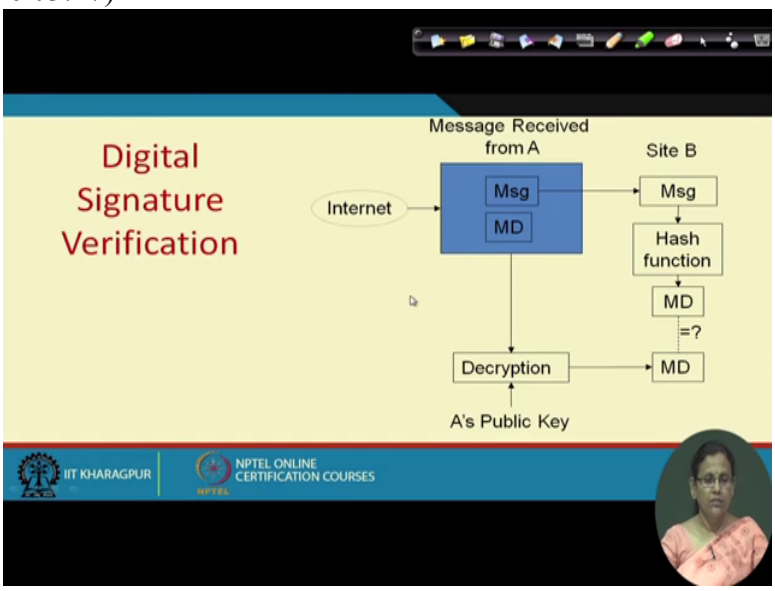
(Refer Slide Time 02:21)



This is the digital signature generation process. In fact about hashing etc, we have already discussed. So besides hashing, it also uses a public key operation. So what happens, the message which is the application data which is supposed to be sent first goes through the hash function and a message digest is generated. Then this message as well as the digest, ok this message digest is then encrypted with A's private key. A is the entity who is actually sending the data. So it is encrypted with A's private key. This encrypted message digest and the

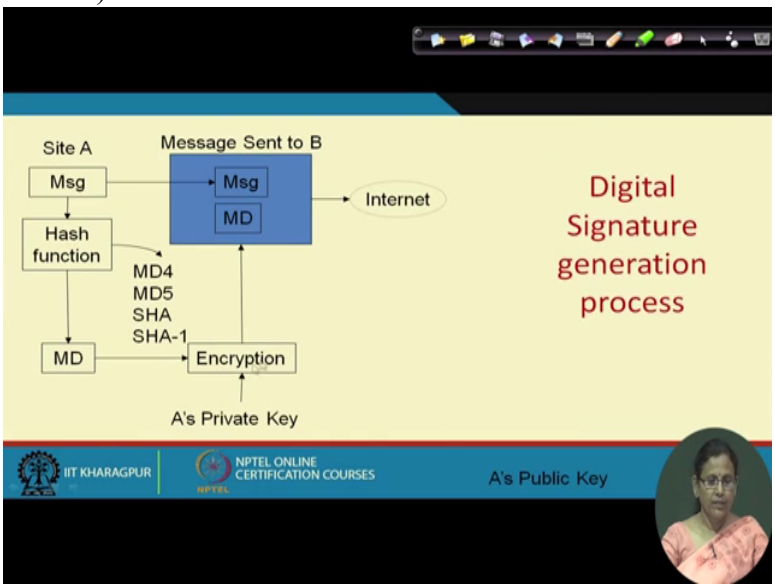
message that is the application data is sent to B over the internet. So this is the process of digital signature generation.

(Refer Slide Time 03:27)



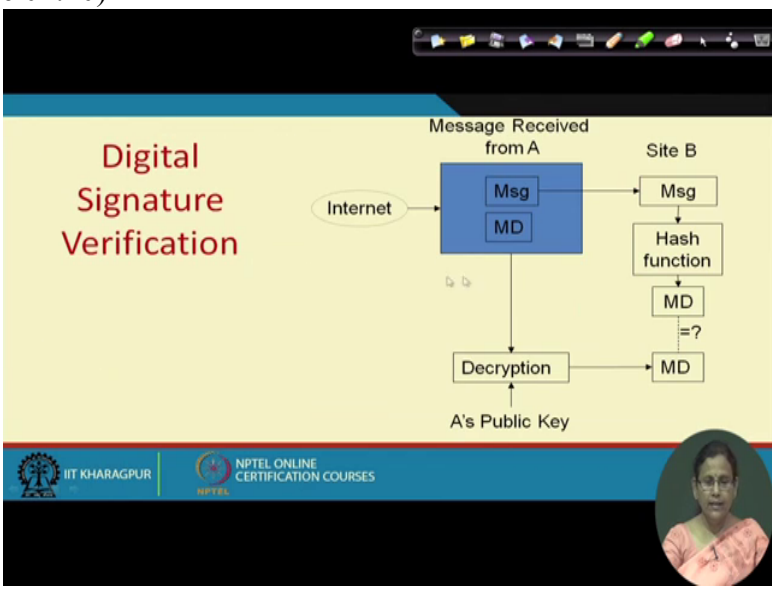
Then at the end of B who is the receiver, two things are received. Once is, first one is the message. Second one is the message digest. So as we have discussed in during your hashing, this message passes through some hash function to produce the message digest at the receiver's end. So if, and the message digest which was encrypted message digest, please see

(Refer Slide Time 04:01)



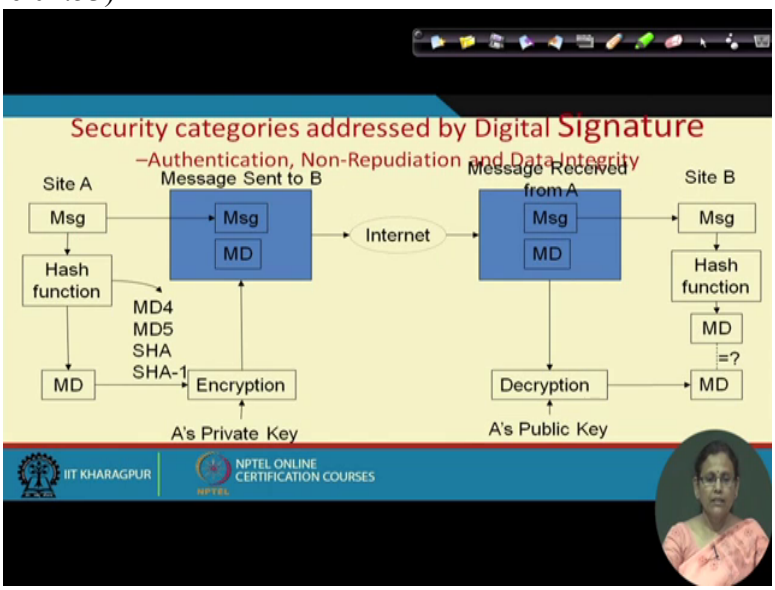
here one encryption operation was done on the hashed value; this was the hashed value and after encryption operation this message digest was generated. So on this one, when it is

(Refer Slide Time 04:20)



sent to the other end, this encrypted message digest is first decrypted using A's public key. Who is A? A is the sender. Now how his public key is known? Because it is public and everybody knows about this key. Using A's public key it gets decrypted and message digest gets generated. Now if both these message digests are same, then we say digital signature is verified.

(Refer Slide Time 04:53)

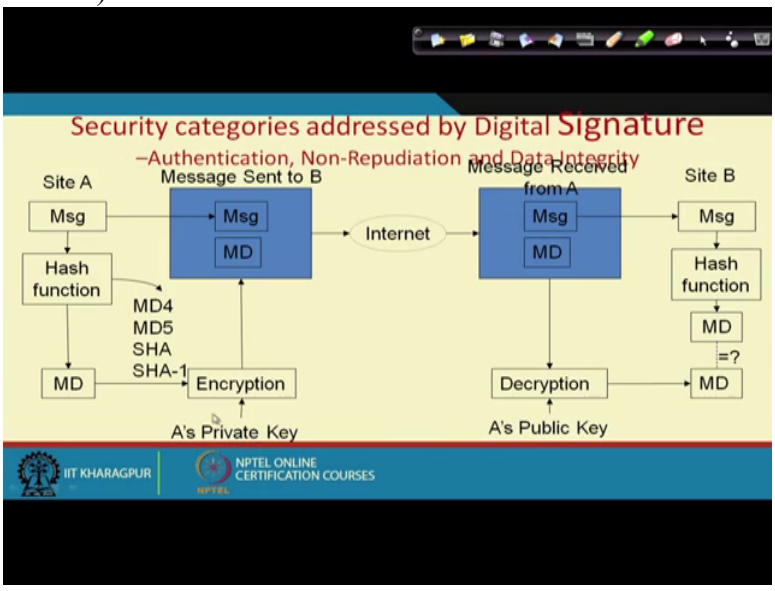


Now as I have told you this digital signature addresses three security categories, authentication, non-repudiation and data integrity. What is authentication? Authentication to make sure that it is actually sent by somebody who claims to be himself. Ok, so if it is sent by me, if somebody is claiming that it is, somebody is claiming that it is sent by me, suppose I am the person A and other person is B, if the B is, if, it is not, only I can claim that I have

(Refer Slide Time 05:36)

sent the message. B cannot. So look, it is,

(Refer Slide Time 05:43)



this message digest is actually getting encrypted by A's [public/private] private key which means it can only be decrypted properly by A's public key. So if it is getting decrypted and this matching happens, which means the key using which it is encrypted belongs to A and because A's private key is only known to him and to nobody in the world which means this particular message digest is sent by A. So B can be sure that it is actually sent by A, not by somebody else.

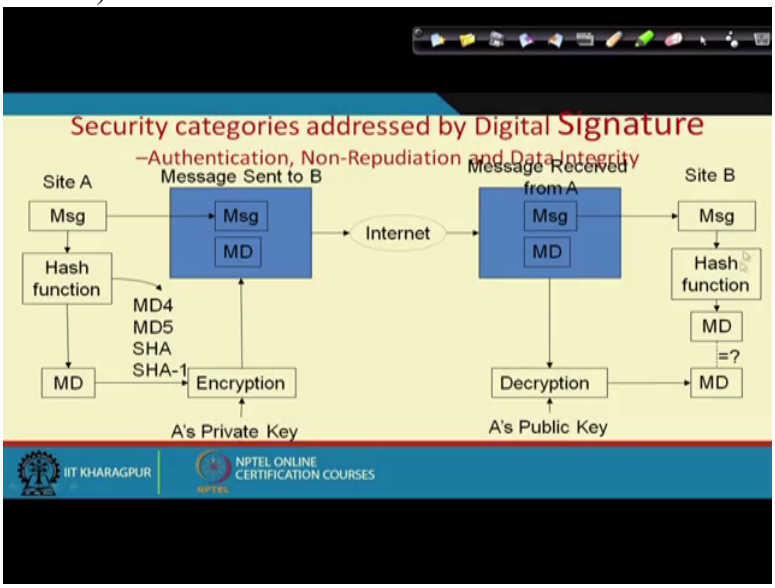
Then comes this non-repudiation. It is about A telling that it has not sent it. Somebody else has sent it. A cannot say it right now because it is getting decrypted properly by his own

public key. So which means it is sent by him only. So non-repudiation is taken care. Next is your data integrity. Now data integrity is about making sure that the data is not

(Refer Slide Time 06:56)

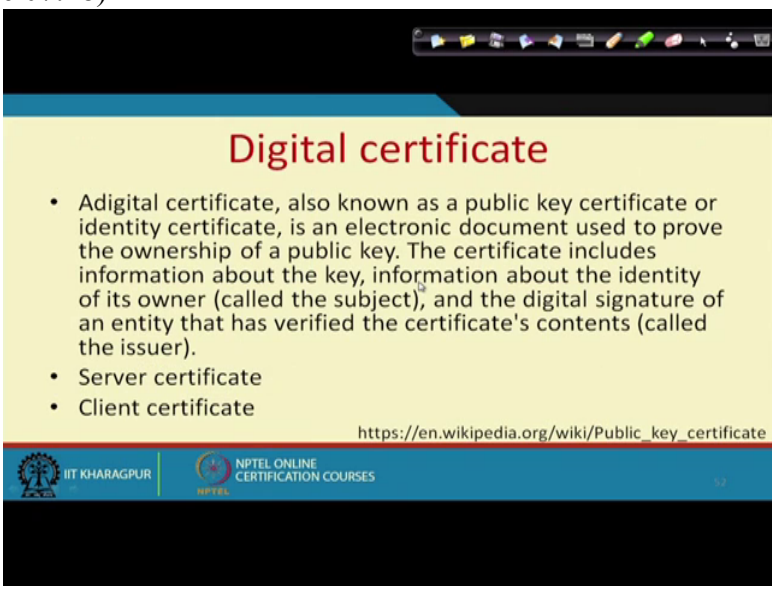
modified on its way. So the data part here is the message part. If the message is modified,

(Refer Slide Time 07:05)



naturally this M D will not match with this. So data integrity is also taken care of. That is how this authenticity, repudiation, non-repudiation and data integrity is taken care of by digital signature.

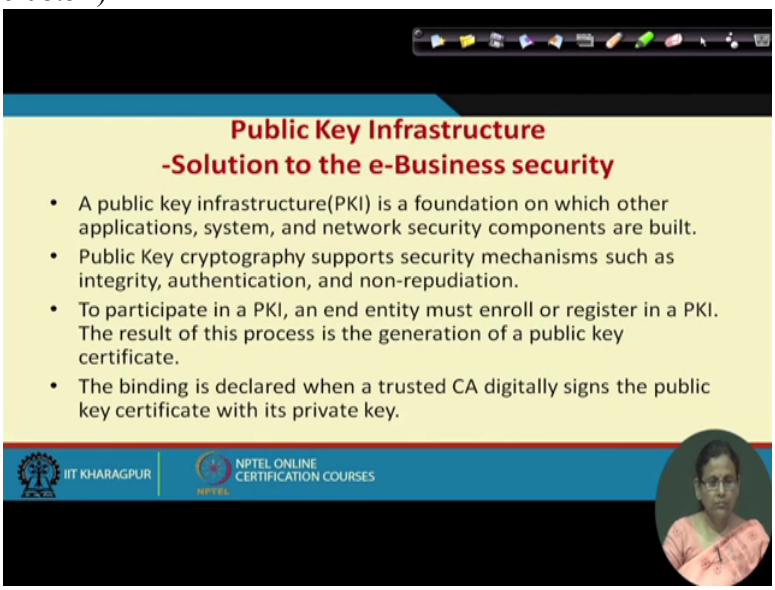
(Refer Slide Time 07:18)



Now one of the very important application of digital signature is getting a digital certificate. So what is a digital certificate? A digital certificate also known as a public key certificate or identity certificate is an electronic document used to prove the ownership of a public key. So long we have been telling that in asymmetric key cryptographic algorithm, two keys are there. One is a public key, one is a private key. And public key is known to everybody. Now why should somebody believe that the public key which I am giving him is actually my public key? It is not somebody else's public key? So to prove my ownership that I own that public key, digital certificates are used.

So the certificate includes the information about the key, information about the identity of the owner, called the subject and the digital signature of another entity who verifies the identity of the subject and accordingly writes the content in the digital certificate. So this fellow is called the certificate issuer. Mostly the servers have this server side certificates and sometimes the clients also own client certificate.

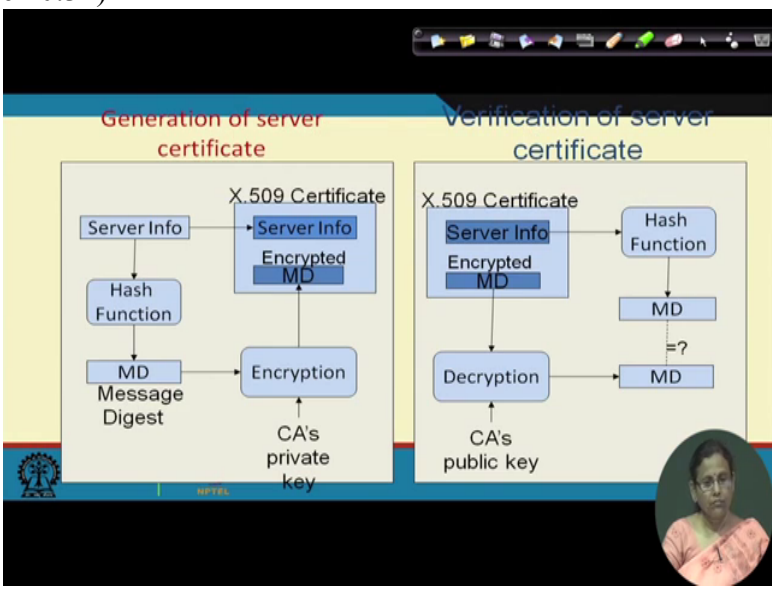
(Refer Slide Time 08:54)



Now in order to provide this private and public key operations which is key to E-Business security, every country has its own public key infrastructure. It is known as P K I infrastructure which is the foundation on which other application systems and network security components are built. This public key cryptography supports security mechanism such as integrity, authentication and non-repudiation.

Then in order to participate in this public key infrastructure, the entity must enroll or register in this, with the appropriate agency. The result of this process is the generation of public key, public key certificate and this binding is declared when a trusted certifying authority digitally signs the public key certificate with its private key. So the certifying authority which is somebody which is universally accepted as a trusted party, so he signs on this digital certificate which represents, shows the data about the certificate owner including his public key. So that is how the public key is believed to be the public key of the person who claims it to be his key.

(Refer Slide Time 10:32)



So the whole idea that we have talked about during digital signature process is now carried out here. So now look at this. Because we have already discussed about it I have put it in one place. This is about generation of server certificate and verification of server certificate. Usually server certificates will be, are called X point 5 0 9 certificate. So as I was telling you the server information is certified by some certifying authority and that is how it is known as a digital certificate. This certifying authority or somebody who is appointed by the certifying authority physically verifies about the server's existence which means the company which owns the server and the information given to C A about the server's, about the server. So this server's information is sent during the secured web transaction to authenticate a server that the client believes that it is talking to the right server.

The server has to produce his digital certificate. So this digital certificate while producing this digital certificate, it has to be transmitted over the internet, this digital certificate contains the information about the server and it has to be transmitted over the internet. So while getting transmitted the facts which are written within this need not be modified. But it is not a secret thing that cryptography is required but it should not be modified on its way. So as we have learnt in our digital signature, the server information is first, first goes through the hash function, message digest is generated.

Now this is encrypted with C A's private key. Who is C A? The certifying authority, the certification authority, with his private key it gets encrypted. Then it is, this encrypted message digest and server information which together is called X point 5 0 9 certificate sent over the internet to the receiver. So when you are connecting with H T T P, for security we are going to learn about what this H T T P S is all about but you must be realizing when you

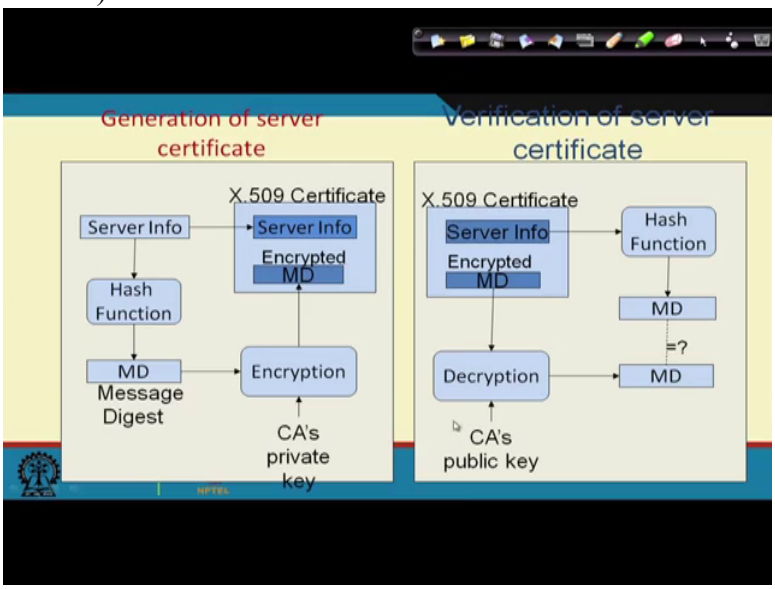
connect to your, through, to your server to another server, through H T T P S protocol, the server has to authenticate itself by producing server certificate so that you believe the server.

So when this server gets this certificate his existence and the information he provides with is verified by the certifying authority. And this information when it is given to the certifying authority, certifying authority now puts his, encrypts this message digest with his encryption, with his own private key to generate this message digest. So which means this message digest if it is decrypted with C A's public key which is anyway known, C As are trusted parties so it is known otherwise, so if it is decrypted which means, this information, this server information is actually certified by this certifying authority, is truly certified by the certifying authority, because nobody else, else's public key can be used for decryption purpose to create the right message digest. So when the, this X point 5 0 9 certificate of the server reaches the other end, the server information once again goes through the hash function. Message digest is generated and this encrypted message digest which is actually encrypted by C A's public, private key is gets decrypted. After it is decrypted this message digest which is generated is compared with the digest which is created at the receiver's end. If they match, then it is verified that, this is actually, this information is actually verified by corresponding certification authority and after this verification process only, the client can believe that the server is actually truly the server with whom it is contacting.

(Refer Slide Time 15:47)

So therefore all the three elements that is authentication, non-repudiation and data integrity, data integrity means your authentication, non-repudiation is done here, authentication because it is getting opened by C A's public key,

(Refer Slide Time 16:06)



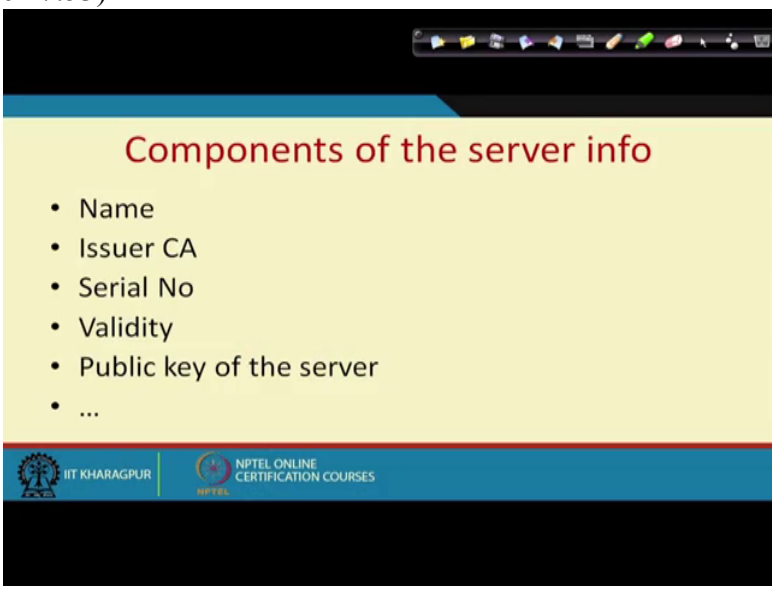
then we know that some authentic person has verified this server information. Then comes the non-repudiation. Once it is opened by the public key, if by chance server does some this, server turns out to be non, is to be entity who is not to be trustworthy then because C A has already approved it and you know that C A is a, is the agency whom you can put your complaint with about the server. C A can never deny that it has actually given this certificate to this particular server. So that is how non-repudiation on the part of certifying authority is achieved. Then your next thing is your authentication, non-repudiation and data integrity, Ok. The data integrity, because

(Refer Slide Time 17:18)

in the, while the data packet is being sent, it is quite possible that the server's information is modified. If it is not then these two will be same and if it is, then the problem will be detected. So which means, if it is tampered with on its way, it can be detected. So that is how your, the last security category is also achieved.

Then what is the component of this

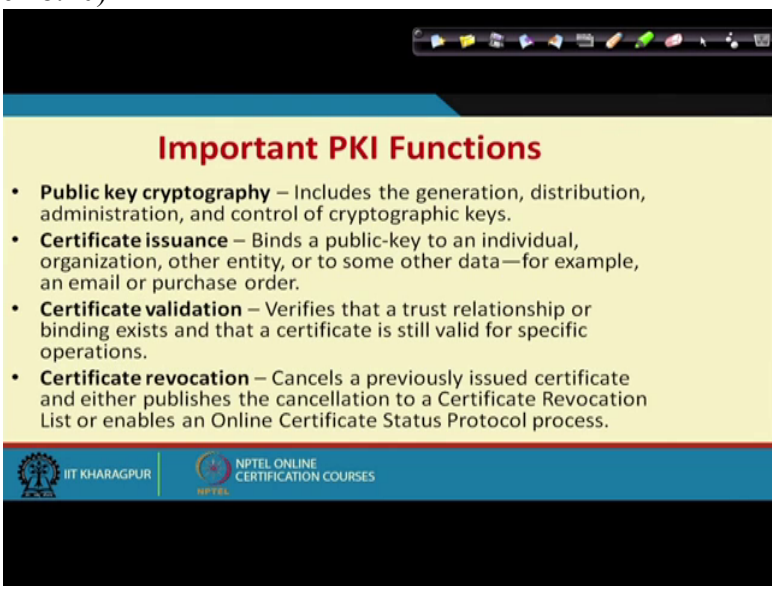
(Refer Slide Time 17:53)



server information? Because the server is getting authenticated, it is the name of the company who is the issuer, certifying authority, what is the serial number, validity, public key of the server because so far we have been telling that public key is known to everybody. So how this

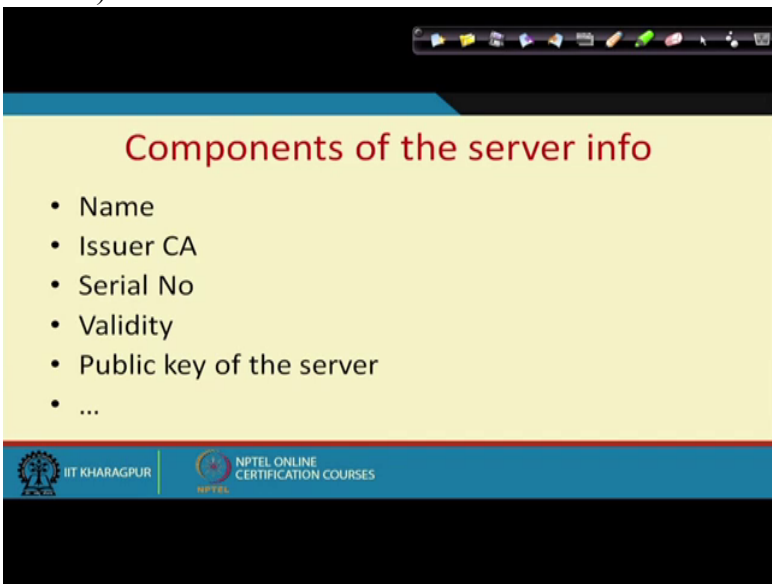
public key distribution takes place? This public key distribution takes place through this server certificate only.

(Refer Slide Time 18:20)



So besides of course,

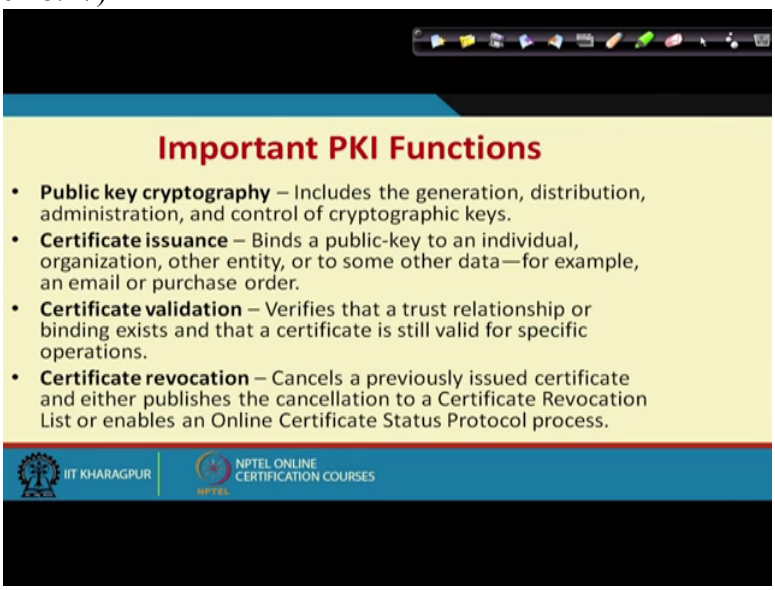
(Refer Slide Time 18:22)



besides this there are many more things you can find out but these are some of the important things.

Now what are

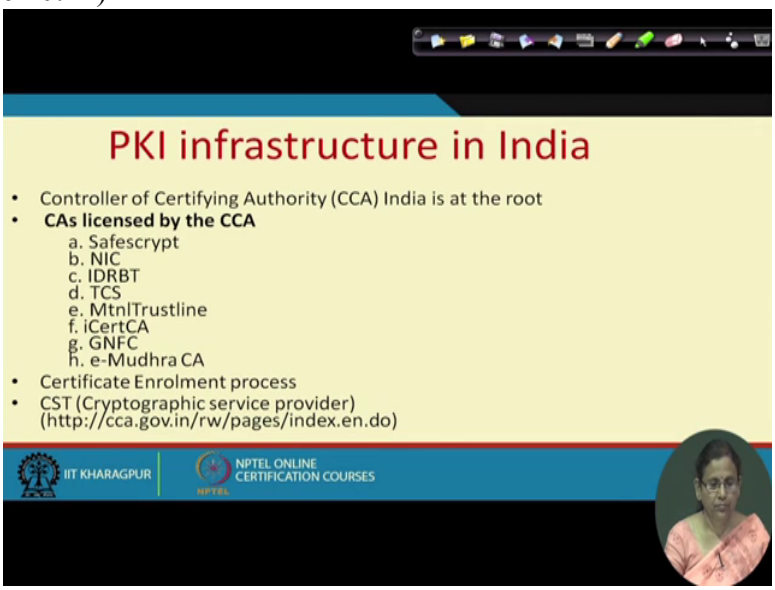
(Refer Slide Time 18:27)



important functions of this public key infrastructure and specifically the Certifying Authority? First of all this public key cryptography, it includes generation, distribution, administration and control of cryptographic keys that is public key, private key pair, then certificate issuance, binding a public key to an individual, organization or some entity or to some data, then certification validation, this is verifying that a trusted relationship or binding exists that the certificate is still valid for specific operation. Then certificate, these are few functions only, there are other functions as well. Certificate revocation, so this is very important.

This certificate which one organization gets from a Certifying Authority are not permanent. They are issued for a specific period. After that period, again that entity whether it is organization or whatever, or individual, he has to once again apply for that and his information once again need to be verified. And as I was telling you, even if a certificate is issued to somebody let's say, for a period of 2 years, within that, within the 2 years, if there is any complaint comes about that the activity, undesirable activity on the part of that server which belongs to certain organization, then the C A has the power to revoke the certificate. So certification revocation is another important P K I function. Besides that there are many other public key cryptographic functions as well.

(Refer Slide Time 20:14)



Then let us look at public key infrastructure in India. Ok, before we talk about public key infrastructure in India, usually this public key infrastructure is arranged in form of a tree. There is a chain. There is a Root Certifying Authority, then he will be licensing many C As, and those C As may again have some other people to work for them. So there is a whole chain of, which means when a, so this certifying authority actually issues a digital certificate to each of its licensee. Then the licensees can issue digital certificates to individuals. So whenever digital certificate of that individual company or individual person gets verified the whole chain of certificates, the server's own certificate, the issuer's certificate, issuer's controlling authority's certificate everything needs to be verified in a chain.

So this, for India, this Controller of Certifying Authority C C A India is at the root of this certification process. Then it has many licensees. These are some of the licensees and if you are interested, if somebody is interested, can go through know more about how to get a digital certificate and all, and about the certificate enrolment process by visiting the C C A's website. With this we finish this lecture, thank you very much.

(Refer Slide Time 22:13)