

System Analysis And Design
Prof. V Rajaraman
Department of Super Computer Education & Research
Indian Institute of Science, Bangalore

Lecture - 36

The encryption methods, we looked at two types of encryption; one is the digital encryption standard with the symmetric key encryption. And an RSA standard, which is really a public key encryption. Actually, I said that the RSA stands for the names of three people are Rivets Shamir and Adelman. They are three persons belonging to the department of computer science and mathematics who together invented the RSA algorithm for this public private key a combination.

And it is extremely useful method. We also saw how the two can be combined. To get the speed of symmetric key encryption and the key distribution problem, which is in the RSA system? So, the two are combined together then you have a effective method which is both fast at the same time it avoids key distribution. It also allows you to change the key for every transmission and that affords you more security.

Because, even if a cryptanalyst who is suppose to try to break the code gets hold of samples of messages. It will be difficult for the analyst to be able to do any kind of a decoding, because the key is continuously being changed. And they are actually randomly picked and you do not really what key he is going to pick. So, generally then the encryption methods have been fairly well standardized and have been used.

And even though, I talked about all algorithms and things like that which is of course, necessary for a computer science and computer application students to know. Because, they had to know what goes inside these coding systems. From the point of the user, he does not really have to understand. Normally these methods are provided on your desktop machine.

And by a click of a button you can ask for encryption using RSA. That is the public key encryption system. So, most of the security methods from the users point of view are primarily using a securised link, which actually when you say secure link effectively. It means that the data has been encrypted. And encryption keys are actually picked based on of course. If it is a private key public key system. It is based on the private key public key algorithm.

So this is essentially, what in other words the point of view from a say a management student or a lay user. He does not really have to know all the intricacies of the algorithm which goes into doing it. But of course, it will be nice to know do what it involves and that is only for education. But, as of today, many of these have been put as software inside a computer. And they are essentially; it is said through a click of a button. You can get hold of these encryption methods.

Now, there are another important requirement in electronic commerce. And that is called digital signature. Now, let us let us see why there is a need for digital signature. Suppose, you send a purchase order or say a letter to a vendor purchase order to a vendor for supplying some items. Or it could be a letter accepting some tender conditions or tender value from a vendor. And you may or it may be some kind of a query to the vendor or clarification and so on.

And the vendor also when he sends his quote, he is got to sign that quote. Because, later on he cannot say that the quote was sent by me, it was sent by somebody else. Because in the internet, you have to really see the other person personally. So, in a non electronic world that is when the internet was not prevalent. Primarily all business communications used to take place by mail. You send by send things by post or by courier. And these are all actually letters which are written, written or typed and then they are signed at the bottom.

Now the, what the signature signifies when a letter comes is that. The person who has signed has read the entire letter and he is authenticating that letter. So, he will stand by tomorrow. Suppose, he has given a code for some buying some for sending you some items, the quotation the terms and conditions will all be kind of typed out. And then, at the bottom, you would have signed it. And also, there will be a seal of the company to authenticate it. And the whole thing is put into may be a sealed envelope and sent to you.

So, you have certain amount of a faith in terms of the fact that he cannot repudiate. In other words, repudiation means he cannot go back. Later on and say I did not really send this letter or I did not really send this quote. Suppose, the quote was low quote and you accepted it and later on he says that I did not give that quotation. Then of course, he can be penalized. Because, he has got this letter you have got that letter it is signed and you can always got to a court of law.

And use that letter and say that this person is repudiated that is in bad faith. That is he did, that is he would do something he did not do it. So, he could be punished either by imposing a penalty or by requiring him to supply the items as quoted. So, the written document gives certain amount of feeling of security to the recipient about the good faith of the person who sent that communication.

Now, in the in the internet world there are two difficulties; one difficulty is that the person with whom you are corresponding. The vendor may have no physical presence what I mean by no physical presence is he may not have a physical shop or physical address. He only has a web presence. He is present in the internet, he has got a web address that is number 1.

But, even a person is in the web address, there are two types of companies which operate. Even if, you have web address you should have some kind of permanent postal address, where you are putting all your computers and working from there or the workstations and so on. So, there must be some physical location, where all these computers are placed. So, there should be an address.

But, as far as the person on the other end of the communication line is concerned. He does not really know. And he does not care, because we are essentially doing all transactions by email. So, it is all web presence which is relevant there. So that is number one that is you do not really know anything about the physical presence of the person, whether he is in the physically present or he is a phantom company which only has a web presence.

And he may be, what they call fly by night operator; that means, somebody who kind of opens shop. And then closing and runs away after a promising a number of things and collecting money may be from you and not delivering. So that is one problem. Second problem is that, suppose you do certain suppose he does send a quote to you the quotation which comes on the email.

So, it is not physically signed it is actually a name may be put or a company name may be put. There is no physical seal also there. Because, it is a certain bits which have come on the internet and gotten typed on your word processor as an email message. So, there is no physical signature. Because, there is no physical signature anybody can really masquerade as you in the sense.

That somebody can who wants to sally your reputation puts your name and send some fake message, so this a really a problem. In other words masquerading as somebody else and sending a message. So that, you had some method of authenticating that is the message indeed came from the person who claims to have send that message that is number 1. That is there is no that is you had to make sure that nobody masquerades.

Secondly, you had to make sure that he cannot repudiate. Suppose, the person did indeed send you a quotation later on he cannot say I did not send it. So, both these requirements of non repudiation and somebody not masquerading as or doing representation job of particular company of a person. These two require an equivalent of the physical signature and that is called the digital signature. And digital signature is now nowadays considered as good as a physical signature.

Because, the main which the digital signature is formed, if a signed message comes to you using a digital signature of the sender. The algorithms which are used are such that it cannot repudiate and nobody else can masquerade. So this particular document, which is neatly signed. Now gives the same kind of security in the sense that any impersonation or any revealing or repudiation can be taken to a court of law. And the court can actually find out, if the digital signature is really authentic signature or not.

The point, I am going to make is that the authenticity of digital signature. Nowadays is as good as the authenticity of a human hand written signature. Further in order to kind of ensure, the codes of law do take cognitions or they do take they do consider digital signature as legal the requirement for legal act and that is been done. The information technology act of 2000 does give a certain kind of a protection for electronic communication.

Now by defining, what digital signature is and by defining, what is repudiation non repudiation, what is masquerading and so on. So, there are two things which are required one is the legal infrastructure and the other is the electronic infrastructure. The legal infrastructure and the electronic infrastructure are now both in place in India and many other countries. Once they are in place, now one can confidently, then use the digital signature. To do communications in commerce like you do physical signature and so on.

In fact, the most important thing about the signature is that it is tied to the message. That is its tied to the letter or the quote which comes. And suppose there is some cuttings in a

physical situation. You cut you sign in the side and also if sometimes if some documents you say so many corrections had been made in this document. But of course, in the electronic world no cutting is required.

Because, as in a word processor change is so easy, if somebody made an error there is no need to kind of cut and kind of cut it by hand and things like that. In any case, you cannot get it by hand, because it is going to come sort of bits. So, in a word processor you kind of go there correct it and the corrected message corrected bit string is there what comes the recipient.

So ultimately, the entire message at the bottom of it there is signature. So, signature must have two characteristics that is one is that it should be unique to the sender. That is if I am sending a message to you I must have a unique signature. And I can show later on in the court of law that is it is been signed by me. Same thing from both sides that is B can also say that A has signed it.

Number 2 is that the signature must be such that it should be tied to the message. In other words the entire message at the bottom which the signature appears that message also should be kind of. In other words, if a message is altered by somebody that alteration should reflect as a part of the signature. So, no alterations are allowed by say vandals and so on. So, the whole point is that the signature also incorporates the entire message. And the message effectively authenticated alright.

(Refer Slide Time: 18:19)

Digital Signature

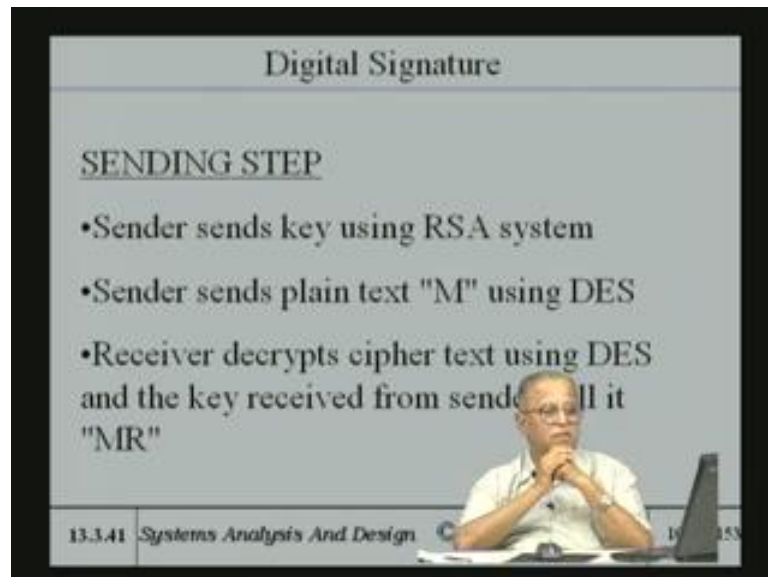
REQUIREMENTS

- Needed to ensure that a message received from say "A" is indeed from him
- Signature should be tied to the message sent by "A"

13.3.41 Systems Analysis And Design © V. Rajaraman 101 of 153

So, to kind of I said in a let me just look at transparencies now just to kind of recapitulate what I have said. It is needed to ensure that the message received from say A is indeed from him. Signature should be tied to the message sent by A these are two important thing I told you about.

(Refer Slide Time: 18:42)



Now, what are they so having said that? Now, we have to say what is the method or technique I used to sign. And the method or technique I used to sign is essentially based on the RSA algorithm. So, the sender sends the key using RSA system. They just like that it is a kind of combination of RSA and DES as usual and sender sends plain text using DES. Receiver decrypts the cipher text using the DES and the key received from sender and call it the received message.

So, message is sent is encrypted. If an RSA system is used, then what will be encrypted, with recipient's public key. So, know the recipients public key, so the recipient's public key is the one which is used to actually encrypt the key. And I after having the encrypted key that is received by the recipient. And that key can be used to decipher, what is sent by DES which is symmetric algorithm.

Of course, one did not use this hybrid. One can just send the message by using RSA only that is what you could do, is take the message. In this case, the message may be a quotation or a purchase order whatever some business document. And you encrypt it

using the public key of the receiver. And the public key and the receiver can decrypt it with its private key. So, the message has come.

So, this is only a little bit of fray I put there. This full is not essential, because the public key private key system is certainly well established. And I will know the public key of the recipient from his website. So, I can actually encrypt it his public key and he will have his own private key and he can decrypt it. So that is that is straight forward. In fact, many of the computers based systems desktop based systems at home.

And even in some companies using only RSA even though the algorithm is very complex and slow by click of a button the entire thing happens. So, I can send a message saying that encrypt using RSA and give the public key of the recipient. And the machine will encrypt with that public key and it will go to the receiver recipient. And he can just click saying that decrypt. And then it will just decrypt and give the plain text.

(Refer Slide Time: 22:03)

Digital Signature

- Sender hashes plain text "M" using a hashing function - let the hashed text be "H"
- Hashed text "H" encrypted by sender using his Private key
- DS is his signature as H encrypted with his private key
- DS decrypted by receiver using sender's Public key and obtains "H"

13.3.42 Systems Analysis And Design © V. Rajaraman 103 of 153

So having done this the sender hashes the message M using a hashing function, what is meant by hash? Is that, you take the entire message. And the entire message could be very long. So, what you try to do here is, you map it map the entire message. After all it is a bit string map it to another smaller equivalent smaller string which is called as hash string is also called as message digest. That is you take a message and using a hashing function is nothing but something which kind of takes preservers.

The content of the message, but makes it shorter that is why it is called a digest. It is something like a when you write an essay you ask somebody asked you to write a summary an abstract or a prosy. So, the message digest is somewhat like an abstract or a prosy of the entire message. The prosy must actually reflect what is contained in on to this it should be unique. In other words two different messages should hash to unique hashed results.

It is like saying two independent, suppose two little bit of articles. There are two articles and two abstracts. If the articles are different on different subjects, the abstracts will also be different. It will reflect what is contained in that and the abstract will be unique. Similarly, the message hash has to be unique that is a correct restrict of a hashing function. There are many hashing functions which have been proposed.

One of them which is called M D 5 message digest algorithm 5 proposed. Again by the company formed by its called RSA Company which also kind of controls the RSA algorithm has found a general acceptance. Because, it has all the desirable qualities of a hashing function desirable qualities being that. The hash or the digest should be shorter than the original message considerably shorter.

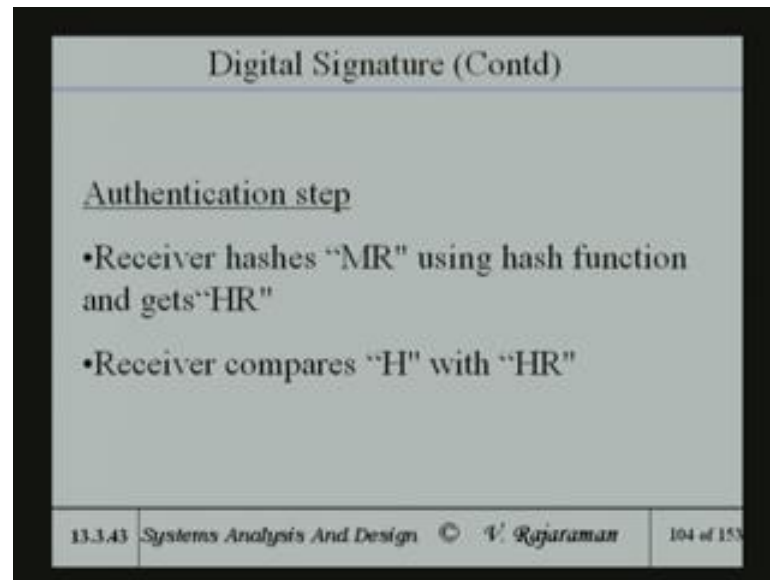
Number 2 is that two different messages even if they kind of only change in a small part still should lead to two unique digests or two unique hashes those two properties of hashing, in fact if it is a mapping which is mapping from a large to a small. So, it is always a possibility that the mapping may not be unique. But, in the case of a digital signature the mapping has got to be unique, in others words you can repudiate.

So, the hashing functions requirement is that it should be short number 1. And then, it should be tied down to the message in the sense. That if any changes in the message takes place the hash will change. So that is a correct restrict of message digest and MD 5 is a good algorithm which is used.

(Refer Slide Time: 22:03) And hashed text is encrypted by sender using his private key, what is meant by that? Is that the private key is unique to be as the sender. So, if I actually hash the take the message and hash it have a unique hash and encrypt it with my private key. Then; that means, that I have signed it, because private key is only known to me. So, having encrypted this message digest.

(Refer Slide Time: 22:03) The receiver can decrypt it with his public key because private key and public key are symmetric. So, the receiver will use this public key use your public key to decrypt it and obtain the this hash which you have encrypted.

(Refer Slide Time: 27:07)



Digital Signature (Contd)

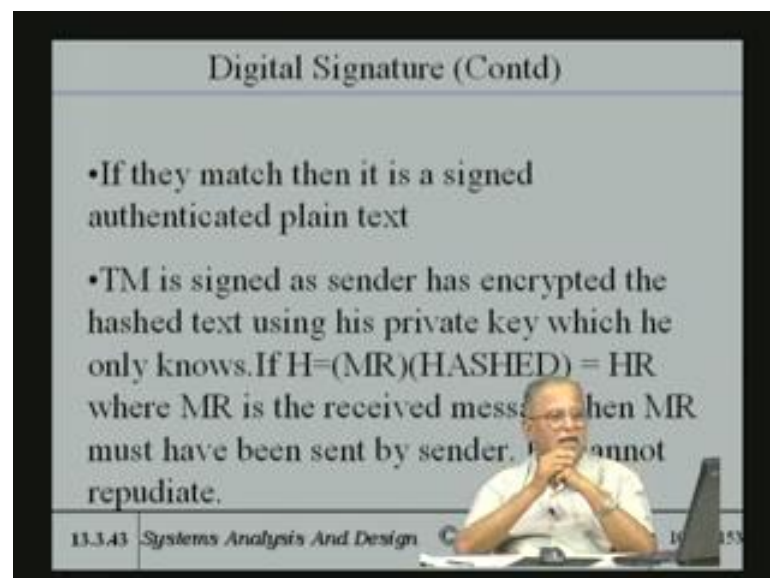
Authentication step

- Receiver hashes "MR" using hash function and gets "HR"
- Receiver compares "H" with "HR"

13.3.43 Systems Analysis And Design © V. Rajaraman 104 of 153

He also would have received the message directly and then he will hash the message. And see if the hashed message received is the same as the decrypted hash message which you signed. If the two are equal then the receiver says that it is properly signed. Because, its tied to the digest or tied to the message.

(Refer Slide Time: 27:39)



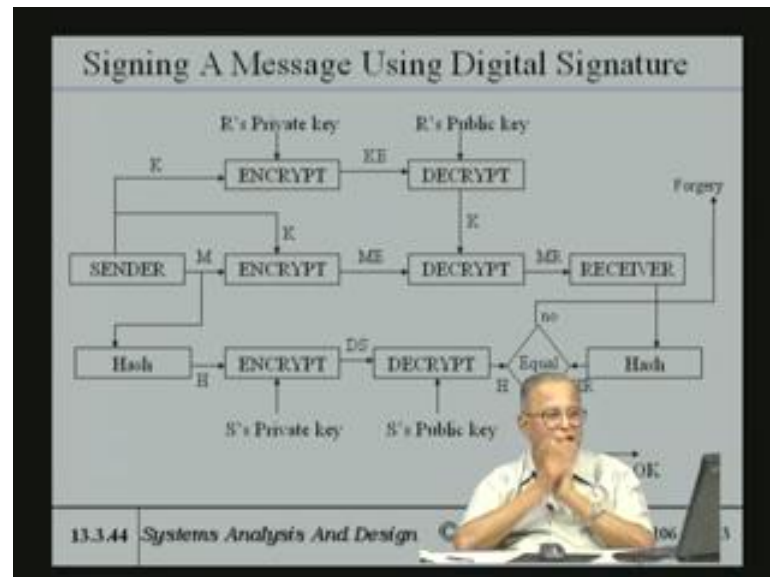
Digital Signature (Contd)

- If they match then it is a signed authenticated plain text
- TM is signed as sender has encrypted the hashed text using his private key which he only knows. If $H = (MR)(HASHED) = HR$ where MR is the received message then MR must have been sent by sender. He cannot repudiate.

13.3.43 Systems Analysis And Design © V. Rajaraman 105 of 153

If the two do not match then receiver says that if they match it is signed authenticated plain text. And if it does not match then of course, he says it is a fake message. It is sent at the reason, why it is called signature as I said it is encrypted with the private key of the sender which only he knows.

(Refer Slide Time: 28:07)



So, this is essentially the picture of the entire methodology block diagram very easy to explain on the hash on the block diagram. The sender in fact, I think we can say it is a fairly straightforward thing, you can see here. In fact, I am using the digital standard encryption also in this case, but that part need not be even necessary. Because, instead of sending the message and encrypting with the key here. The message could as well go here.

So, I can just look at it in the following way, sender sends the message. And the message is what would the message be, I had encrypted with the public key of the receiver. There is an error here looks like. See because, actually I cannot use the receiver's private key I do not really know. The receiver's public key is only what is known to the sender. So, the sender has to encrypt with this is only the signature part see.

So, the actual message part it can be just looked at this way. You just forget about this part which is really the part which does the DES encryption. In fact, even the either way this should be R's that is receiver's public key see encrypted with receiver's public key.

So, the message is encrypted with receiver's public key. And the receiver can use his private key to decrypt.

And you received the message in this case what I have done is key is encrypted. And the key is also sent here and the key. The message will be encrypted using this and decrypted using the same key. So that, you got the received message only mistake is this should be public and this should be private. So, R is public key one which is used to encrypt K and R's private key is used to decrypt K and then the message comes here. So, this is the received message alright.

Now, he takes a hash, the message is taken and it is hashed by the sender using the MD5 algorithm or hashing algorithm. And the hashed function comes here and it is encrypted with the sender's private key. Sender knows his private key and that is what is meant by signature, he's signing with his private key. And so, there is a actually encrypted message digest.

And now, the sender's public key is known by the receiver. So, he can decrypt it using the public key of the sender. And having done that, he will get the hash, because hash is being encrypted and decrypted. So, the hash has come he also receive the message. Just to see that the message is what was sent by the sender or the message is tampered with on the way by somebody changed and so on. And also that certain later can't repudiate. So, the message received by the receiver is hashed by him.

The hash function is publicized for both, because both of them have to use the same hash function. And they basically agree for this instance that both of them will be defined for instance. This hash function again would be normally put this part of the computer program for digital signature. And that program itself will do the digest that is you say you take kind of you pick up an icon and say hash.

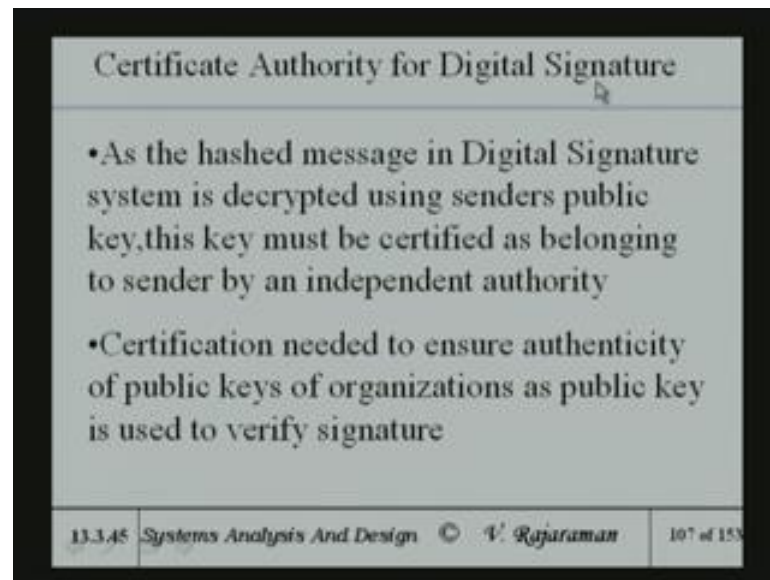
And then it is just hash it. (Refer Slide Time: 28:07) using any defined algorithm which is standard algorithm, the digital encryption standard also. In this case and so the recipient will also use the same algorithm and you will get from the received message the hash function and then, you will compare these two hashes. And if they compare signature is will accept the message. If they are not, they do not match themselves forgery.

Somebody has in between come and done it or it is somebody masqueraded it, because if masqueraded it. Then, somebody knows your private key, if some other private key is used. Then of course, he could not decrypt it also. So, the primarily it kind of protects you against somebody kind of gets your private key. But then, he has changed the message. Then of course, he cannot do anything if you use your private key. Then, it is like using a seal your seal.

So, you cannot lose your private key. So that is got to be extremely confidential with you. So now, because two hashes match nobody on the way could have changed it. So, this is primarily the whole idea. In fact, you can remove this and say message is sent and encrypted by the recipient's public key. That is what is important I think, but this stupid error here I mean at while typing they made a mistake. It should be private key, because any public key algorithm. Public key algorithm only knows the public key of the recipient.

He does not know the private key a person sender knows his own private key. He will know the public key of the he will know only he will not know the private key of any anybody else. So that is highly secret. So, the only for signing you use your private key. And because of the symmetry of the RSA algorithm signature also works, because what had been encrypted with the private key, can be decrypted with the public key. You encrypt with your private key you decrypt it by your public key. So, this is the general idea of how to digital signature.

(Refer Slide Time: 35:15)



Now, there are other problems which arise with digital signature. First of all, you are using the public key while when you are sending this, if we are using the public key of the recipient. (Refer Slide Time: 28:07) See the public key of the recipient is being used here for encrypting. So, the public key should be authenticated.

(Refer Slide Time: 35:15) As the hashed message in digital signature system is decrypted using senders public key. Then, signature also depends upon the senders public key. In other words, I am decrypting using the public key of the sender. So, the senders public key the it has published it. You should be sure that the sender in fact, does have this public key.

And so, there must be some certification authority. As the hashed message in digital signature system is decrypted using senders public key. This key must be certified as belonging to sender by an independent authority. In fact, the information technology act puts down a requirement of certification of public keys. Certification of public keys, the primary authority certification authority which oversees the entire certification process is in the ministry of information technology of the government of India.

And that is official who's designated as the person in charge of this certification authority. Certification authority allows some vendor to give digital certificates. Because, there may be lot of people who want to have public keys. So, one official and one government department may not be in a position to do it very effectively. So, what the

government decided was to kind of some reputable companies to maintain a public key infrastructure.

And have the authority to issue public key certificates. To the various people who wanted. So, normally when two part two parties wanted to actually carry out business among themselves each one will exchange their public key. They did not they also give their certification and certification number and things like that to the other person. Suppose, I want to transact business with you I know your public key by I really want to make sure that.

That is indeed your public key that you do really exists as a legal company. Then, I will ask you for your public key certificate number. And ensuring authority and you had to give me that information. Then, I can go to the public key encrypt the person who has given me that. And code the number and say this person says that he has his public key and certification number is this. Can you let me know whether such a company or a person does exist or not. Certification authority for may be a fee will give you the information.

(Refer Slide Time: 35:15) And the certification authority has to actually in order to authenticate or authenticate.

(Refer Slide Time: 39:29)

The slide is titled "Certificate Authority for Digital Signature". It contains two bullet points: "• Certification authority keeps data base of public keys of organizations participating in e-commerce after verifying their credentials." and "• Potential business partners can authenticate public keys by sending request to certifying authority who certifies after receiving a fee for his services". The footer contains the text "13.3.45 Systems Analysis And Design © V. Rajaraman" and "108 of 153".

Certificate Authority for Digital Signature		
<ul style="list-style-type: none">• Certification authority keeps data base of public keys of organizations participating in e-commerce after verifying their credentials.• Potential business partners can authenticate public keys by sending request to certifying authority who certifies after receiving a fee for his services		
13.3.45	Systems Analysis And Design © V. Rajaraman	108 of 153

The public key what he would normally do is to kind of verify the presence of our company. For instance the whether he has the sales tax registration number income tax payments stuff like that. So, certification authority keeps database of public keys of organizations participating in e commerce after verifying their credentials, what is meant by credential verification? Is essentially as I said physical address just like whenever you want to try to get a phone.

The company will ask you for a physical address and prove the physical address by giving you giving identification card or passport or what have some certified thing. That is passport is considered as good enough document to actually certify an individuals address and his actual presence physical presence, because the passport is issued only after passport verification of the existence of a person.

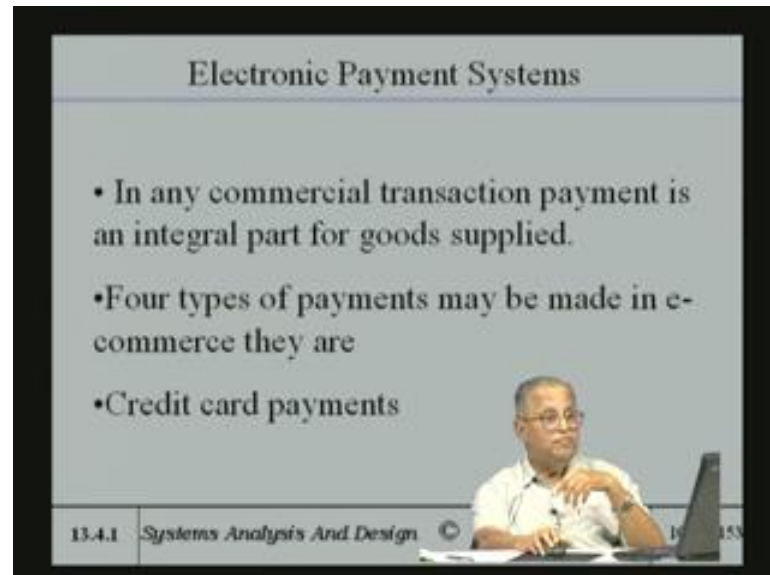
So, the provider like telephone company for giving you a telephone or even a mobile phone is suppose to actually find out using some authentic document like a passport or so on. To authenticate your address and to kind of authenticate, whether you really exist as a person that is you are not being on indulgent that is somebody who does not exist. But pretends to exist, there is been a serious problem recently, because a number of mobile phone companies have been giving mobile phone connections to nonexistent persons.

Particularly, the prepaid cards and prepaid SIM cards and so, for law enforcement when they want to kind of trace a particular mobile phone from SIM card it becomes difficult. Because, the person is kind of phantom person he does not exists really. So, you want to allow that phantom person phantom people in the internet and e commerce that is the reason, why the certification authority actually may even send inspectors to a residence or to your company to find out whether you actually are present.

And ask for documentations like sales tax registration stuff like that before issuing a public key certificate. And this is the primary point and of course, a number companies I know for instance TCS is a recognized company for issuing public key certificates. There are many other companies which are being allowed. The reputable companies which are well known companies which are willing to maintain a public key infrastructure keeps his database public keys and make sure the credential of credentials of all the parties and so on.

And it is a fair amount of work, but of course, you do it at fee and of course. That fee is of course their they will have some little bit profit on doing that.

(Refer Slide Time: 42:51)



(Refer Slide Time: 39:29) So, this primarily done then to conclude this digital signature idea, the two important points is that the message is sent as it is. But, encrypted and its encrypted with the public key of the receiver. And the receiver decrypts it and gets a message, which will be a purchase order or quote or whatever. And signature is done on the digest by the private key of the sender.

See public key is one which see and the private public key is the one which is actually authorized by the certification authority. The reason why public key is authorized is authenticated is because the receiver now decrypts the message digest using the public key of the sender. And gets the message digest. And then, it compares the received message digest with the digest which came by after signing.

And that is how it authenticates the message and that is the primary reason, why the entire digital signature requirement, has three basic requirements. Public key and private keys public key certification and agreement on message digest and a unique message digest, these are requirements of a very digital signature system, because without a certification a certifying authority digital signature will not have any meaning, particularly when it comes to a rectification in the court of law.

The next topic which is important in the electronic commerce is payment. Payment is a very important part of any commercial transaction if you go to a shop and buy some items there are many ways you can pay for the item. One way of paying for the item is by cash good old cash. If it is a small, if it is an item which does not cost too much like your buying a packet of biscuits which may cost 10 or 12 rupees then only you give a cash and be off. With it if it is a very expensive item like may be music system which may cost 10000 rupees.

There are two ways of paying for it. In the normal systems, one way of paying for it is to write a cheque, if you write a cheque of course, the shop keeper should actually trust, you that you have good credit risk. And that your cheque will not be fake. So, he will accept your cheque if you he knows you and if he has faith in you. He may not accept cheques in all in Sunday. Because, a cheque is not any cash, he has to send it to the bank and the bank has to encash it. And you must have some money in your bank if there's not enough money in the bank the cheque will bounce.

But as of today, of course of the law it says that you cannot issue a cheque, we do not have money in the bank. And if you do that you are liable to be prosecuted and sent to jail, but as as our legal system is so slow. That shop keepers do not want to go court and stuff like that. So, they prefer to get cash from you or the third method of paying is a credit card. So, you have a credit card you give the credit card and the credit card is used by the vendor.

And nowadays, it is a very common method apart from credit cards. There is also debit cards debit cards are somewhat different. Credit card is that, you give the credit card and you get a bill from the bank say few days later about 25 days to one-month later. So, you will get some kind of a credit period for you to pay the money. And also there is no need to pay the whole amount simultaneously. You can pay in small small installments,, but of course,, they will charge you interest on outstanding.

So, that is that is one way the other is debit card, debit card is that you have a bank account. And so, the debit card will actually debit in your bank account. So, unless you have money in the bank, you cannot give debit card, because it will be not accepted. Because, if he does not have enough credit balance in your bank the debit card will be rejected.

But, more commonly in moderate house by and large people who have many shops do not even I do not know for what I do not know there is a good reason or not. But, I know that some many shops accept credit cards. But, they do not accept debit cards or because of the fact that there are two different type of equipment they require for these two. And most shops seem to have an equipment for credit card. And they prefer to work with credit card then rather than debit cards, but then anyhow that is up to the up to the shop.

So, similarly the electronic commerce one would like to have a (Refer Slide Time: 42:51) say in any commercial transaction payment is an integral part of goods supplied and it is obvious four types of payments can be made in e commerce. In e commerce also there are number of different payments which can be made. One is credit card payments. See normally in C A to BE commerce customer to business e commerce such as when you want to kind of buy some books from Amazon dot com or India books dot com and so on.

You give credit card number and that is used by the recipient. And then, he authenticates the credit card and gives you the books once the credit card is authenticated alright. So, this is one way of payment. Because, there only thing credit card is given credit card number is given. But, very many people are somewhat worried of giving the credit card number on the internet. Because, unless security is very good if somebody else gets hold of your credit card number then he can masquerade as you.

And then give the credit card number and then get the payment get the goods. The question really is the credit card number must also be signed by some method. Apart from the credit card number itself there should be some signature. That requires certain kind of protocols and certain kind of infrastructure. And in many situations in India that signature part is missing, what they only do is that, the credit card is encrypted and sent and is decrypted by the receiver.

And this is not enough, because encryptions can be sometimes be broken. And also the receiver, if he receives this credit card number. There could be a leakage store is there someone who is employs can get hold of the credit card number. And use it in without authentication which has happened in banks and so on. So, unless it is a value validated system whereby the receiver does not know your credit card number. It cannot work too well and in India.

And also in many countries currently, it turns out that it is a little bit of risk. You are taking and that is the reason, why there is not tremendous growth in the e commerce with credit cards purchase. But because of course, to a small amount of money, we do not mind. But, when large amount of money you do worry about revealing your credit card number on the net. Of course, even otherwise if your credit card number gets known by somebody, he can order something of which very expensive without your knowledge. So, that is the affair.

So, there must be a method of ensuring what I would say the secrecy of the credit card number. And also the credit card later on you cannot repudiate it and so on. So, there must be a signature also for that these two requirements are there. But many of the systems currently in use do not have this. That is the reason people are worried about. Apart from credit card payment, the other payment of course, is by cheque. And normal cheque payment is the one which are used in between two businesses in e commerce, cheque payments are more common.

In fact, it is normally equivalent cheque would be authorizing your bank by the electronic clearance system to debit your account and credit the account of the recipient. That is suppose I ordered some items and I had to pay 2 lacks rupees for those items to a vendor. I kind of send a request to my bank to debit my account per 2 lacks and credit it to the recipients account. And these all done electronically and of course, you got to do extremely securely. So that is a other method of payment.

Third method of payment would be cash payment equivalent of cash. But then, cash has got lot of problems see over the advantage of cash transactions. Cash is anonymous, what is meant by anonymous cash? Is that suppose you lose ten rupees say you drop 10 rupees from your purse. Somebody else picks it up, he can use that 10 rupees. So, it is not kind of tied to you. It is a kind of an exchange mechanism which is kind of open other words cash is anonymous.

So, anonymity of cash transaction to maintain in the web is somewhat difficult. And governments do not also want to have large cash transactions taking place in an anonymous way on the internet. In an actual physical situation also cash transactions beyond a certain amount governments do not normally allow. Because, they put a limit

on how much cash has been put in a bank account. When you exceed an certain amount you have to kind of reveal your income tax pan number and some stuff like that.

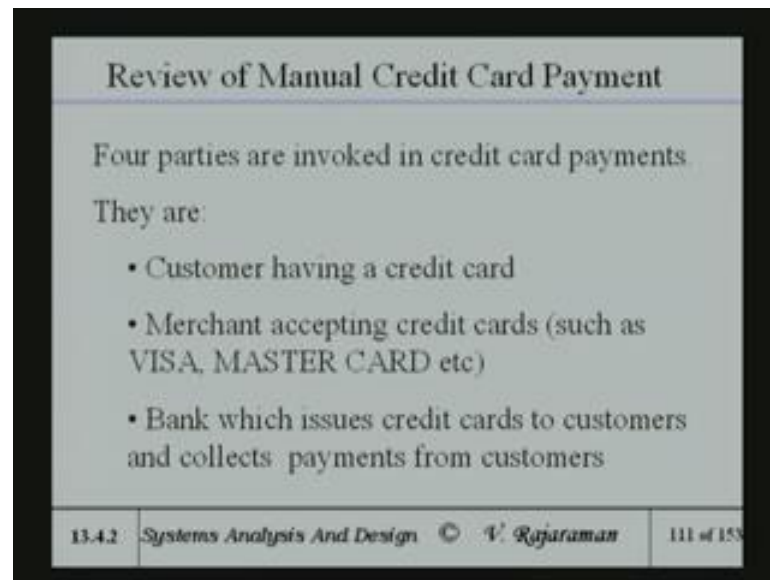
So, by and large cash transactions are discouraged on the net by governments. And so, normally cash transactions are somewhat daisy on the net. And even that, you had been trying to kind of mimic cash transactions is not been very successful. It is because of the limitations of the net itself. The fourth kind of payment its somewhat slightly different from huge cash transactions. These transactions are of small of small amounts, what is meant by small amounts is.

Suppose you want to get say 10 pages of an article. If and then get it to you that 10pages may cost only about 10 rupees something like that. It is a very small transaction. So for small cash transaction, one would like to be able to have some method of debiting. In other words keep some little balance with somebody. And every time you make a small transaction like this you debit that. And so, there is a limit which is put towards cash transaction.

So, you do not come a foul of governments and so on and also the method which is used is such that security is not all that important if it is a small cash transaction. So, you can make it fairly fast. In other words, the point is that if the transaction cost is very large. And the amount is very small one wont like to kind of use a big transaction cost for low cost item. That is the reason, why if you use a credit card in a shop and you want to buy something which is worth 15 rupees and want to give a credit card, he will not accept.

Because, the certain kind of that is a minimum limit which is required above which you had to have transaction for credit cards to be used effectively. Because credit transaction itself, cost some money and that cost may exceed 10 rupees. So, there should be point in using credit cards for small amounts. So, you need to have some other method like of course, in normal shops you use pure cash.

(Refer Slide Time: 58:24)



Review of Manual Credit Card Payment

Four parties are involved in credit card payments.

They are:

- Customer having a credit card
- Merchant accepting credit cards (such as VISA, MASTER CARD etc)
- Bank which issues credit cards to customers and collects payments from customers

13.4.2 Systems Analysis And Design © V. Rajuraman 111 of 153

So now, I would like to look at first manual credit card payment system how does manual credit card system payment work. And then, we will try to see if we can mimic this manual system to an extent possible, because anything which is manual cannot be entirely mimicked in electronic system. So, you would be like to able to limit to an extent feasible.

So, one has to first look at the, what are all the parties involved. Four parties are involved in the credit card payment. Customer having a credit card merchant who accepts a credit card merchant who put notice saying that VISA cards MASTER cards etcetera etcetera and dear so on.

So, there are credit cards many many companies give it and bank which issues credit cards. I mean VISA has a agreement with SBI and also they have agreement with many banks. And you break bank is the one which ultimately handles cash.

(Refer Slide Time: 59:31)

The slide is titled "Review of Manual Credit Card Payment". It contains a single bullet point defining an Acquirer. The footer includes the course name "13.43 Systems Analysis And Design", the copyright notice "© V. Rajaraman", and the slide number "112 of 153".

Review of Manual Credit Card Payment		
<ul style="list-style-type: none">•Acquirer which is financial institution that establishes an account with a merchant,validates credit card information sent electronically by merchant and authorises sale		
13.43	Systems Analysis And Design © V. Rajaraman	112 of 153

And acquirer which is a financial institution that establishes an account with a merchant validates credit card information sent electronically by a merchant and authorizes sale. So, all parties are involved. So, we will continue from this point onwards next time and look at credit card payments in the electronic world involved. So, we will continue from this point onwards from next time and look at credit card payments in the electronic world.