

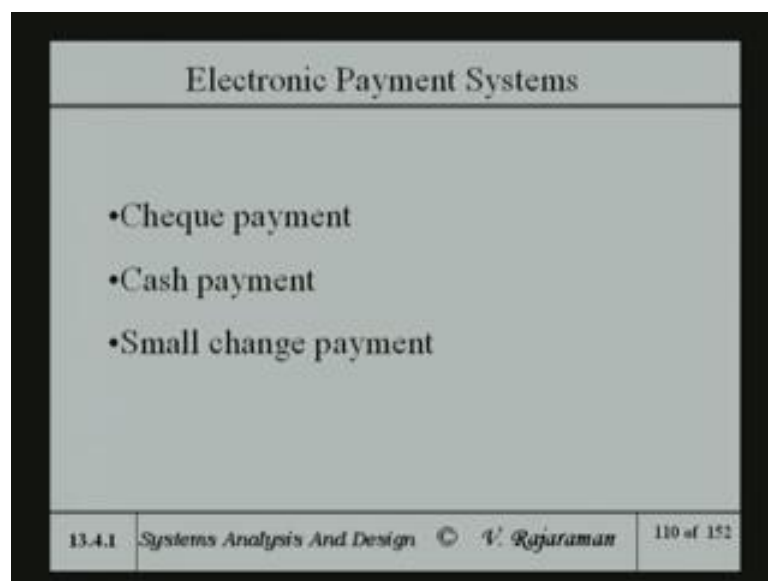
System Analysis and Design
Prof. V Rajaraman
Department of Super Computer Education & Research
Indian Institute of Science (BSc.), Bangalore

Lecture - 37

We talked about the electronic payment systems. We said that in any commercial transaction payment is an integral part, for the goods supplied. And there are four types of payments, which may be made in e commerce. The most common one in customer to business that is or b to c, you might say. B to c commerce is the credit card payment. And that is what, where you spend a fair amount of time because it is an interesting type of an encryption we had to do.

And there are some new standards, which have come up. And I will have to discuss that in some detail to be able to talk about the credit card payment. And apart from credit card payment, there are three other payment techniques.

(Refer Slide Time: 02:11)



One is cheque payment. And I told you last time what the analogy is in terms of when you go to a shop, you can pay by cheque also. If, they trust you. So, in b to b e commerce cheque payments is more common. Of course, cash payments is normally for small amounts. And cash, the greatest value of cash from the point of view of a shop keeper and a customer is that one does not have to authenticate cash. Cash is a does not require

any further authentication. Provided of course, the currency notes and all are not really fake, which is normally not the case.

One other important thing about the cash is anonymity. That is anybody can give cash. When you give cash to a shop keeper, he does not keep down the note down the numbers of your currency note, which you are giving. Because, that will be too difficult and it will too time consuming. So, normally they will not do that I mean, they used to take it everybody vendors cash, the cash has the same value.

So, it is anonymous who paid it? If you ask him he will not be able to know. So, anonymity is one of the greatest assets of cash payment. That is what governments are worried about, anonymous payments through cash. Because, it can be for all kinds of illegal purposes also. And of course, lastly it is small change payments, small change payments are things like. You know, getting few pages of book, copy of that or downloading one music track from an album things like that; which do not require too much of money to transact.

But, then it is a small change after then each transaction cost must be called to low. So, the transaction cost you see is much lower than the cost of actually transacting the business. In other words, the smaller the change you know the one would ideally have situation where. Smaller the change less is the amount of computer time. And other overheads you spend. But, by and large it turns out that the regardless amount. The amount of time spent by the machine would be the same.

But, they normally put some kind of a lower bound, below which you really cannot go. So, these are the four types of payments, we already talked about. And today I will start talking about the credit card payments. Because, as I said in b to c commerce, it is a most common kind of a methodology, which is used for payment.

Now, when you just look at the way in which the manual credit card payment goes on. When you go to a shop and offer a credit card, what are the steps, which are carried out. The reason we would like to kind of look at that is in the electronic commerce world. The same steps are actually mimicked or you try to make an analogy, of the same steps in the computer world you might say.

But there is a some significant differences, which will come out. When we talk about the manual credit card payment, versus the payment on the internet. Because, internet the payments are anonymous, in the sense that anonymity. In the sense that the customer face is not seen by the shop keeper. The shop keepers face is not seen by the customer. The shop keeper or the seller may have only the web presence and the customer may be really transacting business from even a cyber café. He may not own a machine of his own.

So, there is a lot difference because you do not really have an opportunity to see the customer. Similarly, the customer does not have an opportunity to see the shop keeper. So, this creates an extra security concerns, when you come to electronic world. So, in a credit card payment, normally four parties are involved.

(Refer Slide Time: 07:22)

Review of Manual Credit Card Payment

Four parties are invoked 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

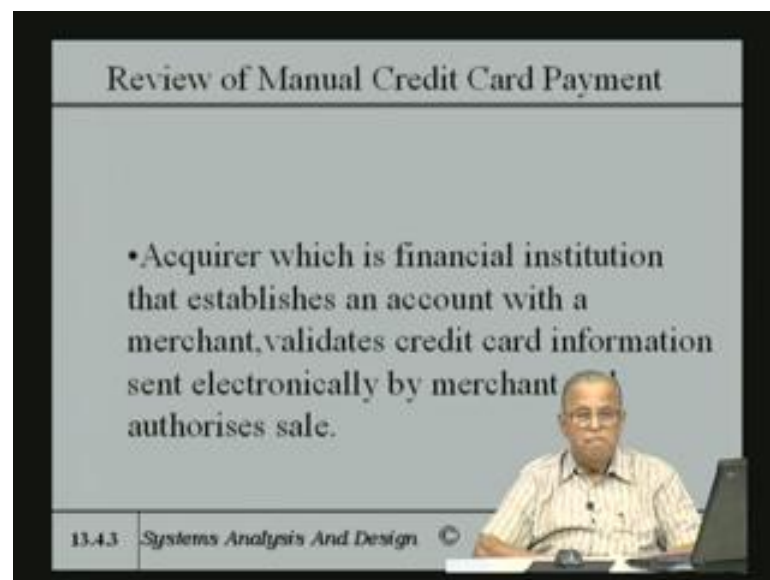
13.4.2 Systems Analysis And Design © V. Rajaraman 111 of 152

One is the customer, who has his credit card. See, the customer who have the credit card is the one who tries to use it in a shop. The merchant who accepts the credit card. And the merchant, normally will accept credit cards from many credit card companies. The most common ones in India are VISA, MASTER CARD, American express and so on. They are number of them and when you go to a shop outside they will have a notice saying that they accept VISA and MASTER cards and Bank of America cards. Whatever or American express cards or whatever, there are number of different agencies, which have an agreement with the shop keepers.

And of course, they also give you a credit card with their own emblem and so on. And they normally the cash is collected by a bank. Whereas the bank have an agreement with the credit card company. And for instance the State Bank of India, the cards are VISA cards, if you go to Canara bank, the Canara bank has got MASTER card as their partner. So, different banks will have different partners. Or in fact, VISA may have more than one bank as it is customer.

And the bank is primarily the intermediary. Who will collect the cash on behalf of the credit card company and then remits the credit card company who get cash. And of course, there is a certain amount of commissions and so on, which are agreed to between the two.

(Refer Slide Time: 09:10)



Review of Manual Credit Card Payment

- Acquirer which is financial institution that establishes an account with a merchant, validates credit card information sent electronically by merchant authorises sale.

13.4.3 Systems Analysis And Design ©

And there is called, there is another party called an acquirer, which is again an intermediary which is a financial institution that establishes an account with a merchant. In other words, the merchant as I said may deal with more than one credit card company. In other words he may accept VISA, MASTER card, American Express and so on. So, the bank only issues one credit card companies cards.

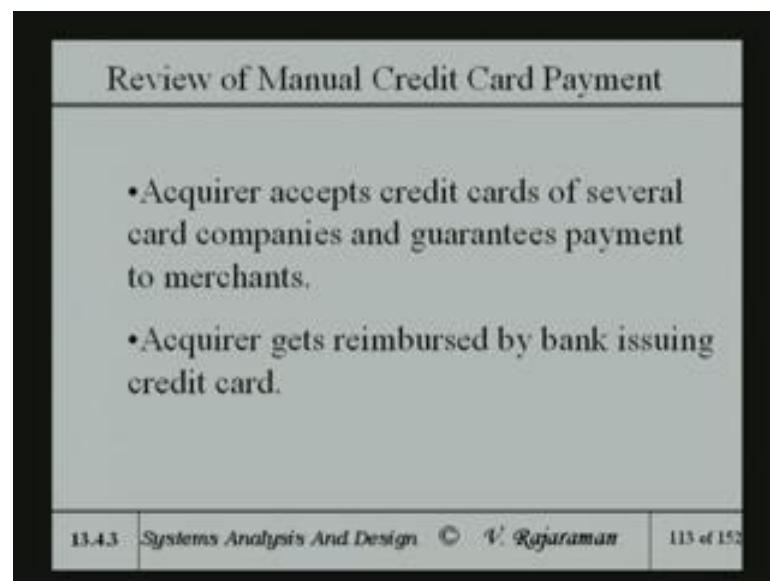
So, the acquirer is somebody holds an arrangement with several credit card companies and also have arrangement with banks. So, the acquirer is called an acquirer from various institutions. May be a bank, one bank which establishes an account with the merchant, validates credit card information, sent electronically by merchant and authorizes sale. For

instance, a particular merchant may have an arrangement alignment with say ICICI bank or Bank of Baroda or whatever it is.

Even if I as a customer go and present a VISA issued by SBI, the merchant will accept it. But, he will transact business with the, in this case acquirer, which may be another bank. And the acquirer is an intermediary you might say between the merchant and the credit card company. And the issuing bank and the customer all four are somewhat involved in the loop. And so acquirer is financial institution that establishes an account with a merchant. Validates credit card information, sent electronically by merchant and authorizes sale. In other words that is the valid point as the merchant is concerned.

Acquirer accepts credit cards of several card companies, as I pointed out and guarantees payment to merchants.

(Refer Slide Time: 11:05)



So, as for the merchant is concerned, he makes the credit sale and provided that sale is okayed by the acquirer. Then the acquirer guarantees the payment to be made to the merchant, he cannot renege in that payment. And the acquirer of course, gets reimbursed by bank issuing credit card. So, there is a, and the bank in turn will collect from the customer. So, there is kind of a complex loop, these goes on.

(Refer Slide Time: 11:41)

Sequence of Transactions in Manual Credit Card Payment

Step 1: Customer presents credit card after purchase. Merchant swipes it on his special phone and enters amount.

Step 2: Data from merchant's terminal goes to acquirer via a private telephone line

13.44 Systems Analysis And Design

Now, the steps, manual steps which take place when a customer presents credit card after a purchase. Merchant swipes what he will do is that, he will create a little slip with the. In other words, the only the amount will be essentially what he does there is a special data terminal in the merchants shop. It is like a telephone terminal and it is connected by a private line to the acquirer.

So, that he does, not normally use the public switched telephone network. It is a special kind of a telephone like instrument with a keyboard and also a place on which the credit card can be swiped. So, what he will do is, he will swipe the credit card enter the amount. And this will go the bank and the bank will say accept, if the credit is good. And so they accept, will be kind of printed on that slip.

And the slip also the will have the amount of purchase and what all you purchased. So, that is a listing of items you purchased, the total amount which you have been charged and it has been Okayed, accepted by the acquirer. And then he asks you to sign that particular. So, merchant swipes in on his special card, enters amount, data from the merchants terminal data goes to the acquirer.

(Refer Slide Time: 13:29)

Sequence of Transactions in Manual Credit Card Payment

Step 3: Acquirer checks with the issuing bank validity of card and credit-available.

Step 4: Acquirer authorizes sale if all OK and sends approval slip which is printed at merchant's terminal.

13.4.4 Systems Analysis And Design © V. Rajaraman 115 of 152

And acquire checks the issuing bank, the validity of the card and the credit available. The credit availability, the acquirer will not know because ultimately the card which is issued to the customer may be by different bank. So, acquirer authorizes sale if all, in other words he gets from the bank issuing the credit card.

(Refer Slide Time: 13:54)

Sequence of Transactions in Manual Credit Card Payment

Step 3: Acquirer checks with the issuing bank validity of card and credit-available.

Step 4: Acquirer authorizes sale if all OK and sends approval slip which is printed at merchant's terminal.

13.4.4 Systems Analysis And Design © V. Rajaraman 115 of 152

It authorizes sale and sends approval slip, which is printed in the merchants terminal which is approved.

(Refer Slide Time: 14:01)

The slide is titled "Sequence Of Transactions In Manual Credit Card Payment". It contains two steps:

- Step 5: Merchant takes customer's signature on the slip-verifies it with the signature on card and delivers the goods.
- Step 6: The acquirer pays the money to merchant and collects it from the appropriate issuing bank. The bank sends monthly statement to customer and collects outstanding amount.

At the bottom of the slide, there is a footer with the text: "13.4.5 Systems Analysis And Design © V. Rajaraman 116 of 152".

And the merchant takes customers signature, physical signature on that slip he takes the physical signature and normally he is suppose to compare that signature, which you put on that slip with the signature in the credit card, the credit card itself got at the back of the card a small place where, you are supposed to sign. So, that signature is there. So, these two signatures are compared by the merchant, just to authenticate that the card really belongs to the person who brought that card.

So, the signature comparison is of course, in the somewhat cursory I might say in other words, it is not all the detail like may be a bank will do if you supply, you know if you visit a lot of cash. But, it is in other words some kind of a comparison of the two signatures and because you have signed it in his presence. So, unless an expert forger, that you may not be able to exactly reproduce what is in that card.

So, he if you sign it in his presence, he understands that you are the legal card owner, he accepts that particular payment from you and gives you the goods, if he suspects any kind of forgery and so on he will not give you the goods. And he will intimate instead the acquirer that this card is probably stolen or whatever it is, if he suspects, but that is entirely up to the merchant, by and large my experience the merchants can trust the customer, particularly if the customer is a regular customer or if the customer looks okay and things like that.

In any case, it is the duty of the merchant to kind of take signature and compare it, because later on if any dispute about the about the sale, about the amount and the quality of the goods also then there is a sign receipt, which is available with the customer and a copy of that is available with the merchant. So, both of them have got that authenticated signed copy and that signed copy can be a legal document, based on which one can probably take legal action if it is called for.

The acquirer pays the money, because later on the acquirer will pay the money to the merchant and collects it from the appropriate issuing bank. The bank sends monthly statements to the customer and collects outstanding amount, that is ultimately see as far as the customer is concerned the convenience for the customer is that he does not have to pay the cash for every transaction.

So, at the end of the month, the total purchases made through the month that is consolidated into one particular statement and that statement is sent by mail to the customer by email or by postal mail or courier or what have you. And the customer is given certain number of days, 10 days, 15 days or whatever to settle the payment with a cheque, you send it to the bank which issued the credit card.

Also the credit card companies again, the reason why it is called credit card is because even if you say you purchased about twelve thousand rupees worth of items in a particular month. And you may not have twelve thousand ready cash to pay then they will say they will pay minimum twelve hundred rupees or whatever and the rest of it is a credit in your account, up to a certain credit limit which he allows and then on that credit, very steep interest rates are charged, what I mean by very steep is that the interest rates are something like two and a half percent a month it is a very, very high interest rate.

And that is the money on which the bank survives, in other words the entire transaction and the amount of money spent by the bank in all doing this and maintaining their accounts, maintaining everything is normally recovered from the people who are the ones who take a debt from the credit card, from the bank invariably at a very high interest rate.

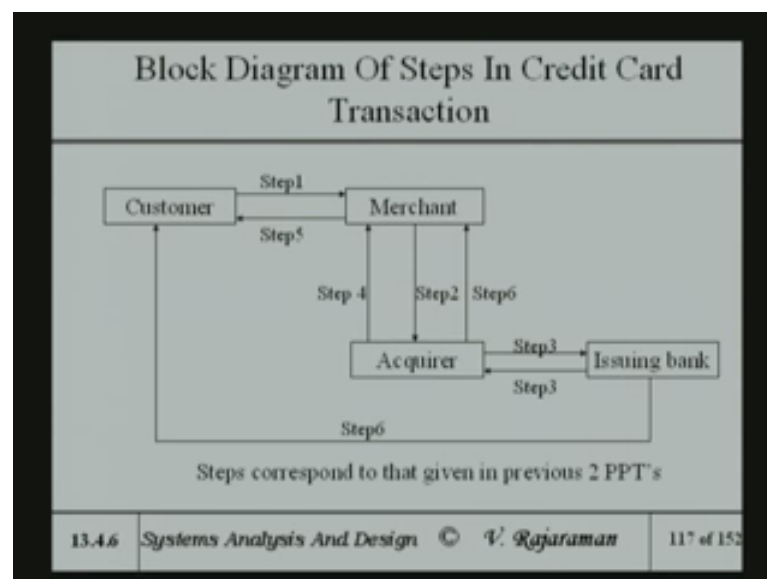
And that is a kind of, if you do not take a you know, if you do not keep a large outstanding then you do not pay interest at all you, just clear your amount every month. But of course, every year they charge you something for the privilege of having a credit

card that is certain yearly subscription, you have to pay to the issuing bank, which will pay which will certainly pay for the reverent or whatever they have done for you.

But, by and large, the point I am trying to make is that the convenience is there for the customer. And so the credit limits also there and the payment is made periodically by the customer as and when the bill comes and. So, have a certain kind of period question period during, which you essentially key have free credit may be almost about almost a month some times, because the begin cycle is one month.

And if you buy in the early part of the month then of course, the whole month you are not paying and you are give given certain number of days of grace breaks later on. So, the point I am trying to make by and large is that the credit card has got to return value from the point of view having some credit also convenience of being able to pay at any given time, but you had also to remember that if you are not able to pay in time, you pay a steep interest rate. So, I put the put down this block diagram.

(Refer Slide Time: 20:27)



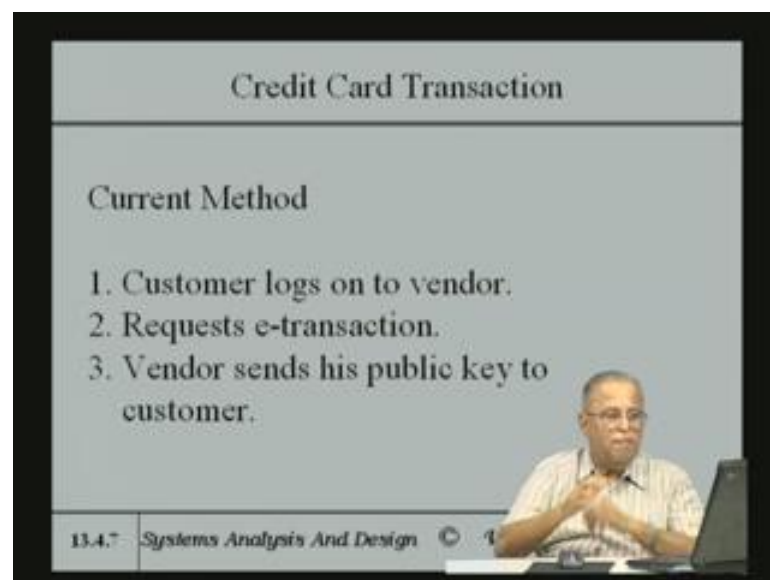
So, various steps, first step is customer purchase the items and presents the credit card and the credit card is swiped by a merchant and goes to the acquirer, the acquirer step three checks with the bank, whether the credit card has got a appropriate credit limit balance and. So, on and okayed by issuing bank tells the acquirer, acquirer in step four tells the merchant its okayed by printing approved on that slip. And then the merchant in

step five takes that signature and gives you the goods and in step six of course, issuing bank will send you the monthly bill and. So, you have to pay for that at that time.

So, these are the various steps involved in things, similarly when the bill is even sent before normally depends upon what kind of payment, the acquirer will have with the merchant. The acquirer will also not pay the merchant instantaneously they will try to accumulate the whole months charges from a merchant at the end of the month, the cash, the cheque, equivalent of whatever has been sold would be credited to the merchants bank account.

So, step six sometimes may acquire, may happen simultaneously that is merchant gets monthly payment and you get a monthly bill. So, this is the manual transaction.

(Refer Slide Time: 21:57)



Credit Card Transaction

Current Method

1. Customer logs on to vendor.
2. Requests e-transaction.
3. Vendor sends his public key to customer.

13.4.7 Systems Analysis And Design © 1

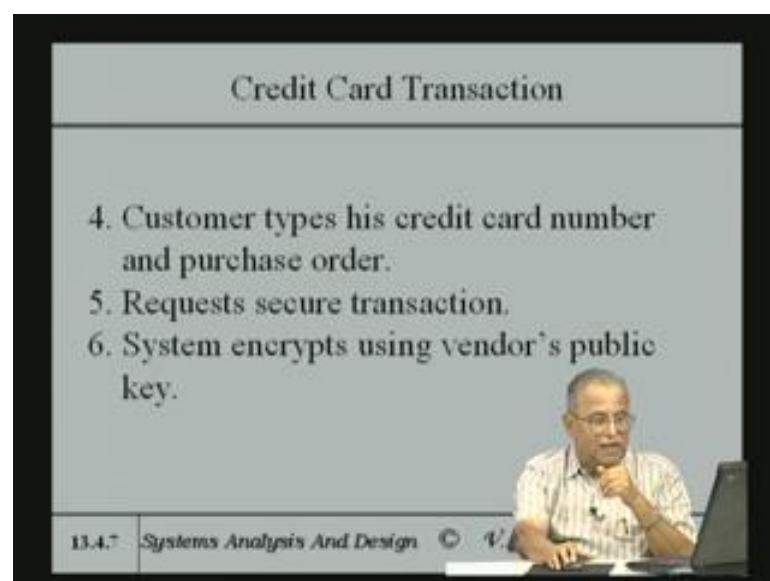
Now, currently in India and also many countries, security of payment of credit card through credit card on the internet is not all that, what I would say all that secure. Security is not all that good, there will be many, many instances of credit cards number being stolen by hackers and so on. So, new types of protocols are coming up and to the best of the knowledge, these new protocols are not yet been implemented in many countries, including India because it requires a far amount of basic infrastructure requirements.

And that basic infrastructure requirement are not yet in place and that also costs both money, as well as certain amount of extra paper work and so on. So, I will first very quickly talk about the current method, which people use in the sense that when go to your terminal and you carry out a credit card transaction, after he makes some purchases from a e shop on the internet.

These steps we go through, you log on to the vendor through (23:29) ok and request an e transaction. So, when you require any e transaction, whether you are going to purchase something, you request a transaction, when you request you request a transaction he will ask you to use secure line, because the credit card number which you are going to reveal should not go through a public switched network in an unencrypted form, in other words insecure method.

If it is not encrypted and send as it to us, you are exposing yourself to snooping by whole lot of hackers, who may get hold of your transmission they look at the transmission they can immediately kind of get your credit card number. So, normally you are asked to send through a secure link, it is called the secure, you know it is a secure link I will call it just a secure link. And the vendor sends his public key to customer, in other words when they ask you to send the secure use the secure link effectively, he is also sending a, in some form his public key you might say.

(Refer Slide Time: 24:46)



Credit Card Transaction

4. Customer types his credit card number and purchase order.
5. Requests secure transaction.
6. System encrypts using vendor's public key.

13.4.7 Systems Analysis And Design © V.

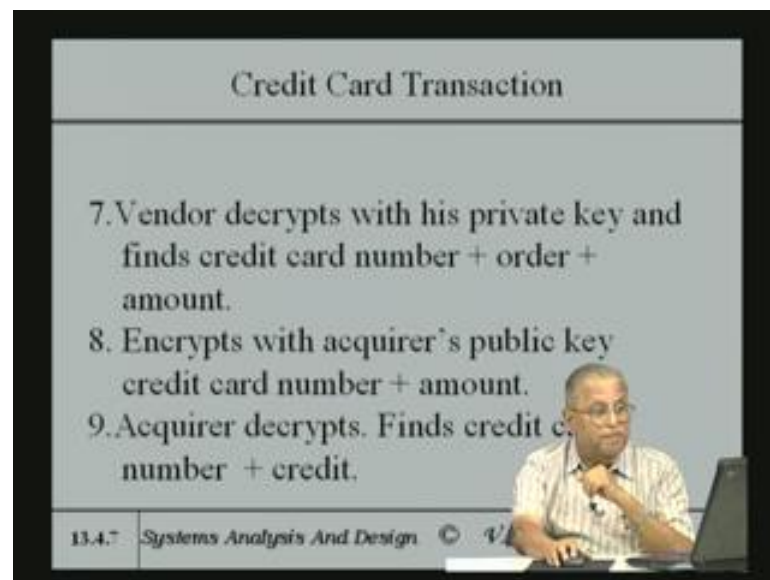
The slide is part of a presentation. In the bottom right corner, there is a small video inset showing a man with glasses and a striped shirt, likely the lecturer, sitting at a desk with a laptop.

Customer types his credit card number and purchase order, on the terminal requests secure transaction, secure transaction is requested system encrypts the vendors, the vendors public key, this transaction. In other words the credit card number in the transaction rather encrypted using the vendors public key, because you know the customer does not have either a private key or public key, he only has his web presence.

As I said the customer may be from a, you know one from a cyber cafe and he may not have his own personal computer at home. So, it is a question of, there is no question of any combination of public and private and so on at this stage, plus customers normally do not have a private and public key as of today. So, the merchant has a public key and a private key that is the minimum requirement as far as the vendor is concerned, in order to be able to e transaction.

He does not have that then of course; he is exposing the customer to the hacking and exposures credit card numbers. But, one would expect the vendor has some, when you say secure link, it is an encrypted link and system encrypts using vendors public key.

(Refer Slide Time: 26:15)



Credit Card Transaction

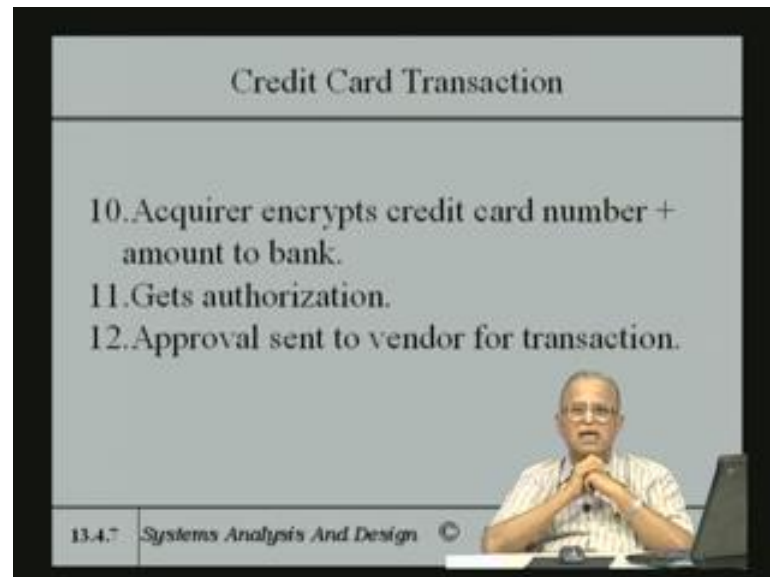
7. Vendor decrypts with his private key and finds credit card number + order + amount.
8. Encrypts with acquirer's public key credit card number + amount.
9. Acquirer decrypts. Finds credit card number + credit.

13.4.7 Systems Analysis And Design © V

Vendor decrypts with his private key and finds credit card number plus order, plus amount. So, the credit card number and what all was in ordered and the amount is found out per by the, because you can decrypt it. And once he gets that, he encrypts that with acquirers public key, the credit card number and an amount and this goes to the acquirer where by again secure link.

And acquirer will decrypt the using his private key and find the credit card number, plus the amount of order and will compare it with the credit, what is the credit which is there, finds the credit card number and the amount of order issued I should really say amount of order. And what were the credit requirement of the customer.

(Refer Slide Time: 27:17)



Acquirer encrypts credit card number and amount to the bank because acquirer does not know credit status of the particular customer, because it may be issuing bank something else. And the bank will authenticate and authorization provided the customers credit limit is okay. And the amount ordered is well within the credit limit and approval is in turn sent to a vendor for the transaction by the acquirer.

So, in other words if some sends its actually mimicking, the same steps which take place in manual thing, except that in this case it turns out the step about physical signature is not there physical signature of the customer is not there, the customers credit card number of course, is there and. So, the checking if it is you know stolen credit card and anybody masquerades as the customer uses the credit card number, showing credit card number on the internet the merchant has no way of really finding out, whether it is a stolen credit card or legal credit card.

It may not be a stolen credit card, it may be a credit card number hacked by somebody and of course, it is very important for the, in this case as you can see.

(Refer Slide Time: 28:47)

Credit Card Transaction

7. Vendor decrypts with his private key and finds credit card number + order + amount.
8. Encrypts with acquirer's public key credit card number + amount.
9. Acquirer decrypts. Finds credit card number + credit.

13.4.7 Systems Analysis And Design © V

The credit card number is available with the vendor and if he does not securely store it and stores it in some careless way in his database, because he has to store it at least temporarily till he gets the amount and normally of course, he also may have to store it for a longer period. In incase if there is a some kind of dispute later on and for dispute resolution, he has to have the credit card number the order and amount.

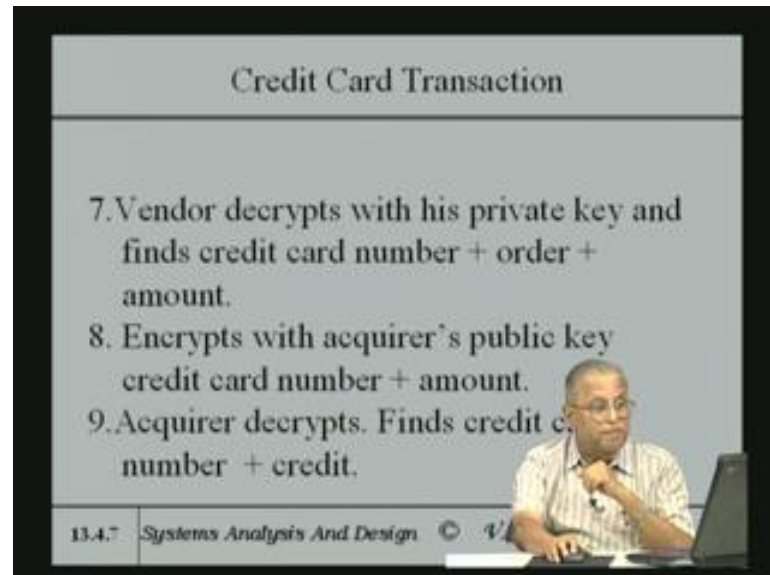
So, at least he knows when the credit card number is presented, what date it is presented, how much is ordered and what is the order for and how much is the amount charged all, these things may be required for a later reference. So, if suppose these are stored in some kind of a database without encryption by the vendor, he is exposing himself to hackers who can steal the credit card number from his database and use it for transactions.

In fact, these actually happened, this situation has happened in some companies abroad to the best to my knowledge, it is been reported in the news paper I mean reported in various magazines and. So, on and lot of people lost their credit card numbers, the result that number of different credit card companies had to reissue whole lot of credit cards. When they reissue a whole lot of credit cards, the huge amount of overhead which they had to take and, so they sued the vendor for having exposed all these credit card numbers.

In fact, in this particular case, the vendor went out of business because he could not pay to all the losses incurred by the credit card company and so on because of his

carelessness. So, it is still important to be able to because, normally credit card number need not be really known by the vendor.

(Refer Slide Time: 31:00)



Credit Card Transaction

7. Vendor decrypts with his private key and finds credit card number + order + amount.
8. Encrypts with acquirer's public key credit card number + amount.
9. Acquirer decrypts. Finds credit card number + credit.

13.4.7 Systems Analysis And Design © 1/1

So, there should not be any exposure by him, he should not really even know it, but it turns out as of now the way which goes on. So, those of you are interested about all types of this kinds of security labs, which is taking place and situation in real life where, lots of what I would say thefts have gone on internet and. So, on that is a magazine called communications of ACM, communications of ACM is ACM is association of computing machinery, USA.

And this particular journal comes every month and it is very interesting for all of you students to kind of, go through that journal because it has got a number of interesting case study and. So, one of information systems, which have been implemented and there are many of course, many other technical articles that appear in that and it is a very gives you a up to date information on what really goes on, in terms of the state of the art there are other interesting kind of articles like legally speaking and so on.

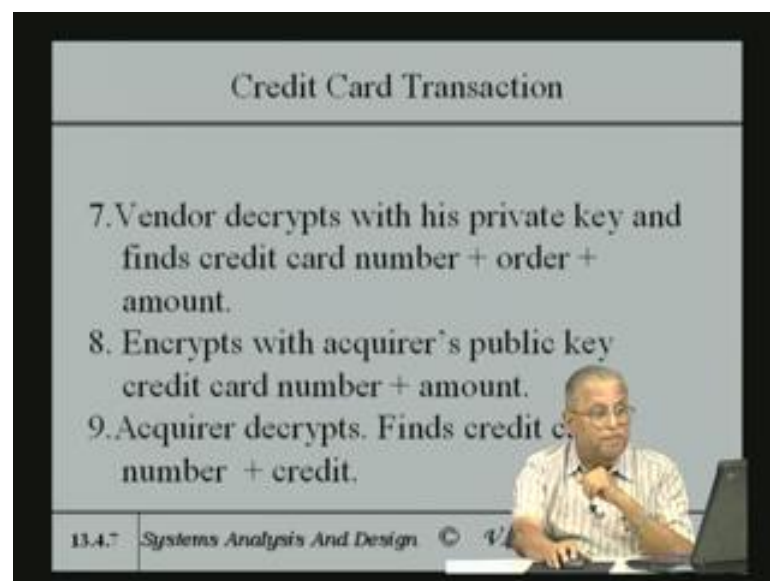
There is one column at the end of that every month issue, there is a one page called inside risks, inside risks is written by various people and they have written a many different situations or cases where, the stealing or security lapses took place on the internet. And because of that large amount of money was actually lost by some company

or the other primarily many of the money, which is lot of the money which is lost is by banking companies.

And they do not normally reveal it, because if they reveal the bank have been losing money by theft of course, it is not a good publicity for them, but by and large they will not give the name of the bank, but they will say that this kind of a situation occurred. So, the inside risks column is a very interesting kind of a column or a page to read, to kind of envier your doing anything related to security at least you know what are all loopholes, which the cleverer hackers seem to be using to kind of break whatever system you make.

So, it is interesting kind of a column where, number of these things have actually appeared and very interesting stories have appeared about situations where, credit card numbers were stolen. So, I would say the more or less the current method. But, so many people are not very much a, they are afraid of revealing the credit number on the net and, but then of course, there are depends on the person.

(Refer Slide Time: 34:07)



Credit Card Transaction

7. Vendor decrypts with his private key and finds credit card number + order + amount.
8. Encrypts with acquirer's public key credit card number + amount.
9. Acquirer decrypts. Finds credit card number + credit.

13.4.7 Systems Analysis And Design © VJ

There are people who take risks as long as the amount is not very large you do not mind, but then of course,, if you loose the credit card number, then that can be very, very bad because somebody can just go ahead and wipe out your entire credit limit and. So, one has to be somewhat worry about it. So, many people kind of try to say, but they will pay pay on delivery. And rather than revealing the credit card number and so on.

(Refer Slide Time: 34:39)

Credit Card Transaction

10. Acquirer encrypts credit card number + amount to bank.
11. Gets authorization.
12. Approval sent to vendor for transaction.

13.4.7 Systems Analysis And Design © V. Rajaraman 121 of 152

So, this is one situation which is currently there.

(Refer Slide Time: 34:41)

Credit Card In E-commerce

Main Problems

Main Problem is: if a merchant had only a web presence, a Customer needs to be reassured that the merchant is genuine.

1. Customers Signature cannot be physically verified. Customer needs electronic signature.

13.4.7 Systems Analysis And Design © V. Rajaraman 118 of 152

So, the main problems, which we have pointed out in the credit card transaction is the merchant see as I said merchant has only got a web presence. A customer needs to be reassured, the merchant are actually genuine because an e shop in internet. In a physical shop when you go to a shop you know the address and later on you have dispute with him, you can go to the address and then you can complain and. So, on and you have his

phone number and what not, in e shop the only thing you have is a URL, the web presence is the only thing.

So, he has to be reassured that the merchant is genuine and customer signature cannot be physically verified as I pointed out. And the customer needs electronic signature, if he really wants to have a secure transaction, equivalent of physical signature must be there in the electronic signature form. When we talked about signing, we talked about encryption, we talked about how transactions are signed on the internet, primarily signature means the customer has got a private key of his own.

So, signature implies a private key, a public key combination and which must be there with every customer and similarly every vendor and the public key should be verifiable and verification, normally takes place through the certification authority. So, certification authority, actually gives okay for the public key of the vendor then the verification authorities responsibility is to make sure the vendor who is an e shop is not a phantom vendor, that is he does really exists.

And he does have a legal he is, in fact a legal entity. And legal entity can means that he can be, if there is any kind of a dispute he can be sued in a court of law, all these things are implied by means of this public key certification, which is given by the certification agency. So, customer also requires the private public key.

(Refer Slide Time: 37:18)

The image shows a presentation slide with a black border. The slide content is as follows:

- Credit Card In E-commerce**
- Main Problems
- 3. Secrecy of credit card number has to be ensured.
- 4. Dispute settlement mechanism must be worked out.

In the bottom right corner of the slide, there is a small video inset showing a man with glasses and a striped shirt sitting at a desk with a laptop, appearing to be the lecturer.

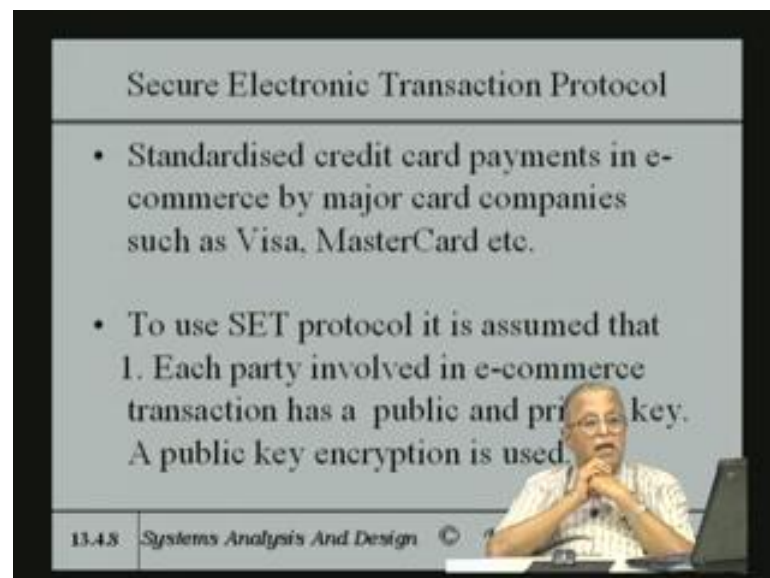
At the bottom left of the slide, the text '13.4.7 Systems Analysis And Design' is visible, followed by a copyright symbol and a logo.

Secrecy of credit card number has to be ensured that is as I said, if the vendor gets hold of the credit card number and he carelessly handles it, then you are exposing yourself to a risk. So, dispute settlement mechanism must be worked out, what is meant by dispute settlement is that suppose, you tell tomorrow that whatever I bought you never charged me or suppose whatever I bought is after all you buy without seeing the item because you order from internet.

So, the item has not been seen by you, if it is something like a ticket there is no question of quality of the ticket, but if you would say a sari which you bought or if you bought some other item like a dress then of course, the quality is important alright. So, there could be a dispute settlement problem, in other words he may he might say that I have revised (38:24) the quality is not the same when he supplied it.

So, then there could be a dispute. So, there should be a dispute settlement mechanism, which must be in place which both in terms of the amount charged versus the quality and. So, on you must have a freedom to return some item, which with which you are not satisfied and get reimbursement for the items returned. So, all these things are implied by the dispute settlement mechanism.

(Refer Slide Time: 38:57)



The image shows a video frame of a presentation. The main content is a slide titled "Secure Electronic Transaction Protocol". The slide lists two bullet points: "Standardised credit card payments in e-commerce by major card companies such as Visa, MasterCard etc." and "To use SET protocol it is assumed that 1. Each party involved in e-commerce transaction has a public and private key. A public key encryption is used." In the bottom right corner of the video frame, a man is visible, sitting at a desk with a laptop, appearing to be the presenter. The bottom of the slide has a footer that reads "13.4.8 Systems Analysis And Design".

Say there is something called as secure electronic transaction protocol, which is really being standardized only recently, may be a couple of years ago. And it has been standardized by cooperation between several credit card companies, many companies

like VISA MASTER Cards American Express and so on. So, all these different card companies got together and said that they need a standard, which is accepted used by everybody and it is called secure electronic transaction protocol.

And as usual the abbreviation is SET protocol, s for secure, e for electronic, t for transaction, SET protocol or SET protocol it is assumed that in that all can be able to apply this protocol. It is assumed that each party involved in e commerce transaction has a public and a private key. And; that means, every customer and every vendor has a private key public key pair and this is you might say, you must ask particularly the customers see vendor of course, there are not that many vendors, but customers can be millions of customers.

So, to expect every customer to have a private key is a really too much, but then I think that is, it is the protocol really expects that and may be. If you are continuously transacting on the internet and you are making large purchases, on the internet large amounts and then you may be it is then if you want to use SET protocol, it would be very advisable from your own safety point of view to use this protocol because its lot more secure than the protocol which I talked about earlier.

So, even though the protocol requires this and also a protocol itself is very complicated, it is as I said it is not for everybody that is going to use a SET protocol, it is for customers who make very large transactions, see and also very large number of transaction. So, I do not really know many would really come to effect, in general see it may be long, but it is interesting the way in which the SET protocol has been approached because the points, which I make are very important to remember.

(Refer Slide Time: 41:49)

Secure Electronic Transaction Protocol

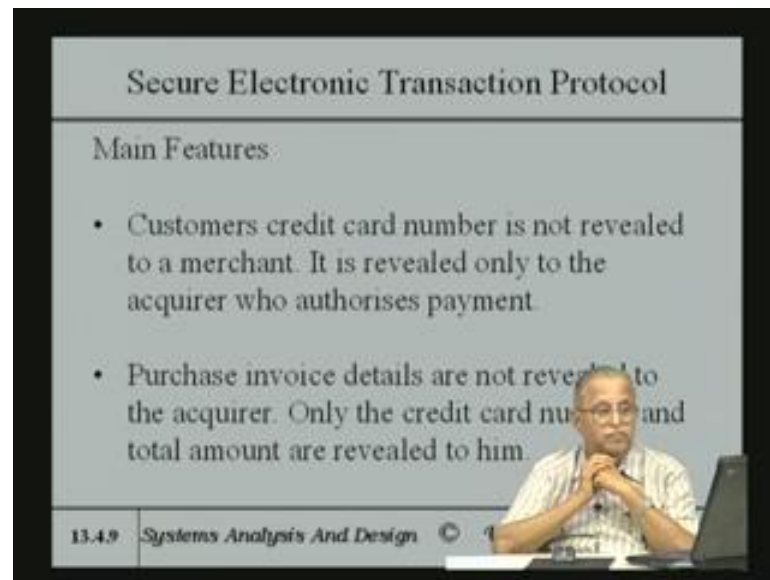
2. All parties have their public keys certified.
3. A standard hashing algorithm is used to create message digest for signature verification.

13.4.8 Systems Analysis And Design © V. Rajuraman 125 of 152

So, all parties must have their private public key certified, including the customer he must have his public key certified. So, that he is of actually physical entity with a certain public key is known to the vendor also see. So, vendor also transacting business with a not a phantom customer, who will disappear tomorrow, but with a customer who is actually has got a physical presence also. So, that is what is important as for as the reason for public certification of customers public key also.

A standard hashing algorithm is used, to create a signature actual digital signature requires hashing, which I pointed out that is message digest. And we talked about the MD 5 product from RSA, which does a hashing. And it is really very reasonably good hashing function, so that two distinct documents will have to do two distinct digest and the digest will authenticate the original document and. So, standard hashing algorithm is used to create message digest for signature verification. So, as I said MD 5 is currently one of the standards which is used.

(Refer Slide Time: 43:09)



Secure Electronic Transaction Protocol

Main Features

- Customers credit card number is not revealed to a merchant. It is revealed only to the acquirer who authorises payment.
- Purchase invoice details are not revealed to the acquirer. Only the credit card number and total amount are revealed to him.

13.4.9 Systems Analysis And Design

The main features of secure electronic transaction protocol is that customers credit card number is not revealed to the merchant, merchant does not have to know the credit card number of the customer, he needs to only know, what the customer wants to purchase. The items he wants to purchase and of course, the total amount he is going to charge, only these two are required, he does not require the number, whereas the customer credit card number is required by the acquirer to be able to check with the bank whether, the credit limit is or not.

And so purchase invoice details are not revealed to the acquirer, the bank or the acquirer did not know, what the person has bought for this he paid through credit card, he only has to know the amount for which the payment has been made, amount and the credit card number. Then what is you know, you might say it is a privacy concern, as far as the because what I mean by privacy concern is that if an acquirer knows exactly what all I am purchasing every month and how much I am incurring for those purchases then it can be used in ways, which is not very desirable let me take an example what I mean by this.

Suppose, you on purchasing a lot of jewelry and the acquirer knows that you are buying a lot of jewelry, at a far amount of high cash and. So, on he can really make that information is made known to many jewelry shops, you end up with getting a whole lot of spam messages, advertising their ware and stuff like that. And even though it is not ethically correct, it may many of the acquirer may be selling this information in order to

be able to you know and also get commission on that, this is been a continuous what I would say privacy issues, which are involved with this many of the western countries have privacy laws.

If the person comes and makes reveals this for even payment or no payment, he is liable to be prosecuted so, but I think many places it really lacks these rules are very lacks. So, that is the reason why, one should not make the acquirer know what he has purchased, of course, the shop must know what he is purchasing because one expects the shop will not reveal, it does not know the credit card number.

So, it will not, it cannot reveal who bought what it only knows somebody bought this much because credit card number uniquely identifies the person. So, the credit card number, the amount and what was purchase is available then you can actually track down see. So, this is where I think the whole point comes in that is, anonymity is preserved by the protocol.

So, the anonymity because the shop keeper knows only what you are buying and how much it is, he does not know what is your credit card number is, the acquirer will know only your credit card number and how much is the amount, what you purchased he does not know. So, this is very important because that is primarily what SET protocol achieves.

(Refer Slide Time: 46:44)

Secure Electronic Transaction Protocol

- Purchase invoice + credit card number is digitally signed by the customer. In case of a dispute an arbitrator can use this to settle the dispute.
(Computer protocol runs to 262 pages and may be found in www.ibm.com/redbook/SG244978)

13.4.9 Systems Analysis And Design © V. Rajaraman 127 of 152

Purchase invoice plus credit card number is digitally signed by a customer. So, the entire invoice and credit card number is signed by a customer using a digital signature in order to sign, I said that it requires private key. So, private key, customer will have a private key he will use the private key to sign it. So, in case of disputes an arbiter can use this signature to settle the dispute that is I ordered these items, but I was not supplied all these items and so on.

Then, you can have dispute settlement mechanism because the signed purchase order is there, both with the acquirer and with the vendor. Both will have it that is what we will see in the SET protocol. In actual protocol is very complicated and it runs 262 pages and found all not read it (47:42)the entire protocol because it goes into all kinds of programs and so on. But, those of you are interested can look at the website of ibm.

(Refer Slide Time: 47:54)

Secure Electronic Transaction Protocol

- Purchase invoice + credit card number is digitally signed by the customer. In case of a dispute an arbitrator can use this to settle the dispute.
(Computer protocol runs to 262 pages and may be found in www.ibm.com/redbook/SG244978)

13.4.9 Systems Analysis And Design © V. Rajaraman 127 of 152

ibm dot com red book slash s g 244978 some number, s g that is the document number where the entire protocol will be found and may be if you are going to implement it later on in your life, when you work for a company dealing with this kind of a financial issues, you may find this reference useful. In any case, you can go to the ibm website and find out and ask the question I want to find out about the secure electronic transaction protocol and you could get it. But, these words of course, many codes will not be given, but I think this book has got some code also given and that will be useful.

So, the dual, see the cricks of the SET protocol is what is known as a dual signature scheme.

(Refer Slide Time: 48:53)

The slide is titled "Secure Electronic Transaction Protocol". Below the title, it says "DUAL SIGNATURE SCHEME". A bullet point states: "Dual signature scheme is an innovation in SET protocol." Below this, it says "Steps followed in the protocol are:" followed by a numbered list: "1. Customer purchase information has 3 parts". This is followed by three sub-points: "(i) Purchase Order (PO)", "(ii) Credit Card Number(CCN)", and "(iii) Amount to be paid". At the bottom of the slide, there is a footer bar with the text "13.4.10 Systems Analysis And Design © V. Rajaraman" on the left and "128 of 152" on the right.

Dual signature scheme is an innovation of the SET protocol and the steps there are number of steps followed by the protocol, let me explain one by one. And I will go then go to the block diagram of the entire transaction, how it take place and then recapitulate what all went on, because it is a very, why I said it is a very complex set of things which happen. And it is not really all that simple, like the earlier protocol I talked about this protocol is little bit more complicated.

Now, the steps followed by this protocol is first of all is customers purchase information has three different parts, one is the purchase order, where all the items are mentioned and the credit card number and the amount to be paid. In fact, the amount to be paid in each purchase item there will be an amount and the total amount will be the total amount to be paid. So, these are three parts, which are there in every purchase order by a customer.

(Refer Slide Time: 50:12)

Secure Electronic Transaction Protocol

2. Merchant should know $(PO + \text{Amount}) = POA$.
3. Acquirer should know $(CCN + \text{Amount}) = CCA$.

13.4.10 Systems Analysis And Design

The purchase should have the purchase order plus the amount, it need not know the credit card number, the acquirer should know the credit card number plus the amount. So, that is called the purchase order plus amount as POA that is purchase order plus amount POA and the credit card number plus amount as CCA, I will give just abbreviation in order to avoid using the long thing every time and POA is purchase order amount and CCA is the credit card and amount.

(Refer Slide Time: 50:47)

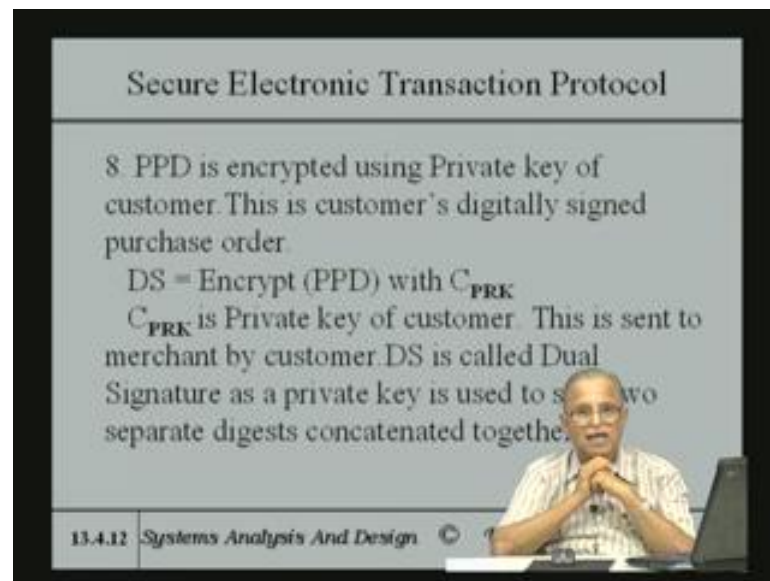
Secure Electronic Transaction Protocol

4. Hash POA using standard Hash algorithm such as RSA's MD5. Call it POD.
5. Hash CCA using MD5. Call it CCD.
6. Concatenate POD and CCD. Call it $(POD || CCD)$.
7. Hash $(POD || CCD)$ giving PPD.

13.4.11 Systems Analysis And Design

Hash POA, the purchase order amount with standard hash algorithm and call it POD the hashing is done primarily for the signature point of view. Hash CCA using MD5 that is the CCA is also along the customer has got that see and calls it CCD, concatenate POD and CCD and call it PPD. What I mean by concatenation is that the two are stuck together you might say, these two are strings of bits and these are concatenated hash this concatenated stuff giving something called PPD all of them using same hashing algorithm.

(Refer Slide Time: 51:35)



The slide is titled "Secure Electronic Transaction Protocol". It lists step 8: "PPD is encrypted using Private key of customer. This is customer's digitally signed purchase order." Below this, it provides the formula $DS = \text{Encrypt}(PPD) \text{ with } C_{PRK}$ and explains that C_{PRK} is the private key of the customer, which is sent to the merchant. It also states that DS is called a Dual Signature because a private key is used to sign two separate digests concatenated together. A presenter is visible in the bottom right corner of the slide frame.

Secure Electronic Transaction Protocol

8. PPD is encrypted using Private key of customer. This is customer's digitally signed purchase order.

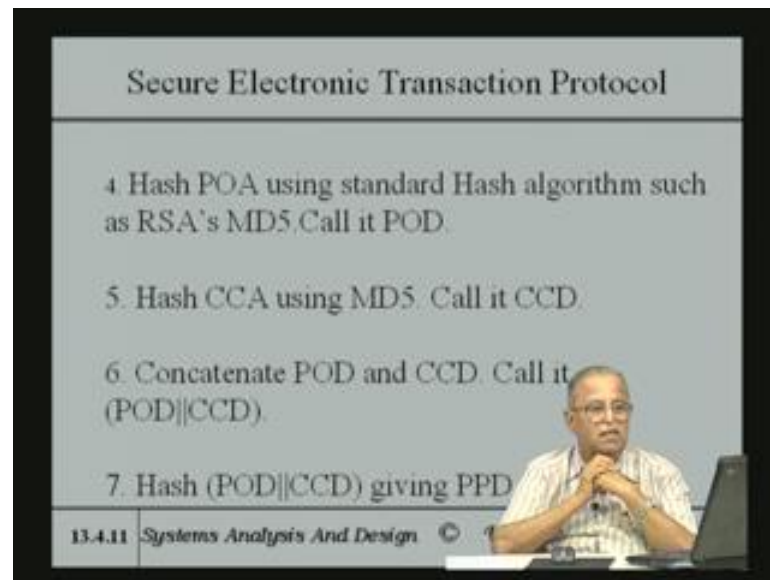
$DS = \text{Encrypt}(PPD) \text{ with } C_{PRK}$

C_{PRK} is Private key of customer. This is sent to merchant by customer. DS is called Dual Signature as a private key is used to sign two separate digests concatenated together.

13.4.12 Systems Analysis And Design

And then PPD is encrypted using the private key of the customer that is signature, as I as we pointed out the signature is the hashing is actually signed; this is customers digitally signed purchase order. So, digital signature will encrypt PPD, encrypted with the private key that is PRK that is private key of the customer. And this is sent to the merchant of the customer, DS is called dual signature as a private key is used to sign two separate digests concatenated together.

(Refer Slide Time: 52:17)



Secure Electronic Transaction Protocol

4. Hash POA using standard Hash algorithm such as RSA's MD5. Call it POD.
5. Hash CCA using MD5. Call it CCD.
6. Concatenate POD and CCD. Call it (POD||CCD).
7. Hash (POD||CCD) giving PPD

13.4.11 Systems Analysis And Design

See you can see here, PPD see we take POA as one and we set CCA as the other. And then both are hashed and then POD is hashed POA and CCD is hashed CCA and now the two hash once concatenated is called PPD. So, in other words all the information, which is contained in CCA and POA CCA together signed is you know, before signing actually digests of both POA and which is actually POD and CCA which is CCD are both concatenated and hashed together.

So, PPD essentially you might say is that is the reason it is called dual signature because I have got two different items, which are being hashed.

(Refer Slide Time: 53:14)

Secure Electronic Transaction Protocol

8. PPD is encrypted using Private key of customer. This is customer's digitally signed purchase order.

$DS = \text{Encrypt (PPD) with } C_{PRK}$

C_{PRK} is Private key of customer. This is sent to merchant by customer. DS is called Dual Signature as a private key is used to sign two separate digests concatenated together.

13.4.12 Systems Analysis And Design © V. Rajaraman

Hashed and then encrypted and this dual signature is the one which is used for later on dispute resolution and so, on.

(Refer Slide Time: 53:26)

Secure Electronic Transaction Protocol

9. POA separately encrypted by customer using merchant's public key and sent to merchant.

10. Merchant decrypts it using his private key. He thus gets Purchase order + Amount.

13.4.12 Systems Analysis And Design © V. Rajaraman 132 of 152

POA is separately encrypted by customer using merchants public key and sent to the merchant because the purchase order and amount, when you strip purchase order amount and credit card number, the purchase order and amount is encrypted because and sent to by public key of the vendor, and of course, if customer must have a certification of that vendor.

And in certification, it is actually public key is used, normally what is supposed to be done is that when you log on to a merchant you using his URL you ask for his public key certification. And he is suppose to send it back to you, when he send sends it back to you then you the authentication then you can probably note down the number or whatever is given with that. And that will give you the idea about the actual legal entity that is he is a legal entity and this is and of course, the public key is known and use the public key to separately encrypt.

(Refer Slide Time: 54:33)

The slide is titled "Secure Electronic Transaction Protocol". It contains two numbered steps:

- 9. POA separately encrypted by customer using merchant's public key and sent to merchant.
- 10. Merchant decrypts it using his private key. He thus gets Purchase order + Amount.

At the bottom of the slide, there is a footer bar with the following text: "13.4.12 Systems Analysis And Design © V. Rajaraman 132 of 152".

The POA that is purchase order plus amount is encrypted by the public key of the merchant. And merchant can now decrypt it using his private key and he gets the purchase order plus amount.

(Refer Slide Time: 54:45)

The slide is titled "Secure Electronic Transaction Protocol". It contains two numbered steps:

- 11. CCD and DS also sent to merchant. From CCD merchant cannot find CCN.
- 12. Merchant can decrypt DS using customer's public key and get PPD. Customer must have a certified public key for verification.

At the bottom of the slide, there is a footer with the text: "13.4.12 Systems Analysis And Design © V. Rajaraman 133 of 152".

CCD and dual signature as well as the concatenated thing that is sent to the merchant, merchant cannot find CCN from this, credit card number cannot be found by him. Merchant can decrypt DS using customers public key and get PPD, PPD is the one which is used as a (55:09) digest because this digest will concatenate with the two parts. So, he can actually verify this, but individual things they cannot verify.

Customer must have certified public key for verification of course, in order to be able to you know DS in order to kind of authenticate the signature, the public key must be certified.

(Refer Slide Time: 55:32)

The slide is titled "Secure Electronic Transaction Protocol". It contains two numbered steps:

- 13. Merchant can compute $H(POD||CCD)$. If $H(POD||CCD)=PPD$, then customer's signature is OK.
- 14. Merchant forwards to acquirer CCA, POD, DS each separately encrypted using acquirer's public key.

At the bottom of the slide, there is a footer with the text: "13.4.13 Systems Analysis And Design © V. Rajaraman 134 of 152".

Merchant can compute hash of POD and CCD and hash of POD and CCD is PPD then customers signature is okay. In other words, he can find out the hash independently because he has got the purchase order and the hashed CCD, these two can he can concatenate himself and then find PPD and by with this customers signature could be found out, merchant forwards the acquirer CCA POD and DS each separately encrypted using acquirers public key.

So, digital signature will also be sent because as for as the customer is concerned, he does not know anything about the acquirer, he only deals with the vendor, the vendor has got all these three. And now the let us just CCA is credit card number plus amount and you might say concatenated in other words, if you kind of we saw that earlier.

(Refer Slide Time: 56:56)

Secure Electronic Transaction Protocol		
<p>2. Merchant should know $(PO + Amount) = POA$.</p> <p>3. Acquirer should know $(CCN + Amount) = CCA$.</p>		
13.4.10	Systems Analysis And Design © V. Rajaraman	129 of 152

CCA the acquirer should really know because he has already striped this and it is actually not available to the merchant. So, the secrecy is maintained.

(Refer Slide Time: 57:04)

Secure Electronic Transaction Protocol		
<p>13. Merchant can compute $H(POD CCD)$ If $H(POD CCD) = PFD$, then customer's signature is OK.</p> <p>14. Merchant forwards to acquirer CCA, POD, DS each separately encrypted using acquirer's public key</p>		
13.4.13	Systems Analysis And Design © V. Rajaraman	134 of 152

The merchant forwards the acquirer CCA, POD, DS each separately encrypted using acquirers public key.

(Refer Slide Time: 57:12)

Secure Electronic Transaction Protocol

15. Acquirer's forwards to bank.

16. Bank finds CCN and Amount. Verifies balance amount. Bank also verifies customer's digital signature using CCD, POD and DS. If all OK acquirer is informed.

13.4.14 Systems Analysis And Design © V. Rajaraman 135 of 152

Acquirer forwards it to a bank of course, in turn bank finds CCN and amount verifies its amount bank, also verifies customers digital signature using CCD, POD and DS, if all acquirer is informed by the bank.

(Refer Slide Time: 57:31)

Secure Electronic Transaction Protocol

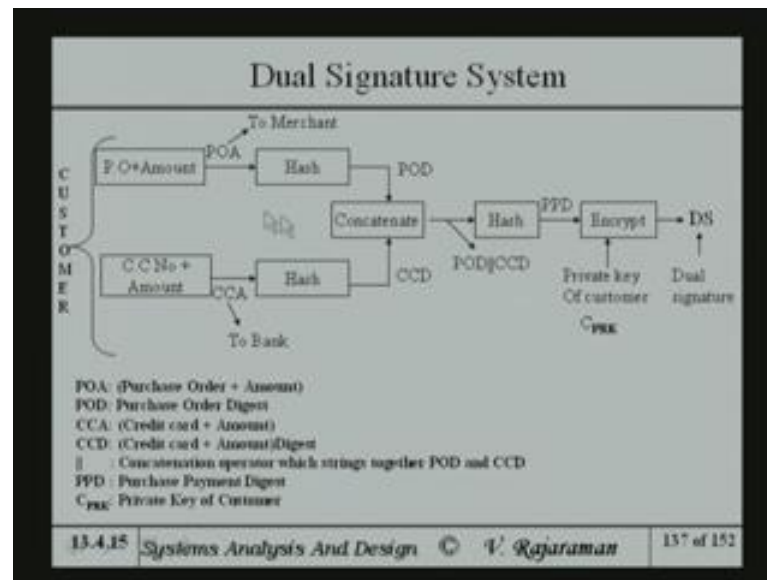
17. Acquirer OK's transaction to merchant.

18. Merchant supplies item. Gets payment from acquirer. Bank collects from customer.

13.4.14 Systems Analysis And Design © V. Rajaraman 136 of 152

And now the transaction Acquirer OK's transaction to the merchant. Merchant supplies item gets payment from acquirer. Bank collects from customer as usual as usual thing.

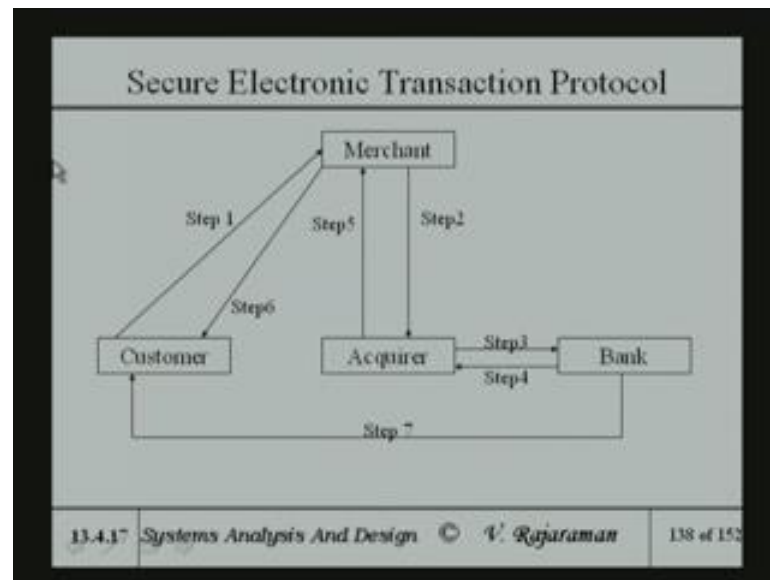
(Refer Slide Time: 57:39)



So, let us just look at what is really happening here with this kind of a. Customer is breaking up purchase order plus amount and credit card number plus amount, he hashes that gets POD and hashes this gets CCD and concatenates POD and CCD thus again hashed and PPD comes, it is encrypted with private key and the dual signature comes this is how the dual signature is generated.

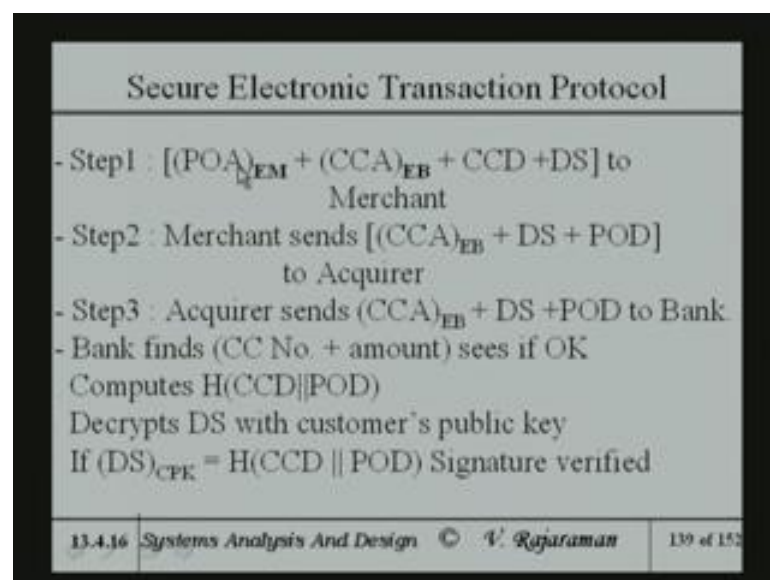
So, POA is purchase order plus amount, purchase order digest, credit card plus amount, credit card plus amount digest and concatenation and PPD is purchase per payment digest and private key of customer that is what is been encrypted that is dual signature.

(Refer Slide Time: 58:33)



So, the steps are of course, customer sends to the merchant all this usual, the merchant sends to the acquirer, the acquirer sends to bank, bank gets back to acquirer, acquirer now okays to merchant, merchant supplies the goods and then the customer gets the you know bill from the customer. And of course, the acquirer will get also from the bank the amount, which is to be collectable and he will pay in turn the customer.

(Refer Slide Time: 59:07)



So, step one is POA is encrypted with the merchants public key, CCA encrypted with banks public key and CCD plus DS is sent to the bank to the merchant. CCA encrypted

see the point I want to make again is that CCA is not sent as it is its encrypted by the banks public key, which cannot be decrypted by the vendor. See, only the bank knows it is private key to be able to kind of decrypt this.

But, he has got this, in order to be able to prove his later on dispute resolution and digital signature of course, is there. Merchant sends CCA plus DS plus POD to the acquirer, acquirer sends CCA and so on. I think I will probably repeat this next time, because I went through little fast and these are the steps, which are important to remember and so. I will repeat this next time and we will look at this transaction using that little block diagram and explain this in better detail. So, we will see you the next time.