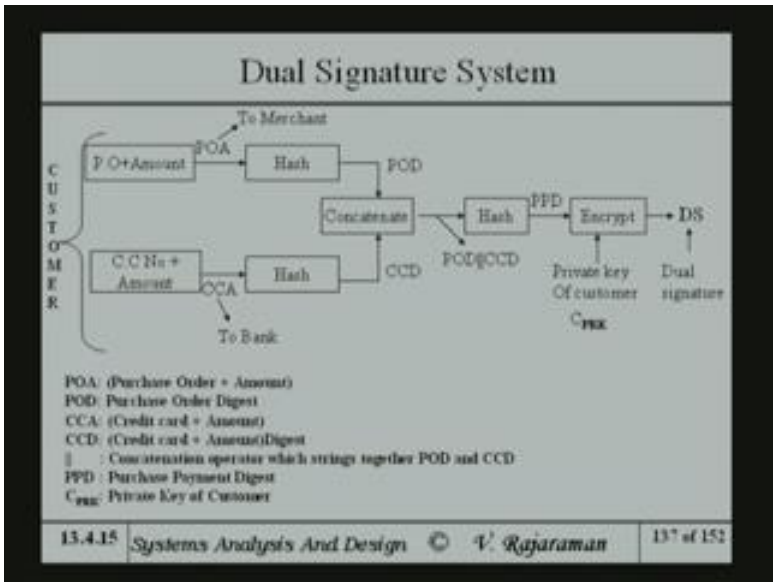
System Analysis and Design
Prof. V Rajaraman
Department of Super Computer Education & Research
Indian Institute of Science., Bangalore

Lecture - 38

The intricacies of the dual signature system, which is currently being standardized for credit card payments as I pointed out, this is not yet entirely used everywhere. But, it is expected that it will be used soon. So, I am given you an idea of what this standard, which is going to be adopted all over the world is going to be and that is dependent on what is called as a dual signature.

(Refer Slide Time: 01:46)



The primary purpose of the dual signature is as I pointed out that as far as the vendor, with whom an order has been placed, is concerned. There is no need for him to know the credit card number. He has to know only what is being purchased and what is the amount of purchase. Similarly, the acquirer need not know the actual items you have purchased. He needs to know only the credit card number and the total amount, which is got to be paid by the customer.

So, that we can check whether the credit card number is a legal number. And while, the credit card owner has an enough balance to be able to pay that amount of money, which is given in the purchase order. So, the whole idea of this system is to make it such that the, purchaser as I as to of course, put the credit card number, plus the purchase order

plus, which consists of two parts namely, the items we purchased and the amount of the total order. So, that is got to be split into two parts.

So, when the customer gives this in his computer the two parts are split. One is the purchase amount plus purchase order plus amount that is what are all the items he is going to purchase. Plus the amount and the credit card number and the amount. These two are two separate entities, which are sent to different people. But, there is need for both of them to available together for dispute resolution.

In other words, tomorrow there is a dispute by the customer saying that he did not really order these items. But, he has been charged then there must be some proof saying that he did order those items. And that is the reason why, that there is a need for this in some encrypted form to be available with the acquirer. So, that any kind of a dispute settlement can take place. Same way it is also got to be available in encrypted form which of course, cannot be read by the vendor to be with him. So, that is whole idea.

Now, the purchase order plus amount is hashed with some kind of a hashing function, which we said was a MD 5. Or an essentially it is an abstract of the order, by good hashing algorithm, which is unique and which is also standard algorithm. So, it is agreed on standard algorithm between all concerns in this electronic commerce. And so he hashes this because the signature really normally consists of the hashes, which are encrypted by private key of the customer.

So, that is the reason why it is hashed and from POD, the POD goes to the hands of the acquirer from this he cannot find out what is the exact items purchased. Because it is a hash it is already been kind of abstracted. And it is another binary string, which is of course; there is one to one correspondence between this and this. But, you cannot go backwards from POD to POA. In other words this forward you do hashing. But, you do not have a backward hash which is available.

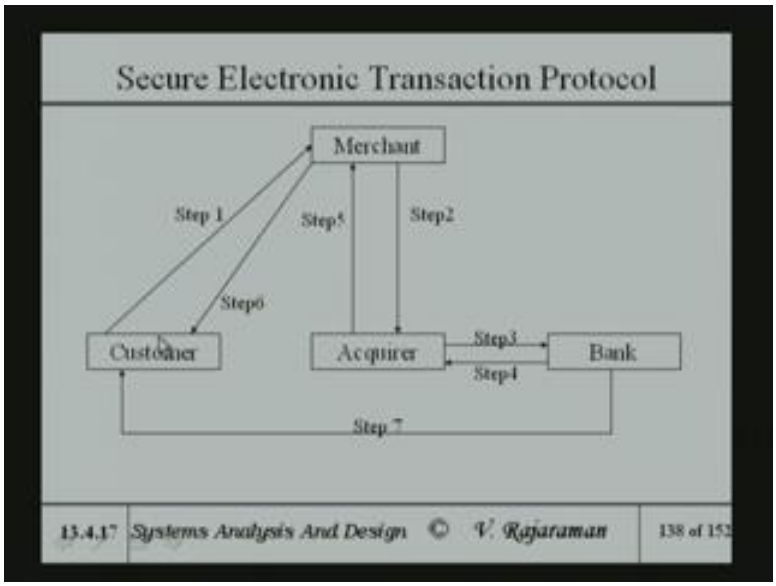
So, similarly the credit card number and the amount is hashed and CCD comes out of this hashing function. So, got to go to the bank, this is got to go to the merchant. Any how these two are essentially concatenated that means, they are put in, if they are binary strings this string. And these strings are joined together that is what is known as concatenation. And the symbol which is used for concatenation is a parallel double line.

So, POD is concatenated with CCD and again hashed to give a PPD and this PPD. The reason why it is concatenated and again hashed is that the PPD effectively contains this information, POA information as well as CCA information. So, PPD is the one which really will bind the customer with the entire order, because here is actually the order has been split into two parts.

So, the entire order essentially the information is contained in this, that is encrypted by the private key of the customer and this is called the dual signature. And this dual signature is the one which is verified by the acquirer, before he how can he verify it, what he can do is of course, he will have the public key of the customer. So, from that he can get hold of PPD. And if he has got PPD available with him then of course, he knows that, that could have come only from the customer because, it is signed by his private key.

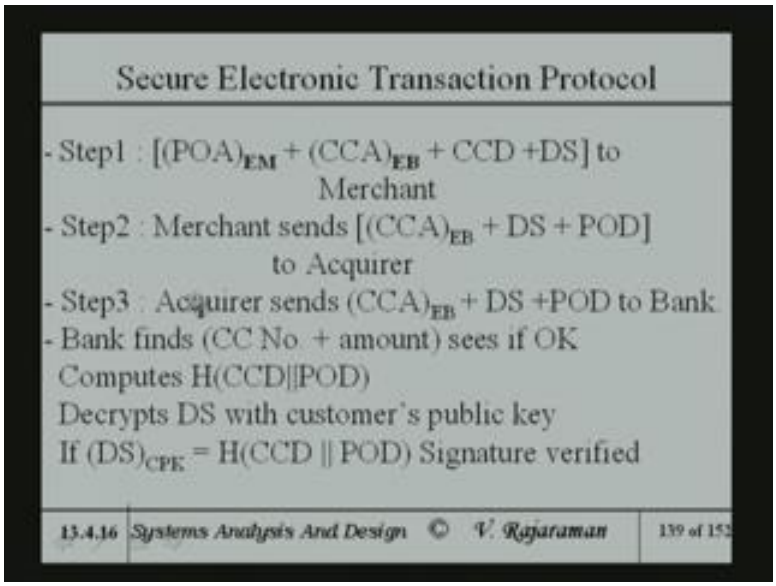
The customers public key is of course, is available with both the acquirer and the merchant or the vendor, whatever you might call. So, I am essentially calling POA as purchase order plus amount and purchase order digest, this is actual hash function is called a digest. And credit card amount and credit card digest and concatenated the values POD, CCD, PPD and then this is the private key.

(Refer Slide Time: 08:04)



Now, the steps are, let us just go through the steps first.

(Refer Slide Time: 08:06)



So, the purchase order amount and amount is encrypted by the public key of the merchant, merchants public key and sent to the merchant. The reason why it is encrypted because I am going to send it through internet and it is got to be encrypted. So, that no hacker gets hold of it and the merchant of course, can decrypt it using his private key and get the purchase order and the amount.

And the credit card number and the amount is encrypted by the acquirers public key or you might say the banks public key. Bank I am essentially assuming the bank and acquire are somewhat same you know the in this context does not really matter. The acquirer is also a bank, but of course, is not the same bank as it issued the credit card to the customer.

So, this is encrypted by the acquirers public key and this and these of course, can be decrypted by the acquirer by using his private key. And he will get the credit card number and the amount separately from that. And because he knows what are the, you know he really check the credit card number and he look at the amount. And see whether it is within the credit limits of the customer. Along with that the digital signature is also sent to him and then the CCD is the digest of CCA that is also sent to him.

So, these are all sent to the merchant, because the merchant will have this available to him, he cannot decrypt it. Because it is encrypted with the acquirers public key and his private key is not available with the merchant. But, then this is only for legal purposes

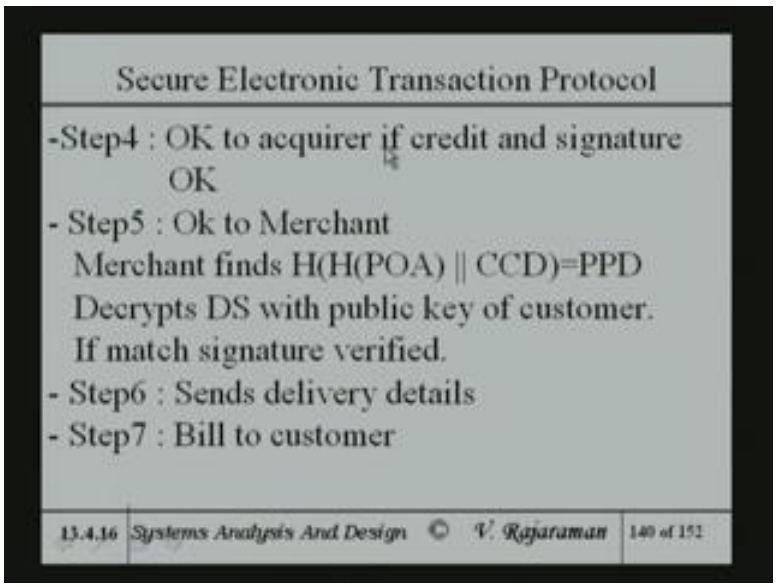
later on to see, that this is what any anyhow this is what he is going to forward to the acquirer. And also for legal purposes that it is actually came to him and anybody can the bank can definitely decrypt it.

The merchant sends the CCA encrypted and digital signature and the POD that is the purchase order digest to the acquirer, purchase order digest is this one, which is digested. That is in other words; hashed acquirer sends CCA that is you know one way you look at this acquirer sends the whole thing as it is to the bank. And the bank decrypts it, finds out the credit card number and amount see, whether it is computes the hash because the CCA, CCD which it has got and the POD.

So, this hash will give the idea for dispute resolution, decrypts DS's customers public key and finds out whether these two are equal. If these two are equal; that means, it is actually a signed one. Now, CCD of course, is available with the, you know CCD has been sent to the bank by the. Because, once the once the CCA is sent the digest can be found out to get this CCD and then POD has been sent.

So, CCD can concatenate with POD can always be found. So, this way you can hash it because hashing algorithm is a standard MD 5 algorithm and. So, you can compare the hashed function with this and they two match you know that it is a correctly signed copy.

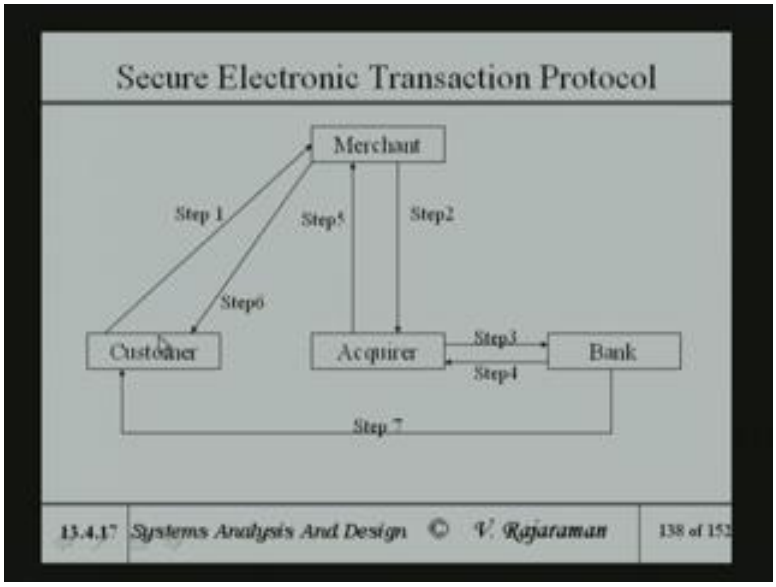
(Refer Slide Time: 12:05)



So, to acquirer and credit the signature or okayed to merchant if the credit is there because actually a bank tells the acquirer, the acquirer in turn tells the merchant. Merchant finds the hash this POD that is the POD concatenated to CCD hashes this finds PPD decrypts DS with public key of customer. And matches whether, this and that DS is verified match then if the signature matches here also then of course, he will send the delivery details and bill to customer.

Because double check, which is taking place one is the check by the bank whether it is properly signed and also merchants signature whether, it is properly signed. It is a kind of a dual kind of signature verification because both of them have to be convinced that it is properly signed because later on, there should not be a dispute between the merchant and the bank and the acquirer. So, this is the whole. So, there are seven steps in this process and this is the seven steps, which I have shown in this picture here.

(Refer Slide Time: 13:21)



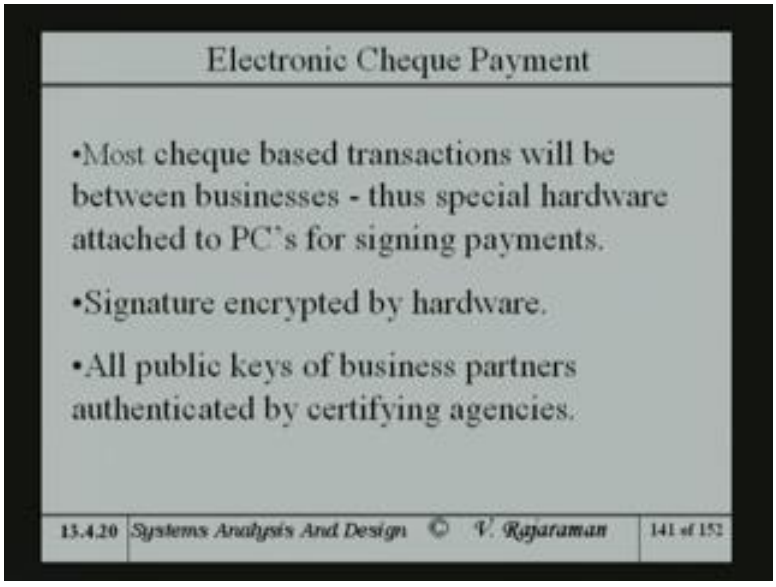
This is the customer sending the purchase order which is striped and then this is, then goes to the acquirer. Acquirer sends to bank, bank checks some Okays payment and this informed to the merchant. And merchant checks the signature and sends it to the customer and ultimately of course, the bank will send the customer a full bill at the end of each month, This, is essentially the method which is used for the dual signature method, which is used for credit card payment.

So, we said that there are four payment methods, one is the credit card payment, the other is the cheque payment, the third one is a small amounts in terms of information goods like, few pages of an article or a music track and things like that. And lastly of course, cash payment, cash payment is the most challenging of the all. So, let us now let us look at the cheque payment.

Cheque payment is normally the one used in b to b e commerce. Because normally business to businesses when, they become partners in e commerce, the two businesses will have a trusted relationship with one another. And because they are businesses, they normally have to essentially pay through cheques, which is legally required particularly if the amount is above a certain value. By and large in b to b commerce, the amounts are fairly large they are not small amounts like 100 rupees or 200 hundred rupees, it is normally much larger.

And of course, credit cards could also be used. But, normally they are not used for very large amounts. And it will use a small amount, but then credit card when you issue it to a bank there is always a question of, who is the authorized person to use it and so on, so what so. But, cheque also there will be some kind of an authorized person to issue the cheque. And that is essentially the most common means of transacting business to business e commerce that is the primary method payment.

(Refer Slide Time: 16:00)

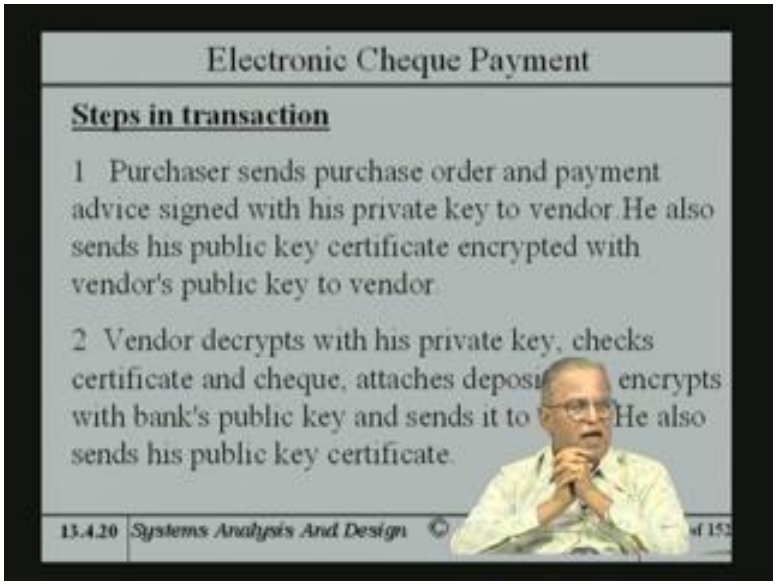


Most cheque based transactions will be as I said between businesses, some very often a special hardware is attached to PC to sign those payments. Of course, again you will be using the public key private key pair. And it could effectively be done by software running in the computer or because if, you are paying a large number of transactions or e transactions and large number of cheques are being paid. Then it may be more economical and faster to have some kind of a hardware means of signing.

And this hardware means, of signing also can be kind of controlled. In other words, not everybody can essentially have the authority to send a cheque. So, the hardware will be with the person who is authorized to send cheques and so on. So, normally signature is encrypted by the hardware. So, the encryption of the signature using the private key of the authorized person, the private key would be possibly stored in the hardware device. And that is the one, which effectively will do the, it is a special purpose you might say small computer to do that.

All public keys of business partners authenticated by certification agent, certifying agencies as I pointed out certifying agencies are necessary to be able to make sure that businesses do exists. Of course, the two businesses decide to kind of become partners in e commerce then they both exchange the digital certificates and. So, they convince one another of their legal presence, before they transact business of huge amounts and so, on.

(Refer Slide Time: 18:05)

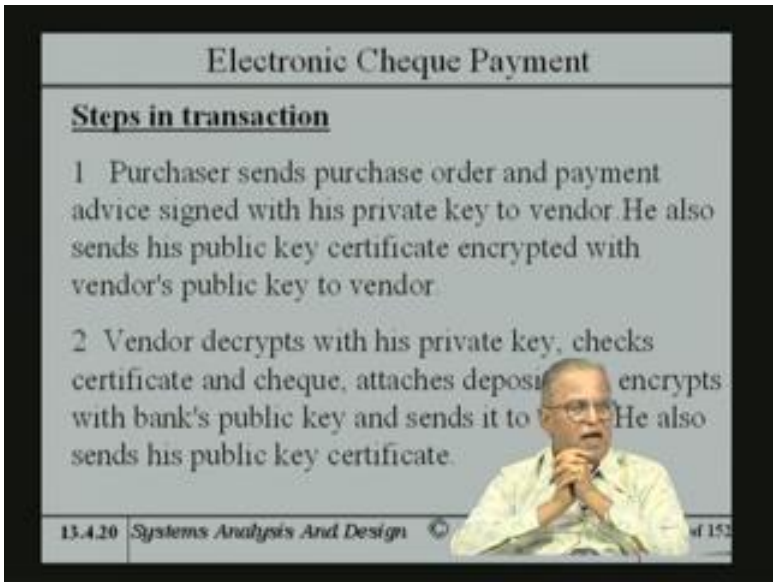


So, the purchaser sends the purchase order and payment advice signed with his private key to the vendor. He also sends his public key certificate encrypted with vendors public key to the vendor, as usual. That is the private key is actually, signed purchase order and the public key certificate is sent. So, that when the vendor decrypts with the public key. If it is a legal public key and belongs to this particular person then he can get back, the purchase order and amount.

And of course, he can also verify the signature, the usual method, method of verifying signature namely, digest can be sent. And but also in the sense that the sign when I say signed the private key, effectively means it is a digest which has been encrypted, that is the signature. The order itself, order itself along the purchase order means the items, which is being ordered plus the agreed on cost of each item, total cost take together really constitute the purchase order, that will be encrypted by with the vendors public key.

So, that the vendor receives that he can use his private key to decrypt it and get the entire purchase order, signature of course, means that you are taking the digest of that. And then the purchaser encrypts with his private key. So, that the public the other side namely, the vendor can decrypt and make sure that the purchase order, which came it is digest and the decrypted digest match. In which case, there is the authentication of the signature is done and authentication of the purchase order is done tomorrow. There cannot be a dispute saying that I did not send the purchase order, because it is signed digest which is there, the digest is actually compared.

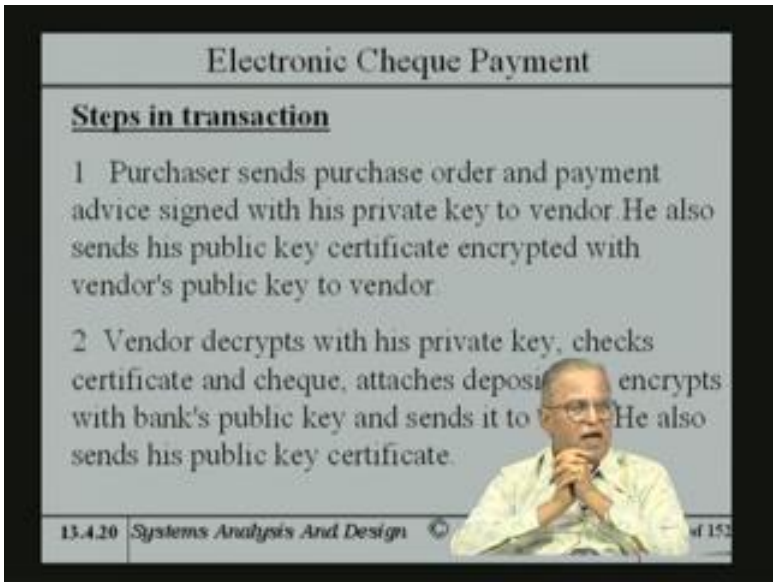
(Refer Slide Time: 20:24)



And vendor decrypts the private key and checks certificate and also the cheque is also sent. In other words, there are two ways in which one can send payment. One way is that first he sends the purchase order he is accepting and all that then goods were supplier and after the goods were supplied, then only the cheque is paid. Because the cheque is paid based on what is accepted, that is the goods, which may come then as I have been pointing out from the beginning will be sent for inspection.

And after inspection, the electric goods no payment will be made, only for accepted goods the payments will be made. So, the accepted goods and their cost and the total amount is the one, which is got to be sent by a cheque.

(Refer Slide Time: 21:18)



So, and the so in order to send a cheque what he would do, see cheque will consist of two parts one is the authorization for payments. So, the normally when we send a cheque in a manual system what we will do, we write out the name of the party concerned to whom it is payable, mark it account payee. And then put the, entry the amount of the cheque and sign it at the bottom that is a physical system.

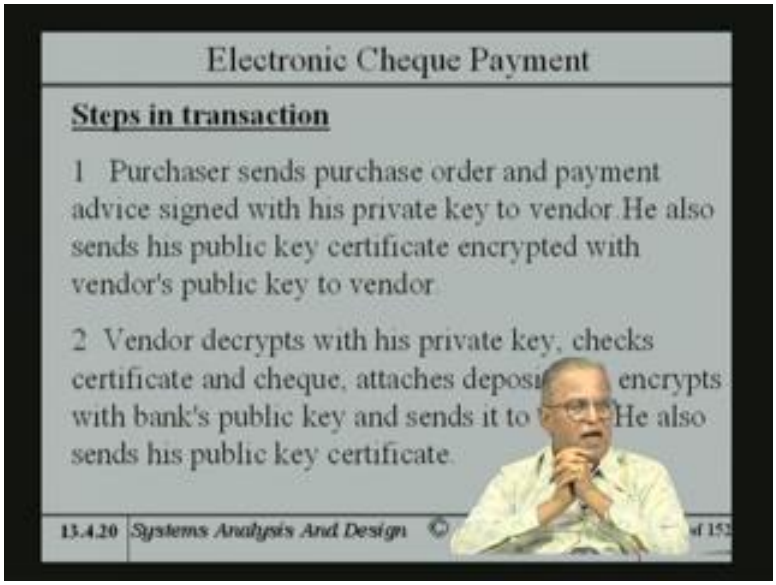
In this system equivalently, what should be done is that the cheque amount, the name of the recipient or in this case it could be a code for the recipient it is a vendor. Vendor code may be the one, which is agreed on between the two. So, the code of the recipient plus of course, the name of the recipient both together, plus the amount. And you may attach this cheque also at the top of it, the items for which the payment is being made.

So, this entire document essentially may be thought of as an e cheque that is as the accepted items list with the agreed on pricing, total amount. And the total amount along with the vendors name and code and this is the total document is digitally signed. So, what is meant by digitally signed is that this document is sent encrypted you with the public key of the vendor. So, you can decrypt it and look at the entire thing.

Along with it a digest is made using MD 5 and that digest is encrypted with the private key of the purchaser. So, when it gets there, that can be decrypted by the public key of the purchaser by the vendor. And then he can also create independently digest from the purchase order the entire amount, which came there with the cheque amount, which is

there. And if these two matches then he know that it is legally signed and that will stand up in a court of law.

(Refer Slide Time: 23:49)



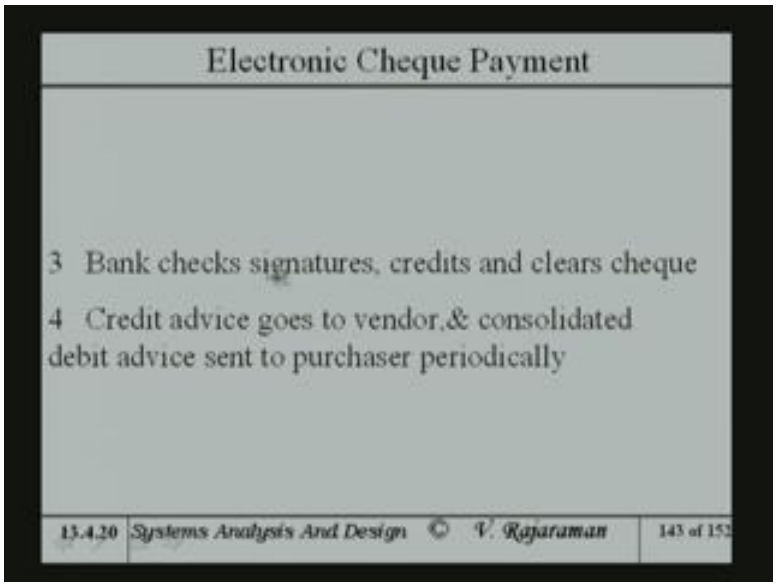
So, once it is signed of course, the public key certificate is sent by the purchaser, if it is not already exchanged and so on. Once it is done then the bank then now what the vendor will do is that, once he gets authentication about the signature he will send this entire thing to the bank. And normally the purchaser will also send to the bank, the signed copy of the purchase order and so that the bank can check whether, this cheque is a valid cheque or not.

So, it is vendor decrypts with private key, checks certificate and cheque, attaches deposit slip along with the cheque, encrypts with banks public key and sends it to the bank. He also sends bank his public key certificate. There is one kind of an exchange between two businesses of exchanging there public keys here also the vendor has a banker. There is no need to exchange the public key certificate, every time between the vendor and the bank.

Because the bank and the vendor has got a trusted relationship, so the vendor if it comes from the vendors code number, automatically the bank will know it is from the particular vendor. So, it will do the decryption and find out the cheque value and for later on dispute resolution it will also have a copy of the certificate, which is this certificate that is signed one from the purchaser.

That of course, may or may not be here. But, it is up to what kind of protocol, the three parties seem to use, because now what he will do, this bank will do is encrypts with bank public key and sends it the. So, bank once it is, it comes the cheque comes with the deposit slip.(Refer Time: 25:55) it will decrypt it.

(Refer Slide Time: 25:58)



Checks, checks the signature and credits and clears the cheque, what is meant by clearing the cheque is that the cheque has to be sent to a clearing organization. Cheques are all cleared in other words, two different banks see what happens is this cheque is issued in the name of some vendor. So, the vendor has to deposit in his bank. But, his bank in turn has to collect the amount from the issuer of the cheque, which is the purchaser and purchaser may have account in different bank.

So, cheque may be on a different bank. So, what the bank will do is that they will send a clearing agency to which all banks send cheques, which emanate from other banks. If it is your own bank there is no problem, immediately they will do the debit and credit. Otherwise it goes to a clearing, clearing agency in India the cheque clearing agency is the, it is the Bank of India, which is a which is an apex body, which has the responsibility of also dispute resolution and. So, on and. So, far and.

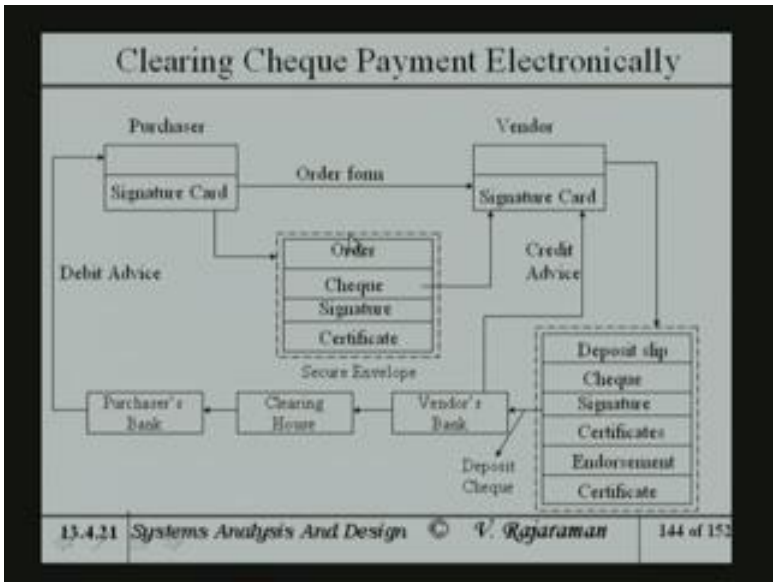
So, both the banks will send it, any bank which has a cheque issued in another banks name; they will send it to the clearing agency. And they will in turn, get it cleared by the by the bank, which is suppose to pay and then credit the account of this bank. All these

of course, done electronically at a reasonably fast speed, now a days clearing is all electronic. And the intermediary is only to keep things somewhat honest, in terms of the any disputes between the two banks, so on and so far.

And the credit advice goes to the vendor, once it is credited and consolidated debit advice is sent to the purchaser, periodically by this bank. In other words, the bank can ultimately the clearance is the money has been taken from his account and. So, he gets a consolidated statement, saying these are all the cheques issued; these are all the payments that have been made. So, we can check that against whatever he has been issuing. So, that there is no possible dispute, which may arise.

So, effectively this is the way in which it goes, the purchaser sends an order and signs it and puts it in a secure.

(Refer Slide Time: 28:44)



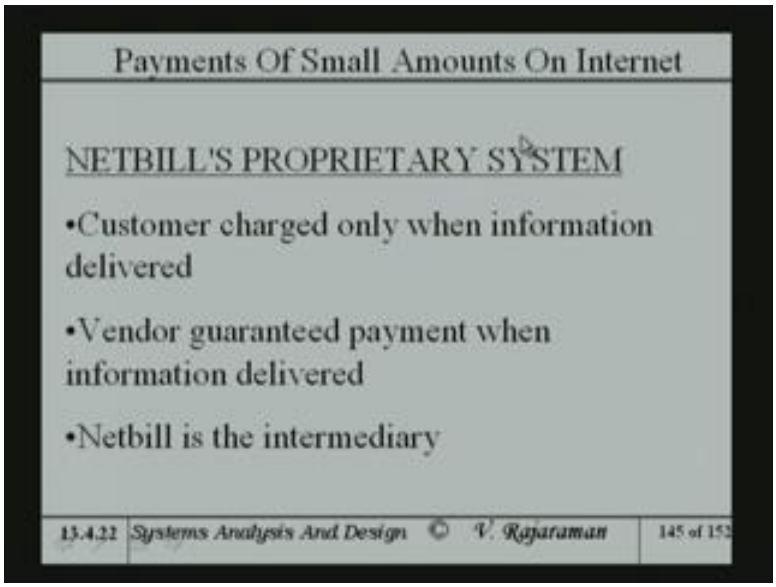
So called secure envelop; that means, it is encrypted on this, on this order cheque signature certificate all of them go together. And here it is vendor verifies the signature and. So, and deposits this cheque, signature certificate endorsement everything, his endorsement will deposit and it goes to the vendors bank. And of course, he signs it in turn. So, that there is no dispute between these two and the vendors bank will send the credit advice when it is been credited, the vendor will go to the clearing house.

And clearing house will send to the purchase, purchasers bank and that will in turn to the debiting because I have not shown the signing and all that here, which is actually imply. In other words, whenever there is an electronic transaction between two boxes over here they have to go through the entire notion of encryption, signing and. So, on just to be makes sure that any kind of a hacking on the transmission lines here are avoided.

Of course, (29:58) in some countries these lines may be entirely private lines, because there is a huge number of money transactions, which goes on between clearing houses and banks. And if this gets hacked, there will be a very, very serious consequences that is the reason why in many countries it is a dedicated line. So, that there is nobody can hack this and there is no need for things like encryption signature and so on.

So, this is the way in which the ultimate balance everything goes on. So, the point really is that the purchaser as well as the vendor have to be able to sign and they have got their own, what I mean by signature card is nothing, but a small piece of hardware of course, it could be a software also, which effectively does the digital signing. And secure envelope means, all these are put together and then encrypted through the public key of this person.

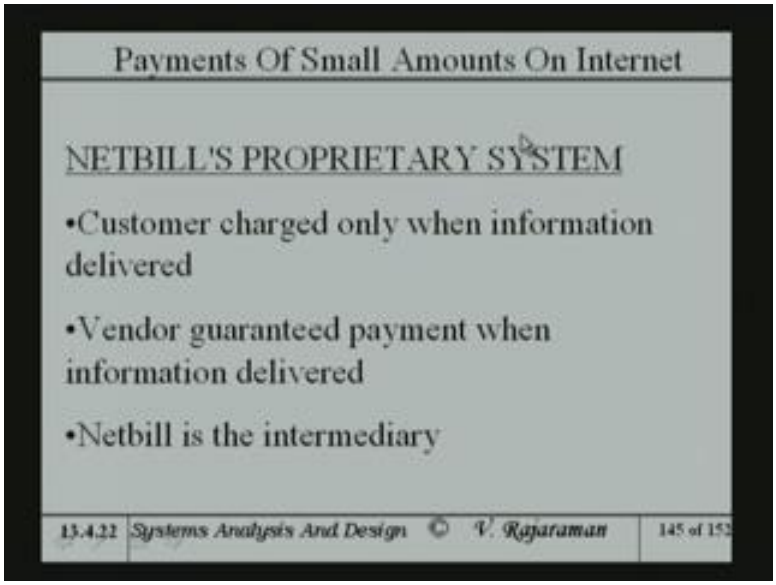
(Refer Slide Time: 31:04)



Now, the next payment means, I am going to talk about is something called it is actually a proprietary system. It is not something which is accepted all over the world. And it is

not actually available many places, it is available in USA. And it is actually administered by a company called Netbill and they got a system to which one can subscribe.

(Refer Slide Time: 31:35)



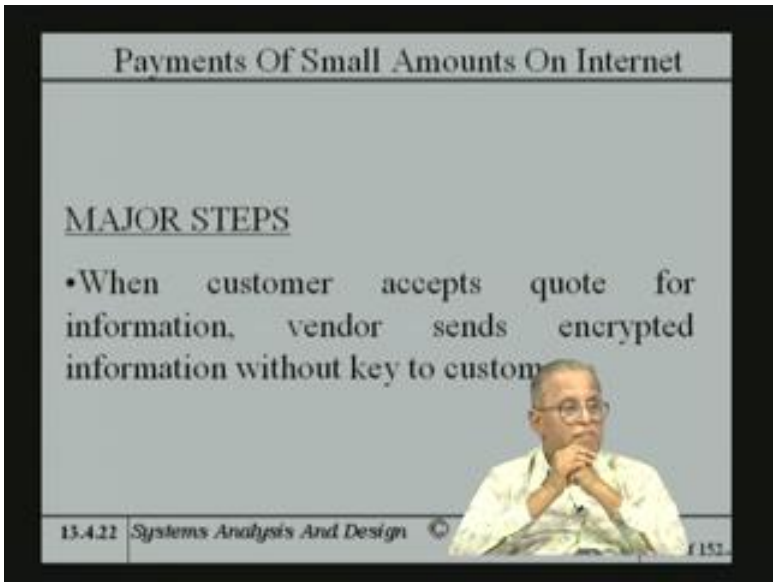
To be able to pay and get information goods, what is meant by information goods or as I said may be articles, that is a text file of some type or it could be a music file or it could be a video file does not matter what file it is. Because they are all ultimately they are all bit strings. So, the primary purpose of this, first of all the amount, which is involved in this, is not very large. It would be in US dollars may be a few dollars, in Indian rupees may be less than a 100 rupee or a few 100s maximum.

So, normally credit cards are used for amount in excess of normally, 500 rupees or so. Smaller amounts, the transaction cost of the credit cards can be quite large, that is if you go through all this dual signature and stuff like that. So, each transaction will cost a lot of money and that is the reason why, for small payments for information goods and. So, on credit cards are not normally used, of course there are new methods which are coming with debit cards and so on.

But, by and large overheads are there, that is the reason why this company finds it profitable and people are willing to kind of pay them because credit card companies as I said survive on late payment and. So, on because they charge interest on late payment and that is what, makes up for their total expenses. And besides that they have a yearly subscription, this will be much smaller amounts which are involved.

So, the primary interesting parts of the system is that customer is charged, only when the information is delivered this and also the customer is satisfied with the information. In other words, satisfied in the sense that he gets what he has ordered and not something else. Vendor is guaranteed payment when information is delivered, the vendor you know he has to be sure that he delivers some say music file, he does get paid. So, that is also ensured and Netbill is intermediary.

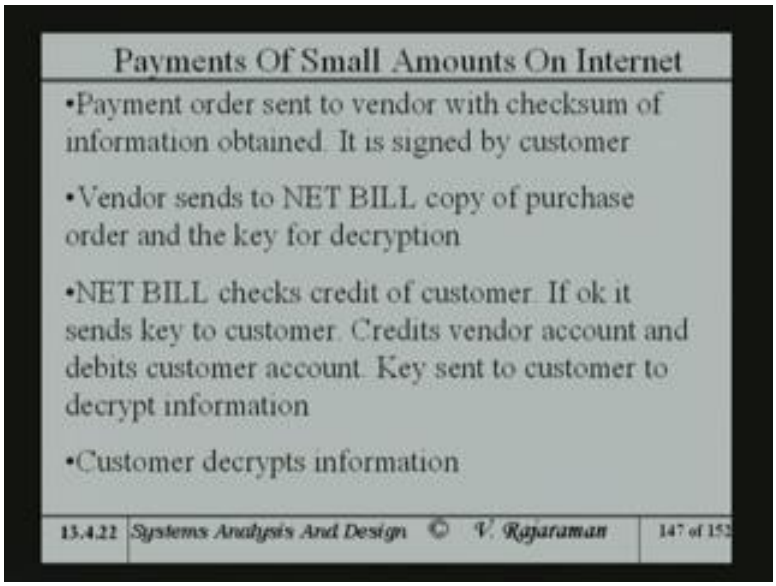
(Refer Slide Time: 34:22)



Major steps are the following, when customer accepts quote for information, vendor sends encrypted information without the key to the customer. So, it is actually encrypted, using some kind of a symmetric key encryption because in this case, the items are not of great value. So, no hacker will be really interested unlike huge payments of cheques and so on. Because this is a, as I said few dollars are may be less than a 100 rupees or a few 100 rupees, people are not interested to go through all that difficulty to do hacking and so on.

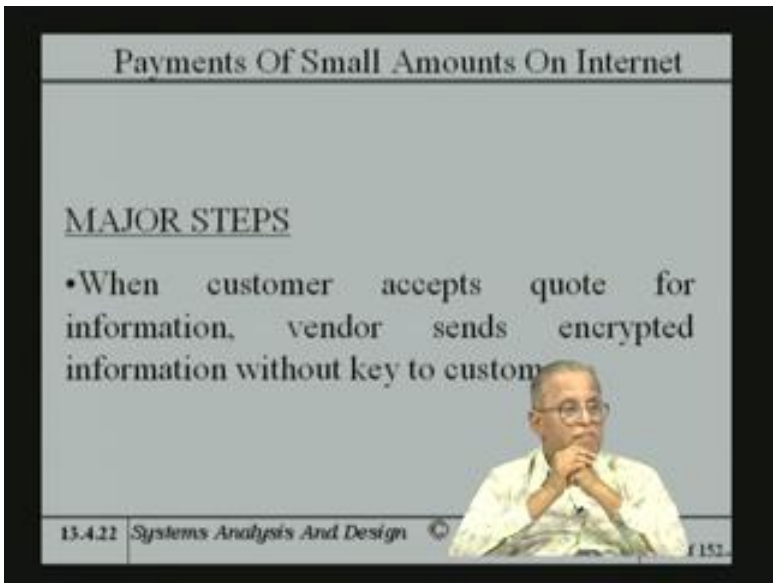
So, by and large, it uses symmetric key, when customer accepts quote for information. So, in other words the vendor sends encrypted information without the key to the customer.

(Refer Slide Time: 35:24)



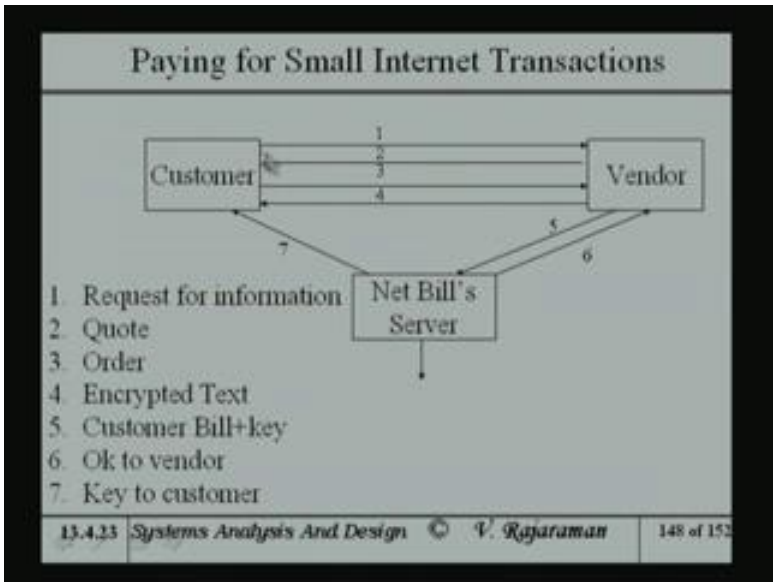
And payment order is sent to the vendor with the checksum of information obtained. In other words, what is meant by that is that when the, see actually the as I pointed out here.

(Refer Slide Time: 35:37)



The steps are first the customer orders, from the. Let us just look at the steps in other words.

(Refer Slide Time: 35:56)



This is the way in which these see customer requests information, customer requests information that is step one and. So, he will send his request information and the vendor will quote saying that this is going to cost you, this much money. Suppose, he orders a particular track of music, for that track this vendor is going is given a quote. And then the quote is accepted, the order comes from the customer to the vendor, the order means he is given accepted the quote, the price is fixed.

And so it is actually, the acceptance order acceptance goes in step three. And step four, once the order is accepted he sends the encrypted text or encrypted music file to the customer. The customer does not get the file right away; because only after he makes a payment, he will get the actual he can actually use it. So, the customer, as I said the fourth is encrypted text goes to the customer.

Now, the vendor will send the customer bill that is the amount, which is he is supposed to paid. Plus key to decrypt that particular information because it is encrypted with an symmetric key. So, it will give the key to the Netbill server, Netbill is intermediary and this Netbill server will first check whether, the customer has got enough credit. So, what is it imply, it implies that the customer as well as the vendor have some account with the Netbill.

So, the customer essentially purchases, you might say or pays some amount say may be a deposit of two couple of 100 dollars or 500 hundred rupees equivalent. It may be

approximately 500 hundred rupees for the items, he is intends to purchase and. So, there is a credit here. So, Netbill actually gets the money ahead of time, its actually debits because it gets money ahead of time.

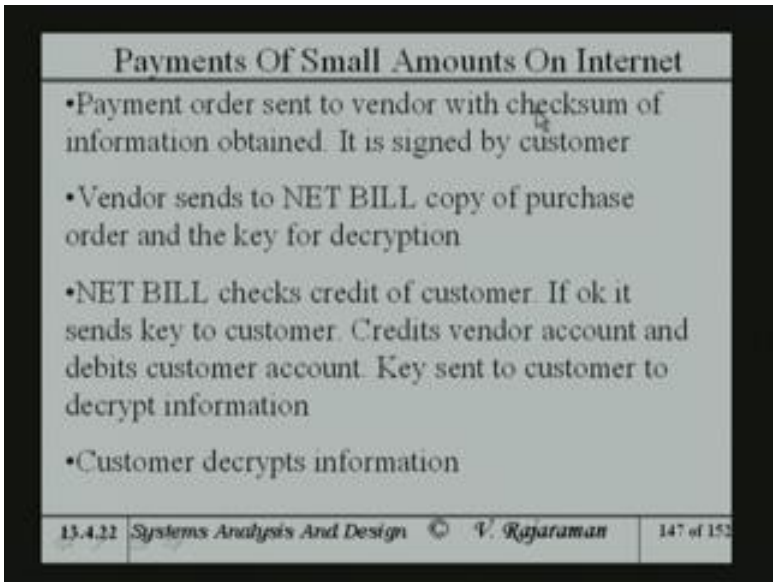
And then their interest on that money, there is a kind of you might say interest value out of which it makes its profit. Because, otherwise for each transaction and all no payment is made by a customer. But, vendor may have to pay some kind of a commission to Netbill because Netbill is going to pay him the money. So, for each transaction the vendor may have to be give a certain little raw royalty or may be commission to the Netbill.

So, it will collect commission from the vendor and of course, the debit, this deposit will also give you certain amount of you might say, short term interest. And these two together is what supports Netbills business model. So, the vendor sends the bill, customers bill plus the key to decrypt to a Netbill server. And the Netbill finds out that the customer has got enough credit in the Netbills account and then he will send an okay to the vendor and when he sends okay to the vendor saying that the transaction is accepted.

And so I am going to supply, the key to the customer when the key goes to the customer. The customer can decrypt this, whatever came to him encrypted with the key decrypt this with the key and hear the music or read the text material whatever it is. And once the key is sent, the transaction is complete as far as the customer is concerned and Netbill is concerned.

So, it will actually okay, once it is okays the vendor is requested to pay the commission, whatever the commission to pay to the Netbill and this transaction is now closed. So, each transaction goes through this.

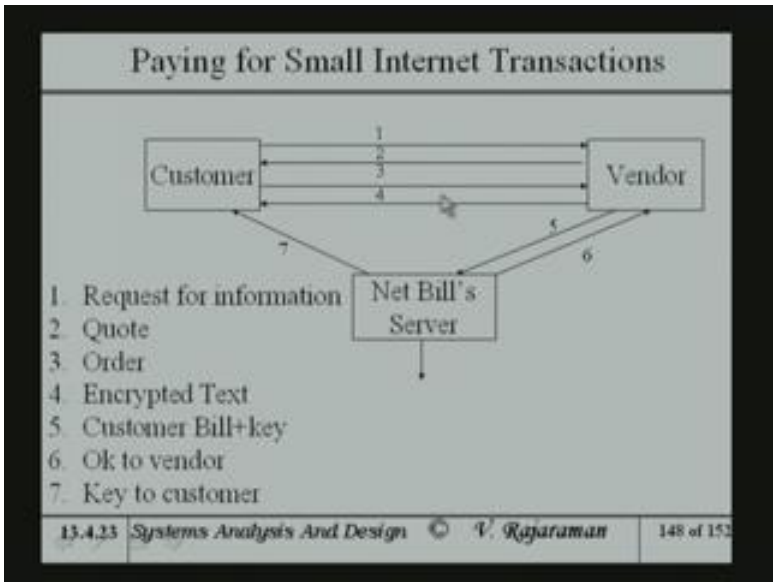
(Refer Slide Time: 40:49)



So, that is essentially what I am writing in words, payment order is sent to the vendor with checksum of information obtained. It is signed by the customer. Vendor sends NET BILL copy of purchase order and key for decryption. NETBILL checks credit of customer it sends key to customer key to enter key to encrypt debits customer account. Key sent to customer to decrypt information. Customer decrypts information that is essentially same steps.

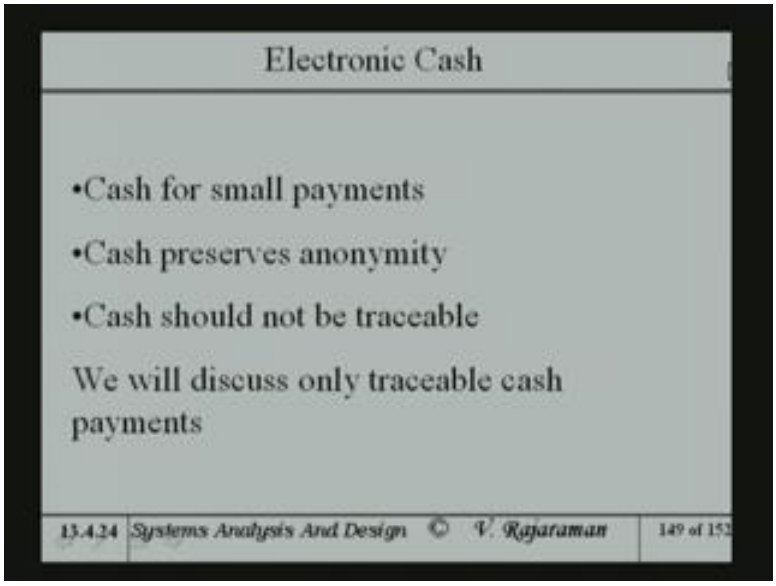
You can now only question, which the question one might ask is the payment order is sent to the vendor with checksum of information obtained, it is signed by the customer. What is meant by that, now the purchase order number that is request information that is number step three, which is the purchase order.

(Refer Slide Time: 41:42)



The purchase order is sent checksum, the checksum means effectively it is hashed, whatever it received at this time the he has to get (Refer Time: 42:04) the customer signs this purchase order of course, that is obvious. And now payment order is sent to the checksum that is primarily for dispute resolution, which is later on if there is any kind of dispute it can be resolved, but the primary steps are these which I explained in fairly great detail.

(Refer Slide Time: 42:28)



Now, the last part is the electronic cash payment, the cash payment is a very tricky affair, because cash preserves anonymity. That is, suppose the cash or the currency notes are issued by a central agency like, Reserve Bank of India, Reserve Bank of India is the one which prints notes and puts in circulation. And of course, this fact that piece of paper whose intrinsic value is nothing still has a value to purchase, comes in the fact that there is an undertaking by the reserve bank that I pay the bearer on demand.

So, much of money in the earlier days whenever a bank, reserve bank of a country was issuing cheques, was issuing currency notes, it is supposed to have gold reserves equal to that currency note which they give out. So, gold reserves was essentially expected to be there to kind of guarantee that the kind currency notes, which have been printed have any value at all.

But now a days of course, that is that gold standard, which is used to be called gold standard is gone and instead they got some kind of a International Monetary Fund, which kind of looks at credits and debits, balance of payment and. So, on and then the value of various currencies float with respect to some standard currencies namely, currently the standard currencies are US dollars and Euros and yen.

Because they are strong economies whatever, it is mean that is the way today. But, whatever as far as general public is concerned that even though RBI sup is the one, which is printing those that will actually transact business. I do not have to tell RBI what transaction is taking place, once it is issued, you have a bank you have a cheque you have a cash rupee note, rupee note is anonymous who has it nobody knows.

So, if I take a dollar of 100 rupees from my friend, nobody get to know except myself and my friend and. So, that is the advantage anonymity of cash there is also disadvantage, which governments are worried about. Because large cash payments is called black money, does not go through banking channels and so on. So, black money are lots of cashes, cash is actually used by for illegal means.

Let like for instance drug trafficking or terrorism and stuff like that, that is why countries are very aware to kind of issuing even currency notes, beyond a certain value. In India for instance, only recently they have started issuing 1000 rupee notes that is the highest currency note, you can which is issued the reason why the value is kind of kept at a ceiling is that to transport huge amounts of cash.

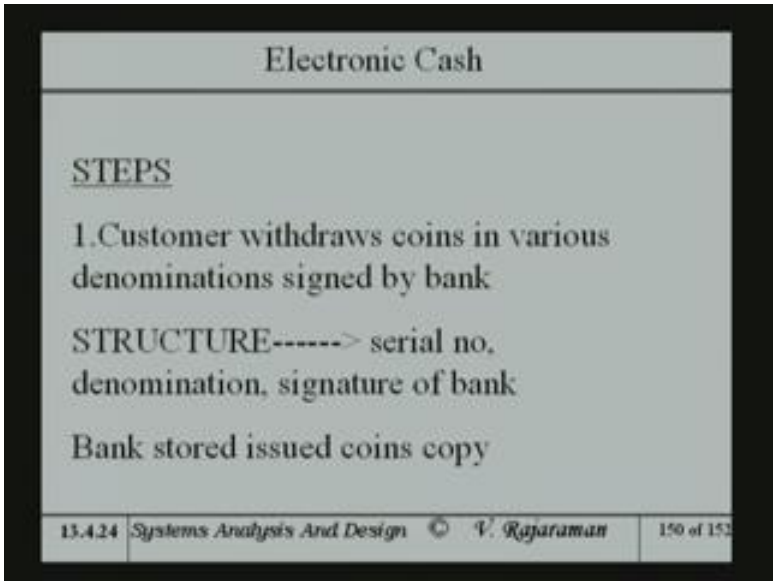
Volume is very high and you cannot smuggle it through customs and. So, on people will find out, when you are smuggling cash from one place to the other. Whereas in electronic in electronic cash, the electronic cash can flow through internet without anybody knowing. And internet does not understand national boundaries, the result that it is very; very governments are very worried of allowing cash transactions to the anonymous transactions, over the internet of particularly of cash.

So, it should be a traceable, see cash is you know real value of cash is not traceable, whereas electronic cash the government do not like non traceable cash, they want it to be traceable. So, we will only discuss traceable cash of course, they are using protocols, which have been invented to make transactions anonymous on the net, that is the algorithms, which are there is one algorithm which sound which is anonymous transactions and. So, on, but it is not normally used because legally, it is not allowed.

So, in this case it is traceable cash so; that means, what is meant by traceable cash there are two things, the anonymity means that if I purchase some items, from a from a shop with cash. And you know as the shop is concerned, I am an anonymous body, I have paid for the goods and have gone away and tomorrow if you ask him, who paid for if it is a like if I bought some saris and. So, on I may have paid 5000 thousand rupees for the sari.

But, to say who paid this 500 thousand who bought this sari it is very difficult for that person to find out. Because very often he will issue cash you know he may not even put the name, because he has got cash. So, the cash will move and he clears it and. So, nobody really asks for a name of a person, unless it is goods, which have the guarantee and stuff like that. So, that is the whole point.

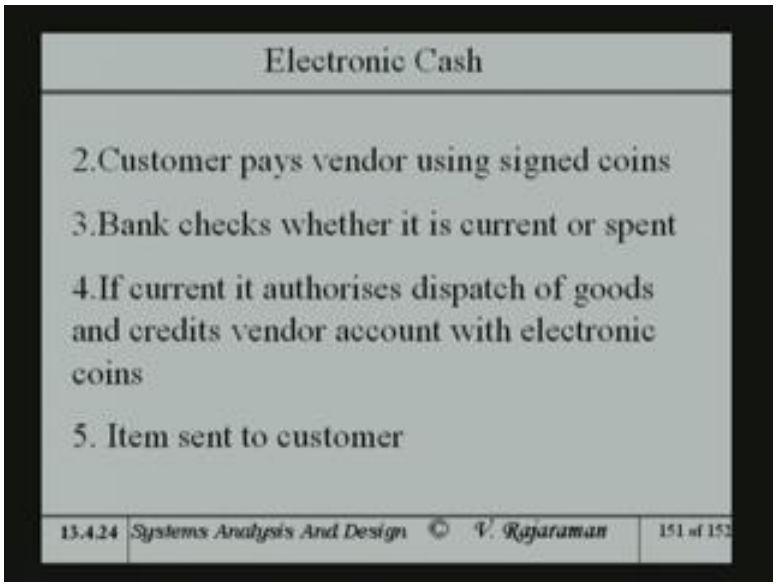
(Refer Slide Time: 48:52)



In the case of the electronic cash, it is traceable actually in this case also it is not anonymous. So, customer withdraws coins, they will give this for small payments only because as I said governments do not like large payments, large cash payments. Customer withdraws coins in various denominations signed by a bank that is a bank is an issuer of this currency, just like reserve bank issues currency notes of various denominations, there are certain designated banks, which deal with electronic cash.

So, they will essentially issue some tokens you might say, each token will say this is one rupee and it will be signed by the banks digital signature and 5 rupee, 10 rupee, 15 rupees, 20 rupees whatever. And it is got a serial number denomination and signature of the bank. So, these three are there in each token bank stored and it stores all the issued coins. So, that it can to whom it is issued and. So, regards that debits that person, when he purchases some goods. So, it requires to store it, for debiting.

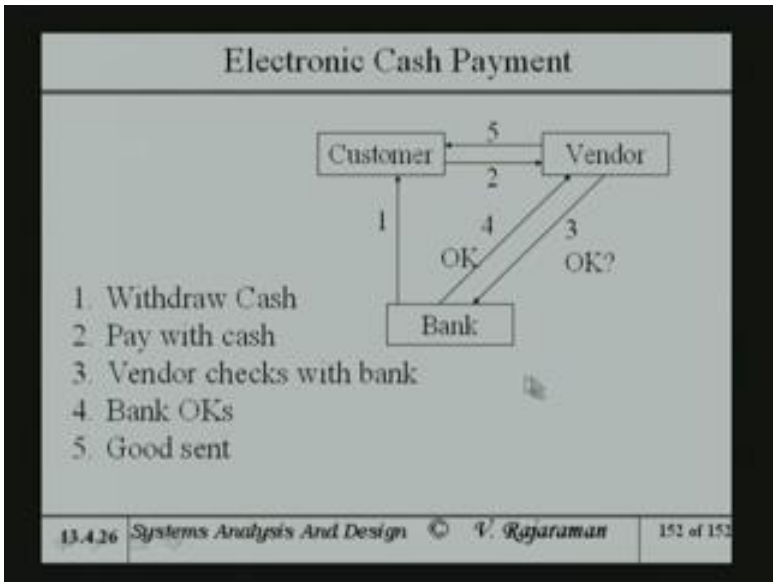
(Refer Slide Time: 50: 07)



Customer pays the vendor using the signed coins, so again electronically. Bank checks whether it is current or spent, in other words the vendor who send that signed coins to the bank. And the bank will see whether it is already spent, if it is already spent means, it is already been encashed that is why it keeps its complete database of what it is issued. If it issue what is issued, it will check whether this coin this coin is given by the vendor he is issued has been already used or not used. If it is not used then; that means, he will allow the authorize to this much of goods and credits vendor account with electronic coins.

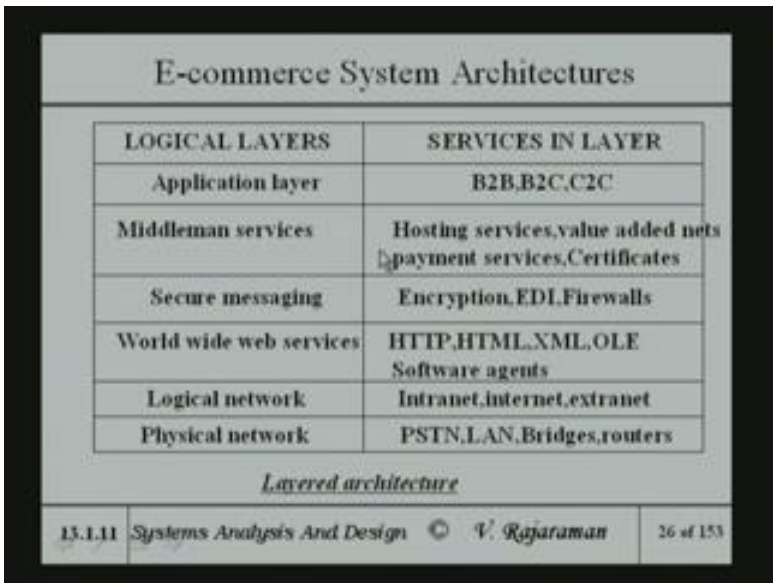
And item is the vendor sends the items to customer and the bank will actually renew this coin, you might say the signed coin from the credit of the purchaser, who has bought these. So, it cannot be used again because it is been taken away from the database.

(Refer Slide Time: 51:20)

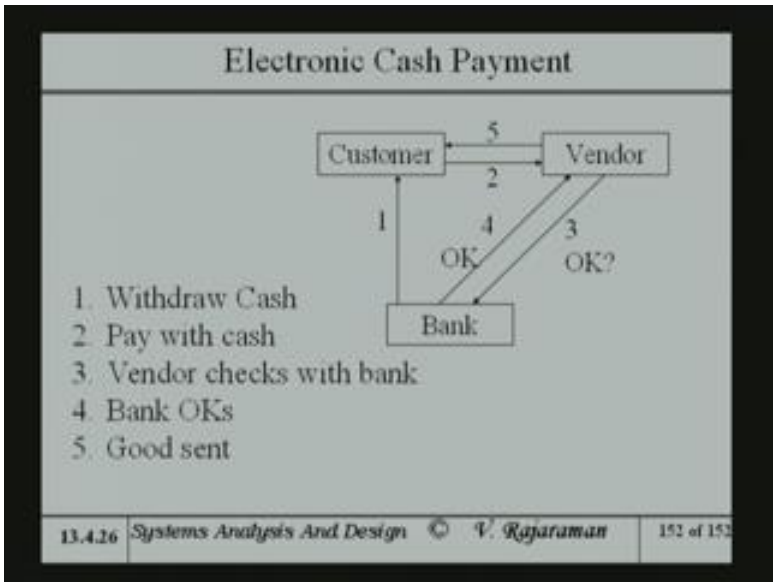


So, primarily the steps are withdraws cash, cash in this case are many denominations signed by the bank and pays with this cash and the vendor sends it to the bank. And bank checks and says it is whether it is or not, it is whether a spent coin or unspent coin once it gets okay. And the bank essentially the vendor will send back the items to him and of course, the bank will pay the vendor the amount.

(Refer Slide Time: 51:55)



So, this is the whole set of things, which go on, this is the cycle and I am not. And I have not spent too much time in this for simple reason is that, it is not all that popular yet. (Refer Slide Time: 52:15)



And because by and large, small cash payments may be physically go to the shop and buy, electronically they really do not do much cash transactions. But, it is interesting never the less, how we tried to mimic cash. In fact, books have been written on this there is a book called electronic money, which discuss all about what cash implies in the case of electronic commerce. And there are number of many interesting articles which have been written and so on.

In fact, an entire issue of one of the IEEE transactions in the computer was issued through electronic cash, to discuss all the advances of electronic cash. Because it is one of the, you might say the last goal post in which people in e commerce are looking for, but then of course, there are road blocks because of the problems with governments in general. Now, this kind of concludes what I had been talking about, in electronic commerce.

Now, there are couple of things I would like to talk about in the remaining time, one is emerging areas in electronic commerce, the what is meant by emerging areas is what is in the horizon, what is slowly coming and may be next five years or. So, what will become very, very prevalent and common and you as a student, what you should be

looking for in terms of the newer were emerging technologies and keep up with those emerging technologies.

One thing, which is very interesting which is happening is what is called mobile commerce or abbreviator is m commerce, the name mobile commerce implies that the commerce is between mobile devices. And where ever mobile device is got an important bearing as you know very well mobile devices have become very, very common. Today in India for instance, the number of mobile phones, which have been given to customers it exceeds the number of fixed phones.

Previously the number of fixed phones was the major item, but mobile phones are almost I think double the number of fixed phones; that means, the people are always in a move. And people always uses their mobile phones for various purposes in of course, besides the talking on the mobile phone as you know mobile phones have become, so powerful you can you can normally can send SMS messages. SMS is very, very commonly used because it is a very inexpensive way of communicating plus of course, you can take a photo on the mobile phone and you can even transmit a photo and so on.

So, you might say mobility have become important, apart from mobile phones there is something called PDAs that is personal digital assistance, which are also connected to the cellular phone system. And with the mobile phone, there is something called wireless application protocol, which is coming for communicating with the mobile phone with the internet, which is different from the TCP IP protocol. TCP IP protocol assumes that the devices or PCs which are connected to the internet.

So, actually they in the TCP IP protocol, the message is cut up into small parts and sent they are assembled. But, the TCPs function is to make sure, that all the pockets have come. And they have been assembled in the right way and that it completes message, whereas in WAP, wireless application protocol they do not do this checking because the bandwidths are more expensive and also not as much as in fixed devices, even if they are changing.

So, there is a wireless application protocol which is used, so that is number one. Now, the question one might ask is why anybody would think of mobile commerce when you have got your PC. In fact, you have a mobile PC in the sense that, there are you know Wi-fi s are available everywhere airports, hotels and so on. And you have wireless

connection with the laptop, with the with the telephone line. So, that of course, is a part of internet, you can connect your personal computer with the internet and you can transact business and so on.

That is not really in mobile commerce, mobile commerce is implication, something to do with the cellular phone network, which is used by cell phones and so on and PDAs and what not. So, the basic difference between cell phones and PCs as PDAs and PCs those cell phones the screen is very small. And also the keyboard is very small and the processor there is much less powerful than PC. So, you got to have methods, which are appropriate for that, so, that is the challenge.

And currently, the two major applications of wireless or mobile e commerce are number one is in supply chain management is. That supply chain management is one of the major applications in e commerce, where you want to kind of order items from multiple vendors. And do it in reasonably fast time, so that you totally be able to reduce the risk. So, in the mobile commerce, what happens is you are able to track the movement of items through you know on a track, called a plane and so on.

Each pocket will have something called a radio frequency identification time or radio frequency time, which effectively gives radio frequency identification. So, if I have a reader, it will tell me, it will track the item exactly where it is. So, am I am able to track the items continuously where it is I can predict much better, when it will come to me. Suppose, I very urgently require one the vendor may direct something on the way from one purchaser to the other purchaser because other one purchaser, there is no very urgent need.

So, this kind of a, what is meant by mobile tracking is one, tracking of items and then rerouting of items and so on and. For similarly, another very interesting application, which people are using is in terms of. Suppose, we are traveling and we want to find out the nearest shop and using a global positioning system on the mobile device, it will give you a little map and say where, you are compared to this shop. So, again you can go to that shop or restaurant and so on.

So, these are all the emerging applications of mobile commerce and. So, we will see that the next 5 years or so this is going to become a very, very important area, which will be appended to the e commerce and. So, one has to look at new protocols, new methods and

new applications new business models and. So, on and I think it is really going to be very, very exciting in this mobile kind of commerce area. So, with this we are stopping, these discussion of electronic commerce and I will go on with the rest of the topics, two more primary modules are left in the next two lectures.