

ELECTRONIC COMMERCE

Learning Units

13.1 What is E-Commerce?

13.2 Electronic Data Interchange

13.3 Security of E-Commerce

13.4 Payment in E-Commerce

Learning Goals

- The basics of Electronic Commerce abbreviated as e-commerce
- The advantages and disadvantages of e-commerce
- Architecture of e-commerce systems
- Electronic Data Interchange in e-commerce
- The need for security in e-commerce transactions and how to ensure it
- How Electronic payment schemes work in e-commerce.

Motivation

- With the emergence of internet and the world wide web new methods of carrying out business transactions using the world wide web began to be explored.
- Electronic Commerce emerged as a very important application of the world wide web.
- Today it is difficult to find an isolated computer. Computers in an organization are interconnected to form intranets and intranets of the cooperating organizations are interconnected to form extranet.

Motivation (Contd)

- It is cheaper and faster to carry out business transactions within an organization and among organizations electronically using the network connection.
- Thus it is important to understand how business transactions are carried out electronically reliably and securely
- When designing information systems it is essential to understand the emerging web based transactions
- A number of organizations are exploring how to carry out all day-to-day operations electronically using the intranet in a so-called paperless system
- It is thus important for a student to understand how to design such systems

What Is Electronic Commerce

DEFINITION

- Sharing Business Information, Maintaining Business relationships and conducting business transactions using computers connected to a Telecommunication Network is called E-Commerce

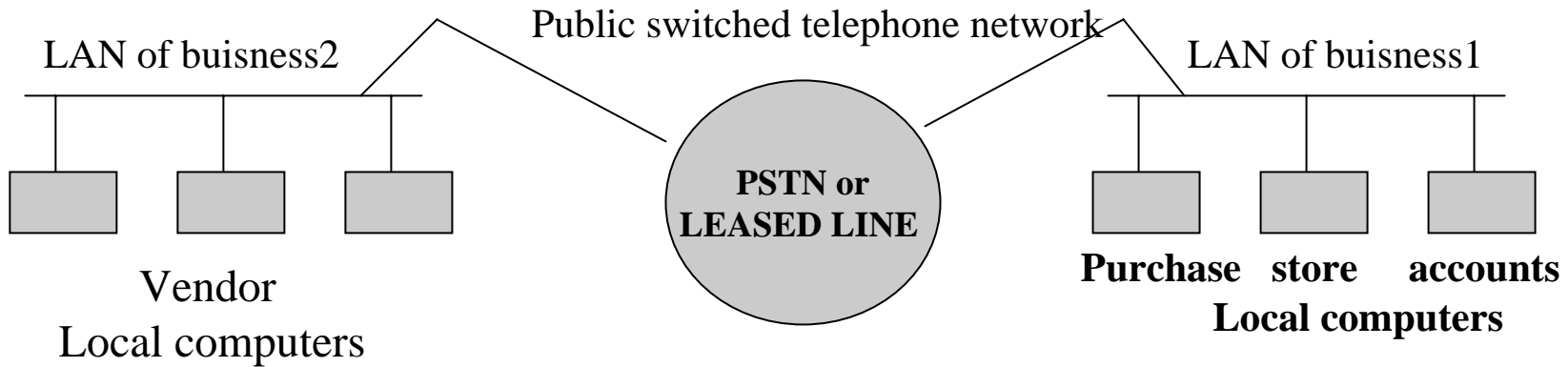
CLASSIFICATION

- CLASSIFIED AS : BUSINESS TO BUSINESS (B2B)
BUSINESS TO CUSTOMER (B2C)
CUSTOMER TO CUSTOMER (C2C)

E-commerce Applications-example

- RETAIL STORES - Books, Music
- AUCTION SITES
- COOPERATING BUSINESSES –Placing orders,paying invoices etc.
- ELECTRONIC BANKING
- BOOKING TICKETS - TRAINS, CINEMA, AIRLINES
- ELECTRONIC PUBLISHING
- FILLING TAX RETURNS WITH GOVERNMENT DEPT.

Business To Business E-commerce



- Local LAN of business would normally follow TCP/IP protocol of internet and is called corporate intranet
- Purchase order entered by business1 in its PC and electronically dispatched to vendor (by e-mail)
- Vendor acknowledges electronically the order
- Vendor dispatches goods(physically) and delivery note electronically to business1

B2B E-commerce (Contd)

- Business 1 can compare delivery note against order -both are in computer readable form
- Discrepancy note(if any) can be immediately sent to the vendor
- Business 1 can carry out all local transactions using its LAN
- Local transactions are inventory update by stores - advice to accounts to pay for goods taken into stock
- Accounts can make payment electronically to Vendor

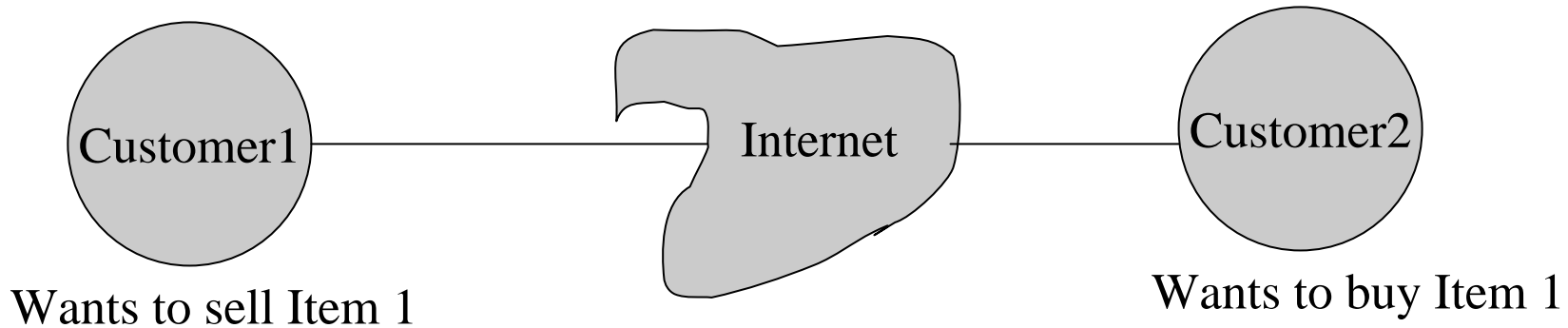
Implementing B2B E-commerce- requirements

1. Agreed on formats for Purchase order, delivery note, payment order etc. Standard known as EDI (Electronic Data Interchange Standard) is used to send documents electronically
2. Each Business must have corporate intranet and the two nets are connected by PSTN or leased line
3. Transactions must be secure - particularly if PSTN is used
4. Secure electronic payment methods are required

Steps In B2C E-commerce

1. Customer uses a browser and locates vendor or he has vendor's web page address
2. Sees Vendor's web page listing of items available, prices etc
3. Customer selects item and places order. Order may include credit card details or may be cash on delivery
4. Vendor checks with credit card company customer's credit
5. Credit card company OKs transaction
6. Vendor acknowledges Customer's order and gives details of delivery date, mode of transport, cost etc
7. Vendor orders with distributor who ships item to vendor's warehouse from where item supplied to customer
8. Customer's credit card company debits his account, credits vendor's account and sends bill to customer for payment

Customer to Customer E-Commerce



Broker's website

- Advertises - "for sale"
- Brings together buyer and seller
- Transports items
- Collects fee from both Seller & Buyer

Advantages Of E-commerce

1. Buying/selling a variety of goods and services from one's home or business
2. Anywhere, anytime transaction
3. Can look for lowest cost for specific goods or service
4. Businesses can reach out to worldwide clients - can establish business partnerships

Advantages Of E-commerce

5. Order processing cost reduced

6. Electronic funds transfer faster

7. Supply chain management is simpler, faster, and cheaper using e-commerce

- Can order from several vendors and monitor supplies.

- Production schedule and inventory of an organization can be inspected by cooperating supplier who can in-turn schedule their work.

Disadvantages Of E-commerce

1. Electronic data interchange using EDI is expensive for small businesses
2. Security of internet is not very good - viruses, hacker attacks can paralyse e-commerce
3. Privacy of e-transactions is not guaranteed
4. E-commerce de-personalises shopping. People go shopping to meet others - window shop and bargain

E-commerce System Architectures

LOGICAL LAYERS	SERVICES IN LAYER
Application layer	B2B,B2C,C2C
Middleman services	Hosting services,value added nets payment services,Certificates
Secure messaging	Encryption,EDI,Firewalls
World wide web services	HTTP,HTML,XML,OLE Software agents
Logical network	Intranet,internet,extranet
Physical network	PSTN,LAN,Bridges,routers

Layered architecture

Electronic Data Interchange

- Computer readable forms for business documents such as invoices, purchase orders, delivery notes needed in B2B e-commerce so that e-documents can be exchanged.
- Essential to eliminate manual data entry which is error prone
- Essential to agree on common formats for commonly used forms.
- Electronic data interchange (EDI) standard gives specifications for commonly used standard business forms
- Currently two standards are available for EDI forms
- It is possible to adapt these standards for documents which use XML for specification.

EDI Standards

- ANSI X.12 standard proposed by American National Standards Institute
- EDIFACT (Electronic Data Interchange For Administration Commerce and Trade) standardized by United Nations Economic Commission for Europe for international trade
- EDIFACT used in India for government transactions - customs, central excise etc.

EDI Transactions in B2B E-commerce

- Cooperating businesses agree on EDI standard
- Programs needed to translate data received in EDI format to a form needed by the application program
- Method of sending/receiving data between businesses to be agreed on - is it PSTN, Extranet or VAN (value added network) service ?
- Important to ensure reliable, guaranteed and secure receipt of electronic documents by intended receiver

EDI Using Value Added Network Service

- VAN provides post box for all subscribers
- Guarantees delivery
- Open 24 hours, 7 days a week
- Provides security, acknowledgement, audit trails for transactions, non repudiation by users
- Some VAN'S provide conversion of EDI forms to application format
- Disadvantage high cost. Used by large businesses - may not be cost-effective for smaller businesses

EDI Using Internet

- Cheaper method for use by small business is to use XML for EDI and e-mail, instead of VAN
- Establish EDI form standard - XML appropriate – Document Type Definition (DTD) publicised using organization's web page- cooperating business can use a DTD to interpret XML documents.
- Use MIME (multipurpose internet mail extension) to attach EDI forms to e-mail messages

EDI Using Internet

- Can use Simple Mail Transfer Protocol(SMTP) of internet
- If secure transmission needed use S/MIME (Security enhanced MIME) which uses encryption and digital signature –(We will describe encryption and digital signature later in this module)
- If very long document or many documents are to be sent together File Transfer Protocol (FTP) may be more appropriate.

EDI Standard

- Defines several hundred transaction sets corresponding to each type of business document such as invoice, purchase order etc.
- Defines data segments - corresponding to groups of data elements such as purchase order line
- Defines data elements - which are individual fields such as price, quantity etc

Security In E-commerce

- Transactions between organizations take place in many e-commerce applications using the Internet
- Internet is widely accessible and insecure as eavesdropping is possible
- Need to protect company confidential information from snoopers
- We need to protect a company's network from unauthorised entry - both hardware and software techniques used
- When an organization receives a message it has to be sure from whom it came and whether the message is authentic and not changed by an unauthorised person
- We thus need a digital signature which can be used in a court of law

Network Security Using Firewall

- Firewall is a security device deployed at the boundary of an organization's network to protect it from unauthorised external access
- It links an organization's intranet to the internet and restricts the type of traffic that it will pass, thus providing security
- Simple firewalls may be implemented in some routers, called packet filtering firewalls, they pass only some packets based on simple specified criteria such as
 - Type of access (such as email, ftp, telnet as determined by TCP port number)
 - Direction of traffic
 - Source or destination IP address
 - Time of day

Proxy Application Gateway

- Primarily for allowing members of an organization on corporate intranet to access internet facility ensuring organizational discipline and security
- Proxy application program running on a firewall machine is the one which acts on behalf of all members of an organization wanting to use the internet
- This program monitors all requests - allows access to only designated addresses outside, limits use of certain browsers and disallows use of some protocols with known security holes
- Proxy application program may also be allowed to run on some user's machine who have authorization for internet use

Hardened Firewalls With Proxy Application Gateway

- Any one from inside or outside an organization give their user id, password, service required to the firewall machine which acts as one's proxy (ie. does ones work on his behalf)
- Proxy firewall is now server to the requestor's desktop PC and also a client to some other requested service acting on requestor's behalf
- Firewall needs proxy agent for each service requested such as FTP, HTTP, TELNET etc

Hardened Firewalls With Proxy Application Gateway

- Now proxy firewall is the initiator of all sessions and thus knows every activity - thus ensuring security
- Firewall with a proxy function replaces the source address of transaction requestor with its own IP address
 - this ensures that others on internet see only firewall's IP address - all other IP addresses of organization are hidden

Data Encryption With Secret Keys

- Data sent via a public network may be accessed and used by unauthorized persons
- Thus necessary to scramble it so that even if one accesses it, it cannot be understood
- Similarly data stored in data bases accessible via internet should be scrambled
- Method of scrambling known as encryption
- Method of unscrambling known as decryption

Plain Text And Ciphertext

- Plain text is data in its natural form
- Encryption is taking data in any form (Text, Audio, Video etc.) and transforming it to another form which cannot be understood
- Transformed data is known as cryptogram or cipher text

Example Text Encryption

Start plaintext

THIS IS A MESSAGE X

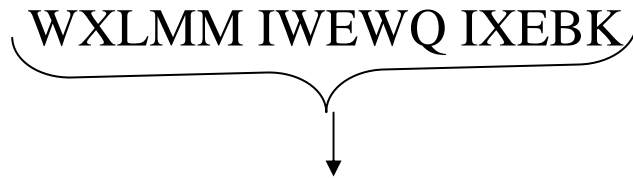
Block plaintext (5character blocks)

THISI SAMES SAGEX

Transpose characters with
permutation (4 1 2 5 3)


STHII ESASM ESAXG

Substitute character by
the one 4 letters away
(eg A → E, Z → D)


WXLMM IWEWQ IXEBK

Cipher text

This is an example of two transformations - permutation followed by substitution

The keys are permutation function and substitution function

Symmetric Encryption.

PLAINTEXT $(m_1, m_2 \dots m_n)$

CIPHER TEXT $(c_1, c_2, c_3 \dots c_n)$

Where $c_i = k(T_i (m_i))$ In which T_i is permutation of i^{th} character and k is substitution.

- Decryption by applying same transformations in reverse on cipher text.
- This method called symmetric key encryption as encryption and decryption performed using same key.
- Normally the encryption/decryption algorithm is publicised. Only key is secret.

Symmetric Encryption

- Problem is to ensure secrecy of key when it is sent to partner.
- If the key is to be sent to many partners need for separate key for each partner. Directory of who was sent which key is to be kept and used for each transaction. Directory should be secure.
- If large number of partners are there key distribution very difficult.
- Advantage of symmetric key is easy and fast to transform plain text to cipher text.

Digital Encryption Standard

DES - Proposed by IBM in 1975

Standardised by US Govt in 1977

Reasonably secure

It is a combination of permutation and substitution on blocks of 64 bits. A message is broken up into 64 bit blocks and each block is separately encrypted.

Digital Encryption Standard

#General idea used in DES

M = PLAINTEXT	01101100	11011000	11011010	
K = KEY	10101111	00101100	01011011	
E = $M \oplus K$	11000011	11110100	10000001	encryption
M = $E \oplus K$	01101100	11011000	11011010	decryption

See simplicity of Transformation using Exclusive OR

Digital Encryption Standard Algorithm

Before applying DES the text is split up into the 64 bit blocks.
DES applied on each 64 bit block.

Encryption method

Step 1: Apply an initial permutation on a block. Result is $B=IP(P)$
where P is the 64 bit block IP Initial Permutation function and
 B the result.

Step 2: Split B into 32 bit blocks
 L_i = leftmost 32 bits
 R_i = rightmost 32 bits.

Step 3: Pick a 56 bit key. Permute it

Step 4: Left circular shift it by 1 bit giving K_1 .

Digital Encryption Standard Algorithm

Step 5: Perform a complex sequence of operations and obtain $X_1 = F(R_1, K_1)$ (The complex set of operations include table look up and dropping bits).

Step 6: Find $R_2 = L_1 \oplus X_1$

Step 7: Set $L_2 = R_1$

Repeat steps 2 to 7 16 times to get $B_{16} = L_{16}, R_{16}$

Step 8: Apply inverse of initial permutation on B_{16}

The result is the encrypted block

Digital Encryption Standard Algorithm

- In summary the DES encryption applies the following transformation 16 times. The i^{th} round transformation are

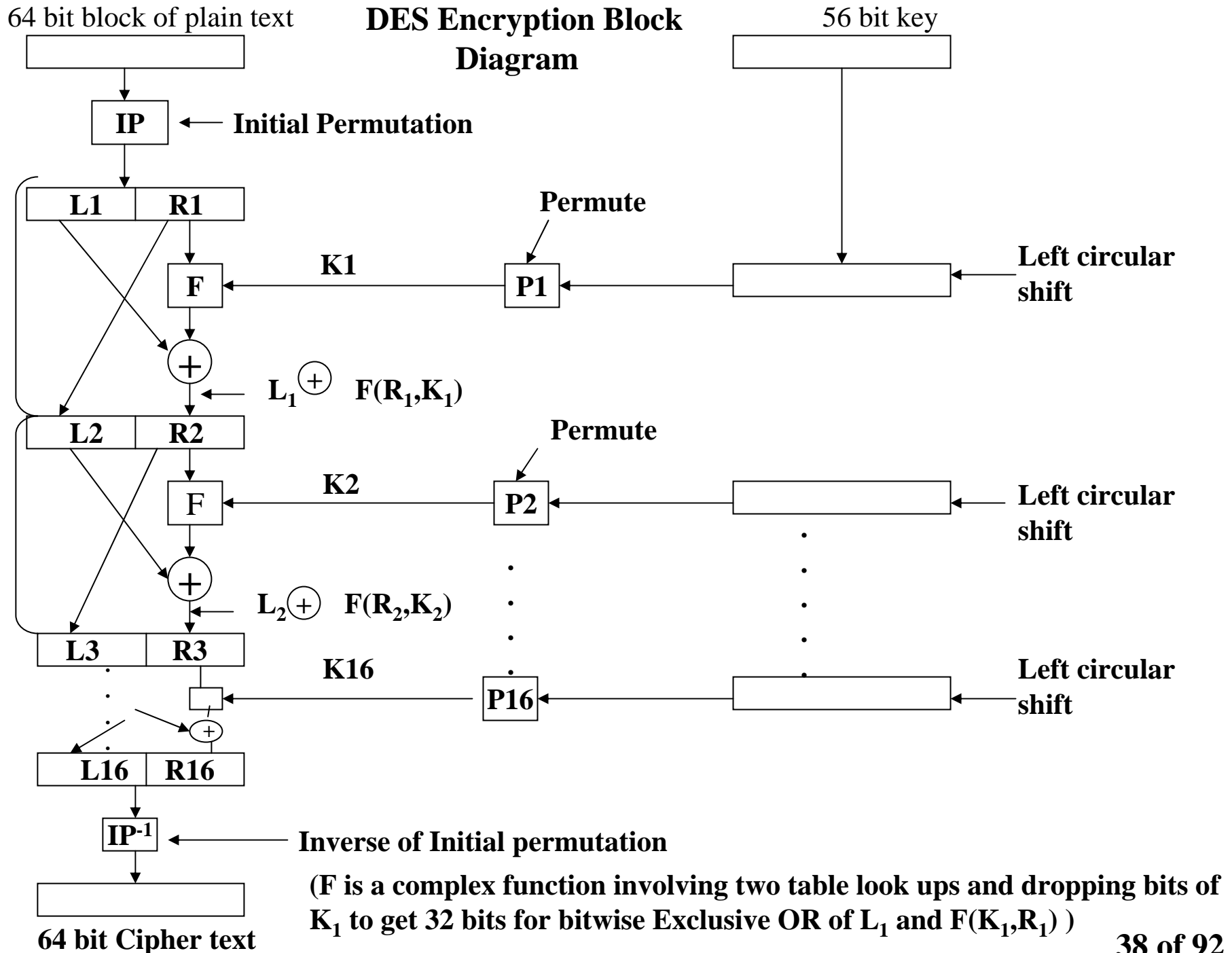
$$\begin{aligned}L_{i+1} &= R_i \\ R_{i+1} &= L_i \oplus F(R_i, K_i)\end{aligned}$$

- Each round has a different key K_i
- For Decryption the process of encryption is reversed. The encrypted block is permuted using IP^{-1} . On this transformations are applied starting with K_{16} and going to K_1 last. The keys and F are same as those used in encryption process.

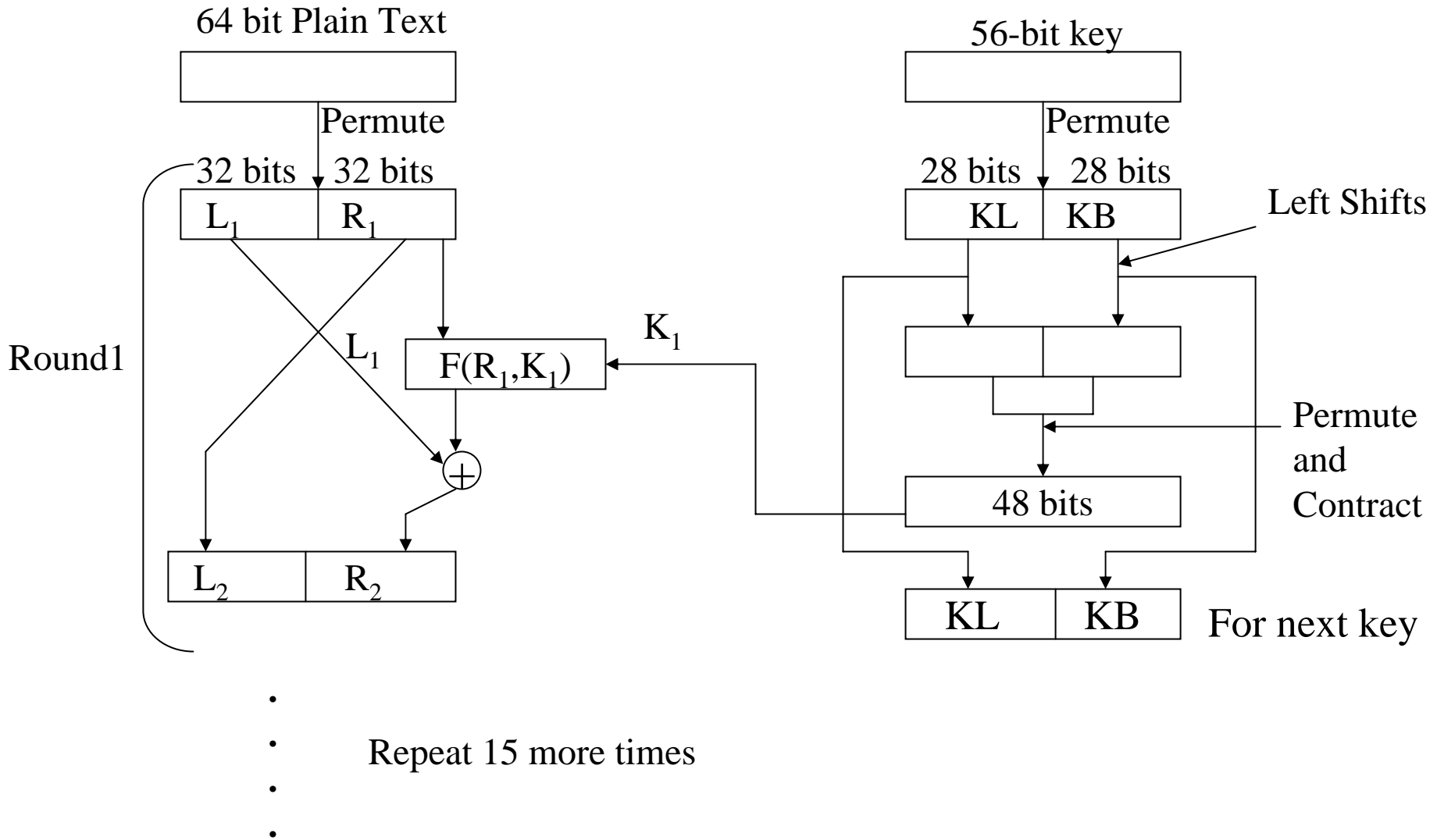
Digital Encryption Standard Algorithm

- The encryption process uses simple binary operations. They can thus be realised in hardware as an integrated circuit chip.
- DES chips are inexpensive. Key externally fed.
- The complex encryption algorithm is explained using two block diagrams in the next two transparencies.

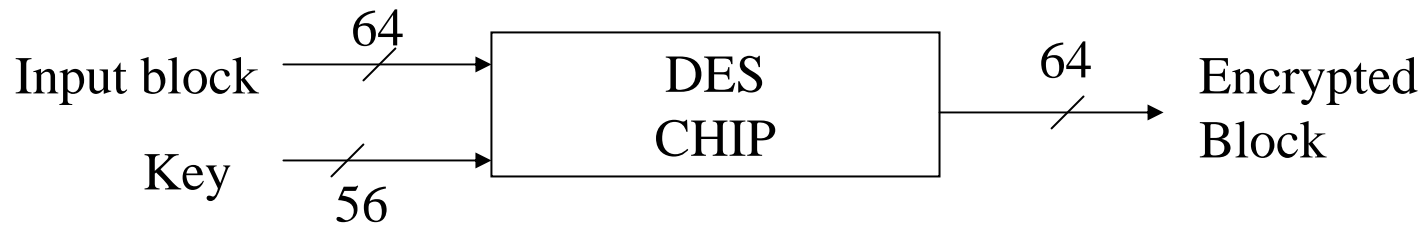
DES Encryption Block Diagram



Details of One Round of DES Encryption



DES Chip



- Observe that from initial key others are derived by circular shifts
- Decryption chip inputs encrypted block and key and the output is decrypted block

DES - Discussion

- Cryptanalysis is technique for breaking a code, given samples of encrypted messages.
- If plain text also known it is somewhat easier.
- DES code can be broken if key is found.
- The easiest method of breaking a code is by brute force of trying out all possible keys to decrypt message.

DES - Discussion

- With increase in speed of computers it has now been shown that DES key can be found in less than 12 hrs with a fast computer (1 Million decryption per microsecond)
- Thus DES is practically useless now (original DES was invented in mid 70s)
- New more secure symmetric encryption algorithm is needed
- An extension of DES called triple DES is shown to be more secure.

Triple DES

- Triple DES uses three different keys and three executions of DES algorithm.
- The algorithm is
Cipher text = $E_{k_3} [D_{k_2} [E_{k_1} [\text{Plain Text}]]]$
where $E_k[X]$ = DES Encryption of X using key K
and $D_k[X]$ = DES Decryption of X using key K
- Remember that in DES Decryption of encrypted plain text with a different key is almost same as another encryption.
- This is true as encryption and decryption use the same algorithm

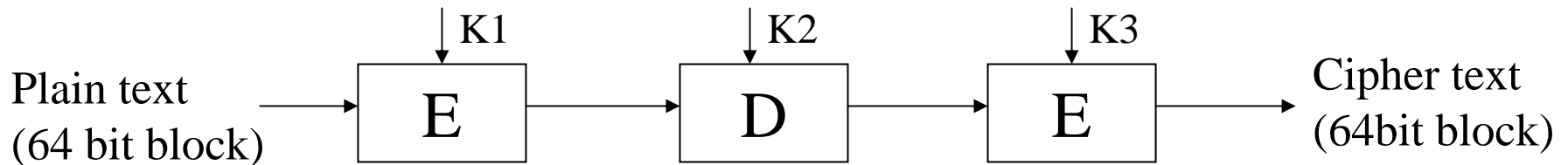
Triple DES

- To decrypt cipher text we reverse the operations.

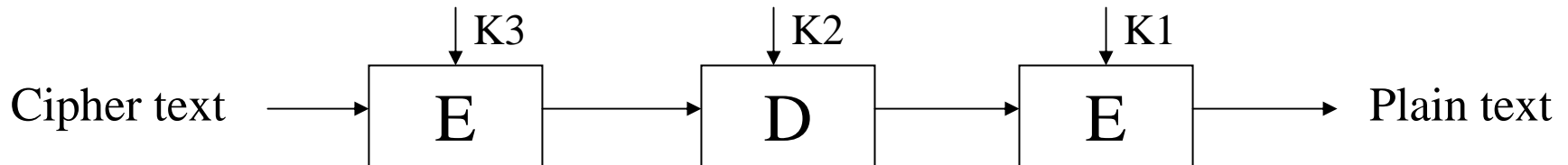
$$\text{Plain text} = D_{k_1}[E_{k_2}[D_{k_3}[\text{Cipher Text}]]]$$

BLOCK DIAGRAMS OF TRIPLE DES

Encryption



Decryption



Triple DES(Contd)

- Using DES thrice is equivalent to having a DES key length of 168 bits.
- Brute force method to break triple DES with 10^6 decrypts per micro second will take 5.9×10^{30} years!
- Even at 10^{12} fold increase in computer speed will make triple DES secure against brute force attacks to break code
- The only reason D is used as middle step in triple DES is to allow data encrypted using single DES hardware. In this case $K_3=K_2=K_1$ (Single key used) (See block diagram)

Triple DES(Contd)

- Triple DES will be quite popular for a foreseeable future as it is very secure, can be realised by simple hardware.
- Triple DES has two disadvantages
 1. It is slow to implement in software
 2. It uses 64 bit blocks.
- Thus new standards were explored.

Requirements of Symmetric Key Cryptography Algorithm(NIST) –Advanced Encryption System(AES)

- National Institute for Standards Technology put out a call for proposals for new crypto system with following requirements.
- Must provide a high level of security (i.e. difficult to decrypt in finite time)
- Must be completely specified and easily understood.
- Security must reside in key – Not in algorithm

Requirements of Symmetric Key Cryptography Algorithm(NIST) –Advanced Encryption System(AES)

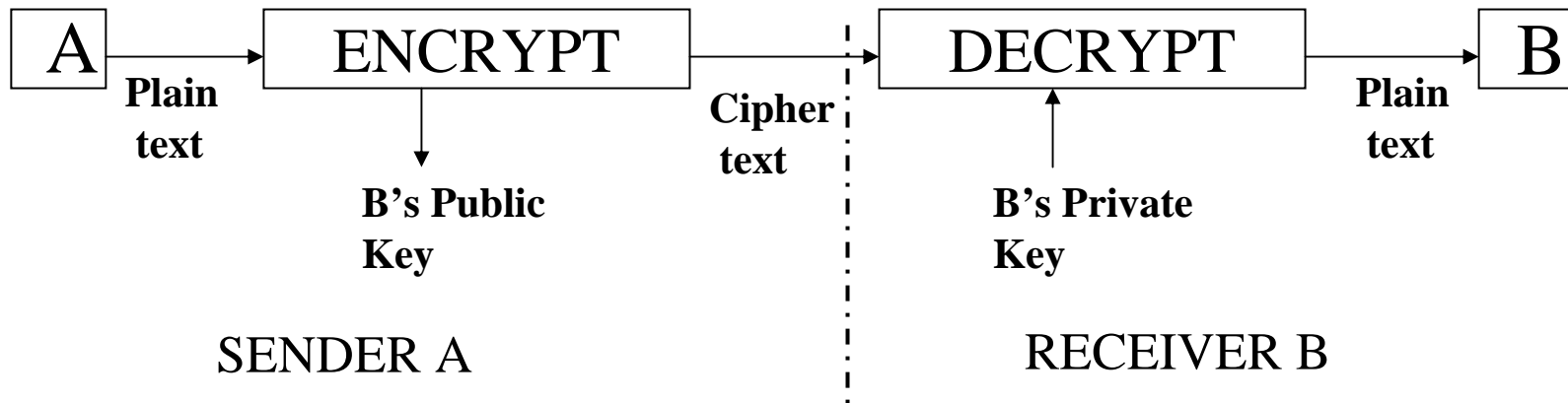
- Must be available for all users
- Adaptable for use in diverse applications e.g.credit cards
- Implementable economically in electronic devices
- Must be efficient to use as both software and hardware
- Must allow one to validate it.

Requirements of Symmetric Key Cryptography Algorithm(NIST) –Advanced Encryption System(AES)

- Must be exportable
- No trap door
- Must use 128 blocks and key lengths of 128,192 or 256 bits depending on the level of security desired.
- In October 2000 it announced the selection of an algorithm – called Rijin dael(Pronounce RAIN DOLL) as new Advance Encryption Standard (AES)
- Details may be found in www.nist.gov/aes

Public Key Encryption

- In Private Key Encryption transmission of key without compromising not easy
- It is necessary to assign different private key to each business partner. When this is done a directory of keys should be kept which should be secret. This is difficult.
- Only secure way is to change the private key every time a message is sent
- Public Key Encryption eliminates the key distribution problem
- There is a pair of keys for each organization - A Private Key and its Public Key
- If A wants to send message to B, A encrypts the message with B's Public Key
When message is received by B he decrypts it with his Private Key



RSA Code Details."R" Wants To Find His Public And Private Keys

1. Pick large primes p and q . Let $n = p * q$
- 2 Find $\phi = (p-1)*(q-1)$
- 3 Find e relatively prime to ϕ , i.e. $\gcd(\phi, e) = 1$; $1 < e < \phi$. $\{e, n\}$ is R's Public Key
- 4 Find a number d which satisfies relation
$$(d * e) \bmod (\phi) = 1$$
 $\{d, n\}$ is R's Private key

RSA Code Details.”R” Wants To Find His Public And Private Keys

5. Let plain text = t. Encrypt t using R’s public key.

$$\text{Encryption} = t^e \pmod{n} = c \text{ (cipher text)}$$

6. Decryption $c^d \pmod{n} = t$

(Both n and e should be known to encrypt. Similarly both n and d should be known to decrypt)

Example Of RSA Use

- This example is a toy example to illustrate the method. In practice the primes p and q will be very large – each at least 300 digits long to ensure security.

RSA Algorithm

1. Pick as prime numbers $p=3, q=11$

$$n = p * q = 33$$

Note : The message to be encrypted should be smaller than 33. If we do letter by letter encryption of English alphabets (A to Z \rightarrow 1 to 26) this is OK

2. $\phi = (p-1) \times (q-1) = 2 \times 10 = 20$

Example Of RSA Use

RSA Algorithm (Contd)

3. Pick a number relatively prime to 20.

We pick 7. The Public key of R = {7,33}

4. To pick private key of R find d from relation $(d \times e) \bmod(\phi) = 1$
 $(d \times 7) \bmod (20) = 1$

This gives $d = 3$

Therefore, the private key of R = {3,33}

Applying RSA Algorithm

1. Let the message be CODE

If we use code C=3, O=14, D=4, E=5

The message is 3,14,4,5

2. We will encrypt one letter at a time

Thus cipher of plain text 3 is

$$3^e \text{ mod } (n) = 3^7 \text{ mod } (33)$$

$$3^7 \text{ mod } (33) = 2187 \text{ mod } (33) = 9$$

$$(14)^7 \text{ mod } (33) = 105413504 \text{ mod } (33) = 20$$

$$(4)^7 \text{ mod } (33) = 16384 \text{ mod } (33) = 16$$

$$(5)^7 \text{ mod } (33) = 78125 \text{ mod } (33) = 14$$

3. Thus cipher text = 9,20,16,14

Applying RSA Algorithm

4. Decryption : $c^d \bmod (n)$ $d=3, n=33$

$$9^3 \bmod (33) = 729 \bmod(33) = 3$$

$$20^3 \bmod(33) = 8000 \bmod(33)=14$$

$$16^3 \bmod(33) = 4096 \bmod(33) =4$$

$$14^3 \bmod(33) = 2744 \bmod(33) =5$$

We see that we get the original text 3,14,4,5

Discussion on RSA

- The security RSA encryption is dependent on the fact that factorising a large prime number to its factors is very difficult.
- RSA algorithm is symmetric. In other words if a plain text is encoded by the private key of S, the sender, it can be decrypted using the public key of R, the receiver (We will find later that this symmetry property is used in creating digital signature)
- Example using S's keys
 - S's Private key = {3,33}
 - S's Public key = {7,33}

Discussion on RSA

- If we encrypt a plain text using S's private key and send it to R, R must be able to decrypt it with S's public key.
- Assume Plain text is encrypted with S's private key and get cipher text = $(14)^3 \bmod (33) = 5$
- Decrypting with S's Public key we get
$$\begin{aligned} & (5)^7 \bmod (33) \\ & = 78125 \bmod (33) \\ & = \{(2367 \times 33) + 14\} \bmod (33) \\ & = 14 \end{aligned}$$

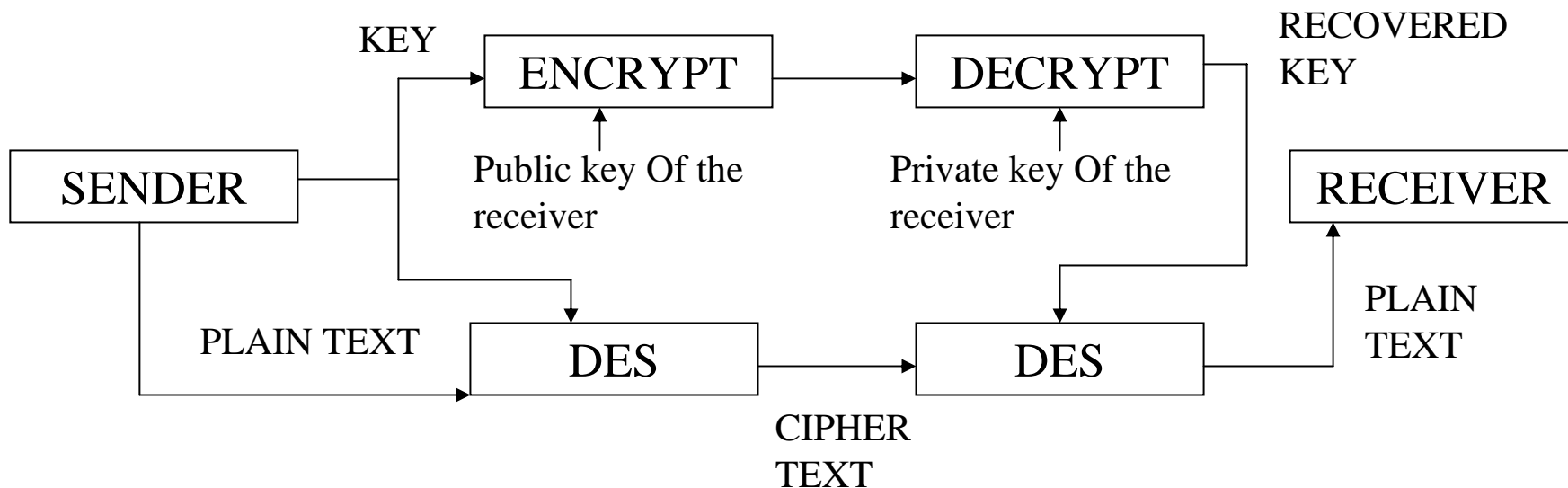
DISCUSSION – RSA Vs DES

- RSA Public key has two keys – a private secret key and a public open key.
- RSA implemented as a program (software) It is computationally complex to encode plain text and decode cipher text using RSA
- DES Same key for encryption and decryption It is a single key system - Also called symmetric key system

DISCUSSION – RSA Vs DES

- DES computationally simple-implemented in hardware - thus very fast
- Each communication between two businesses can use a different key –provided key is securely exchanged
- If key can be sent separately encrypted using RSA, then a recipient can use this to decrypt DES encrypted message.
- We look next at combining DES and RSA.

Combining RSA And DES



Advantages:

- Key is sent along with the plain text. Encrypted using RSA
- Key small-fast to encrypt/decrypt
- Each transaction using DES can have a different key- higher security and also fast.Key directory not needed.

Digital Signature

REQUIREMENTS

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

SENDING STEP

- Sender sends key using RSA system
- Sender sends plain text "M" using DES
- Receiver decrypts cipher text using DES and the key received from sender call it "MR"

Digital Signature

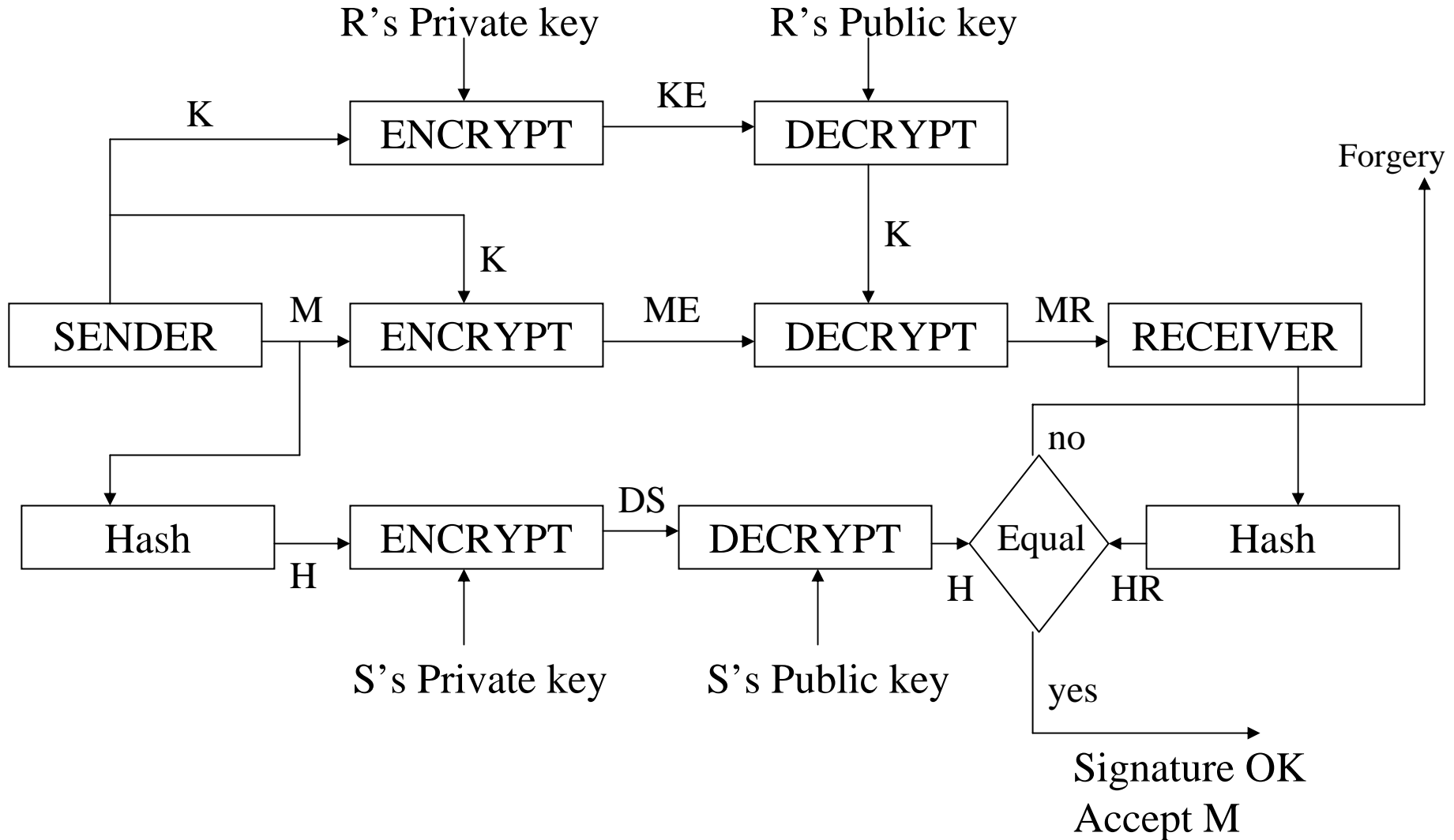
- Sender hashes plain text "M" using a hashing function - let the hashed text be "H"
- Hashed text "H" encrypted by sender using his Private key
- DS is his signature as H encrypted with his private key
- DS decrypted by receiver using sender's Public key and obtains "H"

Digital Signature (Contd)

Authentication step

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

Signing A Message Using Digital Signature



Certificate Authority For Digital Signature

- As the hashed message in Digital Signature system is decrypted using senders public key,this key must be certified as belonging to sender by an independent authority
- Certification needed to ensure authenticity of public keys of organizations as public key is used to verify signature
- Certification authority keeps data base of public keys of organizations participating in e-commerce after verifying their credentials.
- Potential business partners can authenticate public keys by sending request to certifying authority who certifies after receiving a fee for his services

Electronic Payment Systems

- In any commercial transaction payment is an integral part for goods supplied.
- Four types of payments may be made in e-commerce they are
 - Credit card payments
 - Electronic cheque payments
 - Micro or small payments for internet based services such as music download.
 - Electronic-cash payments

Each of these requires a different system of payment. We will examine first credit card payments.

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

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 and authorises sale based on customer's credit status.
- Acquirer accepts credit cards of several card companies and guarantees payment to merchants.
- Acquirer gets reimbursed by bank issuing credit card.

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

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

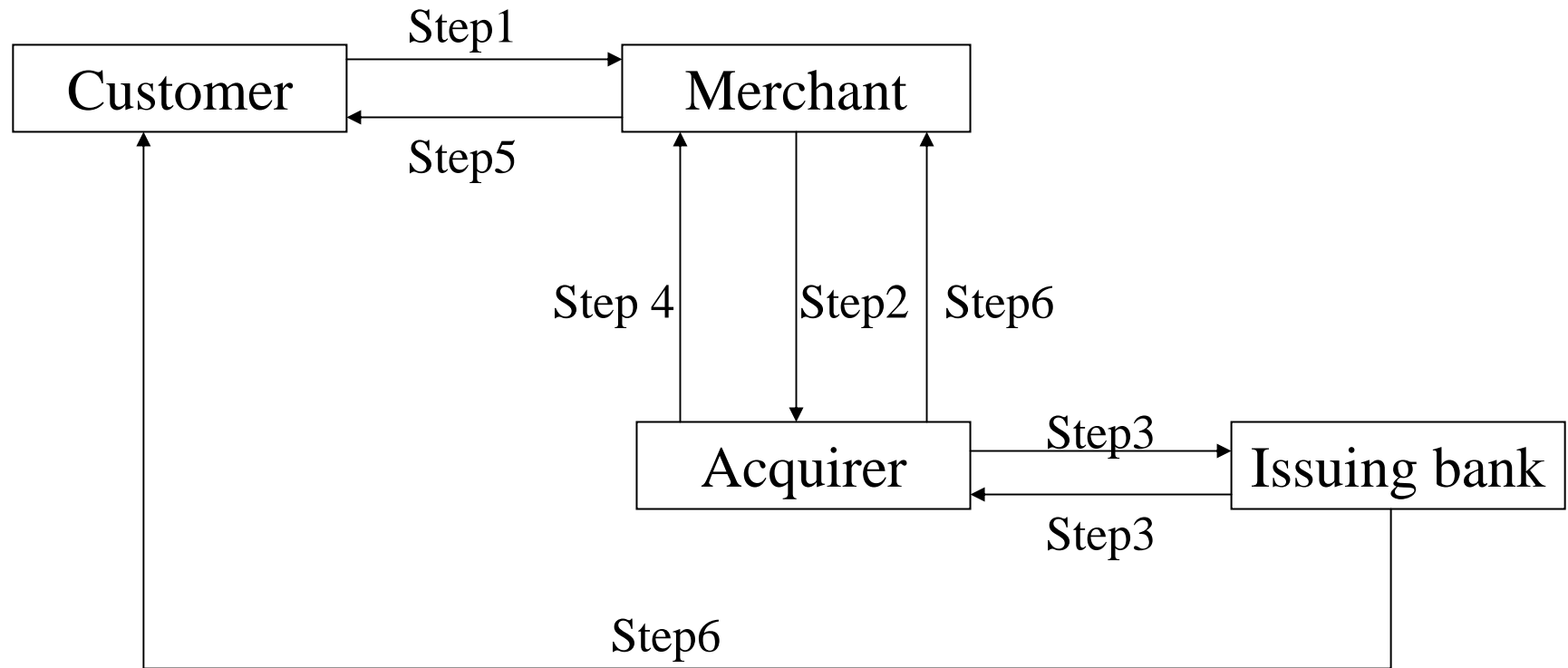
Sequence Of Transactions In Manual Credit Card Payment

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

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.

Block Diagram Of Steps In Credit Card Transaction



Steps correspond to that given in previous 2 PPT's

Credit Card In E-commerce

Main Problems

1. Main Problem is: if a merchant had only a web presence, a Customer needs to be reassured that the merchant is genuine.
2. Customers Signature cannot be physically verified. Customer needs electronic signature.
3. Secrecy of credit card number has to be ensured.
4. Dispute settlement mechanism must be worked out.

Secure Electronic Transaction Protocol

- Standardised credit card payments in e-commerce by major card companies such as Visa, MasterCard etc.
- 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.
 2. All parties have their public keys certified.
 3. A standard hashing algorithm is used to create message digest for signature verification.

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
- 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)

Secure Electronic Transaction Protocol

DUAL SIGNATURE SCHEME

- Dual signature scheme is an innovation in SET protocol

Steps followed in the protocol are:

1. Customer purchase information has 3 parts
 - (i) Purchase Order (PO)
 - (ii) Credit Card Number (CCN)
 - (iii) Amount to be paid
2. Merchant should know $(PO + \text{Amount}) = POA$
3. Acquirer should know $(CCN + \text{Amount}) = CCA$

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

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.

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

Secure Electronic Transaction Protocol

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

Secure Electronic Transaction Protocol

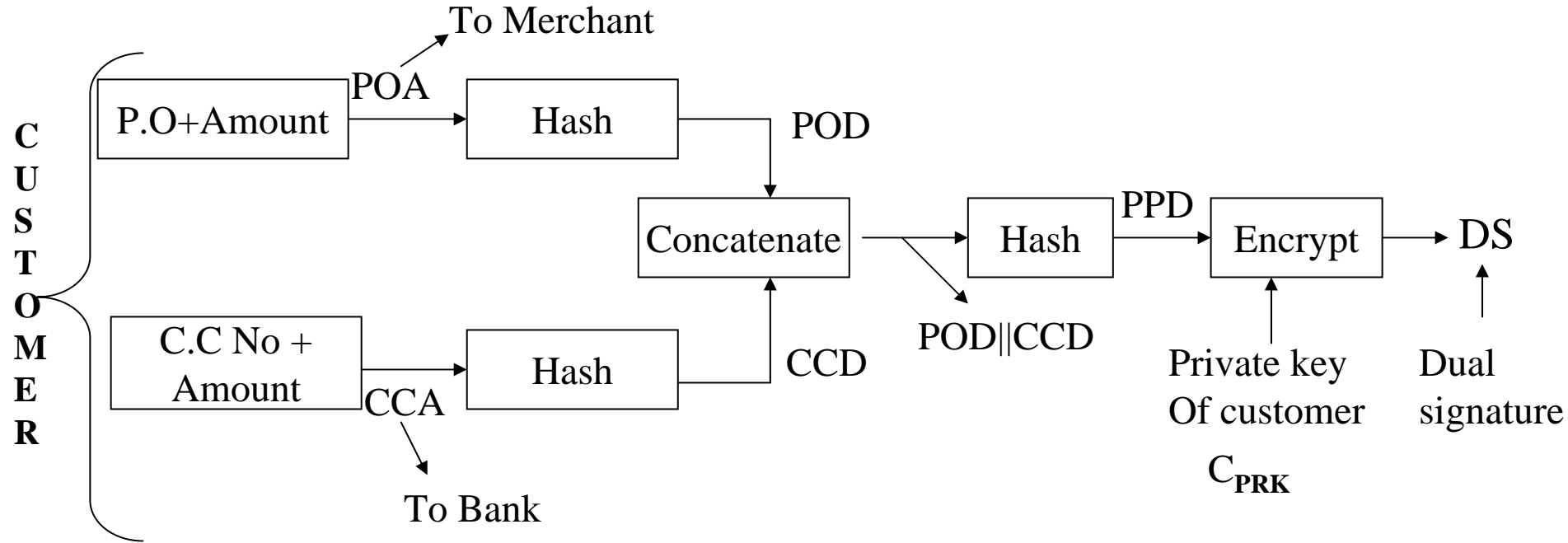
15. Acquirer's forwards to bank.

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.

17. Acquirer OK's transaction to merchant

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

Dual Signature System



POA: (Purchase Order + Amount)

POD: Purchase Order Digest

CCA: (Credit card + Amount)

CCD: (Credit card + Amount)Digest

|| : Concatenation operator which strings together POD and CCD

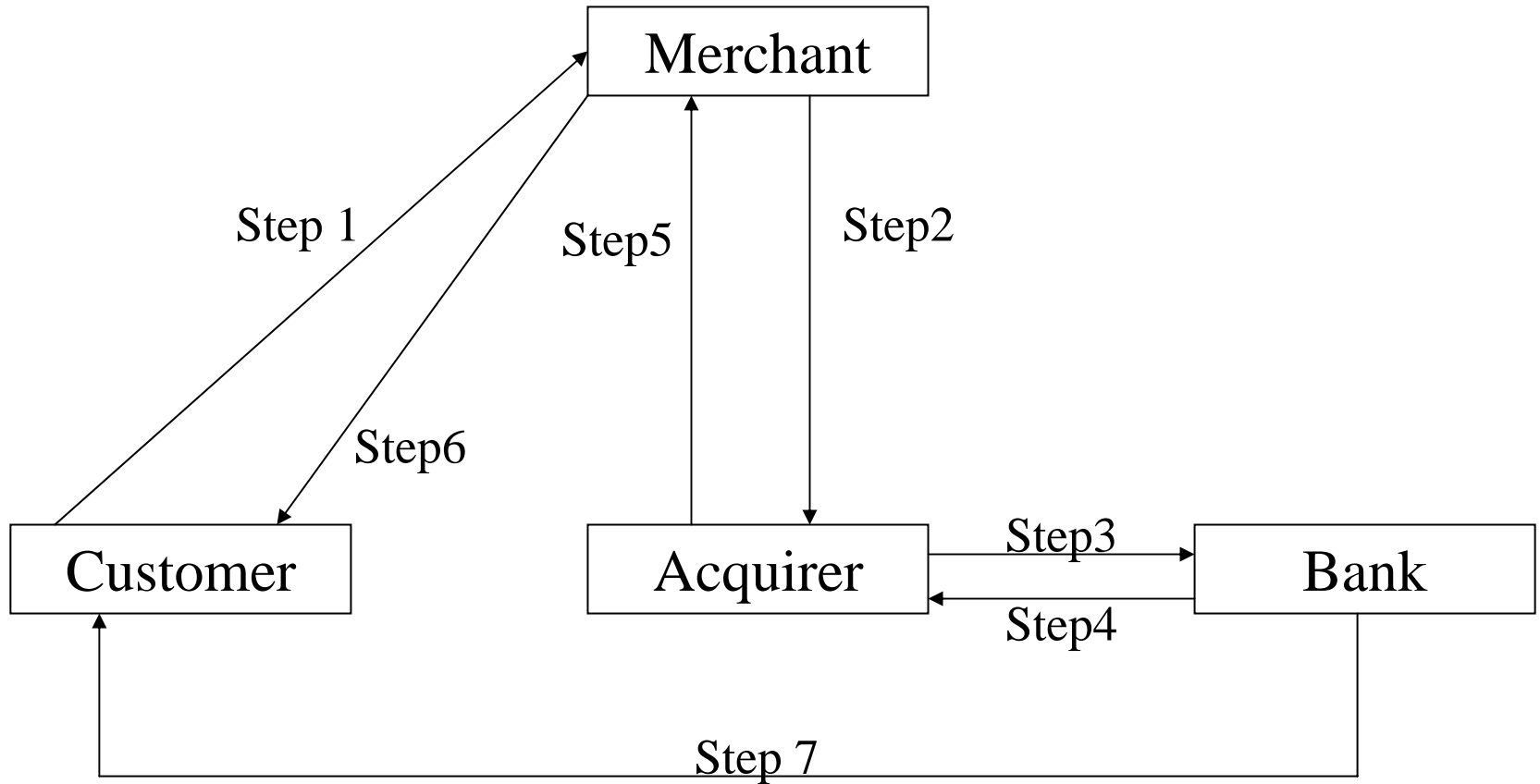
PPD : Purchase Payment Digest

C_{PRK} : Private Key of Customer

Secure Electronic Transaction Protocol

- Step1 : $[(POA)_{EM} + (CCA)_{EB} + CCD + DS]$ to Merchant
- Step2 : Merchant sends $[(CCA)_{EB} + DS + POD]$ to Acquirer
- Step3 : Acquirer sends $(CCA)_{EB} + DS + POD$ to Bank.
- Bank finds (CC No. + amount) sees if OK
Computes $H(CCD || POD)$
Decrypts DS with customer's public key
If $(DS)_{CPK} = H(CCD || POD)$ Signature verified
- Step4 : OK to acquirer if credit and signature OK
- Step5 : Ok to Merchant
Merchant finds $H(H(POA) || CCD) = PPD$
Decrypts DS with public key of customer. If match signature verified.
- Step6 : Sends delivery details
- Step7 : Bill to customer

Secure Electronic Transaction Protocol



Secure Electronic Transaction Protocol

Step1: Customer fills Purchase order, amount and credit card number in his PC. A software in PC strips it into two parts Purchase Order + Amount (POA), Credit Card No. + Amount(CCA)

POA is encrypted using merchants.

Public key and CCA with bank's public key. These are sent with customer's public key certificates, CCD and DS. Merchant verifies DS.

Step2: Merchant forwards to acquirer DS and CCD (These are encrypted using acquirer's public key)

Step3: Acquirer forwards to bank. Bank decrypts CCA with its private key. Checks validity of credit card and balance. If OK informs acquirer

Secure Electronic Transaction Protocol

Step4: Acquirer OK's transaction to merchant and credits merchant's account.

Step5: Merchant accepts customer's order and proceeds to dispatch items.

Step6: At the end of the month bank sends bill to customer.

(All these done by clicks of mouse button)

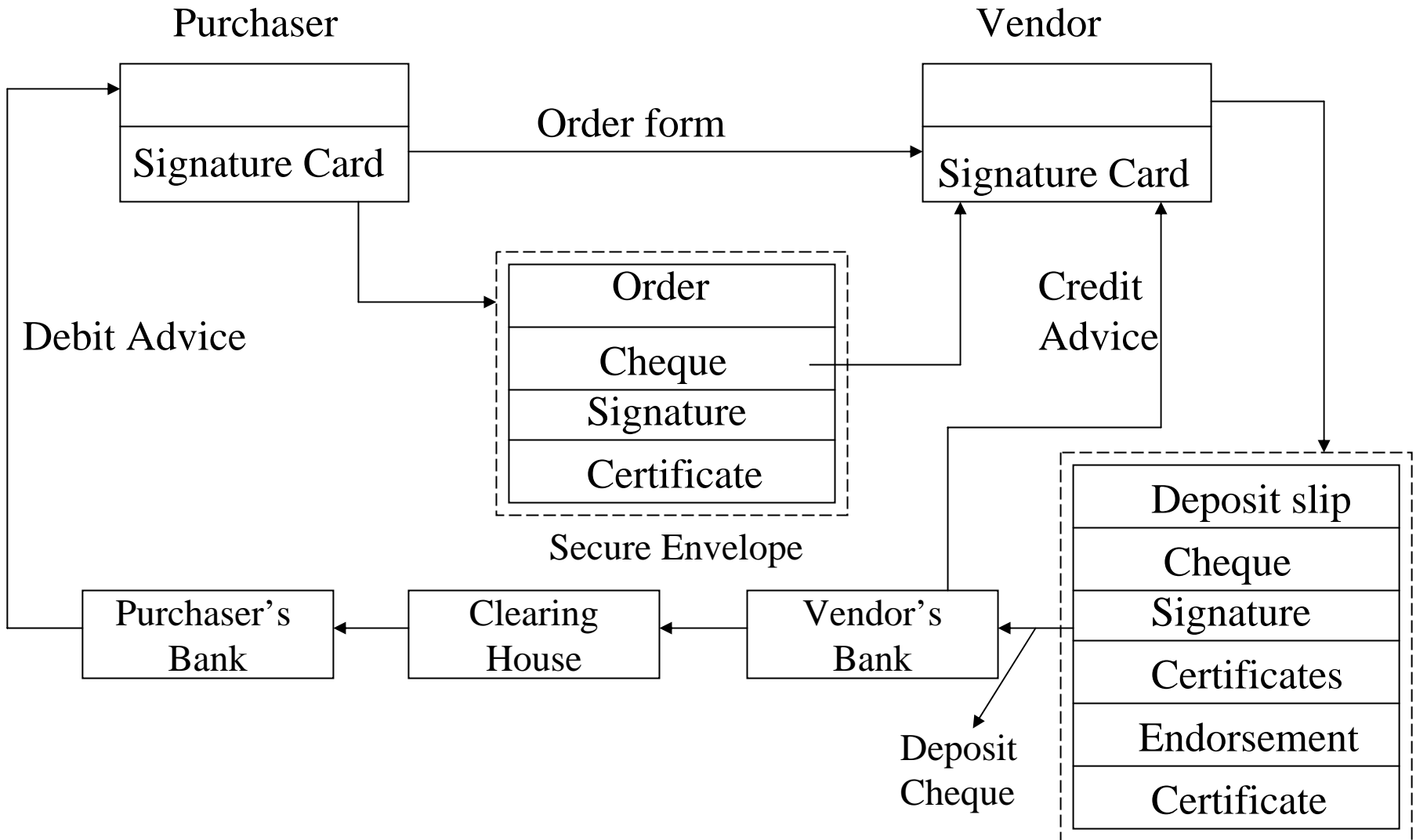
Electronic Cheque Payment

- Most cheque based transactions will be between businesses -thus special hardware attached to PC's for signing payments
- Signature encrypted by hardware
- All public keys of business partners authenticated by certifying agencies

Steps in transaction

- 1 Purchaser sends purchase order and payment advice signed with his private key to vendor. He also sends his public key certificate encrypted with vendor's public key to vendor
- 2 Vendor decrypts with his private key, checks certificate and cheque, attaches deposit slip, encrypts with bank's public key and sends it to bank. he also sends his public key certificate
- 3 Bank checks signatures, credits and clears cheque
- 4 Credit advice goes to vendor, & consolidated debit advice sent to purchaser periodically

Clearing Cheque Payment Electronically



Payments Of Small Amounts On Internet

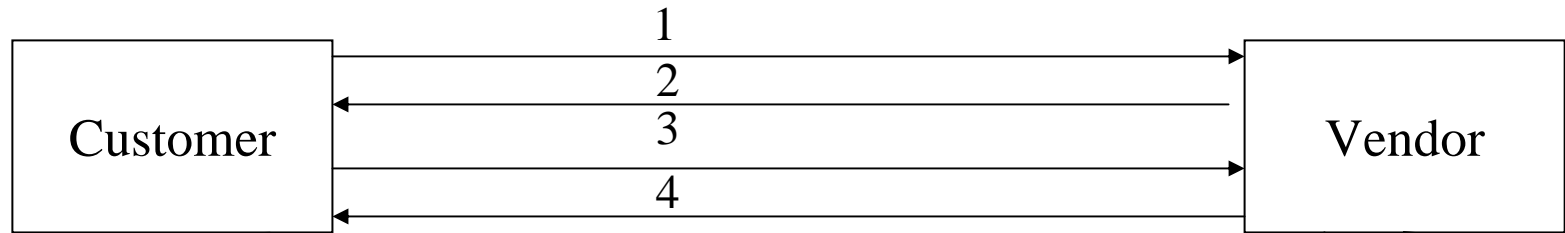
NETBILL'S PROPRIETARY SYSTEM

- Customer charged only when information delivered
- Vendor guaranteed payment when information delivered
- Netbill is the intermediary

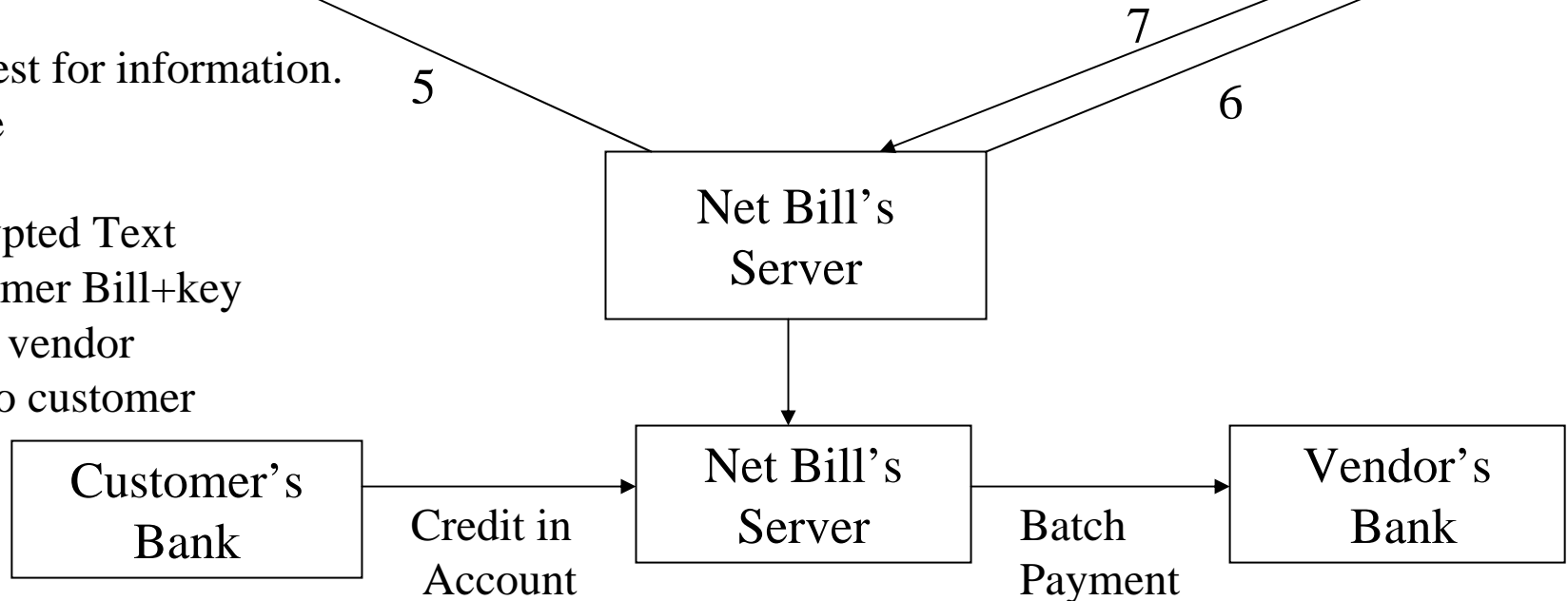
MAJOR STEPS

- When customer accepts quote for information, vendor sends encrypted information without key to customer
- Payment order sent to vendor with checksum of information obtained. It is signed by customer
- Vendor sends to NET BILL copy of purchase order and the key for decryption
- NET BILL checks credit of customer. If ok it sends key to customer. Credits vendor account and debits customer account. Key sent to customer to decrypt information
- Customer decrypts information

Paying for Small Internet Transactions



1. Request for information.
2. Quote
3. Order
4. Encrypted Text
5. Customer Bill+key
6. Ok to vendor
7. Key to customer



Electronic Cash

- Cash for small payments
- Cash preserves anonymity
- Cash should not be traceable

We will discuss only traceable cash payments

STEPS

1.Customer withdraws coins in various denominations signed by bank

STRUCTURE-----> serial no, denomination, signature of bank

Bank stores issued coins copy

2.Customer pays vendor using signed coins

3.Bank checks whether it is current or spent

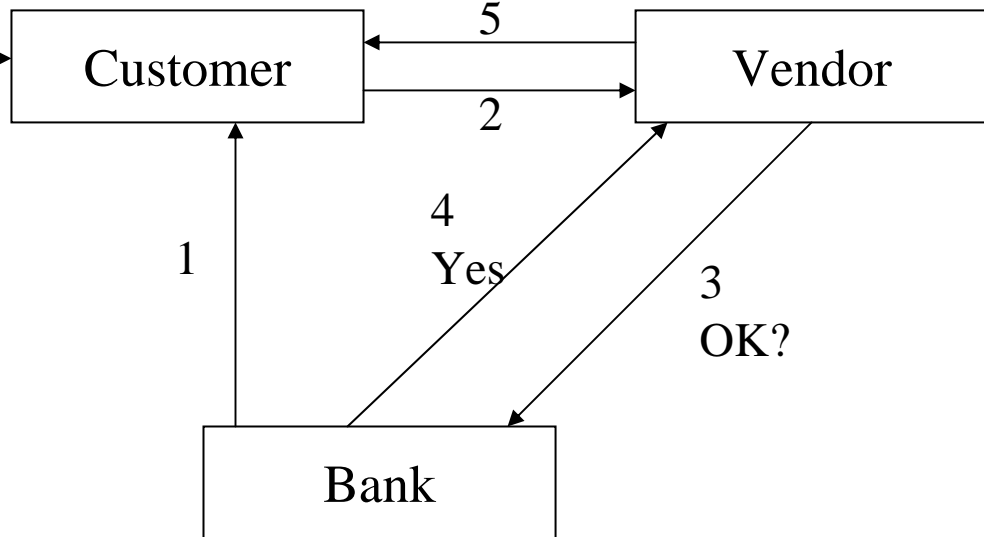
4.If current it authorises dispatch of goods and credits vendor account with electronic coins

Electronic Cash(contd)

- Cheaper than credit card transaction
- DES normally used for these transaction as it is cheap and amounts involved is small

Electronic Cash Payment

Amt	ID	Signature
10	1568	86ABC
5	6789	86ABC



1. Withdraw
2. Pay
3. Check if OK
4. Replying OK
5. Accept order

Spent	Coins
Amt	ID
.	.
.	.