Learning Objectives

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.
- 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
Electronic Commerce

13.1 What is E-Commerce?
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

LAN of business2
Vendor
Local computers

Public switched telephone network

LAN of business1

Vendor
Local computers

Purchase
store
accounts
Business To Business E-commerce (contd.)

- 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
Steps In B2C E-commerce

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

Customer1

Wants to sell Item 1

Internet

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

Customer2

Wants to buy Item 1
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 paralise 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

<table>
<thead>
<tr>
<th>LOGICAL LAYERS</th>
<th>SERVICES IN LAYER</th>
</tr>
</thead>
<tbody>
<tr>
<td>Middleman services</td>
<td>Hosting services, value added nets, payment services, Certificates</td>
</tr>
<tr>
<td>Secure messaging</td>
<td>Encryption, EDI, Firewalls</td>
</tr>
<tr>
<td>World wide web services</td>
<td>HTTP, HTML, XML, OLE, Software agents</td>
</tr>
<tr>
<td>Logical network</td>
<td>Intranet, internet, extranet</td>
</tr>
<tr>
<td>Physical network</td>
<td>PSTN, LAN, Bridges, routers</td>
</tr>
</tbody>
</table>

*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 (contd.)

- 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
Security In E-commerce

- 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 unauthorized 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
Proxy Application Gateway

• 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 databases 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

Block plaintext (5-character blocks)

Transpose characters with permutation (4 1 2 5 3)

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

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

The keys are permutation function and substitution function

This Is A Message

Thisi Sames SAGEX

4 → 1

Sthii Esasm Esaxg

Wxlmm Iwewq Ixebk

Cipher Text
Symmetric Encryption.

PLAINTEXT  \((m_1,m_2…m_n)\)

CIPHER TEXT  \((c_1 c_2, c_3….c_n)\)

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 ⊕ K     11000011  11110100  10000001 encryption
M = E ⊕ 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.
Digital Encryption Standard Algorithm

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

$Li =$ leftmost 32 bits

$Ri =$ rightmost 32 bits.

Step 3: Pick a 56 bit key. Permute it
Digital Encryption Standard Algorithm

Step 4: Left circular shift it by 1 bit giving K1.

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).
Digital Encryption Standard Algorithm

Step 6: Find $R_2 = L_1 + X_1$

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

$$L_{i+1} = R_i$$

$$R_{i+1} = L_i \oplus F(R_i, K_i)$$

• 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.
64 bit block of plain text

- **Initial Permutation**

- **Round 1**
  - **L1** \( \rightarrow \) **R1**
  - **F**
  - **L1** + \( F(R_1, K_1) \)

- **Round 2**
  - **L2** \( \rightarrow \) **R2**
  - **F**
  - **L2** + \( F(R_2, K_2) \)

- **...**

- **Round 16**
  - **L16** \( \rightarrow \) **R16**
  - **F**
  - **L16** + \( F(R_{16}, K_{16}) \)

- **Inverse of Initial permutation**

- **64 bit Cipher text**

**DES Encryption Block Diagram**

- **IP**
- **P1**
- **P2**
- **P16**

**56 bit key**

- **Left circular shift**

(F is a complex function involving two table lookups and dropping bits of \( K_1 \) to get 3 bits for bitwise Exclusive OR of \( L_1 \) and \( F(K_1, R_1) \) )
Details of One Round of DES Encryption

64 bit Plain Text

32 bits

L₁

Permute

32 bits

R₁

F(R₁,K₁)

K₁

L₂

R₂

Round1

56-bit key

Permute

28 bits

KL

KB

28 bits

Permute

48 bits

Left Shifts

Permute and Contract

For next key

Repeat 15 more times
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 a technique for breaking a code, given samples of encrypted messages.
- If plain text is also known, it is somewhat easier.
- DES code can be broken if the key is found.
- The easiest method of breaking a code is by brute force, trying out all possible keys to decrypt the 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 = \( E_{k3} \left[ D_{k2} \left[ E_{k1} \left[ \text{Plain Text} \right] \right] \right] \)

where \( E_k[X] = \text{DES Encryption of } X \text{ using key } K \) and \( D_k[X] = \text{DES Decryption of } X \text{ using key } K \)

• 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.
  Plain text = $D_{k1}[E_{k2}[D_{k3}[\text{Cipher Text}]])$

Block Diagrams Of Triple Des

Encryption

Plain text (64 bit block) → $E$ → $D$ → $E$ → Cipher text (64 bit block)

Decryption

Cipher text → $E$ → $D$ → $E$ → Plain text
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 $5.9 \times 10^{30}$ years!
- Even at $10^{12}$ fold increase in computer speed will make triple DES secure against brute force attacks to break code.
Triple DES (Contd)

- 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 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

- Public Key Encryption eliminates the key distribution problem
- There is a pair of keys for each organization - A's 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
Public Key Encryption

A → ENCRYPT → B

<table>
<thead>
<tr>
<th>A</th>
<th>ENCRYPT</th>
<th>B</th>
<th>Plain text</th>
<th>Cipher text</th>
</tr>
</thead>
<tbody>
<tr>
<td>Plain text</td>
<td>B’s Public Key</td>
<td>Cipher text</td>
<td>B’s Private Key</td>
<td>Plain text</td>
</tr>
</tbody>
</table>

SENDER A → ENCRYPT → RECEIVER B
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 $\varphi = (p-1)*(q-1)$
3. Find e relatively prime to $\varphi$, i.e. gcd($\varphi$, e) = 1; 1 < e < $\varphi$.
   \{e, n\} is R's Public Key
RSA Code Details.”R” Wants To Find His Public And Private Keys

4. Find a number d which satisfies relation
   \[(d * e) \mod (\phi) = 1\]
   \{d,n\} is R’s Private key

5. Let plain text = t. Encrypt t using R’s public key.
   Encryption = \(t^e \mod n = c\) (cipher text)

6. Decryption \(c^d \mod n = t\)

(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 $p=3, q=11$
   
   $n = p \times q = 33$

   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 \((d \times e) \mod (\varphi) = 1\)
   \((d \times 7) \mod (20) = 1\)
   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
   \[ 3^e \mod (n) = 3^7 \mod(33) \]
   \[ 3^7 \mod (33) = 2187 \mod (33) = 9 \]
   \[ (14)^7 \mod (33) = 105413504 \mod(33) = 20 \]
   \[ (4)^7 \mod (33) = 16384 \mod (33) = 16 \]
   \[ (5)^7 \mod (33) = 78125 \mod(33) = 14 \]
Applying RSA Algorithm

3. Thus cipher text = 9, 20, 16, 14
4. Decryption: \[ c^d \mod (n) \]
\[ d=3, n=33 \]
\[ 9^3 \mod (33) = 729 \mod (33) = 3 \]
\[ 20^3 \mod (33) = 8000 \mod (33) = 14 \]
\[ 16^3 \mod (33) = 4096 \mod (33) = 4 \]
\[ 14^3 \mod (33) = 2744 \mod (33) = 5 \]
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 = $(14)^3 \mod (33) = 5$
• Decrypting with S’s Public key we get

$$(5)^7 \mod (33)$$

$= 78125 \mod (33)$$

$= ((2367 \times 33) + 14) \mod (33)$$

$= 14$$
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

Sender

Plain Text

DES

Encrypt

Public Key Of the Receiver

Recovered Key

Plain Text

DES

Decrypt

Private Key Of the Receiver

Receiver

Cipher Text
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

Sender

M → Hash → ENCRYPT → S’s Private key → K → ENCRYPT → S’s Private key → DS → ENCRYPT → S’s Public key → ME → DECRYPT → R’s Public key → KE → DECRYPT → R’s Private key → K → Hash → Equal → no → Forgery

Signature OK

Accept M
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
Certificate Authority For Digital 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

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

2. Secrecy of credit card number has to be ensured.
3. 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 + Amount) = POA

3. Acquirer should know (CCN + 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

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

\( C_{PRK} \) 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.

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 $H(POD||CCD)$

   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.
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

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

- Step 1: \([(\text{POA})_{\text{EM}} + (\text{CCA})_{\text{EB}} + \text{CCD} + \text{DS}]\) to Merchant

- Step 2: Merchant sends \([(\text{CCA})_{\text{EB}} + \text{DS} + \text{POD}]\) to Acquirer

- Step 3: Acquirer sends \((\text{CCA})_{\text{EB}} + \text{DS} + \text{POD}\) to Bank.

- Bank finds (CC No. + amount) sees if OK

  Computes \(H(\text{CCD} || \text{POD})\)

  Decrypts DS with customer’s public key

  If \((\text{DS})_{\text{CPK}} = H(\text{CCD} || \text{POD})\) Signature verified
Secure Electronic Transaction Protocol

- Step 4: OK to acquirer if credit and signature OK
- Step 5: Ok to Merchant
- Merchant finds $H(H(POA) \ || \ CCD)=PPD$
- Decrypts DS with public key of customer. If match signature verified.
- Step 6: Sends delivery details
- Step 7: Bill to customer
Secure Electronic Transaction Protocol

1. Customer 
2. Merchant
3. Acquirer
4. Bank

Steps:
- Step 1
- Step 2
- Step 3
- Step 4
- Step 5
- Step 6
- Step 7
Secure Electronic Transaction Protocol

Step 1: 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.

Step 2: Merchant forwards to acquirer DS and CCD (These are encrypted using acquirer’s public key).

Secure Electronic Transaction Protocol

Step 4: Acquirer OK’s transaction to merchant and credits merchant's account.

Step 5: Merchant accepts customer’s order and proceeds to dispatch items.

Step 6: 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
Electronic Cheque Payment

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

- Purchaser
  - Signature Card
  - Order form
  - Debit Advice
  - Purchaser’s Bank

- Vendor
  - Signature Card
  - Credit Advice
  - Deposit slip
  - Cheque
  - Signature
  - Certificates
  - Endorsement
  - Certificate
  - Vendor’s Bank

- Clearing House
  - Secure Envelope
  - Order
  - Cheque
  - Signature
  - Certificate

- Depositing Cheque
  - Clearing House
  - Purchaser’s Bank
  - Vendor’s Bank

Flowchart Diagram:

- Signature Card
- Order form
- Debit Advice
- Purchaser’s Bank
- Secure Envelope
- Cheque
- Signature
- Certificate
- Credit Advice
- Deposit slip
- Cheque
- Signature
- Certificates
- Endorsement
- Certificate
- Vendor’s Bank
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
Payments Of Small Amounts On Internet

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
Electronic Cash (contd.)

**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

<table>
<thead>
<tr>
<th>Amt</th>
<th>ID</th>
<th>Signature</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>1568</td>
<td>86ABC</td>
</tr>
<tr>
<td>5</td>
<td>6789</td>
<td>86ABC</td>
</tr>
</tbody>
</table>

### Diagram

1. **Customer**
   - **Vendor**
   - **Bank**

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

### Transaction Details

<table>
<thead>
<tr>
<th>Spent</th>
<th>Coins</th>
</tr>
</thead>
<tbody>
<tr>
<td>Amt</td>
<td>ID</td>
</tr>
<tr>
<td>.</td>
<td>.</td>
</tr>
<tr>
<td>.</td>
<td>.</td>
</tr>
</tbody>
</table>
13.1 By Electronic Commerce we mean:
   a. Commerce of electronic goods
   b. Commerce which depends on electronics
   c. Commerce which is based on the use of internet
   d. Commerce which is based on transactions using computers connected by telecommunication network

13.2 For carrying out B2B e-Commerce the following infrastructure is essential:
   (i) World Wide Web
   (ii) Corporate network
   (iii) Electronic Data Interchange standards
   (iv) Secure Payment Services
   (v) Secure electronic communication link connecting businesses
   a. i, ii, iii
   b. ii, iii, iv
   c. ii, iii, iv, v
   d. i, ii, iii, iv, v

13.3 For carrying out B2C e-Commerce the following infrastructure is essential
   (i) World Wide Web
   (ii) Corporate network
   (iii) Electronic Data Interchange standards
   (iv) Secure Payment Services
   (v) Secure electronic communication link connecting businesses
   a. i, iv
   b. i, iii, iv
   c. ii, iii
   d. i, ii, iii, iv

13.4 For carrying out C2C e-Commerce the following infrastructure is essential
   (i) World Wide Web
   (ii) Corporate network
   (iii) Electronic Data Interchange standards
   (iv) Secure Payment Services
   (v) Secure electronic communication link connecting businesses
   a. i and ii
13.5 Advantages of B2C commerce are

(i) Business gets a wide reach to customers
(ii) Payment for services easy
(iii) Shop can be open 24 hours a day seven days a week
(iv) Privacy of transaction always maintained

a. i and ii  
b. ii and iii  
c. i and iii  
d. iii and iv

13.6 B2C commerce

a. includes services such as legal advice  
b. means only shopping for physical goods  
c. means only customers should approach customers to sell  
d. means only customers should approach business to buy

13.7 Advantages of B2C commerce to customers are

(i) wide variety of goods can be accessed and comparative prices can be found  
(ii) shopping can be done at any time  
(iii) privacy of transactions can be guaranteed  
(iv) security of transactions can be guaranteed

a. i and ii  
b. ii and iii  
c. iii and iv  
d. i and iv

13.8 Disadvantages of e-Commerce in India are

(i) internet access is not universally available  
(ii) Credit card payment security is not yet guaranteed  
(iii) Transactions are de-personalized and human contact is missing  
(iv) Cyberlaws are not in place

a. i and ii
13.9 Electronic Data Interchange is necessary in
   a. B2C e-Commerce
   b. C2C e-Commerce
   c. B2B e-Commerce
   d. Commerce using internet

13.10 EDI requires
   a. representation of common business documents in computer readable forms
   b. data entry operators by receivers
   c. special value added networks
   d. special hardware at co-operating Business premises

13.11 EDI standards are
   a. not universally available
   b. essential for B2B commerce
   c. not required for B2B commerce
   d. still being evolved

13.12 EDIFACT is a standard
   a. for representing business forms used in e-Commerce
   b. for e-mail transaction for e-Commerce
   c. for ftp in e-Commerce
   d. protocol used in e-Commerce

13.13 EDIFACT standard was developed by
   a. American National Standard Institute
   b. International Standard Institute
   c. European Common Market
   d. United Nations Economic Commission for Europe

13.14 ANSI X.12 is a standard developed by
   a. American National Standard Institute
   b. International Standard Institute
   c. European Common Market
   d. United Nations Economic Commission for Europe
13.15 In B2B e-Commerce

(i) Co-operating Business should give an EDI standard to be used
(ii) Programs must be developed to translate EDI forms to a form accepted by application program
(iii) Method of transmitting/receiving data should be mutually agreed
(iv) It is essential to use internet

a. i, ii
b. i, ii, iii
c. i, ii, iii, iv
d. ii, iii, iv

13.16 EDI use

a. requires an extranet
b. requires value added network
c. can be done on internet
d. requires a corporate intranet

13.17 EDI over internet uses

a. MIME to attach EDI forms to e-mail messages
b. FTP to send business forms
c. HTTP to send business forms
d. SGML to send business forms

13.18 For secure EDI transmission on internet

a. MIME is used
b. S/MIME is used
c. PGP is used
d. TCP/IP is used

13.19 EDI standard

a. is not easily available
b. defines several hundred transaction sets for various business forms
c. is not popular
d. defines only a transmission protocol

13.20 By security in e-Commerce we mean

(i) Protecting an organization’s data resource from unauthorized access
(ii) Preventing disasters from happening
(iii) Authenticating messages received by an organization

(iv) Protecting messages sent on the internet from being read and understood by unauthorized persons/organizations

a.  i, ii  

b.  ii, iii  

c. iii, iv  

d. i, iii, iv

13.21 A firewall is a

a. wall built to prevent fires from damaging a corporate intranet  

b. security device deployed at the boundary of a company to prevent unauthorized physical access  

c. security device deployed at the boundary of a corporate intranet to protect it from unauthorized access  

d. device to prevent all accesses from the internet to the corporate intranet

13.22 A firewall may be implemented in

a. routers which connect intranet to internet  

b. bridges used in an intranet  

c. expensive modem  

d. user’s application programs

13.23 Firewall as part of a router program

a. filters only packets coming from internet  

b. filters only packets going to internet  

c. filters packets travelling from and to the intranet from the internet  

d. ensures rapid traffic of packets for speedy e-Commerce

13.24 Filtering of packets by firewall based on a router has facilities to

a. i, iii  

b. i, ii, iii  

c. i, ii, iii, iv  

d. ii, iii, iv

13.25 Main function of proxy application gateway firewall is

a. to allow corporate users to use efficiently all internet services  

b. to allow intranet users to securely use specified internet services  

c. to allow corporate users to use all internet services
13.26 **Proxy application gateway**

(i) acts on behalf of all intranet users wanting to access internet securely

(ii) monitors all accesses to internet and allows access to only specified IP addresses

(iii) disallows use of certain protocols with security problems

(iv) disallows all internet users from accessing intranet

a. i, ii  
   b. i, ii, iii  
   c. i, ii, iii, iv  
   d. ii, iii, iv

13.27 **A hardened firewall host on an intranet**

(i) has a proxy application gateway program running on it

(ii) allows specified internet users to access specified services in the intranet

(iii) initiates all internet activities requested by clients and monitors them

(iv) prevents outsiders from accessing IP addresses within the intranet

a. i, ii  
   b. i, ii, iii  
   c. i, ii, iii, iv  
   d. ii, iii, iv

13.28 **A hardened firewall host on an Intranet is**

a. a software which runs in any of the computers in the intranet

b. a software which runs on a special reserved computer on the intranet

c. a stripped down computer connected to the intranet

d. a mainframe connected to the intranet to ensure security

13.29 **By encryption of a text we mean**

a. compressing it

b. expanding it

c. scrambling it to preserve its security

d. hashing it

13.30 **Encryption is required to**

(i) protect business information from eavesdropping when it is transmitted on internet

(ii) efficiently use the bandwidth available in PSTN

(iii) to protect information stored in companies’ databases from retrieval
(iv) to preserve secrecy of information stored in databases if an unauthorized person retrieves it
   a. i and ii
   b. ii and iii
   c. iii and iv
   d. i and iv

13.31 Encryption can be done
   a. only on textual data
   b. only on ASCII coded data
   c. on any bit string
   d. only on mnemonic data

13.32 By applying permutation (31254) and substitution by 5 characters away from current character (A → F, B → G etc.) the following string ABRACADABRA becomes
   a. FGWCAAADRBVF
   b. RABCAAADRBVF
   c. WFGHFFFFWGF
   d. None of the above

13.33 The following ciphertext was received. The plaintext was permuted using permutation (34152) and substitution. Substitute character by character +3 (A → D, etc). The plain text after decryption is: Cipher text : PDLJDLXHVQC
   a. MAIGAIUESNZ
   b. IAMAGENIUSZ
   c. LDPDJHPLXVZ
   d. IAMAGENIUSC

13.34 By symmetric key encryption we mean
   a. one private key is used for both encryption and decryption
   b. private and public key used are symmetric
   c. only public keys are used for encryption
   d. only symmetric key is used for encryption

13.35 The acronym DES stands for
   a. Digital Evaluation System
   b. Digital Encryption Standard
13.36 **DES works by using**
   a. permutation and substitution on 64 bit blocks of plain text
   b. only permutations on blocks of 128 bits
   c. exclusive ORing key bits with 64 bit blocks
   d. 4 rounds of substitution on 64 bit blocks with 56 bit keys

13.37 **DES**
   (i) is a symmetric key encryption method
   (ii) guarantees absolute security
   (iii) is implementable as hardware VLSI chip
   (iv) is a public key encryption method
   a. i and ii
   b. ii and iii
   c. i and iii
   d. iii and iv

13.38 **DES using 56 bit keys**
   a. Cannot be broken in reasonable time using presently available computers
   b. Can be broken only if the algorithm is known using even slow computers.
   c. Can be broken with presently available high performance computers.
   d. It is impossible to break ever.

13.39 **Triple DES uses**
   a. 168 bit keys on 64-bit blocks of plain text
   b. Working on 64-bit blocks of plain text and 56 bit keys by applying DES algorithm for three rounds.
   c. Works with 144 bit blocks of plain text and applies DES algorithm once.
   d. Uses 128 bit blocks of plain text and 112 bit keys and apply DES algorithm thrice.

13.40 **ripple DES**
   a. Cannot be broken in reasonable time using presently available computers.
   b. Can be broken only if the algorithm is known using even slow computer.
   c. Can be broken with presently available high performance computers.
   d. It is impossible to break ever.
13.41 **Triple DES**
   a. is a symmetric key encryption method
   b. guarantees excellent security
   c. is implementable as a hardware VLSI chip
   d. is public key encryption method with three keys.

13.42 **Public key encryption method is a system**
   a. which uses a set of public keys one for each participant in e-Commerce
   b. in which each person who wants to communicate has two keys; a private key known to him only and a public key which is publicized to enable others to send message to him.
   c. which uses the RSA coding system.
   d. which is a standard for use in e-Commerce.

13.43 **Public key system is useful because**
   a. it uses two keys.
   b. there is no key distribution problem as public key can be kept in a commonly accessible database.
   c. private key can be kept secret.
   d. it is a symmetric key system.

13.44 **In public key encryption if A wants to send an encrypted message**
   a. A encrypts message using his private key
   b. A encrypts message using B’s private key
   c. A encrypts message using B’s public key
   d. A encrypts message using his public key

13.45 **In public key encryption system if A encrypts a message using his private key and sends it to B**
   a. if B knows it is from A he can decrypt it using A’s public key
   b. Even if B knows who sent the message it cannot be decrypted
   c. It cannot be decrypted at all as no one knows A’s private key
   d. A should send his public key with the message

13.46 **Message can be sent more securely using DES by**
   a. encrypting plain text by a different randomly selected key for each transmission
b. encrypting plain text by a different random key for each message transmission and sending the key to the receiver using a public key system
c. using an algorithm to implement DES instead of using hardware
d. designing DES with high security and not publicizing algorithm used by it

13.47 **DES and public key algorithm are combined**
(i) to speed up encrypted message transmission
(ii) to ensure higher security by using different key for each transmission
(iii) as a combination is always better than individual system
(iv) as it is required in e-Commerce
   a. i and ii
   b. ii and iii
   c. iii and iv
   d. i and iv

13.48 **A digital signature is**
   a. a bit string giving identity of a correspondent
   b. a unique identification of a sender
   c. an authentication of an electronic record by tying it uniquely to a key only a sender knows
   d. an encrypted signature of a sender

13.49 **A digital signature is required**
(i) to tie an electronic message to the sender’s identity
(ii) for non repudiation of communication by a sender
(iii) to prove that a message was sent by the sender in a court of law
(iv) in all e-mail transactions
   a. i and ii
   b. i, ii, iii
   c. i, ii, iii, iv
   d. ii, iii, iv

13.50 **A hashing function for digital signature**
(i) must give a hashed message which is shorter than the original message
(ii) must be hardware implementable
(iii) two different messages should not give the same hashed message
(iv) is not essential for implementing digital signature
13.51 **Hashed message is signed by a sender using**
   a. his public key  
   b. his private key  
   c. receiver’s public key  
   d. receiver’s private key

13.52 **While sending a signed message, a sender**
   a. sends message key using public key encryption using DES and hashed message using public key encryption  
   b. sends message using public key encryption and hashed message using DES  
   c. sends both message and hashed message using DES  
   d. sends both message and hashed message using public key encryption

13.53 **The responsibility of a certification authority for digital signature is to authenticate the**
   a. hash function used  
   b. private keys of subscribers  
   c. public keys of subscribers  
   d. key used in DES

13.54 **Certification of Digital signature by an independent authority is needed because**
   a. it is safe  
   b. it gives confidence to a business  
   c. the authority checks and assures customers that the public key indeed belongs to the business which claims its ownership  
   d. private key claimed by a sender may not be actually his

13.55 **The Secure Electronic Transaction protocol is used for**
   a. credit card payment  
   b. cheque payment  
   c. electronic cash payments  
   d. payment of small amounts for internet services
13.56 In SET protocol a customer encrypts credit card number using
   a. his private key
   b. bank’s public key
   c. bank’s private key
   d. merchant’s public key

13.57 In SET protocol a customer sends a purchase order
   a. encrypted with his public key
   b. in plain text form
   c. encrypted using Bank’s public key
   d. using digital Signature system

13.58 One of the problems with using SET protocol is
   a. the merchant’s risk is high as he accepts encrypted credit card
   b. the credit card company should check digital signature
   c. the bank has to keep a database of the public keys of all customers
   d. the bank has to keep a database of digital signatures of all customers

13.59 The bank has to have the public keys of all customers in SET protocol as it has to
   a. check the digital signature of customers
   b. communicate with merchants
   c. communicate with merchants credit card company
   d. certify their keys

13.60 In electronic cheque payments developed, it is assumed that most of the transactions will be
   a. customers to customers
   b. customers to business
   c. business to business
   d. banks to banks

13.61 In cheque payment protocol, the purchase order form is signed by purchaser using
   a. his public key
   b. his private key
   c. his private key using his signature hardware
   d. various public keys
13.62 In the NetBill’s protocol for small payments for services available in the internet.
(i) the customer is charged only when the information is delivered
(ii) the vendor is guaranteed payment when information is delivered
(iii) the customer must have a certified credit card
(iv) the customer must have a valid public key
a. i, ii
b. i, ii, iii
c. i, ii, iii, iv
d. i, ii

13.63 In NetBill’s protocol for small payments for internet services
(i) Key to decrypt information is sent to customer by NetBill only when there is enough amount in debit account
(ii) The vendor supplies the key to NetBill server when he receives payment
(iii) Checksum of encrypted information received by customer is attached to his payment order
(iv) Vendor does not encrypt information purchased by customer
a. i, ii
b. i, ii, iii
c. i, ii, iii, iv
d. i, ii, iv

13.64 In Electronic cash payment
a. a debit card payment system is used
b. a customer buys several electronic coins which are digitally signed by coin issuing bank
c. a credit card payment system is used
d. RSA cryptography is used in the transactions

13.65 In Electronic cash payment
(i) a customer withdraws “coins” in various denominations signed by the bank
(ii) the bank has a database of issued coins
(iii) the bank has a database of spent coins
(iv) the bank cannot trace a customer
a. i, ii
b. i, ii, iii
Multiple Choice Questions

c. i, ii, iii, iv

d. ii, iii, iv
Key to Objective Questions

13.1 d  13.2 c  13.3 a  13.4 c  13.5 c  13.6 a
13.7 a  13.8 c  13.9 c  13.10 a  13.11 b  13.12 a
13.13 d  13.14 a  13.15 b  13.16 c  13.17 a  13.18 b
13.25 b  13.26 b  13.27 c  13.28 b  13.29 c  13.30 d
13.31 c  13.32 c  13.33 b  13.34 a  13.35 b  13.36 a
13.44 c  13.45 a  13.46 b  13.47 a  13.48 c  13.49 b  13.50 c
13.51 b  13.52 a  13.53 c  13.54 c
13.55 a  13.56 b  13.57 d  13.58 c  13.59 a  13.60 c
13.61 c  13.62 d  13.63 b  13.64 b  13.65 b
SUMMARY OF MODULE 13

1. The sharing of business information, maintaining business relationships and conducting business transactions by using telecommunication networks is usually defined as Electronic Commerce.

2. E-commerce is normally categorised as Business to Business (B2B), Business to Customer (B2C) and Customer to Customer (C2C).

3. The major advantages of E-Commerce are anytime, anywhere transaction, reduction in cost of transactions, reduction in time to market products, faster inter-business transaction and faster transfer of funds.

4. The major disadvantages of E-commerce are poor security of transactions unless special precautions are taken, loss of privacy, lack of legislation to settle disputes and menace of hackers.

5. E-Commerce architecture consists of the following layers:
   The lowest layer in the physical network which may be a LAN connected by unshielded twisted pair wires, Public Switched Telephone Networks, WAN using optical fibre etc. The next layer is the logical network such as internet, intranet and extranet (all of which use TCP/IP protocol). Resting on this is the world wide web and services on it such as web pages, browsers, and search engines. Above this is the security layer which deals with encryption, digital signatures etc. Resting on this are Electronic Data Interchange and Electronic payment services. All these layers are necessary to write application systems.

6. At the physical level most organizations use local area networks using unshielded twisted pair cables and Ethernet protocol. The cheapest method of interconnecting organizations is to use Public Switched Telephone Network.
7. Internet is the most important logical network which enables E-Commerce. The internet protocol called TCP/IP is universally used. Organizational private networks which use TCP/IP protocol are called intranets. Organizational intranets are often connected by a private secure communication link. Such a network is called an Extranet.

8. World wide web is a global multimedia information service available on the internet. It supports web pages prepared using hyper text markup language.

9. Web pages are located using a scheme known as Universal Resource Locator (URL) which is its address. Web browsers are used to locate web pages.

10. Web pages are created using a language known as hypertext markup language (HTML). Words can be picked and tagged to connect the page with other related pages.

11. It is imperative for every organization to have a website in today's internet world which publicise their functions. The page must be attractively designed and updated regularly.

12. Electronic Data Interchange (EDI) is essential in E-Commerce. EDI replaces printed forms by a standard electronic format which can be interpreted correctly by computer programs of cooperating businesses.

13. EDI standards have been published by American Network National Standards Institute and by United Nations Economic Commission for Europe. The United Nations standard is called EDIFACT and may become the standard for international commerce.

14. Value Added Network Services provide electronic post boxes to their clients to exchange EDI documents. They guarantee security and delivery of documents.
They also provide services to convert an organization's forms to standard format such as EDIFACT.

15. If internet is used for exchanging business documents Secure Multipurpose Internet Mail Extension (S/MIME) standard is recommended.

16. An organization's intranet is connected to the internet via a proxy server or a hardware unit. This is called a firewall. Firewall protects an organization's computers from unauthorized intruders.

17. Messages exchanged between organizations using the internet can be easily tapped by eavesdroppers. It is thus necessary to scramble them to prevent eavesdroppers from understanding the messages. It is done by encrypting messages.

18. Message (plain text) is encrypted by transposing characters of the plain text by a specified permutation and substituting characters by other characters. The encrypted text is called ciphertext.

19. This general idea is used in a standard encryption method called Digital Encryption Standard (DES). DES encrypts 64 bit blocks with a 56 bit key.

20. DES has been implemented as a hardware device. DES hardware may be attached to a computer's output port so that messages sent from the computer are encrypted. The receiver can decrypt it if he is given the key.

21. A system in which the encrypting and decrypting keys are same is called a symmetric key system.

22. The main problem with a symmetric key system is the need to distribute the key securely to all participating businesses. Symmetric key encryption/decryption is fast.

23. Two key based system called RSA system does not require distributing secret keys.
It has two keys for each participant in the communication, a private key and a public key. If A wants to send a message to B, A encrypts the message using B's public key. B decrypts it using his private key. Thus there is no key distribution problem. It is, however, slower than the symmetric key system.

24. RSA system is based on the fact that it is difficult to factor two prime components from their product, particularly, when the prime numbers are large.

25. In RSA system, a message encrypted with a private key, can be decrypted with the corresponding public key. This is used in digital signature.

26. In order to sign a message the sender hashes the message with a known algorithm to get a message digest MD. MD is encrypted with the sender's private key and sent to the intended receiver. Let us call it MDₐ. The message itself is encrypted with a symmetric key and sent. The recipient decrypts the message and computes the message digest MD using the known hashing algorithm. He then decrypts the encrypted message digest MDₐ using the sender's public key. If (MDₑ) decrypted = MD then the message is not a forgery as only the sender knows his private key. This signature ties the signature to the message and cannot be repudiated by the sender.

27. To ensure that public keys of organizations do belong to them there are certification authorities which check the legitimacy of organizations and issue public key certificates.

28. In E-Commerce payments are made as credit card payments, cheque payments or cash payments. Besides this a system to make small payments for information goods (such as files, books etc.) downloaded from the internet is needed.

29. Credit card payments are made using a protocol called Secure Electronic
Transaction (SET protocol). It uses RSA system and digital signatures.

30. Cheque payments are made between organizations using digitally signed cheques and public key certificates issued by a certifying authority.

31. Payment for small transactions is made using digital coins issued by banks to customer after debiting the customer's account. A digital coin consists of amount, identification number and banks signature. These coins are given in exchange for goods. The bank reimburses the vendor after checking its signature and ensuring that the coin has not been spent earlier.

32. A system called NetBill has been proposed for small payment for information services on the internet. It ensures that a key is given to a customer for decrypting information only after payment is received by the vendor. It also guarantees delivery of contracted information by the vendor.
Worked Examples

13.1 Explain B2B e-Commerce using an example of a book distributor who stocks a large number of books, which he distributes via a large network of book sellers. Assume that the distributor has stocks of books of a large number of publishers and book sellers order books as and when their stock is low.

Distributors give 1 month’s time to booksellers for payment

13.2 Explain B2C e-Commerce of a customer reserving airline tickets from his home or place of work.

B2C e-Commerce involves the business between an individual and an organization.

For the case given in question, the customer has to visit the site of the travel agency or a broker and get the status of the availability of tickets. If ticket is
available he/she will book the ticket and input the credit card details. He/She will be given the details of delivery of ticket. The block diagram below depicts the total process.

13.3 **Explain C2C e-Commerce with an appropriate example**

Here the selling and purchasing is carried out between two individuals. One is a seller and the other is a buyer. The items are usually used items, collector's items such as stamps/coins or antiques. The seller posts the description of the item and the expected price of the item on a web site maintained by a company which acts as a middle man or broker.

For example: Consider a company Y which acts as a broker. Suppose an individual A has to sell some items, so it will post the description of the items in Y’s site. A person B is interested to purchase some items, then he/she will visit Y’s site.

Here we can have three cases.

**Case I:**
The broker Y can just acts as an advertising agency and make the two persons meet each other and carry out further transaction. For this it gets some commission from both the parties.

This is described in the block diagram below:
Case II:
The broker Y can act as an advertising agency, make the two persons negotiate the price. Then Y takes all responsibilities until the item is delivered. For this it gets some commission from both the parties.

This is described in the block diagram below:
The broker Y can act as an advertising agency and displays items posted by the seller with prices. Both the buyer and seller will not have knowledge of each other. Y takes all responsibilities until the item is delivered. For this he gets some commission from both the parties.

This is described in the block diagram below:

13.4 What do you understand by EDI? Is EDI used in B2C or B2B e-Commerce? Why is EDI important in e-Commerce?

EDI stands for Electronic Data Interchange. It is a standard electronic format used for purchase orders, invoices etc. When such electronic forms are received they can be interpreted correctly by recipient's computer program and used.

EDI is used in B2B e-Commerce. It is important in e-Commerce because there is no manual intervention and data transfer is faster. As the format is agreed between two organizations, communication is simple.
13.5 What is VAN? What services do VANs provide? What are the advantages and disadvantages of VAN?
VAN stands for Value Added Networks which provide services to Businesses which are members.
VANs provide post boxes for each of its subscribers who want to use their services. Some VANs provide conversion of forms to standard EDI format. The disadvantage of VAN services is high cost.

13.6 Why is security important in e-Commerce? What are the security issues to be taken into account while designing a security system for e-Commerce?
Since in e-Commerce the transaction and communication takes place between two entities using PSTN, security issue is important.
The different security issues that are taken into account, while designing a security system for e-Commerce are given below:
- As internet connects several networks one has to be sure that unauthorised persons do not gain access to the company’s confidential information. Both hardware and software solutions are needed to ensure this.
- The communication between companies should be protected from snoopers.
- When a company receives a message, it must be sure from whom it has come. In electronic communication system there should be digital signature so that the receiver knows that it has come from an authorised business. It should also ensure that the authentication of digital signature must be maintainable in a court of law in case of disputes.

13.7 What is a firewall? What are the functions of a firewall?
A firewall is a set of related programs, located at a network gateway server that protects the resources of private network from other networks. Basically firewall, working closely with a router program, filters all network packets to determine whether to forward them toward their destination.
The different functions of firewall are:
- Protection from vulnerable service
- Control access to site system
- Concentrated security
- Enhance privacy
- Logging and statistics on Network use and misuse

13.8 What is a hardened firewall host? What are its functions? In what way is it different from proxy application gateway?
The hardened firewall is a computer that will require inside or outside users to connect to the trusted applications in it before connecting to external world. The major functions of hardened firewall are:
- Security processes are concentrated on one machine
- Names of systems on LAN, e-mail address etc., are hidden from outsiders
- Network service management is simplified by locating services such as ftp, e-mail, search engines etc., in the firewall machine.
The difference between hardened firewall and proxy application gateway is that for hardened firewall the inside or outside users are required to connect to the trusted application in firewall machine before connecting to any machine. All the information will pass through this computer, hence it is more secure.

13.9 Given a plain text:

THIS IS A SAMPLE SENTENCE FOR ENCRYPTION.

Apply the permutation (231564) and the substitution: (letter \( \rightarrow \) letter + 6 ) and obtain the cipher text.

Step 1: write the message in block of 6 characters

THISIS ASAMPLE SESENTE NCEFOR ENCRYPTION

Step 2: follow permutation(231564)

HITISS AAPMLE SEETE NCEYPR TION

Step 3: make substitution (Letter \( \rightarrow \) Letter + 6)

NOZOYY YGGVRS YKKZKT IKTUXL TIKEVXZOUT

13.10 What is DES? Explain what DES does when the following hexadecimal plain text is input to a DES hardware.

A1907FBCD986543201FED14E890ABCA5

DES is a symmetric cryptographic algorithm. It is a block cipher, and encrypts data in 64-bit blocks. The same algorithm and key are used for both encryption and decryption.

The key length is 56 bits. The key is usually expressed as a 64-bit number, but every eighth bit is used for parity checking and is ignored. These parity bits are the least-significant bits of the key bytes.

After the initial permutation, the block is broken into a right half and a left half, each 32 bits long. Then there are 16 rounds of identical operations, called Function f, in which the data are combined with the key. After the sixteenth round, the right and left halves are joined, and a final permutation (the inverse of the initial permutation) finishes off the algorithm.

In each round as shown in the figure (page 210) the key bits are shifted, and then 48 bits are selected from the 56 bits of the key. The right half of the data is expanded to 48 bits, combined with 48 bits of a shifted and permuted key via an XOR, then again converted to 32 new bits, and permuted again. These four operations make up Function f. The output of Function f is then combined with the left half via another XOR. The result of these operations becomes the new right half; the old right half becomes the new left half. These operations are repeated 16 times, making 16 rounds of DES.

If \( B_i \) is the result of the \( i \)th iteration, \( L_i \) and \( R_i \) are the left and right halves of \( B_i \), \( K_i \) is the 48-bit key for round \( i \), and \( f \) is the function and does all the substituting and permuting and XORing with the key, then a round looks like:

\[
L_i = R_{i-1}
\]

\[
R_i = L_{i-1} \oplus f(R_{i-1}, K_i)
\]

For more information on DES please refer to book “APPLIED CRYPTOGRAPHY” written by Bruce Schneier.
13.11 What do you understand by symmetric key cryptography? What are the main advantages and disadvantages of symmetric key cryptography?
The cryptography in which the same key is used for encryption and decryption and known to both parties while exchanging information is known as symmetric key or private key cryptography.

The disadvantage of this method is, the difficulty in securely distributing the keys to authorised parties.

13.12 What is public key encryption? In what way is it different from private key encryption? Why is it important in e-Commerce?
The encryption in which two keys are used for encryption and decryption is called public key encryption. One of these keys is known as public key which is available to anyone wanting to send encrypted message.

It is different from private key encryption in the sense that it uses two keys. One key is used for encryption and other is used for decryption. A private encryption, on the other hand uses one key for both encryption and decryption.

Public key system is important in e-Commerce because the public key of an organization is publicized globally. The customers encrypt a message using receiving organization’s public key, which is decrypted by the receiving organization using its private key. Similarly the organization encrypts the message using particular customer’s public key which is then decrypted by the customer using their private key.

With this secure communication can be established which is an important aspect of e-Commerce.

13.13 What are the main differences between DES based encryption and RSA based encryption? Is it possible to combine these two systems? If so explain how?
The main difference between DES based encryption and RSA based encryption is

- DES uses a single key for both encryption and decryption whereas RSA uses two keys for the same
- DES is faster as it is implemented through hardware
- RSA is secure but slow since it uses complex computational procedure. Breaking the key is not easy

Yes, one can combine the two keys. DES can be used to encrypt/decrypt messages using one key. The key itself can be sent using RSA.

13.14 Give a block diagram of a system for transmitting a signed purchase order from business 1 to business 2.
See Fig. 16.13 of text.

13.15 What types of electronic payment systems are required in e-Commerce? Why are there different types of payment systems? Explain the necessary characteristics of each type of payment system and give an example each of where it is used.
The different types of electronic payment systems required in e-Commerce are: cash payments, credit card payments and cheque payments.

Each of these payments have their own advantages and disadvantages

Cash payment is used for small transactions and mostly used for C2C e-Commerce
Credit card is used for middle size transactions and mostly used for B2C e-Commerce.
Cheque payment system is used for voluminous transactions and mostly used for B2B e-Commerce.
The characteristics of e-Cash or electronic cash payments are:

- e-Cash must have monetary value
- e-Cash must be interoperable i.e., exchangeable for other e-cash, paper-cash, goods and services
- It must be storable and retrievable

The characteristics of credit card transactions are:

- The credit card number entered by the customer should be encrypted
- The merchant should not have the knowledge of the credit card number of the customer

The characteristics of cheque payment are:

- Both the parties involved in business should have public key certificates
- The cheque should be cleared by a clearing house before any transaction occurs

Necessary dedicated hardware device is required for signing and encrypting the order.

13.16 Explain SET protocol used in credit card transactions. What is the main interesting aspect of SET protocol which gives confidence to customers transacting business using the internet?

See Sec 16.6.1 steps 1 to 7

The main interesting aspect of SET protocol which gives the confidence to the customer is that the merchant does not know the credit card number of the customer.

13.17 What are the main characteristics of cash payment in contrast with cheque payment? Why are governments not sympathetic to large cash transactions in e-Commerce?

Cash payments are used in C2B applications which involve small payments whereas cheque payment system is generally used in B2B applications in which higher amount of transactions are carried out.

Cheque payments are much more secure and traceable compared to cash payments.

A sophisticated scheme called transaction blinding has been invented, using which cash payments cannot be traced. As governments do not like untraceable large cash transactions it is not sympathetic to large cash transactions in e-Commerce.

13.18 Explain how cash transactions take place in e-Commerce. What special precautions should be taken by a bank to ensure that a customer does not double spend the same electronic coins issued to him/her?

Cash Transaction in e-Commerce

A customer can withdraw “coins” in various denomination from his bank and keeps in his PC. The withdrawal takes place by the customer giving a serial
number and denomination of each coin and requesting his bank to digitally sign it. The signed coins are of the form:

(serial no., denomination, signature of bank).

The bank will store a copy of issued coins. The customer pays a vendor by cash by sending the signed coin. The vendor sends it to the issuing bank (or to his bank which may deal with the issuing bank via a clearing house). The bank checks whether it has been signed by it and not yet spent. If it is OK it informs the vendor, who now can despatch the goods. The bank transfers the cash to the vendor’s account. The coin is stored in the “spent amount database” of the bank so that if the coin is presented again it can be dishonored.

Bank manages “spent amount database” which stores the information about the coin spent by the customer. If the customer tries to reuse the coin bank can easily trace it out from the “spent amount database”
13.1 By Electronic Commerce we mean:
   a. Commerce of electronic goods
   b. Commerce which depends on electronics
   c. Commerce which is based on the use of internet
   d. Commerce which is based on transactions using computers connected by telecommunication network

13.2 For carrying out B2B e-Commerce the following infrastructure is essential:
   (i) World Wide Web
   (ii) Corporate network
   (iii) Electronic Data Interchange standards
   (iv) Secure Payment Services
   (v) Secure electronic communication link connecting businesses

   a. i, ii, iii
   b. ii, iii, iv
   c. ii, iii, iv, v
   d. i, ii, iii, iv, v

13.3 For carrying out B2C e-Commerce the following infrastructure is essential
   (i) World Wide Web
   (ii) Corporate network
   (iii) Electronic Data Interchange standards
   (iv) Secure Payment Services
   (v) Secure electronic communication link connecting businesses

   a. i, iv
   b. i, iii, iv
   c. ii, iii
   d. i, ii, iii, iv

13.4 For carrying out C2C e-Commerce the following infrastructure is essential
   (i) World Wide Web
   (ii) Corporate network
   (iii) Electronic Data Interchange standards
13.5 **Advantages of B2C commerce are**

(i) Business gets a wide reach to customers

(ii) Payment for services easy

(iii) Shop can be open 24 hours a day seven days a week

(iv) Privacy of transaction always maintained

a. i and ii

b. ii and iii

c. i and iii

d. iii and iv

13.6 **B2C commerce**

a. includes services such as legal advice

b. means only shopping for physical goods

c. means only customers should approach customers to sell

d. means only customers should approach business to buy

13.7 **Advantages of B2C commerce to customers are**

(i) wide variety of goods can be accessed and comparative prices can be found

(ii) shopping can be done at any time

(iii) privacy of transactions can be guaranteed

(iv) security of transactions can be guaranteed

a. i and ii

b. ii and iii

c. iii and iv

d. i and iv
13.8 Disadvantages of e-Commerce in India are

(i) internet access is not universally available
(ii) Credit card payment security is not yet guaranteed
(iii) Transactions are de-personalized and human contact is missing
(iv) Cyberlaws are not in place

a. i and ii  
b. ii and iii  
c. i, ii, iii  
d. i, ii, iii, iv

13.9 Electronic Data Interchange is necessary in

a. B2C e-Commerce  
b. C2C e-Commerce  
c. B2B e-Commerce  
d. Commerce using internet

13.10 EDI requires

a. representation of common business documents in computer readable forms  
b. data entry operators by receivers  
c. special value added networks  
d. special hardware at co-operating Business premises

13.11 EDI standards are

a. not universally available  
b. essential for B2B commerce  
c. not required for B2B commerce  
d. still being evolved

13.12 EDIFACT is a standard

a. for representing business forms used in e-Commerce  
b. for e-mail transaction for e-Commerce  
c. for ftp in e-Commerce  
d. protocol used in e-Commerce

13.13 EDIFACT standard was developed by

a. American National Standard Institute
b. International Standard Institute  
c. European Common Market  
d. United Nations Economic Commission for Europe  

**13.14 ANSI X.12 is a standard developed by**  
a. American National Standard Institute  
b. International Standard Institute  
c. European Common Market  
d. United Nations Economic Commission for Europe  

**13.15 In B2B e-Commerce**  
(i) Co-operating Business should give an EDI standard to be used  
(ii) Programs must be developed to translate EDI forms to a form accepted  
     by application program  
(iii) Method of transmitting/receiving data should be mutually agreed  
(iv) It is essential to use internet  
     a. i, ii  
     b. i, ii, iii  
     c. i, ii, iii, iv  
     d. ii, iii, iv  

**13.16 EDI use**  
a. requires an extranet  
b. requires value added network  
c. can be done on internet  
d. requires a corporate intranet  

**13.17 EDI over internet uses**  
a. MIME to attach EDI forms to e-mail messages  
b. FTP to send business forms  
c. HTTP to send business forms  
d. SGML to send business forms  

**13.18 For secure EDI transmission on internet**  
a. MIME is used  
b. S/MIME is used
13.19 **EDI standard**
- is not easily available
- defines several hundred transaction sets for various business forms
- is not popular
- defines only a transmission protocol

13.20 **By security in e-Commerce we mean**
(i) Protecting an organization’s data resource from unauthorized access
(ii) Preventing disasters from happening
(iii) Authenticating messages received by an organization
(iv) Protecting messages sent on the internet from being read and understood by unauthorized persons/organizations

a. i, ii
b. ii, iii
c. iii, iv
d. i, iii, iv

13.21 **A firewall is a**
- wall built to prevent fires from damaging a corporate intranet
- security device deployed at the boundary of a company to prevent unauthorized physical access
- security device deployed at the boundary of a corporate intranet to protect it from unauthorized access
- device to prevent all accesses from the internet to the corporate intranet

13.22 **A firewall may be implemented in**
- routers which connect intranet to internet
- bridges used in an intranet
- expensive modem
- user’s application programs

13.23 **Firewall as part of a router program**
- filters only packets coming from internet
b. filters only packets going to internet  
c. filters packets travelling from and to the intranet from the internet  
d. ensures rapid traffic of packets for speedy e-Commerce

13.24 **Filtering of packets by firewall based on a router has facilities to**
   a. i, iii  
   b. i, ii, iii  
   c. i, ii, iii, iv  
   d. ii, iii, iv

13.25 **Main function of proxy application gateway firewall is**
   a. to allow corporate users to use efficiently all internet services  
   b. to allow intranet users to securely use specified internet services  
   c. to allow corporate users to use all internet services  
   d. to prevent corporate users from using internet services

13.26 **Proxy application gateway**
   (i) acts on behalf of all intranet users wanting to access internet securely  
   (ii) monitors all accesses to internet and allows access to only specified IP addresses  
   (iii) disallows use of certain protocols with security problems  
   (iv) disallows all internet users from accessing intranet  
   a. i, ii  
   b. i, ii, iii  
   c. i, ii, iii, iv  
   d. ii, iii, iv

13.27 **A hardened firewall host on an intranet**
   (i) has a proxy application gateway program running on it  
   (ii) allows specified internet users to access specified services in the intranet  
   (iii) initiates all internet activities requested by clients and monitors them  
   (iv) prevents outsiders from accessing IP addresses within the intranet  
   a. i, ii  
   b. i, ii, iii  
   c. i, ii, iii, iv  
   d. ii, iii, iv
13.28 **A hardened firewall host on an Intranet is**
   a. a software which runs in any of the computers in the intranet
   b. a software which runs on a special reserved computer on the intranet
   c. a stripped down computer connected to the intranet
   d. a mainframe connected to the intranet to ensure security

13.29 **By encryption of a text we mean**
   a. compressing it
   b. expanding it
   c. scrambling it to preserve its security
   d. hashing it

13.30 **Encryption is required to**
   (i) protect business information from eavesdropping when it is transmitted on internet
   (ii) efficiently use the bandwidth available in PSTN
   (iii) to protect information stored in companies’ databases from retrieval
   (iv) to preserve secrecy of information stored in databases if an unauthorized person
       retrieves it
   a. i and ii
   b. ii and iii
   c. iii and iv
   d. i and iv

13.31 **Encryption can be done**
   a. only on textual data
   b. only on ASCII coded data
   c. on any bit string
   d. only on mnemonic data

13.32 **By applying permutation (31254) and substitution by 5 characters away from current character (A → F, B → G etc..) the following string ABRACADABRA becomes**
   a. FGWCAAADRB
   b. RABCAADRB
   c. WFGHFFFIWGF
13.33 The following ciphertext was received. The plaintext was permuted using permutation (34152) and substitution. Substitute character by character +3 (A → D, etc). The plaintext after decryption is: Cipher text:

PDLJDLXHVQC

a. MAIGAIUESNZ
b. IAMAGENIUSZ
c. LDPDJHPLXVZ
d. IAMAGENIUSC

13.34 By symmetric key encryption we mean

a. one private key is used for both encryption and decryption
b. private and public key used are symmetric
c. only public keys are used for encryption
d. only symmetric key is used for encryption

13.35 The acronym DES stands for

a. Digital Evaluation System
b. Digital Encryption Standard
c. Digital Encryption System
d. Double Encryption Standard

13.36 DES works by using

a. permutation and substitution on 64 bit blocks of plain text
b. only permutations on blocks of 128 bits
c. exclusive ORing key bits with 64 bit blocks
d. 4 rounds of substitution on 64 bit blocks with 56 bit keys

13.37 DES

(i) is a symmetric key encryption method
(ii) guarantees absolute security
(iii) is implementable as hardware VLSI chip
(iv) is a public key encryption method

a. i and ii
b. ii and iii
13.38 **DES using 56 bit keys**

a. Cannot be broken in reasonable time using presently available computers.

b. Can be broken only if the algorithm is known using even slow computers.

c. Can be broken with presently available high performance computers.

d. It is impossible to break ever.

13.39 **Triple DES uses**

a. 168 bit keys on 64-bit blocks of plain text.

b. Working on 64-bit blocks of plain text and 56 bit keys by applying DES algorithm for three rounds.

b. Works with 144 bit blocks of plain text and applies DES algorithm once.

b. Uses 128 bit blocks of plain text and 112 bit keys and apply DES algorithm thrice.

13.40 **ripple DES**

a. Cannot be broken in reasonable time using presently available computers.

b. Can be broken only if the algorithm is known using even slow computer.

b. Can be broken with presently available high performance computers.

b. It is impossible to break ever.

13.41 **Triple DES**

a. is a symmetric key encryption method.

b. guarantees excellent security.

c. is implementable as a hardware VLSI chip.

d. is public key encryption method with three keys.

13.42 **Public key encryption method is a system**

a. which uses a set of public keys one for each participant in e-Commerce.

b. in which each person who wants to communicate has two keys; a private key known to him only and a public key which is publicized to enable others to send message to him.

c. which uses the RSA coding system.

d. which is a standard for use in e-Commerce.
13.43 Public key system is useful because
   a. it uses two keys.
   b. there is no key distribution problem as public key can be kept in a commonly accessible database.
   c. private key can be kept secret.
   d. it is a symmetric key system.

13.44 In public key encryption if A wants to send an encrypted message
   a. A encrypts message using his private key
   b. A encrypts message using B’s private key
   c. A encrypts message using B’s public key
   d. A encrypts message using his public key

13.45 In public key encryption system if A encrypts a message using his private key and sends it to B
   a. if B knows it is from A he can decrypt it using A’s public key
   b. Even if B knows who sent the message it cannot be decrypted
   c. It cannot be decrypted at all as no one knows A’s private key
   d. A should send his public key with the message

13.46 Message can be sent more securely using DES by
   a. encrypting plain text by a different randomly selected key for each transmission
   b. encrypting plain text by a different random key for each message transmission and sending the key to the receiver using a public key system
   c. using an algorithm to implement DES instead of using hardware
   d. designing DES with high security and not publicizing algorithm used by it

13.47 DES and public key algorithm are combined
(ii) to ensure higher security by using different key for each transmission
(iii) as a combination is always better than individual system
(iv) as it is required in e-Commerce
   a. i and ii
   b. ii and iii
13.48 **A digital signature is**
   a. a bit string giving identity of a correspondent
   b. a unique identification of a sender
   c. an authentication of an electronic record by tying it uniquely to a key only a sender knows
   d. an encrypted signature of a sender

13.49 **A digital signature is required**
(i) to tie an electronic message to the sender’s identity
(ii) for non repudiation of communication by a sender
(iii) to prove that a message was sent by the sender in a court of law
(iv) in all e-mail transactions
   a. i and ii
   b. i, ii, iii
   c. i, ii, iii, iv
   d. ii, iii, iv

13.50 **A hashing function for digital signature**
(i) must give a hashed message which is shorter than the original message
(ii) must be hardware implementable
(iii) two different messages should not give the same hashed message
(iv) is not essential for implementing digital signature
   a. i and ii
   b. ii and iii
   c. i and iii
   d. iii and iv

13.51 **Hashed message is signed by a sender using**
   a. his public key
   b. his private key
   c. receiver’s public key
   d. receiver’s private key
13.52 While sending a signed message, a sender
   a. sends message key using public key encryption using DES and hashed message using public key encryption
   b. sends message using public key encryption and hashed message using DES
   c. sends both message and hashed message using DES
   d. sends both message and hashed message using public key encryption

13.53 The responsibility of a certification authority for digital signature is to authenticate the
   a. hash function used
   b. private keys of subscribers
   c. public keys of subscribers
   d. key used in DES

13.54 Certification of Digital signature by an independent authority is needed because
   a. it is safe
   b. it gives confidence to a business
   c. the authority checks and assures customers that the public key indeed belongs to the business which claims its ownership
   d. private key claimed by a sender may not be actually his

13.55 The Secure Electronic Transaction protocol is used for
   a. credit card payment
   b. cheque payment
   c. electronic cash payments
   d. payment of small amounts for internet services

13.56 In SET protocol a customer encrypts credit card number using
   a. his private key
   b. bank’s public key
   c. bank’s private key
   d. merchant’s public key

13.57 In SET protocol a customer sends a purchase order
Multiple Choice Questions

13.58 One of the problems with using SET protocol is
   a. the merchant’s risk is high as he accepts encrypted credit card
   b. the credit card company should check digital signature
   c. the bank has to keep a database of the public keys of all customers
   d. the bank has to keep a database of digital signatures of all customers

13.59 The bank has to have the public keys of all customers in SET protocol as it has to
   a. check the digital signature of customers
   b. communicate with merchants
   c. communicate with merchants credit card company
   d. certify their keys

13.60 In electronic cheque payments developed, it is assumed that most of the transactions will be
   a. customers to customers
   b. customers to business
   c. business to business
   d. banks to banks

13.61 In cheque payment protocol, the purchase order form is signed by purchaser using
   a. his public key
   b. his private key
   c. his private key using his signature hardware
   d. various public keys

13.62 In the NetBill’s protocol for small payments for services available in the internet.
   (i) the customer is charged only when the information is delivered
   (ii) the vendor is guaranteed payment when information is delivered
(iii) the customer must have a certified credit card
(iv) the customer must have a valid public key
   a. i, ii
   b. i, ii, iii
   c. i, ii, iii, iv
   d. i, ii, iv

13.63 In NetBill’s protocol for small payments for internet services
(i) Key to decrypt information is sent to customer by NetBill only when there is
   enough amount in debit account
(ii) The vendor supplies the key to NetBill server when he receives payment
(iii) Checksum of encrypted information received by customer is attached to his
   payment order
(iv) Vendor does not encrypt information purchased by customer
   a. i, ii
   b. i, ii, iii
   c. i, ii, iii, iv
   d. i, ii, iv

13.64 In Electronic cash payment
   a. a debit card payment system is used
   b. a customer buys several electronic coins which are digitally signed by coin
      issuing bank
   c. a credit card payment system is used
   d. RSA cryptography is used in the transactions

13.65 In Electronic cash payment
(i) a customer withdraws “coins” in various denominations signed by the bank
(ii) the bank has a database of issued coins
(iii) the bank has a database of spent coins
(iv) the bank cannot trace a customer
   a. i, ii
   b. i, ii, iii
   c. i, ii, iii, iv
   d. ii, iii, iv
Key to Objective Questions

13.1 d 13.2 c 13.3 a 13.4 c 13.5 c 13.6 a
13.7 a 13.8 c 13.9 c 13.10 a 13.11 b 13.12 a
13.13 d 13.14 a 13.15 b 13.16 c 13.17 a 13.18 b
13.25 b 13.26 b 13.27 c 13.28 b 13.29 c 13.30 d
13.31 c 13.32 c 13.33 b 13.34 a 13.35 b 13.36 a
13.44 c 13.45 a 13.46 b 13.47 a 13.48 c 13.49 b 13.50 c
13.51 b 13.52 a 13.53 c 13.54 c
13.55 a 13.56 b 13.57 d 13.58 c 13.59 a 13.60 c
13.61 c 13.62 d 13.63 b 13.64 b 13.65 b
Question Bank

13.1 Define E-Commerce. What are the different types of E-Commerce?

13.2 Explain B2B E-Commerce using an example of a book distributor who stocks a large number of books, which he distributes via a large network of book sellers. Assume that the distributor has stocks of books of a large number of publishers and book sellers order books as and when their stock is low. Distributors give 1 month's time to booksellers for payment.

13.3 Explain B2C E-Commerce of a customer reserving airline tickets from his home or place of work.

13.4 Explain C2C E-Commerce with an appropriate example.

13.5 List the advantages and disadvantages of E-Commerce.

13.6 Explain the system architecture of E-Commerce by looking at it as a set of layers with the physical network at the bottom layer and applications at the top layer.

13.7 Define internet. Why is internet important in E-Commerce?

13.8 What do you understand by EDI? Is EDI used in B2C or B2B E-Commerce? Why is EDI important in E-Commerce?

13.9 What are two major EDI standards used in E-Commerce? Which is the standard accepted for Government transactions in India?

13.10 What is VAN? What services do VANs provide? What are the advantages and disadvantages of VAN?

13.11 If internet is to be used for EDI which mail standard is used?

13.12 If email is to be used to exchange EDI between two businesses what are the points on which they should agree?

13.13 Why is security important in E-Commerce? What are the security issues to be taken into account while designing a security system for E-Commerce?

13.14 What is a firewall? What are the functions of a firewall?

13.15 What is packet screening? Which hardware device performs packet screening?

13.16 What is a proxy application gateway? What are the functions of this gateway?

13.17 What is a hardened firewall host? What are its functions? In what way is it different from proxy application gateway?

13.18 Given a plain text:

THIS IS A SAMPLE SENTENCE FOR ENCRYPTION.
Apply the permutation (231564) and the substitution: (letter \(\rightarrow\) letter + 6 ) and obtain the cipher text.

13.19 What is DES? Explain what DES does when the following hexadecimal plain text is input to DES hardware.

\[\text{A1907FB9065A81FED14E890DCA5}\]

13.20 What do you understand by symmetric key cryptography? What are the main advantages and disadvantages of symmetric key cryptography?

13.21 What is public key encryption? In what way is it different from private key encryption? Why is it important in E-Commerce?

13.22 What are the main differences between DES based encryption and RSA based encryption? Is it possible to combine these two systems? If so explain how?

13.23 Given two prime numbers 23 and 41 design a RSA system. Explain with an example how it works.

13.24 What is a digital signature? Why is it necessary in E-Commerce? What are the necessary conditions a hash function used in digital signature should satisfy?

13.25 Give a block diagram of a system for transmitting a signed purchase order from business 1 to business 2.

13.26 What is a certifying authority? Why is a certifying authority required in E-Commerce? How a certifying authority does perform its tasks?

13.27 What types of electronic payment systems are required in E-Commerce? Why are there different types of payment systems? Explain the necessary characteristics of each type of payment system and give an example each of where it is used.

13.28 Explain SET protocol used in credit card transactions. What is the main interesting aspect of SET protocol which gives confidence to customers transacting business using the internet?

13.29 In using SET protocol who has to keep a data base of public keys of all customers? How the customer does assured that he will not be double charged for the same item purchased?

13.30 What are the main differences between electronic cheque payment and credit card payment in E-Commerce? Explain cheque transaction protocol used in E-Commerce.

13.31 Why is a different payment system needed for small payment for internet services? Explain how one such system functions. How does the system make sure that payment
is made only after information for which payment has been made is actually delivered to the customer?

13.32 What are the main characteristics of cash payment in contrast with cheque payment? Why are governments not sympathetic to large cash transactions in E-Commerce?

13.33 Explain how cash transactions take place in E-Commerce. What special precautions should be taken by a bank to ensure that a customer does not double spend the same electronic coins issued to him/her?
References


2. There are many books on E-Commerce, which describe E-Commerce in detail. Among these are: E. Awad, Electronic Commerce, Prentice-Hall of India, New Delhi, 2002. This book takes managers perspective and not very strong on technology aspects of E-Commerce. All the examples have a strong American bias as the book is primarily intended for students in America. The language is clear but the book is verbose. What can be said in 100 pages is said in 400 pages as it includes all kinds of gossip not relevant to students wanting the learn the subject.


5. Most traditional Systems Analysis and Design book such as the one by Kendall and Kendall do not separately discuss E-Commerce; they have a cursory treatment at various places in the book.