MODULE 13

ELECTRONIC COMMERCE

OBJECTIVE QUESTIONS

There are 4 alternative answers to each question. One of them is correct. Pick the correct answer. Do not guess. A key is given at the end of the module for you to verify your answer

LEARNING UNIT 1

13.1.1 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

13.1.2 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

13.1.3 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

13.1.4 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 (b) ii and iv
(c) i (d) i and iv

13.1.5 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

13.1.6 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

13.1.7 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

13.1.8 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

LEARNING UNIT 2

13.2.1 Electronic Data Interchange is necessary in

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

13.2.2 EDI requires

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

13.2.3 EDI standards are

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

13.2.4 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

13.2.5 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

13.2.6 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

13.2.7 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

13.2.8 EDI use

(a) requires an extranet

(b) requires value added network

(c) can be done on internet

(d) requires a corporate intranet

13.2.9 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

13.2.10 For secure EDI transmission on internet

(a) MIME is used

(b) S/MIME is used

(c) PGP is used

(d) TCP/IP is used

13.2.11 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

LEARNING UNIT 3

13.3.1 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

13.3.2 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

13.3.3 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

13.3.4 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

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

(i) prevent access to internet to some clients in the intranet
(ii) prevent access at certain specified times
(iii) filter packets based on source or destination IP address
(iv) prevent access by certain users of the internet to other specified users of the internet

(a) i, iii (b) i, ii, iii
(c) i, ii, iii, iv (d) ii, iii, iv

13.3.6 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

13.3.7 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

13.3.8 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

13.3.9 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

13.3.10 By encryption of a text we mean

(a) compressing it

(b) expanding it

(c) scrambling it to preserve its security

(d) hashing it

13.3.11 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

13.3.12 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

13.3.13 By applying permutation (31254) and substitution by 5 characters away from current character (A → F , B → G etc..) the following string ABRACADABRA becomes

(a) FGWCAAADRBF

(b) RABCAAADRBF

(c) WFGHFFFIWGF

(d) None of the above

13.3.14 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

13.3.15 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

13.3.16 The acronym DES stands for
(a) Digital Evaluation System
(b) Digital Encryption Standard
(c) Digital Encryption System
(d) Double Encryption Standard

13.3.17 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

13.3.18 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

13.3.19 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.

13.3.20 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.

13.3.21 Triple 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.

13.3.22 Triple DES

(i) is a symmetric key encryption method
(ii) guarantees excellent security
(iii) is implementable as a hardware VLSI chip
(iv) is public key encryption method with three keys.

13.3.23 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

13.3.24 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

13.3.25 In public key encryption if A wants to send an encrypted message to B

(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

13.3.26 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

13.3.27 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

13.3.28 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

13.3.29 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

13.3.30 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

13.3.31 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

13.3.32 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

13.3.33 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

13.3.34 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

13.3.35 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

LEARNING UNIT 4

13.4.1 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

13.4.2 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

13.4.3 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

13.4.4 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

13.4.5 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

13.4.6 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

13.4.7 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

13.4.8 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

13.4.9 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

13.4.10 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

13.4.11 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

13.1.1 d	**13.1.2 c**	**13.1.3 a**	**13.1.4 c**	**13.1.5 c**	**13.1.6 a**
13.1.7 a	**13.1.8 c**	**13.2.1 c**	**13.2.2 a**	**13.2.3 b**	**13.2.4 a**
13.2.5 d	**13.2.6 a**	**13.2.7 b**	**13.2.8 c**	**13.2.9 a**	**13.2.10 b**
13.2.11 b	**13.3.1 d**	**13.3.2 c**	**13.3.3 a**	**13.3.4 c**	**13.3.5 b**
13.3.6 b	**13.3.7 b**	**13.3.8 c**	**13.3.9 b**	**13.3.10 c**	**13.3.11 d**
13.3.12 c	**13.3.13 c**	**13.3.14 b**	**13.3.15 a**	**13.3.16 b**	**13.3.17 a**
13.3.18 c	**13.3.19 c**	**13.3.20 b**	**13.3.21 a**	**13.3.22 b**	**13.3.23 b**
13.3.24 b	**13.3.25 c**	**13.3.26 a**	**13.3.27 b**	**13.3.28 a**	**13.3.29 c**
13.3.30 b	**13.3.31 c**	**13.3.32 b**	**13.3.33 a**	**13.3.34 c**	**13.3.35 c**
13.4.1 a	**13.4.2 b**	**13.4.3 d**	**13.4.4 c**	**13.4.5 a**	**13.4.6 c**
13.4.7 c	**13.4.8 d**	**13.4.9 b**	**13.4.10 b**	**13.4.11 b**	