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.

Deleted: r

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.

Deleted: ck po

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

Deleted: prepared using hyper text markup language.

Deleted: ¶

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.

Deleted: html

Deleted: mpile

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

Deleted: which

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 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.

Deleted: Network

Deleted: -Commerce

Deleted: n

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.

Deleted: le

16. An organizaion'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 unauthorised intruders.

Deleted: f

17. Messages exchanged between organizations using the internet can be easily tapped by eaves droppers. 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.

Deleted: it

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.

Deleted: It is, however, 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.

Deleted: when

Deleted: is known

Deleted: RSA system is symmetric.

Deleted: other words

Deleted: is

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 MD_e. 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 MD_e using the sender's public key. If (MD_e) 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.

Deleted: it

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.

Deleted: downloads

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

Deleted: k

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.

Deleted: csutomer's

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.

Formatted

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 → 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 a DES hardware.

A1907FBCD986543201FED14E890ABCA5

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 does a certifying authority performs 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 does the customer 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?