1. **(a) Differentiate between E-commerce and E-business.**

**Answer:**

E-commerce and E-business are two related but distinct concepts that involve the use of digital technologies to conduct various types of transactions. Here is a table that summarizes some of the key differences between them:

| **E-commerce** | **E-business** |
| --- | --- |
| E-commerce refers to the online buying and selling of goods and services over the internet. | E-business refers to the use of internet, intranet, or extranet to perform any kind of business activity, such as procurement, customer education, supply chain management, etc. |
| E-commerce is a subset of E-business, as it only covers the commercial aspect of online transactions. | E-business is a superset of E-commerce, as it encompasses all the aspects of online business operations, including internal and external processes. |
| E-commerce mainly involves business-to-customer (B2C) transactions, where the seller and the buyer interact directly through a website or an app. | E-business often involves business-to-business (B2B) transactions, where the seller and the buyer use multiple websites, apps, CRMs, ERPs, etc. to connect different business processes. |
| E-commerce requires the use of internet only, as it is based on web-based platforms. | E-business may use internet, intranet, or extranet, depending on the type and scope of the business activity. |
| E-commerce is more suitable for selling products or services that can be delivered digitally or physically. | E-business is more suitable for providing information, support, or solutions that can enhance the efficiency or convenience of the business. |

**(b) Mention the most important factors in successful E-commerce site designing with proper diagram.**

**Answer:**

There are many factors that contribute to the success of an E-commerce site design, but some of the most important ones are:

* **Design matching your products**: The appearance and feel of your website should match what you’re selling. Your website should reflect your brand identity and product features through graphics, color scheme, font, etc
* **Product showcase and descriptions**: You should display your products prominently and clearly on your website, using high-quality photos and informative descriptions. Your customers should be able to see the details and benefits of your products, as well as any instructions or specifications they need to know before buying
* **Shipping rates**: You should provide complete and transparent information about your shipping options and costs, preferably with a link on each product page. If possible, offer free or low shipping fees, or at least inform your customers about the shipping rates early in the shopping process. High or hidden shipping fees are one of the main reasons why customers abandon their carts
* **Shopping cart design**: Your shopping cart should be easy and convenient to use, allowing your customers to add, remove, or change their orders. It should also feature product photos, recommendations, a search bar, an order summary, a ‘continue shopping’ option, and reviews. You can also use cross-selling and upselling techniques to increase your sales
* **Guest checkout**: You should allow your customers to checkout without creating an account, as many customers prefer not to share their personal information or go through a lengthy registration process. You can still offer them the option to create an account later, or to sign in with their social media accounts
* **Payment methods**: You should offer a variety of secure and convenient payment methods, such as credit cards, debit cards, PayPal, Google Pay, etc. You should also display trust badges and security certificates to assure your customers that their transactions are safe and protected
* **Customer service**: You should provide excellent customer service, such as live chat, phone, email, or social media support, to answer your customers’ questions, concerns, or complaints.
* **Mobile optimization**: You should make sure that your website is responsive and adaptable to different devices and screen sizes, especially mobile phones. More and more customers are using their smartphones to shop online, so you should provide them with a smooth and user-friendly mobile experience.

**(c) Using appropriate figure differentiate between Two-tire and Multi-tier system.**

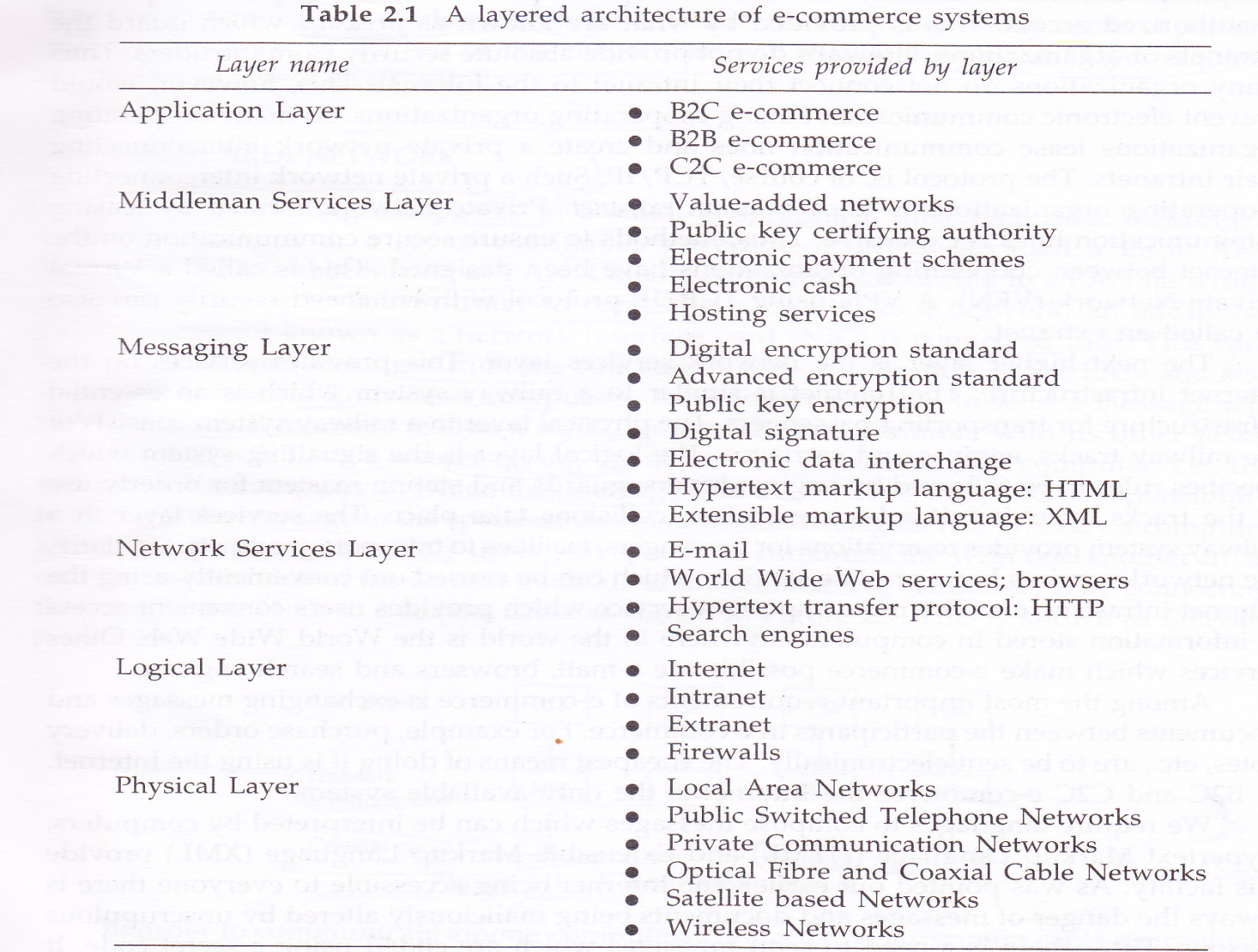
**Answer:**

Here is a table that summarizes the differences between two-tier and multi-tier systems in e-commerce:

| **Aspect** | **Two-tier** | **Multi-tier** |
| --- | --- | --- |
| Architecture | A client layer and a server layer | A client layer, an application layer, and a data layer |
| Communication | The client communicates directly with the server | The client communicates with the application layer, which communicates with the data layer |
| Advantages | Simpler to design and implement | More scalable, secure, modular, and performant |
| Disadvantages | Less flexible, robust, and efficient | More complex, costly, and overhead |

1. **(a) Draw a table showing different layers of e-commerce architecture and discuss the services provided by them.**

**Answer:**

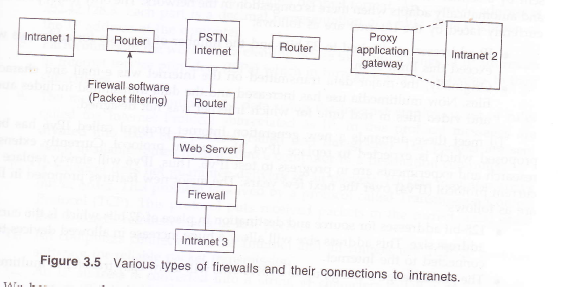


**(b) State the function of Firewall in e-commerce.**

**Answer:**

A firewall is a network security device that monitors and controls the incoming and outgoing traffic on an e-commerce system. It allows or blocks data packets based on a set of rules or policies. The main function of a firewall in e-commerce is to protect the system from external threats, such as hackers, malware, or denial-of-service attacks. A firewall can also help to:

* Monitor and control the bandwidth usage of the system, by prioritizing or limiting the traffic for certain applications, websites, or users.
* Enhance the performance and reliability of the system, by filtering out unwanted or malicious traffic and reducing the network congestion.
* Enforce the compliance and privacy of the system, by preventing unauthorized access to sensitive data or resources, such as customer information, payment details, or inventory records.
* Support the scalability and modularity of the system, by allowing the system to be divided into different layers or zones, each with its own security level and firewall configuration.

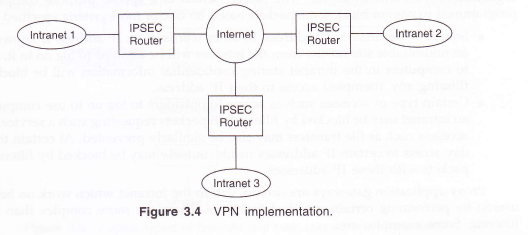


**(c) Explain briefly how VPN is implemented to ensure security.**

**Answer:**

A VPN (Virtual Private Network) is a service that allows users to access the internet securely and privately. A VPN works by creating an encrypted connection between the user’s device and a VPN server, which acts as a proxy for the user’s online activity. The VPN server then routes the user’s internet traffic through its own network, hiding the user’s IP address and location from anyone who might be monitoring the network. This way, a VPN protects the user’s data and identity from hackers, ISPs, government agencies, or other third parties who might want to spy on or censor the user’s online activity.

To implement a VPN, the user needs to install a VPN software on their device, which will encrypt and decrypt the data sent and received by the user. The VPN software will also connect the user to a VPN server, which can be located in different countries or regions. The user can choose which VPN server to connect to, depending on their preferences or needs. For example, if the user wants to access a website that is blocked in their country, they can connect to a VPN server in a different country where the website is not blocked. The VPN server will then fetch the website for the user and send it back to the user’s device through the encrypted connection.



1. **(a) Distinguish between confidentiality, authenticity, non-repudiation and integrity of messages sent between a customer and a company in e-commerce.**

**Answer:**

Confidentiality, authenticity, non-repudiation and integrity are four important properties of secure communication in e-commerce. They can be defined as follows:

* **Confidentiality** means that only the authorized parties can access the content of the messages. This prevents unauthorized disclosure of sensitive information, such as personal data, payment details, or business secrets. Confidentiality can be achieved by using encryption algorithms, such as AES, to transform the messages into unreadable form.
* **Authenticity** means that the parties can verify the identity of each other and the source of the messages. This prevents impersonation, spoofing, or phishing attacks, where an attacker pretends to be someone else. Authenticity can be achieved by using digital signatures, certificates, or public-key cryptography, such as RSA, to prove the ownership of the messages.
* **Non-repudiation** means that the parties can prove the existence and the content of the messages. This prevents denial or dispute of the messages, such as claiming that a message was never sent, received, or modified. Non-repudiation can be achieved by using timestamps, hashes, or message authentication codes, such as HMAC, to create a record of the messages.
* **Integrity** means that the messages are not altered or corrupted during the transmission. This prevents tampering, modification, or insertion of malicious data, such as viruses, malware, or ransomware. Integrity can be achieved by using checksums, hashes, or message authentication codes, such as HMAC, to detect any changes in the messages.

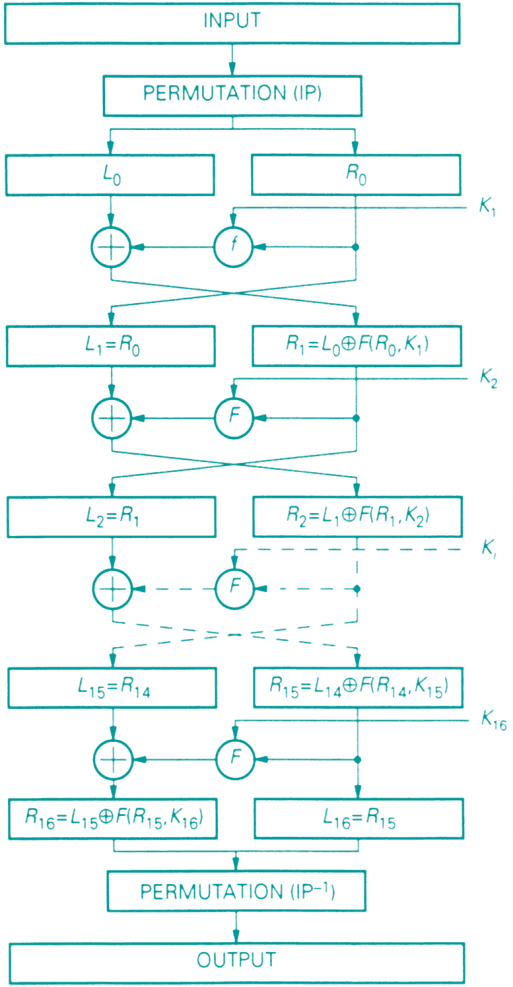
**(b) Describe the DES algorithm briefly giving the various steps it uses for encryption. Is it considered secure currently? If not explain why it is not secure.**

**Answer:**

The DES algorithm is a symmetric-key block cipher that encrypts and decrypts 64-bit blocks of data using a 56-bit key. It was developed by IBM in the 1970s and adopted as a standard by the US government in 1977. The algorithm consists of the following steps:

* **Initial permutation**: The input block is permuted according to a fixed table, resulting in two 32-bit halves.
* **16 rounds of encryption**: Each round consists of four operations:
  + **Expansion**: The right half of the block is expanded from 32 bits to 48 bits using another fixed table.
  + **Key mixing**: The expanded right half is XORed with a subkey derived from the main key using a key schedule algorithm.
  + **Substitution**: The result of the XOR operation is divided into eight 6-bit pieces, each of which is mapped to a 4-bit output using a predefined substitution box (S-box).
  + **Permutation**: The outputs of the S-boxes are concatenated and permuted again using a fixed table.
  + The output of this round becomes the new right half, and the original right half becomes the new left half.
* **Final permutation**: The final output is obtained by swapping the left and right halves and applying the inverse of the initial permutation.

The decryption process is the same as the encryption process, except that the subkeys are applied in reverse order.



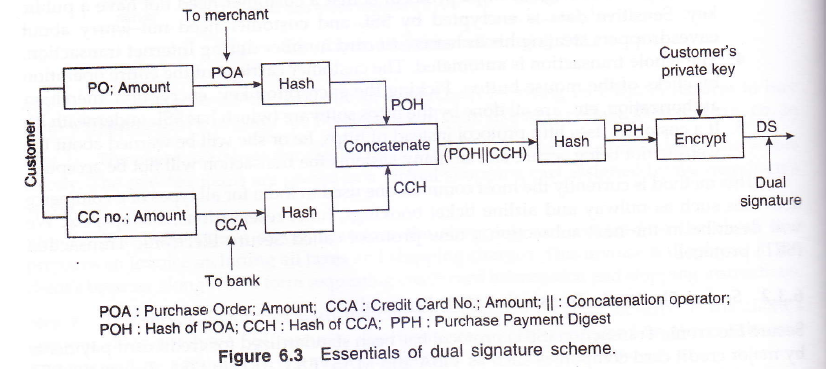
The DES algorithm is not considered secure today, because its key size is too small to resist brute-force attacks. In 1999, a machine built by the Electronic Frontier Foundation (EFF) cracked a DES key in less than 23 hours. Moreover, DES is vulnerable to various cryptanalytic techniques, such as differential and linear cryptanalysis. To improve the security of DES, several variants have been proposed, such as Triple DES, which applies DES three times with different keys. However, modern applications prefer to use more advanced algorithms, such as AES, which have larger key sizes and better performance.

**(c) What is dual signature? What is the purpose of dual signature in SET protocol?**

**Answer:**

A **dual signature** is a concept introduced with the **Secure Electronic Transaction** (**SET**) protocol, which aims at connecting two information pieces meant for two different receivers:

* Order Information (OI) for the merchant
* Payment Information (PI) for the bank



The purpose of the dual signature is to ensure that the OI and PI are linked together, and that the merchant cannot see the PI, and the bank cannot see the OI. This way, the customer’s privacy and security are protected, and the merchant and the bank can verify the authenticity and integrity of the transaction.

1. **(a) What is digital signature? How is an e-document signed by a sender and sent to receiver? How does the recipient of a signed e-document authenticate the signature?**

**Answer:**

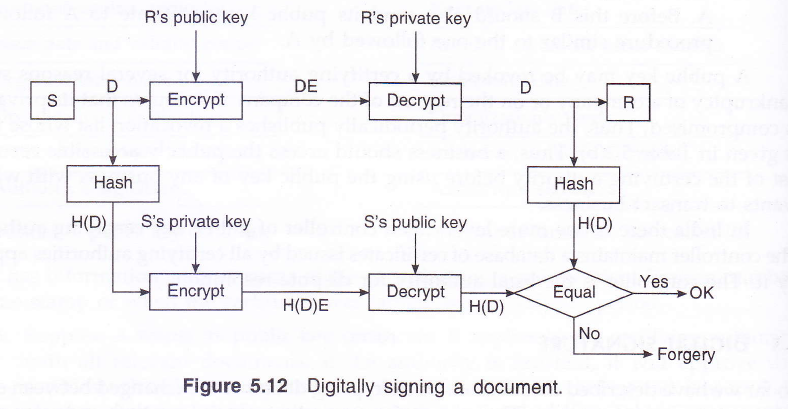
A **digital signature** is a type of electronic signature that uses cryptographic techniques to verify the identity and integrity of the sender and the document. A digital signature consists of two components: **a public key and a private key**. The public key is shared with anyone who needs to verify the signature, while the private key is kept secret by the signer.

**To sign an e-document, the sender follows these steps:**

* The sender creates a message digest, which is a hash of the document using a hash function (such as SHA-256).
* The sender encrypts the message digest with their private key, using a digital signature algorithm (such as RSA or ECDSA). This encrypted message digest is the digital signature.
* The sender attaches the digital signature and the public key to the document and sends it to the receiver.

**To authenticate the signature, the receiver follows these steps:**

* The receiver verifies that the public key belongs to the sender, using a certificate authority (CA) or a web of trust (WoT).
* The receiver decrypts the digital signature with the public key, using the same digital signature algorithm as the sender. This reveals the message digest.
* The receiver creates a message digest of the document, using the same hash function as the sender.
* The receiver compares the two message digests. If they match, the signature is valid and the document is authentic and unaltered. If they do not match, the signature is invalid or the document is tampered with.



**(b) Illustrate how the encryption and decryption works in RSA algorithm using two prime numbers 3 and 11. Apply the algorithm to a message ‘CSEJU’.**

**Answer:**

The RSA algorithm is a public-key cryptosystem that uses two large prime numbers to generate a pair of keys: a public key and a private key. The public key can be used to encrypt messages, and the private key can be used to decrypt them. The security of the algorithm relies on the difficulty of factoring the product of the two prime numbers.

To illustrate how the encryption and decryption works in RSA algorithm using two prime numbers 3 and 11, we can follow these steps:

* First, we compute the modulus n by multiplying the two prime numbers: n = 3 \* 11 = 33.
* Next, we compute the totient function phi(n) by multiplying the decrements of the two prime numbers: phi(n) = (3 - 1) \* (11 - 1) = 20.
* Then, we choose an encryption exponent e that is coprime to phi(n), meaning they have no common factors except 1. For example, we can choose e = 3, since gcd(3, 20) = 1.
* After that, we find a decryption exponent d that satisfies the equation e \* d = 1 mod phi(n), meaning the remainder of dividing e \* d by phi(n) is 1. For example, we can choose d = 7, since 3 \* 7 = 21 and 21 mod 20 = 1.
* Now, we have the public key (n, e) = (33, 3) and the private key (n, d) = (33, 7).
* To encrypt a message m, we use the formula c = m^e mod n, where c is the cipher-text. To decrypt a cipher-text c, we use the formula m = c^d mod n, where m is the plaintext.

To apply the algorithm to a message CSEJU, we need to convert the letters to numbers using some scheme, such as A = 1, B = 2, …, Z = 26. For example, we can convert CSEJU to 3 19 5 10 21. Then, we encrypt each number using the public key (33, 3). For example, to encrypt 3, we compute 3^3 mod 33 = 27. Similarly, we encrypt the other numbers and get the ciphertext 27 24 12 12 18. To decrypt the ciphertext, we use the private key (33, 7). For example, to decrypt 27, we compute 27^7 mod 33 = 3. Similarly, we decrypt the other numbers and get the plaintext 3 19 5 10 21. Then, we convert the numbers back to letters using the same scheme and get the message CSEJU.

1. **(a) Write down the drawbacks of traditional payment system.**

**Answer:**

Here are some of the main disadvantages of using cash, cheques, and credit cards as payment methods:

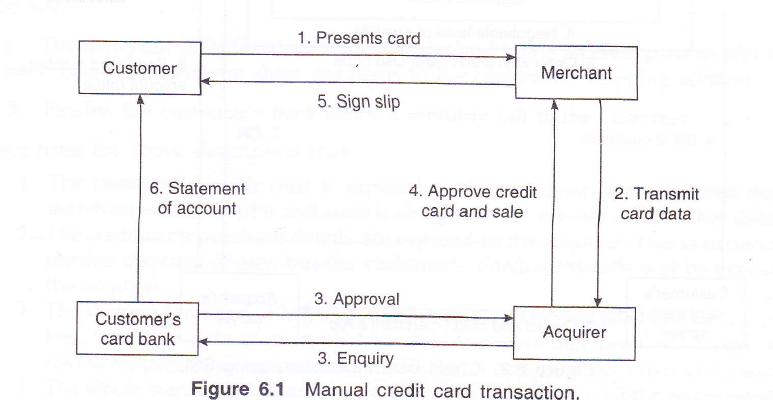
* **They are inconvenient**: They often require physical presence and do not offer the option to transact remotely. They require manual tracking and record-keeping, which can be time-consuming and error-prone.
* **They are not as secure**: Cash can be easily stolen or lost, cheques can be easily forged, and credit cards can be hacked. From June 2020 to June 2021, there were $490.1 million in fraudulent transactions on cards in Australia.
* **They are costly**: Traditional payment systems have high transaction costs for businesses and customers. For example, if you want to use an American Express to purchase something, you’ll likely be paying a percentage fee.
* **They have a slow processing time**: Traditional payment systems can be extremely slow to process, particularly when compared to today’s payment methods. For instance, depositing a cheque into your bank account could take several days for the funds to become available.

**(b) Enumerate the entities involved in a credit card payment system and their individual roles.**

**Answer:**

There are four parties involved in credit card transactions when a customer visits a shop to buy items. They are:

1. A **customer** who owns a credit card.
2. A **merchant** who accepts credit cards (typically a merchant would accept credit cards of several companies such as Visa, Master card, etc.)
3. A **bank** which issues credit cards to customers, guarantees payment to merchants and collects bills from its customers.
4. An **acquirer** which is normally another bank which establishes an account with a merchant, validates card information presented by a merchant and approves sales based on a customer's credit status.

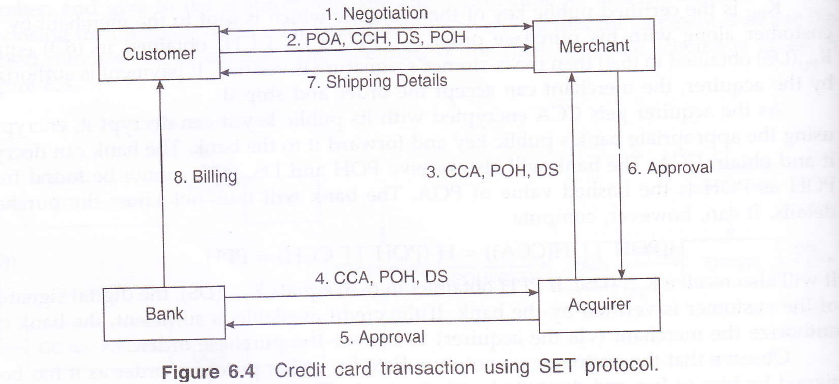


Credit card transactions are carried out as follows:

1. A customer presents a credit card to a merchant after purchasing items from a store and agreeing to pay the billed amount.
2. The merchant swipes the card using a teleterminal which reads the data contained in the magnetic strip of the card and enters the transaction amount. The card data and amount are transmitted to the acquirer via a private communication line.
3. The acquirer's computer forwards the data to the bank which issued the card. The bank checks the validity of the card, credit available on the card and approves transaction provided the card and credit are OK.
4. The acquirer sends approval to merchant. The terminal at the merchant's premises prints a slip in duplicate approving the sale and the amount charged. The acquirer also credits the merchant's account with sale amount minus commission. The acquirer collects the amount from customer's bank.
5. The merchant requests the customer to sign the approval slip, compares the signature with that in the card and if OK delivers the goods.
6. The bank sends a monthly statement to the customer and collects the outstanding amount.

**(c) Explain with a block diagram how credit card transaction is performed using SET protocol.**

**Answer:**



The procedure is below:

**Step 1:** The customer's PC and merchant's server exchange their certified public keys. The merchant also sends acquirer's public key to the customer. They also negotiate the type of public key encryption and the hashing function to be used.

**Step 2:** The customer fills the purchase order, amount payable and credit card number in his or her PC. Software in the PC strips it into two parts; purchase order and amount (POA) and the credit card number and amount (CCA). POA is encrypted using merchant's public key and CCA with acquirer's public key. The PC also computes POH, CCH and the dual signature DS. These are also sent along with POA to the merchant. The merchant verifies signature and proceeds further if the signature is OK.

**Step 3:** The merchant forwards encrypted CCA, POH and DS to the acquirer.

**Step 4:** The acquirer forwards it to the customer's bank.

**Step 5:** The customer's bank checks the credit card number, credit available and the dual signature of the customer. The result of verification is sent to the acquirer.

**Step 6:** The acquirer in turn approves or rejects the transaction and informs the merchant. It credits in merchant's account.

**Step 7:** The merchant approves the order and sends to the customer the shipping details.

**Step 8:** At the end of the month the bank which issued customer's credit card sends a consolidated bill to the customer.