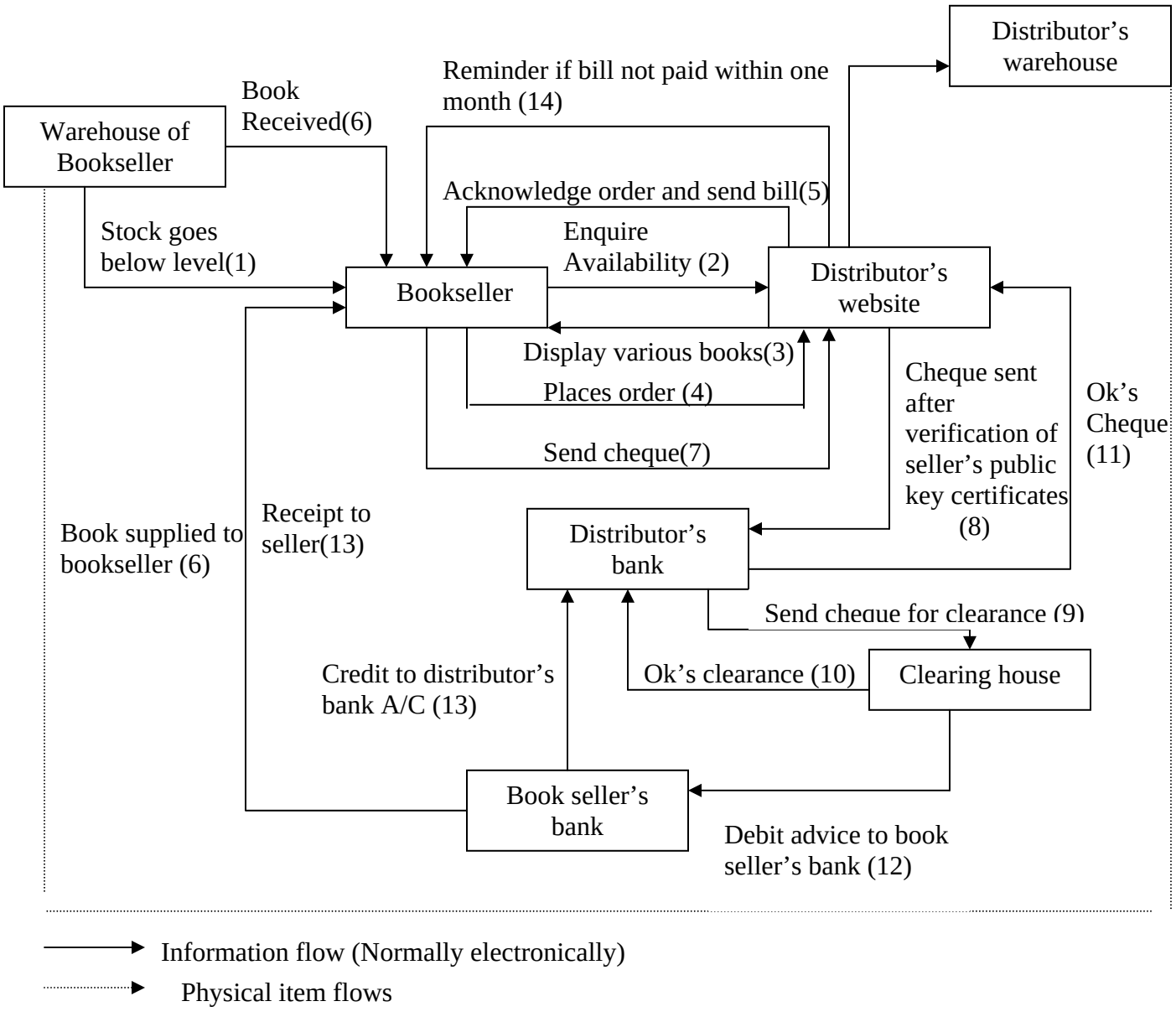
MODULE 13

ELECTRONIC COMMERCE

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



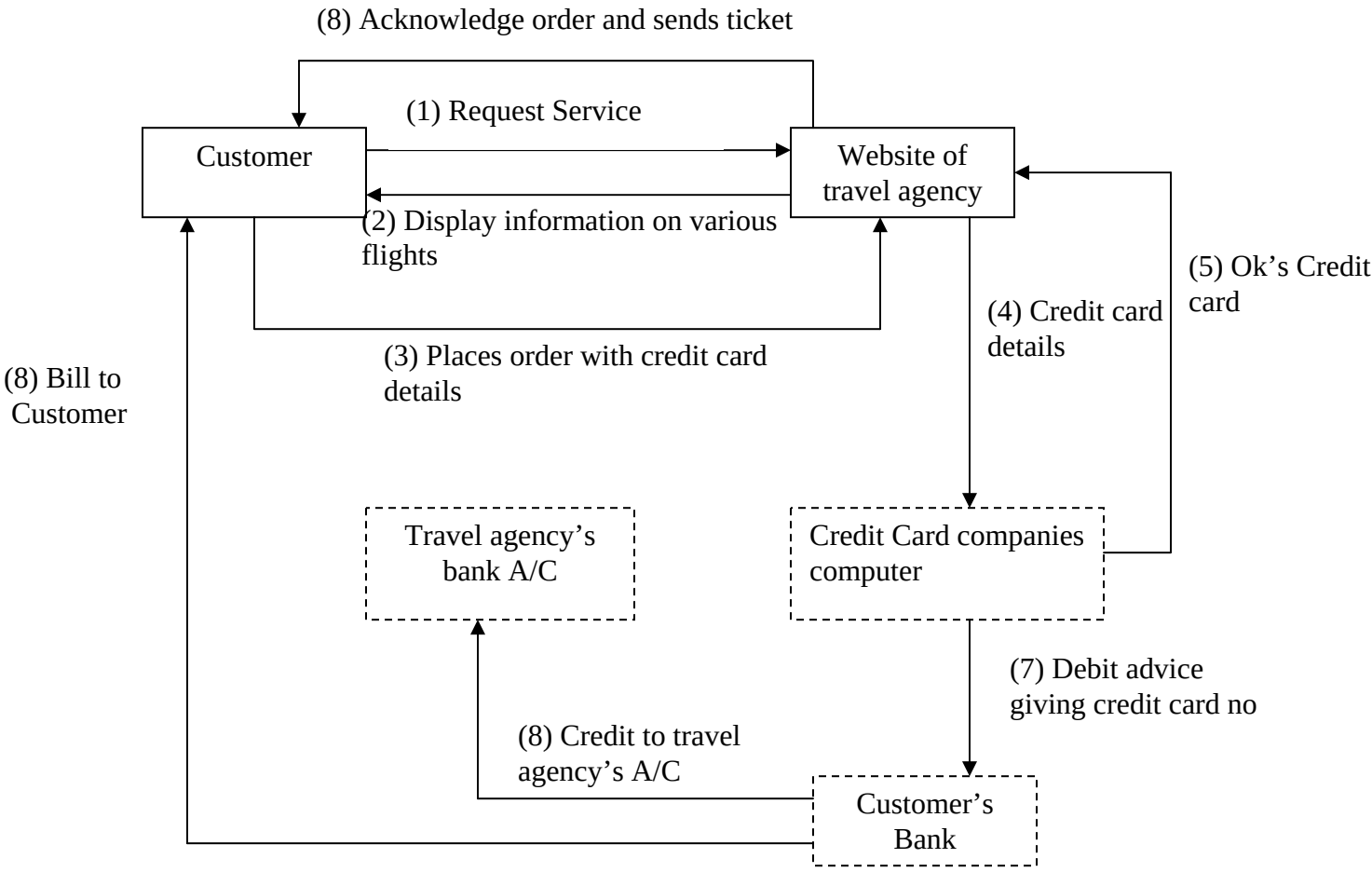
13.2 Explain B2C e-Commerce of a customer reserving airline tickets from his home

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.

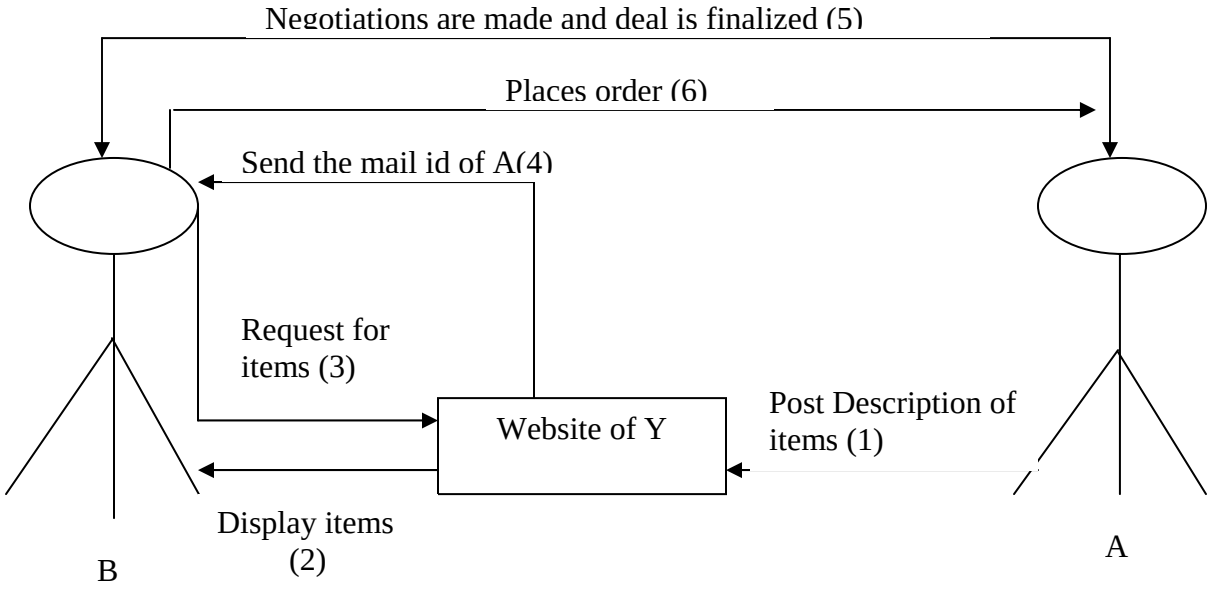
For example: Consider a company Y which acts as a broker. Suppose an indivi-dual A has to sell some items, so it will post the description of the items in Y's site. A person B is interested to purchase some items, then he/she will visit Y's site.

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.

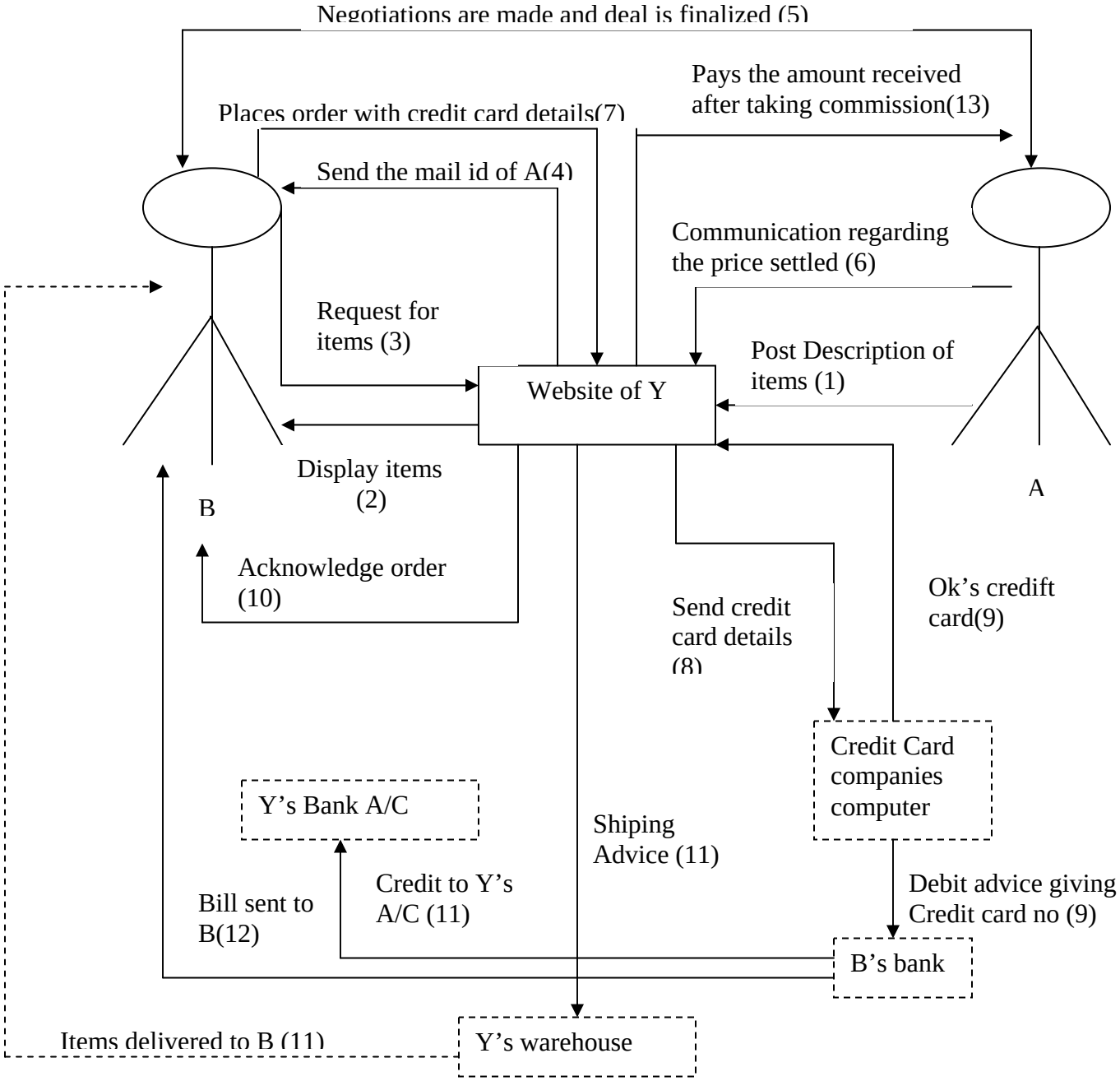
This is described in the block diagram below:



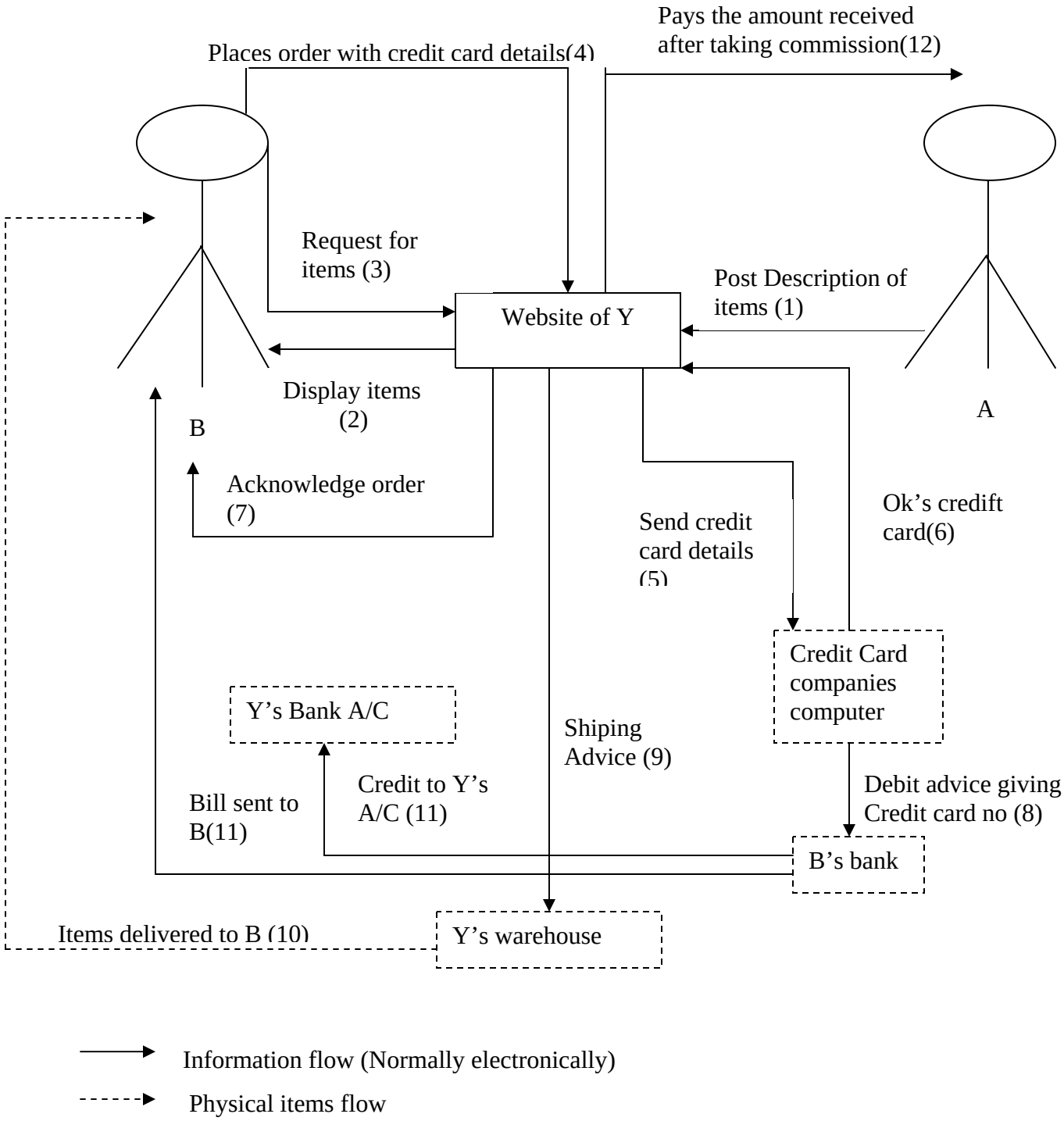
Case II:

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:



Case III:
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 → letter + 6) and obtain the cipher text.

Step 1: write the message in block of 6 characters
THISIS ASAMPL ESENTE NCEFOR ENCRYP TION

Step 2: follow permutation(231564)
HITISS SAAPLM SEETEN CENORF NCEYPR TION

Step 3: make substitution (Letter → 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.

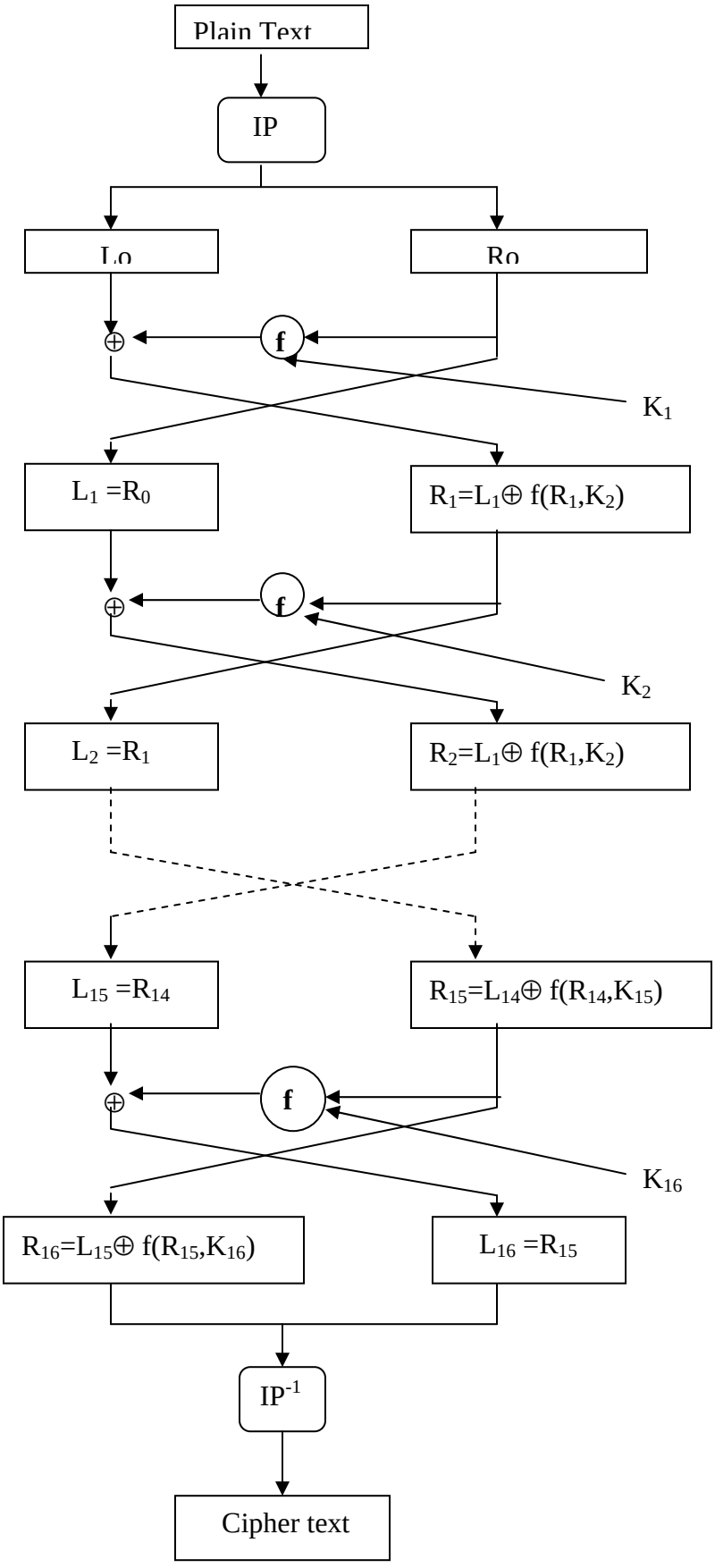
In each round as shown in the figure (page 210) the key bits are shifted, and then 48 bits are selected from the 56 bits of the key. The right half of the data is expanded to 48 bits, combined with 48 bits of a shifted and permuted key via an XOR, then again converted to 32 new bits, and permuted again. 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.


Plain Text
IP
L0
R0
f
K1
L1 =R0
R1=L1⊕ f(R1,K2)
f
K2
L2 =R1
R2=L1⊕ f(R1,K2)
L15 =R14
R15=L14⊕ f(R14,K15)
f
K16
R16=L15⊕ f(R15,K16)
L16 =R15
IP-1
Cipher text

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

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.
persons.

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".