MyNotes On Changes/Revision in

INFORMATION TECHNOLOGY [PAPER 7A]

for CA-Intermediate (IPC) Course

Dear Students,

As most of you are aware that ICAI has revised Study Material for CA-Intermediate (IPC) Course [Earlier knows as CA-IPCC/PCC] in July 2012 and the revised study material is First Time applicable in CA examinations in May 2013.

In past few days I have received so many queries from students about what is in course or what changes have been made. So, finally I decided to come with an amendment booklet containing changes made in ICAI Study material.

Students must note that ICAI has removed Unit I & II from chapter -1 and not complete Chapter 1 & 2 from November 2012 examinations and onwards.

NOTE: ALL NOTES GIVEN IN CLASSES TO MY REGULAR STUDENTS ARE THOROUGHLY REVISED AND CONTAIN ALL CHANGES GIVEN IN THIS BOOKLET. SO THEY NEED NOT TO REFER THIS BOOKLET.

FROM THE DESK OF:

CA KUNAL AGRAWAL
[ACA, DISA (ICAI), B.COM.]

Authored by::

CA KUNAL AGRAWAL

[ACA, DISA (ICAI), B.COM.]
CONTACT NO. +91-99295-03735

Regular Classes @
BADALA COMMERCE CLASSES, UDAIPUR

Changes Made in Chapter – 3

1. TYPES OF MODEM

Modem is the coding/encoding device which converts digital computer signals into analog signals and converts an analog signal into a digital computer signals. Modems are required if digital computers are connected to an analog channel like old telephone lines.

Types of MODEMs: MODEMs are classified on the basis of different criteria such as the place where they are installed, the manner in which they accept information and the way they transmit signals. Based on these criteria, MODEMs are classified into the following types:

External vs. Internal Modems (on the basis of place where they are installed)

External modem separated from the computer system unit and is connected to the serial port of the computer by means of a cable.
An internal modem is a circuit board (a modem card) installed inside a desktop or laptop computer, allowing the computer to communicate over a network with other connected computers.

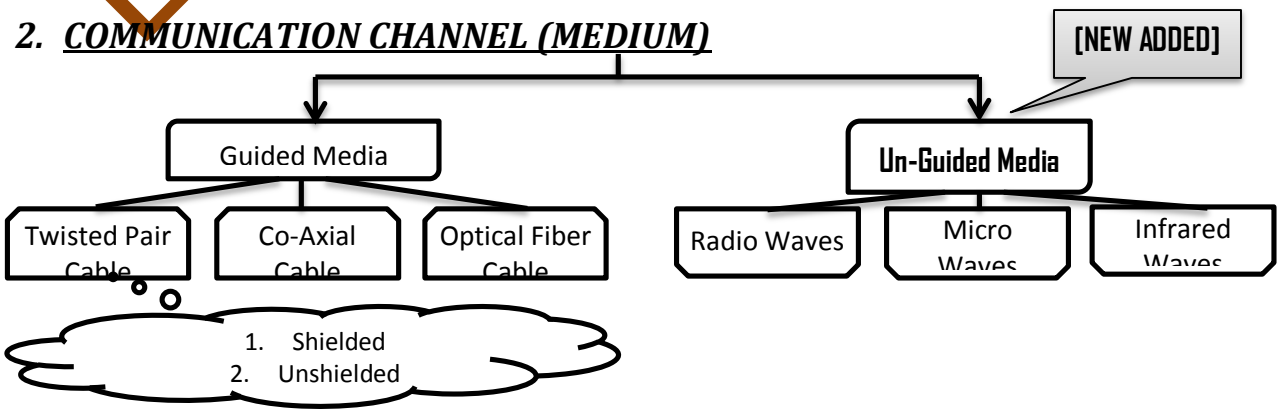
Standard vs. Intelligent Modems (on the basis of the manner in which they accept information)

Standard modems are usually operated by commands entered from a keyboard. Users control the functions (dialing, etc.) of a modem through the keyboard.
Intelligent modems are also called Advanced modems that can accept new instructions and then respond to the commands while transmitting data and information. These can be done by microprocessor chips and internal Read Only Memory (ROM) contained in the modem. These modems are more expensive.

Short~Haul and Wireless Modems (on the basis of the way the signals are transmitted)

Short-haul modems are devices that transmit signals down the cable through any COM1 port. They sometimes are called modem eliminators, because they do not require an external power source. This type of modem can be used within or across several buildings in a company or a university campus.
Wireless modems transmit the data signals through the air instead of by using a cable. They sometimes are called a radiofrequency modem. This type of modem is designed to work with cellular technology

2. COMMUNICATION CHANNEL (MEDIUM)



Unguided Media: Unguided Transmission Media consists of a means for the data signals to travel but nothing to guide them along a specific path. The data signals are not bound to a cabling media and as such are often called Unbound Media. Some of the common examples of unguided media are:

1. ***Radio Waves***:
   a. Do not require any physical media or cables for data transmission.
   b. Invisible form of electromagnetic radiation that varies in wavelength from around a millimetre to 100,000 km, making it one of the widest ranges in the electromagnetic spectrum.
   c. Radio waves are most commonly used transmission media in the wireless Local Area Networks.
2. ***Micro Waves***:
   a. Microwaves are radio waves with wavelengths ranging from as long as one meter to as short as one millimetre, or equivalently, with frequencies between 300 MHz (0.3 GHz) and 300 GHz.
   b. These are used for communication, radar systems, radio astronomy, navigation and spectroscopy.
3. ***Infrared Waves***:
   a. Infrared light is used in industrial, scientific, and medical applications.
   b. Night-vision devices using infrared illumination allow people or animals to be observed without the observer being detected.
   c. Infrared tracking, also known as infrared homing, refers to a passive missile guidance system which uses the emission from a target of electromagnetic radiation in the infrared part of the spectrum to track it.

Some portion revised in July 2012

3. TRANSMISSION TECHNIQUES:

Based on the techniques used to transfer data, communication networks can be categorized into Broadcast and Switched networks.
In Broadcast networks, data transmitted by one node is received by many, sometimes all, of the other nodes.
In switched-communication networks, however, the data transferred from source to destination is routed through the switch nodes. The way in which the nodes switch data from one link to another as it is transmitted from source to destination node is referred to as a "switching technique". Three common switching techniques are Circuit Switching, Packet Switching, and Message Switching.

3.1 Circuit Switching:

- ✓ In circuit switching a single circuit is formed between two devices and communication is allowed for a limited duration of the call until the call is cut as in a telephone or a VPDN.
- ✓ In circuit switching, this path is decided upon before the data transmission starts.
- ✓ Like in home phones when we place a call, we either get our destination party or encounter a busy signal. A single circuit is used for the entire duration of the call.

3.2 Message Switching:

May 2011

- ✓ In this technique, intermediate switch will store data received from sending device and forward it when network is available.
- ✓ So, when congestion occurs or all network resources are occupied, rather than discarding (or delete) the traffic (data), the message-switched network will store and delay the traffic until sufficient resources are available for successful delivery of the message.

- ✓ There is no direct connection between the source and destination nodes.
- ✓ Each intermediary node within the network must store all messages before retransmitting them one at a time as proper resources become available. This characteristic is often referred to as "**store-and forward**".

- ✓ Message switching techniques were originally used in data communications. Early examples of message switching applications are paper tape relay systems and telex networks. Electronic mail (e-mail) and voice mail are also examples of message switching systems.

3.3 Packet Switching:

In Packet Switching a message is broken into small parts (packets) and routed individually through the network depending on the availability of a channel for each packet instead of a continuous stream. This type of transmission is popular in case on Internet.

CIRCUIT SWITCHING	PACKET SWITCHING
A dedicated path is used throughout the data transmission.	Each packet is transmitted through different routes.
It is more reliable because of the availability of a circuit dedicated for a session.	It is less reliable because non-availability of dedicated lines.
Circuit switching is old and expensive	Packet switching is more modern and less expensive

4. *DISADVANTAGES OF THREE TIER ARCHITECTURE:*

- Creates an increased need for network traffic management, server load balancing, and fault tolerance.
- Maintenance tools are currently inadequate for maintaining server libraries. This is a potential obstacle for simplifying maintenance and promoting code reuse throughout the organization.

5. *FEATURES OF DATA CENTERS (ONLY NEW POINTS COVERED)*

Backup Systems	A data center should have the provision of automatically providing backup data services to all shared hosting solutions. Full back up may be taken for full system restoration and off-server and off-site backup services should also be available as well.
Continuous Monitoring 24x7	24x7x365 monitoring must be there in data centers for the security of the data. Such a monitoring will be done for all the hardware including routers, switches, UPS systems and servers. In addition, the network operations and all the critical services related to the Internet and associated technologies namely FTP, HTTP, SMTP should also be monitored.
Environment – Cooling	Cooling infrastructure is a significant part of a data center. The complex cooling infrastructure creates the optimal computing environment, ensuring the longevity of the servers. The quad-compressor / dual-blower redundant systems provide a virtually dust-free and particle – free computing environment, with temperature, humidity, and air-quality regulation.

6. DATA CENTER PROTECTION CHALLENGES AND BEST PRACTICE SOLUTIONS

Large enterprises IT management look for ways to mitigate the cost, risk and complexity of data protection throughout their enterprises – including data centers, disaster recovery sites and branch locations. Some of the top challenges faced by the management are as follows:

1. **Control skyrocketing data growth**:
   1) Data growth is the biggest data center hardware infrastructure challenge for large enterprises.
   2) Data deduplication technologies that helps in reducing data storage needs by eliminating redundant data.

2. **System performance and scalability**:
   To avoid data center sprawl in the data protection environment, IT managers should look ahead 3-5 years and choose a data protection "target" system that will scale to accommodate the performance and capacity they will need without adding new system.

3. **Network congestion and connectivity architecture:**
   1) The new generation of servers with multicore processors demands significantly high input/output (I/O).
   2) Vendors should help its customers to be strategic with their network infrastructure.

4. **IT administration and staff time at premium**:
   1) Minimum requirements for large enterprise data protection platforms include:
      a. Automatic load balancing and tuning.
      b. Automatic system monitoring and "phone home" functionality. Choose systems that preemptively identify potential hardware issues and notify administrators before a problem arises.
      c. Provide dashboards and reporting.

5. **Inadequate Disaster Recovery plans:**
   1) Large enterprises that have been using physical tape backup systems in branch offices are particularly vulnerable to downtime and data loss in the event of a disaster.
   2) Enterprise IT managers should consider the use of remote-office backup, deduplication, replication and restore operations from a data center headquarters.

6. **Adopting new risk prone, cost-effective data protection technologies**:
   IT managers should look for enterprise-class data protection solutions that mitigate migration costs and risk with features such as robust tape emulation and storage pooling.

7. **Resource balancing**:
   1) The enterprise chief technical officer today needs to strike a working balance between reduced operational budgets, maximizing availability, ensuring round-the-clock monitoring etc..
   2) This is why even some of the largest enterprises in the world choose to host their mission-critical and sensitive data with established data centers.

7. THREATS AND VULNERABILITIES:

A threat is anything that can disrupt the operation, functioning, integrity, or availability of a network or system.

Network security threats can be categorized into four broad themes:

1. **Unstructured threats** –
   a. These originate mostly from inexperienced individuals using easily available hacking tools from the Internet.
   b. Many tools available to anyone on the Internet can be used to discover weaknesses in a company's network. These include port-scanning tools, address-sweeping tools, and many others.
   c. Most of these kinds of probes are done more out of curiosity than with a malicious intent in mind.
2. **Structured threats** –
   a. These originate from individuals who are highly motivated and technically competent and usually understand network systems design and the vulnerabilities of those systems.
   b. They can understand as well as create hacking scripts to penetrate those network systems.
   c. An individual who presents a structured threat typically targets a specific destination or group. Usually, these hackers are hired by organized crime, industry competitors, or state-sponsored intelligence organizations.
3. **External threats** –
   a. These originate from individuals or organizations working outside an organization, which does not have authorized access to organization's computer systems or network.
   b. They usually work their way into a network from the Internet or dialup access servers.
4. **Internal threats** –
   a. Typically, these threats originate from individuals who have authorized access to the network.
   b. These users either have an account on a server or physical access to the network. An internal threat may come from a discontented former or current employee or contractor.
   c. It has been seen that majority of security incidents originate from Internal threats.

Vulnerabilities: Vulnerability is an inherent weakness in the design, configuration, or implementation of a network or system that renders it susceptible to a threat.

The following facts are responsible for occurrence of vulnerabilities in the software:

1. **Software Bugs** –
   a. Software bugs are so common that users have developed techniques to work around the consequences, and bugs that make saving work necessary every half an hour or crash the computer every so often are considered to be a normal part of computing.
   b. For example - buffer overflow, failure to handle exceptional conditions, access validation error, input validation errors are some of the common software flaws.
2. **Timing Windows** –

This problem may occur when a temporary file is exploited by an intruder to gain access to the file, overwrite important data, and use the file as a gateway for advancing further into the system.

3. **Insecure default configurations** –
   a. Insecure default configurations occur when vendors use known default passwords to make it as easy as possible for consumers to set up new systems.
   b. Unfortunately, most intruders know these passwords and can access systems effortlessly.
4. **Bad Protocols** –
   a. Some protocols, or the standards by which information is exchanged over the internet, lack any security at all.
   b. For example, unsolicited commercial email, commonly referred to as "spam," is the irritating result of poor protocol programming.
5. **Trusting Untrustworthy information**-
   a. This is usually a problem that affects routers, or those computers that connect one network to another.
   b. When routers are not programmed to verify that they are receiving information from a unique host, bogus routers can gain access to systems and do damage.
6. **End users** –
   a. Generally, users of computer systems are not professionals and are not always security conscious.
   b. For example, when the number of passwords of an user increases, user may start writing them down, in the worst case to places from where they are easy to find.
   c. In addition to this kind of negligence towards security procedures users do human errors, for example save confidential files to places where they are not properly protected.

8. *IDS COMPONENTS*

Intrusion Detection Systems are generally made up of following major components:

1. **Sensors**: These are deployed in a network or on a device to collect data. They take input from various resources, including network packets, log files, and system call traces. Input is collected, organized, and then forwarded to one more analyzers.
2. ***Analysers***: Analysers in IDS collect data forwarded by sensors and then determine if an intrusion has actually occurred. Output from analyzers should include evidence supporting the intrusion report. The analyzers may also provide recommendations and guidance on mitigation steps.
3. ***User interface***: The user interface of the IDS provides the end users a view and way to interact with the system. Through the interface, the user can control and configure the system. Many user interfaces can generate reports as well.
4. **Honeypot**:
   a. In fully deployed IDS, some administrators may choose to install a “Honeypots”, essentially a system components setup as bait or decoy for intruders.
   b. Honeypots can be used as early warning systems on an attack, decoys from critical systems, and data collection sources for attack analysis.
   c. A honeypot should only be deployed when the organization has the resources to maintain it.
   d. Many IDS vendors maintain honeypots for research purposes and to develop new intrusion signatures. A honeypot left unmanaged may become a significant liability because attackers may use a compromised honeypot to attack other systems.

Changes Made in Chapter – 4

9. MAJOR FUNCTIONAL COMPONENTS OF THE WWW

1) **HTML** – Hyper Text Markup Language is the language in which web pages are written. It is language used to create web pages.
2) **HTTP** – Hypertext Transfer Protocol (HTTP) is defined as trhe set of rules for transferring files (text, graphic images, sound, video and other multimedia files) on the World Wide Web.
3) **URIs**: Uniform Resource Identifier (URI) is a string of character used to identify a resource. It is of 2 types.
   a. URN – Uniform Resource Name identifies a resource by NAME.
   b. URL – Uniform Resource Locator identifies network location of a resources. The format of a URL is 'protocol/Internet address/Web page address.
   c. For example – http://www.icai.org/ipcc.html
4) **Web Hardware & Software**:
   a. Web pages resides on server that run special software that allow users to access web pages.
   b. A user can directly access any Web page on one of these servers and then follow the links to other pages. This process creates a Web of links around the world and, thus, the name World Wide Web is given.
   c. Computer reading the Web pages are classed Web Clients. Web clients view the pages with a program called Web Browser.
   d. A browser fetches a Web page from a server by a HTTP request. This request is a standard HTTP request containing a page address.
   e. The browser software interprets the HTML commands and displays the information on user's monitor. It is important to note that different browsers can interpret an HTML command differently and thus display text differently.

10. DIFFERENCE BETWEEN INTERNET AND WWW

	Internet	WWW
Nature	Hardware	Software
Comprises of	Network of Computers, copper wires, fiber - optic cables & wireless networks	Files, folders & documents stored in various computers
Governed By	Internet Protocol	Hyper Text Transfer Protocol
Dependency	This is the base platform and is independent of WWW Other services over the Internet includes e0-mail, chat & file transfer service.	It depends on the Internet to work

11. INTERNET PROTOCOL SUITE

Layer	TCP / IP Protocols
1. Application	FTP, HTTP, IRC, POP3, SMTP, NMTP
2. Transport	TCP, UDP
3. Network	IP (IPv4, IPv6), ARP
4. Link	Ethernet, Wi-Fi, Token ring, PPP

1) **HTTP – Hyper Text Transfer Protocol** :
   a. The WWW is driven by two fundamental technologies: HTTP and HTML.
      i. HTTP is the Hypertext Transfer Protocol that controls how Web-server & Web browser communicate with each other.
      ii. HTML is the Hypertext Markup Language that defines the structure and contents of a page.
   b. To receive a Web page, the browser sends a HTTP request to a web server.
   c. Most web browsers are capable of FTP as well as viewing web pages, the HTTP tells the browsers what kind of information to expect.

2) **SMTP – Simple Mail Transfer Protocol** :
   a. The Simple Mail Transfer Protocol (SMTP) controls the transfer of email message on the internet using TCP.
   b. An SMTP transaction consists of 3 command/reply sequences such as:
      i. MAIL command, to establish the return address.
      ii. RCPT command, to establish a recipient of the message. This command can be issued multiple times, one for each recipient.
      iii. DATA command to send message text. It consists of a message header and a message body separated by an empty line. DATA command is actually group of commands, and the server replies twice:
         1. Once that DATA command from client is proper, to acknowledge that server is ready to receive text, and
         2. The second time after end-of-data sequence, to rather accept or reject the entire message.

3) **FTP – File Transfer Protocol** :
   a. The File Transfer Protocol (FTP) is used widely on the Internet for transferring files to and from a remote host.
   b. FTP is commonly used for uploading pages to a Web site and for providing online file archives.
   c. An FTP URL has the basic form: ftp://user:pass@host/directory/file
   d. FTP distinguishes between text files and binary files.

4) **NNTP - Network News Transfer Protocol** :
   a. The Network News Transfer Protocol (NNTP) is the basis for tens of thousands of newsgroups that provide a public forum for millions of Internet users.
   b. NNTP consists of two components:
      i. A list of newsgroups supported by a specific newsgroup server (newsgroups are typically selected by an Internet service provider);
      ii. And a database of messages that are currently available for any particular newsgroup.

5) **CGI - Common Gateway Interface** :
   a. The Common Gateway Interface is used with many Web servers to provide processing beyond the normal HTTP Web interface.
   b. CGI requests are submitted from Web browsers to Web servers. When a server receives a CGI request, it typically executes a script (or a program) to process the request and return a result to the browser.
   c. Like when we enter roll no on result site, roll no is submitted to web server using HTTP request, then server execute a kind of CGI script and display result.

6) **TCP - Transmission Control Protocol** :
   a. The TCP provides reliable transmission of data in an IP environment.
   b. TCP corresponds to the transport layer (Layer 4) of the OSI reference model.
   c. Among the services TCP provides are stream data transfer, reliability, efficient flow control, full-duplex operation, and multiplexing.

7) **IP - Internet Protocol** :
   a. The Internet Protocol (IP) is a network-layer (Layer 3) protocol
   b. It contains addressing information and some control information that enables packets to be routed.

8) **VoIP - Voice over Internet Protocol**:
   a. Voice over IP (VoIP) commonly refers to the communication protocols, technologies, methodologies, and transmission techniques used to transmit voice communications and multimedia data over Internet Protocol (IP) networks, such as the Internet.
   b. This allows delivery of voice communications over IP networks, for example, phone calls.

9) **ARP - Address Resolution Protocol ARP** :
   a. For two machines on a given network to communicate, they must know the other machine's physical (or MAC) addresses.
   b. By broadcasting Address Resolution Protocols (ARPs), a host can dynamically discover the MAC-layer address corresponding to a particular IP network-layer address.

10) **ICMP - Internet Control Message Protocol** :
   a. The Internet Control Message Protocol (ICMP) is a network-layer Internet protocol
   b. It provides errors reports and other information regarding IP packet processing back to the source.

11) **UDP - User Datagram Protocol** :
   a. The User Datagram Protocol is another transport layer protocol that provides a connectionless method of communicating between machines.
   b. The operation of UDP is much different than TCP.
   c. UDP is simpler, but it is essentially unreliable.
   d. There is no guarantee that a packet will ever reach its destination. In addition, UDP has no flow control. If we send messages too quickly, packets may be lost.

Just for understanding

TCP → Speed Post
UDP → Normal Post

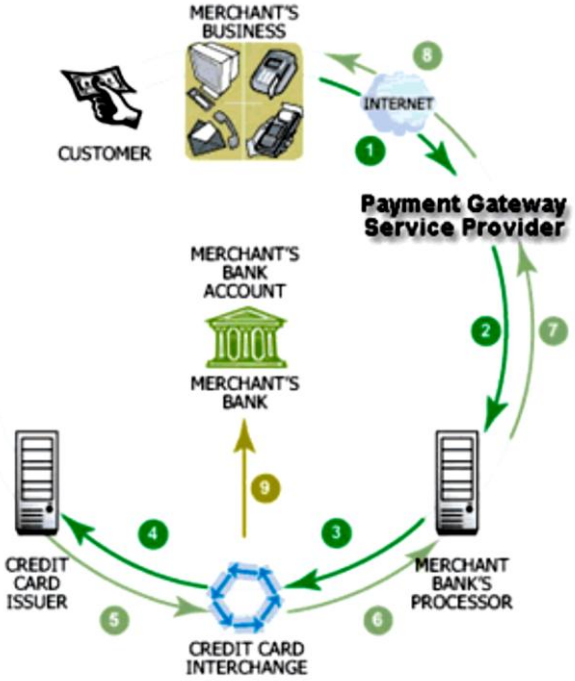
12) **Telnet**:
   a. Telnet is a protocol that allows us to connect to remote computers (called hosts) over a TCP/IP network (such as the Internet).
   b. We use software called a telnet client on our computer to make a connection to a telnet server (i.e., the remote host).
   c. In most cases, we will need to log into the remote host, which requires that we have an account on that system.

12. HOW CREDIT CARD ARE PROCESSED???

Before going further let's understand same important terms:

- ✓ ***Acquirer***: A bank that processes and settles a merchant's credit card transactions with the help of a card issuer.
- ✓ ***Cardholder***: The owner of a card that is used to make credit card purchases.
- ✓ ***Card network***: Visa, MasterCard or other networks that act as an intermediary between an acquirer and an issuer to authorize credit card transactions.
- ✓ ***Discount fee***: A processing fee paid by merchants to acquirers to cover the cost of processing credit cards.
- ✓ ***Interchange fee***: A charge paid by merchants to a credit card issuer and a card network as a fee for accepting credit cards. They generally range from 1 to 3 percent.
- ✓ ***Issuer***: A financial institution, bank, credit union or company that issues or helps issue cards to cardholders.

A general life cycle of electronic payment through credit card is shown below



Step 1: Authorization–

This is the first step in processing a credit card. After a merchant swipes the card, the data is submitted to merchant's bank, called an acquirer, to request authorization for the sale. The acquirer then routes the request to the card issuing bank, where it is authorized or denied, and the merchant is allowed to process the sale.

1) The cardholder requests a purchase from the merchant.
2) The merchant submits the request to the acquirer.
3) The acquirer sends a request to the issuer to authorize the transaction.
4) An authorization code is sent to the acquirer if there is valid credit available.
5) The acquirer authorizes the transaction.
6) The cardholder receives the product.

Step 2: Batching–

This is the second step in processing a credit card. At the end of a day, the merchant reviews all the day's sales to ensure they were authorized and signed by the cardholder. It then transmits all the sales at once, called a batch, to the acquirer to receive payment.

1) The merchant stores all the day's authorized sales in a batch.
2) The merchant sends the batch to the acquirer at the end of the day to receive payment.

Step 3: Clearing–

This is the third step in processing a credit card. After the acquirer receives the batch, it sends it through the card network, where each sale is routed to the appropriate issuing bank. The issuing bank then subtracts its interchange fees, which are shared with the card network, and transfers the remaining amount through the network back to the acquirer.

1) The batch is sent through the card network to request payment from the issuer.
2) The card network distributes each transaction to the appropriate issuer.
3) The issuer subtracts its interchange fees, which are shared with the card network, and transfers the amount.
4) The card network routes the amount to the acquirer.

Step 4: Funding–

This is the fourth and final step in processing a credit card.After receiving payment from the issuer, minus interchange fees, the acquirer subtracts its discount fee and sends the remainder to the merchant. The merchant is now paid for the transaction, and the cardholder is billed.

1) The acquirer subtracts its discount rate and pays the merchant the remainder.
2) The cardholder is billed.

Using Credit Card over Internet

1) Using a credit card to make a purchase over the Internet follows the same scenario.

2) But on the Internet, added steps must be taken to provide for secure transactions and authentication of both buyer and seller.

3) To address these growing security concerns the two leading credit card brands, Visa and MasterCard, teamed up some years ago to develop a common standard to process card transactions on the Internet, called the Secure Electronic Transaction (SET) standard.

4) Secured Electronic Transaction (SET) protocol (SET) was developed by MasterCard and Visa for handling credit card transactions over the Internet. SET uses digital certificates to ensure the identities of all parties involved in a purchase. SET also encrypts credit card and purchase information before transmission on the Internet.

5) SET addresses **seven major business requirements**:

   SET is a standard which will ensure that credit card and associated payment order information travels safely and securely between the various involved parties on the Internet.

   a. Provide confidentiality of payment information and enable confidentiality of order information that is transmitted along with the payment information.
   b. Ensure the integrity of all transmitted data.
   c. Provide authentication that a cardholder is a legitimate user of a branded Payment card account.
   d. Provide authentication that a merchant can accept branded payment card transactions through its relationship with an acquiring financial institution.
   e. Ensure the use of the best security practices and system design techniques to protect all legitimate parties in an electronic commerce transaction.
   f. Create a protocol that neither depends on transport security mechanisms nor prevents their use.
   g. Facilitate and encourage interoperability among software and network providers.

SET principally uses cryptography which is defined as the science of encrypting messages, that is, converting clear text to cipher text using an algorithm, and then converting it back from cipher text to clear text using the same or another algorithm. Secret Key Cryptography (SKC) and Public Key Cryptography (PKC) are two common encryption methods.

⇒ **In Secret key Cryptography (also called Symmetric Key Cryptography), the sender uses a single 56-bit key (also called a symmetric key) to encrypt information, and the receiver will use the same key to decrypt.**

⇒ **A much more secure and sophisticated encryption method is Public Key Cryptography (PKC), also known as Asymmetric Key Cryptography, which uses two keys. Any one key (it does not matter which) can be used to encrypt and the other can be used to decrypt.**

13. E-COMMERCE RISK AND SECURITY CONSIDERATIONS

The different dimensions of E-commerce security are as follows:

1. **Integrity** -The ability to ensure that information being displayed on a web site or transmitted or received over the internet has not been altered in any way by an unauthorized party.

2. **Non-repudiation** -The ability to ensure that e-commerce participants do not deny (i.e. repudiate) their online actions.

3. **Authenticity** -The ability to identify the identity of a person or entity with whom we are dealing in the internet.

4. **Confidentiality** -The ability to ensure that messages and data are available only to those who are authorized to view them.

5. **Privacy** -The ability to control the use of information about oneself.

5. **Availability** -The ability to ensure that an e-commerce site continues to function as intended.

Dear Students,

I have something very important to share with you.
I have noticed that students generally take ITSM as just a theory subject and not give much importance to this subject.
Here I want to tell you that in today's global competitive environment, Information Technology is just like life blood for any organisation. The need is to understand it and implement it.
And as you all know job/work profile of Chartered Accountants is very diverse, they are expected to have knowledge of Information Technology.
Same case is with Strategic Management. A Chartered Accountant is supposed to have part in strategic decision of the organisation.

So, friends do not take this subject just as another theory paper but give adequate importance to this paper.

One more thing, syllabus of this paper is much lesser as compared to other subject. So, if proper time is given you can even score very well in this paper.

With Best Wishes....

FROM THE DESK OF:

CA KUNAL AGRAWAL
[ACA, DISA (ICAI), B.COM.]