COURSE CONTENT

Unit I

Computer Fundamentals

What is Computer?

Computer is an advanced electronic device that takes raw data as input from the user and processes these data under the control of set of instructions (called program) and gives the result (output) and saves output for the future use. It can process both numerical and non-numerical (arithmetic and logical) calculations.

A computer has four functions:

a. accepts data	**Input**
b. processes data	**Processing**
c. produces output	**Output**
d. stores results	**Storage**

CENTRAL PROCESSING UNIT (CPU)

The main unit inside the computer is the CPU. This unit is responsible for all events inside the computer. It controls all internal and external devices, performs arithmetic and logic operations. The CPU (Central Processing Unit) is the device that interprets and executes instructions

Software

Software, simply are the computer programs. The instructions given to the computer in the form of a program is called Software. Software is the set of programs, which are used for different purposes. All the programs used in computer to perform specific task is called Software.

Types of software

1**. System software:**

a) Operating System Software

DOS, Windows XP, Windows Vista, Unix/Linux, MAC/OS X etc.

b) Utility Software

Windows Explorer (File/Folder Management), Windows Media Player, Anti-Virus Utilities, Disk Defragmentation, Disk Clean, BackUp, WinZip, WinRAR

2. Application software:

a) Package Software

Ms. Office 2003, Ms. Office 2007, Macromedia (Dreamweaver, Flash, Freehand), Adobe (PageMaker, PhotoShop)

b) Tailored or Custom Software

SAGE (Accounting), Galileo/Worldspan (Travel) etc.

3. Computer Languages & Scripting:

a) Low Level Language

i) Machine Level Language

ii) Assembly Language

Machine language: These language instructions are directly executed by CPU

Assembly language: The endeavor of giving machine language instructions a name structure that means bit strings of instructions of machine language are given name here

High Level Language: The user friendly language ...more natural language than assembly language.

Assembler is needed to convert assembly language into machine language.

Complier is needed to convert high level to machine language.

b) High Level Language

COBOL (COmmon Business Oriented Language), FORTRAN (FORmula TRANslation), BASIC (Beginner's All-purpose Symbolic Instruction Code), C, C++ etc. are the examples of High Level Language.

Types of Computer

On the basis of working principle

a) Analog Computer

An analog computer (spelt analogue in British English) is a form of computer that uses *continuous* physical phenomena such as electrical, mechanical, or hydraulic quantities to model the problem being solved.

b) Digital Computer

A computer that performs calculations and logical operations with quantities represented as digits, usually in the binary number system.

c) Hybrid Computer (Analog + Digital)

A combination of computers those are capable of inputting and outputting in both digital and analog signals. A hybrid computer system setup offers a cost effective method of performing complex simulations.

On the basis of Size

a) Super Computer

The fastest type of computer. Supercomputers are very expensive and are employed for specialized applications that require immense amounts of mathematical calculations. For example, weather forecasting requires a supercomputer. Other uses of supercomputers include animated graphics, fluid dynamic calculations, nuclear energy research, and petroleum exploration.

The chief difference between a supercomputer and a mainframe is that a supercomputer channels all its power into executing a few programs as fast as possible, whereas a mainframe uses its power to execute many programs concurrently.

b) Mainframe Computer

A very large and expensive computer capable of supporting hundreds, or even thousands, of users simultaneously. In the hierarchy that starts with a simple microprocessor (in watches, for example) at the bottom and moves to supercomputers at the top, mainframes are just below supercomputers. In some ways, mainframes are more powerful than supercomputers because they support more simultaneous programs. But supercomputers can execute a single program faster than a mainframe.

c) Mini Computer

A midsized computer. In size and power, minicomputers lie between *workstations* and *mainframes*. In the past decade, the distinction between large minicomputers and small mainframes has blurred, however, as has the distinction between small minicomputers and workstations. But in general, a minicomputer is a multiprocessing system capable of supporting from 4 to about 200 users simultaneously.

Generations of Computers

Using size and features as the bases, computers are classified into various Generations. These generations of computers are discussed below:

FIRST GENERATION

The first generation computers were bulky in size. They were able to execute

Hundreds of instructions per second and were expensive as well. They used vacuum tubes as their main components. Machine language is a first generation language, for example EDVAC, UNIVAC etc.

SECOND GENERATION

The second-generation computers were smaller in size as compared to the first generation computers. These were capable of executing thousands of instructions per second, with a transistor as its main component. Assembly language is the second generation language in which programs were written using mnemonic codes, for example,PDP (Programmed data processor), PDP1 etc.

THIRD GENERATION

The third generation computers were more advanced and used integrated circuits. These computers contained thousands of components per circuit. They were cheaper than second-generation computers. The languages used in this generation were BASIC, COBOL etc. for example, IBM 307 Series, PDP II etc.

FOURTH GENERATION

The fourth generation computers used complex circuits like the large-scale integrated circuits called microprocessors or chips, which surprisingly cost less than the third generation computers. These computers were able to execute millions of instructions persecond. The languages used in this generation are C++, SQL etc. for example, CRAY 2, IBM3090/600 Series.

FIFTH GENERATION

These computers work on artificial languages (AI) like LISP, PROLOG etc. They use super/ultra large-scale integrated circuits, which is also called parallel processing method. They execute billions of instructions per second, for example, Laptops, Palmtops, PDA (Personal Digital Assistant) etc.

Computer Virus

A computer virus is a type of malicious software program ("malware") that, when executed, replicates by reproducing itself (copying its own source code) or infecting other computer programs by modifying them Infecting computer programs can include as well, data files, or the "boot" sector of the hard drive. When this replication succeeds, the affected areas are then said to be "infected" with a computer virus. The term "virus" is also commonly, but erroneously, used to refer to other types of malware. "Malware" encompasses computer viruses along with many other forms of malicious software, such as computer "worms", ransom ware, Trojan horses, key loggers, root kits, spyware, adware, malicious Browser Helper Object (BHOs) and other malicious software. The majority of active malware threats are actually trojan horse programs or computer worms rather than computer viruses. The term computer virus, coined by Fred Cohen in 1985, is a misnomerViruses often perform some type of harmful activity on infected host computers, such as acquisition of hard disk space or central processing unit (CPU) time, accessing private information (e.g., credit card numbers), corrupting data, displaying political or humorous messages on the user's screen, spamming their e-mail contacts, logging their keystrokes, or even rendering the computer useless. However, not all viruses carry a destructive "payload" or attempt to hide themselves—the defining characteristic of viruses is that they are self-replicating computer programs which install themselves without user consent.

Types of computer viruses

Macro viruses

Many common applications, such as Microsoft Outlook and Microsoft Word, allow macro programs to be embedded in documents or emails, so that the programs may be run automatically when the document is opened. A macro virus (or "document virus") is a virus that is written in a macro language, and embedded into these documents so that when users open the file, the virus code is executed, and can infect the user's computer. This is one of the reasons that it is dangerous to open unexpected or suspicious attachments in e-mails. While not opening attachments in e-mails from unknown persons or organizations can help to reduce the likelihood of contracting a virus, in some cases, the virus is designed so that the e-mail appears to be from a reputable organization (e.g., a major bank or credit card company

Boot sector viruses

Boot sector viruses specifically target the boot sector and/or the Master Boot Record (MBR) of the host's hard drive or removable storage media (flash drives, floppy disks, etc.)

Email virus

Email virus – A virus that specifically, rather than accidentally, uses the email system to spread. While virus infected files may be accidentally sent as email attachments, email viruses are aware of email system functions. They generally target a specific type of email system (Microsoft’s Outlook is the most commonly used), harvest email addresses from various sources, and may append copies of themselves to all email sent, or may generate email messages containing copies of themselves as attachments

Polymorphic viruses

Polymorphic code was the first technique that posed a serious threat to virus scanners. Just like regular encrypted viruses, a polymorphic virus infects files with an encrypted copy of itself, which is decoded by a decryption module. In the case of polymorphic viruses, however, this decryption module is also modified on each infection. A well-written polymorphic virus therefore has no parts which remain identical between infections, making it very difficult to detect directly using "signatures". Antivirus software can detect it by decrypting the viruses using an emulator, or by statistical pattern analysis of the encrypted virus body. To enable polymorphic code, the virus has to have a polymorphic engine (also called "mutating engine" or "mutation engine") somewhere in its encrypted body. See polymorphic code for technical detail on how such engines operate

Antivirus software

Many users install antivirus software that can detect and eliminate known viruses when the computer attempts to download or run the executable file (which may be distributed as an email attachment, or on USB flash drives, for example). Some antivirus software blocks known malicious websites that attempt to install malware. Antivirus software does not change the underlying capability of hosts to transmit viruses. Users must update their software regularly to patch security vulnerabilities ("holes"). Antivirus software also needs to be regularly updated in order to recognize the latest threats. This is because malicious hackers and other individuals are always creating new viruses. The German AV-TEST Institute publishes evaluations of antivirus software for Windows and Android.

Examples of Microsoft Windows anti virus and anti-malware software include the optional Microsoft Security Essentials (for Windows XP, Vista and Windows 7) for real-time protection, the Windows Malicious Software Removal Tool (now included with Windows (Security) Updates on "Patch Tuesday", the second Tuesday of each month), and Windows Defender (an optional download in the case of Windows XP). Additionally, several capable antivirus software programs are available for free download from the Internet (usually restricted to non-commercial use). Some such free programs are almost as good as commercial competitors Common security vulnerabilities are assigned CVE IDs and listed in the US National Vulnerability Database. Secunia PSI is an example of software, free for personal use, that will check a PC for vulnerable out-of-date software, and attempt to update it. Ransom ware and phishing scam alerts appear as press releases on the Internet Crime Complaint Center noticeboard. Ransomware is a virus that posts a message on the user's screen saying that the screen or system will remain locked or unusable until a ransom payment is made. Phishing is a deception in which the malicious individual pretends to be a friend, computer security expert, or other benevolent individual, with the goal of convincing the targeted individual to reveal passwords or other personal information.Other commonly used preventative measures include timely operating system updates, software updates, careful Internet browsing (avoiding shady websites), and installation of only trusted software Certain browsers flag sites that have been reported to Google and that have been confirmed as hosting malware by Google.

There are two common methods that an antivirus software application uses to detect viruses, as described in the antivirus software article. The first, and by far the most common method of virus detection is using a list of virus signature definitions. This works by examining the content of the computer's memory (its Random Access Memory (RAM), and boot sectors) and the files stored on fixed or removable drives (hard drives, floppy drives, or USB flash drives), and comparing those files against a database of known virus "signatures". Virus signatures are just strings of code that are used to identify individual viruses; for each virus, the antivirus designer tries to choose a unique signature string that will not be found in a legitimate program. Different antivirus programs use different "signatures" to identify viruses. The disadvantage of this detection method is that users are only protected from viruses that are detected by signatures in their most recent virus definition update, and not protected from new viruses (see "zero-day attack").