
3.0 INTRODUCTION

In this unit we will describe the various ways in which loss or corruption of data can occur and the means by which this can be avoided. Our main thrust would be directed towards PCs, but we would also look at the measures available on larger machines. We will also discuss about cryptography.

Once more and more information is kept in digital form, the protection of data in computer systems begins to pose challenges to designers, researchers and system managers. It is clear that when such data involves financial transaction, there has to be complete reliability. Even in University examination systems, the security of the data is very important. In an information society, even for businesses the competition would be on the basis of the information available. Therefore, pilfering of information or eavesdropping when data is being communicated from one part of the organisation to another, can be a serious threat.

One of the methods adopted from time immemorial -relates to jumbling up- the message so that-.it cannot be easily understood. Of course, persons wanting to get the information, would want to break through the jumbled message, and will try to find a meaningful content.

The field of cryptography (from the Greek kryptos, "hidden" and Graphein, "to 'write"), deals with the methodologies involved in creating cryptograms i.e. messages which should appear to be meaningless, except for those who have been provided the means to extract the original text from the jumbled up text.

3.1 OBJECTIVES

At the end of this session, you should be able to:

- define the computer security
- give various security measures to be undertaken
- explain physical security and software security
- appreciate the possible approaches to cryptography
- define the concepts of cryptanalysis.

3.2 DEFINITIONS

Generally the terms privacy, integrity and confidentiality are loosely construed to be synonymous with security. These however have different connotations with respect to data or information. They also address different areas of information systems. To better understand the measures and to ensure protection in each area, let us see their definitions.

SECURITY:

"Data or information security is the protection of data against accidental or intentional, destruction, disclosure or modification". Computer data security refers to the technological safeguards and managerial procedure, which can be applied to computer hardware, software and data to ensure that organisational assets and individual privacy are protected.

PRIVACY:

"Is a concept applied to an individual". It is the right of an individual to decide what information he/she wishes to share with others or is willing to accept from others.

3.3 SECURITY STATUS ON PC

Before studying the ways in which security can be compromised, let us see what some of the leading magazines have to say about PC security.

The "New Scientist" in its issue of 7 July 83 warned: "New PC users beware ! PCs are the biggest threat to Computer Security. Micros are left in unguarded offices or at home, where data snoopers may steal confidential files or data, if not the machine itself".

A few years later "PC Week" in its issue of 7 May 85, Cautioned: " The PC has NO inherent security. For a user with confidential data, the data stored in the PC is vulnerable because anyone can walk up and turn the switch ON and access information.

The same article had this to say for networked PCs: "Put your PC on-line and you are open to a New World of terrors. A LAN is an open opportunity for mischievous or disloyal co-workers to get confidential information. A telephone connection can invite everyone from the 10-year-old down the street to the KGB - to intercept your communiques and romp through your memory banks, borrowing a file here, erasing others there, until the only memory you have of your data is an ulcer".

The article Digital defence in the February 7-21, 95 issue of Business Today has the following to say "If you marvel at the speed, efficiency, and ease-of-use with which your computer system crunches, sorts and spews out data, remember this : it's just as simple for a digital desperado on the prowl to coax out the same data from the system."

3.4 BREACHES OF SECURITY

The above warnings paint a fairly bleak picture for PC users. Some of the ways in which data loss or manipulation can occur have been hinted at in these articles. Let us look at the details of the manner in which losses can occur.

Theft of PC and Media:

May sound preposterous but it is a distinct possibility. A smart person with a false calling card can take away the PC for repairs and of course never show his face again ! However, electronic media like floppies and CD-ROMs are slightly safe as it is far easier to lock up floppies in a safer place.

Damage due to Breakage:

Floppies are easily breakable. It is hard to visualise dropping PCs but it can happen if they are shifted from one place to another. More likely is that something may get dropped on the PC resulting in damage. Damage can also occur due to natural causes such as storms or floods, or due to electrical or other fires.

Environmental Damage:

The manufacturer recommends some environmental conditions like temperature and humidity ranges, voltage limits, dust micron limits etc. If the conditions in your office remain outside - these limits the PC and media are likely to get damaged.

Inadvertent Corruption/Loss:

This can occur due to:

- Usage of inferior media : If sub-standard media is used, as it would be generally cheaper, after using it for some time it may develop faults and data held on it may become unusable. One hears about frequent corruption of data on inferior floppies.
- Erasure of Files : Files may get erased from the media due to incorrect actions by the operator. Corruption may occur due to the PC being subjected to frequent power failures, wrong programming techniques or defective software.

Environmental losses:

Excessive dust or humidity can result in corruption of disc surfaces or read/write heads resulting in loss of data.

Malicious damage/Leakage: We now turn to the real problem of computer installations, be they stand alone PCs or large main frames with hundred of terminals. It is not necessary that outsiders would do this; it is equally possible that some unhappy or impish insiders may wreck havoc.

Unauthorised Access:

As the saying goes "Curiosity killed that Cat", but it does not stop the human from trying to look at things they should not or need not. Information on personnel, finance, products or assets can be accessed and copied for malafide use.

Modifications Erasures etc.: The person accessing data files may be authorised to read the data only, but he would like to alter, modify or erase the data by writing into that file.

Computer Viruses:

This is the latest threat to computer users. These can be introduced deliberately or unknowingly by anyone at anytime and the consequences to the user would be equally disastrous. The problems created by viruses include:

- Destruction of file Allocation Table (FAT) - user loses everything on his media;
- Erasing of specific programs and/or data on discs
- Alter contents of fields in the file;
- Suppress execution of RAM resident programs;
- Destroy parts of programs/data held on disc by creating bad sectors;
- Reduction of free space on disc;
- Formatting of discs or tracks on discs in a different way;
- Overwriting of entire disc directories;
- "Hang" the system at periodic intervals so that keyboards become inoperative;
- Automatic copying of results obtained by other programs into some designated areas.

Data Tapping:

In large computer systems or when systems are networked, data has to travel between the processing unit and terminals, or different processors, over communication lines. Any person trying to get access to data can intercept the traffic on the circuit by tapping into the cable at convenient points. This may even enable him to send spurious channel over the network and access the computer itself by emulating terminal responses. Very sophisticated means have been developed which allow a person to 'listen' to the traffic on a line even without physically connecting into it. Thus the data following over communication lines is ever susceptible to "eavesdropping".

3.5 SECURITY MEASURES

The measures for data protection taken by an organisation reflect its awareness and attitude towards information and Information Technology. If top management treats computers as a dehumanised, intangible, but necessary evil, the measures taken to protect data, individual privacy and data integrity would, at best, be lackadaisical. On the other hand, if the

management considers information as an important resource and computers as an aid in decision making one would find a positive approach and involvement by the management towards security of information. This attitude naturally percolates down to the lower levels and the workers consider the computer correspondingly as an enemy or an ally.

One of the best and first steps in ensuring data security is to create an awareness and develop a culture within the organisation towards the ways in which information can be lost/ altered and what would be the consequences, of such an occurrence, to the organisation and individuals. The other steps that can be taken are:

- IT Planning: the organisation must decide on a policy for introduction of IT. This must be done at the highest level and should address issues such as level of protection for various aspects of information relating to the organisation;
- Selection of technology: keeping in mind obsolescence due to new innovations and necessity for keeping in step;
- Identification of points of exposure of weak links to device means to plug them;
- Physical protection of machine and media.

Control and Monitoring the access to data, its usage by persons and its integrity must be clearly defined and responsibility for ensuring these must rest on persons designated for these tasks; an audit procedure would go a long way in ensuring adherence to laid down guidelines. While the above are relevant for any computer based MIS implementation, in case of PCs, the rules for acquisition and use must be unambiguously stated. Additional points to be looked into are:

- Information classification;
- Responsibilities for Security;
- User training to increase security awareness and propagation of "do's and don'ts"
- Guidelines for creation and changes to passwords etc.

There are four time-honoured principles for ensuring security and recovery in case of breaches of security:

Prevent: The best method is of course stopping all breaches of security before they occur. 'Need-to-know' policy is an offshoot of the principle of prevention.

Detect: Howsoever, one may try to ensure it, total security is almost impossible. The next principle, therefore, is that you must be able to detect breaches to security, whenever they occur, within the shortest possible time. This helps in damage assessment and, also, in devising further preventive measures.

Minimise Damage: The aim here is to contain the damage, when losses occur, to reduce the adverse effects of such damage.

Recovery: There must be enough resilience in the system to recoup the losses/damage and become functional, by reinstating the status, at the earliest.

We would now look at the various measures available to the PC user, to ensure security of machine and data, relating to the principles enumerated above.

3.5.1 Physical Security

These measures are for PCs being used in offices. The PC may be in use by an individual or being shared between two or more users. The measures available are:

- Physically bolt down the PC to a table so that it cannot be casually lifted and taken away.

- Locate the PC in such a way that it is conveniently accessible to the user, but hidden from casual passers-by;
- Have likeable cupboards for floppies and keep them locked at all times, except when used;
- Keyboard and PC locking devices can be fitted so that the PC cannot be operated unless these locks are opened;
- Keep a record of all floppies in use; do not permit alien floppies into the organisation;
- Use lockable rooms for PCs, specially those handling sensitive data. Make it a practice to lock the room when leaving it for even a short time.
- The above apply to servers, gateways and the like.

Environmental Conditions: The PCs are fairly rugged and can tolerate wide ranges of temperatures, humidity and voltages. However, to ensure trouble free and prolonged life, consider the following measures:

- Have temperature and humidity gauges placed in the close proximity of PC; and keep a casual watch to ensure that conditions are within limits. Switch off if the limits are exceeded;
- If your normal electrical supply is subject to large variations of voltage and frequency or spikes, it is prudent to have voltage and frequency stabilizers for the PC;
- Ensure that excessive dust or paper scrap does not accumulate near the PC;
- The plug sockets should fit snugly and cables leading to terminals and printers should be secured properly and not left hanging;
- You may consider putting a thin transparent plastic cover on the keyboard if it does not hamper your handling the keyboard;
- The most important is the use of a vacuum cleaner at regular intervals.

3.5.2 Software Security

As is apparent from the views on security of various leading magazines, provided on PCs, there is hardly any security provided on the PC. There are some measures you can take to ensure that data is not corrupted or modified by unauthorised users and to reinitiate the database to its known status in case this happens and these are:

- Use original software for Operating System, compilers or software packages. You may have to pay for it, but you can then be sure that it would be bug-free, known also as "licensed" software;
- Use correct procedures for shutting down the PC so that all files etc. would be properly closed;
- If you develop your own applications introduce passwords to access your application; these passwords should not be visible on the screen when keyed-in;

- Keep back-ups of all your files. Whenever you operate on any file, (especially in update/append/alter mode), if you have your own programs - they should include a "copy" procedure; this ensures that a back up of your data files would always be automatically taken.

3.5.3 Network Security

The protection required for networked systems is much more extensive as physical security measures are totally inadequate. It is also extremely difficult to know- who, when and how someone is accessing your data. in LANs, generally there would be one server which holds the shareable data on network and services the requests of various nodes. The normal method used is password identity for permitting access; the measures that can be adopted for additional security are:

- Keep the servers away and limit physical access to them.
- Run servers in the background mode; thus the server can be booked on, for use in the network, but, for direct use of the server, a separate password would be necessary;
- Some networks provide auditing facilities, which can be used to advantage;
- Be aware that the network cables can be tapped, so try and shield or conceal them to prevent easy access; if possible use optical fibre;
- Use codes and ciphers in data communication; remember, however, that this would impose considerable overheads on your resources;
- Use fibre-optic cables. for highly sensitive networks as they are difficult to tap; however, here too it may be possible to steal data through sensing the perturbations of the fibre itself,
- Prohibit the use of passwords embedded in communication access scripts; if this is unavoidable, use encryption for passwords;
- Consider the use of see-through devices for any system accessed through networks or through dial up.

Protection against virus:

A number of measures are available for reducing the risk of being attacked by computer virus:

- Build employee awareness of the risk;
- Do not allow the use of outside programs for company PCs or networks;
- Do not interface company networks to outside "Bulletin Boards"
- Make system/server files "Read only";
- Try and obtain source code for important software in use and compile it in-house;
- If source code is difficult to follow, it should ring a warning bell in your head;
- Check executable code using "debug" or separate utilities to study code structure and check spaces for viruses.

3.5.4 Password Security

In most organisations or computer systems, the only authorisation for data access is giving the correct password; rightly speaking, this is only one step; the whole process would be:

Identification:

An identification user code only indicates an object with a unique identity assigned to it. Thus it should not become authorisation to access data without further checks, if some measure of security is desired;

Authentication:

This process verifies that a person or object is who he, she or it claims to be. This could be achieved by asking some standard questions (from a large selection) and getting answers to them. If the answers match with those held on the systems, the person or object is authenticated. Biometric and other physical authentication processes are also popular in systems where security is a primary concern.

Authorisation:

This is the last step in the process. Through this you can ensure that only a given user, terminal or other resource can access data to which permission has been granted to read, write or alter. Thus a matrix can be created to indicate which users have access to which file, records or fields. If the user request passes the matrix he is allowed access, otherwise he is denied access to some parts of the database.

Other Aspects

We have had a fairly close look at the measures for data protection available on stand alone as well as networked PCs. Some of the measures that we studied can be implemented only on mini and mainframe systems easily, while trying to introduce them on PCs may incur too much of resource overheads. We would now take a quick look at the protection, detection and recovery mechanisms available on large systems. This is in order to give you pointers for discerning when to go in for a larger system rather than a PC LAN and what facilities to look for.

Database Access:

Larger systems provide various mechanisms to prevent access to data. User classes can be defined automatically prohibiting access to data by user class. User can be given only "query view" of the data so that he can have only "read" access to a limited amount of data. In some systems, certain terminal numbers can display or access only some parts of database, thus, even a user, with higher access permissions cannot access some data on those terminals.

Access to Operating Systems:

In some systems the operating system is written in a lower level language and users are not given the use of that language. Thus, the user cannot alter any part of the operating system. Some operating systems follow the concept of access control levels. In this any program which has equal or higher access control level cannot access any routines which are below that level. The operating system routines are placed at much lower level and paths are predefined for access to these, which incidentally, are via other system routines placed at a high level. From this point of view 'UNIX' is not a secure Operating System as, 'C', which is the language in which 'UNIX' is written, is also available to the user as a programming language, however, it has many good security features.

Access Control Cards:

This is the latest method and is also available on PCs. Here an additional card is inserted on the PC. This card has its own memory and software. The user can program up to ten complex account codes. Anyone wanting access to a PC has first to pass through authentication routines through this card. Only when he passes, is he allowed to access the PC itself. These codes can be reprogrammed whenever required. Thus the basic problem of preventing access to the operating system of the PC can be solved to a large extent.

3.6 CRYPTOGRAPHY: A BRIEF HISTORY

In the current scenario of computer usage that predict is that networks are likely to be present everywhere, security has become much talked about issue. Especially, with the relatively easy access to the Internet, the confidence in the sanctity of the data is a major concern.

However, the science of Cryptology is at least 4,000 years old. Cryptology is defined as "the design and analysis of codes and ciphers." In its first 3,000 years, Cryptology was developed independently in several ancient cultures, including Egypt, India and Mesopotamia. Perhaps the oldest evidence of Cryptology is an ancient inscription, carved about 1900 BC, in the main chamber of an Egyptian tomb. It used some unusual hieroglyphic symbols in place of more ordinary symbols. Although the inscription utilised one of the important methods of cryptography transformation of the text-it was not secret writing. The intention appears to have been to impart authority and dignity to the writing.

However, rather better known technique is attributed to Julius Caesar, who used a simple cipher system more than 2,000 years ago to conceal military information. The method consisted of replacing the letters of alphabets in the original text by letters that are a fixed number of places away. For example, 'A' could be replaced by 'D', 'B' by 'E' and so on. Thus, the key for the cipher would be as follows:

Plain: A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

Cipher: D E F G H I J K L M N O P Q R S T U V W X Y Z A B C

Using this system, the secret message "**ZHOFRPH WR WKH FRPSXWHU FRXUVH**" would actually mean "**Welcome to the Computer course**". There were of course other systems developed around the similar time in history which included approaches such as:

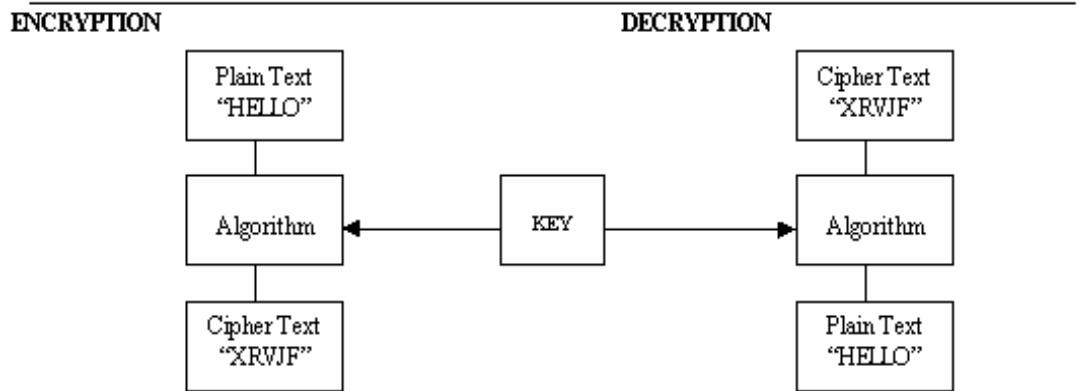
- Writing secret messages backwards.
- Writing messages vertically rather than horizontally.
- Substituting dots for vowels.
- Using alphabets of other languages such as Greek or Hebrew.
- Substituting special symbols for the normal letters of the alphabets.

A Caesar type encryption mechanism can be easily detected by trying all possible displacements till the message becomes meaningful.

3.7 CRYPTOGRAPHY

Cryptography is the process of transforming plain text or original information into an unintelligible form (cipher text) so that it may be sent over unsafe channels of communication. A data string (key) controls the transformation process. Anyone getting hold of the cipher text while it is on the unsafe channel would need to have the appropriate key, to be, able to get to the original information. The authorised receiver is assumed to have that key. This is illustrated in the following figure:

Encryption Process



The stage of conversion of the plain text into a cryptogram is called Encrypting or enciphering or encoding. Reconverting the cryptogram back into the original form, when done by the authorised person is called decrypting or deciphering or decoding.

3.7.1 Cipher Systems

Although there may appear to be many variations, there are mainly two basic classes of cipher systems. These two classes are called transposition and substitution.

Transposition Cipher

A transposition involves rearrangement or change in the sequence of the letters of the plain text message without any change in their identity. However, the substitution involves a replacement of the plain text letters by other letters (or other symbols) without any change in their sequence. Transposition and substitution may be combined in a single cryptosystem.

The Caesar Cipher mechanism was described earlier and is a specific case of what may be called a "transposition type cipher".

Code System

A code system is a specialised form of substitution in which entire words, long phrases or even sentences of the plain text are replaced by arbitrarily selected equivalents. These may be other words, groups of letters, groups of figures or some combination of these. It is only in rare cases that the substitution process is applied to elements smaller than whole words.

A code system, therefore, makes use of a codebook in which the words, phrases and sentences of the vocabulary are listed in an organised manner and accompanied by their equivalent code groups. Many large commercial firms have their own private codes, constructed especially for their use.

In modern times, communication does not take place only through the passage of text. The same general ideas of substitution and transposition, which were used for literal cryptosystems, are also used for encryption, for speech (ciphony), facsimile (cifax) and television (civision). In literal cryptosystems, the unit of encryption is usually a single character. But in ciphony, cifax, or civision, the relevant unit is a timed portion of the continuously varying audio or image-scanning signal. Ciphony, cifax, civision system are categorised as privacy system or security systems. Privacy system mainly offers the protection against direct listening or direct viewing. The security systems, on the other hand,

offer greater protection which actually in some cases will attempt protection against analysis as well.

3.7.2 Data Encryption Standard (DES)

IBM developed the Data Encryption Standards (DES) algorithm in the early 1970s. DES specifies a method for encrypting 64-bit blocks of clear data plain text into corresponding 64-bit blocks of cipher text employing a user-specified 56-bit key. DES may be double-or triple-encrypted for additional security, with the user employing a different key after each transmission.

Because 2^{56} combinations of the keying variable are possible (and these keying variables can be changed readily), the algorithm is deemed by some experts to be highly secure.

Cryptography experts in industry and government agencies maintain that DES is still a reliable standard. Operating at one try per microsecond, it would require approximately 2,284 years to break the code. Another consideration is the effect on security if the length of time the key is operative is shorter than the time it would take to search for the key.

DES is commonly used in the design, generation, and verification of personal identification numbers (PINs). These personal passwords are at the heart of the security scheme for validating ownership of automatic teller machine (ATM) debit cards. Message authentication also uses the DES algorithm.

Some experts believe that the DES is breakable. It may be possible for a parallel processor using special integrated circuits to go through all the permutations of a single DES transmission in one day. Although DES offers a high degree of security for commercial threats, the security of DES is lower for national or military threats.

The two main components of the DES-based system are an algorithm and a key. The DES algorithm is a complex interactive process comprised of substitutions, permutations, and mathematical operations.

The important feature about the DES approach is that the algorithms is fixed and is public information. However, the actual key used is shared secret between the originator and the receiver of a transmission. Advances in DES include lengthening a key to 128 bits and the multi-pass DES, which involves several passes usually three of encryption and decryption using different keys.

3.7.3 RSA Approach to Encryption

In its continuing search for a truly secret code, another encryption method which is now known as the RSA after its three inventors from the Massachusetts Institute of Technology, namely, Ronald Rivest, Adi Shamir and Leonard Adelman is now considered an important standard. The principle behind the RSA method is that it is easier to multiply two numbers than to factorise their product. This is even more so if the two numbers in question are large prime numbers. For example, it is easy to multiply the prime numbers 11,927 and 20,903 and get the number 249, 310,081. But if you are given the number 249, 310, 081 it is rather difficult to find its prime factors. But if the number is small, such as 35, it is easy to see that its prime factors are 5 and 7. The factoring of 29083 into 127 and 229 comes somewhere in between in terms of level of difficulty. There are an infinite number of prime numbers, and there is no known pattern to them except that they are prime.

Relying on this difficulty, Rivest and his colleague in the year 1977 had proposed the system, which is now known as RSA-129. RSA-129 is a 129 digit number given below which was open to challenge by anyone in the world factorise into its prime factors. This challenge stood unbroken for about 17 years. But in 1993 it was broken through a cooperative effort of academics and hobbyists using over 1500 computers working for over 8 months on the Internet. The RSA-129, 114, 381, 625, 757, 888, 867, 669, 235, 779, 976, 146, 612, 010, 218, 296, 721, 242, 362, 562, 561, 842, 935, 706, 935, 245, 733, 897, 830, 597, 1239 563, 958, 705, 058, 989, 075, 147, 599, 290, 026, 879, 543, 541, factors into the following two prime numbers, one of which is the following number of 64 digits, 3, 490, 529, 510, 847, 650, 949, 147, 849, 619, 903, 898, 133, 417, 764, 638, 493, 387, 843, 990, 820, 577 and the other 32, 769, 132, 993, 266, 709, 549, 961, 988, 190, 834, 461, 413, 177, 642, 967, 992, 942, 539, 798, 288, 533 of 65 digits.

The episode about the RSA is an interesting one to show that what may be considered difficult and impenetrable today may actually be rather easily broken into by more and more powerful computers of tomorrow.

The pursuit of truly secret code, physicists have been contemplating new approaches based on quantum keys. These ideas are still at a theoretical stage but with the kind of development seen in the past in other aspects of the computer industry, it may not be difficult to imagine that this approach of quantum cryptography can become a reality in the coming decade.

3.8 CRYPTANALYSIS

The interpretation of secret communications without any previous knowledge of the system or the key is called cryptanalysis. In the case of modern cryptosystem, this requires extensive theoretical study, unusual power of observation, inductive and deductive reasoning, great concentration and perseverance. Also necessary are vivid imagination guided by good judgment. This has to be supplemented by a special aptitude and intuition gained from long and varied practical experience. It is possible that isolated, short cryptogram may resist solution indefinitely, even if it is in a fairly simple system.

However, a large volume of material even in a very complex cryptosystem-may well be solved with time and effort, and especially with the help of modern powerful computers.

In general, the art of cryptanalysis may be reduced to three basic steps:

- (a) arrangement and rearrangement of data to disclose non-random characteristics or manifestations (e.g., in frequency counts, repetitions, patterns, and symmetrical phenomena);
- (b) recognition of the non-random characteristics or manifestations when disclosed;
- (c) an explanation of the non-random characteristics when recognised. The requirements for the first step are experience or ingenuity and time-which may be appreciably reduced by the use of machine aids; for the second step, experience or statistics; and for the third step, experience or imagination, and intelligence.

3.9 OPEN QUESTIONS AND ACTIVITIES

1. Explore about the basic requirements for your account and password from the system administration of your LAN.
2. Explore the backup policy of your centre.
3. Explore the encryption standards followed if any.

3.10 SUMMARY

It is becoming increasingly essential for all organisations to ensure data security. Ensuring data security on PCs and LANs is a major problem as, inherently, very few mechanism are provided to guard against data loss, corruption, misuse or eavesdropping. Unless the organisation creates security awareness in its work force, any measures for data security are not likely to prove successful.

The organisation must decide on the IT and security policy at the highest level and ensure its strict implementation for a reasonably successful outcome. There are a number of measures available to the organisation, especially on larger system, to ensure data security. Equal attention, however, needs to be paid to PC security, as there is an increasing use of PCs as terminals. That is where, this unit will bring awareness.

In this unit, the major approaches to cryptography have been illustrated. From the elementary Caesar Cipher to the RSA-129, is the range covered. An idea has also been given about the concept of cryptanalysis. This unit only introduces you to these concepts and we do not expect that you will be an expert in Cryptography.

3.11 FURTHER READINGS

1. Andrew S. Tanenbaum, Computer Networks, Third Edition, Prentice-Hall of India
2. William Stalling, Data and Computer Communication, Prentice-Hall of India