UNIT 4 NETWORK SECURITY

Structure **Page Nos.**

4.0 INTRODUCTION TO SECURITY

Use of technology among people is increasing day by day. Such technologies are Computers, Internet (or Network), Mobile phone, Laptops, Tablets, Hard-disk etc. These technologies have internal and external memory which contains electronic data. This data can be confidential, public or private. Now, the security of such data becomes mandatory for all users so as to prevent it from any form of attack which can make this data corrupted. Therefore, Security is a very essential part of day-to-today activities. Now, we will start with defining the term "Security".
Security can be defined by the following statements –

- the state of being secure
- precautions taken to ensure against theft, espionage, etc
- protection of assets
- free from danger or attack or threat
- form of protection

Overall, Security ensures that all processes work as expected. It is the most critical factor and has minimal standard which should be maintained by an individual or organization. This brings reliability, safety and assurance of being protected.
In this unit, you will be introduced to types of security and its services like Confidentiality, Availability, Integrity, Authentication, and Non-Repudiation etc. In addition, you will be introduced to the concepts of Cryptography and Cryptology which further define the way in which encryption and decryption can be done. Also, Public and Private Key Cryptography are introduced at later stages. Finally, we will discuss about the Public and Private Key Cryptography algorithms like RSA, DES and MD5.

4.1 OBJECTIVES

After going through this unit you will be able to:

- define the Security and its types;
- define the Security Services;
- discuss Block cipher and Stream Cipher;
- define the define the Cryptography and Cryptology
- define Public and Private Key Cryptography; and
- Define RSA, DES and MD5.

4.2 TYPES OF SECURITY

Information Technology (IT) Security – consists of following types:

1. Application security,
2. Computer security,
3. Data security,
4. Information security
5. Network security

4.2.1 Application Security

Application security prevents attack and vulnerabilities on an application. This application can be a mobile application or any other application such as web application etc. The security of an application remains throughout its lifecycle from initial phase to its running phase (or application phase) and on maintenance phase too.

4.2.2 Computer Security

Computer security is about securing a computer system (Desktop or Laptop etc) or a host. This type of security ensures a computer virus free with the help of an anti-virus software. Moreover, a computer should use genuine and updated software and hardware. Also it should be protected with a password. This type of security is a form of computer security.

4.2.3 Data Security

Data Security involves security of electronic data which is present on any hard-disks / secondary storage either of computer system or on network, on server, etc. Such security can be implemented by using passwords, cryptography (through encryption and decryption), biometric authentication, or through access control list etc.

4.2.4 Information Security

Information Security is defined as protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction. This involves security of electronic data which is present on any database or file in any electronic memory. “Data Security” and “Information Security” are used interchangeably and are almost similar.

4.2.5 Network Security

Network Security takes care of a network, its associated processes and aims to secure it. This network can be an organizational/company internal network or any external network. All data which is coming inside the network and going outside the network is analyzed and monitored to keep the network danger free. Moreover, every process which is part of the network is also monitored.

☞ Check Your Progress 1

1. **State True or False** ☐

   a) National Security is part of Monetary Security. ☐

   b) Network Security monitors data incoming inside a network as well as going outside the network. ☐

   c) Information and data security are almost the same type of security. ☐

   d) Application security, Computer security, Data security, and Network security – all these are part of Information security. ☐

   e) Application level security talks deals with all the application of mobile, web etc. ☐

   f) Information Security deals with information present at network only. ☐

2. Define Security in your own terms?

   ……

   ……

   ……

   ……

3. How computer security and data security differ from each other?

   ……

   ……

   ……

4.3 NEED OF SECURITY

The question which arises here is why there is a need of security? The following vulnerabilities protections are the answer to the question -

- To isolate data from getting hacked, corrupted, unauthorized access, unauthorized modified, unauthorized deleted etc
- To maintain confidentiality, availability and integrity of data
- To prevent electronic mail from getting hacked and unauthorized access
- To protect easy passwords and pins being cracked
- To eradicate vulnerabilities (weakness) in the system or data

4.4 SECURITY SERVICES

In order to overcome the above mentioned vulnerabilities of a system or data or network etc, there are 5 major security services (Figure 1) – Confidentiality, Integrity, Availability, Non-Repudiation and Authentication which are as follows:

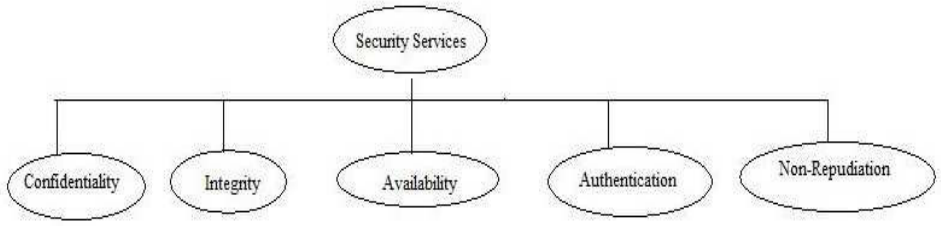


Figure 1: Security Services

4.4.1 Confidentiality

Confidentiality means keeping information secret from unauthorized access and is probably the most common aspect of information security. It is important to protect confidential information. An organization needs to guard against those malicious actions that endanger the confidentiality of its information. For example, an account user is authorized to see his account transaction online and no other account user can access this data as it is confidential.

4.4.2 Integrity

Information needs to be changed constantly. In a bank, when a customer deposits or withdraws money, the balance of their account needs to be changed. Integrity means that changes should be done only by authorized users and through authorized mechanisms. Moreover, the changes should get reflected at all the ends on which the changed information is accessed.

4.4.3 Availability

The third component of information security services is availability. The information created and stored by an organization needs to be available to authorized users and applications. Information is useless if it is not available o authorized users. Information needs to be changed constantly, which means that it must be accessible to those authorized to access it. Unavailability of information is just as harmful to an organization as a lack of confidentiality or integrity. Imagine what would happen to a bank if the customers could not access their accounts for transactions. Therefore, information should be accessible and useable upon appropriate demand by an authorized user and availability is the prevention of unauthorized withholding of information.

4.4.4 Authentication

Authentication is the process by which a person or other entity proves that it is who (or what) it says it is. For example, a bank authenticates a person or entity that deal before transferring something valuable, such as information or money, to or from, it. Authentication is achieved by presenting some unique identifying entity to the endpoint that is undertaking the process. An example of this process is the way you authenticate yourself with an ATM - here you insert your bank card (something you have) and enter your personal identification number (PIN –Personal Identification Number, something you know). Another example can be the authentication process

for email account. In this case, you have the email address and you know the corresponding account password to access the account.

4.4.5 Non-Repudiation

Non-repudiation is the prevention of either the sender or the receiver denying a transmitted message. A system must be able to prove that certain messages were sent and received. Non-repudiation is often implemented by using digital signatures. For example, a user A sent a message to user B. At later stage, user A should not deny of having sent the message to user B.

Other Security Service –

Access Control

Access control means control of access through identification and authentication. A system needs to be able to identify and authenticate users for access to data, applications and hardware. In a large system there may be a complex structure determining which users and applications have access to which objects. This is done through Access Control List (ACL). For example, an account holder while checking his data online can only view data but cannot modify it. This is because of the reason of access given to the user on the basis of his role and identity.

☞ Check Your Progress 2

1. **State True or False** ☐

   i) Confidentiality means to hide the data from everyone. ☐

   ii) Availability of resources or data defines the security service "Availability". ☐

   iii) Authentication is about "what you know" and "what you have". ☐

   iv) Unauthorized access is a type of vulnerability. ☐

   v) Maintaining confidentiality, availability and integrity of data are the one of the parameters for a requirement of security. ☐

2. Discuss all the possible vulnerabilities which can be a threat to information?

   ……

   ……

   ……

3. What do you understand by Security Services?

   ……

   ……

   ……

4.5 AUTHENTICATION AND PRIVACY

Authentication and Privacy refer to the problems of ensuring that communication takes place only between authorized and authenticated users or the right parties without disclosing information to unauthorized users. There is much needed security

infrastructure in place for authentication and privacy based on well known techniques in symmetric and asymmetric cryptography.
Authentication as explained in previous section is all about identifying the user and based on his identification, giving access and rights to the user. In this section, we will discuss about how an authentication can be done with the help of identification.

Authentication-Identification

Identification is all about being able to identify yourself to a computer and is absolutely essential -

- ATM, e-banking identifies a user with the help of PIN
- Access to e-mail, computer accounts, identifies a user with the help of a password
- Access to personal information (e.g., staff or student portal)

Non-computer identification

- Bank teller knows you by sight
- Bank teller checks your picture against a photo ID
- Bank back office compares cheque signature to one on record
- All examples of biometric identification.

Computer Identification

- How we identify a human to a computer?
- Username/Passwords (common),
- Token, e.g. ATM card,
- Cryptographic protocols,
- Combinations, e.g. token and password,
- Biometrics, e.g. face recognition, finger prints, and retina/iris scans

Privacy

Handling user privacy and maintaining user security are tough tasks to do. In most of the cases, it is done through a technique called “Cryptography”.
Cryptography is defined as a process of conversion of plain and readable text to cipher and (unreadable) text called encryption. For example, in Figure 2, the plain text “I am doing bca from ignou” is converted to cipher text “L dp grlqj efd iurp ljqrx” by using Caesar cipher cryptographic algorithm**.**

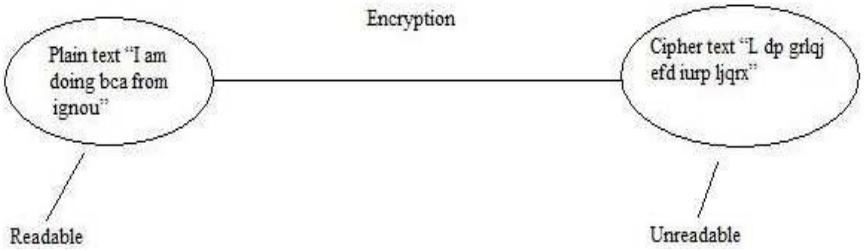


Figure 2: Process of Encryption

Decryption is the process of converting cipher and unreadable text to plain and readable text (called decryption). In given Figure 3, cipher text "L dp grlqj efd iurp ljqrx" is converted to plain text "I am doing bca from ignou" with the help of decryption process.

Please note – Both the process "Encryption" and "Decryption" are performed with the help of a key. Either the same key is used for both encryption (called symmetric or private key encryption) or separate keys (one for encryption and other one for decryption) are used called the asymmetric or public key encryption.

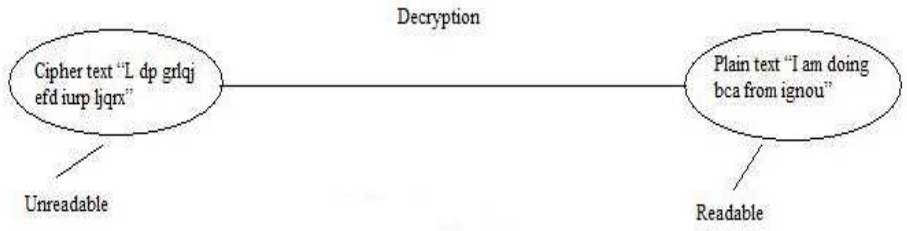


Figure 3: Process of Decryption

Cryptanalysis is the reverse process of cryptography. It means an attacker tries to find the plain text from captured cipher text. But the attacker does this without any key. The key is secured and attacker does not have any kind of access to the key. He only has the cipher text on which he applies reverse engineering.

Please Note – There is a very little difference between "Decryption" and "Cryptanalysis" as in both the cases, the aim is to know or to find the plain text behind cipher text. In decryption, the key is always available to the user who wants to decrypt the cipher text. But in case of cryptanalysis, there is no such key available to decrypt cipher text. In this situation, it is the attacker and not the user who wants to find the cipher text "without key" in order to break the cipher algorithm which is used to convert the plain text into an unreadable cipher text. The main motive is to attack the system with wrong intensions. In case of decryption part, the user uses the key to decrypt the plain text and there is no such wrong intension. The user with a key is always considered as right or authoritive person to decrypt the cipher text into its corresponding plain text.

Cryptology is the combination of Cryptography and Cryptanalysis (Figure 4).

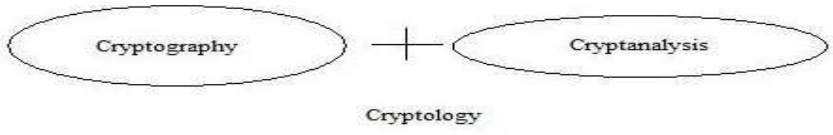


Figure 4: Cryptology

Cryptography - the process of encryption can be Symmetric (Secret Key or Private Key) and Asymmetric which will be discussed in detail in coming sections.

☛ Check Your Progress 3

1. How "Authentication" can be proved through "Identification"?

……

……

2. Difference between Cryptography and Cryptanalysis.

……

……

……

……

3. Define Encryption and Decryption?

……

……

……

……

4.6 BLOCK AND STREAM CIPHERS

Now we will discuss the method in which the plain text is converted into cipher text. In some methods, plain text is treated as numerous units or blocks and then it is converted into cipher text. But in some methods, plain text is divided into bits and these bits individually are given as input to the method which converts each single bit to the cipher text. So therefore, there are two cipher methods (Block Cipher and Stream Cipher) in which plain text is given as input in order to convert them to their corresponding cipher text.

Block Cipher, as the name suggests, takes input (i.e. plain text) and divides the plain text into number of units or blocks. After receiving input, plain text as a unit or block is encrypted with the key and converts it to a cipher text. For example, (Figure 5) the plain text "I am doing bca from ignou" is converted to cipher text "L dp grlqj efd iurp ljqrx" If this cipher text is produced by using Block cipher, then this cipher treats the plain text as "I" as first unit or block, "am" as second unit, "doing" as third unit, "bca" as fourth unit, "from" as fifth unit, and "ignou" as last and sixth unit. The corresponding cipher text produced as "L dp grlqj efd iurp ljqrx" where "L" is the cipher text for first unit, "dp" is the cipher produced for second unit, "grlqj" as the cipher for third unit, "efd" is cipher for fourth unit, "iurp" cipher for fifth unit and "ljqrx" cipher for last unit.

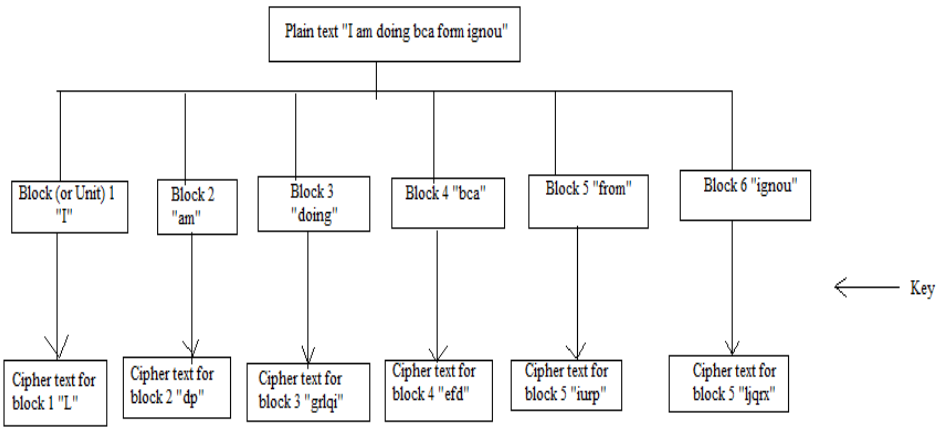


Figure 5: Block Cipher

Now we will discuss advantages and disadvantages of Block Cipher –

Advantages of Block Cipher -

- It is faster than stream cipher.
- If any block contains any transmission error then it will not have affect on other blocks.
- It is not sufficient in hardware but may be used to connect keyboard to CPU (central process unit)
- Block ciphers can be easier to implement in software, because there is no bit manipulation like in stream cipher which is time consuming process and treats data in computer-sized blocks
- Block Cipher is more suitable in trading applications.
- Short blocks at the end of a message can also be added with blank or zero status.

Disadvantages of Block Cipher -

- If two same unit or blocks of plaintext is there, then the cipher produces same cipher text for units or blocks.
- It is easy to insert or delete units/blocks .
- Block encryption may be more susceptible to cryptanalysis attack as compared to stream cipher as block cipher provides strong hints to attacker because two same units produce same cipher text.
- Block encryption is more susceptible to replay as compared to stream encryption.

Stream Cipher takes input (i.e. plain text) and divide this plain text into number of bits (combination of such bits is palin text). After receiving single bit which represents as a part of plain text is encrypted with the key and converts it to a cipher text. For example, (Figure 6) the plain text "I am doing bca from ignou" is converted to cipher text "L dp grlqj efd iurp ljqrx" If this cipher text is produced by using Stream cipher, then this cipher treats each alphabet as a single bit and converts each bit one after another to cipher text. "I" as first bit, "a" as second bit, "m" as third bit, "d" as fourth bit, "o" as fifth bit and so on. The corresponding cipher text produced as "L dp grlqj efd iurp ljqrx" where "L" is the cipher text for first bit, "d" for second bit, "p" is the cipher produced for third bit, "g" cipher text for fourth bit, "r" cipher for fifth bit and so on like this. Please note that we have taken this example for simplicity. Also we have used Caesar cipher cryptographic algorithm for both the stream.

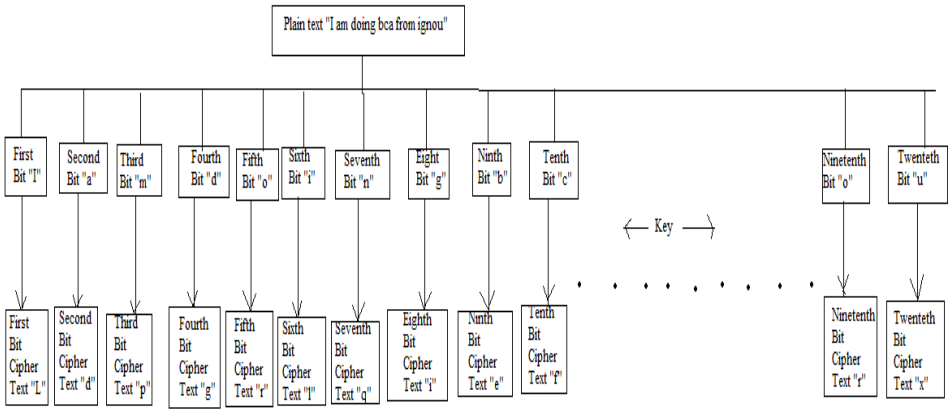


Figure 6: Stream Cipher

Now we will discuss advantages and disadvantages of Stream Cipher –

Advantages of Stream Cipher -

- Stream cipher is suitable for hardware implementation as only encryption and decryption data one bit at a time.
- Stream cipher is less susceptible to cryptanalysis than block cipher as block cipher provides strong hints to attacker because two same units produce same cipher text.
- Stream cipher is less to vulnerable to insertion or deletion of units.
- This cipher can be more easily analyzed mathematically.
- It is more suitable for military applications.
- It is less useful for attackers as same plain text is encrypted but in single individual bits and not in units.
- Self-synchronous stream ciphers are non-periodic because each key character is function dependent on the entire preceding message stream.
- Self – synchronous cipher protect against all type of authenticity threats because any change to the cipher text affects the key stream

Disadvantage of Stream Cipher -

- If during transmission, any bit is lost or become erroneous, then it is difficult to re-arrange and collect all the converted cipher text which in return may result in re-transmission of the entire plain text.
- It is slower than block but can be configured to make faster by implemented in special purpose hardware capable of encryption several million bits for second.
- It is not suitable for the software.

4.7 PUBLIC AND PRIVATE KEY CRYPTOGRAPHY

Encryption and Decryption:
Encryption is the conversion of data into a form, called a ciphertext, which cannot be easily understood by unauthorised entities whereas Decryption is the process of converting encrypted data back into its original form, so it can be understood.
Most security technologies rely, to some degree, on encryption of text or data. For example, encryption is used in the creation of certificates and digital signatures, for the secure storage of secrets or transport of information. Encryption can be anything from a simple process of substituting one character for another, in which case the key is the substitution rule, to some complex mathematical algorithm. It is to be assumed that the more difficult is to decrypt the ciphertext, the better. Trade-off - if the algorithm is too complex and it takes too long to use, or requires keys that are too large to store easily, it becomes impractical to use. There is a need a balance between the strength of the encryption; that is, how difficult it is for someone to discover the algorithm and the key, and ease of use. There are two main types of encryption in use for computer security, referred to as symmetric and asymmetric key encryption**.**

Symmetric Key

Symmetric key cryptography, also called private or secret key cryptography, is the classic cryptographic use of keys:

Here the same key is used to encrypt and decrypt the data. In given Figure 7, User A and User B both uses same secret/shared key to encrypt and decrypt the message.

Figure 7: Symmetric/Private Key Cryptography

Asymmetric Key

In asymmetric key cryptography, different keys are used for encrypting and decrypting a message. In that case, one key can be made public called the public key while the other is kept private known as private key. There are advantages to this public-key–private-key arrangement, often referred to as public key cryptography. (1) The necessity of distributing secret keys to large numbers of users is eliminated, and (2) the algorithm can be used for authentication as well as for creating cipher text. In given Figure 8, User A takes plain text and encrypts it with public key of User B which is publically available. When User B receives cipher text, it decrypts the cipher text with its own (Private/ Secret Key).

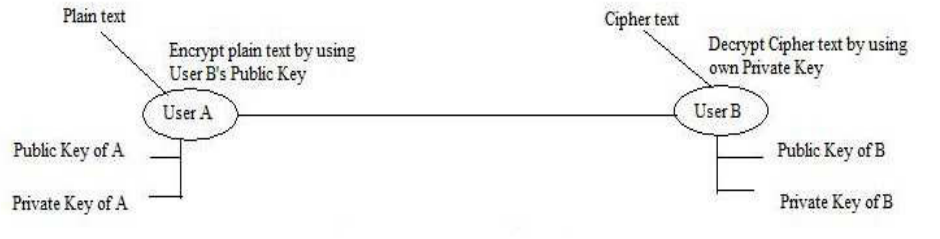


Figure 8: Asymmetric Key Cryptography

Comparison between Symmetric and Asymmetric Cryptography

- Symmetric Cryptography uses single key to encrypt and decrypt data whereas Asymmetric Cryptography uses public key to encrypt the data and private key to decrypt it.
- Symmetric key cryptography is much faster than asymmetric key encryption.
- Symmetric key cryptography does not require a lot of computer resources when compared to public key encryption which uses up more computer resources.
- In Symmetric Cryptography, secret key exchange is a problem. But in asymmetric cryptography, there is no such key exchange problem.
- In Symmetric Cryptography, origin and authenticity of message cannot be guaranteed whereas Asymmetric Cryptography provides method for message authentication, detection of tampering, non-repudiation.
- Symmetric Cryptography prevents widespread message security compromise but in Asymmetric Cryptography, widespread security compromise is possible.

☞ Check Your Progress 4

1. **State True or False**

i) Symmetric Key Cryptography uses two different key for encryption and decryption.

ii) Block Cipher is slower than Stream Cipher.

iii) Public key and Private key are the part of asymmetric key cryptography.

iv) Cipher text is the output of the process called "Encryption".

v) Authenticity of messages is guaranteed by asymmetric key Cryptography.

2. Discuss advantages and disadvantages of Block and Stream Ciphers?

……

……

……

……

……

3. State the difference between Symmetric and Asymmetric Cryptography?

……

……

……

……

……

4.8 INTRODUCTION TO RSA, MD5 AND DES

Data Encryption Standard (DES)

Data Encryption Standard (DES) was developed as a standard for communications and data protection by an IBM research team, in response to a public request for proposals by the NBS - the National Bureau of Standards (which is now known as NIST). DES was developed in the 1970s by the National Bureau of Standards with the help of the National Security Agency. Its purpose is to provide a standard method for protecting sensitive commercial and unclassified data. IBM created the first draft of the algorithm, calling it LUCIFER. DES officially became a federal standard in November of 1976.
The Data Encryption Standard (DES) is a symmetric-key block cipher published by the National Institute of Standards and Technology (NIST) in 1977. DES has been the most widely used symmetric-key block cipher since its publication.

DES takes 64 bit plain text converts it into 64 bit cipher text with the help of 64 bit key (Figure 9) which is later reduced to 56 bit key as every 8^{th} bit of 64 bit is discarded to form a key of 54 bit. As DES is a block cipher, it takes plain text as block of 64 bit.

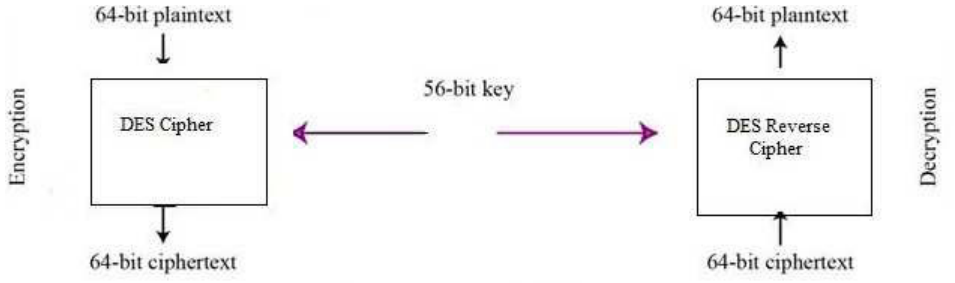


Figure 9: Data Encryption Standard (DES)

RSA

RSA is an asymmetric block cipher (as two different keys are used for encryption and decryption). It was developed by Ron **R**ivest, Adi **S**hamir and Leonard **A**dleman in 1977. A user of RSA chooses two large prime numbers and then calculates the product of two large prime numbers. The prime factors must be kept secret. Anyone can use the public key to encrypt a message, but with currently published methods, if the public key is large enough, only someone with knowledge of the prime factors can feasibly decode the message. Whether breaking RSA encryption is as hard as factoring is an open question known as the RSA problem. The following steps are involved in RSA to calculate encryption key and decryption key.

- Choose two large prime numbers p and q
- Multiply p and q together to get n
- Choose the encryption key e, such that e and $(p - 1) \times (q - 1)$ are relatively prime.
- Two numbers are relatively prime if they have no common factor greater than one $(1<e<((p - 1) x (q – 1))$
- Compute decryption key d such that
- $d = e \ mod \ ((p - 1) \times (q - 1))$
- Construct public key as (e, n) and construct cipher text, $c = p^e \ mod \ (n)$
- Construct private key as (d, n) and construct plain text, $p = c^d \ mod \ (n)$

Now we will take two prime numbers to find the public and private key and cipher text and plain text.

- Choose two large prime numbers $p=61$ and $q= 53$
- Multiply p and q together to get $n =61*53=3233$
- Choose the encryption key e, such that e and $(p - 1) \times (q - 1)$ are relatively prime.
  - $(p-1) =(61-1)=60$
  - $(q-1) =(53-1)=52$
  - $(p - 1) x (q - 1) =60*52=3120$
  - Choosing a relatively prime number between $1<e<3120$ which is not a multiple of 3120. We can choose e=17
- Compute decryption key d such that
- $d = 17 \ mod \ (3120) = 2753$
- Construct public key as $(17, 3233)$ and construct cipher text, $c = 65^{17} \ mod \ (3233)=2790$

- Construct private key as *(2753, 3233)* and construct plain text, $p = 2790^{2753} \mod (3233)=65$

Message Digest5

Before starting MD5, we will first discuss about has *Hash Functions* which takes input a plain text or a message and converts it to a hash value with the help of hash algorithm. Hash Functions are called "*One-way Functions"* as the hash value, which is the result of converted plain text, *cannot be converted back* to the plain text or message**.** Every message produces different hash value. No two different plain messages can have same hash value. Similarly, One hash value belongs to one plain text message only.

The **MD5 Message-Digest Algorithm** is a widely used cryptographic hash function that produces a 128-bit (16-byte) hash value. MD5 has been employed in a wide variety of security applications, and is also commonly used to check data integrity. MD5 was designed by Ron Rivest in 1991 to replace an earlier hash function, MD4. An MD5 hash is typically expressed as a hexadecimal number, 32 digits long. The following are the steps for Message Digest 5 algorithm –

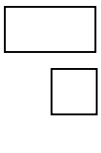
MD5 takes input of arbitrary length and gets broken into blocks of size 512 bits. It produces output of 128 bits.

- Append padding bits so *length ≡ 448 mod 512* (padded message 64 bits less than an integer multiplied by 512)
- Append length: a 64-bit representation of the length to the original message (before the padding) → total length of message k*512 bits
- Initialize MD buffer: 128-bit buffer holds intermediate and final results (4 32-bit registers, ABCD)
- Process message in 512-bit blocks
- 4 rounds of processing
- Similar structure but different logical function
- Each round takes the 512-bit input and values of ABCD and modifies ABCD
- Output: from the last stage is a 128-bit digest
- Every bit of plain text influences every bit of the the hash code
- Complex repetition of the basic functions → unlikely that two random messages would have similar regularities
- MD5 is as strong as possible for 128-bit digest (Rivest's conjecture)

Cryptographic checksum is just as a regular checksum protects the receiver from accidental changes to the message, a cryptographic checksum protects the receiver from malicious changes to the message. One-way function given a cryptographic checksum for a message, it is virtually impossible to figure out what message produced that checksum; it is not computationally feasible to find two messages that hash to the same cryptographic checksum.

If you are given a checksum for a message and you are able to compute exactly the same checksum for that message, then it is highly likely this message produced the checksum you were given.

☞ **Check Your Progress 5**



1. **State True or False**

   1. Data Encryption Standard (DES) is a symmetric-key block cipher.
   2. RSA was developed in 1978.
   3. RSA is an example of symmetric-key block cipher.
   4. RSA takes two large prime numbers as its input.
   5. Message Digest 5 (MD5) is a "One-way hash function".

2. Discuss about Data Encryption Standard (DES)?

   ……
   ……
   ……
   ……

3. Explain RSA with the help of an example?

   ……
   ……
   ……
   ……

4.9 SUMMARY

This completes our discussion on the introductory concepts of Security. The Security Services discussed in the unit are the basic mandatory services but there can be other services for security. There are many other services such as Accessibility, Authorization etc. Moreover, the security and various cryptography algorithms are introduced and designed in order to prevent passive and active attacks like Man-in-the-middle attack, Brute Force attack, Denial of Service (DOS), Distributed Denial of Service (DDOS), Virus, Worm, Trojan Horse etc.
The information given on various topics such as Cryptographic Algorithm, Block and Stream Ciphers, Security attacks, Vulnerabilities, RSA, DES, MD5 etc is exhaustive yet can be supplemented with additional reading. However, Security is an emerging field and implementation of security can be achieved by using various security tools like Intrusion Detection and Prevention Systems (IDPS), Encase, Process Viewer etc.

4.10 SUGGESTED READING

- Stallings, William 2006. *Cryptography and Network Security. Fourth Edition*, Pearson Prentice Hall Cambridge: Pearson Education Inc .
- Kahate, Atul. 2003. *Cryptography and Network Security*. Tata McGraw-Hill Publication.
- Schneier, Bruce. 2008. *"Schneier on Security"* Wiley Publications.
- Ferguson, Niels. Schneier, Bruce. and Kohno, Tadayoshi. 2010. *Cryptography Engineering,* John Wiley & Sons

- Kaufman, Charlie. Perlman, Radia. Speciner, Mike 2002. *Network Security: Private Communication in a Public World (2nd Edition)* . Prentice Hall
- Tipton, Harold F. and Krause, Micki. 2004. *Information Security Management Handbook,* Fifth Edition. Auerbach Publications.
- Rosenberg, Jothy. and Remy, David. *Securing Web Services with WS-Security: De-mystifying WS-Security, WS-Policy, SAML, XML Signature, and XML Encryption*
- Pfleeger, Charles P. and Pfleeger, Shari Lawrence. 2007 *Security in Computing*, Third Edition. Prentice Hall Publication
- Ellis, Juanita. Speed, Tim. and Crowell, William P. 2001. "*The Internet Security Guidebook: From Planning to Deployment,"* Academic Press
- Canavan, John E. 2001. *"The Fundamentals of Network Security"* Artech House.
- www.wikipedia.com

4.11 SOLUTIONS / ANSWERS

☞ Check Your Progress 1

1. a) False
   b) True
   c) True
   d) False
   e) True
   f) False

2. Security can be defined by the following statements –
   - the state of being secure
   - precautions taken to ensure against theft, espionage, etc
   - protection of assets
   - free from danger or attack or threat
   - form of protection

3. **Computer Security**

   Computer security is about securing a computer system (Desktop or Laptop etc) or a host. This type of security ensures a computer danger free and contains no virus by using anti-virus software. Moreover, a computer should use genuine and updated software and hardware. Also it should be protected with password. This type of security is a form of computer security.

4. **Data Security**

Data Security involves security of electronic data which is present on any file, folder, organization, network, computer system, electronic mail, hard-disk etc. Such security can be implemented by using passwords, cryptography (through encryption and decryption), biometric authentication, or through access control list etc.

☞ Check Your Progress 2

1. i) False

ii) True

iii) True

iv) True

v) False.

2. Following are the Vulnerabilities -

- To isolate data from getting hacked, corrupted, unauthorized access, unauthorized modified, unauthorized deleted etc
- To maintain confidentiality, availability and integrity of data
- To prevent electronic mail from getting hacked and unauthorized access
- To protect easy passwords and pins being cracked
- To eradicate vulnerabilities (weakness) in the system or data

3. In order to overcome all the vulnerabilities of a system or data or network etc, there are 5 major security services – Confidentiality, Integrity, Availability, Non-Repudiation and Authentication. If all these five basic security services are ensured then the system or network or data will be free of virus, danger etc.

☞ Check Your Progress 3

1. **Authentication-Identification**

Identification is all about being able to identify yourself to a computer and is absolutely essential -

- ATM, e-banking identifies a user with the help of PIN
- Access to e-mail, computer accounts, identifies a user with the help of a password
- Access to personal information (e.g., staff or student portal)

Non-computer identification

- Bank teller knows you by sight
- Bank teller checks your picture against a photo ID
- Bank back office compares cheque signature to one on record
- All examples of biometric identification.

Computer Identification

- How we identify a human to a computer?
- Username/Passwords (common),
- Token, e.g. ATM card,
- Cryptographic protocols,
- Combinations, e.g. token and password,
- Biometrics, e.g. face recognition, finger prints, and retina/iris scans

2. **Cryptography** is defined as a process of conversion of plain and readable text to cipher and unreadable text (called encryption). For example, in Figure 2, the plain text “I am doing bca from ignou” is converted to cipher text “L dp grlqj efd iurp ljqrx” by using Caesar cipher cryptographic algorithm**.**

Cryptanalysis is the reverse process of cryptography. It means an attacker tries to find the plain text from captured cipher text. But the attacker does this without any key. The key is secured and attacker does not have any kind of access to the key. He only has the cipher text on which he will apply reverse engineering.

3. **Encryption** is defined as a process of conversion of plain and readable text to cipher and unreadable text . For example, in figure 3, the plain text "I am doing bca from ignou" is converted to cipher text "L dp grlqj efd iurp ljqrx" by using Caesar cipher cryptographic algorithm

   Decryption is the process of converting cipher and unreadable text to plain and readable text (called decryption). In given Figure 3, cipher text "L dp grlqj efd iurp ljqrx" is converted to plain text "I am doing bca from ignou" with the help of decryption process..

☞ Check Your Progress 4

1. i) False
   ii) False
   iii) True
   iv) False
   v) True.

2. Following are the advantages and disadvantages of Block and Stream Cipher -

   Advantages of Block Cipher -

   - It is faster than stream cipher.
   - If any block contains any transmission error then it will not have affect on other blocks.
   - It is not sufficient in hardware but may be used to connect keyboard to CPU (central process unit)
   - Block ciphers can be easier to implement in software, because there is no bit manipulation like in stream cipher which is time consuming process and treats data in computer-sized blocks
   - Block Cipher is more suitable in trading applications.
   - Short blocks at the end of a message can also be added with blank or zero status.

   Disadvantages of Block Cipher -

   - If two same unit or blocks of plaintext is there, then the cipher produces same cipher text for units or blocks.
   - It is easy to insert or delete units/blocks .
   - Block encryption may be more susceptible to cryptanalysis attack as compared to stream cipher as block cipher provides strong hints to attacker because two same units produce same cipher text.
   - Block encryption is more susceptible to replay as compare to stream encryption.

   Advantages of Stream Cipher -

- Stream cipher is suitable for hardware implementation as only encryption and decryption data one bit at a time.
- Stream cipher is less susceptible to cryptanalysis than block cipher as block cipher provides strong hints to attacker because two same units produce same cipher text.
- Stream cipher is less to vulnerable to insertion or deletion of units.
- This cipher can be more easily analyzed mathematically.
- It is more suitable for military applications.
- It is less useful for attackers as same plain text is encrypted but in single individual bits and not in units.
- Self-synchronous stream ciphers are non-periodic because each key character is function dependent on the entire preceding message stream.
- Self – synchronous cipher protect against all type of authenticity threats because any change to the cipher text affects the key stream

Disadvantage of Stream Cipher -

- If during transmission, any bit is lost or become erroneous, then it is difficult to re-arrange and collect all the converted cipher text which in return may result in re-transmission of the entire plain text.

It is slower than block but can be configured to make more fast by implemented in special purpose hardware capable of encryption several million bits for second.

- It is not suitable for the software.

3. **Comparison between Symmetric and Asymmetric Cryptography**

- Symmetric Cryptography uses single key to encrypt and decrypt data whereas Asymmetric Cryptography uses public key to encrypt the data and private key to decrypt it.
- Symmetric key cryptography is much faster than asymmetric key encryption.
- Symmetric key cryptography does not require a lot of computer resources when compared to public key encryption which uses up more computer resources.
- In Symmetric Cryptography, secret key exchange is a problem. But in asymmetric cryptography, there is no suck key exchange problem.
- In Symmetric Cryptography, origin and authenticity of message cannot be guaranteed whereas Asymmetric Cryptography provides method for message authentication, detection of tampering, non-repudiation.
- Symmetric Cryptography prevents widespread message security compromise but in Asymmetric Cryptography, widespread security compromise is possible.

☞ Check Your Progress 5

1. i) True

   ii) False

iii) False

iv) True

v) True.

2. The Data Encryption Standard (DES) is a symmetric-key block cipher published by the National Institute of Standards and Technology (NIST) in 1977. DES has been the most widely used symmetric-key block cipher since its publication.

   DES takes 64 bit plain text converts it into 64 bit cipher text with the help of 64 bit key (Figure 9) which later reduced to 56 bit key as every 8^{th} bit of 64 bit is discarded to form a key of 54 bit. As DES is a block cipher, it takes plain text as block of 64 bit.

3. RSA is an asymmetric block cipher (as two different keys are used for encryption and decryption). It was developed by Ron **R**ivest, Adi **S**hamir and Leonard **A**dleman in 1977. Now RSA with an example.

   - Choose two large prime numbers $p=61$ and $q= 53$
   - Multiply p and q together to get $n =61*53=3233$
   - Choose the encryption key e, such that e and $(p - 1)$ x $(q - 1)$ are relatively prime.
     - $(p-1) =(61-1)=60$
     - $(q-1) =(53-1)=52$
     - $(p - 1) x (q - 1) =60*52=3120$
     - Choosing a relatively prime number between $1<e<3120$ which is not a multiple of 3120. We can choose e=17
   - Compute decryption key d such that
   - $d = 17 \bmod (3120) = 2753$
   - Construct public key as $(17, 3233)$ and construct cipher text, $c = 65^{17} \bmod (3233)=2790$
   - Construct private key as $(2753, 3233)$ and construct plain text, $p = 2790^{2753} \bmod (3233)=65$