COMPUTER AND NETWORK SECURITY.

SUB CODE- CSE 423

WRITTEN BY-
ISRAT JAHAN.
PDF CREATE BY-
M.H.SUMI.

Subject Code: CSE-423

Computer and Network Security

Note: The Question bank has been prepared according to our textbooks

প্রশ্ন ব্যাংক আমাদের পাঠ্য বই অনুযায়ী প্রস্তুত করা হয়েছে

Chapter 1 Page No: 146

Overview

1. what do you mean by network security?(2012,2015)
2. What are the traditional methods for network security? (2012,2015)
3. What is cryptography? (2016,2014)
4. Briefly explain OSI security architecture. (2016)
5. Define security attack. (2011,2014)
6. Briefly explain different types of security attacks. (2011)
   Or, discuss in a nutshell the different types of security attack with suitable figure. (2014)
7. Briefly explain different types of security services. (2013)
8. Distinguish network threats and attacks. (2016)
9. Describe general model for network security briefly. (2010,2014,2015)
   Or, draw network security model and discuss about it. (2016)
10. State the differences between active attacks and passive attacks.(2010,2015)
11. Compare the security system on public key cryptography and private key cryptography. (2012,2016)
12. What are the general approaches to attack a conventional encryption scheme? (2010)
13. write down three independent dimensions of cryptography. (2016)
14. define encryption. State the applications of the public key cryptosystem. (2015,2011)

Chapter 2 Page No: 159
Classical Encryption Techniques

1. Explain the difference between symmetric and asymmetric encryption, listing and advantage and disadvantage of each. (2013)
2. How a plant text can be converted into a cipher text? (2012)
3. Describe symmetric key cryptographic algorithm with example. (2012)
   Or, Explain the symmetric cipher model with its ingredients.(2010,2015)
4. differentiate between symmetric and asymmetric encryption.(2011)
   or, write the differences between symmetric cipher models and the asymmetric cipher model. (2010)
5. briefly explain cryptanalysis and brute force attacks. (2010)
6. give example of brute force attack. what is brute force attack? (2016,2014)
7. Explain various types of cryptanalysis attack with necessary diagram. (2014)
8. distinguish between a season key and a master key. (2011,2014)
9. explain the one time pad with example. (2010)
10. explain the rules for encrypting plain text using playfair cypher with suitable example.
    (2010, 2016)
11. what is the difference between a monoalphabetic cipher and a polyalphabetic cipher. (2016)
12. what are the differences between an unconditionally secure cipher and a computationally secure cipher. (2014)

Chapter 3 Page No:172
Block Ciphers and the Data Encryption Standard

1. what is data encryption standard? (2012)
2. describe the operation of feistal cipher. (2012)
3. Why block cipher modes are convenient? (2012,2015)
4. Discuss the strength of DES algorithm. (2012,2014)
5. draw single round DES architecture and briefly explain its operational procedure. (2013)
6. A fiestel cipher is used in the DES algorithm. Describe the of a Feistal cipher. (2013)
   what is Feistel cypher? How it works in a cryptographic algorithm? (2015)
7. state the DES process with diagram. (2010)
   or, briefly explain general DES encryption algorithm. (2014)
8. define steganography. which parameters and design choice determine the actual algorithm of a Feistel cipher? (2014)
9. Why is the middle portion of 3DES decryption rather than an encryption? (2012, 2014)
10. what is triple encryption? how many keys are used in this encryption technique?
11. write short notes on linear cryptanalysis and differential cryptanalysis. (2010)

Chapter 4 Page No:190
Advanced Encryption Standard

1. write the final set of criteria used by NIST to evaluate candidate ASE cipher? (2010,2014,2015)
2. explain the salient features of AES. (2010)
3. state the differences between rijndael and AES? (2010)
4. what is the difference between AES decryption algorithm and the equivalent inverse cipher? (2011,2014)
5. differentiate between AES and DES. (2015)

Chapter 6 Page No:193
Block Cipher Operation & Pseudorandom Number

1. mention the weakness of electronic code book mode. (2010)
2. describe briefly about the block cipher modes of operation. (2011)
3. why do some block cipher modes of operation only use encryption while others use both encryption and decryption. (2011,2014)
4. what is a pseudorandom generator? Give an example describing how it works?(2013)
5. explain how access control lists are used to represent access control matrix. (2013)
6. what is the difference between a block cipher and a stream cipher? (2011,2014) or, make a comparison between is stream ciphers and block cipher with example. (2013)

Chapter 9 Page No: 199
Public-Key Cryptography and RSA

1. describe public key algorithm with required diagram. (2015)
2. what functions should be provided by a public key infrastructure (PKI)? Is it possible to operate such an encryption technique without a PKI? (2013)
3. Explain the RSA algorithm and its security mechanisms. (2014)
4. explain public key cryptography for encryption and authentication. (2013)
   or, briefly explain public key cryptosystem and authentication. (2010)
5. perform encryption and decryption operation using RSA algorithm for a specific case. (2012)

Chapter 10 Page No: 207
Other Public-Key Cryptosystems

1. explain Diffic Hellman key exchange algorithm. (2010,2014,2015)
2. user A and B exchange the key using Diffie Hellman algorithm. Assume α =5, q=11, X_A =2 and X_B =3. Find the value of Ya,Yb and K. (2011,2013,2014)
3. users A and B use the DP Hellman key exchange technique with a common prime q= 71 and a primitive root α=7.
   (i) if user A has private key Xa= 5 , what is the A's public key Ya?
   (ii) if user B has private key Xb=12, what is the B's public key Yb?
   (iii) what is the shared secret key? (2016)
4. define an elliptic curve. With example discuss ECC over prime field. (2013)
5. State and explain man in the middle attack. (2010,2016)

Chapter 11 Page No: 211
Cryptographic Hash Functions

1) what is hash function? Explain the SHA-512 logic algorithm. (2016)
2) make comparison between MD5 and SHA algorithm. (2011,2012)
   or, draw an analogy between MD5 and SHA algorithm. (2014)
3) define institution and the methods used for intrusion detection. (2011)
4) what is message authentication?(2011,2012,2016)
5) define Mac. How message authentication is performed? (2013)
   or, what is message authentication code? What are some approaches to producing message authentication? (2015)
6) differentiate Mac and hash function. What is the role of compression function in hash function? (2012)

Chapter 13 Page No: 215
Digital Signatures

1) what is digital signature?(2012,2011,2014, 2015)
2) Describe digital signature with block diagram. (2015)
3) state the requirements for a digital signature? (2010)
   or, what requirements should a digital signature scheme satisfy? (2012)
4) Describe about the digital signature standard (DSS). (2011)
5) write down digital signature algorithm. (2016)
6) distinguish between direct and arbitrage digital signature. (2012)
7) what are the typical contents of X.509 certificate format? State the purpose of different fields of certificate revocation list (CRL). What is Delta revocation? (2012,2014)
8) what is meant by certificate revocation? When does it occurs when a certificate is revoked, who is responsible for the revocation? (2013)
9) what is the purpose of the X-509 standard? (2015)
10) what are the key features of SET and SET participants? (2016)
    or, what is the meaning of SET? Write about its feature. (2011)
11) what is mean by SET? What are the steps involved in SET transaction? (2012)
12) what is kerberos? (2015)
13) Explain the Characteristics of Kerberos.

Chapter 22 Page No: 225
Firewalls

1) what is a firewall and what are its limitations? Why corporate house implement more than one firewall for security? (2012)
2) what is firewall? What are the advantages of firewall? (2011,2016)
3) define a worm .diagrammatically illustrate a digital immune system. (2011,2016)
4) Write short notes on the following
   a) key exchange of a diffie Hellman algorithm; (2012)
   b) digital signature standard; (2012)
   c) security attacks; (2012)
   d) digital immune system(2012)
   e) MIME contents(2012)
   i. Feistel cipher(2016)
   ii. (iii)PRNG(2016)
   iii. (iv) elliptic curve cryptography (ECC) (2016)
   iv. (iv)SET (2015)
   v. (vii) Unix password scheme(2015, 2014)
   vi. product Cipher (2014)
   vii. hash function(2014)
   viii. IPSec ESP format(2014)

Chapter 1
Overview

1. what do you mean by network security?(2012,2015)

answer: Network security is any activity designed to protect the usability and integrity of your network and data. It includes both hardware and software technologies. Effective network security manages access to the network. It targets a variety of threats and stops them from entering or spreading on your network.

2. What are the traditional methods for network security? (2012,2015)

Answer: three key objectives that are at the heart of computer security:

1) **Confidentiality:** This term covers two related concepts:
   - i. **Data confidentiality:** Assures that private or confidential information is not made available or disclosed to unauthorized individuals.
   - ii. **Privacy:** Assures that individuals control or influence what information related to them may be collected and stored and by whom and to whom that information may be disclosed.
2) **Integrity:** This term covers two related concepts:
   - i. **Data integrity:** Assures that information and programs are changed only in a specified and authorized manner.
   - ii. **System integrity:** Assures that a system performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system.
3) **Availability:** Assures that systems work promptly and service is not denied to authorized users.

3. What is cryptography? (2016,2014)

answer:

Cryptography is a technique to provide message confidentiality.

The term **cryptography** is a Greek word which means "secret writing" .It is an art and science of transforming messages so as to make them secure and immune to attacks. Cryptography involves the process of encryption and decryption. This process is depicted.

4. Briefly explain OSI security architecture. (2016)

Answer: The OSI security architecture is useful to managers as a way of organizing the task of providing security. Furthermore, because this architecture was developed as an international standard, computer and communications vendors have developed security features for their products and services that relate to this structured definition of services and mechanisms.

The OSI security architecture focuses on security attacks, mechanisms, and services. These can be defined briefly as

- ✓ **Security attack:** Any action that compromises the security of information owned by an organization.
- ✓ **Security mechanism:** A process (or a device incorporating such a process) that is designed to detect, prevent, or recover from a security attack.
- ✓ **Security service:** A processing or communication service that enhances the security of the data processing systems and the information transfers of an organization. The services are intended to counter security attacks, and they make use of one or more security mechanisms to provide the service.

5. Define security attack. (2011,2014)

Answer:

Security attack is Any action that compromises the security of information owned by an organization.

A useful means of classifying security attacks, used both in X.800 and RFC 2828, is in terms of passive attacks and active attacks. A passive attack attempts to learn or make use of information from the system but does not affect system resources. An active attack attempts to alter system resources or affect their operation.

6. **Briefly explain different types of security attacks. (2011)**
   Or, discuss in a nutshell the different types of security attack with suitable figure. (2014)

Answer: **Passive Attacks**

Passive attacks are in the nature of eavesdropping on, or monitoring of, transmissions. The goal of the opponent is to obtain information that is being transmitted. Two types of passive attacks are release of message contents and traffic analysis.

i) **The release of message** contents is easily understood (Figure 1 a). A telephone conversation, an electronic mail message, and a transferred file may contain sensitive or confidential information. We would like to prevent an opponent from learning the contents of these transmissions.

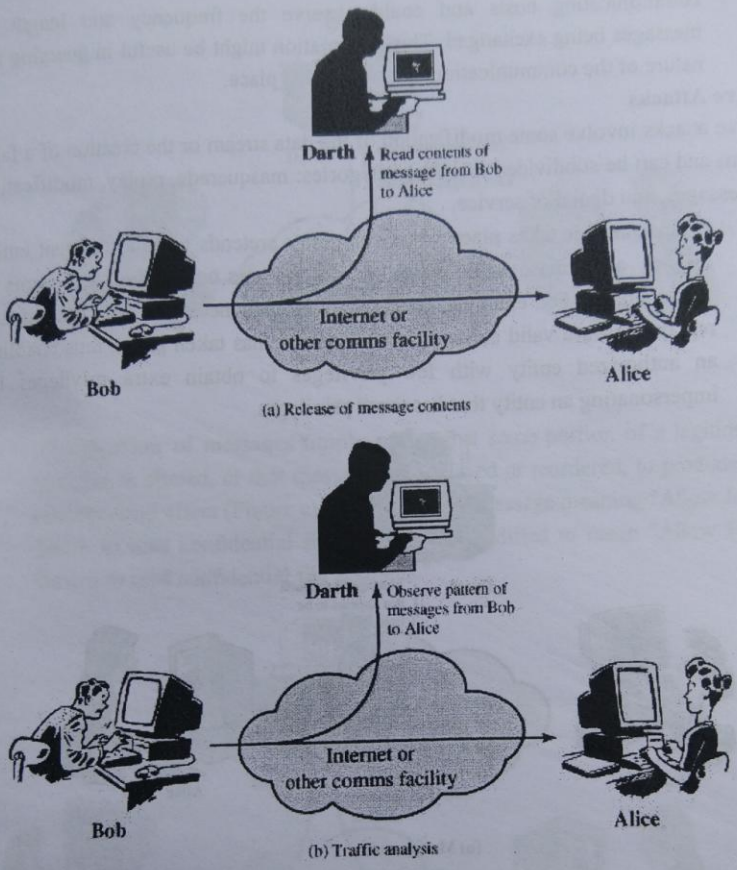


Figure 1. Passive Attacks

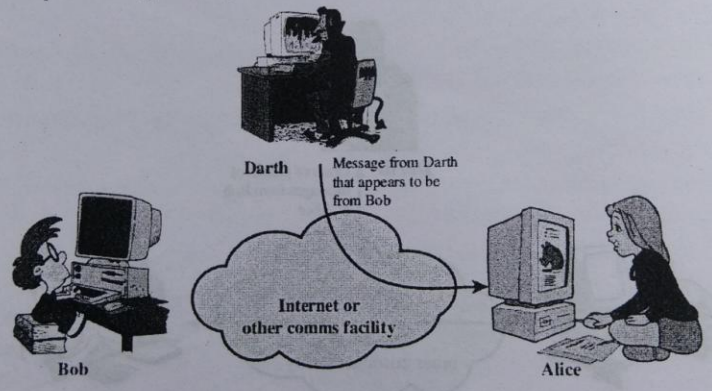
ii) **traffic analysis**, A second type of passive attack, **traffic analysis**, is subtler (Figure 1b). Suppose that we had a way of masking the contents of messages or other information traffic so that opponents, even if they captured the message, could not extract the information from the message. The common technique for masking contents is encryption. If we had encryption protection in place, an opponent might still be able to observe the pattern of these messages. The opponent could determine the location and identity of

communicating hosts and could observe the frequency and length of messages being exchanged. This information might be useful in guessing the nature of the communication that was taking place.

Active Attacks

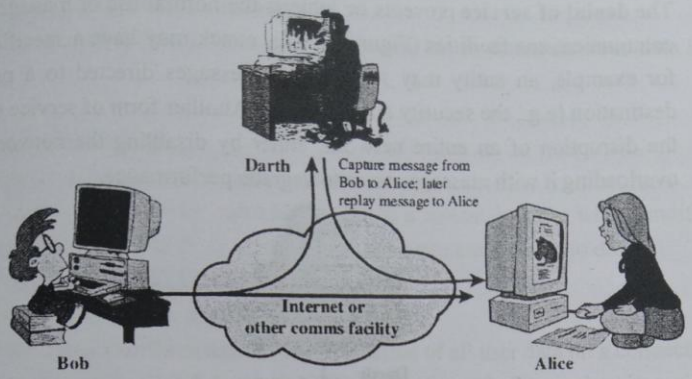
Active attacks involve some modification of the data stream or the creation of a false stream and can be subdivided into four categories: masquerade, replay, modification of messages, and denial of service.

i) A **masquerade** takes place when one entity pretends to be a different entity (Figure a). A masquerade attack usually includes one of the other forms of active attack. For example, authentication sequences can be captured and replayed after a valid authentication sequence has taken place, thus enabling an authorized entity with few privileges to obtain extra privileges by impersonating an entity that has those privileges.



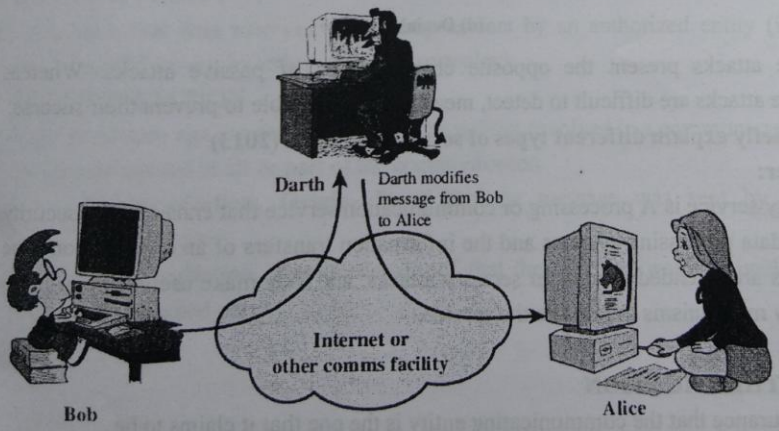
(a) Masquerade

ii) **Replay** involves the passive capture of a data unit and its subsequent retransmission to produce an unauthorized effect (Figure b).



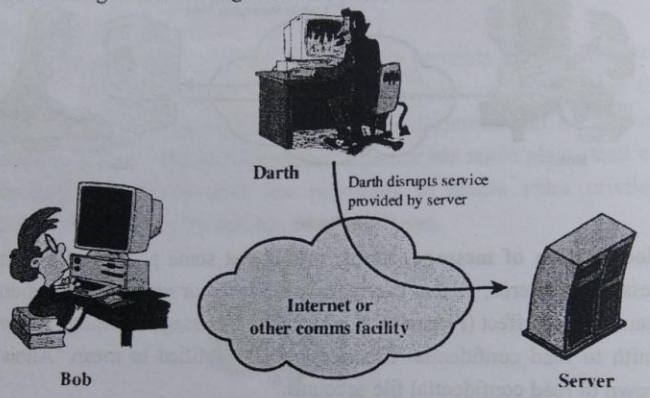
(b) Replay

iii) **Modification of messages** simply means that some portion of a legitimate message is altered, or that messages are delayed or reordered, to produce an unauthorized effect (Figure c). For example, a message meaning "Allow John Smith to read confidential file accounts" is modified to mean "Allow Fred Brown to read confidential file accounts."



(c) Modification of messages

iv) The **denial of service** prevents or inhibits the normal use or management of communications facilities (Figure d). This attack may have a specific target; for example, an entity may suppress all messages directed to a particular destination (e.g., the security audit service). Another form of service denial is the disruption of an entire network, either by disabling the network or by overloading it with messages so as to degrade performance.



(d) Denial of service

Active attacks present the opposite characteristics of passive attacks. Whereas passive attacks are difficult to detect, measures are available to prevent their success.

7. Briefly explain different types of security services. (2013)

Answer:

Security service is A processing or communication service that enhances the security of the data processing systems and the information transfers of an organization. The services are intended to counter security attacks, and they make use of one or more security mechanisms to provide the service.

a) AUTHENTICATION

The assurance that the communicating entity is the one that it claims to be.

i. Peer Entity Authentication

Used in association with a logical connection to provide confidence in the identity of the entities connected.

ii. **Data-Origin Authentication**

In a connectionless transfer, provides assurance that the source of received data is as claimed.

b) ACCESS CONTROL

The prevention of unauthorized use of a resource

(i.e., this service controls who can have access to a resource, under what conditions access can occur, and what those accessing the resource are allowed to do).

c) DATA CONFIDENTIALITY

The protection of data from unauthorized disclosure.

i. **Connection Confidentiality** -The protection of all user data on a connection.
ii. **Connectionless Confidentiality**- The protection of all user data in a single data block
iii. **Selective-Field Confidentiality** - The confidentiality of selected fields within the user data on a connection or in a single data block.
iv. **Traffic-Flow Confidentiality**- The protection of the information that might be derived from observation of traffic flows.

d) DATA INTEGRITY

The assurance that data received are exactly as sent by an authorized entity (i.e., contain no modification, insertion, deletion, or replay).

e) NONREPUDIATION

Provides protection against denial by one of the entities involved in a communication of having participated in all or part of the communication.

i. **Nonrepudiation, Origin**- Proof that the message was sent by the specified party.
ii. **Nonrepudiation, Destination**-Proof that the message was received by the specified party.

8. Distinguish network threats and attacks. (2016)

Answer:

Threat

A potential for violation of security, which exists when there is a circumstance, capability, action, or event that could breach security and cause harm. That is, a threat is a possible danger that might exploit a vulnerability.

Attack

An assault on system security that derives from an intelligent threat; that is, an intelligent act that is a deliberate attempt (especially in the sense of a method or technique) to evade security services and violate the security policy of a system.

9. Describe general model for network security briefly. (2010,2014,2015)
Or, draw network security model and discuss about it. (2016)

Answer:

A message is to be transferred from one party to another across some sort of internet. The two parties, who are the principals in this transaction, must cooperate for the exchange to take place. A logical information channel is established by defining a route through the internet from source to destination and by the cooperative use of communication protocols (e.g., TCP/IP) by the two principals.

Security aspects come into play when it is necessary or desirable to protect the information transmission from an opponent who may present a threat to confidentiality, authenticity, and so on. All the techniques for providing security have two components:

- ✓ A security-related transformation on the information to be sent. Examples include the encryption of the message, which scrambles the message so that it is unreadable by the opponent, and the addition of a code based on the contents of the message, which can be used to verify the identity of the sender
- ✓ Some secret information shared by the two principals and, it is hoped, unknown to the opponent. An example is an encryption key used in conjunction with the transformation to scramble the message before transmission and unscramble it on reception.

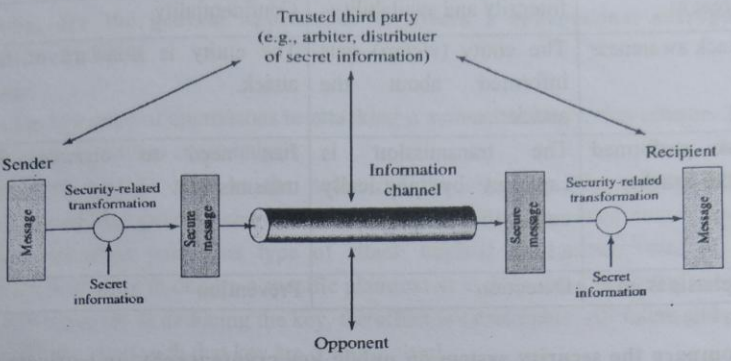


Figure : Model for Network Security

This general model shows that there are four basic tasks in designing a particular security service:

1. Design an algorithm for performing the security-related transformation. The algorithm should be such that an opponent cannot defeat its purpose.
2. Generate the secret information to be used with the algorithm.
3. Develop methods for the distribution and sharing of the secret information.
4. Specify a protocol to be used by the two principals that makes use of the security algorithm and the secret information to achieve a particular security service.

10. State the differences between active attacks and passive attacks. (2010,2015)

Answer:

BASIS FOR COMPARISON	ACTIVE ATTACK	PASSIVE ATTACK
Basic	Active attack tries to change the system resources or affect their operation.	Passive attack tries to read or make use of information from the system but does not influence system resources.
Modification in the information	Occurs	does not take place
Harm to the system	Always causes damage to the system.	Do not cause any harm.

Threat to	Integrity and availability	Confidentiality
Attack awareness	The entity (victim) gets informed about the attack.	The entity is unaware of the attack.
Task performed by the attacker	The transmission is captured by physically controlling the portion of a link.	Just need to observe the transmission.
Emphasis is on	Detection	Prevention

11. Compare the security system on public key cryptography and private key cryptography. (2012,2016)

Answer:

Private Key Cryptography	Public Key Cryptography
1. The same length algorithm with the same key is used for encryption and decryption.	1. One algorithm is used for encryption and decryption with a pair of keys, one for encryption and one for decryption.
2. The sender and receiver must share the algorithm and the key.	2. The sender and receiver must each have one of the matched pair of keys. (not the same one One)
3. The key must be kept secret.	3. One of the two keys must be kept secret
4. It must be impossible or at least impractical to decipher a message if no other information is available.	4. It must be impossible or at least impractical to decipher a message if no other information is available.
5. Knowledge of the algorithm plus samples of cipher text must be insufficient to determine the key.	5. Knowledge of the algorithm plus one of the keys plus samples of cipher text must be insufficient to determine the other key.

12. What are the general approaches to attack a conventional encryption scheme? (2010)

Answer:

There are two general approaches to attacking a symmetric encryption scheme. The first attack is known as cryptanalysis.

Cryptanalytic attacks rely on the nature of the algorithm plus perhaps some knowledge of the general characteristics of the plaintext or even some sample plaintext-ciphertext pairs.This type of attack exploits the characteristics of the algorithm to attempt to deduce a specific plaintext or to deduce the key being used. If the attack succeeds in deducing the key, the effect is catastrophic: All future and past messages encrypted with that key are compromised.

The second method, known as the brute-force attack, is to try every possible key on a piece of ciphertext until an intelligible translation into plaintext is obtained. In this method, the attacker tries to determine the key by attempting all possible keys. If the key is 8 bits long, then the number of possible keys is $2^8 = 256$. The attacker knows the ciphertext and the algorithm, now he attempts all the 256 keys one by one for decryption. The time to complete the attack would be very high if the key is long.

13. write down three independent dimensions of cryptography. (2016)

answer:

Cryptographic systems are characterized along three independent dimensions:

1. The type of operations used for transforming plaintext to cipher text. All encryption algorithms are based on two general principles: substitution, in which each element in the plaintext (bit, letter, group of bits or letters) is mapped into another element, and transposition, in which elements in the plaintext are rearranged. The fundamental requirement is that no information be lost (i.e., that all operations are reversible). Most systems, referred to as product systems, involve multiple stages of substitutions and transpositions.
2. The number of keys used. If both sender and receiver use the same key, the system is referred to as symmetric, single-key, secret-key, or conventional encryption. If the sender and receiver use different keys, the system is referred to as asymmetric, two-key, or public-key encryption.
3. The way in which the plaintext is processed. A block cipher processes the input one block of elements at a time, producing an output block for each input block. A

stream cipher processes the input elements continuously, producing output one element at a time, as it goes along.

14. define encryption. State the applications of the public key cryptosystem. (2015,2011)

answer:

Encryption is the method by which plaintext or any other type of data is converted from a readable form to an encoded version that can only be decoded by another entity if they have access to a decryption key. Encryption is one of the most important methods for providing data security, especially for end-to-end protection of data transmitted across networks.

Business Applications

The main business applications for public-key cryptography are:

- ✓ **Digital signatures** - content is digitally signed with an individual's private key and is verified by the individual's public key
- ✓ **Encryption** - content is encrypted using an individual's public key and can only be decrypted with the individual's private key
- ✓ **Security Benefits of Digital Signatures**
- ✓ Assuming the private key has remained secret and the individual it was issued to is the only person with access to it, digitally signing documents and emails offers the following benefits.
- ✓ **Authentication** – since the individual's unique private key was used to apply the signature, recipients can be confident that the individual was the one to actually apply the signature
- ✓ **Non-repudiation** – since the individual is the only one with access to the private key used to apply the signature, he/she cannot later claim that it wasn't him/her who applied the signature
- ✓ **Integrity** - when the signature is verified, it checks that the contents of the document or message match what was in there when the signature was applied. Even the slightest change to the original document would cause this check to fail.

Security Benefits of Encryption

Assuming the individual's private key has not been compromised, encrypting data and messages offers the following security benefits.

- ✓ **Confidentiality** - because the content is encrypted with an individual's public key, it can only be decrypted with the individual's private key, ensuring only the intended recipient can decrypt and view the contents
- ✓ **Integrity** - part of the decryption process involves verifying that the contents of the original encrypted message and the new decrypted match, so even the slightest change to the original content would cause the decryption process to fail

Chapter 2
Classical Encryption Techniques

1. Explain the difference between symmetric and asymmetric encryption, listing and advantage and disadvantage of each. (2013)

Answer:

Symmetric key encryption

Symmetric key encryption is also known as shared-key, single-key, secret-key, and private-key or one-key encryption. In this type of message encryption, both sender and receiver share the same key which is used to both encrypt and decrypt messages. Sender and receiver only have to specify the shared key in the beginning and then they can begin to encrypt and decrypt messages between them using that key. Examples include AES (Advanced Encryption Standard) and TripleDES (Data Encryption Standard).

Advantages

- **Simple:** This type of encryption is easy to carry out. All users have to do is specify and share the secret key and then begin to encrypt and decrypt messages.
- **Encrypt and decrypt your own files:** If you use encryption for messages or files which you alone intend to access, there is no need to create different keys. Single-key encryption is best for this.
- **Fast:** Symmetric key encryption is much faster than asymmetric key encryption.
- **Uses less computer resources:** Single-key encryption does not require a lot of computer resources when compared to public key encryption.
- **Prevents widespread message security compromise:** A different secret key is used for communication with every different party. If a key is compromised, only the

messages between a particular pair of sender and receiver are affected. Communications with other people are still secure.

Disadvantages

- **Need for secure channel for secret key exchange:** Sharing the secret key in the beginning is a problem in symmetric key encryption. It has to be exchanged in a way that ensures it remains secret.
- **Too many keys:** A new shared key has to be generated for communication with every different party. This creates a problem with managing and ensuring the security of all these keys.
- **Origin and authenticity of message cannot be guaranteed:** Since both sender and receiver use the same key, messages cannot be verified to have come from a particular user. This may be a problem if there is a dispute.

Asymmetric/Public Key Encryption

Also known as public key encryption, this method of encrypting messages makes use of two keys: a public key and a private key. The public key is made publicly available and is used to encrypt messages by anyone who wishes to send a message to the person that the key belongs to. The private key is kept secret and is used to decrypt received messages. An example of asymmetric key encryption system is RSA.

Advantages

- **Convenience:** It solves the problem of distributing the key for encryption.Everyone publishes their public keys and private keys are kept secret.
- **Provides for message authentication:** Public key encryption allows the use of digital signatures which enables the recipient of a message to verify that the message is truly from a particular sender.
- **Detection of tampering:** The use of digital signatures in public key encryption allows the receiver to detect if the message was altered in transit. A digitally signed message cannot be modified without invalidating the signature.
- **Provide for non-repudiation:** Digitally signing a message is akin to physically signing a document. It is an acknowledgement of the message and thus, the sender cannot deny it.

Disadvantages

- **Public keys should/must be authenticated:** No one can be absolutely sure that a public key belongs to the person it specifies and so everyone must verify that their public keys belong to them.
- **Slow:** Public key encryption is slow compared to symmetric encryption. Not feasible for use in decrypting bulk messages.
- **Uses up more computer resources:** It requires a lot more computer supplies compared to single-key encryption.
- **Widespread security compromise is possible:** If an attacker determines a person's private key, his or her entire messages can be read.
- **Loss of private key may be irreparable:** The loss of a private key means that all received messages cannot be decrypted.

Comparison of Symmetric Encryption and Asymmetric Encryption

Comparison Factor	Symmetric Encryption	Asymmetric Encryption
Number of Cryptographic Keys	Symmetric encryption incorporates only one key for encryption as well as decryption.	Asymmetric Encryption consists of two cryptographic keys. These keys are regarded as **Public Key** and **Private Key**.
Complexity	Symmetric encryption is a simple technique compared to asymmetric encryption as only one key is employed to carry out both the operations.	Contribution from separate keys for encryption and decryption makes it a rather complex process.
Swiftness of Execution	Due to its simplistic nature, both the operations can be carried out pretty quickly.	Because of encryption and decryption by two separate keys and the process of comparing them make it a tad slow procedure.
Algorithms Employed	• RC4 • AES • DES • 3DES • QUAD	• RSA • Diffie-Hellman • ECC • El Gamal • DSA

2. How a plant text can be converted into a cipher text? (2012)

Answer:

There are two primary ways in which a plain text can be modified to obtain cipher text: Substitution Technique and Transposition Technique.

1. Substitution Technique:

Substitution technique involves the replacement of the letters by other letters and symbols. In a more straightforward way, the characters of plaintext are replaced, and other substitute characters, numbers and symbols are used at their place.

Types of Substitution Technique:

1. **Caesar Cipher –**
   In this all characters of plain text is replaced by other characters with same pattern. For example, a replaced with D, B replaced with E.
2. **Mono Alphabetic Cipher –**
   Major disadvantage of caesar cipher is that all elements are substituted with same technique, it make easy for cryptanalyst to crack it. In Mono Alphabetic Cipher, There is no relation between Substitution of characters. Therefore it makes harder for cryptanalyst to crack it. For example, a can be replaced with B-Z, B can be replaced with A, C-Z.
3. **Homophonic Substitution Cipher –**
   In this technique, one plain text alphabet can map to more than one cipher text alphabet. This is the best substitution technique with maximum security. For example, a can be replaced with D and E.
4. **Polygram Substitution Cipher –**
   In this rather than replacing one alphabet, block of alphabet is replaced. For example,

   Polygram Subsitution
   HELLO ----------> YUQQW
   HELL ----------> TEUI

5. **Vigenere Cipher –**
   This technique uses multiple character keys .Each of the keys encrypts one single character. Each character is replaced by a number (A=0, B=1, …Z=25). After all keys are used, they are recycled. For encryption, Formula used : E=(M+K)mod 26

Plaintext: ATTACKATDAWN
Key: LEMONLEMONLE
Ciphertext: LXFOPVEFRNHR

2. Transposition Technique:

In transposition technique, the identity of the characters remains unchanged, but their positions are changed to create the ciphertext.

Types of Transpositional Techniques:

- ✓ **Rail Fence Technique** – It uses a simple algorithm:
  1. Write down plain text message as sequence of diagonals.
  2. Read the plain text written in step 1 as sequence of rows.

Plain text: come home

c m h m
o e o e

Cipher text : (READ ROW BY ROW) cmhmoeoe

- ✓ **Simple Columnar Transposition Technique** – It uses a simple algorithm:
  1. Write the plain text message row by row in predefined columns.
  2. Read the message column by column. It can be in any order.
  3. Message thus obtained is cipher text message.

Plain text: come niki (suppose we have 4 columns)

C1 C2 C3 C4
c o m e
n i k i

Now we can read in any order of columns. Lets read it by 3 -> 2 -> 4 ->1

Cipher text : mkoieicn

- ✓ **Vernam Cipher** – It uses a simple algorithm:
  1. Treat each plain text character as a number in increasing sequence (A=0, B=1, …Z=25).
  2. Do the same for each character of key.
  3. Add each number corresponding to plain text alphabet and key.
  4. If sum produced greater than 26, subtract 26 form it.
  5. Translate each number of sum back to alphabet, it gives our cipher text.

Plain text: HOW ARE YOU
Key : NCBTZQARX
H O W A R E Y O U

```
 7 14 22  0 17  4  24 14 20
+
 N  C  B  T  Z  Q  A  R  X
13  2  1 19 25 16  0 17 23
-------------------------------
20 16 23 19 42 20 24 31 43
```

Subtract 26 if >26: 20 16 23 19 16 20 24 5 17
Cipher text : U Q X T R U Y F R
Cipher text : UQXTRUYFR

3. Describe symmetric key cryptographic algorithm with example. (2012)
Or, Explain the symmetric cipher model with its ingredients.(2010,2015)

Answer: A symmetric encryption scheme has five ingredients (Figure 2.1):

- **Plaintext:** This is the original intelligible message or data that is fed into the algorithm as input.
- **Encryption algorithm:** The encryption algorithm performs various substitutions and transformations on the plaintext.
- **Secret key:** The secret key is also input to the encryption algorithm.The key is a value independent of the plaintext and of the algorithm. The algorithm will produce a different output depending on the specific key being used at the time.The exact substitutions and transformations performed by the algorithm depend on the key.
- **Ciphertext:** This is the scrambled message produced as output. It depends on the plaintext and the secret key. For a given message, two different keys will produce two different ciphertexts. The ciphertext is an apparently random stream of data and, as it stands, is unintelligible.

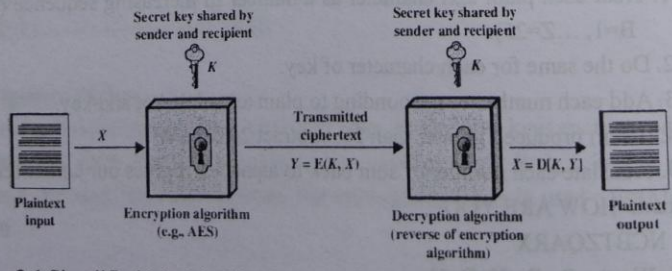


Figure 2.1 Simplified Model of Symmetric Encryption

- **Decryption algorithm:** This is essentially the encryption algorithm run in reverse. It takes the ciphertext and the secret key and produces the original plaintext.

There are two requirements for secure use of conventional encryption:

1. We need a strong encryption algorithm. At a minimum, we would like the algorithm to be such that an opponent who knows the algorithm and has access to one or more ciphertexts would be unable to decipher the ciphertext or figure out the key.This requirement is usually stated in a stronger form:The opponent should be unable to decrypt ciphertext or discover the key even if he or she is in possession of a number of ciphertexts together with the plaintext that produced each ciphertext.

2. Sender and receiver must have obtained copies of the secret key in a secure fashion and must keep the key secure. If someone can discover the key and knows the algorithm, all communication using this key is readable.

4. differentiate between symmetric and asymmetric encryption.(2011)
or, write the differences between symmetric cipher models and the asymmetric cipher model. (2010)

Comparison of Symmetric Encryption and Asymmetric Encryption

Comparison Factor	**Symmetric Encryption**	**Asymmetric Encryption**
Number of Cryptographic Keys	Symmetric encryption incorporates only one key for encryption as well as decryption.	Asymmetric Encryption consists of two cryptographic keys. These keys are regarded as **Public Key** and **Private Key**.
Complexity	Symmetric encryption is a simple technique compared to asymmetric encryption as only one key is employed to carry out both the operations.	Contribution from separate keys for encryption and decryption makes it a rather complex process.
Swiftness of Execution	Due to its simplistic nature, both the operations can be carried out pretty quickly.	Because of encryption and decryption by two separate keys and the process of comparing them make it a tad slow procedure.

Algorithms Employed	• RC4 • AES • DES • 3DES • QUAD	• RSA • Diffie-Hellman • ECC • El Gamal • DSA

5. briefly explain cryptanalysis and brute force attacks. (2010)

answer:

Typically, the objective of attacking an encryption system is to recover the key in use rather than simply to recover the plaintext of a single ciphertext.There are two general approaches to attacking a conventional encryption scheme:

• **Cryptanalysis:** Cryptanalytic attacks rely on the nature of the algorithm plus perhaps some knowledge of the general characteristics of the plaintext or even some sample plaintext–ciphertext pairs. This type of attack exploits the characteristics of the algorithm to attempt to deduce a specific plaintext or to deduce the key being used.

• **Brute-force attack:** The attacker tries every possible key on a piece of ciphertext until an intelligible translation into plaintext is obtained. On average, half of all possible keys must be tried to achieve success.

6. give example of brute force attack. what is brute force attack? (2016,2014)

answer:

A brute force attack is a trial-and-error method used to obtain information such as a user password or personal identification number (PIN). In a brute force attack, automated software is used to generate a large number of consecutive guesses as to the value of the desired data. Brute force attacks may be used by criminals to crack encrypted data, or by security analysts to test an organization's network security.

A brute force attack is also known as brute force cracking or simply brute force.

One example of a type of brute force attack is known as a dictionary attack, which might try all the words in a dictionary. Other forms of brute force attack might try commonly-used passwords or combinations of letters and numbers.

An attack of this nature can be time- and resource-consuming. Hence the name "brute force attack;" success is usually based on computing power and the number of combinations tried rather than an ingenious algorithm.

The following measures can be used to defend against brute force attacks:

- Requiring users to create complex passwords
- Limiting the number of times a user can unsuccessfully attempt to log in
- Temporarily locking out users who exceed the specified maximum number of failed login attempts

7. Explain various types of cryptanalysis attack with necessary diagram. (2014)

Answer:

The basic intention of an attacker is to break a cryptosystem and to find the plaintext from the ciphertext. To obtain the plaintext, the attacker only needs to find out the secret decryption key, as the algorithm is already in public domain.

Hence, he applies maximum effort towards finding out the secret key used in the cryptosystem. Once the attacker is able to determine the key, the attacked system is considered as broken or compromised.

Based on the methodology used, attacks on cryptosystems are categorized as follows –

- ✓ **Ciphertext Only Attacks (COA)** – In this method, the attacker has access to a set of ciphertext(s). He does not have access to corresponding plaintext. COA is said to be successful when the corresponding plaintext can be determined from a given set of ciphertext. Occasionally, the encryption key can be determined from this attack. Modern cryptosystems are guarded against ciphertext-only attacks.
- ✓ **Known Plaintext Attack (KPA)** – In this method, the attacker knows the plaintext for some parts of the ciphertext. The task is to decrypt the rest of the ciphertext using this information. This may be done by determining the key or via some other method. The best example of this attack is linear cryptanalysis against block ciphers.
- ✓ **Chosen Plaintext Attack (CPA)** – In this method, the attacker has the text of his choice encrypted. So he has the ciphertext-plaintext pair of his choice. This simplifies his task of determining the encryption key. An example of this attack is differential cryptanalysis applied against block ciphers as well as hash functions. A popular public key cryptosystem, RSA is also vulnerable to chosen-plaintext attacks.
- ✓ **Dictionary Attack** – This attack has many variants, all of which involve compiling a 'dictionary'. In simplest method of this attack, attacker builds a dictionary of ciphertexts and corresponding plaintexts that he has learnt over a

period of time. In future, when an attacker gets the ciphertext, he refers the dictionary to find the corresponding plaintext.

8. distinguish between a season key and a master key. (2011,2014)

answer:

A **session key** is a temporary encryption key used between two principals.

A **master key** is a long-lasting key that is used between a key distribution center and a principal for the purpose of encoding the transmission of session keys. Typically, the master keys are distributed by non-cryptographic means.

Session key	Master key
Communication between end systems is encrypted using temporary key, often referred to as a session key.	Session keys are transmitted in encrypted form, using master key that is shared by the keys distribution center and an end system.
The session key is used for the duration of a logical connection, such as a frame relay connection or transport connection, and then discarded.	For each end system or user, there is a unique master key that it shares with the key distribution center. These master keys must be distributed in some fashion.

9. explain the one time pad with example. (2010)

answer:

One-Time Pad

The circumstances are –

- The length of the keyword is same as the length of the plaintext.
- The keyword is a randomly generated string of alphabets.
- The keyword is used only once.

Security Value

Let us compare Shift cipher with one-time pad.

Shift Cipher – Easy to Break

In case of Shift cipher, the entire message could have had a shift between 1 and 25. This is a very small size, and very easy to brute force. However, with each character now having its own individual shift between 1 and 26, the possible keys grow exponentially for the message.

One-time Pad – Impossible to Break

Let us say, we encrypt the name "point" with a one-time pad. It is a 5 letter text. To break the ciphertext by brute force, you need to try all possibilities of keys and

conduct computation for (26 x 26 x 26 x 26 x 26) = 26^5 = 11881376 times. That's for a message with 5 alphabets. Thus, for a longer message, the computation grows exponentially with every additional alphabet. This makes it computationally impossible to break the ciphertext by brute force.

10. explain the rules for encrypting plain text using playfair cypher with suitable example. (2010, 2016)

answer:

In playfair cipher, initially a key table is created. The key table is a 5×5 grid of alphabets that acts as the key for encrypting the plaintext. Each of the 25 alphabets must be unique and one letter of the alphabet (usually J) is omitted from the table as we need only 25 alphabets instead of 26. If the plaintext contains J, then it is replaced by I.

The sender and the receiver deicide on a particular key, say 'tutorials'. In a key table, the first characters (going left to right) in the table is the phrase, excluding the duplicate letters. The rest of the table will be filled with the remaining letters of the alphabet, in natural order. The key table works out to be –

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

Process of Playfair Cipher

- ✓ First, a plaintext message is split into pairs of two letters (digraphs). If there is an odd number of letters, a Z is added to the last letter. Let us say we want to encrypt the message "hide money". It will be written as –

  HI DE MO NE YZ

- ✓ The rules of encryption are –
  - If both the letters are in the same column, take the letter below each one (going back to the top if at the bottom)

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

'H' and 'I' are in same column, hence take letter below them to re
HI → QC

- ✓ If both letters are in the same row, take the letter to the right of each one (going back to the left if at the farthest right)

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

'D' and 'E' are in same row, hence take letter to the right of th
replace. DE → EF

- If neither of the preceding two rules are true, form a rectangle with the two letters and take the letters on the horizontal opposite corner of the rectangle.

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

'M' and 'O' nor on same column or same row, hence form rectangle as shown, and replace letter by picking up opposite corner letter on same row
MO -> NU

Using these rules, the result of the encryption of 'hide money' with the key of 'tutorials' would be –

QC EF NU MF ZV

Decrypting the Playfair cipher is as simple as doing the same process in reverse. Receiver has the same key and can create the same key table, and then decrypt any messages made using that key.

11. what is the difference between a monoalphabetic cipher and a polyalphabetic cipher. (2016)

answer:

Comparison Between Monoalphabetic and Polyalphabetic Cipher

Monoalphabetic Cipher	Polyalphabetic cipher
Once a key is chosen, each alphabetic character of plaintext is mapped onto a unique alphabetic character of a ciphertext.	Each alphabetic character of plaintext can be mapped onto "m" alphabetic characters of a ciphertext.
The relationship between a character in the plaintext and the characters in the ciphertext is one-to-one.	The relationship between a character in the plaintext and the characters in the ciphertext is one-to-many.
A stream cipher is a monoalphabetic cipher if the value of ki does not depend on the position of the plaintext character in the plaintext stream	A stream cipher is a polyalphabetic cipher if the value of id does depend on the position of the plaintext character in the plaintext stream.
Monoalphabetic cipher includes additive, multiplicative, affine and monoalphabetic substitution cipher.	Polyalphabetic cipher includes autokey, Playfair, Vigenere, Hill, one-time pad, rotor, and Enigma cipher.

12. what are the differences between an unconditionally secure cipher and a computationally secure cipher. (2014)

Answer:

An encryption scheme is unconditionally secure if the ciphertext generated by the scheme does not contain enough information to determine uniquely the corresponding plaintext, no matter how much ciphertext is available.

An encryption scheme is said to be **computationally secure** if:

1. the cost of breaking the cipher exceeds the value of the encrypted information, and
2. the time required to break the cipher exceeds the useful lifetime of the information.

Chapter 3
Block Ciphers and the Data Encryption Standard

1. what is data encryption standard? (2012)

answer:

The Data Encryption Standard (DES) is a symmetric-key block cipher published by the National Institute of Standards and Technology (NIST).

DES is an implementation of a Feistel Cipher. It uses 16 round Feistel structure. The block size is 64-bit. Though, key length is 64-bit, DES has an effective key length of 56 bits, since 8 of the 64 bits of the key are not used by the encryption algorithm (function as check bits only).

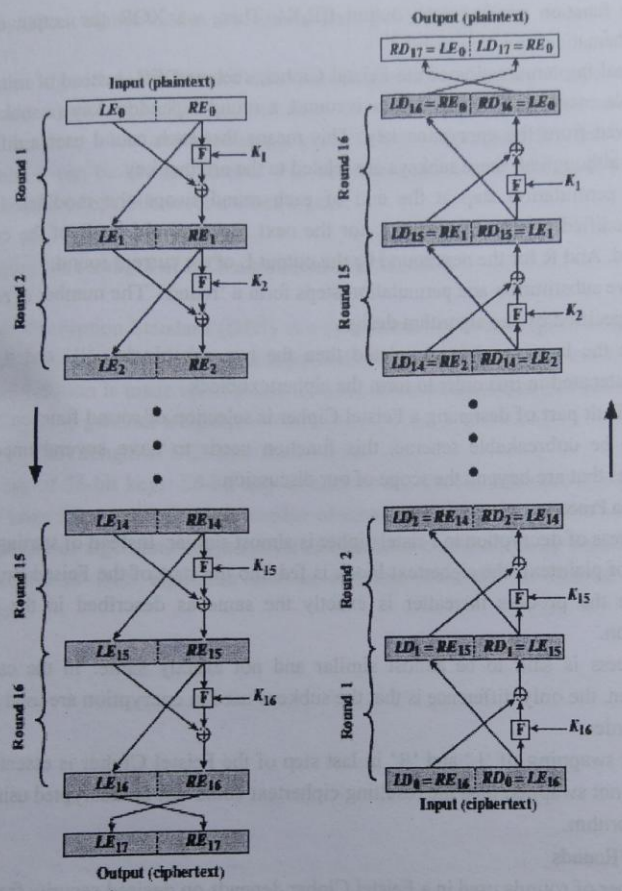
2. describe the operation of feistal cipher. (2012)

answer: Feistel Cipher is not a specific scheme of block cipher. It is a design model from which many different block ciphers are derived. DES is just one example of a Feistel Cipher. A cryptographic system based on Feistel cipher structure uses the same algorithm for both encryption and decryption.

Encryption Process

The encryption process uses the Feistel structure consisting multiple rounds of processing of the plaintext, each round consisting of a "substitution" step followed by a permutation step.

Feistel Structure is shown in the following illustration –



- ✓ The input block to each round is divided into two halves that can be denoted as L and R for the left half and the right half.
- ✓ In each round, the right half of the block, R, goes through unchanged. But the left half, L, goes through an operation that depends on R and the encryption key. First, we apply an encrypting function 'f' that takes two input – the key K and R.

The function produces the output f(R,K). Then, we XOR the output of the mathematical function with L.

- ✓ In real implementation of the Feistel Cipher, such as DES, instead of using the whole encryption key during each round, a round-dependent key (a subkey) is derived from the encryption key. This means that each round uses a different key, although all these subkeys are related to the original key.
- ✓ The permutation step at the end of each round swaps the modified L and unmodified R. Therefore, the L for the next round would be R of the current round. And R for the next round be the output L of the current round.
- ✓ Above substitution and permutation steps form a 'round'. The number of rounds are specified by the algorithm design.
- ✓ Once the last round is completed then the two sub blocks, 'R' and 'L' are concatenated in this order to form the ciphertext block.

The difficult part of designing a Feistel Cipher is selection of round function 'f'. In order to be unbreakable scheme, this function needs to have several important properties that are beyond the scope of our discussion.

Decryption Process

The process of decryption in Feistel cipher is almost similar. Instead of starting with a block of plaintext, the ciphertext block is fed into the start of the Feistel structure and then the process thereafter is exactly the same as described in the given illustration.

The process is said to be almost similar and not exactly same. In the case of decryption, the only difference is that the subkeys used in encryption are used in the reverse order.

The final swapping of 'L' and 'R' in last step of the Feistel Cipher is essential. If these are not swapped then the resulting ciphertext could not be decrypted using the same algorithm.

Number of Rounds

The number of rounds used in a Feistel Cipher depends on desired security from the system. More number of rounds provide more secure system. But at the same time, more rounds mean the inefficient slow encryption and decryption processes. Number of rounds in the systems thus depend upon efficiency–security tradeoff.

3. Why block cipher modes are convenient? (2012,2015)

Answer:

Encryption algorithms are divided into two categories based on input type, as block cipher and stream cipher. Block cipher is an encryption algorithm which takes fixed size of input say b bits and produces a ciphertext of b bits again. If input is larger than b bits it can be divided further. For different applications and uses, there are several modes of operations for a block cipher.

4. Discuss the strength of DES algorithm. (2012,2014)

answer:

The Data Encryption Standard (DES) is a symmetric key block cipher which takes 64-bit plaintext and 56-bit key as an input and produces 64-bit cipher text as output. The DES function is made up of P and S-boxes. P-boxes transpose bits and S-boxes substitute bits to generate a cipher.

Strength- The strength of DES lies on two facts:

a. The use of 56-bit keys: 56-bit key is used in encryption, there are 256 possible keys. A brute force attack on such number of keys is impractical.

b. The nature of algorithm: Cryptanalyst can perform cryptanalysis by exploiting the characteristic of DES algorithm but no one has succeeded in finding out the weakness.

5. draw single round DES architecture and briefly explain its operational procedure. (2013)

answer:

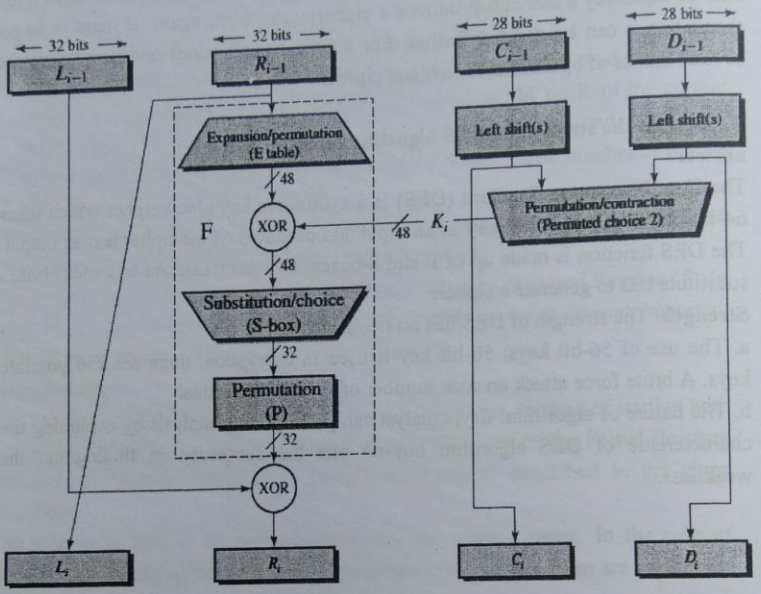


Figure : Single Round of DES Algorithm

Figure shows the internal structure of a single round.

Again, begin by focusing on the left-hand side of the diagram. The left and right halves of each 64-bit intermediate value are treated as separate 32-bit quantities, labeled L (left) and R (right). As in any classic Feistel cipher, the overall processing at each round can be summarized in the following formulas:

$$L_i = R_{i-1}$$
$$R_i = L_{i-1} \oplus F(R_{i-1}, K_i)$$

The round key K_i is 48 bits. The R input is 32 bits. This R input is first expanded to 48 bits by using a table that defines a permutation plus an expansion that involves duplication of 16 of the R bits .The resulting 48 bits are XORed with K_i. This 48-bit result passes through a substitution function that produces a 32-bit output,

6. A fiestel cipher is used in the DES algorithm. Describe the of a Feistal cipher. (2013)

what is Feistel cypher? How it works in a cryptographic algorithm? (2015)

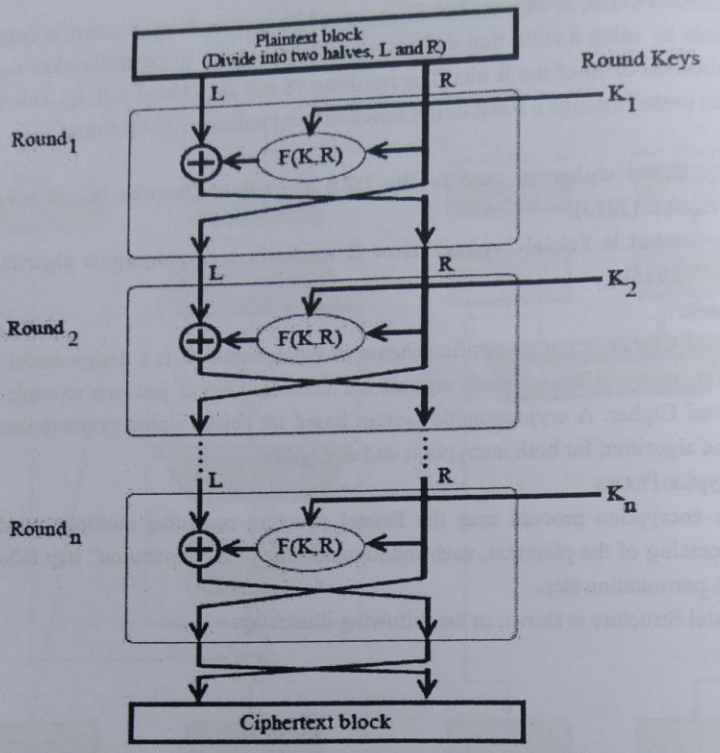
Answer:

Feistel Cipher is not a specific scheme of block cipher. It is a design model from which many different block ciphers are derived. DES is just one example of a Feistel Cipher. A cryptographic system based on Feistel cipher structure uses the same algorithm for both encryption and decryption.

Encryption Process

The encryption process uses the Feistel structure consisting multiple rounds of processing of the plaintext, each round consisting of a "substitution" step followed by a permutation step.

Feistel Structure is shown in the following illustration –



- ✓ The input block to each round is divided into two halves that can be denoted as L and R for the left half and the right half.
- ✓ In each round, the right half of the block, R, goes through unchanged. But the left half, L, goes through an operation that depends on R and the encryption key. First, we apply an encrypting function 'f' that takes two input – the key K and R. The function produces the output f(R,K). Then, we XOR the output of the mathematical function with L.
- ✓ In real implementation of the Feistel Cipher, such as DES, instead of using the whole encryption key during each round, a round-dependent key (a subkey) is derived from the encryption key. This means that each round uses a different key, although all these subkeys are related to the original key.

- ✓ The permutation step at the end of each round swaps the modified L and unmodified R. Therefore, the L for the next round would be R of the current round. And R for the next round be the output L of the current round.
- ✓ Above substitution and permutation steps form a 'round'. The number of rounds are specified by the algorithm design.
- ✓ Once the last round is completed then the two sub blocks, 'R' and 'L' are concatenated in this order to form the ciphertext block.

The difficult part of designing a Feistel Cipher is selection of round function 'f'. In order to be unbreakable scheme, this function needs to have several important properties that are beyond the scope of our discussion.

Decryption Process

The process of decryption in Feistel cipher is almost similar. Instead of starting with a block of plaintext, the ciphertext block is fed into the start of the Feistel structure and then the process thereafter is exactly the same as described in the given illustration.

The process is said to be almost similar and not exactly same. In the case of decryption, the only difference is that the subkeys used in encryption are used in the reverse order.

The final swapping of 'L' and 'R' in last step of the Feistel Cipher is essential. If these are not swapped then the resulting ciphertext could not be decrypted using the same algorithm.

Number of Rounds

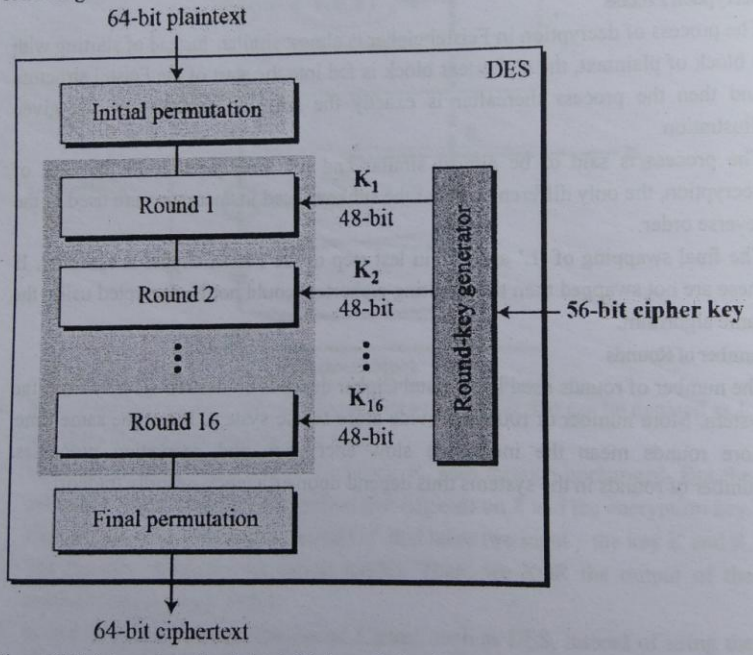
The number of rounds used in a Feistel Cipher depends on desired security from the system. More number of rounds provide more secure system. But at the same time, more rounds mean the inefficient slow encryption and decryption processes. Number of rounds in the systems thus depend upon efficiency–security tradeoff.

7. state the DES process with diagram. (2010)
or, briefly explain general DES encryption algorithm. (2014)

answer:

The Data Encryption Standard (DES) is a symmetric-key block cipher published by the National Institute of Standards and Technology (NIST).

DES is an implementation of a Feistel Cipher. It uses 16 round Feistel structure. The block size is 64-bit. Though, key length is 64-bit, DES has an effective key length of 56 bits, since 8 of the 64 bits of the key are not used by the encryption algorithm (function as check bits only). General Structure of DES is depicted in the following illustration –

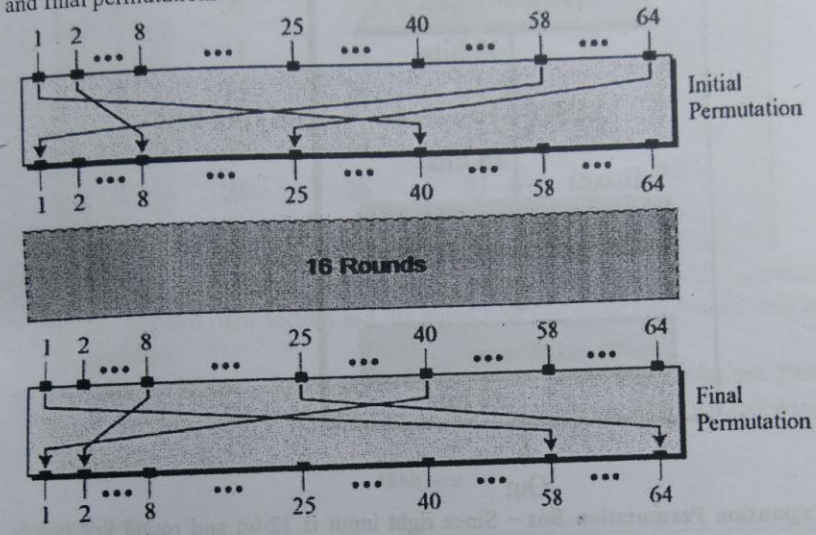


Since DES is based on the Feistel Cipher, all that is required to specify DES is –

- Round function
- Key schedule
- Any additional processing – Initial and final permutation

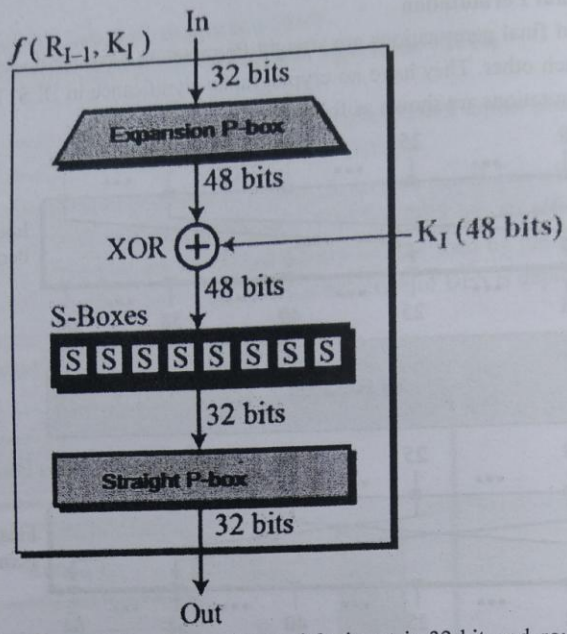
Initial and Final Permutation

The initial and final permutations are straight Permutation boxes (P-boxes) that are inverses of each other. They have no cryptography significance in DES. The initial and final permutations are shown as follows –

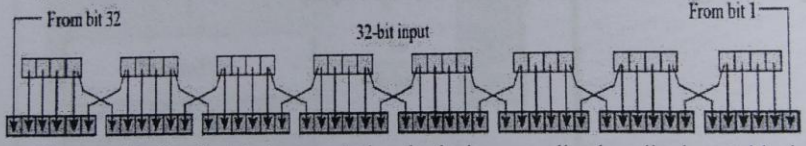


Round Function

The heart of this cipher is the DES function, f. The DES function applies a 48-bit key to the rightmost 32 bits to produce a 32-bit output.



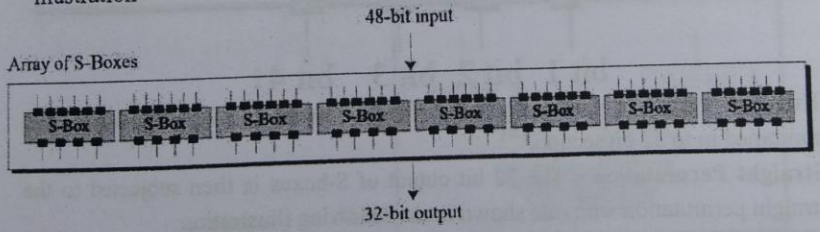
- **Expansion Permutation Box** – Since right input is 32-bit and round key is a 48-bit, we first need to expand right input to 48 bits. Permutation logic is graphically depicted in the following illustration –



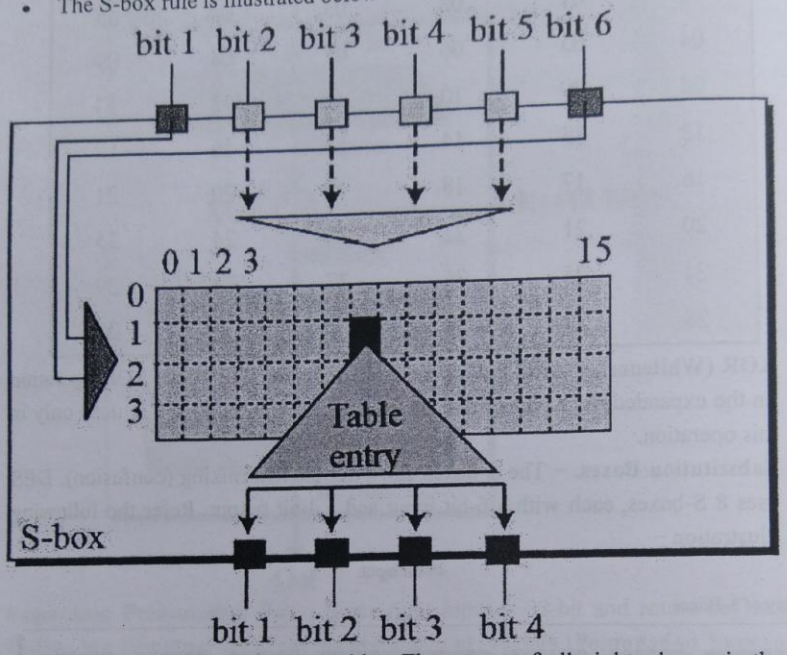
- The graphically depicted permutation logic is generally described as table in DES specification illustrated as shown –

32	01	02	03	04	05
04	05	06	07	08	09
08	09	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	31	31	32	01

- **XOR (Whitener).** – After the expansion permutation, DES does XOR operation on the expanded right section and the round key. The round key is used only in this operation.
- **Substitution Boxes.** – The S-boxes carry out the real mixing (confusion). DES uses 8 S-boxes, each with a 6-bit input and a 4-bit output. Refer the following illustration –



- The S-box rule is illustrated below –

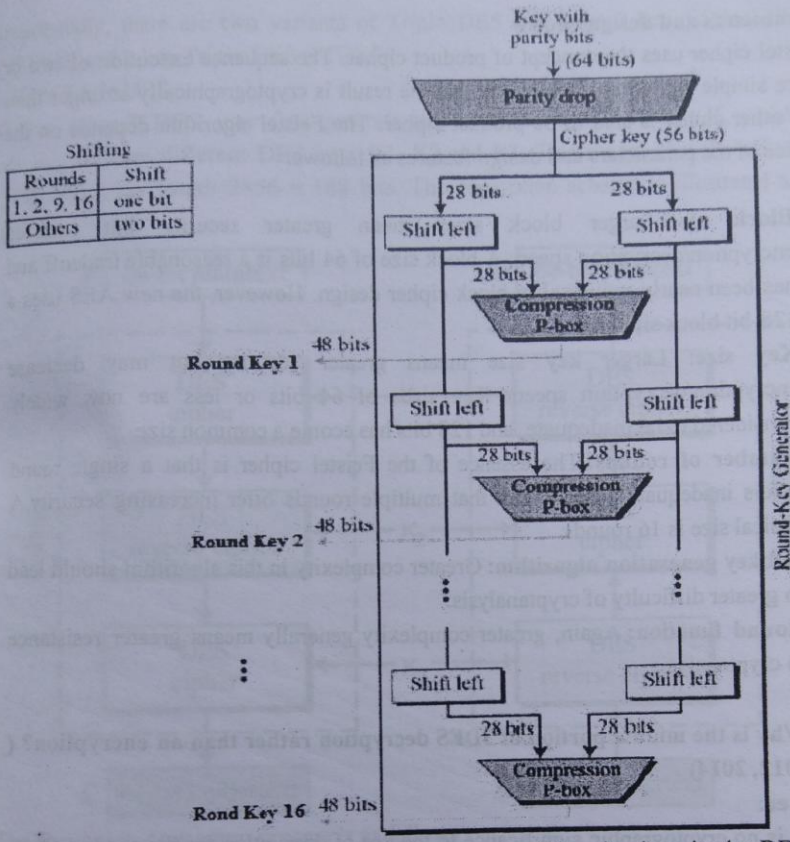


- There are a total of eight S-box tables. The output of all eight s-boxes is then combined in to 32 bit section.
- **Straight Permutation** – The 32 bit output of S-boxes is then subjected to the straight permutation with rule shown in the following illustration:

16	07	20	21	29	12	28	17
01	15	23	26	05	18	31	10
02	08	24	14	32	27	03	09
19	13	30	06	22	11	04	25

Key Generation

The round-key generator creates sixteen 48-bit keys out of a 56-bit cipher key. The process of key generation is depicted in the following illustration –



The logic for Parity drop, shifting, and Compression P-box is given in the DES description.

8. define steganography. which parameters and design choice determine the actual algorithm of a Feistel cipher? (2014)

answer:

A plaintext message may be hidden in one of two ways. The methods of **steganography** conceal the existence of the message, whereas the methods of cryptography render the message unintelligible to outsiders by various transformations of the text.

parameters and design choice

Feistel cipher uses the concept of product cipher. The sequence execution of two or more simple ciphers in such a way that the result is cryptographically stronger than any other cipher is said to be product cipher. The Feistel algorithm depends on the choice of the parameters and design features as follows:

- ✓ **Block size:** Larger block sizes mean greater security but reduced encryption/decryption speed. A block size of 64 bits is a reasonable tradeoff and has been nearly universal in block cipher design. However, the new AES uses a 128-bit block size.
- ✓ **Key size:** Larger key size means greater security but may decrease encryption/decryption speed. Key sizes of 64 bits or less are now widely considered to be inadequate, and 128 bits has ecome a common size.
- ✓ **Number of rounds:** The essence of the Feistel cipher is that a single round offers inadequate security but that multiple rounds offer increasing security.A typical size is 16 rounds.
- ✓ **Subkey generation algorithm:** Greater complexity in this algorithm should lead to greater difficulty of cryptanalysis.
- ✓ **Round function:** Again, greater complexity generally means greater resistance to cryptanalysis.

9. Why is the middle portion of 3DES decryption rather than an encryption? (2012, 2014)

Answer:

There is no cryptographic significance to the use of decryption for the second stage. Its only advantage is that it allows users of 3DES to decrypt data encrypted by users of the older single DES by repeating the key.

10. what is triple encryption? how many keys are used in this encryption technique?

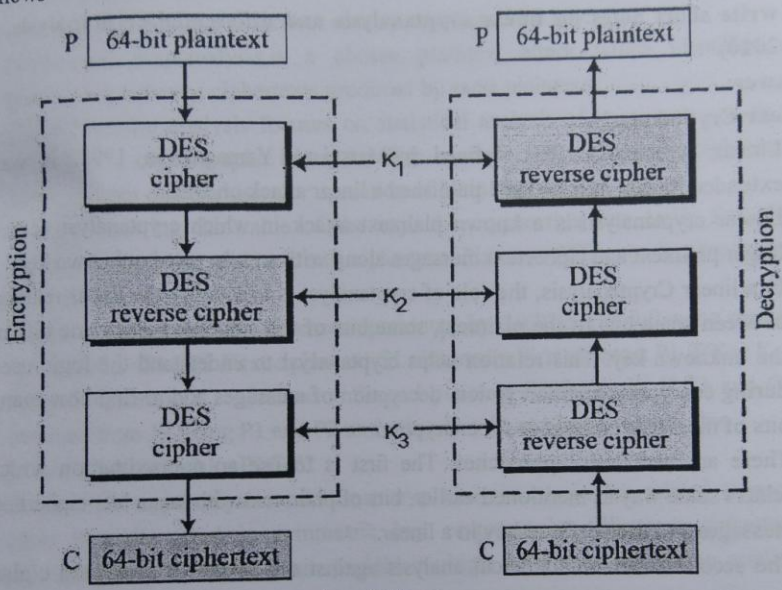
answer:

The pragmatic approach was not to abandon the DES completely, but to change the manner in which DES is used. This led to the modified schemes of Triple DES (sometimes known as 3DES).

Incidentally, there are two variants of Triple DES known as 3-key Triple DES (3TDES) and 2-key Triple DES (2TDES).

3-KEY Triple DES

Before using 3TDES, user first generate and distribute a 3TDES key K, which consists of three different DES keys K1, K2 and K3. This means that the actual 3TDES key has length 3×56 = 168 bits. The encryption scheme is illustrated as follows –



The encryption-decryption process is as follows –

- Encrypt the plaintext blocks using single DES with key K_1.
- Now decrypt the output of step 1 using single DES with key K_2.
- Finally, encrypt the output of step 2 using single DES with key K_3.
- The output of step 3 is the ciphertext.
- Decryption of a ciphertext is a reverse process. User first decrypt using K_3, then encrypt with K_2, and finally decrypt with K_1.

Due to this design of Triple DES as an encrypt–decrypt–encrypt process, it is possible to use a 3TDES (hardware) implementation for single DES by setting K_1, K_2, and K_3 to be the same value. This provides backwards compatibility with DES.

Second variant of Triple DES (2TDES) is identical to 3TDES except that $K_3$is replaced by K_1. In other words, user encrypt plaintext blocks with key K_1, then decrypt with key K_2, and finally encrypt with K_1 again. Therefore, 2TDES has a key length of 112 bits.

Triple DES systems are significantly more secure than single DES, but these are clearly a much slower process than encryption using single DES.

11. write short notes on linear cryptanalysis and differential cryptanalysis. (2010)

Answer:

Linear Cryptanalysis

- Linear cryptanalysis first defined by Matsui and Yamagishi in 1992. It was extended Matsui later in 1993 published a linear attack on DES.
- Linear cryptanalysis is a known plaintext attack in which cryptanalyst access larger plaintext and ciphertext messages along with an encrypted unknown key.
- In a linear Cryptanalysis, the role of cryptanalyst is to identify the linear relation between some bits of the plaintext, some bits of the ciphertext and some bits of the unknown key. This relation helps cryptanalyst to understand the logic used during encryption and decryption. decryption of messages and to find how many bits of messages undergoes for encryption.
- There are two basic approaches. The first is to use an approximation which relates some way as mentioned earlier. bits of plain text with some bits ciphertext messages and user-defined key in a linear.
- The second focus on statistical analysis against one round of decrypted cipher text. The cryptanalyst each cipher text using all possible sub keys for one round of encryption and studies the resulting intermediate cipher text to analyze the random result.
- The sub key obtained during this pro and dec g this process called as candidate key used during encryption of a large amount of data.

Differential Cryptanalysis

- Differential cryptanalysis is a method for breaking certain classes of cryptosystems. It was invented in 1990 by Israeli researchers Eli Biham and Adi Shamir.
- Differential cryptanalysis is available to obtain clues about some bits of the key, thereby shortening an exhaustive search. By analyzing the changes in some chosen plaintexts, and the difference in the outputs resulting from encrypting each one, it is possible to recover some properties of the key.
- Differential cryptanalysis is a chosen plaintext attack which identifies a relationship between ciphertexts produced by same plaintexts.
- The differential analysis focuses on statistical analysis of two inputs and two outputs of a cryptographic algorithm. For example, assume that the ciphertext obtained from one exclusive-or operation of plain text and key.
- Without knowing the value of the key, the cryptanalyst can easily find the differences between plaintext and ciphertext. Plaintext difference is represented by P1⊕P2.
- Whereas the ciphertext difference represented by C1⊕C2. The following proves that C1⊕C2 =P1⊕P2 First ciphertext C1 obtained = First plaintext P1 ⊕Key K
- Second ciphertext C2 obtained = Second plaintext P2 ⊕Key K, if C1 and C2 obtained from XORing P1 and P2 and using Key K, can be represented by,

C1⊕C2=P1⊕K⊕P2⊕K=P1⊕P2

- Differential cryptanalysis and linear cryptanalysis attacks are related to each other basically used in symmetric key cryptography. Whatever ciphertext produced from the same plain text the multiple rounds of encryption applied using for each round.
- Subkey Cryptanalyst studies changes to the intermediate cipher text obtained between multiple rounds of encryption. The attacks can be combined, which is called differential linear cryptanalysis.

Chapter 4
Advanced Encryption Standard

1. write the final set of criteria used by NIST to evaluate candidate ASE cipher?
(2010,2014,2015)

answer: The final set of criteria used by NIST to evaluate candidate ASE cipher

a) General security;
b) software implementations;
c) restricted-space environments;
d) hardware implementations;
e) attacks on implementations;
f) encryption vs. decryption;
g) key agility;
h) other versatility and flexibility;
i) potential for instruction-level parallelism.

2. explain the salient features of AES. (2010)

answer:

The more popular and widely adopted symmetric encryption algorithm likely to be encountered nowadays is the Advanced Encryption Standard (AES). It is found at least six time faster than triple DES.

The features of AES are as follows –

- Symmetric key symmetric block cipher
- 128-bit data, 128/192/256-bit keys
- Stronger and faster than Triple-DES
- Provide full specification and design details
- Software implementable in C and Java

3. state the differences between rijndael and AES? (2010)

answer: AES was developed by NIST .AES is a symmetric block cipher that is intended to replace DES. NIST selected Rijndael as the proposed AES algorithm.

AES is a reduced version of Rijndael where it is only defined for block sizes of 128 bit whereas Rijndael is defined for block sizes of 128, 192 and 256 bit. If a different

block size between encryption and decryption is used, then it is not possible to recover the original plaintext.

Rijndael-256 and Rijndael-192 must be seen as completely different algorithms from AES (Rijndael-128). They are inherently incompatible.

4. what is the difference between AES decryption algorithm and the equivalent inverse cipher? (2011,2014)

answer:

In AES decryption, we use inverse shift rows inverse sub bytes, add round key, inverse mix columns. But in equivalent inverse cipher, we interchange inverse shift rows and inverse sub bytes.

The difference of equivalent decryption algorithms and standard decryption algorithms can be summarized as:

- ✓ Standard decryption algorithms use same round keys as the encryption algorithm, but applies transformation procedures in a different sequence.
- ✓ Equivalent decryption algorithms have the same sequence of applying transformation procedures as the encryption algorithm, but uses modified round keys.

5. differentiate between AES and DES. (2015)

answer:

BASIS FOR COMPARISON	DES (DATA ENCRYPTION STANDARD)	AES (ADVANCED ENCRYPTION STANDARD)
Basic	In DES the data block is divided into two halves.	In AES the entire data block is processed as a single matrix.
Principle	DES work on Feistel Cipher structure.	AES works on Substitution and Permutation Principle.
Plaintext	Plaintext is of 64 bits	Plaintext can be of 128,192, or 256 bits
Key size	DES in comparison to AES has smaller key size.	AES has larger key size as compared to DES.

Rounds	16 rounds	10 rounds for 128-bit algo 12 rounds for 192-bit algo 14 rounds for 256-bit algo
Rounds Names	Expansion Permutation, Xor, S-box, P-box, Xor and Swap.	Subbytes, Shiftrows, Mix columns, Addroundkeys.
Security	DES has a smaller key which is less secure.	AES has large secret key comparatively hence, more secure.
Speed	DES is comparatively slower.	AES is faster.

Chapter 6
Block Cipher Operation & Pseudorandom Number

1. mention the weakness of electronic code book mode. (2010)

In reality, any application data usually have partial information which can be guessed. For example, the range of salary can be guessed. A ciphertext from ECB can allow an attacker to guess the plaintext by trial-and-error if the plaintext message is within predictable.

For example, if a ciphertext from the ECB mode is known to encrypt a salary figure, then a small number of trials will allow an attacker to recover the figure. In general, we do not wish to use a deterministic cipher, and hence the ECB mode should not be used in most applications.

2. describe briefly about the block cipher modes of operation. (2011)

A block cipher processes the data blocks of fixed size. Usually, the size of a message is larger than the block size. Hence, the long message is divided into a series of sequential message blocks, and the cipher operates on these blocks one at a time.

Electronic Code Book (ECB) Mode

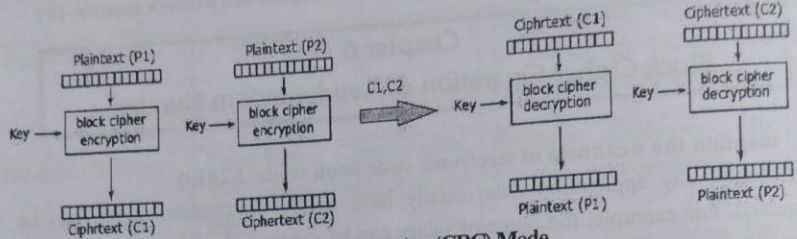
This mode is a most straightforward way of processing a series of sequentially listed message blocks.

Operation

- ✓ The user takes the first block of plaintext and encrypts it with the key to produce the first block of ciphertext.
- ✓ He then takes the second block of plaintext and follows the same process with same key and so on so forth.

The ECB mode is deterministic, that is, if plaintext block P1, P2,..., Pm are encrypted twice under the same key, the output ciphertext blocks will be the same.

In fact, for a given key technically we can create a codebook of ciphertexts for all possible plaintext blocks. Encryption would then entail only looking up for required plaintext and select the corresponding ciphertext. Thus, the operation is analogous to the assignment of code words in a codebook, and hence gets an official name – Electronic Codebook mode of operation (ECB). It is illustrated as follows –



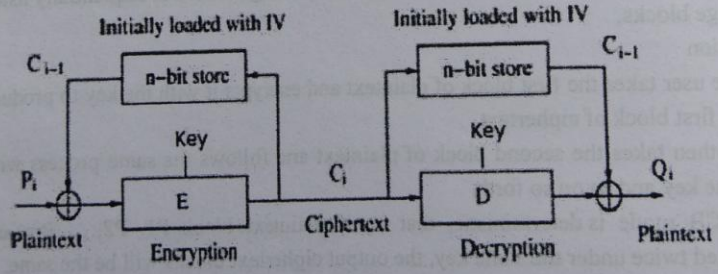
Cipher Block Chaining (CBC) Mode

CBC mode of operation provides message dependence for generating ciphertext and makes the system non-deterministic.

Operation

The operation of CBC mode is depicted in the following illustration. The steps are as follows –

- ✓ Load the n-bit Initialization Vector (IV) in the top register.
- ✓ XOR the n-bit plaintext block with data value in top register.
- ✓ Encrypt the result of XOR operation with underlying block cipher with key K.
- ✓ Feed ciphertext block into top register and continue the operation till all plaintext blocks are processed.
- ✓ For decryption, IV data is XORed with first ciphertext block decrypted. The first ciphertext block is also fed into to register replacing IV for decrypting next ciphertext block.



Cipher Feedback (CFB) Mode

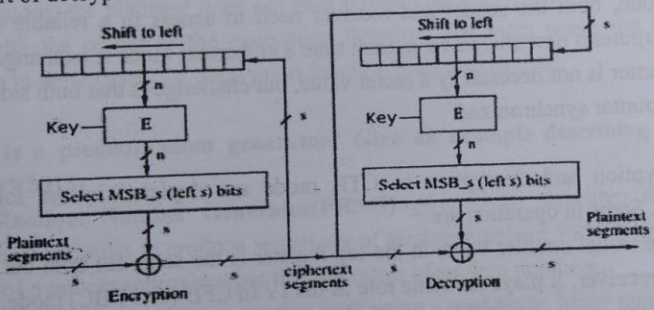
In this mode, each ciphertext block gets 'fed back' into the encryption process in order to encrypt the next plaintext block.

Operation

The operation of CFB mode is depicted in the following illustration. For example, in the present system, a message block has a size 's' bits where $1 < s < n$. The CFB

mode requires an initialization vector (IV) as the initial random n-bit input block. The IV need not be secret. Steps of operation are –

- ✓ Load the IV in the top register.
- ✓ Encrypt the data value in top register with underlying block cipher with key K.
- ✓ Take only 's' number of most significant bits (left bits) of output of encryption process and XOR them with 's' bit plaintext message block to generate ciphertext block.
- ✓ Feed ciphertext block into top register by shifting already present data to the left and continue the operation till all plaintext blocks are processed.
- ✓ Essentially, the previous ciphertext block is encrypted with the key, and then the result is XORed to the current plaintext block.
- ✓ Similar steps are followed for decryption. Pre-decided IV is initially loaded at the start of decryption.

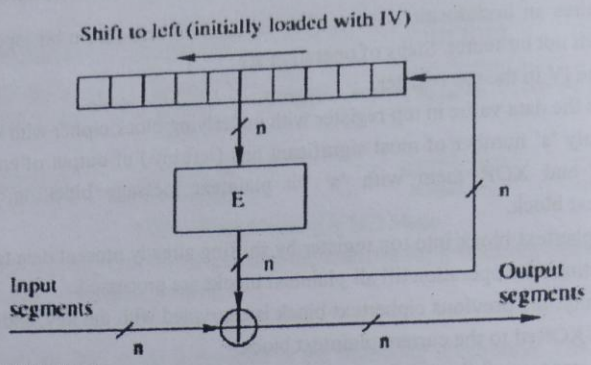


Output Feedback (OFB) Mode

It involves feeding the successive output blocks from the underlying block cipher back to it. These feedback blocks provide string of bits to feed the encryption algorithm which act as the key-stream generator as in case of CFB mode.

The key stream generated is XOR-ed with the plaintext blocks. The OFB mode requires an IV as the initial random n-bit input block. The IV need not be secret.

The operation is depicted in the following illustration –



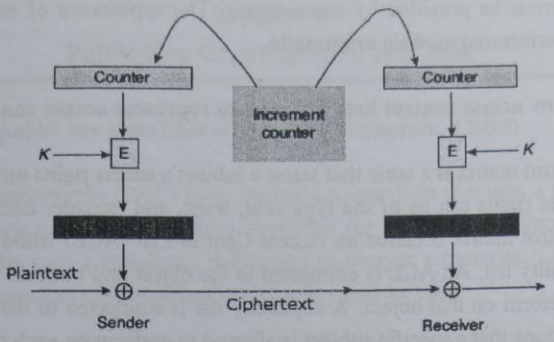
Counter (CTR) Mode

It can be considered as a counter-based version of CFB mode without the feedback. In this mode, both the sender and receiver need to access to a reliable counter, which computes a new shared value each time a ciphertext block is exchanged. This shared counter is not necessarily a secret value, but challenge is that both sides must keep the counter synchronized.

Operation

Both encryption and decryption in CTR mode are depicted in the following illustration. Steps in operation are –

- Load the initial counter value in the top register is the same for both the sender and the receiver. It plays the same role as the IV in CFB (and CBC) mode.
- Encrypt the contents of the counter with the key and place the result in the bottom register.
- Take the first plaintext block P1 and XOR this to the contents of the bottom register. The result of this is C1. Send C1 to the receiver and update the counter. The counter update replaces the ciphertext feedback in CFB mode.
- Continue in this manner until the last plaintext block has been encrypted.
- The decryption is the reverse process. The ciphertext block is XORed with the output of encrypted contents of counter value. After decryption of each ciphertext block counter is updated as in case of encryption.



3. **why do some block cipher modes of operation only use encryption while others use both encryption and decryption. (2011,2014)**

In some modes, the plaintext does not pass through the encryption functions, but is XORed with the output of the encryption function. The math works out that for decryption in these cases, the encryption function must also be used.

4. **what is a pseudorandom generator? Give an example describing how it works?(2013)**

Pseudo Random Number Generator(PRNG) refers to an algorithm that uses mathematical formulas to produce sequences of random numbers. PRNGs generate a sequence of numbers approximating the properties of random numbers.

A PRNG starts from an arbitrary starting state using a **seed state**. Many numbers are generated in a short time and can also be reproduced later, if the starting point in the sequence is known. Hence, the numbers are **deterministic and efficient**.

Linear Congruential Generator is most common and oldest algorithm for generating pseudo-randomized numbers. The generator is defined by the recurrence relation:

$\mathbf{X_{n+1} = (aX_n + c) \bmod c}$

where X is the sequence of pseudo-random values

m, $0 <$ m- modulus

a, $0 <$ a $<$m- multiplier

c, $0 <= c <$m- increment

x_0, $0 <= x_0 <$m- the seed or start value

We generate the next random integer using the previous random integer, the integer constants, and the integer modulus. To get started, the algorithm requires an initial

Seed, which must be provided by some means. The appearance of randomness is provided by performing **modulo arithmetic.**.

5. **explain how access control lists are used to represent access control matrix. (2013)**

An access control matrix is a table that states a subject's access rights on an object. A subject's access rights can be of the type read, write, and execute. Each column of the access control matrix is called an Access Control List (ACL) while each row is called a capability list. An ACL is connected to the object and outlines actions each subject can perform on that object. A capability list is connected to the subject and outlines the actions that a specific subject is allowed to perform on each object.

6. **what is the difference between a block cipher and a stream cipher? (2011,2014)**
   or, make a comparison between is stream ciphers and block cipher with example. (2013)

Comparison Chart

STREAM CIPHER	BLOCK CIPHER
In stream cipher keys and algorithms are applied to each binary digit in a tiara stream, one bit at a time, rather dun mcrypting block of data.	Block cipher is main method of encrypting text in which keys and algorithm are applied to block of data rather that individual bits like stream cipher.
Stream cipher is less time consuming.	Block cipher is more time consuming.
Because of a bit encrypting at a time. stream cipher is faster than block cipher.	As block of data is encrypting at a time block cipher is slower than stream cipher.
Stream Cipher doesn't used in chaining modes of operation.	Block Cipher used in chaining modes of operation.
Hardware implementation is easy using stream cipher.	Software implementation is easy using block cipher.
One Time Pad is the best example of stream Cipher	Data Encryption Standard (DES) is the best example of block cipher.
Requires less code.	Requires more code.
Application: SSL	Application: Database, file encryption.

Chapter 9
Public-Key Cryptography and RSA

1. describe public key algorithm with required diagram. (2015)

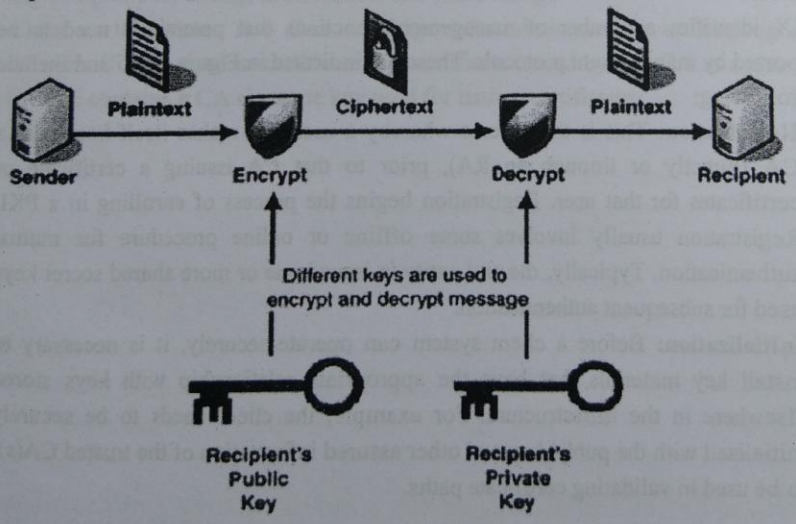
answer:

Public key cryptography (PKC) is an encryption technique that uses a paired public and private key (or asymmetric key) algorithm for secure data communication. A message sender uses a recipient's public key to encrypt a message. To decrypt the sender's message, only the recipient's private key may be used.

Symmetric cryptography was well suited for organizations such as governments, military, and big financial corporations were involved in the classified communication.

With the spread of more unsecure computer networks in last few decades, a genuine need was felt to use cryptography at larger scale. The symmetric key was found to be non-practical due to challenges it faced for key management. This gave rise to the public key cryptosystems.

The process of encryption and decryption is depicted in the following illustration –



The most important properties of public key encryption scheme are –

- Different keys are used for encryption and decryption. This is a property which set this scheme different than symmetric encryption scheme.
- Each receiver possesses a unique decryption key, generally referred to as his private key.
- Receiver needs to publish an encryption key, referred to as his public key.
- Some assurance of the authenticity of a public key is needed in this scheme to avoid spoofing by adversary as the receiver. Generally, this type of cryptosystem involves trusted third party which certifies that a particular public key belongs to a specific person or entity only.
- Encryption algorithm is complex enough to prohibit attacker from deducing the plaintext from the ciphertext and the encryption (public) key.
- Though private and public keys are related mathematically, it is not be feasible to calculate the private key from the public key. In fact, intelligent part of any public-key cryptosystem is in designing a relationship between two keys.

2. what functions should be provided by a public key infrastructure (PKI)? Is it possible to operate such an encryption technique without a PKI? (2013)

Answer:

PKIX identifies a number of management functions that potentially need to be supported by management protocols. These are indicated in Figure 14.16 and include the following:

- ✓ **Registration:** This is the process whereby a user first makes itself known to a CA (directly or through an RA), prior to that CA issuing a certificate or certificates for that user. Registration begins the process of enrolling in a PKI. Registration usually involves some offline or online procedure for mutual authentication. Typically, the end entity is issued one or more shared secret keys used for subsequent authentication.
- ✓ **Initialization:** Before a client system can operate securely, it is necessary to install key materials that have the appropriate relationship with keys stored elsewhere in the infrastructure. For example, the client needs to be securely initialized with the public key and other assured information of the trusted CA(s), to be used in validating certificate paths.

- ✓ **Certification:** This is the process in which a CA issues a certificate for a user's public key, returns that certificate to the user's client system, and/or posts that certificate in a repository.
- ✓ **Key pair recovery:** Key pairs can be used to support digital signature creation and verification, encryption and decryption, or both. When a key pair is used for encryption/decryption, it is important to provide a mechanism to recover the necessary decryption keys when normal access to the keying material is no longer possible, otherwise it will not be possible to recover the encrypted data. Loss of access to the decryption key can result from forgotten passwords/PINs, corrupted disk drives, damage to hardware tokens, and so on.Key pair recovery allows end entities to restore their encryption/decryption key pair from an authorized key backup facility (typically, the CA that issued the end entity's certificate).
- ✓ **Key pair update:** All key pairs need to be updated regularly (i.e., replaced with a new key pair) and new certificates issued. Update is required when the certificate lifetime expires and as a result of certificate revocation.
- ✓ **Revocation request:** An authorized person advises a CA of an abnormal situation requiring certificate revocation. Reasons for revocation include private key compromise, change in affiliation, and name change.
- ✓ **Cross certification:** Two CAs exchange information used in establishing a cross-certificate. A cross-certificate is a certificate issued by one CA to another CA that contains a CA signature key used for issuing certificates.

3. Explain the RSA algorithm and its security mechanisms. (2014)

Answer:

This cryptosystem is one the initial system. It remains most employed cryptosystem even today. The system was invented by three scholars **Ron Rivest, Adi Shamir,** and **Len Adleman** and hence, it is termed as RSA cryptosystem.

We will see two aspects of the RSA cryptosystem, firstly generation of key pair and secondly encryption-decryption algorithms.

Generation of RSA Key Pair

Each person or a party who desires to participate in communication using encryption needs to generate a pair of keys, namely public key and private key. The process followed in the generation of keys is described below –

- **Generate the RSA modulus (n)**
  - Select two large primes, p and q.
  - Calculate n=p*q. For strong unbreakable encryption, let n be a large number, typically a minimum of 512 bits.
- **Find Derived Number (e)**
  - Number **e** must be greater than 1 and less than $(p - 1)(q - 1)$.
  - There must be no common factor for e and $(p - 1)(q - 1)$ except for 1. In other words two numbers e and $(p - 1)(q - 1)$ are coprime.
- **Form the public key**
  - The pair of numbers (n, e) form the RSA public key and is made public.
  - Interestingly, though n is part of the public key, difficulty in factorizing a large prime number ensures that attacker cannot find in finite time the two primes (p & q) used to obtain n. This is strength of RSA.
- **Generate the private key**
  - Private Key d is calculated from p, q, and e. For given n and e, there is unique number d.
  - Number d is the inverse of e modulo $(p - 1)(q - 1)$. This means that d is the number less than $(p - 1)(q - 1)$ such that when multiplied by e, it is equal to 1 modulo $(p - 1)(q - 1)$.
  - This relationship is written mathematically as follows –

$$ed = 1 \bmod (p - 1)(q - 1)$$

The Extended Euclidean Algorithm takes p, q, and e as input and gives d as output.

Example

An example of generating RSA Key pair is given below. (For ease of understanding, the primes p & q taken here are small values. Practically, these values are very high).

- Let two primes be p = 7 and q = 13. Thus, modulus n = pq = 7 x 13 = 91.
- Select e = 5, which is a valid choice since there is no number that is common factor of 5 and (p − 1)(q − 1) = 6 × 12 = 72, except for 1.
- The pair of numbers (n, e) = (91, 5) forms the public key and can be made available to anyone whom we wish to be able to send us encrypted messages.
- Input p = 7, q = 13, and e = 5 to the Extended Euclidean Algorithm. The output will be d = 29.
- Check that the d calculated is correct by computing −

$$de = 29 \times 5 = 145 = 1 \bmod 72$$

- Hence, public key is (91, 5) and private keys is (91, 29).

Encryption and Decryption

Once the key pair has been generated, the process of encryption and decryption are relatively straightforward and computationally easy.

Interestingly, RSA does not directly operate on strings of bits as in case of symmetric key encryption. It operates on numbers modulo n. Hence, it is necessary to represent the plaintext as a series of numbers less than n.

RSA Encryption

- Suppose the sender wish to send some text message to someone whose public key is (n, e).
- The sender then represents the plaintext as a series of numbers less than n.
- To encrypt the first plaintext P, which is a number modulo n. The encryption process is simple mathematical step as −

$$C = P^e \bmod n$$

- In other words, the ciphertext C is equal to the plaintext P multiplied by itself e times and then reduced modulo n. This means that C is also a number less than n.
- Returning to our Key Generation example with plaintext P = 10, we get ciphertext C −

$$C = 10^5 \bmod 91$$

RSA Decryption

- The decryption process for RSA is also very straightforward. Suppose that the receiver of public-key pair (n, e) has received a ciphertext C.
- Receiver raises C to the power of his private key d. The result modulo n will be the plaintext P.

Plaintext = C^d mod n

- Returning again to our numerical example, the ciphertext C = 82 would get decrypted to number 10 using private key 29 –

Plaintext = 82^{29} mod 91 = 10

4. explain public key cryptography for encryption and authentication. (2013) or, briefly explain public key cryptosystem and authentication. (2010)

Answer:

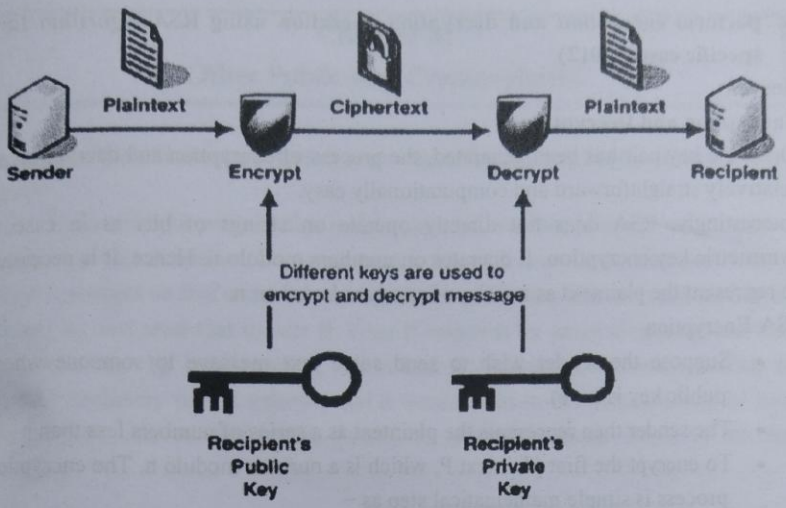
Public Key Cryptography

Unlike symmetric key cryptography, we do not find historical use of public-key cryptography. It is a relatively new concept.

Symmetric cryptography was well suited for organizations such as governments, military, and big financial corporations were involved in the classified communication.

With the spread of more unsecure computer networks in last few decades, a genuine need was felt to use cryptography at larger scale. The symmetric key was found to be non-practical due to challenges it faced for key management. This gave rise to the public key cryptosystems.

The process of encryption and decryption is depicted in the following illustration –



The most important properties of public key encryption scheme are –

- ✓ Different keys are used for encryption and decryption. This is a property which set this scheme different than symmetric encryption scheme.
- ✓ Each receiver possesses a unique decryption key, generally referred to as his private key.
- ✓ Receiver needs to publish an encryption key, referred to as his public key.
- ✓ Some assurance of the authenticity of a public key is needed in this scheme to avoid spoofing by adversary as the receiver. Generally, this type of cryptosystem involves trusted third party which certifies that a particular public key belongs to a specific person or entity only.
- ✓ Encryption algorithm is complex enough to prohibit attacker from deducing the plaintext from the ciphertext and the encryption (public) key.
- ✓ Though private and public keys are related mathematically, it is not be feasible to calculate the private key from the public key. In fact, intelligent part of any public-key cryptosystem is in designing a relationship between two keys.

5. perform encryption and decryption operation using RSA algorithm for a specific case. (2012)

Answer:

Encryption and Decryption

Once the key pair has been generated, the process of encryption and decryption are relatively straightforward and computationally easy.

Interestingly, RSA does not directly operate on strings of bits as in case of symmetric key encryption. It operates on numbers modulo n. Hence, it is necessary to represent the plaintext as a series of numbers less than n.

RSA Encryption

- Suppose the sender wish to send some text message to someone whose public key is (n, e).
- The sender then represents the plaintext as a series of numbers less than n.
- To encrypt the first plaintext P, which is a number modulo n. The encryption process is simple mathematical step as –

$$C = P^e \bmod n$$

- In other words, the ciphertext C is equal to the plaintext P multiplied by itself e times and then reduced modulo n. This means that C is also a number less than n.
- Returning to our Key Generation example with plaintext P = 10, we get ciphertext C –

$$C = 10^5 \bmod 91$$

RSA Decryption

- The decryption process for RSA is also very straightforward. Suppose that the receiver of public-key pair (n, e) has received a ciphertext C.
- Receiver raises C to the power of his private key d. The result modulo n will be the plaintext P.

$$\text{Plaintext} = C^d \bmod n$$

- Returning again to our numerical example, the ciphertext C = 82 would get decrypted to number 10 using private key 29 –

$$\text{Plaintext} = 82^{29} \bmod 91 = 10$$

Chapter 10
Other Public-Key Cryptosystems

1. explain Diffic Hellman key exchange algorithm. (2010,2014,2015)

Answer:

Figure shows a simple protocol that makes use of the Diffie-Hellman calculation. Suppose that user A wishes to set up a connection with user B and use a secret key to encrypt messages on that connection. User A can generate a one-time private key X_A, calculate Y_A, and send that to user B. User B responds by generating a private value X_B, calculating Y_B, and sending Y_B to user A. Both users can now calculate the key. The necessary public values q and α would need to be known ahead of time. Alternatively, user A could pick values for q and α include those in the first message.

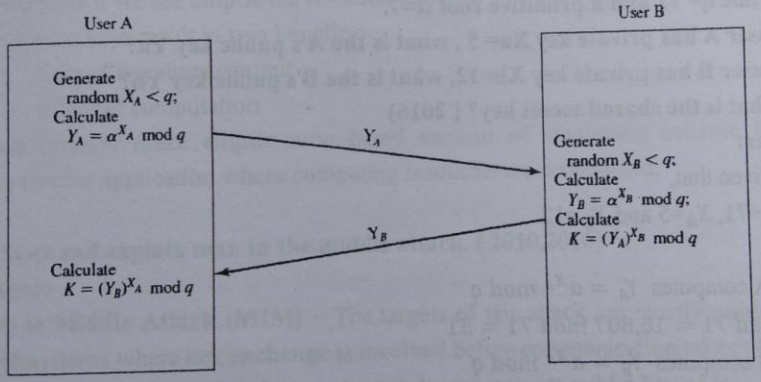


Figure : Diffie-Hellman Key Exchange

2. user A and B exchange the key using Diffie Hellman algorithm.Assume α =5, q=11, X_A =2 and X_B =3. Find the value of Ya,Yb and K. (2011,2013,2014)

Answer:

Here given that,

α=5, q=11, X_A=2 and X_B=3

Now, A computes $Y_A = \alpha^{X_A} \bmod q$

$= 5^2 \ mod \ 11 = 3$

Now, B computes $Y_B = \alpha^{X_B} \ mod \ q$

$= 5^3 \ mod \ 11 = 4$

After they exchange public keys, each can compute the common secret key:

A computes $K=(Y_B)^{X_A} \ mod \ q$

$= 4^2 \ mod \ 11 = 5$

B computes $K=(Y_A)^{X_B} \ mod \ q$

$= 3^3 \ mod \ 11 = 5$

the value of $Y_A = 3, Y_B = 4$ and $K = 5$

3. users A and B use the DP Hellman key exchange technique with a common prime q= 71 and a primitive root α=7.

(i) if user A has private key Xa= 5 , what is the A's public key Ya?

(ii) if user B has private key Xb=12, what is the B's public key Yb?

(iii) what is the shared secret key? (2016)

Answer:

Here given that,

α=7, q=71, X_A=5 and X_B=12

Now, A computes $Y_A = \alpha^{X_A} \ mod \ q$

$= 7^5 \ mod \ 71 = 16{,}807 \ mod \ 71 = 51$

Now, B computes $Y_B = \alpha^{X_B} \ mod \ q$

$= 7^{12} \ mod \ 71 = 4$

After they exchange public keys, each can compute the common secret key:

A computes $K=(Y_B)^{X_A} \ mod \ q$

$= 4^5 \ mod \ 71 = 30$

B computes $K=(Y_A)^{X_B} \ mod \ q$

$= 51^{12} \ mod \ 71 = (51^4 \ mod \ 71 * \ 51^4 \ mod \ 71 * \ 51^4 \ mod \ 71) mod \ 71$

$= 111 \ mod \ 71 = 30$

So the screate key is 30.

5. define an elliptic curve. With example discuss ECC over prime field. (2013)

Answer:

Elliptic Curve Cryptography (ECC)

Elliptic Curve Cryptography (ECC) is a term used to describe a suite of cryptographic tools and protocols whose security is based on special versions of the discrete logarithm problem. It does not use numbers modulo p.

ECC is based on sets of numbers that are associated with mathematical objects called elliptic curves. There are rules for adding and computing multiples of these numbers, just as there are for numbers modulo p.

ECC includes a variants of many cryptographic schemes that were initially designed for modular numbers such as ElGamal encryption and Digital Signature Algorithm.

It is believed that the discrete logarithm problem is much harder when applied to points on an elliptic curve. This prompts switching from numbers modulo p to points on an elliptic curve. Also an equivalent security level can be obtained with shorter keys if we use elliptic curve-based variants.

The shorter keys result in two benefits –

- Ease of key management
- Efficient computation

These benefits make elliptic-curve-based variants of encryption scheme highly attractive for application where computing resources are constrained.

6. State and explain man in the middle attack. (2010,2016)

Answer:

Man in Middle Attack (MIM) – The targets of this attack are mostly public key cryptosystems where key exchange is involved before communication takes place.

- ✓ Host A wants to communicate to host B, hence requests public key of B.
- ✓ An attacker intercepts this request and sends his public key instead.
- ✓ Thus, whatever host A sends to host B, the attacker is able to read.
- ✓ In order to maintain communication, the attacker re-encrypts the data after reading with his public key and sends to B.
- ✓ The attacker sends his public key as A's public key so that B takes it as if it is taking it from A.

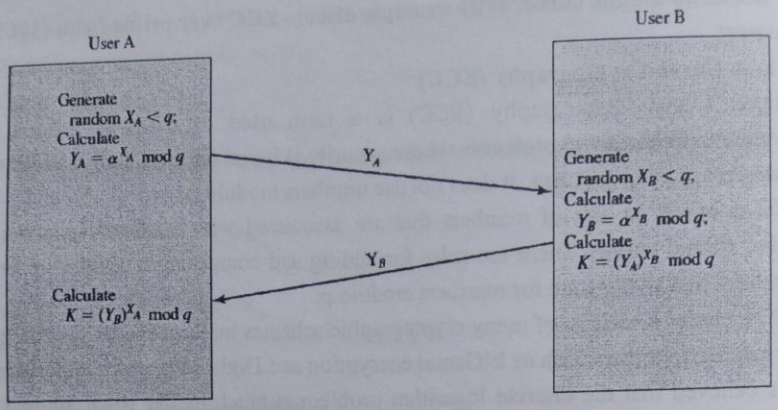


Figure: MAN IN MIDDLE

differentiate the following item: (2014)

(i) link and end to end encryption;

Link encryption encrypts all the data along a specific communication path, as in a satellite link, T3 line, or telephone circuit. Not only is the user information encrypted, but the header, trailers, addresses, and routing data that are part of the packets are also encrypted. The only traffic not encrypted in this technology is the data link control messaging information, which includes instructions and parameters that the different link devices use to synchronize communication methods. Link encryption provides protection against packet sniffers and eavesdroppers. In **end-to-end encryption,** the headers, addresses, routing, and trailer information are not encrypted, enabling attackers to learn more about a captured packet and where it is headed.

Chapter 11
Cryptographic Hash Functions

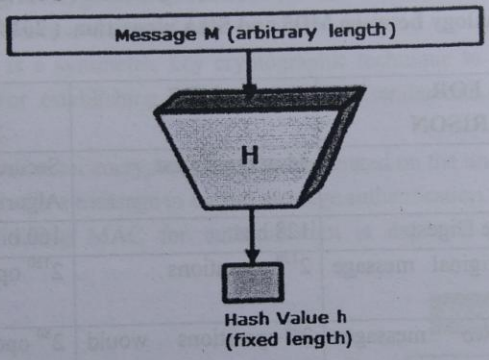
1. what is hash function? Explain the SHA-512 logic algorithm. (2016)

answer:

Hash functions are extremely useful and appear in almost all information security applications.

A hash function is a mathematical function that converts a numerical input value into another compressed numerical value. The input to the hash function is of arbitrary length but output is always of fixed length.

Values returned by a hash function are called **message digest** or simply **hash values**. The following picture illustrated hash function –



Secure Hash Function (SHA)

Family of SHA comprise of four SHA algorithms; SHA-0, SHA-1, SHA-2, and SHA-3. Though from same family, there are structurally different.

- The original version is SHA-0, a 160-bit hash function, was published by the National Institute of Standards and Technology (NIST) in 1993. It had few weaknesses and did not become very popular. Later in 1995, SHA-1 was designed to correct alleged weaknesses of SHA-0.
- SHA-1 is the most widely used of the existing SHA hash functions. It is employed in several widely used applications and protocols including Secure Socket Layer (SSL) security.

- In 2005, a method was found for uncovering collisions for SHA-1 within practical time frame making long-term employability of SHA-1 doubtful.
- SHA-2 family has four further SHA variants, SHA-224, SHA-256, SHA-384, and SHA-512 depending up on number of bits in their hash value. No successful attacks have yet been reported on SHA-2 hash function.
- Though SHA-2 is a strong hash function. Though significantly different, its basic design is still follows design of SHA-1. Hence, NIST called for new competitive hash function designs.
- In October 2012, the NIST chose the Keccak algorithm as the new SHA-3 standard. Keccak offers many benefits, such as efficient performance and good resistance for attacks.

2. make comparison between MD5 and SHA algorithm. (2011,2012)
or, draw an analogy between MD5 and SHA algorithm. (2014)

answer:

BASIS FOR COMPARISON	MD5	SHA1
Stands for	Message Digest	Secure Hash Algorithm
Length of Message Digest	128 bits	160 bits
Discerning of original message would require	2^{128} operations	2^{160} operations
For finding two messages generating the same message digest	2^{64} operations would be needed	2^{80} operations are required
Security	Poor	Moderate
Speed	Fast	Slow

3. define institution and the methods used for intrusion detection. (2011)

answer:

An intrusion detection system (IDS) is a system that monitors network traffic for suspicious activity and issues alerts when such activity is discovered. While anomaly detection and reporting is the primary function, some intrusion detection systems are capable of taking actions when malicious activity or anomalous traffic is detected, including blocking traffic sent from suspicious IP addresses.

Although intrusion detection systems monitor networks for potentially malicious activity, they are also prone to false alarms (false positives). Consequently, organizations need to fine-tune their IDS products when they first install them. That means properly configuring their intrusion detection systems to recognize what normal traffic on their network looks like compared to potentially malicious activity.

4. what is message authentication?(2011,2012,2016)

Message authentication ensures that the message has been sent by a genuine identity and not by an imposter.

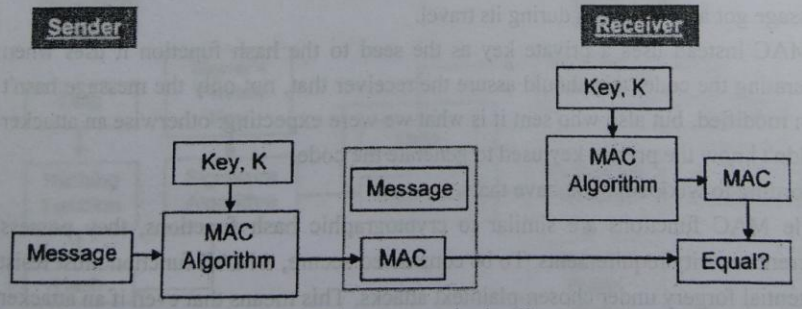
5. define Mac. How message authentication is performed? (2013)
or, what is message authentication code? What are some approaches to producing message authentication? (2015)

Message Authentication Code (MAC)

MAC algorithm is a symmetric key cryptographic technique to provide message authentication. For establishing MAC process, the sender and receiver share a symmetric key K.

Essentially, a MAC is an encrypted checksum generated on the underlying message that is sent along with a message to ensure message authentication.

The process of using MAC for authentication is depicted in the following illustration –



Let us now try to understand the entire process in detail –

- ✓ The sender uses some publicly known MAC algorithm, inputs the message and the secret key K and produces a MAC value.
- ✓ Similar to hash, MAC function also compresses an arbitrary long input into a fixed length output. The major difference between hash and MAC is that MAC uses secret key during the compression.

- ✓ The sender forwards the message along with the MAC. Here, we assume that the message is sent in the clear, as we are concerned of providing message origin authentication, not confidentiality. If confidentiality is required then the message needs encryption.
- ✓ On receipt of the message and the MAC, the receiver feeds the received message and the shared secret key K into the MAC algorithm and re-computes the MAC value.
- ✓ The receiver now checks equality of freshly computed MAC with the MAC received from the sender. If they match, then the receiver accepts the message and assures himself that the message has been sent by the intended sender.
- ✓ If the computed MAC does not match the MAC sent by the sender, the receiver cannot determine whether it is the message that has been altered or it is the origin that has been falsified. As a bottom-line, a receiver safely assumes that the message is not the genuine.

6. differentiate Mac and hash function. What is the role of compression function in hash function? (2012)

The main difference is conceptual: while **hashes** are used to guarantee the integrity of data, a **MAC** guarantees integrity AND authentication.

This means that a hash code is blindly generated from the message without any kind of external input: what you obtain is something that can be used to check if the message got any alteration during its travel.

A MAC instead uses a private key as the seed to the hash function it uses when generating the code: this should assure the receiver that, not only the message hasn't been modified, but also who sent it is what we were expecting: otherwise an attacker couldn't know the private key used to generate the code.

According to wikipedia you have that:

While MAC functions are similar to cryptographic hash functions, they possess different security requirements. To be considered secure, a MAC function must resist existential forgery under chosen-plaintext attacks. This means that even if an attacker has access to an oracle which possesses the secret key and generates MACs for messages of the attacker's choosing, the attacker cannot guess the MAC for other messages without performing infeasible amounts of computation.

Chapter 13
Digital Signatures

1. what is digital signature?(2012,2011,2014, 2015)

answer:

Digital signatures are the public-key primitives of message authentication. In the physical world, it is common to use handwritten signatures on handwritten or typed messages. They are used to bind signatory to the message.

Similarly, a digital signature is a technique that binds a person/entity to the digital data. This binding can be independently verified by receiver as well as any third party.

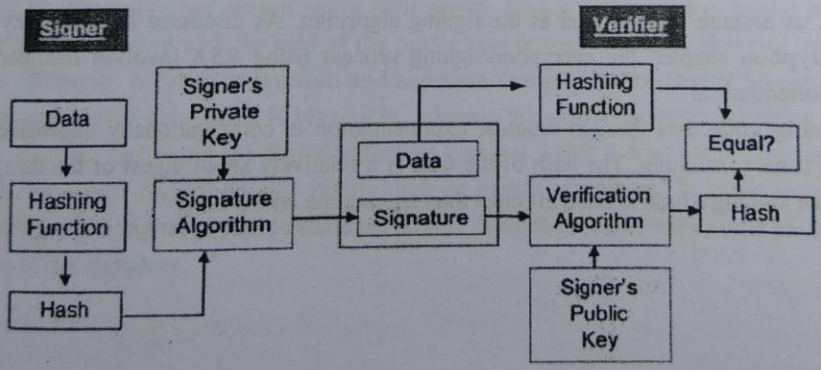
Digital signature is a cryptographic value that is calculated from the data and a secret key known only by the signer.

2. Describe digital signature with block diagram. (2015)

Answer:

Model of Digital Signature

As mentioned earlier, the digital signature scheme is based on public key cryptography. The model of digital signature scheme is depicted in the following illustration –



The following points explain the entire process in detail –

- ✓ Each person adopting this scheme has a public-private key pair.
- ✓ Generally, the key pairs used for encryption/decryption and signing/verifying are different. The private key used for signing is referred to as the signature key and the public key as the verification key.
- ✓ Signer feeds data to the hash function and generates hash of data.
- ✓ Hash value and signature key are then fed to the signature algorithm which produces the digital signature on given hash. Signature is appended to the data and then both are sent to the verifier.
- ✓ Verifier feeds the digital signature and the verification key into the verification algorithm. The verification algorithm gives some value as output.
- ✓ Verifier also runs same hash function on received data to generate hash value.
- ✓ For verification, this hash value and output of verification algorithm are compared. Based on the comparison result, verifier decides whether the digital signature is valid.
- ✓ Since digital signature is created by 'private' key of signer and no one else can have this key; the signer cannot repudiate signing the data in future.

It should be noticed that instead of signing data directly by signing algorithm, usually a hash of data is created. Since the hash of data is a unique representation of data, it is sufficient to sign the hash in place of data. The most important reason of using hash instead of data directly for signing is efficiency of the scheme.

Let us assume RSA is used as the signing algorithm. As discussed in public key encryption chapter, the encryption/signing process using RSA involves modular exponentiation.

Signing large data through modular exponentiation is computationally expensive and time consuming. The hash of the data is a relatively small digest of the data, hence signing a hash is more efficient than signing the entire data.

3. state the requirements for a digital signature? (2010)
or, what requirements should a digital signature scheme satisfy? (2012)

answer Four Common Digital Signature Requirements

a) The Digital Signature must be unique to the person using it
b) The Digital Signature must be capable of verification
c) The Digital Signature must be under the sole control of the person using it
d) The Digital Signature must be linked to data in such a manner that if the data is changed, the Digital Signature is invalidated

4. Describe about the digital signature standard (DSS). (2011)

Answer:

The Digital Signature Standard is intended to be used in electronic funds transfer, software distribution, electronic mail, data storage and applications which require high data integrity assurance. The Digital Signature Standard can be implemented in software, hardware or firmware.

The algorithm used behind the Digital Signature Standard is known as the Digital Signature Algorithm. The algorithm makes use of two large numbers which are calculated based on a unique algorithm which also considers parameters that determine the authenticity of the signature. This indirectly also helps in verifying the integrity of the data attached to the signature. The digital signatures can be generated only by the authorized person using their private keys and the users or public can verify the signature with the help of the public keys provided to them. However, one key difference between encryption and signature operation in the Digital Signature Standard is that encryption is reversible, whereas the digital signature operation is not. Another fact about the digital signature standard is that it does not provide any capability with regards to key distribution or exchange of keys. In other words, security of the digital signature standard largely depends on the secrecy of the private keys of the signatory.

5. write down digital signature algorithm. (2016)

DSA is a United States Federal Government standard for digital signatures. It was proposed by the National Institute of Standards and Technology (NIST) in August 1991 for use in their Digital Signature Standard (DSS), specified in FIPS 186 in 1993.

The first part of the DSA algorithm is the public key and private key generation, which can be described as:

- ✓ Choose a prime number q, which is called the prime divisor.
- ✓ Choose another primer number p, such that p-1 mod q = 0. p is called the prime modulus.
- ✓ Choose an integer g, such that 1 < g < p, g**q mod p = 1 and g = h**((p–1)/q) mod p. q is also called g's multiplicative order modulo p.
- ✓ Choose an integer, such that 0 < x < q.
- ✓ Compute y as g**x mod p.
- ✓ Package the public key as {p,q,g,y}.
- ✓ Package the private key as {p,q,g,x}.

The second part of the DSA algorithm is the signature generation and signature verification, which can be described as:

To generate a message signature, the sender can follow these steps:

- Generate the message digest h, using a hash algorithm like SHA1.
- Generate a random number k, such that 0 < k < q.
- Compute r as (g**k mod p) mod q. If r = 0, select a different k.
- Compute i, such that k*i mod q = 1. i is called the modular multiplicative inverse of k modulo q.
- Compute s = i*(h+r*x) mod q. If s = 0, select a different k.
- Package the digital signature as {r,s}.

To verify a message signature, the receiver of the message and the digital signature can follow these steps:

- Generate the message digest h, using the same hash algorithm.
- Compute w, such that s*w mod q = 1. w is called the modular multiplicative inverse of s modulo q.
- Compute u1 = h*w mod q.
- Compute u2 = r*w mod q.
- Compute v = (((g**u1)*(y**u2)) mod p) mod q.
- If v == r, the digital signature is valid.

6. distinguish between direct and arbitrage digital signature. (2012)

answer:

The Direct Digital Signature

Understanding a direct digital signature begins by recognizing there are only two parties involved in the passing of the signed information: the sender and the receiver. Direct digital signatures only require these two entities because the receiver of the data (digital signature) knows the public key used by the sender. And the sender of the signature trusts the receiver not to alter the document in any way.

The Arbitrated Digital Signature

Implementing an arbitrated digital signature invites a third party into the process called a "trusted arbiter." The role of the trusted arbiter is usually twofold: first this independent third party verifies the integrity of the signed message or data. Second, the trusted arbiter dates, or time-stamps, the document, verifying receipt and the passing on of the signed document to its intended final destination.

7. what are the typical contents of X.509 certificate format? State the purpose of different fields of certificate revocation list (CRL). What is Delta revocation? (2012,2014)

Structure of X509 Certificates

Subject. Provides the name of the computer, user, network device, or service that the CA issues the certificate to. The subject name is commonly represented by using an X.500 or Lightweight Directory Access Protocol (LDAP) format.

Serial Number. Provides a unique identifier for each certificate that a CA issues.

Issuer. Provides a distinguished name for the CA that issued the certificate. The issuer name is commonly represented by using an X.500 or LDAP format. For a root CA, the Issuer and Subject are identical. For all other CA certificates and for end entity certificates, the Subject and Issuer will be different.

Valid From. Provides the date and time when the certificate becomes valid.

Valid To. Provides the date and time when the certificate is no longer considered valid.

Public Key. Contains the public key of the key pair that is associated with the certificate.

In addition to the fields defined in X.509 version 1, X.509 version 3 certificates include optional fields or extensions that provide additional functionality and

features to the certificate. These extensions are not necessarily included in each certificate that a CA issues:

Subject alternative name. A subject can be presented in many different formats. For example, if the certificate must include a user's account name in the format of an LDAP distinguished name, e-mail name, and a user principal name (UPN), you can include the e-mail name or UPN in a certificate by adding a subject alternative name extension that includes these additional name formats. Subject alternative name is only used in end entity certificates, not in CA certificates.

Basic constraints. This X509 version 3 extension is used to distinguish between end-entity certificates and CA certificates. There are still some PKI clients today that do not recognize basic constraints, which can make it possible for an end-entity to act as a CA. Windows Server 2003 and Windows 2000 operating systems honor basic constraints in accordance with Internet Engineering Task Force (IETF) Request for Comments (RFC) 2459 and will reject CA certificates that do not contain this extension.

Name constraints. This extension restricts the namespaces that are permitted or excluded by a qualified subordinate CA and its subordinates when issuing certificates.

Policies. Defines the list of acceptable issuance and application policies for certificate usage. These policies are identified in the certificate by object identifiers (also known as OIDs).

Policy mapping. Allows a policy from one domain to be mapped onto a policy of another domain.

Policy constraints. Restricts the subordination levels in a certificate hierarchy to which a policy is applied. These extensions are used in conjunction with issuance and application policies only.

Application policy. Defines which applications can be used in conjunction with certain certificates.

Application policy mapping. Identifies equivalence between the application policies of two organizations that cross certify by using certificate application policies.

Cross certificate distribution points. Identifies where cross certificates related to a particular certificate can be obtained and how often the cross certificates at that location are updated.

CRL distribution points (CDP). Provides one or more URLs where the application or service can retrieve a certificate revocation list (CRL) from. Used when an application or service must determine whether a certificate has been revoked before its validity period has expired.

Authority Information Access (AIA). Provides one or more URLs from where an application or service can retrieve the issuing CA certificate. Used to validate the certificate of the CA that issued the certificate also referred to as the parent CA for revocation and validity.

Enhanced Key Usage (EKU). Defines which applications can be used in conjunction with certain certificates. Because some implementations of public key infrastructure (PKI) applications might not understand application policies, both application policies and enhanced key usage sections appear in certificates issued by a Microsoft CA.

8. what is meant by certificate revocation? When does it occurs when a certificate is revoked, who is responsible for the revocation? (2013)

answer:

A Certificate Revocation List (CRL) is a list of digital certificates that have been revoked by the issuing Certificate Authority (CA) before their scheduled expiration date and should no longer be trusted. CRLs are a type of blacklist and are used by various endpoints, including Web browsers, to verify whether a certificate is valid and trustworthy. Digital certificates are used in the encryption process to secure communications, most often by using the TLS/SSLprotocol. The certificate, which is signed by the issuing Certificate Authority, also provides proof of the identity of the certificate owner.

9. what is the purpose of the X-509 standard? (2015)

answer:

X.509 defines a framework for the provision of authentication services by the X.500 directory to its users. The directory may serve as a repository of public-key certificates. Each certificate contains the public key of a user and is signed with the private key of a trusted certification authority. In addition, X.509 defines alternative authentication protocols based on the use of public-key certificates.

10. what are the key features of SET and SET participants? (2016)
or, what is the meaning of SET? Write about its feature. (2011)
answer:

Secure Electronic Transaction or SET is a system which ensures security and integrity of electronic transactions done using credit cards in a scenario. SET is not some system that enables payment but it is a security protocol applied on those payments. It uses different encryption and hashing techniques to secure payments over internet done through credit cards.

Participants in SET :

In the general scenario of online transaction, SET includes similar participants:

1. **Cardholder** – customer
2. **Issuer** – customer financial institution
3. **Merchant**
4. **Acquirer** – Merchant financial
5. **Certificate authority** – Authority which follows certain standards and issues certificates(like X.509V3) to all other participants.

SET functionalities :

- **Provide Authentication**
  - **Merchant Authentication** – To prevent theft, SET allows customers to check previous relationships between merchant and financial institution. Standard X.509V3 certificates are used for this verification.
  - **Customer / Cardholder Authentication** – SET checks if use of credit card is done by an authorized user or not using X.509V3 certificates.
- **Provide Message Confidentiality** : Confidentiality refers to preventing unintended people from reading the message being transferred. SET implements confidentiality by using encryption techniques. Traditionally DES is used for encryption purpose.
- **Provide Message Integrity** : SET doesn't allow message modification with the help of signatures. Messages are protected against unauthorized modification using RSA digital signatures with SHA-1 and some using HMAC with SHA-1,

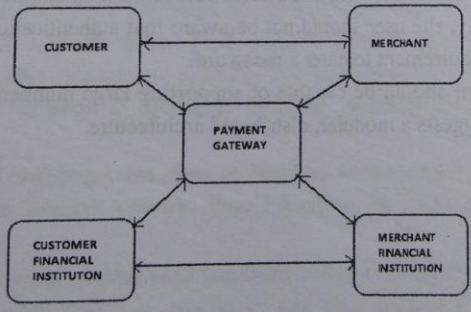
11. what is mean by SET? What are the steps involved in SET transaction? (2012)

answer:

Secure Electronic Transaction or SET is a system which ensures security and integrity of electronic transactions done using credit cards in a scenario. SET is not some system that enables payment but it is a security protocol applied on those payments. It uses different encryption and hashing techniques to secure payments over internet done through credit cards. SET protocol was supported in development by major organizations like Visa, Mastercard, Microsoft which provided its Secure Transaction Technology (STT) and NetScape which provided technology of Secure Socket Layer (SSL).

SET protocol restricts revealing of credit card details to merchants thus keeping hackers and thieves at bay. SET protocol includes Certification Authorities for making use of standard Digital Certificates like X.509 Certificate.

Before discussing SET further, let's see a general scenario of electronic transaction, which includes client, payment gateway, client financial institution, merchant and merchant financial institution.



12. what is kerberos? (2015)

Answer:

Kerberos authentication is currently the default authorization technology used by Microsoft Windows, and implementations of Kerberos exist in Apple OS, FreeBSD, UNIX, and Linux.

Microsoft introduced their version of Kerberos in Windows2000. It has also become a standard for websites and Single-Sign-On implementations across platforms. The Kerberos Consortium maintains Kerberos as an open-source project.

13. Explain the Characteristics of Kerberos.

Ans: Characteristics of Kerberos.

- ✓ **Secure:** A network eavesdropper should not be able to obtain the necessary information to impersonate a user. More generally, Kerberos should be strong enough that a potential opponent does not find it to be the weak link.
- ✓ **Reliable:** For all services that rely on Kerberos for access control, lack of availability of the Kerberos service means lack of availability of the supported services. Hence, Kerberos should be highly reliable and should employ a distributed server architecture, with one system able to back up another.
- ✓ **Transparent:** Ideally, the user should not be aware that authentication is taking place, beyond the requirement to enter a password.
- ✓ **Scalable:** The system should be capable of supporting large numbers of clients and servers. This suggests a modular, distributed architecture.

Chapter 22
Firewalls

1. what is a firewall and what are its limitations? Why corporate house implement more than one firewall for security? (2012)

answer:

A firewall is a device installed between the internet network of an organization and the rest of Internet. When a computer is connected to Internet, it can create many problems for corporate companies. Most companies put a large amount of confidential information online. Such an information should not be disclosed to the unauthorized persons. Second problem is that the virus, worms and other digital pests can breach the security and can destroy the valuable data.

Firewall Limitations

A firewall is a crucial component of securing your network and is designed to address the issues of data integrity or traffic authentication (via stateful packet inspection) and confidentiality of your internal network (via NAT). Your network gains these benefits from a firewall by receiving all transmitted traffic through the firewall. Your network gains these benefits from a firewall by receiving all transmitted traffic through the firewall. The importance of including a firewall in your security strategy is apparent; however, firewalls do have the following limitations:

- A firewall cannot prevent users or attackers with modems from dialing in to or out of the internal network, thus bypassing the firewall and its protection completely.
- Firewalls cannot enforce your password policy or prevent misuse of passwords. Your password policy is crucial in this area because it outlines acceptable conduct and sets the ramifications of noncompliance.
- Firewalls are ineffective against nontechnical security risks such as social engineering, as discussed in Chapter 1, "There Be Hackers Here."
- Firewalls cannot stop internal users from accessing websites with malicious code, making user education critical.
- Firewalls cannot protect you from poor decisions.
- Firewalls cannot protect you when your security policy is too lax.

2. what is firewall? What are the advantages of firewall? (2011,2016)

answer:

A firewall is a device installed between the internet network of an organization and the rest of Internet. When a computer is connected to Internet, it can create many problems for corporate companies. Most companies put a large amount of confidential information online. Such an information should not be disclosed to the unauthorized persons. Second problem is that the virus, worms and other digital pests can breach the security and can destroy the valuable data.

Advantages of using firewalls based on packet filtering

Low cost.

Packet filters make use of current network routers.

Makes Security Transparent to End-Users.

Easy to install.

Packet filters make use of current network routers. Therefore implementing a packet filter security system is typically less complicated than other network security solutions.

High speed

Packet filters are generally faster than other firewall technologies because they perform fewer evaluations.

3. define a worm .diagrammatically illustrate a digital immune system. (2011,2016)

worm

A computer worm is self-replicating malware that duplicates itself to spread to uninfected computers. Worms often use parts of an operating system that are automatic and invisible to the user. It is common for worms to be noticed only when their uncontrolled replication consumes system resources, slowing or halting other tasks.

digital immune system

i. The Digital Immune system is a comprehensive approach to virus protection developed by IBM. The motivation for this development has been the rising threat of Internet-based virus propagation.

ii. Traditionally the virus threat was characterized by the relatively slow spread of new viruses and new mutations. Antivirus software was typically updated on a monthly basis and this has been sufficient to control the problem.

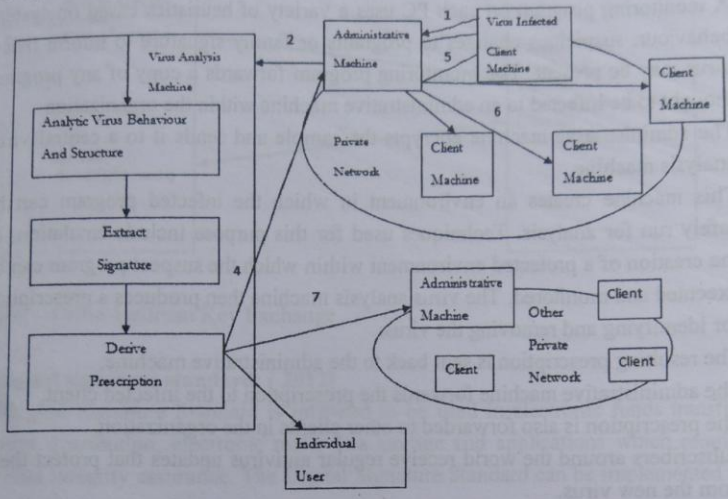


Figure 6.1 Digital Immune System Figure 6.1 Digital Immune System

iii. Also traditionally, the Internet played a comparatively small role in the spread of viruses. Two major trends in Internet technology had an increasing impact on the rate of virus propagation in recent years:

- **Integrated Mail Systems:** Systems such as Lotus Notes and Microsoft Outlook make it very simple to send anything to anyone and to work with objects that are received.
- **Mobile-Program Systems:** Capabilities such as Java and ActiveX allow programs to move on their own form one system to another.

iv. In response to threat posed by these Internet-based capabilities, IBM has developed a prototype digital immune system. The objective of this system is to provide rapid response time so that viruses can be stamped out almost as soon as they are introduced.

v. When a new virus enters an organization, the immune system automatically captures it, analyzes it, adds detection and shielding for it, removes it and passes

information about that virus to systems running IBM antivirus so that it can be detected before it is allowed to run elsewhere.

vi. The operation of digital immune system as follows:

- A monitoring program on each PC uses a variety of heuristics based on system behaviour, suspicious changes to programs or family signature to inform that a virus may be present. The monitoring program forwards a copy of any program thought to be infected to an administrative machine within the organization.
- The administrative machine encrypts the sample and sends it to a central virus analysis machine.
- This machine creates an environment in which the infected program can be safely run for analysis. Techniques used for this purpose include emulation, or the creation of a protected environment within which the suspect program can be executed and monitored. The virus analysis machine then produces a prescription for identifying and removing the virus.
- The resulting prescription is sent back to the administrative machine.
- The administrative machine forwards the prescription to the infected client.
- The prescription is also forwarded to other clients in the organization.
- Subscribers around the world receive regular antivirus updates that protect them from the new virus.

vii. The success of digital immune system depends on the ability of the virus analysis machine to detect new and innovative virus strains.

viii. By constantly analyzing and monitoring the viruses found in the wild, it should be possible to continuously update the Digital Immune System software to keep up with the threat.

6. Write short notes on the following

(a) key exchange of a diffie Hellman algorithm; (2012)

Figure shows a simple protocol that makes use of the Diffie-Hellman calculation. Suppose that user A wishes to set up a connection with user B and use a secret key to encrypt messages on that connection. User A can generate a one-time private key X_A, calculate Y_A, and send that to user B. User B responds by generating a private value X_B , calculating Y_B , and sending Y_B to user A. Both users can now calculate the key. The necessary public values q and α would need to be known ahead of time. Alternatively, user A could pick values for q and α include those in the first message.

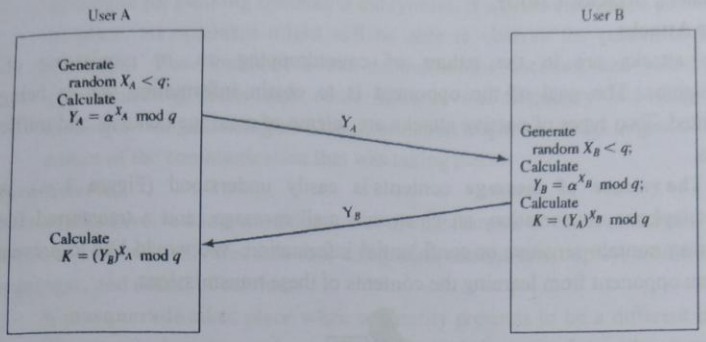


Figure : Diffie-Hellman Key Exchange

(c) digital signature standard; (2012)

The Digital Signature Standard is intended to be used in electronic funds transfer, software distribution, electronic mail, data storage and applications which require high data integrity assurance. The Digital Signature Standard can be implemented in software, hardware or firmware.

The algorithm used behind the Digital Signature Standard is known as the Digital Signature Algorithm. The algorithm makes use of two large numbers which are calculated based on a unique algorithm which also considers parameters that determine the authenticity of the signature. This indirectly also helps in verifying the integrity of the data attached to the signature. The digital signatures can be generated only by the authorized person using their private keys and the users or public can verify the signature with the help of the public keys provided to them. However, one key difference between encryption and signature operation in the Digital Signature Standard is that encryption is reversible, whereas the digital signature operation is not. Another fact about the digital signature standard is that it does not provide any capability with regards to key distribution or exchange of keys. In other words, security of the digital signature standard largely depends on the secrecy of the private keys of the signatory.

(d) security attacks; (2012)

Passive Attacks

Passive attacks are in the nature of eavesdropping on, or monitoring of, transmissions. The goal of the opponent is to obtain information that is being transmitted. Two types of passive attacks are release of message contents and traffic analysis.

iii) **The release of message** contents is easily understood (Figure 1 a). A telephone conversation, an electronic mail message, and a transferred file may contain sensitive or confidential information. We would like to prevent an opponent from learning the contents of these transmissions.

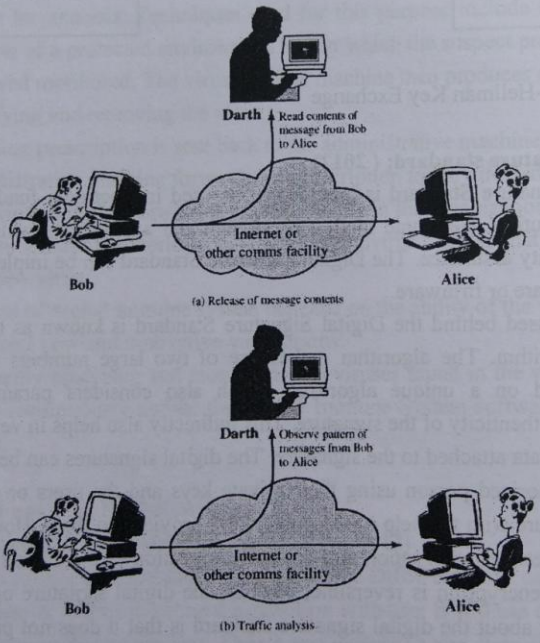


Figure 1. Passive Attacks

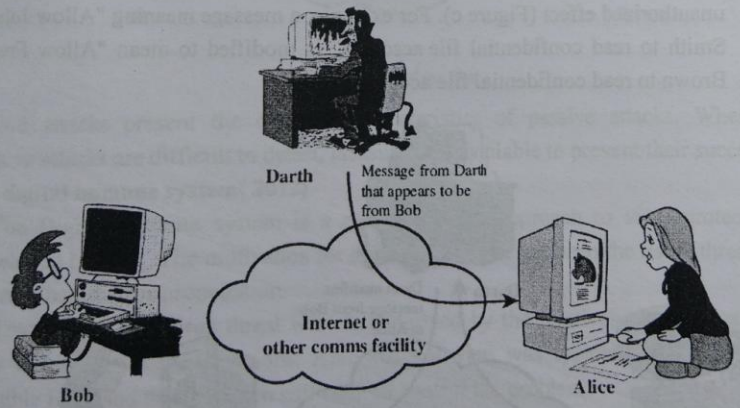
iv) **traffic analysis**, A second type of passive attack, **traffic analysis**, is subtler (Figure 1b). Suppose that we had a way of masking the contents of messages or other information traffic so that opponents, even if they captured the message, could not extract the information from the message. The common

technique for masking contents is encryption. If we had encryption protection in place, an opponent might still be able to observe the pattern of these messages. The opponent could determine the location and identity of communicating hosts and could observe the frequency and length of messages being exchanged. This information might be useful in guessing the nature of the communication that was taking place.

Active Attacks

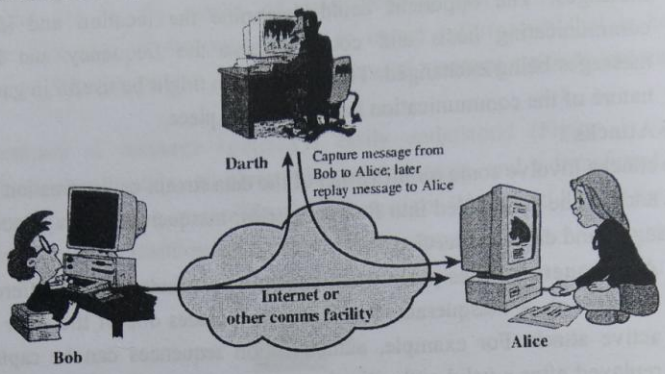
Active attacks involve some modification of the data stream or the creation of a false stream and can be subdivided into four categories: masquerade, replay, modification of messages, and denial of service.

v) A **masquerade** takes place when one entity pretends to be a different entity (Figure a). A masquerade attack usually includes one of the other forms of active attack. For example, authentication sequences can be captured and replayed after a valid authentication sequence has taken place, thus enabling an authorized entity with few privileges to obtain extra privileges by impersonating an entity that has those privileges.



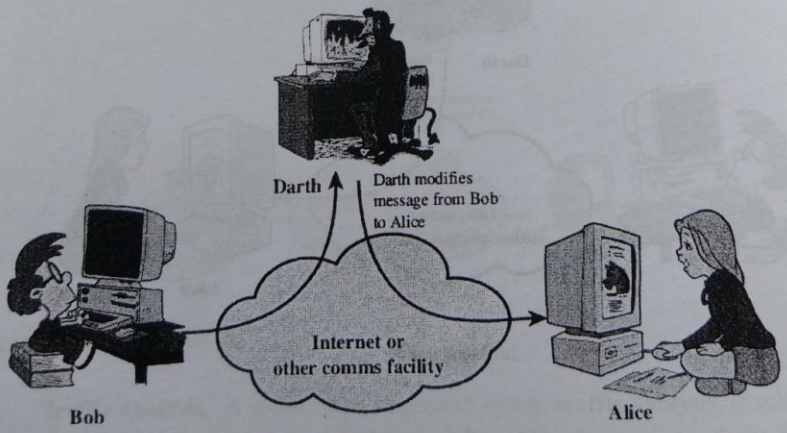
(a) Masquerade

vi) **Replay** involves the passive capture of a data unit and its subsequent retransmission to produce an unauthorized effect (Figure b).



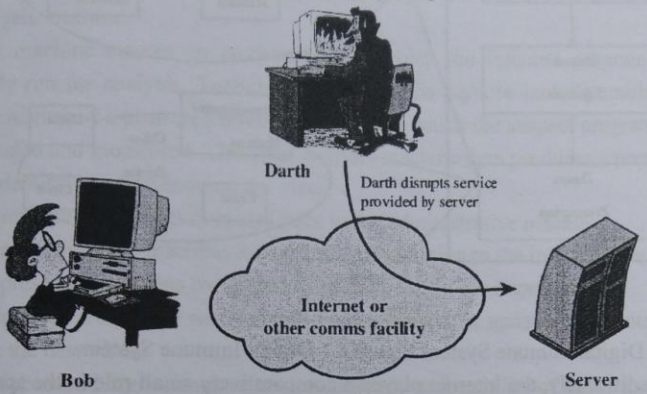
(b) Replay

vii) **Modification of messages** simply means that some portion of a legitimate message is altered, or that messages are delayed or reordered, to produce an unauthorized effect (Figure c). For example, a message meaning "Allow John Smith to read confidential file accounts" is modified to mean "Allow Fred Brown to read confidential file accounts."



(c) Modification of messages

viii) The **denial of service** prevents or inhibits the normal use or management of communications facilities (Figure d). This attack may have a specific target; for example, an entity may suppress all messages directed to a particular destination (e.g., the security audit service). Another form of service denial is the disruption of an entire network, either by disabling the network or by overloading it with messages so as to degrade performance.



(d) Denial of service

Active attacks present the opposite characteristics of passive attacks. Whereas passive attacks are difficult to detect, measures are available to prevent their success.

(e) digital immune system(2012)

i. The Digital Immune system is a comprehensive approach to virus protection developed by IBM. The motivation for this development has been the rising threat of Internet-based virus propagation.

ii. Traditionally the virus threat was characterized by the relatively slow spread of new viruses and new mutations. Antivirus software was typically updated on a monthly basis and this has been sufficient to control the problem.

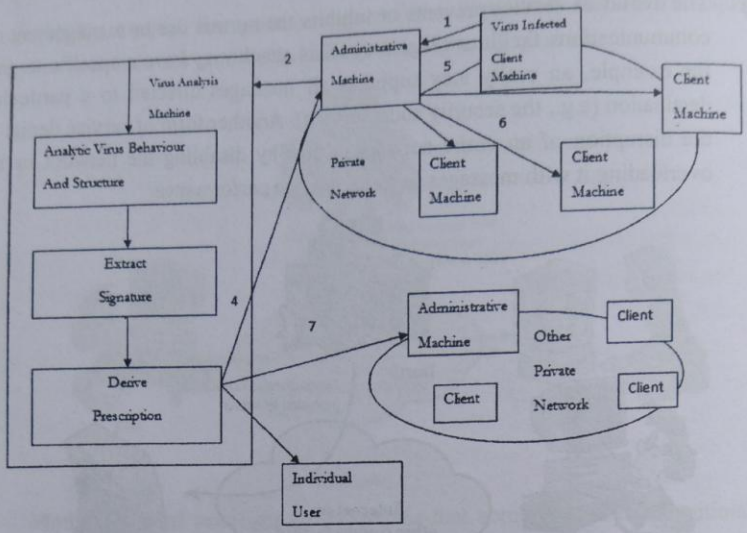


Figure 6.1 Digital Immune System Figure 6.1 Digital Immune System

iii. Also traditionally, the Internet played a comparatively small role in the spread of viruses. Two major trends in Internet technology had an increasing impact on the rate of virus propagation in recent years:

- **Integrated Mail Systems:** Systems such as Lotus Notes and Microsoft Outlook make it very simple to send anything to anyone and to work with objects that are received.
- **Mobile-Program Systems:** Capabilities such as Java and ActiveX allow programs to move on their own form one system to another.

iv. In response to threat posed by these Internet-based capabilities, IBM has developed a prototype digital immune system. The objective of this system is to provide rapid response time so that viruses can be stamped out almost as soon as they are introduced.

v. When a new virus enters an organization, the immune system automatically captures it, analyzes it, adds detection and shielding for it, removes it and passes information about that virus to systems running IBM antivirus so that it can be detected before it is allowed to run elsewhere.

vi. The operation of digital immune system as follows:

- ✓ A monitoring program on each PC uses a variety of heuristics based on system behaviour, suspicious changes to programs or family signature to inform that a virus may be present. The monitoring program forwards a copy of any program thought to be infected to an administrative machine within the organization.
- ✓ The administrative machine encrypts the sample and sends it to a central virus analysis machine.
- ✓ This machine creates an environment in which the infected program can be safely run for analysis. Techniques used for this purpose include emulation, or the creation of a protected environment within which the suspect program can be executed and monitored. The virus analysis machine then produces a prescription for identifying and removing the virus.
- ✓ The resulting prescription is sent back to the administrative machine.
- ✓ The administrative machine forwards the prescription to the infected client.
- ✓ The prescription is also forwarded to other clients in the organization.
- ✓ Subscribers around the world receive regular antivirus updates that protect them from the new virus.

vii. The success of digital immune system depends on the ability of the virus analysis machine to detect new and innovative virus strains.

viii. By constantly analyzing and monitoring the viruses found in the wild, it should be possible to continuously update the Digital Immune System software to keep up with the threat.

(f) MIME contents(2012)

Answer:

Multipurpose Internet Mail Extensions (MIME) is an Internet standard that extends the format of email to support:

- ✓ Text in character sets other than ASCII
- ✓ Non-text attachments: audio, video, images, application programs etc.
- ✓ Message bodies with multiple parts
- ✓ Header information in non-ASCII character sets

Virtually all human-written Internet email and a fairly large proportion of automated email is transmitted via SMTP in MIME format.

MIME is specified in six linked RFC memoranda: RFC 2045, RFC 2046, RFC 2047, RFC 4288, RFC 4289 and RFC 2049; with the integration with SMTP email specified in detail in RFC 1521 and RFC 1522.

Although MIME was designed mainly for SMTP, the content types defined by MIME standards are also of importance in communication protocols outside of email, such as HTTP for the World Wide Web. Servers insert the MIME header at the beginning of any Web transmission. Clients use this content type or media type header to select an appropriate viewer application for the type of data the header indicates. Some of these viewers are built into the Web client or browser (for example, almost all browsers come with GIF and JPEG image viewers as well as the ability to handle HTML files).

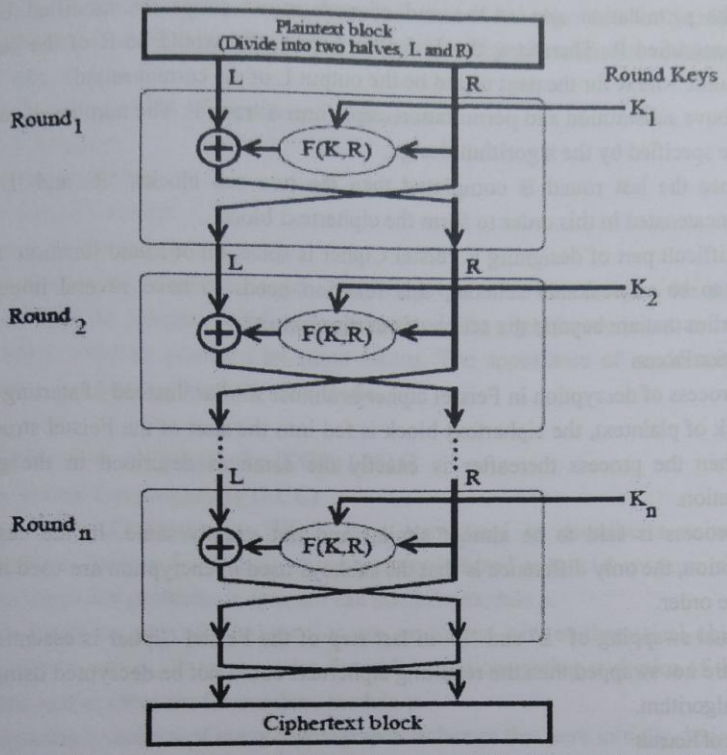
(i) Feistel cipher(2016)

Feistel Cipher is not a specific scheme of block cipher. It is a design model from which many different block ciphers are derived. DES is just one example of a Feistel Cipher. A cryptographic system based on Feistel cipher structure uses the same algorithm for both encryption and decryption.

Encryption Process

The encryption process uses the Feistel structure consisting multiple rounds of processing of the plaintext, each round consisting of a "substitution" step followed by a permutation step.

Feistel Structure is shown in the following illustration –



- ✓ The input block to each round is divided into two halves that can be denoted as L and R for the left half and the right half.
- ✓ In each round, the right half of the block, R, goes through unchanged. But the left half, L, goes through an operation that depends on R and the encryption key. First, we apply an encrypting function 'f' that takes two input – the key K and R. The function produces the output f(R,K). Then, we XOR the output of the mathematical function with L.
- ✓ In real implementation of the Feistel Cipher, such as DES, instead of using the whole encryption key during each round, a round-dependent key (a subkey) is derived from the encryption key. This means that each round uses a different key, although all these subkeys are related to the original key.

- ✓ The permutation step at the end of each round swaps the modified L and unmodified R. Therefore, the L for the next round would be R of the current round. And R for the next round be the output L of the current round.
- ✓ Above substitution and permutation steps form a 'round'. The number of rounds are specified by the algorithm design.
- ✓ Once the last round is completed then the two sub blocks, 'R' and 'L' are concatenated in this order to form the ciphertext block.

The difficult part of designing a Feistel Cipher is selection of round function 'f'. In order to be unbreakable scheme, this function needs to have several important properties that are beyond the scope of our discussion.

Decryption Process

The process of decryption in Feistel cipher is almost similar. Instead of starting with a block of plaintext, the ciphertext block is fed into the start of the Feistel structure and then the process thereafter is exactly the same as described in the given illustration.

The process is said to be almost similar and not exactly same. In the case of decryption, the only difference is that the subkeys used in encryption are used in the reverse order.

The final swapping of 'L' and 'R' in last step of the Feistel Cipher is essential. If these are not swapped then the resulting ciphertext could not be decrypted using the same algorithm.

Number of Rounds

The number of rounds used in a Feistel Cipher depends on desired security from the system. More number of rounds provide more secure system. But at the same time, more rounds mean the inefficient slow encryption and decryption processes. Number of rounds in the systems thus depend upon efficiency–security tradeoff.

(iii)PRNG(2016)

Pseudo Random Number Generator(PRNG) refers to an algorithm that uses mathematical formulas to produce sequences of random numbers. PRNGs generate a sequence of numbers approximating the properties of random numbers.

A PRNG starts from an arbitrary starting state using a **seed state**. Many numbers are generated in a short time and can also be reproduced later, if the starting point in the sequence is known. Hence, the numbers are **deterministic and efficient**.

Linear Congruential Generator is most common and oldest algorithm for generating pseudo-randomized numbers. The generator is defined by the recurrence relation:

$X_{n+1} = (aX_n + c) \bmod c$

where X is the sequence of pseudo-random values

m, $0 < m$- modulus

a, $0 < a < m$- multiplier

c, $0 <= c < m$- increment

x_0, $0 <= x_0 < m$- the seed or start value

We generate the next random integer using the previous random integer, the integer constants, and the integer modulus. To get started, the algorithm requires an initial Seed, which must be provided by some means. The appearance of randomness is provided by performing **modulo arithmetic.**.

(iv) elliptic curve cryptography (ECC) (2016)

Elliptic Curve Cryptography (ECC)

Elliptic Curve Cryptography (ECC) is a term used to describe a suite of cryptographic tools and protocols whose security is based on special versions of the discrete logarithm problem. It does not use numbers modulo p.

ECC is based on sets of numbers that are associated with mathematical objects called elliptic curves. There are rules for adding and computing multiples of these numbers, just as there are for numbers modulo p.

ECC includes a variants of many cryptographic schemes that were initially designed for modular numbers such as ElGamal encryption and Digital Signature Algorithm.

It is believed that the discrete logarithm problem is much harder when applied to points on an elliptic curve. This prompts switching from numbers modulo p to points on an elliptic curve. Also an equivalent security level can be obtained with shorter keys if we use elliptic curve-based variants.

The shorter keys result in two benefits –

- Ease of key management
- Efficient computation

These benefits make elliptic-curve-based variants of encryption scheme highly attractive for application where computing resources are constrained.

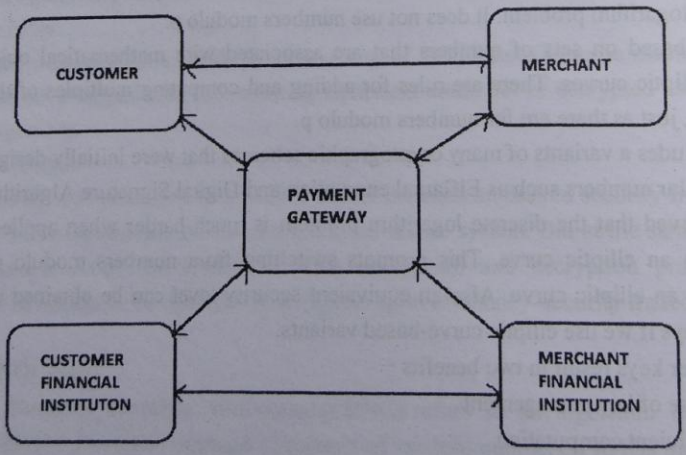
(iv)SET (2015)

Secure Electronic Transaction (SET) Protocol

Secure Electronic Transaction or SET is a system which ensures security and integrity of electronic transactions done using credit cards in a scenario. SET is not some system that enables payment but it is a security protocol applied on those payments. It uses different encryption and hashing techniques to secure payments over internet done through credit cards. SET protocol was supported in development by major organizations like Visa, Mastercard, Microsoft which provided its Secure Transaction Technology (STT) and NetScape which provided technology of Secure Socket Layer (SSL).

SET protocol restricts revealing of credit card details to merchants thus keeping hackers and thieves at bay. SET protocol includes Certification Authorities for making use of standard Digital Certificates like X.509 Certificate.

Before discussing SET further, let's see a general scenario of electronic transaction, which includes client, payment gateway, client financial institution, merchant and merchant financial institution.



Requirements in SET :

SET protocol has some requirements to meet, some of the important requirements are :

- It has to provide mutual authentication i.e., customer (or cardholder) authentication by confirming if the customer is intended user or not and merchant authentication.
- It has to keep the PI (Payment Information) and OI (Order Information) confidential by appropriate encryptions.
- It has to be resistive against message modifications i.e., no changes should be allowed in the content being transmitted.
- SET also needs to provide interoperability and make use of best security mechanisms.

Participants in SET :

In the general scenario of online transaction, SET includes similar participants:

1. **Cardholder** – customer
2. **Issuer** – customer financial institution
3. **Merchant**
4. **Acquirer** – Merchant financial
5. **Certificate authority** – Authority which follows certain standards and issues certificates(like X.509V3) to all other participants.

SET functionalities :

- **Provide Authentication**
  - **Merchant Authentication** – To prevent theft, SET allows customers to check previous relationships between merchant and financial institution. Standard X.509V3 certificates are used for this verification.
  - **Customer / Cardholder Authentication** – SET checks if use of credit card is done by an authorized user or not using X.509V3 certificates.
- **Provide Message Confidentiality** : Confidentiality refers to preventing unintended people from reading the message being transferred. SET implements confidentiality by using encryption techniques. Traditionally DES is used for encryption purpose.
- **Provide Message Integrity** : SET doesn't allow message modification with the help of signatures. Messages are protected against unauthorized modification using RSA digital signatures with SHA-1 and some using HMAC with SHA-1,

(vii) Unix password scheme(2015, 2014)

UNIX password scheme

In most of the computer security contexts, user authentication is the fundamental building block and primary line of defense. User authentication is the basis for most type of access control and for user accountability.

Hashed passwords are widely used in UNIX like operating system. UNIX uses hashed password and salt value are used in UNIX like operating system. This password scheme is completely different form windows like operating system. Windows uses only encryption of passwords rather than like UNIX that's why windows have not much of powerful authentication scheme. UNIX password scheme is explained below and fig 1 shows UNIX password scheme.

To load new password in system user have to select new password. This password is combined with the salt value. Salt values are of fixed length and can be anything like time, date etc. But latest implementation uses random number as a salt value.
The password and salt value are given input to the hashed algorithm to produce fixed length of hashed value. The hashed value is then stored with the plain text copy of salt value in the password file for corresponding user ID.

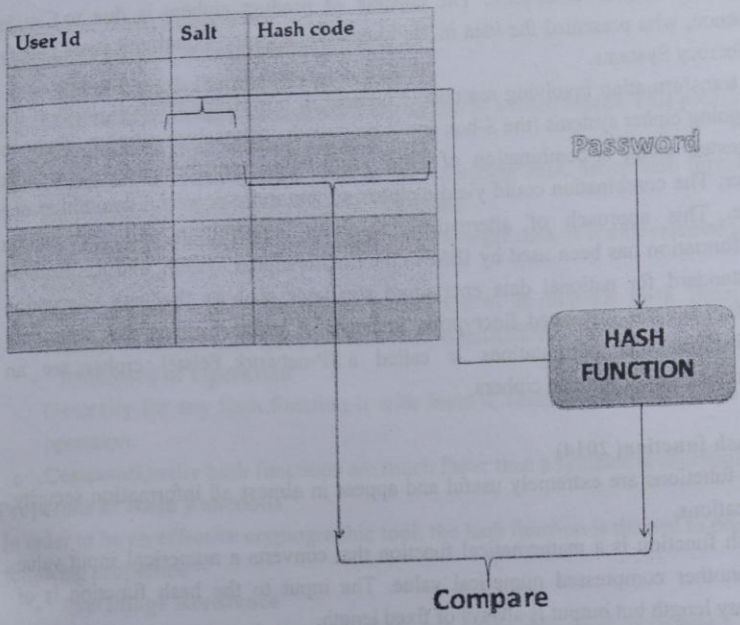


fig1.UNIX password scheme

When user attempts to log on to UNIX system, the user provides an ID and password. The operating system uses ID as index in password file and retrieves plain text salt value and encrypted password. The new provided password and salt value are given as input to encryption algorithm. Algorithm generates encrypted password which is compared with the encrypted value returned with salt value if the both matches then only log-in is allowed otherwise denied.

The other benefit of this mechanism is even if two users chooses same password it does not conflict because salt value for each user ID is different.

(a) product Cipher (2014)

In cryptography, a **product cipher** combines two or more transformations in a manner intending that the resulting cipher is more secure than the individual components to make it resistant to cryptanalysis. The product cipher combines a sequence of simple transformations such as substitution (S-box), permutation (P-

box), and modular arithmetic. The concept of product ciphers is due to Claude Shannon, who presented the idea in his foundational paper, Communication Theory of Secrecy Systems.

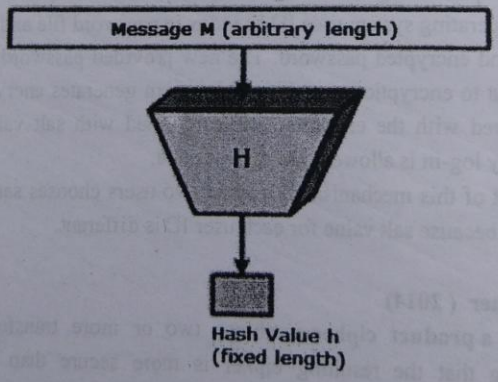
For transformation involving reasonable number of n message symbols, both of the foregoing cipher systems (the S-box and P-box) are by themselves wanting. Shannon suggested using a combination of S-box and P-box transformation—a product cipher. The combination could yield a cipher system more powerful than either one alone. This approach of alternatively applying substitution and permutation transformation has been used by IBM in the Lucifer cipher system, and has become the standard for national data encryption standards such as the Data Encryption Standard and the Advanced Encryption Standard. A product cipher that uses only substitutions and permutations is called a SP-network. Feistel ciphers are an important class of product ciphers.

(d) hash function(2014)

Hash functions are extremely useful and appear in almost all information security applications.

A hash function is a mathematical function that converts a numerical input value into another compressed numerical value. The input to the hash function is of arbitrary length but output is always of fixed length.

Values returned by a hash function are called **message digest** or simply **hash values**. The following picture illustrated hash function –



Features of Hash Functions

The typical features of hash functions are –

- **Fixed Length Output (Hash Value)**
  - Hash function coverts data of arbitrary length to a fixed length. This process is often referred to as **hashing the data**.
  - In general, the hash is much smaller than the input data, hence hash functions are sometimes called **compression functions**.
  - Since a hash is a smaller representation of a larger data, it is also referred to as a **digest**.
  - Hash function with n bit output is referred to as an **n-bit hash function**. Popular hash functions generate values between 160 and 512 bits.
- **Efficiency of Operation**
  - Generally for any hash function h with input x, computation of h(x) is a fast operation.
  - Computationally hash functions are much faster than a symmetric encryption.

Properties of Hash Functions

In order to be an effective cryptographic tool, the hash function is desired to possess following properties –

- **Pre-Image Resistance**
  - This property means that it should be computationally hard to reverse a hash function.
  - In other words, if a hash function h produced a hash value z, then it should be a difficult process to find any input value x that hashes to z.
  - This property protects against an attacker who only has a hash value and is trying to find the input.
- **Second Pre-Image Resistance**
  - This property means given an input and its hash, it should be hard to find a different input with the same hash.
  - In other words, if a hash function h for an input x produces hash value h(x), then it should be difficult to find any other input value y such that h(y) = h(x).
  - This property of hash function protects against an attacker who has an input value and its hash, and wants to substitute different value as legitimate value in place of original input value.

- **Collision Resistance**
  - This property means it should be hard to find two different inputs of any length that result in the same hash. This property is also referred to as collision free hash function.
  - In other words, for a hash function h, it is hard to find any two different inputs x and y such that $h(x) = h(y)$.
  - Since, hash function is compressing function with fixed hash length, it is impossible for a hash function not to have collisions. This property of collision free only confirms that these collisions should be hard to find.
  - This property makes it very difficult for an attacker to find two input values with the same hash.
  - Also, if a hash function is collision-resistant **then it is second pre-image resistant.**

(e)IPSec ESP format(2014)

In computing, **Internet Protocol Security (IPsec)** is a secure network protocol suite that authenticates and encrypts the packets of data sent over an internet protocol network. It is used in virtual private networks (VPNs).

IPsec includes protocols for establishing mutual authentication between agents at the beginning of a session and negotiation of cryptographic keys to use during the session. IPsec can protect data flows between a pair of hosts (host-to-host), between a pair of security gateways (network-to-network), or between a security gateway and a host (network-to-host). Internet Protocol security (IPsec) uses cryptographic security services to protect communications over Internet Protocol (IP) networks. IPsec supports network-level peer authentication, data-origin authentication, data integrity, data confidentiality (encryption), and replay protection.

The initial IPv4 suite was developed with few security provisions. As a part of the IPv4 enhancement, IPsec is a layer 3 OSI model or Internet Layer end-to-end security scheme, while some other Internet security systems in widespread use operate above layer 3, such as Transport Layer Security (TLS) and Secure Shell (SSH), both of which operate at the Application layer. IPsec can automatically secure applications at the IP layer.

Security architecture

The IPsec is an open standard as a part of the IPv4 suite. IPsec uses the following protocols to perform various functions

- Authentication Headers (AH) provides connectionless data integrity and data origin authentication for IP datagrams and provides protection against replay attacks.
- Encapsulating Security Payloads (ESP) provides confidentiality, connectionless integrity, data-origin authentication, an anti-replay service (a form of partial sequence integrity), and limited traffic-flow confidentiality.
- Security Associations (SA) provides the bundle of algorithms and data that provide the parameters necessary for AH and/or ESP operations. The Internet Security Association and Key Management Protocol (ISAKMP) provides a framework for authentication and key exchange, with actual authenticated keying material provided either by manual configuration with pre-shared keys, Internet Key Exchange (IKE and IKEv2), Kerberized Internet Negotiation of Keys (KINK), or IPSECKEY DNS records.

Authentication Header

The Security Authentication Header (AH) is derived partially from previous IETF standards work for authentication of the Simple Network Management Protocol (SNMP) version 2. Authentication Header (AH) is a member of the IPsec protocol suite. AH ensures connectionless integrity by using a hash function and a secret shared key in the AH algorithm. AH also guarantees the data origin by authenticating IP packets. Optionally a sequence number can protect the IPsec packet's contents against replay attacks, using the sliding window technique and discarding old packets.

- In IPv4, AH prevents option-insertion attacks. In IPv6, AH protects both against header insertion attacks and option insertion attacks.
- In IPv4, the AH protects the IP payload and all header fields of an IP datagram except for mutable fields (i.e. those that might be altered in transit), and also IP options such as the IP Security Option (RFC 1108). Mutable (and therefore unauthenticated) IPv4 header fields are DSCP/ToS, ECN, Flags, Fragment Offset, TTL and Header Checksum.
- In IPv6, the AH protects most of the IPv6 base header, AH itself, non-mutable extension headers after the AH, and the IP payload. Protection for the IPv6 header excludes the mutable fields: DSCP, ECN, Flow Label, and Hop Limit

AH operates directly on top of IP, using IP protocol number 51.