Q.2a. Define Virus. What are the four phases of Viruses? In addition, list out the types of Viruses.

A virus is a piece of software that can "infect" other programs by modifying them; the modification includes a copy of the virus program, which can then go on to infect other programs. It can be compared to biological viruses, and like them, a computer virus carries in its instructional code the recipe for making perfect copies of it. Once a virus is executing, it can perform any function, such as erasing files and programs.

Dormant Phase: This virus is idle one and activated by some event such as a file.
Propagation Phase: Virus places an identical copy of itself
Triggering Phase: Virus is activated to perform the functions
Execution Phase: Virus is performed

A virus is a program that can infect other program by modifying them the modification includes a copy of the virus program, which can then go on to infect other program.
Types:
1) Parasitic virus
2) Memory-resident virus
3) Boot sector virus
4) Stealth virus
5) Polymorphic virus

b.What are the key principles of security?

Authenticity: When sending and receiving a message, placing an order, or submitting a payment electronically, both parties want to validate that the other party is who they claim to be. Each party wants to know the identity of the other to avoid fraud and misrepresentation. One way to ensure authenticity is to limit remote access to a network (for example from home or from a separate corporate location) to trusted parties by using Virtual Private Network (VPN) technology.

Data integrity: A message received should be identical to the message that was sent. A business needs to be guaranteed that data is not changed in transit, whether deliberately or by accident. A sealed envelope prevents tampering with paper documents and the nature of the printed page makes it difficult to alter without detection. On the Internet, digital signature technology can create virtual envelopes that can be verified by the recipient to ensure that no unapproved changes have been made. To ensure the integrity of stored data, firewalls are used to guard against unauthorized access and anti-virus software protects against virus invasion. In addition, data backups and infrastructure redundancy allow recovery in the event that data or equipment is damaged.

Non-repudiation: A business needs to be certain that the receiving party cannot deny that a transaction has occurred. In physical transactions, receipts, signatures and third party witnesses are used for this purpose. In electronic transactions there must also be a transaction record that links the sender and receiver. Digital signatures, digital certificates and strong authentication procedures are emerging as the means to address non-repudiation.

Access Control: When access to electronic resources is limited to authorized parties only, a business must be sure that no others can access the systems or information. In the non-digital world, access control is provided by lock and key. In the digital world, a variety of techniques are used to control access: firewalls, access privileges, network traffic monitoring, Intrusion Detection Systems (IDS), user identification and authentication techniques (such as passwords and digital certificates) and Virtual Private Networks (VPN).

Availability: If a business relies on electronic information or services, it must be available when customers need it. Messages must be delivered reliably, and information stored and retrieved as required.

c.Find the order of all elements in G = $<Z_{10}*, x>$

Ans : Page 282, Ref book

Q.3a. Explain following Feistel cipher, polyalphabetic cipher.

Substitution of single letters separately simple substitution can be demonstrated by writing out the alphabet in some order to represent the substitution. This is termed a substitution alphabet. The cipher alphabet may be shifted or reversed or scrambled in a more complex fashion, in which case it is called a mixed alphabet or deranged alphabet. Traditionally, mixed alphabets may be created by first writing out a keyword, removing repeated letters in it, and then writing all the remaining letters in the alphabet in the usual order.

In a poly alphabetic cipher, multiple cipher alphabets are used. To facilitate encryption, all the alphabets are usually written out in a large table, traditionally called a tableau. The tableau is usually 26×26, so that 26 full cipher text alphabets are available. The method of filling the tableau, and of choosing which alphabet to use next, defines the particular poly alphabetic cipher. All such ciphers are easier to break than once believed, as substitution alphabets are repeated for sufficiently large plaintexts.

Feistel Cipher- P-139 of Ref book

b. What is affine cipher? Use an affine cipher to encrypt the message "hello" with the key-pair (7, 2).

Ans : Page 67, Ref book

Q.4 a. Explain DES with neat diagram. What is the purpose of the S-boxes in DES? How is the S-box constructed?

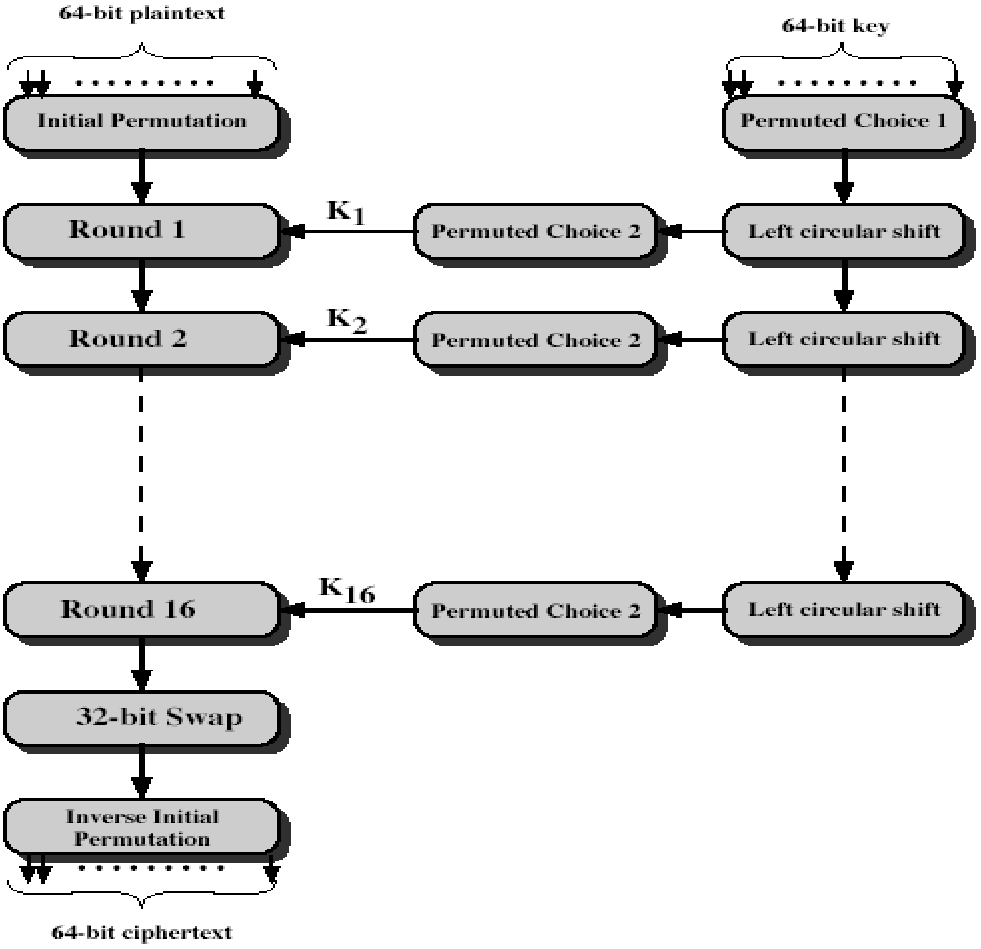


Figure 3.7 General Depiction of DES Encryption Algorithm

DES ENCRYPTION

Design criteria for S-boxes were not made public, so there was a concern that cryptanalysis is possible for an opponent who knows the weaknesses in S-boxes. Up to now, there are no published results about such weaknesses in S-boxes.

DES also appears to be resistant to timing attack but suggest some avenues to explore. Timing attack tries to understand essence of algorithm by analysis of time of its work on different inputs. One of such approaches yields a Hamming weight (number of bits equal to 1) of the secret key.

Each of the eight S-boxes consists of a 4×16 table lookup for an output 4-bit word. The first and the last bit of the 6-bit input word are decoded into one of 4 rows and the middle 4 bits decoded into one of 16 columns for the table lookup.

The goal of the substitution carried out by an S-box is to enhance diffusion, as mentioned previously. As you will recall from the E-step described in Section 3.3.1, the expansion-permutation step (the E-step) expands a 32-bit block into a 48-bit block by attaching a bit at the beginning and a bit at the end of each 4-bit sub-block, the two bits needed for these attachments belonging to the adjacent blocks.

In cryptography, an **S-Box** (**Substitution-box**) is a basic component of symmetric key algorithms which performs substitution. In block ciphers, they are typically used to obscure the relationship between the key and the ciphertext - Shannon's property of confusion. In many cases, the S-Boxes are carefully chosen to resist cryptanalysis.
In general, an S-Box takes some number of input bits, *m*, and transforms them into some number of output bits, *n*: an *m*×*n* S-Box can be implemented as a lookup table with 2^m words of *n* bits each. Fixed tables are normally used, as in the Data Encryption Standard (DES), but in some ciphers the tables are generated dynamically from the key.

b.Write about linear profile and round characteristics of DES.

Ans : Page 655, Ref book

Q.5 a. Explain RSA Algorithm. Given the two prime numbers p=61 and q=53, find N, e, and d.

Ans The RSA cryptosystem is the most widely-used public key cryptography algorithm in the world. It can be used to encrypt a message without the need to exchange a secret key separately. The RSA algorithm can be used for both public key encryption and digital signatures. Its security is based on the difficulty of factoring large integers.

Party A can send an encrypted message to party B without any prior exchange of secret keys. A just uses B's public key to encrypt the message and B decrypts it using the private key, which only he knows. RSA can also be used to sign a message, so A can sign a message using their private key and B can verify it using A's public key. When we talk about the *key length* of an RSA key, we are referring to the length of the modulus, *n*, in bits. The minimum recommended key length for a secure RSA transmission is currently 1024 bits. A key length of 512 bits is now no longer considered secure, although cracking it is still not a trivial task for the likes of you and me. The longer your information is needed to be kept secure, the longer the key you should use. Keep up to date with the latest recommendations in the security journals.

There is small one area of confusion in defining the key length. One convention is that the key length is the position of the most significant bit in *n* that has value '1', where the least significant bit is at position 1. Equivalently, key length = ceiling($\log_2$(n+1)). The other convention, sometimes used, is that the key length is the number of bytes needed to store *n* multiplied by eight, i.e. ceiling($\log_{256}$(n+1))*8.

1. Choose two distinct prime numbers, such as

   $p = 61$ and $q = 53$.

2. Compute *n* = *pq* giving

   $$n = 61 \times 53 = 3233.$$

3. Compute the totient of the product as φ(*n*) = (*p* − 1)(*q* − 1) giving

$$\varphi(3233) = (61 - 1)(53 - 1) = 3120.$$

4. Choose any number 1 < *e* < 3120 that is coprime to 3120. Choosing a prime number for *e* leaves us only to check that *e* is not a divisor of 3120.

   Let $e = 17.$

5. Compute *d*, the modular multiplicative inverse of *e* (mod φ(*n*)) yielding

$$d = 2753.$$

The **public key** is (*n* = 3233, *e* = 17). For a padded plaintext message *m*, the encryption function is

$$c(m) = m^{17} \pmod{3233}.$$

The **private key** is (*n* = 3233, *d* = 2753). For an encrypted ciphertext *c*, the decryption function is c^{2753}(mod 3233).

$$m(c) = c^{2753} \pmod{3233}.$$

For instance, in order to encrypt *m* = 65, we calculate

$$c \equiv 65^{17} \pmod{3233} \equiv 2790$$

To decrypt *c* = 2790, we calculate

$$m \equiv 2790^{2753} \pmod{3233} \equiv 65$$

b.Describe the advantages and disadvantages of symmetric and asymmetric key cryptography.

Methods of encrypting messages include the: Symmetric Key Encryption and Asymmetric or Public Key Encryption methods.

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.

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:

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. **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.

Q.6a. What is message digest (HD)? What are two important properties of good HD algorithm?

Ans A message digest is also a hash function. It takes a variable length input - often an entire disk file - and reduces it to a small value (typically 128 to 512 bits). Give it the same input, and it always produces the same output. And, because the output is very much smaller than the potential input, for at least one of the output values there must be more than one input value that can produce it; we would expect that to be true for all possible output values for a good message digest algorithm.

There are two other important properties of good message digest algorithms. The first is that the algorithm cannot be predicted or reversed. That is, given a particular output value, we cannot come up with an input to the algorithm that will produce that output, either by trying to find an inverse to the algorithm, or by somehow predicting the nature of the input required. With at least 128 bits of output, a brute force attack is pretty much out of the question, as there will be 1.7 x 10^{38} possible input values of the same length to try, on average, before finding one that generates the correct output. Compare this with some of the figures given in "Strength of RSA" earlier in this chapter, and you'll see that this task is beyond anything anyone would be able to try with current technology. With numbers as large as these, the idea that any two *different* documents produced at random during the course of human history would have the same 128-bit message digest is unlikely!

The second useful property of message digest algorithms is that a small change in the input results in a significant change in the output. Change a single input bit, and roughly half of the output bits should change. This is actually a consequence of the first property, because we don't want the output to be predictable based on the input. However, this aspect is a valuable property of the message digest all by itself.

b. Explain length field and padding in SHA_{512}. **What is the number of padding bits if the length of the original message is 2590 bits?**

Ans : Page 369of , Ref book

Q.7 a. Explain concept of digital signature. What is the important aspect that establishes trust in digital signatures?

Ans A digital signature is used to authenticate -digital information such as documents, e-mail messages, and macros - by using computer cryptography. Digital signatures help to establish the following assurances:

- Authenticity: The digital signature helps to assure that the signer is who they claim to be.
- Integrity: The digital signature helps to assure that the content has not been changed or tampered with since it was digitally signed.

- Non-repudiation: The digital signature helps to prove to all parties the origin of the signed content. "Repudiation" refers to the act of a signer's denying any association with the signed content.

To make these assurances, the content must be digitally signed by the content creator, using a signature that satisfies the following criteria:

- The digital signature is valid.
- The certificate associated with the digital signature is current (not expired).
- The signing person or organization, known as the publisher, is trusted
- The certificate associated with the digital signature is issued to the signing publisher by a reputable certificate authority (CA).

b. The Diffie-Hellman key exchange is susceptible to two attacks. Give an overview of both attacks.

Ans : Page 449, 450 of Ref book

Q.8 a. What is MIME? MIME allows seven different types of data. Briefly explain each and its subtypes.

Ans : Page 492, 493 of ,Ref book

b. Explain the concept of key rings in PGP.

Ans PGP makes use of four types of keys:
1. One-time session symmetric keys
2. Public keys
3. Private keys
4. Passphrase based symmetric keys

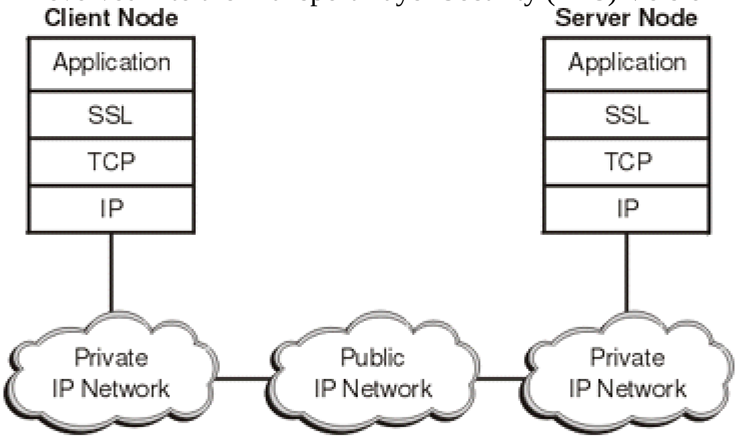
Three separate requirements can be identified with respect to these keys:
1. A means of generating unpredictable session keys is needed
2. We would like to allow a user to have multiple public-key/private-key pairs. As a result there is not a one-to-one correspondence between users and their public keys. Thus, some means is needed for identifying particular keys.
3. Each PGP entity must maintain a file of its own public/private key pairs as well as a file of public keys of correspondents.

Q.9 a. Why is the SSL layer positioned between the application layer and the transport layer?

Ans SSL is positioned as a protocol layer between the Transmission Control Protocol (TCP) layer and the application to form a secure connection between clients and servers so that they can communicate in a secure manner over a network by providing:

- Privacy, where data messages are encrypted so that only the two application endpoints understand the data.
- Integrity, where message digests detect if any data was altered in flight.
- Authentication, which verifies the identity of the remote node, application, or user by using digital certificates.

SSL is a set of rules governing authentication and encrypted communication between clients and servers. SSL is widely used on the Internet by an increasing number of varied applications, especially for interactions that involve exchanging confidential information such as credit card numbers. SSL evolved into the Transport Layer Security (TLS) Version 1 standard.



This type of secure connection ensures that all data exchanged between clients and servers is encrypted, and is therefore not readable by a third party on the Internet. SSL has gained popularity in the Internet industry primarily because of its use of public-key certificates as a means of authenticating principles.

To establish the connection, SSL requires, at a minimum, a server certificate. As part of the initial SSL handshake process, the server presents its certificate to the client to authenticate the server's identity. The authentication process uses public-key encryption and digital signatures to confirm that the server is, in fact, who the server claims to be (that is, the server's certificate is valid).

Once the server has been authenticated (that is, the client determines that the server's certificate is valid), the client and server use techniques of public-key encryption to exchange a symmetric key, which is then used to encrypt all the information exchanged for the remainder of the SSL session. Message digests are used to detect data tampering. A different key is created for each client and server connection.

b. Differentiate between TLS and SSL.

Alert Message: If a client has no certificate to use, he can pass a message “No Certificate” in TLS protocol. While in SSL, if a client has no certificate, there is no need for a separate message.

Message Authentication: TLS applies MAC (H-MAC) in many implementations while SSL uses MD5 and SHA. The benefit for using H-MAC is it can be operated by any hash function.

Key Material Generation: TLS applies the HMAC standard and PRF (pseudorandom function) to generate the key. SSL uses RSA, Diffie-Hellman, or Fortezza/DMS to generate key material.

Certificate Verify Message: In TLS, certificate verification message is already contained in the handshake message, which is already exchanged in session. In SSL, it requires a tough procedure to pass a certificate verification message.

Finished: In TLS, the finished message is created thorough PRF output with the help of “client finished” or “server finished” message. In SSL, the finished message is created in the same manner in which the key was generated. It uses cipher suite and parameter information.

Text Book

1. **Behrouz A. Forouzan, Cryptography & Network Security, Special Indian Edition**