Assignment - 3

Module 4

1. List & explain various types of threats to network security.

- Internet infrastructure attacks are broadly classified into:
  1. DNS hacking
  2. Routing table poisoning
  3. Packet mistreatment
  4. Denial of service.

(1) DNS Hacking Attacks:

- Domain Name System (DNS) server is a distributed hierarchial & global directory that translates domain names into numerical IP address.
- DNS is a critical infrastructure, & all hosts contact DNS to access servers & start connection. In the normal mode of operation, hosts send UDP queries to the DNS server. Servers reply with a proper answer, or direct the queries to smaller servers. A DNS also stores info^n other than host addresses.
- An attack on DNS can potentially affect a large portion of the Internet.
- A DNS hacking attack may result in the lack of data authenticity & integrity.

(2) Routing table poisoning attacks:

- It is the undesired modification of routing tables. An attacker can do this by maliciously modifying the routing info^n update packets sent by routers.
- Any false entry in a routing table could lead to significant consequences, such as congestion, an overwhelmed host, looping, illegal access to data, & network partition.
- Two types of routing table poisoning attacks are the link attack and the router attack.

(3) Packet-Mistreatment Attacks:

- A packet-mistreatment attack can occur during any data transmission. A hacker may capture certain data packets & mistreat them. This type of attack is very difficult to detect.
- The attack may result in congestion, lowering, throughput, & denial-of-service attacks.
- can be subclassified into link attacks & router attacks. The link attack causes interruption, modification, or replication of data packets.

(4) Denial-of-Service Attacks:

- A denial-of-service attack is a type of security breach that prohibits a user from accessing normally provided services.
- The denial of services does not result in info" theft or any kind of info" loss but can nonetheless be very dangerous, as it can cost the target person a large amount of time & money.
- Usually, a denial of service attack affects a specific network service such as e-mail / DNS.

2) Discuss ~~case~~ in detail about RSA algorithm.

→ • In the RSA scheme, the key length is typically 512 bits. which requires an enormous computational power. A plaintext is encrypted in blocks, with each block having a binary value less than some number n.

- Encryption & Decryption are done as follows beginning with the generation of a public key and a private key.

Begin Key Generation Algorithm:

1. choose two roughly 256-bit prime no's, a & b, and define n = ab
2. Find x. Select encryption key x such that x and (a-1)(b-1) are relatively prime.
3. Find y. Calculate decryption key y.
   $xy \bmod (a-1)(b-1) = 1$
4. At this point a & b can be discarded.
5. the public key = (x, n)
6. the private key = (y, n)

- In this algorithm, x and n are known to both sender & receiver, but only the receiver must know y. Also a & b must be large & about the same size & both greater than 1.024 bits. The larger these two values, the more secure the encryption.

* Encryption: $C = m^x \bmod n$
* Decryption: $m = C^y \bmod n$

3) Explain SHA algorithm in detail.

→ The Secure Hash Algorithm (SHA) was proposed as part of the digital signature standard. SHA-1, the 1st version of this standard, takes messages with a maximum length of 2^{24} and produces 160 bit digest. With this algm, SHA-1 uses 5 registers, R1 through R_5, to maintain a "state" of 20 bytes.

- The first step is to pad a message m with length lm. The message length is forced to $lm = 448 \bmod 512$. In other words the length of the padded message becomes 64 bits less than the multiple of 512 bits

- The no. of padding bits can be as low as 1 bit and as high as 512 bits.
- After padding the 2nd step is to extend each block of 512-bit (16 32 bits) words $\{m_0, M_1 \ldots M_{15}\}$ to words of 80 32 bits using:

$w_i = m_i$ for $0 \le i \le 15$

And

$w_i = w_{i-3} \oplus w_{i-8} \oplus w_{i-14} \oplus w_{i-16} \lhd j$ for $16 \le i \le 79$

where $\lhd j$ means left Rotation by j bits. This way, bits are shifted several times & the incoming block is mixed with the state. Next bits from each block of w_i are mixed into the state in four steps, each maintaining 20 rounds. For any values of a, b & c and bit no. i, we define a function $F_i(a,b,c)$ as follows:

$$F_i(a,b,c) = \begin{cases} (a \wedge b) \vee (a \wedge c) & 0 \le i \le 19 \\ a \oplus b \oplus c & 20 \le i \le 39 \\ (a \wedge b) \vee (a \wedge c) \vee (b \wedge c) & 40 \le i \le 59 \\ a \oplus b \oplus c & 60 \le i \le 79 \end{cases}$$

Then the 80 steps ($i = 0, 1, 2 \ldots 79$) of the 4 rounds are described as follows:

$S = (R_1 \lhd 5) + F_i(R_2, R_3, R_4) + R_5 + w_i + C_i$

$R_5 = R_4$

$R_4 = R_3$

$R_3 = R_2 \lhd 30$

$R_2 = R_1$

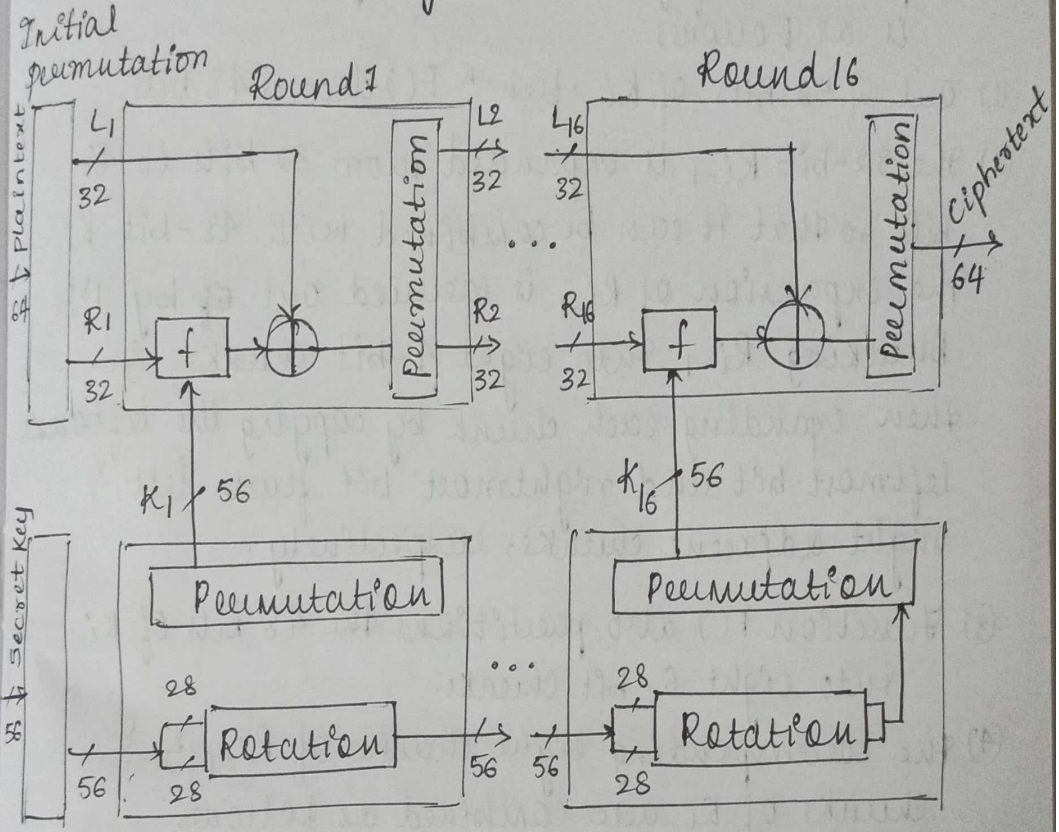
$R_1 = S.$

where C_i is a constant value specified by the standard for round i. The message digest is produced by concentration of the values in R_1 through R_5.

4. Demonstrate DES with a neat block diagram.

→ With the Data Encryption Standard (DES), plaintext messages are converted into 64 bit blocks, each encrypted using a key. The key length is 64 bits but contains only 56 usable bits. Thus, the last bit of each 8 byte in the key is a parity bit for the corresponding byte.

- DES consists of 16 identical rounds of an operation as shown in Fig below:



Begin DES Algorithm:

1. Initialize - Before round 1 begins, all 64 bits of an incoming message and all 56 bits of the secret key are separately permuted.
2. Each incoming 64-bit message is broken into two 32-bits halves denoted by L_i & R_i.
3. The 56 bits of the key are also broken into two 28-bit halves, and each half is rotated one/two bits positions, depending on the round.
4. All 56 bits of the key are permitted, producing version K_i of the key on round i.

5. In this stage, is a logic-Exclusive-OR, & the description of func^n F() appears next. Then Li & Ri are determined by:

$L_i = R_{i-1}$

and

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

6. All 64 bits of a message are permuted. The operation of func^n F() at any round i of DES is as Follows:

(1) Out of 52 bits of Ki, func^n F() chooses 48 bits.

(2) The 32-bit R_{i-1} is expanded from 32 bits to 48 bits so that it can be combined with 48-bit Ki. The expansion of R_{i-1} is carried out by 1st breaking R_{i-1} into eight 4-bit chunks & then expanding each chunk by copying the leftmost bit and rightmost bit from left & right adjacent chunks, respectively.

(3) Function F() also partitions the 48 bits of Ki into eight 6-bit chunks.

(4) The corresponding eight chunks of R_{i-1} & 8 chunks of Ki are combined as follows:

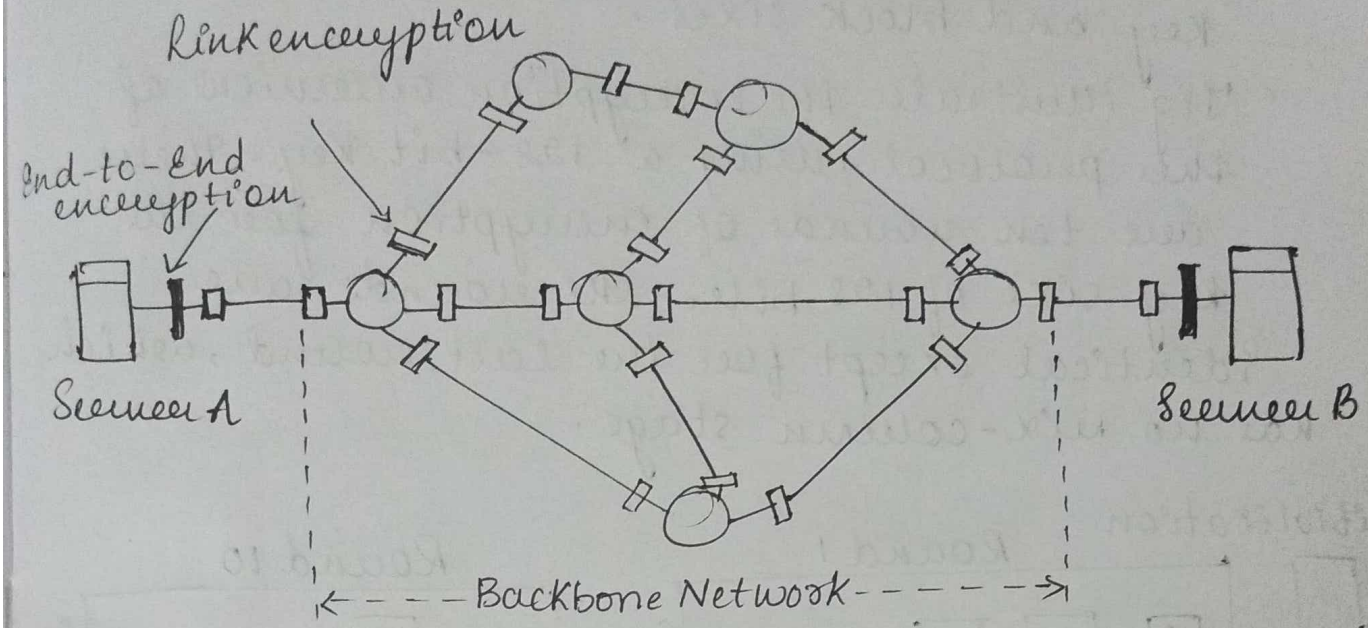
$R_{i-1} = R_{i-1} \oplus K_i$.

5? Discuss about cryptographic attacks and its drawback.

→ Cryptography is the process of transforming a piece of information or message shared by two parties into some sort of code. The message is scrambled before transmission so that it is undetectable by outside watchers. This kind of message needs to be decoded at the receiving end before any futher processing.

In computer communication networks, data can travel b/w 2 users while it is encrypted. In Fig below 2 senders are exchanging data while two types of encryption devices are installed in their communication network.

- In this Fig, sender A encodes its data, which can be decoded only at the other end sender.



- The 2 types of encryption techniques are secret-key encryption & public-key encryption. In a secret key model, both sender & receiver conventionally use the same key for an encryption process. In a public key model; a sender & a receiver each use a different key.

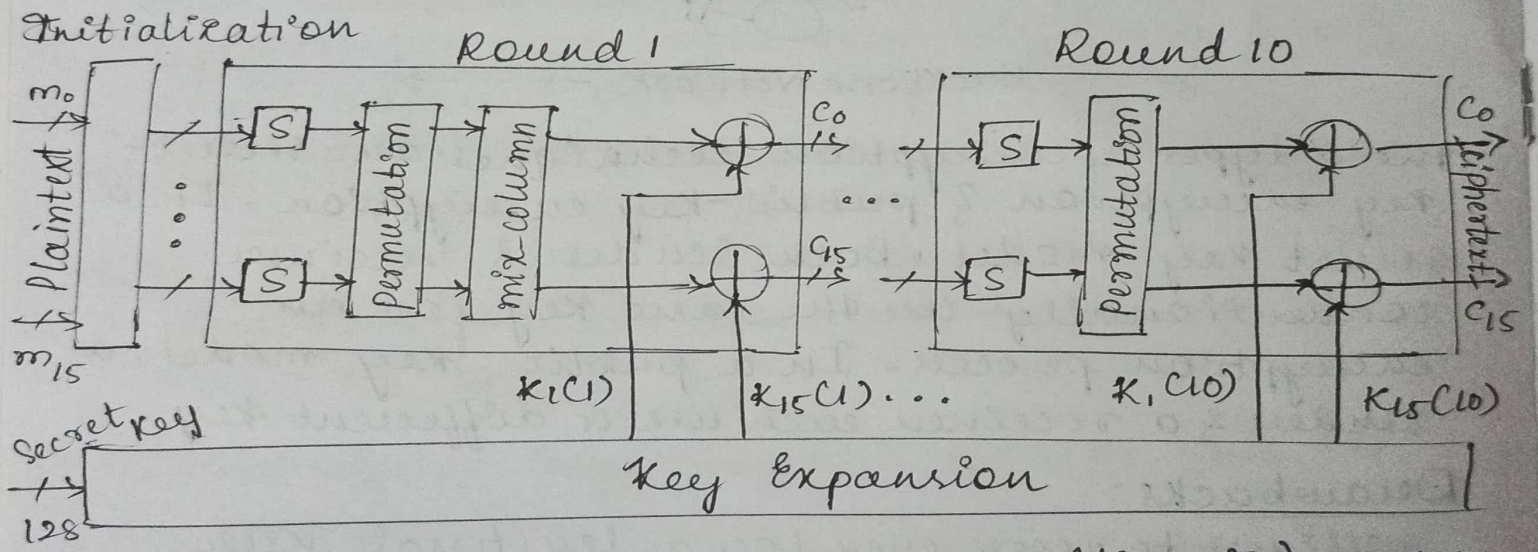
Drawbacks:

- difficult to access even for a legitimate user.
- high availability causes security issues.
- Selective access control. Security can't be realized.
- doesn't guard against the vulnerabilities & threats that emerge from the poor design of systems.
- Cryptography comes at cost. The cost is in terms of time & money.

6) Explain Advanced Encryption Standard algorithm in detail.

→ The AES protocol has a better security strength than DES. AES supports 128 bit symmetric block messages & uses 128-192, or 256 bits keys. The no. of rounds in AES is variable from 10 to 14 rounds; depending on the key and block sizes.

- Fig illustrates the encryption overview of this protocol, using a 128-bit key. There are ten rounds of encryption for the key size of 128 bits. All rounds are identical except for the last round, which has no mix-column stage.



- A single block of 128-bit plaintext (16 bytes) as an input arrives from the left. The plaintext is formed as 16 bytes m_0 through m_{15} & is fed into round 1 after an initialization stage. In this round, substitute units - indicated by S in the fig - perform a byte-by-byte substitution of blocks.

- The ciphers in the form of rows & columns move through a permutation stage to shift rows to mix columns.
- At the end of this round, all 16 blocks of ciphers are Exclusive-ORed with the 16 bytes of round 1 key $K_0(1)$ through $K_{15}(1)$.
- The 128 bit key is expanded for 10 rounds.
- The AES decryption algm is fairly simple & is basically the reverse of the encryption algm at each stage of a round. All stages of each round are reversible.

Module 5:

1) List the various properties of audio & video.

→ Properties of Video:

* Most salient characteristic of video is its high bit rate.
  - video streaming consumes most bandwidth, having a bit rate of more than 10 times greater than that of the normal HTTP & music-streaming applications.

* video can be compressed-
  - A video is a sequence of images, typically being displayed at a constant rate.
  - there are two types of redundancy in video, both of which can be exploited by video compression.

* Spatial redundancy - is the redundancy within a given image.
  - can be efficiently compressed without significantly sacrificing image quality.

* Temporal redundancy reflects repetition from image to subsequent image.

- We can also use compression to create multiple versions of the same video, each at a different quality level.

→ properties of Audio:

* Digital audio has significantly lower bandwidth requirements than video.
* Analog audio can be converted to a digital signal using pulse code modulation ~~(PCM)~~ data
* PCM-encoded speech and music, however are rarely used in the Internet. Instead, as with video, ~~compression techniques for near CD-quality~~ compression techniques are used to reduce the bit rates of the stream.
* A popular compression technique for near CD-quality stereo music is MPEG 1 layer 3, more commonly known as MP3.
* MP3 encoders can compress to many different rates: 128 Kbps is the most common encoding rate & produces very little sound degrading.
* As with video, multiple versions of a prerecorded audio stream can be created each at a different bit rate.

2) Explain the UDP streaming and HTTP streaming.

→ UDP streaming:

- With UDP streaming, the servers transmits video at a rate that matches the client's video consumption rate by clocking out the video chunks over UDP at a steady rate.

- eg: If the video consumption rate is 2Mbps and each UDP Packet carries 8,000 bits of video, then the server would transmit one UDP packet into its socket every (8000 bits)/(2 Mbps) = 4 msec.
- UDP does not employ a congestion-control mechanism, the server can push packets into the network at the consumption rate of the video without the rate-control restrictions of TCP.
- The client & server also maintain, in parallel a separate control connection over which the client sends commands regarding session state changes. The Real-time Streaming Protocol is a popular open protocol for such a control connection.

→ HTTP streaming:

- In HTTP streaming, the video is simply stored in an HTTP server as an ordinary file with a specific URL.
- When a user wants to see the video, the client establishes a TCP connection with the server & issues an HTTP GET request for that URL.
- The server then sends the video file, within an HTTP response message, as quickly as possible, that is, as quickly as TCP congestion control & flow control will allow.
- On the client side, the bytes are collected in a client application buffer. Once the no. of bytes in this buffer exceeds a predetermined threshold, the client application begins playback - specifically, it periodically grabs video frames from the client applica-tion buffer, decompresses the frames,

& displays them on the user's screen.

4) Explain Content Distribution Network.

→ • Streaming stored video to locations all over the world providing continuous playout & high interactivity is clearly a challenging task.

- For a Internet video company, the most straightforward approach to providing streaming video service is to build a single massive data center which stores all of its videos in the data center, & ~~the~~ ~~was~~ stream the videos directly from the data center to clients worldwide.
- But this approach face some problems:
  - Single massive data ~~to~~ center is single point of failure.
  - It leads long path to distant clients.
  - It may create network congestion.
- In order to meet the challenge of distributing massive amounts of video data to users distributed around the world, almost all major video-streaming companies make use of ~~CDNS~~ CDN.
- The CDN may be a private CDN, that is owned by the content provider itself. for eg: Google's CDN distributes Youtube videos & other types of content.
- CDN's typically adopt 2 diff. server placement philosophies:-(1) Enter Deep
  (2) Bring Home.