Assignment-I

First sessional question paper

Q2 Answer the following Question

1) IEEE 802.11 defines nines services that need to be provided by the wireless LAN to achieve functionality equivalent to that which is inherent to wired LANs

* Following Table lists the services and indicates two ways of categorizing them

2) The Service provider can be either the station or the DS. Station service are implements in an AP or in another special-purpose device attached to the distribution System.

2) Three of the services are used to control IEEE 802.11 LAN access and confidentiality Six of the services are used to support - delivery of MSDU's between Stations

3) If the MSDU is too large to be transmitted in a single MPDU, it may be fragmented and transmitted in a series of MPDU's

IEEE 802.11 Services

Service	Provider	Used to support
Association	Distribution system	MSDU Delivery
Authentication	Distribution system	LAN access & Security
Deauthentication	Station	LAN access & Security
Disassociation	station	MSDU Delivery
Distribution	Distribution System	MSDU Delivery
Integration	Distribution system	MSDU Delivery
MSDU dilvery	Distribution System	MSDU Delivery
Privacy	Station	LAN access & Security
Reassociation	Distribution system	MSDU delivery

=> Distribution of messages within a DS distribution and integration are used for distribution of message.

=> Distribution is the primary service to exchange MPDU's when the MPDU's must traverse the DS to get from a station in one BSS to a station in another BSS

3) For example. Suppose a frame is to be sent from station 2 to station 7. The frame is sent from STA2 to AP1, which is the AP for this BSS.

2) The AP gives the frame to DS, which has job of directing the frame to the AP associated with STA7 in the target BSS

4) AP 2 recives the frame and forwards it to STA7. How the message is transported through the DS is left the scope of IEEE 802.11 standard.

2) The Integration service
* Transfer of message between IEEE 802.11 LAN and a station an integration IEEE 802.11 LAN

Here Integrated means a wired LAN counted to a DS and whose stations may be logically connected to the IEEE 803.11 LAN via Integration service

2) Association Related services

.) Distribution Service requires information about the stations with in the ESS, which is provided by association

.) Before distribution, service can deliver acceptdata to and from a station it must associated

2) No transition

o) A station is either stationary or moves only with in the direct communication range of the communicating stations of a single BSS.

2) BSS transition

o) Station movement from one BSS to another within the same ESS. Here, delivery of data to the station requires the addressing capability to recongized the new location of the station

2) ESS transition

o) Station movement from a BSS in one BSS to a BSS within another ESS. It is supported only if the station can move.

2) Association Related services

o) To deliver a message within a DS the distribution service needs to know whose the ~~dist~~ distribution station is located, the identity of the AP to deliver message

⇒ Association

- Establishes an initial association between a station and an AP

⇒ Reassociation

- Enable an established association between a station and an AP to another, allowing a mobile station to move from one BSS to another.

⇒ Desassociation

- A notification from either a station or an AP that an existing association is terminated. A station should give this notification before leaving an ESS or shutting down

B) Explain four IEEE 802.11i phase of the operation?

⇒ Following are four phases of operations for IEEE 802.11i

1) Discovery

- An AP uses messages called Beacons and probe responses to advertise its IEEE 802.11i Security policy.

- The STA uses these to identify an AP for a WLAN with which it wishes to communicate

2) Authentication

- During this phase, the STA and AS prove their identifies to each other

- The AP blocks non-authentication traffic between the STA and AS unit the authenticates transaction is succesful

- the AP does not participate in the authentication transaction other than forwading traffic between the STA and AS

3) key generation and Distribution

- the AP and the STA perform several operations that Cryptographic keys to be generated and placed on the AP the STA. frames are exchanged between the AP and STA only.

4) protected data Transfer

- Frames are exchanged between the STA and the end station through the AP

- As denoted by the shading and the encryption module icon, data transfer occurs between the STA and the AP only security is ~~the~~ not provided end-to-end.

5) Connection termination

⇒ The AP and STA exchange frames. During this phase, the secure connection is turn down and the connection is restored to the original state

6) Define five principles services provided by PGP?

- Five principles services provided by PGP

1) Authentication
- The sender creates a message
- SHA-1 is used to generate a 160-bit hashcode of the message
- The hash code is encrypted with RSA using the sender's private key, and the result is prepended to the message.
- The reciver uses RSA with the senders public key to decrypt and recover the hash code.

2) The Combination of SHA-1 and RSA provides an effective digited signature scheme
- As an alternative, signatures, can be generated using DS/SHA-1.
- Signature are appended with the messages in most of the cases but sometimes

2) Cofidentiality

- Confidentality is provided by encrypting messages to be transmitted or to be stored locally as files.

- In both cases, the symmetic encryption algorithm CAST-128 may be used

- Alternatively, IDEA or 3DES may be used. The 64-bit Cipher feedback (CFB) mode is used.

- A new symmetric key is generated as a random 128-bit number for each message, also called session key or one-time key.

- Session key is bounded with the message and transmitted. Its secured by receiver's public key.

3) Confidentiality and Authentication

- Both services may be used for the same message

- First, a signature is generated for the plaintext message and prepended to the message

- Then, the plaintext message plus signature is encrypted using CAST-128, and the session key is encrypted using RSA

- Authentave, the message can be encrypted first and then signature can be generated but note preferable if third party verification is to be done

4) Compression

- As a default, PGP compresses the message after applying the signature but before an encryption

- This has the effect benefiting of saving space both for email transmission and for the file storage

- The Compression would constain message has less than the original plaintext, cryptanalysis is more difficult

- The Compression algorithm used in ZIP, which is discribed in Appendix G

5) Email compalibilty

- When PGP is used, at least part of block to be transmitted is encrypted.
- If only the signature service is used then the message digest is encrypted.
- The scheme are used for this purpose is radix-64 conversion
- If the Confidentity service is used the message plus signature are encrypted

D) What are the reasons for explosive growth of PGP? Discuss in brief

- PGP has grown explosively and is how widely used. A number of reasons can be listed for this growth

- It is available free worldwide and is used on all platforms. The Commercial version comes with a vendor support.
- It is based on algorithms that extensively scheme and are public reviewed.
- It has a wide range of applicability from Corporations to Individuals wanting to communicate worldwide securly.
- It was not developed by nor is it controlled by, any governmental or standard organization.
- PGP is now on Internet standards track

Q3 Do as Directed.

A) Explain the CIA Triad of the security requirment what are the other additional Concepts that define security objectives?

1) Confidentiality

- Data Confidentiality
- Assures that private or confidential information is not made available or

disclosed to unauthorized individual

2) privacy

·) That individuals control or the influence what information related to them may be collected and stored and by whom and to whom that information may disclosed.

2) Integrity

·) Data Integrity

·) Assure that information and programs are changed only in a specified and authorized manner

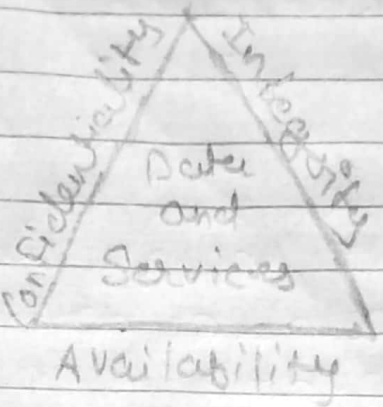
·) System Integrity

1) That a system performs intended function in an coripaired manner, free from deliberate or unathorized manipulation of System.

3) Availability

·) Assours that System works prompts and is not denied to authorized users

* CIA TRIAD



* Two other additional concepts are as follows

1) Authenticity
-) Verifying that users are who they say they are and that each input arriving at the system came from a trusted source.

2) Accountability
-) The security goal that generates the request for actions of an entity to be traced to that entity

B) Give the overview of Explain the Advanced Cryption Standard (AES) algrothim and describe the encryption and description process in detail?

1) In 1997 NIST issued a call for proposals for a new AES

2) Should have a security strength equal or better than 3DES and significatly improved efficenly

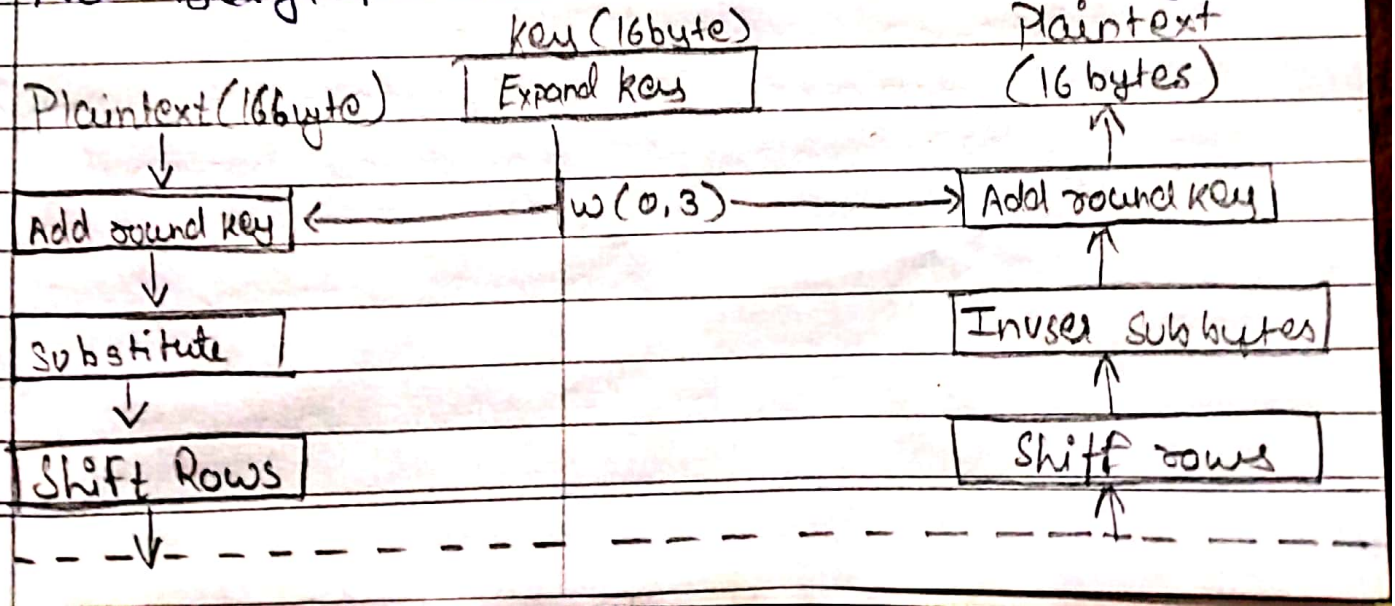
3) Must be a symmetic block Cipher with a block length of 128 bits and support for key lengths 128, 192 and 256 bits.

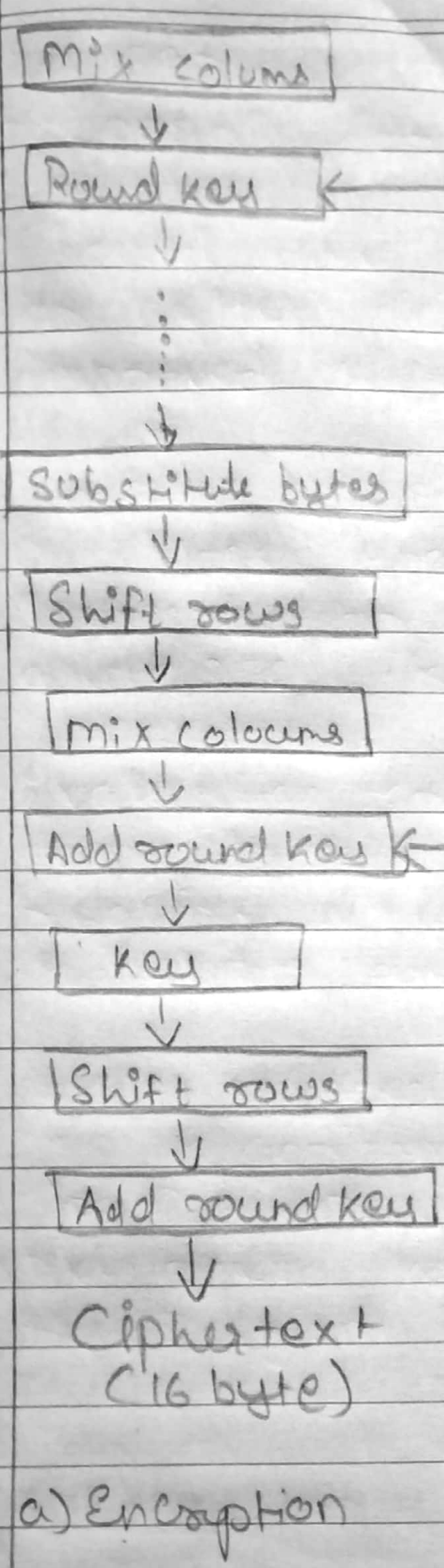
4) Evaluation criteria individual security. Computational efficienty, memory requirements, hardware and software suitability and flexibility.

5) NIST selected Rijndal as the proposed AES algorithm

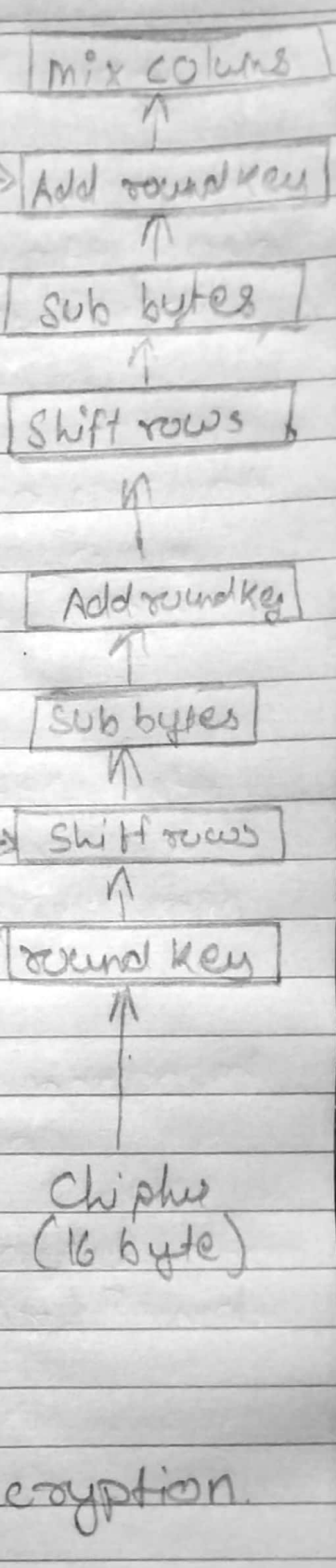
6) FIPS PUB 197

7) Developers has two Cryptographers from the Belgium Dr. Joan and Dr. Rijman





a) Encryption



b) Decryption

Q3) Do as Directed.

a) Explain the feisted Encryption structure and its rounds for encrption and desrption. Also discuss the time required for exhative key search for various key size and number of alternative keys?

1) Block size

- Larger block sizes mean greater security reduced encryption and desrption

2) Key size

- large key size means greater security but may d encryption and descrption on sped.

3) Number of rounds

- The essence of a symmetric block cipher is that a single round offer inadequate security but that multiple rounds in security.

4) subkey generation algorithm

- Greater complexity in this algorithm should lead to greater difficulty of the Cryptanalysis

5) Round function

·) Greater complexity generally means greater resistance to cryptanalysis

6) Fast software encryption & decryption

·) In many cases, encryption is embedd in applications or ability functions in ~~ash~~ such a way as to a hardware implementation accordingly to sped of execution.

7) Ease of analysis

·) If the alagorithm can be concisely and clearly explained, it is easier to analyze that algorithm for cryptanalytic vulnerabilities and there for develop a hyphr level of assces as to its ~~strength~~ strength.

Block size	key size	Number of Rounds	subkey alogrithm
Round function	Fast software encryption decryption		Ease of analysis

3) Give an overview of DES & 3DES algorithm?

DES: Data Encryption Standard

- Most widely used encryption scheme
- Issued in 1977 as federal Information processing standard 46 (FIPS 46) by National Institute of Standards and Techology (NIST)
- The algorithm itself is refered to as the Data Encryption Algorithm (DEA)

* DES Algorithm

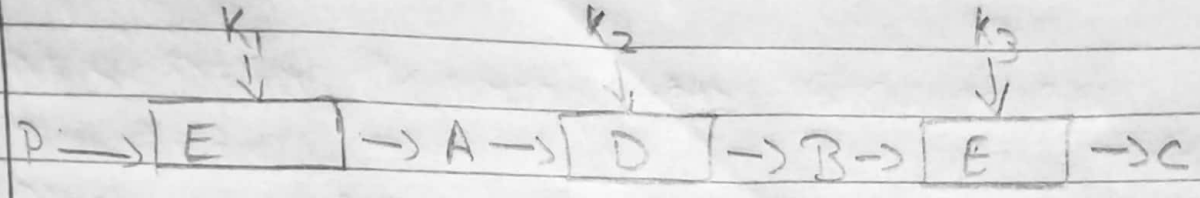
i) plaintext is 64 bits in length
ii) Key is a 56 bits in length
iii) Structure is a minor variation of the Feistal Network
iv) There are 16 rounds of processing
vi) process of description is same to process of encryption.

Strength of DES
1) Algorithm of ITSELF

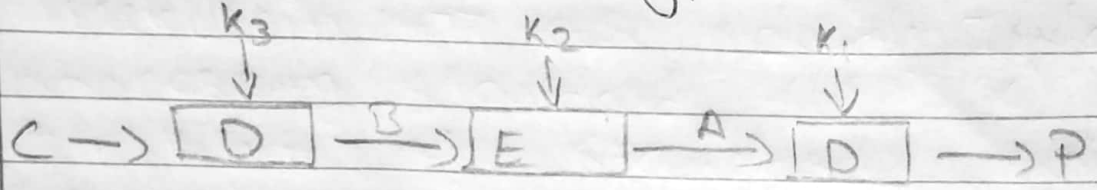
2) The case of a 56-bit key

* Triple DES

1)



a) Encryption



b) Decryption

Triple DES

i) Guidelines for 3DES

i) 3DES is the FIPS-approved symmetric encryption algorithm of choice

ii) Government organisations with legacy DES systems are encouraged to transition to 3DES