chapter-3
IP Security

- Use of IP security
- Component of IP security
- Working of IP security
- IPsec Architecture
- Difference between IPsec & SSL.

- Internet Protocol Security (IPSec)

> IPsec (Internet protocol security) is an Internet Engineering Task force (IETF) standard suite of protocols between two communication points across the IP network that provide data authentication, integrity and confidentiality.

> Internet Protocol Security (IPSec) is a network protocol suite that authenticates and encrypts the packets of data sent over a network.

> Internet Protocol security (IPSec) is a set of protocols that provide security for Internet protocol. It can use cryptography to provide security.

> IPsec can be used for the setting up of virtual private networks (VPNs) in a secure.

- Uses of IP security
  - To encrypt application layer data.
  - To provide security for routers sending routing data across the public internet.
  - To provide authentication without encryption, like to authenticate that the data originates from a known sender.
  - To protect network data by setting up circuits using IPsec tunneling in which all data being sent between the two endpoints is encrypted, as with VPN connection.

- Components of IP security:

  - Encapsulating security Payload (ESP)
  - Authentication Header (AH)
  - Internet key Exchange (IKE)

  - Encapsulating security Payload (ESP): It provides data integrity, encryption, authentication, and anti-replay. It also provides authentication for payload.

  - Authentication Header (AH): It also provides data integrity, authentication, and anti-replay and it doesnot provide encryption. The anti-replay protection protects against the unauthorized transmission of packets. It doesnot protect data confidentiality.

  - Internet key Exchange (IKE): It is a network security protocol designed to dynamically exchange encryption keys and find a way over Security Association (SA) between 2 devices. The security Association (SA) establishes shared security attributes between 2

network entities to support secure communication. The key Management Protocol (ISAKMP) and Internet Security Association provides a framework for authentication and key exchange.

- IPSec Mode
  1. Tunnel Mode
  2. Transport Mode.

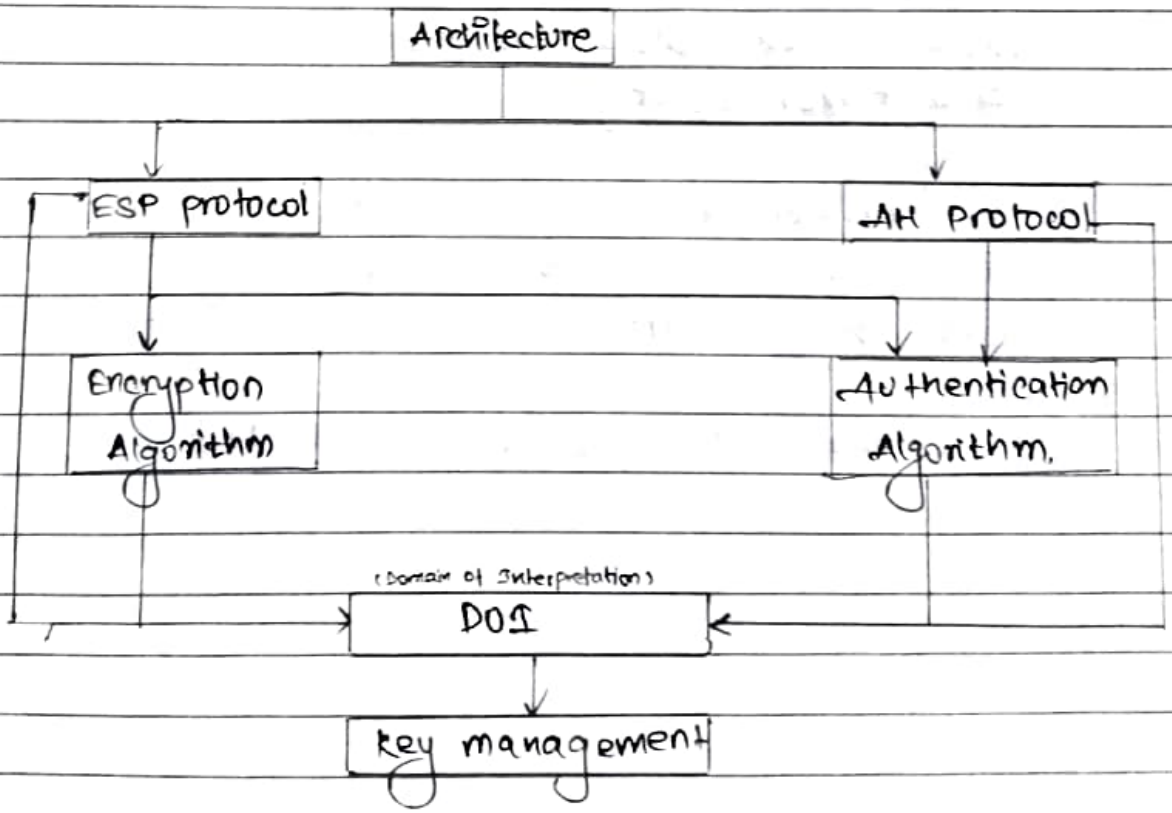
1) Tunnel Mode: This will take the whole IP packet to form secure communication between two places, or gateways.

2) Transport Mode: This only encapsulates the IP payload (not the entire IP packet as in tunnel mode) to ensure a secure channel of communication.

Architecture of IP security.

- IPsec architecture uses two protocols to secure the traffic or data flow. These protocols are ESP (Encapsulation security payload) and AH (Authetication Header).

- IPsec Architecture includes protocols, algorithms, DOI, and key Management. All these components are very important in order to provide the three main services.
  - Confidentiality
  - Authenticity
  - Integrity



Working on IP Security

- The host checks if the packet should be transmitted using IPSec or not. This packet traffic triggers the security policy for itself. This is done when the system sending the packet applies appropriate encryption. The incoming packets are also checked by the host that they are encrypted properly or n...
- The IKE phase 1 starts in which the 2 hosts (using IPSec) authenticate themselves to each other to start a secure channel. It has 2 modes. The main mode provides greater security and the Aggressive mode which enables the host to establish an IPSec circuit more quickly
- The channel created in the last step is then used to securely negotiate the way the IP circuit with encrypt data across the IP circuit
- Now, the IKE phase 2 is conducted over the secure

Remaining pdf

- Features of IPsec:

- Authentication: IPsec provides authentication of IP packets
- Confidentiality:
- Integrity
- Key management
- Tunneling
- Flexibility
- Interoperability

- Advantages of IPsec:

- Strong Security:
- Wide compatibility
- Flexibility
- Scalability
- Improved network performance

- Disadvantages of IPsec:

- Configuration complexity
- Compatibility issues
- Performance impact
- Key management
- Limited protection.

Virtual Private Network (VPN)

> A virtual private network extends a private network across a public network, and enables users to send and receive data across shared or public networks as if their computing devices were directly connected to the private network.

> Applications running across a VPN ~~over~~ may therefore benefit from the functionality, security and management of the private network.

> A fundamental requirement for VPN is security

> Use of a public network exposes corporate traffic to eavesdropping and provides an entry point for unauthorized users.

> To counter this problem, a VPN is needed. In essence, a VPN uses encryption and authentication in the lower protocol layers to provide a secure connection through an otherwise insecure network, typically the Internet.

> The most common protocol mechanism used for this purpose is at the IP level and is known as IPsec.

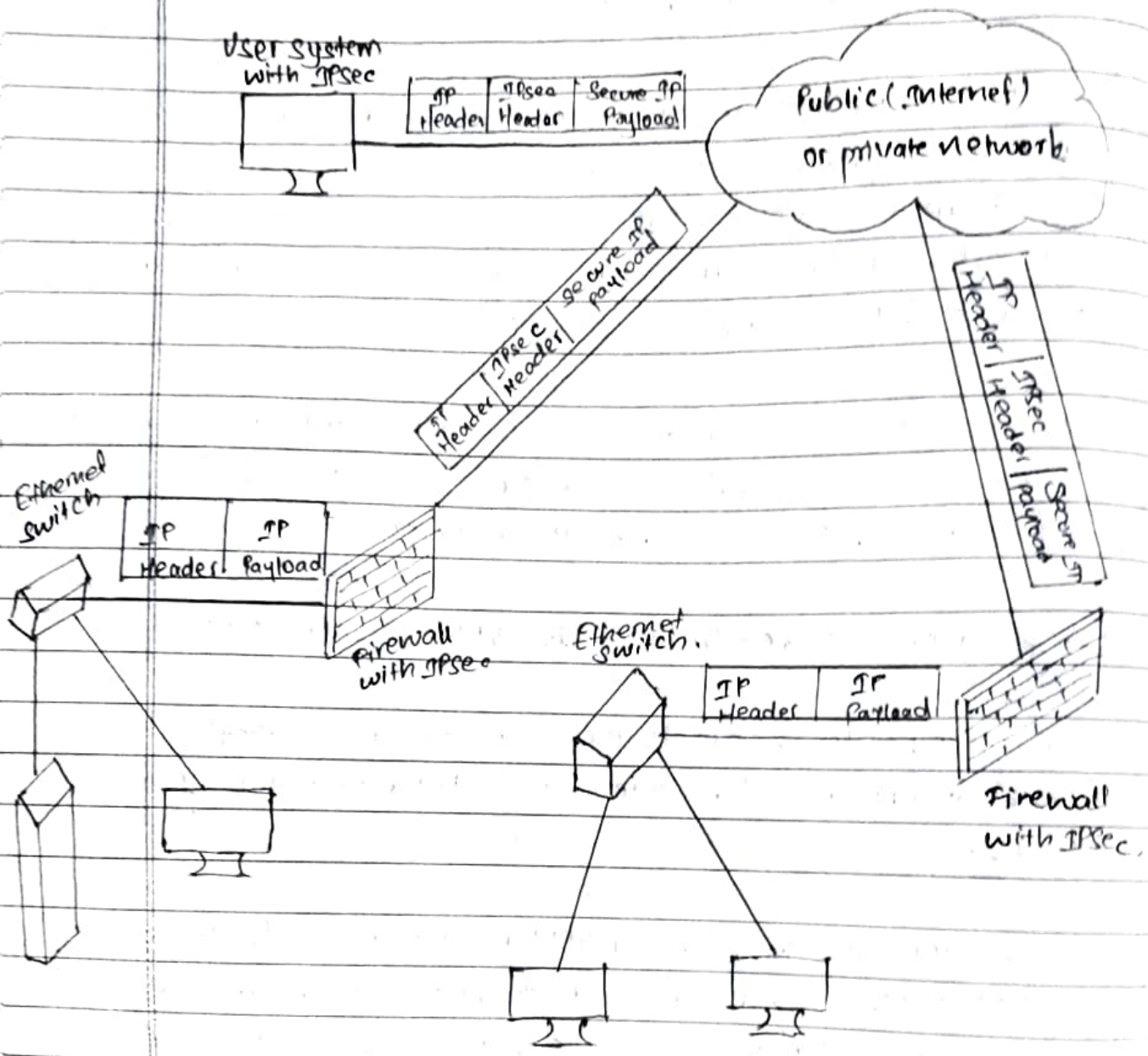


Fig: A VPN Security Scenario

chapter-4
Transport layer security

- Benefits of TLS
- Working of TLS
- Secure electronics transaction (SET) protocol
- Difference between secure Socket layer & Transport layer security
- Secure socket layer (SSL)

- Secure Socket layer (SSL):

> Secure sockets layer (SSL) is a standard protocol used for the secure transmission of documents over a network.

> Developed by Netscape, SSL technology creates a secure link between a web server and browser to ensure private and integral data transmission.

> SSL uses Transport Control Protocol (TCP) for communication.

> In SSL, the word socket refers to the mechanism of transferring data between a client and server over a network.

> When using SSL for secure Internet transactions, a web server needs an SSL certificate to establish a secure SSL connection

> SSL encrypts network connection segments above the transport layer, which is a network connection component above the program layer.

> SSL follows an asymmetric cryptographic mechanism, in which a web browser creates a public key and a private (secret) key.

> The public key is placed in a data file known as a certificate signing request (CSR). The private key is issued to the recipient only.

* Objectives of SSL are :
1) Data integrity
2) Data privacy
3) client - server authentication.

* Architecture of SSL.
- SSL is designed to make use of TCP to provide a reliable end-to-end secure service.
- SSL is not a single protocol but rather two layers of protocols.

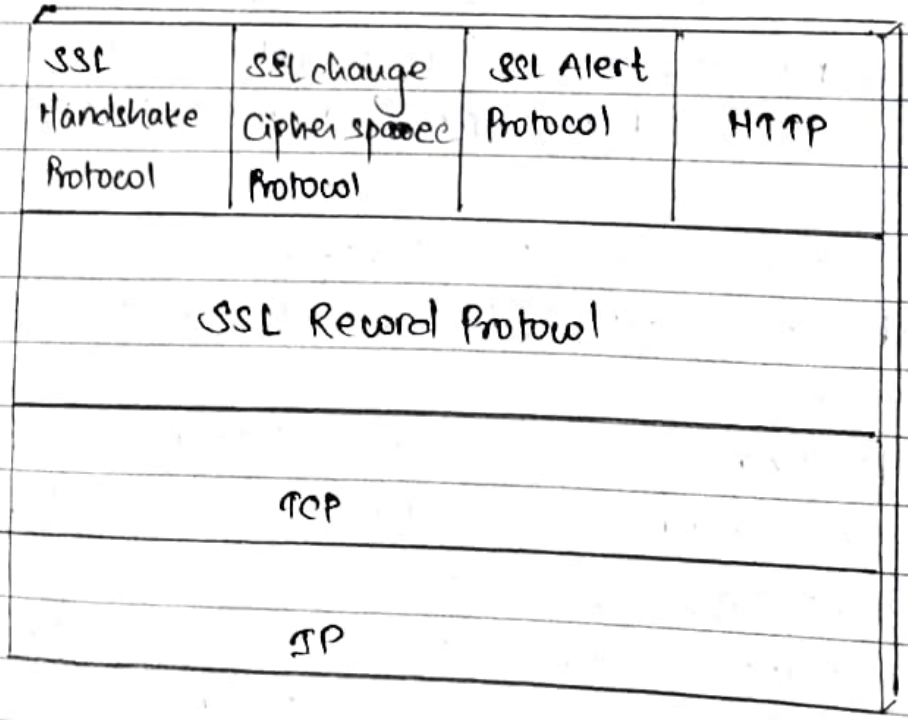


fig: SSL Architecture

- The SSL Record protocol provides basic security services to various higher layer protocols.

- In particular, the Hypertext Transfer Protocol (HTTP), which provides the transfer service for web client / server interaction, can operate on top of SSL.

- Three higherlayer protocols are defined as part of SSL: the handshake Protocol, The change Cipher Spec Protocol, and the Alert Protocol.

* Handshakinge protocol:
> This protocol allows the server and client to authenticate each other and to negotiate an encryption and MAC algorithm and cryptographic keys to be used to protect data sent in an SSL record.
> The Handshake protocol is used before any application data is transmitted.
> It consists of a series of messages exchanged by client and server.

* SSL Record Protocol:
The SSL Record Protocol provides two services for SSL connections:
- Confidentiality: The Handshake protocol defines a shared secret key that is used for conventional encryption of SSL payloads.
- Message Integrity: The Handshake protocol also defines a shared secret key that is used to form a message authentication code (MAC).

Change Cipher Spec Protocol:

> The change cipher spec protocol is one of the three SSL specific protocols that use the SSL Record Protocol, and it is the simplest.

> Cipher suite is a list that contains the combinations of cryptographic algorithms supported by the client, in decreasing order of preference.

> Each element of the list (each cipher suite) defines both a key exchange algorithm and a cipher spec.

SSL Alert Protocol:

> The Alert protocol is used to convey SSL related alerts to the peer entity.

> As with other applications that use SSL, alert messages are compressed and encrypted, as specified by the current state.

4-way handshaking process of SSL are:

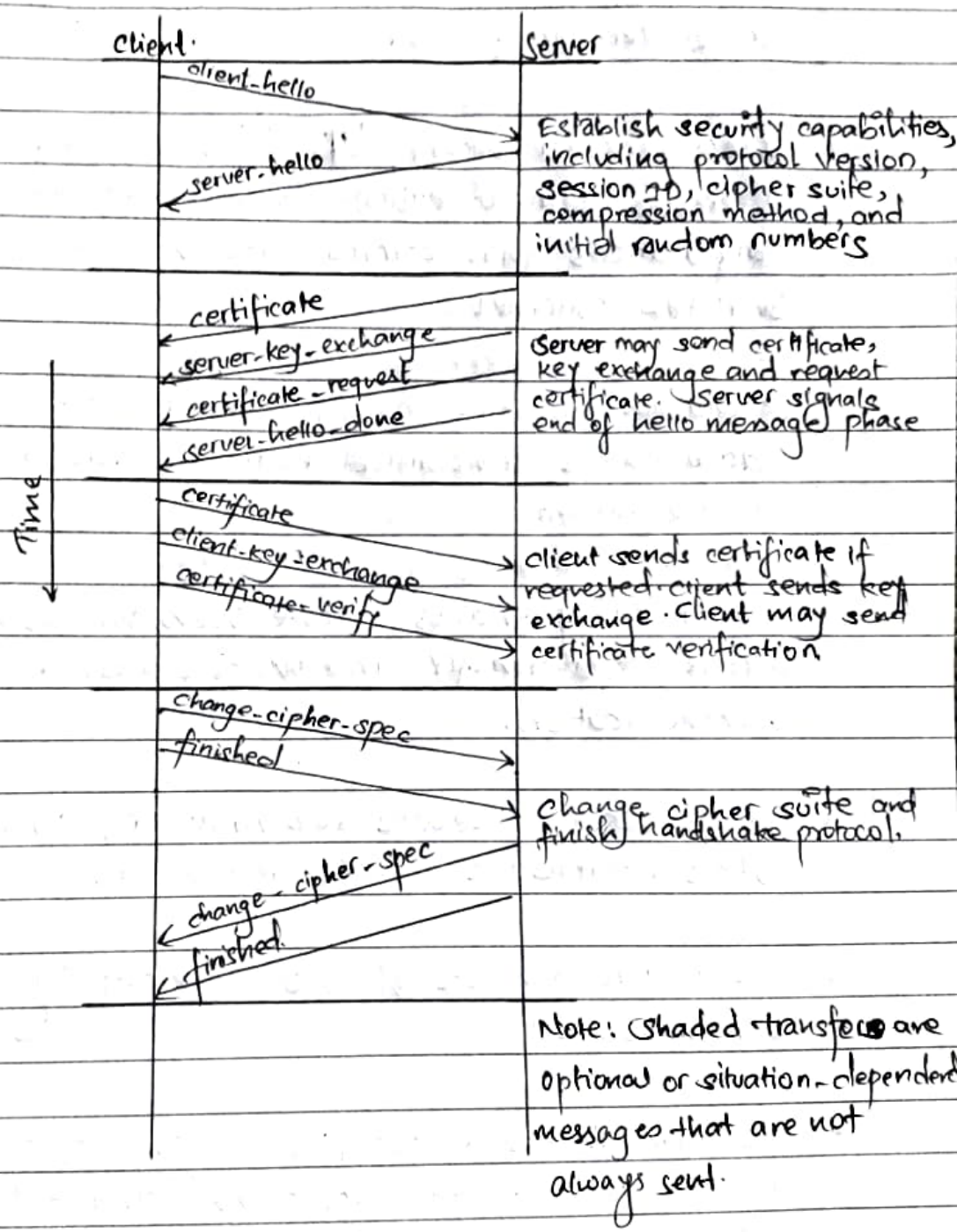


fig: Handshake protocol - Action.

* Transport Layer Security:

- TLS (Transport Layer Security) is just an updated, more secure, version of SSL.

- Transport Layer Security (TLS) is a protocol that provides communication security between client / server applications that communicate with each other over the Internet.

- It enables privacy, integrity and protection for the data that's transmitted between different nodes on the Internet.

- TLS primarily enables secure web browsing, application access, data transfer and most Internet-based communication.

- TLS is used to secure web browsers, web servers, VPNs, database servers and more.

- TLS protocol consists of two different layers of sub-protocols:

- TLS Handshake protocol: Enables the client and server to authenticate each other and select a encryption algorithm prior to sending the data

- TLS Record protocol: It works on top of the standard TCP protocol to ensure that the created connection is secure and reliable. It also provides data encapsulation and data encryption services.

H/W

- Benefit
- Working principle
- Compare TLS & SSL.

~~Shear: Shearing transformation~~

Secure Electronic Transaction:

- A secure electronic transaction (SET) is an open-source and cryptography-based protocol for secure payment processing via non-secure network.

- In 1996, SET was launched and backed by VISA, MasterCard & other payment processing industry leaders.

- SET's algorithm ensures data confidentiality, data integrity & ~~card~~ cardholder / merchant authentication.

- An SET system includes the following components.

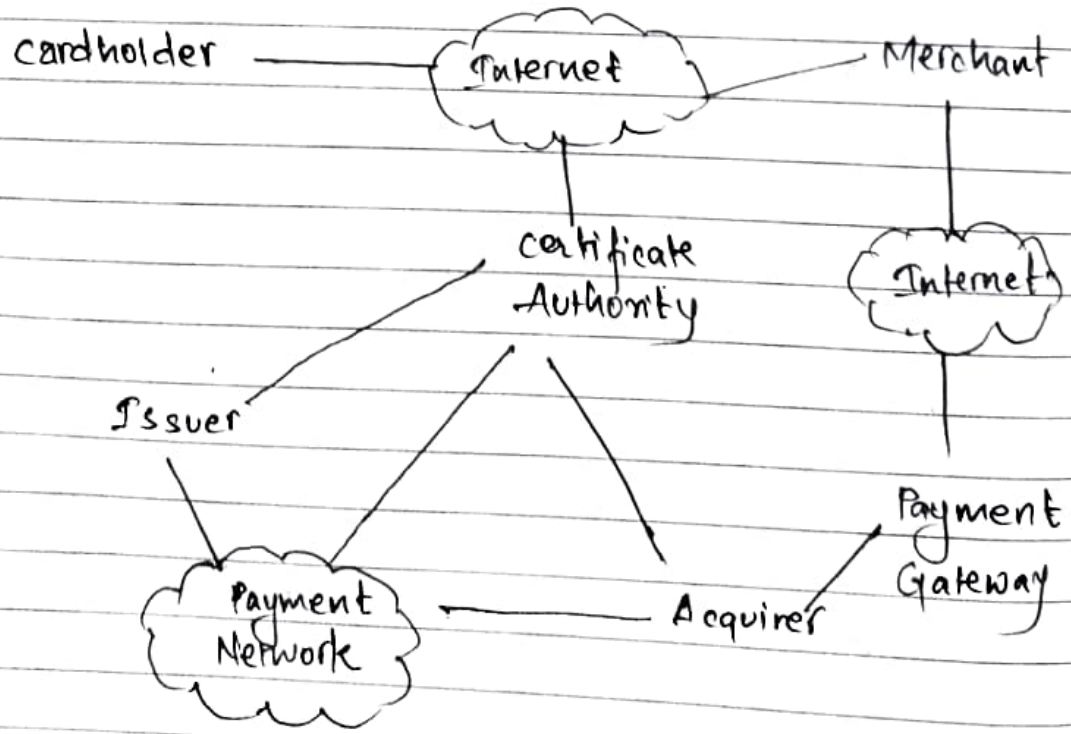


Fig: Participants in the SET System.

- Merchant
- Cardholder / acquirer
- card issuer
- Payment gateway
- certificateon authority (CA)
- Dual Signature : A guaranted SET data integrity innovation that links two different recipient messages

Working Principle:

- Assume that a customer has a SET-enabled browser and that the transaction provider (bank, store, etc) has a SET-enabled server.

- The customer opens a Mastercard or visa bank account. Any issuer of a credit card is some kind of bank.

- The customer receives a digital certificate. This electronic file functions as a credit card for online purchases or other transactions. It includes a public key with an expiration date. It has been through a digital switch to the bank to ensure its validity.

- Third-party merchants also receive certificates from the bank. These certificates include the merchant's public key and the bank's public key.

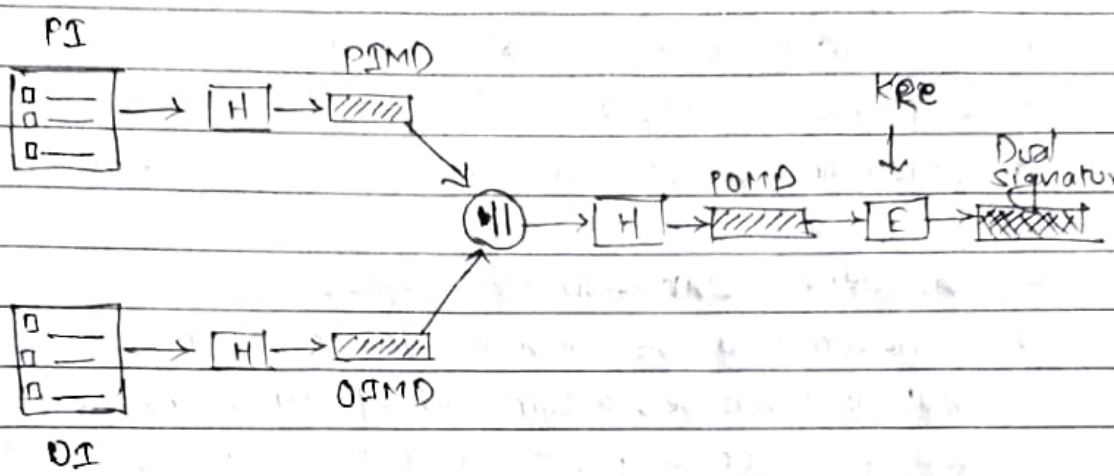
- The browser sends the order information. This message is encrypted with the merchant's public key, the payment information, which is encrypted with the bank's public key (which can't be read by the merchant), and information that ensures the payment can only be used with this particular

order

- The merchant verifies the customer by checking the digital signature on the customer's certificate.
- The merchant sends the order message along to the bank. This includes the bank's public key, the customer's payment information (which the merchant can't decode), and the merchant's certificate.
- The bank verifies the merchant and the message. The bank uses the digital signature on the certificate with the message and verifies the payment part of the message.
- The bank digitally signs and sends authorization to the merchant, who can then fill the order.

* Functions of SET:
- Dual Signature
- Payment Processing.

- Dual Signature:



PI = Payment Information
OI = Order Information
H = Hash function (SHA-1)
|| = concatenation

PIMD = PI message digest
OIMD = OI message digest
POMD = Payment Order message digest
E = Encryption (RSA)
KRe = Customer's private signature key

Fig: Construction of Dual signature.

Chapter-5

Intrusion Detection & Prevention System

- classification of Intrusion detection system
- Detection methods of IDS
- classification of Intrusion Prevention system
- Detection method of Intrusion prevention system
- Comparison of IPS with IDS
- Approaches to Intrusion detection & prevention.

* Intruders & Intrusion Techniques

- Intrusion is a phenomenon that performs an activity that compromises a computer system by breaking the security or causing it to enter into an insecure state.
- A set of attempts to compromise a computer or a computer network resource security is regarded as an intrusion.
- The entity involved to perform such activity is called intruder.
- Intruders are also refered as attackers, interceptors or hackers.

* Types of Intruders:

1) Masquerader
- An unauthorized user who penetrates a system's access control to exploit other's account.
- Most likely an outside to the system.

2) Misfeasor
- An legitimate user but accesses data, program or resources for which he/she is not authorized.
- Generally an insider

3) Clandestine
- An individual who seizes supervisory control and evades auditing and access control.
- May be an insider or outsider.

* Classification of Intrusion:
- Attempted break-in
- Masquerade attack
- Penetration of the security control system
- Leakage
- Denial of service
- Malicious use.

- Intrusion Detection

> In addition to security services (eg: data confidentiality, integrity, authentication, etc), intrusion detection (ID) techniques are used to strengthen the system security and increase its resistance to internal and external attacks.

> These techniques are implemented by an intrusion detection system (IDs).

> Generally, IDs main task is to detect an instrusion and, if necessary or possible to undertake some measures eliminating it.

The goals of intrusion detection system are:

> Detect a wide variety of instrusions.

> Detect instructions in a timely fashion.

> Present the analysis in a simple, easy-to-~~easy~~ understand format.

> Be accurate

- formalizing this type of analysis provides a statistical and analytical basis for monitoring a system for instructions.
- Three types of analyses - ~~normality~~ anamoly detection, misuse (or signature) detection, and specification detection.

Anamoly modeling:

- Anamoly detection analyzes a set of characteristics of the system and compares their behavior with a set of expected values.

- It reports when the computed statistics do not match the expected measurements.

- Anamoly detection uses the assumption that unexpected behavior is evidence of an intrusion.

- There are three different statistical models:

1) Threshold metric model:
> If, over a specific period of time, fewer than (minimum of) m or more than (maximum of) n events occur, the behavior is considered anomalous.
> Determining the threshold complicates use of this model.
> The threshold must take into account of differing levels of characteristics of the users.

2) Statistical moments model:
> The analyzer knows the mean and standard deviation (first two moments) and possibly other measures of correlation (higher moments).
> If values fall outside the expected interval for that moments the behavior that the values represent is considered anomalous.

3) Markov Model:
> Examine a system at some particular point in time.
> Events preceding that time have put the system into a particular state.
> When the next event occurs, the system transitions into a new state.
> Over a time, a set of probabilities of transition can

be developed.

> When an event occurs that causes a transition that has a low probability, the event is deemed anomalous.

> The anomalies are now no longer based on statistics of the occurrence of individual events, but on sequences of events.

> This approach promoted misuse detection and was used to develop effective anomaly detection mechanisms.

Misuse Modeling:

- Misuse detection determines whether a sequence of instructions being executed is known to violate the site security policy being executed.
- If so, it reports a potential intrusion.
- In some contexts, the term "misuse" refers to an attack by an insider or authorized user.
- In the context of intrusion detection systems, it means "rule-based detection."
- Modeling of misuse requires a knowledge of system vulnerabilities or potential vulnerabilities that attackers attempt to exploit.
- The intrusion detection system incorporates this knowledge into a rule set.

Specification Modeling:

- Specification-based detection determines whether or not a sequence of instructions violates a specification of how a program, or system, should execute. If so, it reports a potential intrusion.

- Anamoly detection has been called the art of looking for unusual states.

- Misuse detection, similarly, is the art of looking for states known to be bad.

- Specification detection takes the opposite approach; it looks for states known not to be good, and when the system enters such a state, it reports a possible intrusion.

⇒ Architecture of IDS:

- An intrusion detection system consists of three parts.
- The agent corresponds to the logger. It acquires

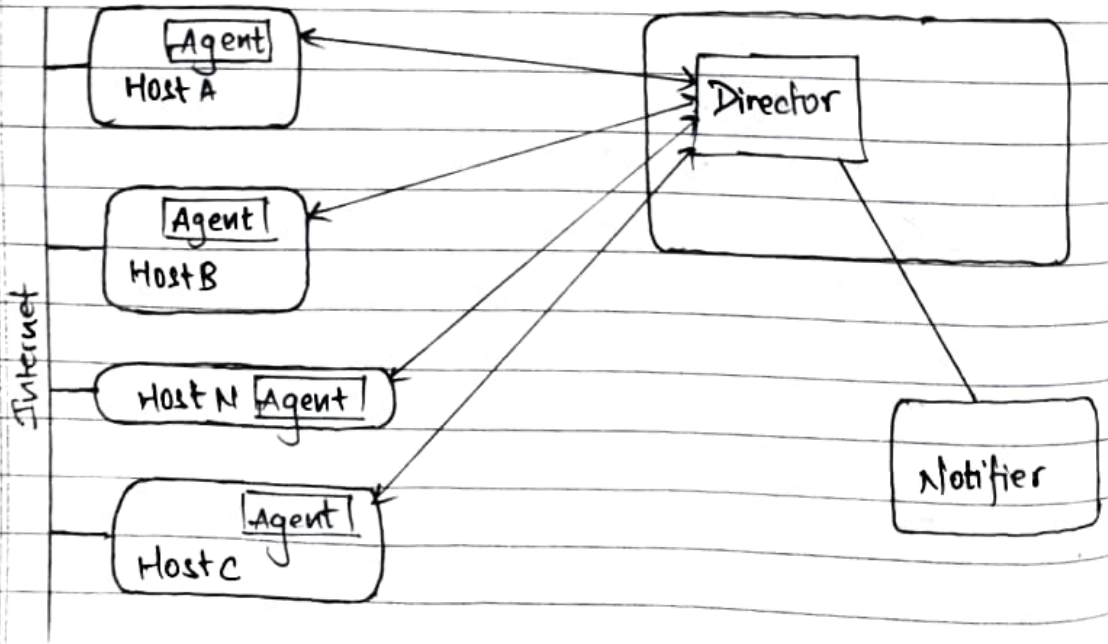


fig: Architecture of an intrusion detection system

Classwork:

plaintext: A B C I J K D E F M N Z
key: BIT
Calculate Cipher Text by using: a) playfair algorithm.
b) ceaser algorithm
.

a) Playfair algorithm:

Plain text: AB CI JK DE FM NZ

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

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

AB → CI
CI → BT
JK → BL
DE → EF
FM → MR
NZ → OY

b) Ceaser Algorithm

plaintext: ABCIJK DEF MN2

Key: 3.

ciphertext: DEFLMN GHI PQC

Agent:

- An agent obtains information from a data source (or set of data sources)
- The source may be a log file, another process, or a network.
- The information, once acquired, may be sent directly to the director.
- An agent can obtain information from a single host, from a set of hosts or from a network.

1) Host-based Information Gathering:

- Host-based agents usually use system and application logs to obtain records of events, and analyze them to determine what to pass to the director.
- The events to look for, and to analyze, are determined by the goals of the intrusion detection mechanism.
- The logs may be security-related logs or other logs such as accounting logs.

2) Network-Based Information Gathering:

- Network-based agents use a variety of devices and software to monitor network traffic.
- This technique provides information of a different flavor than host-based monitoring provides.
- It can detect network-oriented attacks, such as a denial of service attack introduced by flooding a network.
- It can monitor traffic for a large number of hosts. It can examine the content of the traffic itself (called content monitoring).
- Network-based agents may use network sniffing to read the network traffic.

3) Combining sources:

- The goal of an agent is to provide the director with information so that the director can report possible violations of the security policy (intrusions).
- An aggregate of information is needed. However, the information can be viewed at several levels.
- The agent, or the director, must either obtain information at the level of abstraction at which it looks for security problems or be able to map the information into an appropriate level.

Director:

The director itself reduces the incoming log entries to eliminate unnecessary and redundant records. It then uses an analysis engine to determine if an attack (or the precursor to an attack) is underway.

- The analysis engine may use any of, or a mixture of, several techniques to perform its analysis.
- Because of functioning of the director is critical to the effectiveness of the intrusion detection system, it is usually run on a separate system.
- This allows the system to be dedicated to the director's activity.
- It has the side effect of keeping the specific rules and profiles unavailable to ordinary users.
- Then attackers lack the knowledge needed to evade the intrusion detection system by conforming to known profiles or using only techniques that the rules do not include.
- The director must correlate information from multiple logs.
- Many types of directors alter the set of rules that they use to make decisions.

- These adaptive directors alter the profiles, add (or delete) rules, and otherwise adapt to changes in the systems being monitored.

- Typical adaptive directors use aspects of machine learning or planning to determine how to alter their behavior

- Directors rarely use only one analysis technique, because different techniques highlight different aspects of intrusions.

- The results of each are combined, analyzed and reduced, and then used.

* Types of Intrusion:

Monitoring Network Traffic for Intrusions: NSM

- The Network Security Monitor (NSM) ~~dev~~
Distributed Intrusion Detection System (DIDS)
AAFID (Autonomous Agent for Intrusion Detection Sys...

* Intrusion Response,

- Once an instrusion is detected, how can the system be protected?
- The field of intrusion response deals with this problem.
- It's goal is to handle the ~~attack in~~ (attempted) attack in such a way that damage is minimized (as determined by the security policy)
- Some intrusion detection mechanisms may be augmented to thwart instructions.
- Otherwise, the security officers must respond to the attack and attempt to repair any damage.

* Intrusion Handling

- When an intrusion occurs, the security policy of the site has been violated.
- Handling the intrusion means restoring the system to comply with the site's security policy and taking any actions against the attacker that the policy specifies.

- Intrusion handling consist of six phases:

1) Preparing to attacks: This step occurs before any attacks are detected. It establishes procedures and mechanisms for detecting and responding to attacks.

2) Identification of an attack: This triggers the remaining phases.

3) Containment (confinement) of the attack: This step limits the damage as much as possible.

4) Eradication of the attack: This step stops the attack and blocks further similar attacks.

5) Recovery from the attack: This step restores the system to a secure state (with respect to the site security policy).

6) Follow-up to the attack: This step involves taking action against the attacker, identifying problems in the handling of the incident, and recording lessons learned (or lessons not learned that should be learned).

* Intrusion prevention System:

> An Intrusion prevention system (IPS) is a cybersecurity tool that examines network traffic to identify potential threats and automatically take action against them.

> An IPS recognize and block malicious software or vulnerability exploits before they can move further into the network and cause damage.

> IPS tools continually monitor and log network activity in real time..

> An intrusion prevention system expands on the capabilities of intrusion detection systems, which are similar but less advanced tools.

> Unlike an IPS, and IDS can detect but not respond to malicious activity.

* Detection methods of Intrusion Prevention System

1) Signature-based detection: With this technique, the IPS scans for attack signatures of known network threats.

2) Anamoly-based detection: Using this technique, the IPS searches for unexpected network behavior.

3) Policy-based detection: This technique involves looking for activity that breaks enterprise security policies, which administrators establish in advance.

Types of Intrusion Prevention System

1) Network-based intrusion prevention system (NIPS): A NIPS scans all network traffic for suspicious activity.

2) Host-based intrusion prevention system (HIPS): A HIPS has a more limited scope than a NIPS, as it resides on a single host and analyzes only traffic there.

3) Wireless intrusion prevention systems (WIPS): A WIPS monitors wireless network traffic for signs of possible intrusion.

4) Network behavior analysis (NBA): NBA involves analyzing network behavior for abnormal traffic flows that might indicate issues such as DDoS attacks or malware.

IDS Vs IPS

Most organizations have either an IDS ~~and~~ or an IPS and many ~~both~~ have both as part of their security information and event management framework.

	IDS	IPS
Name	Intrusion Detection system	Intrusion prevention system
Description	A system that monitors network traffic for suspicious activity and alerts users when such activity is discovered.	A system that monitors network traffic and alerts for suspicious activity, like an IDS, but also takes preventative action against suspicious activity
location	A host-based intrusion detection system is installed on the client computer. A network-based intrusion detection system resides on the network.	located between a company's firewall and the rest of its network.
Use	warns of suspicious activity taking place, but it doesn't prevent it.	warns of suspicious activity taking place and prevents it.
False positive	IDS false positives are usually just a minor	IPS false positives can be more serious, when an

inconvenience. Although the IDS incorrectly labels legitimate traffic as malicious, it does not prevent the traffic from entering the network.

IPS mistakes legitimate traffic for a threat, it stops the legitimate traffic from entering the network, which would impact any part of the organization, not just the IT team.

Chapter 6: Wireless Network Security

- IEEE 802.11 Wireless LAN overview
- IEEE 802.11 Wireless LAN security
- Wireless Application protocol overview
- Wireless transport layer security
- WAP End to End security

IEEE 802.11 WIRELESS LAN OVERVIEW

- In 1990, the IEEE 802 committee formed a new working group, IEEE 802.11, with a charter to develop a protocol and transmission specifications for wireless LANs (WLANs)

- Sub-Topics
  - The Wi-Fi Alliance
  - IEEE 802 Protocol Architecture
  - IEEE 802.11 Network components and Architectural Model
  - IEEE 802.11 Services

The Wi-Fi Alliance

- The first 802.11 standard was 802.11b
- But problem of products from different vendors will successfully interoperate
- As solution, Wireless Ethernet Compatibility Alliance (WECA), an industry consortium, was formed in 1999.
- This organization, subsequently renamed the Wi-Fi (Wireless Fidelity) Alliance, created a test suite to certify interoperability for 802.11b products.
- Wi-Fi certification has been extended to 802.11g products. The Wi-Fi Alliance has also developed a certification process for 802.11a products, called Wi-Fi 5.
- Wi-Fi Alliance has developed certification procedures for IEEE 802.11 security standards, referred to as Wi-Fi Protected Access (WPA)
- WPA2, incorporates all the features of the IEEE 802.11i WLAN security specification.

IEEE 802.11 Terminology:

Access point (AP): Any entity that has station functionality and provides access to the distribution system via the wireless medium for associated stations.

Basic service set (BSS): A set of stations controlled by a single coordination function.

Coordination function: The logical function that determines when a station operating within a BSS is permitted to transmit and may be able to

receive PDUs.

Distribution system (DS): A system used to interconnect a set of BSSs and integrated LANs to create an ESS.

Extended service set (ESS): A set of one or more interconnected BSSs and integrated LANs that appear as a single BSS to the LLC layer at any station associated with one of these BSSs.

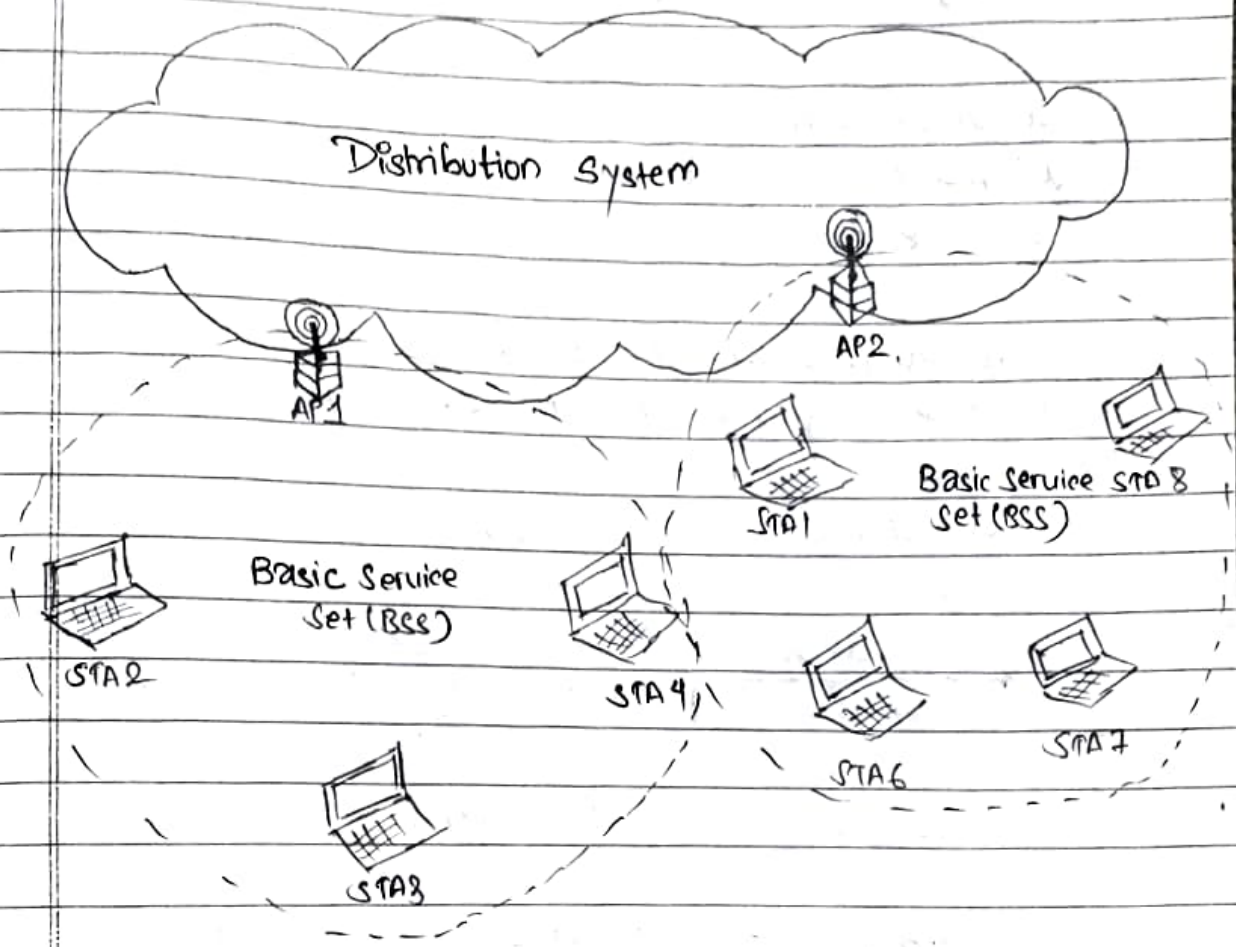
MAC protocol data unit (MPDU): The unit of data exchanged between two peer MAC entities using the services of the physical layer.

MAC service data unit (MSDU): Information that is delivered as a unit between MAC users.

Station: Any device that contains an IEEE 802.11 conformant MAC and physical layer.

Date
Page

IEEE 802.11 Network components and Architectural Model.



IEEE 802 Protocol Architecture.

Media Access Control Functionality:

- On transmission, assemble data into a frame, known as a MAC protocol data unit (MPDU) with address and error-detection fields.
- On reception, disassemble frame, and perform address recognition and error detection.
- Govern access to the LAN transmission medium.

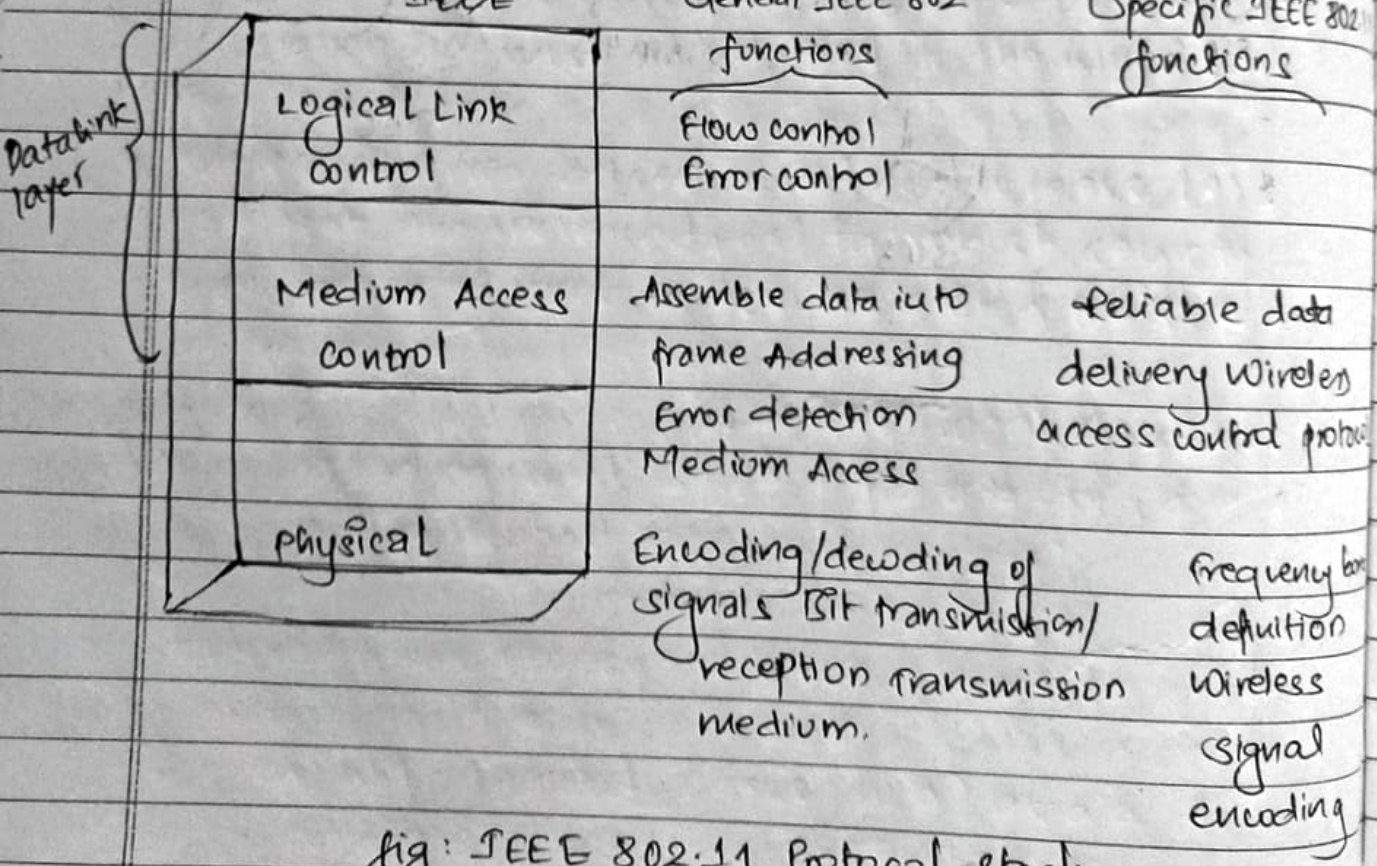


fig: IEEE 802.11 Protocol stack.

Date
Page

IEEE 802.11 services.

Service	Provider	Used to support
Association	Distribution system	MSDU delivery
Authentication	Station	LAN access and security
Deauthentication	Station	LAN access and security
Disassociation	Distribution system	MSDU delivery
Distribution	Distribution system	MSDU delivery
Integration	Distribution system	MSDU delivery
MSDU delivery	Station	MSDU delivery
Privacy	Station	LAN access and security
Reassociation	Distribution system	MSDU delivery

IEEE 802.11i Services

- Authentication
- Access Control
- Privacy with message integrity

IEEE 802.11i Wireless LAN Security

- There are two characteristics of a wired LAN that are not inherent in a wireless LAN.
  - In order to transmit over a wired LAN, a station must be physically connected to the LAN.
  - Similar, in order to receive a transmission from a station that is part of wired LAN, the receiving station also must be attached to the wired LAN.

- These differences between wired and wireless LANs suggest the increased need for robust security services and mechanisms for wireless LANs.

- Solution: Wired Equivalent Privacy (WEP) algorithm providing with security features for privacy and authentication.

- Problem: Weak Privacy

- Solution: WiFi Protected Access (WPA) as a Wi-Fi standard. According to 802.11i standard.

- The final form of the 802.11i standard is referred to as Robust Security Network (RSN).

- The Wi-Fi Alliance certifies vendors in compliance with the full 802.11i specification under the WPA2 program.

Robust Security Network (RSN)

Access Control	Authentication and key Generation	Confidentially, Data Origin Authentication and Integrity and Replay Protection.	
IEEE 802.1 Port-based Access control	Extensible Authentication protocol (EAP)	TKIP	CCMP

a) Services and protocols.

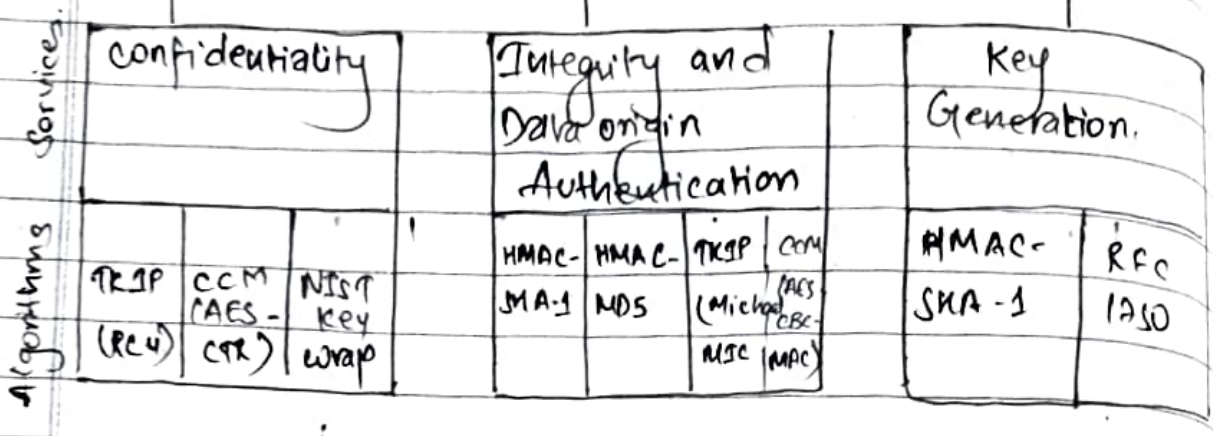
CBC-MAC = Cipher Block Chaining Message Authentication Code (MAC)

CCM = Counter Mode with Cipher Block Chaining Message Authentication code

CCMP = Counter Mode with Cipher Block Chaining MAC protocol

TKIP = Temporal key Integrity Protocol.

Robust Security Network (RSN)



b) Cryptographic algorithms.

IEEE 802.11i Phases of Operation

The operation of an IEEE 802.11i RSN has following possibilities.

1) Two wireless stations in the same BSS communicating via the access point (AP) for that BSS.

2) Two wireless stations (STAs) in the same ad hoc IBSS communicating directly with each other.

3) Two wireless stations in different BSSs communicating via their respective APs across a distribution system.

4) A wireless station communicating with an end station on a wired network via its AP and the distribution system.

- case 1 and case 2 security is provided but case 3 and case 4 security is provided but only between STA and its AP.

Solution: 5 phases of operation for an RSN and maps them to the network components involved.

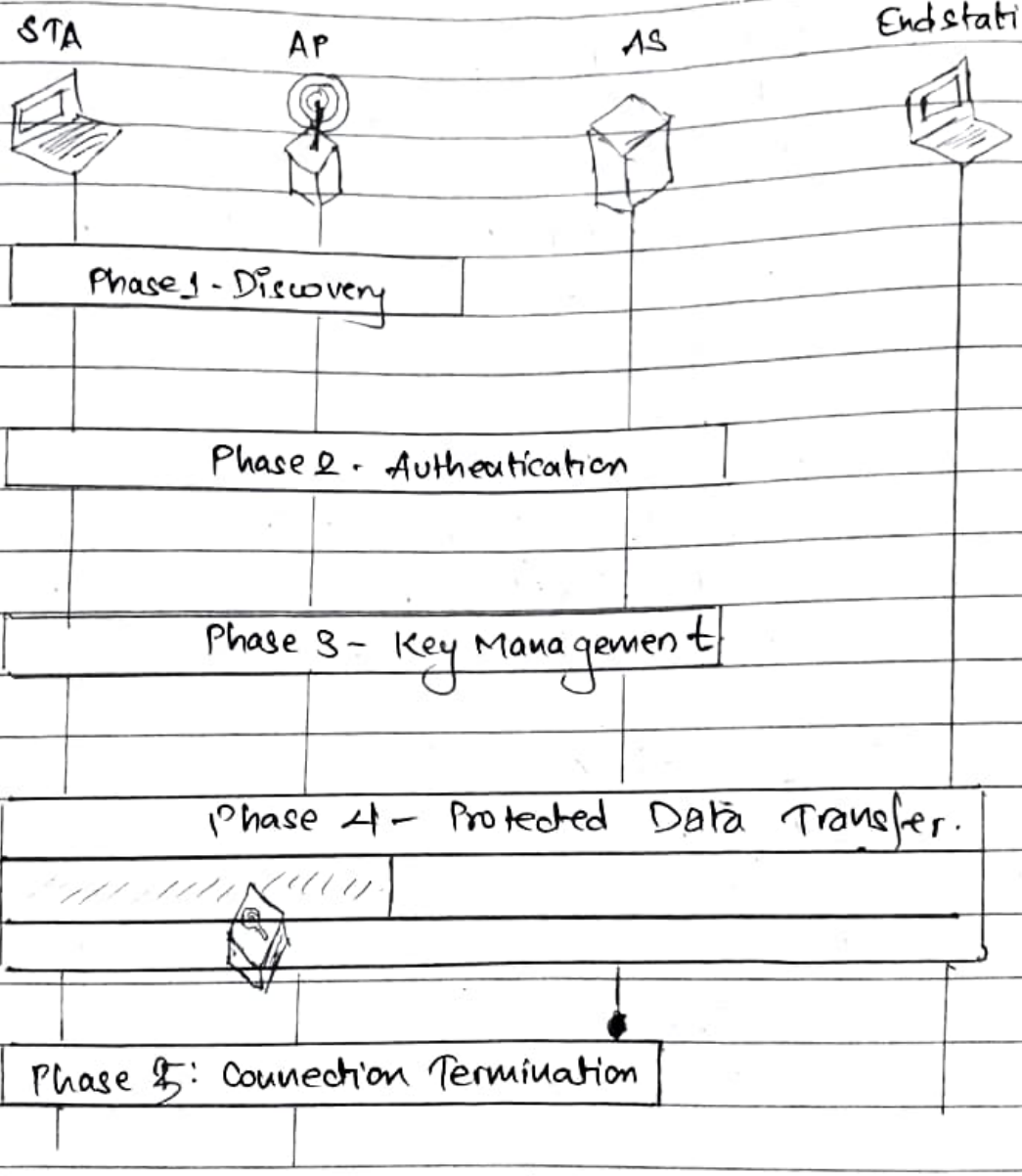


fig: IEEE 802.11i Phases of operation.

Wireless Application Protocol overview

- WAP is designed to work with all wireless network technologies (eg: GSM, CDMA and TDMA)
- WAP is based on existing Internet standards such as IP, XML, HTML, and HTTP as much as possible.
- Wireless Application Protocol (WAP) is a universal, open standard provide mobile users of wireless phones and other wireless terminals to provide access to telephony and information services, including the Internet and the web.
- The wireless devices have limited processors, memory, and battery life.
- The wireless networks are characterized by relatively low bandwidth, high latency, and unpredictable availability and stability compared to wired connections.
- WAP is designed to deal with these challenges.

The WAP specification includes.

- A programming model based on the WWW programming model.
- A markup language, the wireless markup language adhering to XML.
- A specification of a small browser suitable for a mobile wireless terminal.
- A lightweight communicates protocol stack.
- A framework of wireless telephony applications (WTA).

Date
Page

WAP Architecture.

- Next WAP architecture, illustrates the overall stack architecture implemented in a WAP client.
- HTTPs or WSP may provide the Hypermedia Transfer service.
- common services fall into two categories: a) security services and b) service discovery.

- Security services:
  - cryptographic library
  - Authentication
  - Identity
  - PKI (Public key Interface and cryptography)
  - Secure Transport (WTLS and TLS wireless Transport layer security)
  - Secure Bearer (IPv4 and IPv6 through IPSec)

- service Discovery:
  - EFI: the External Functionality Interface (EFI, discover external functions/services)
  - Provisioning (to access services)
  - Navigation discovery (allows a device to discover new network services (eg: secure pull proxies))
  - Service lookup (DNS lookup)

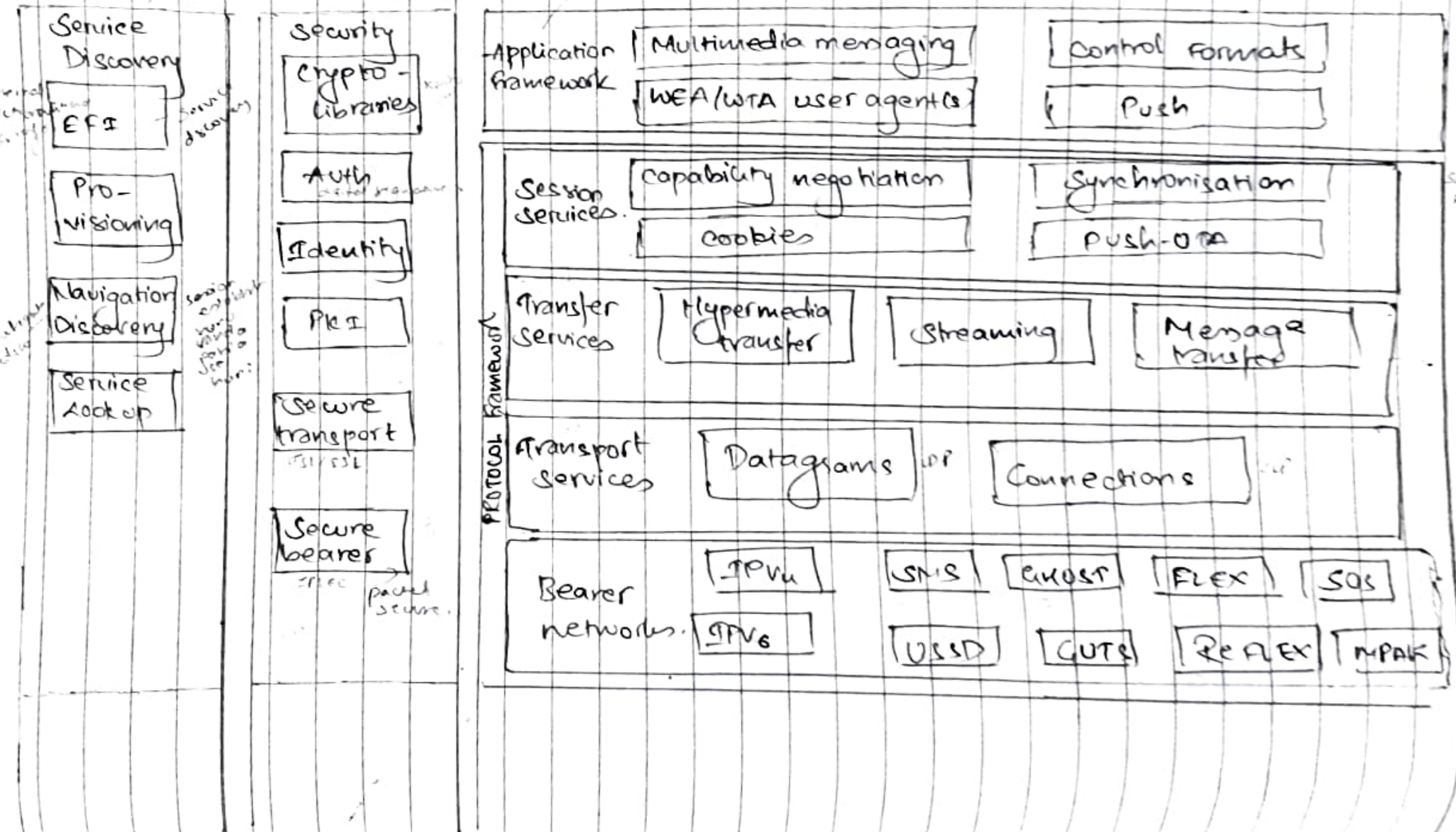


Fig: Architecture of WAP

Date
Page

Wireless Application Environment

- The WAE specifies an application framework for wireless devices (such as mobile telephones, pagers and PDAs.
- WAE consist of tools and formats to ease the task of developing application and devices supported by WAP.
- The major elements of the WAE model (figure in previous slide) are:
  - WAE user agents (functionality to display content)
  - Wireless telephony applications (WTA)
  - Standard content encoding
  - PUSH (Push-OTA push over the Air session service.
  - Multimedia messaging.

Wireless Transport Layer Security

* WAP End-to-End Security

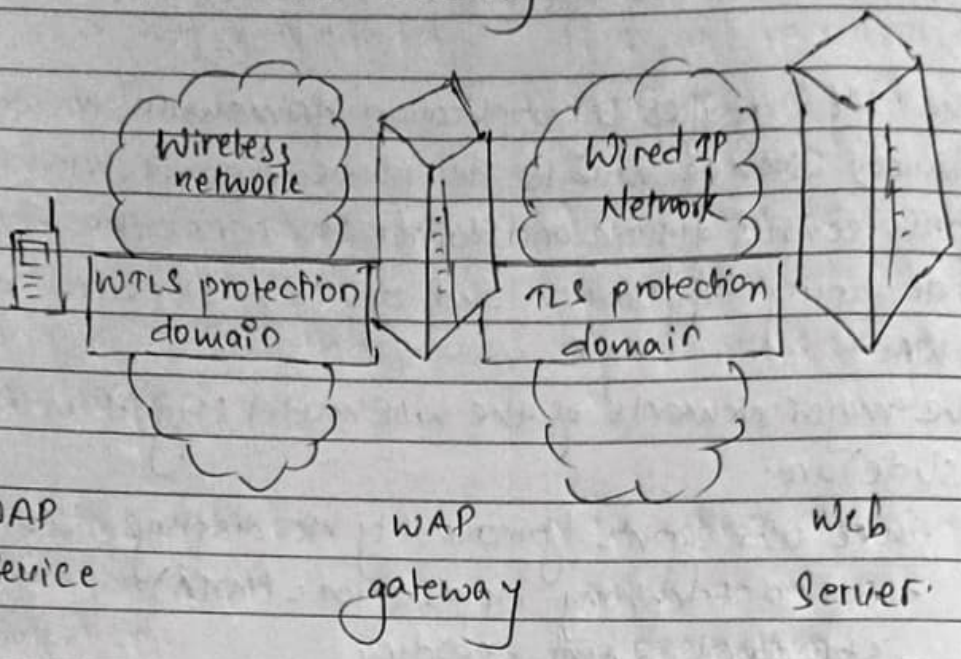


fig: Security Zones Using Standard security Services.

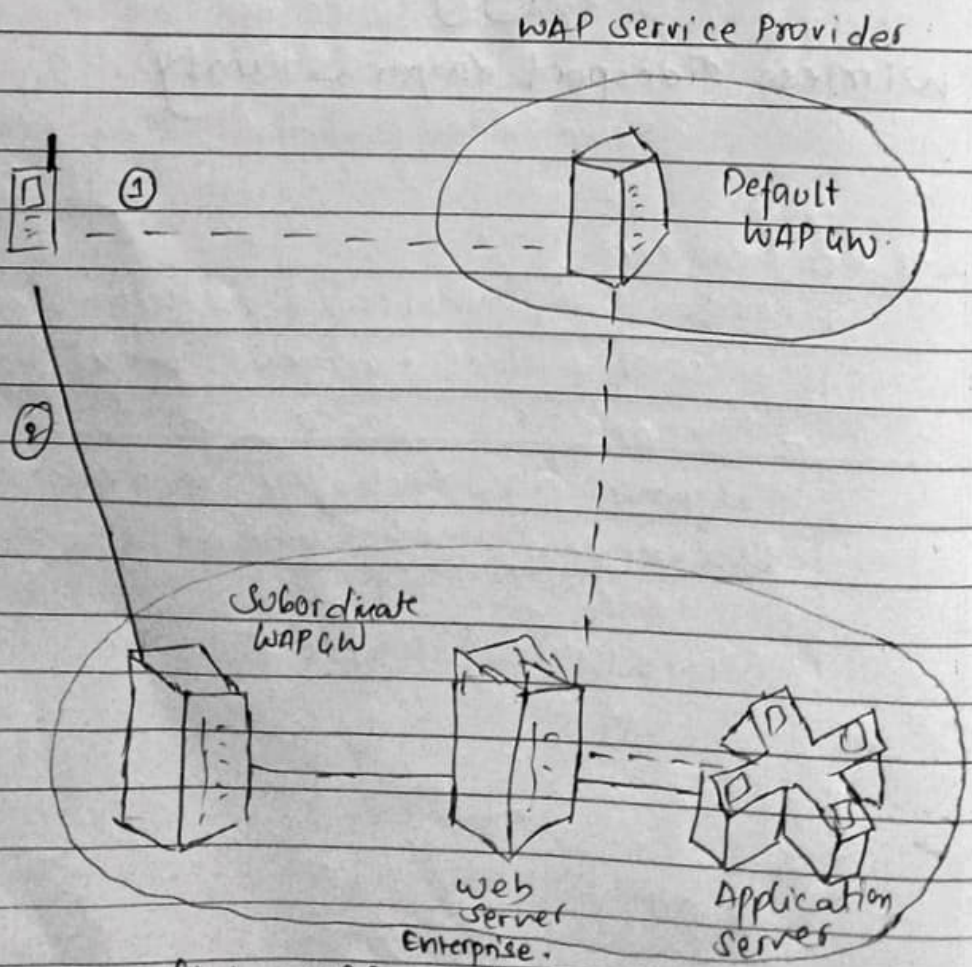


fig: WAP 2 End-to-End Security Scheme.

Ch-1

Information Security

- Approaches to information security implementation
- Objective of Information security
- Needed of information security
- Threads to information security
- Active & passive attack in information security.
- Difference between active & passive attack

Active attack	Passive attack.
1) In active attacks, the attacker intercepts the connection and efforts to modify the message's content.	1) In passive attacks, the attacker observes the messages, then copy and save them and can use it for malicious purposes.
2) In an active attack, the attacker modifies	2) In passive attacks, information remains unchanged
3) In active attacks, the victim gets notified about the attack.	3) Unlike active attacks, in passive attacks, victims do not get informed about the attack.
4) The damage done with active attacks can be harmful to the system and its resources.	4) The passive attacks do not harm the system.

5) In active attacks, the system resources can be changed.	5) In passive attacks, the system resources remain unchanged.
6) They are dangerous for the integrity and availability of the message	6) They can be dangerous for confidentiality of the message.
7) In active attacks, attention is on detection.	7) In active attacks, attention is on prevention.

esnnvkq.

Chapter-8

Cryptography

- Elementary cryptography
- Substitution ciphers
- Transposition ciphers
- Play fair cipher with examples
- Hill cipher
- Vigenere cipher
- Data encryption standard
- RSA algorithm
- Uses of encryption

* Cryptography:

- Cryptography is the technique of converting ordinary plain text into unintelligible text and vice-versa.

- It is the practice and study of techniques for secure communication in the presence of third parties

- It is also refered by the terms ~~cryptogra~~ cryptology and cryptanalysis.

- It is a method of storing and transmitting data in a particular form so that only those for whom it is intended can read and process it.

- ~~Cryptography~~ Cryptology is about constructing and analyzing protocols that prevent third parties or the public from reading private messages.

. Cryptography is most often associated with scrambling plain text into cipher text (a process called encryption), then back again (known as decryption).

* Encryption:
Encryption is the process of encoding a message or information in such a way that only authorized parties can access it and those who are not authorized cannot.

* Decryption:
Decryption is the process of taking encoded or encrypted text or other data and converting it back into text that you or the computer can read and understand (original form) (ie. ciphertext ⇒ plain text)

* Transposition cipher:
A transposition cipher rearranges the characters in the plaintext to form ciphertext. The letters are not changed. Eg: HELLO WORLD
HLDOL
ELWRD

The rearrangement of the text is based on the permutation. It just rearranges the given information without modifying it.

* Substitution cipher:
A substitution cipher changes characters in the plain text to produce the ciphertext.
eg: HELLO WORLD
KHOOR ZRUOG
(Key 3)

- Mono alphabetic cipher:
  Mono alphabetic cipher is a substitution cipher in which for a given key, the cipher alphabet for each plain alphabet is fixed throughout the encryption process for example, if 'A' is encrypted as 'D' for any number of occurrence in that plain text, 'A' will always get encrypted to 'D'

  Example: ceasar cipher

- Polyalphabetic cipher:
  Polyalphabetic cipher is a substitution cipher in which the cipher alphabet for the plain alphabet may be different at different places during the encryption process. Examples: playfair and Vigenere cipher are polyalphabetic cipher.

ψ Ceaser Cipher:

- It is a mono-alphabetic cipher where in each letter of the plaintext is substituted by another letter to form the cipher text. It is a simplest form of substitution cipher scheme.

- This cryptosystem is generally referred to as the shift cipher. The concept is to replace each alphabet by another alphabet which is 'shifted' by some fixed number between 0 and 25.

- sender and receiver agree on a 'secret shift number' for shifting the alphabet.

Example:

- plaintext:
  I AM THE STUDENT OF BIT
  key: 3
- Cipher text:
  [redacted]
  L DP WKH VWXGHQW RI ELW

Playfair cipher:

- The Playfair cipher was the first practical diagraph substitution cipher. The scheme was invented in 1854 by charles Wheatstone.

- In playfair cipher encrypt: a pair of alphabets (diagraphs) instead of a single alphabet

Generate the key square (5x5):

- In playfair cipher, initially a key table is created. The key table is a 5x5 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 replayed by I.

- The initial alphabets in the key square are the unique alphabets of the key in the order in which they appear followed by the remaining letters of the alphabet in order.

Algorithm to encrypt the plain text:
The plaintext is split into pairs of two letters (digraphs). If there is an odd number of letters, a Z is added to the last letter.

Example:
KEY: TUTORIALS.

Key generation:

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

Example 2:
KEY: ~~KATHMANDU~~ JHAPANEPAL

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

Example: 3

Key: Tutorials

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

Plain text: I AM A STUDENT OF PU

IA MA ST UD EN TO FP U2

↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓

TC KL AO TE FM UR UN IW

Example 4:

Key: KATHMANDU

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

Plain text: JOURNEY AND DESTINATION

JO UR NE YA ND DE ST IN AT TO N2

↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓

ER BQ EO WH DU XF QM EB TH ER CV

Cipher text: ER BQ EO WH DU NF QM EB TH ER CV.

Vigenere Cipher:

- This scheme of cipher uses a text string (say, a word) as a key, which is then used for doing a number of shifts on the plain text.

- For example: Let's assume the key is 'point'. Each alphabet of the key is converted to its respective numeric value: In this case, p → 16, o → 15, i → 9, n → 14 and t → 20

  Thus, the key is: 16 15 9 14 20

Example: (0 – 26)

Key = NEPAL

13 4 15 0 11

Plaintext: NEPAL IS THE BEAUTIFUL COUNTRY

~~13 4 15 0 11~~ 8 17 14 24 25 10 7 10 6

N E P A L I S T H E B E A U T I

13 4 15 0 11 .

F U L C O U N T R Y .

KEY: NEPAL

plain text: NEPAL IS BEAUTIFUL COUNTRY

N	E	P	A	L	I	S	B	E	A	U	T	I	F	U	L
13	4	15	0	11	13	4	15	0	11	13	4	15	0	11	13
A	I	E	A	W	V	W	Q	E	L	H	X	F	[illegible]		Y

C	O	U	N	T	R	Y
4	15	0	11	13	4	15
G	D	U	Y	G	V	N

- Hill cipher:

* Hill cipher is a polygraphic substitution cipher based on linear algebra.

* Each letter is represented by a number modulo 26. Often the simple scheme A=0, B=1, ... , Z=25 is used, but this is not an essential feature of the cipher.

* To encrypt a message, each block of n letters is multiplied by an invertible n * n matrix, against modulus 26.

* To decrypt the message, each block is multiplied by the inverse of the matrix used for encryption.

* The matrix used for encryption is the cipher key, and it should be chosen randomly from the set of invertible n×n matrices (modulo 26)

Example:

Plain text = BJTP

n = 4

Key = A B C A F G H B A C D E Y Z N O

5 x 5.

A	B	C		
0	1	2	0	
5	6	7	1	
0	2	3	4	
24	25	13	14.	

.

1
8
19
15

Now,

$$\begin{bmatrix} 0 & 1 & 2 & 0 \\ 5 & 6 & 7 & 1 \\ 0 & 2 & 3 & 4 \\ 24 & 25 & 13 & 14 \end{bmatrix} \begin{bmatrix} 1 \\ 8 \\ 19 \\ 15 \end{bmatrix} = \begin{bmatrix} 0\times1+1\times8+2\times19+0\times15 \\ 5\times1+6\times8+7\times19+1\times15 \\ 0\times1+2\times8+3\times19+4\times15 \\ 24\times1+25\times8+13\times19+14\times15 \end{bmatrix}$$

$$= \begin{bmatrix} 46 \\ 201 \\ 133 \\ 681 \end{bmatrix} = \begin{bmatrix} 20 \\ 19 \\ 3 \\ 5 \end{bmatrix} \pmod{26}$$

Cipher = U T D F

- Symmetric Key Cryptography

* Symmetric-key algorithms are the algorithms for cryptography that use the same cryptographic keys for both encryption of plaintext and decryption of ciphertext.

* Symmetric-key systems are simplier and faster, but their main drawback is that the two parties must somehow exchange the key in a secure way.

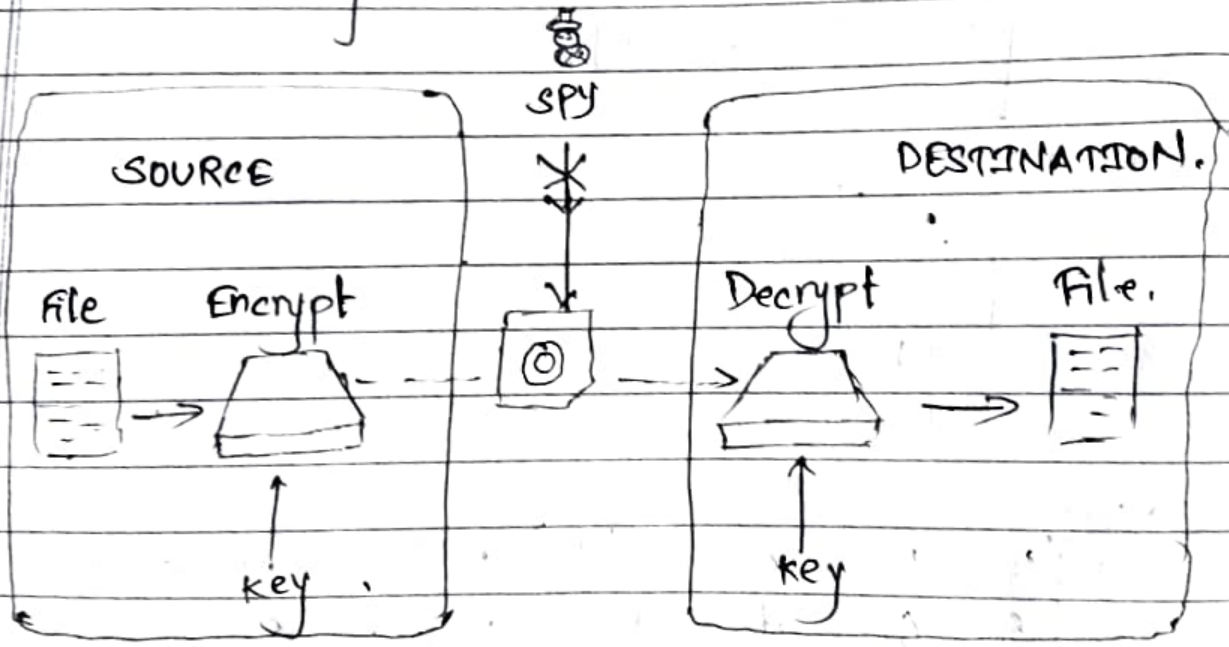


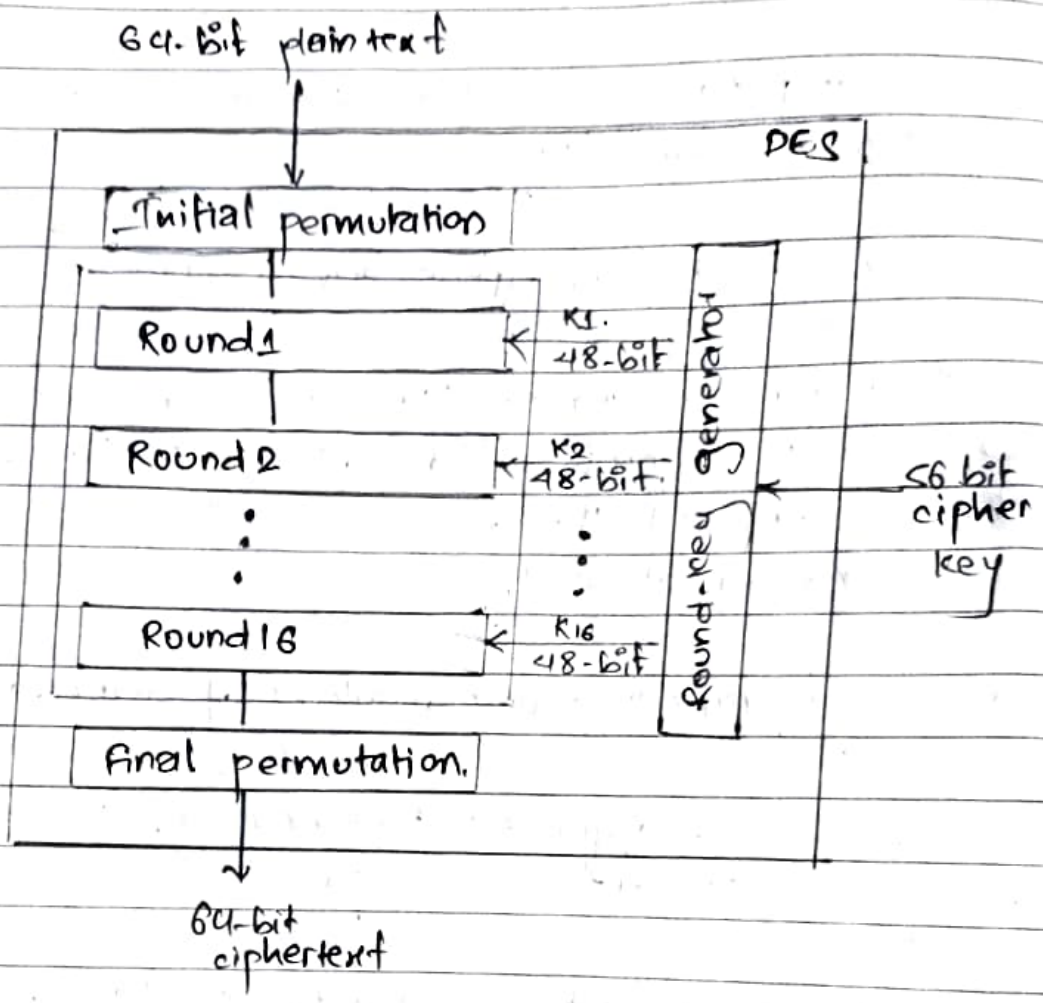
Fig: Traditional cryptography

- Symmetry-key cryptography is sometimes called secret key cryptography.
- The most popular symmetric-key system is the Data Encryption Standard (DES).

Imp Data Encryption Standard (DES)

- The Data Encryption Standard (DES) works by using the same key to encrypt and decrypt a message, so both the sender and the receiver must know and use the same private key.
- DES is a symmetric key method of data encryption.
- DES has been upgraded by the more secure Advanced Encryption Standard (AES) algorithm.
- Originally designed by researchers at IBM in the early 1970s, DES was adopted by the US government as an official Federal Information Processing Standard (FIPS) in 1977 for the encryption of commercial and sensitive yet unclassified government computer data.
- It was the first encryption algorithm approved by the US government for public disclosure.

- General Structure of DES



- The Data Encryption Standard is a block cipher, meaning a cryptographic key and algorithm are applied to a block of data simultaneously rather than one bit at a time.

- To encrypt a plaintext message, DES groups it in 64-bit blocks. Each block is enciphered using the secret key into a 64-bit ciphertext by means transposition and substitution.

- The process involves 16 rounds and encrypting blocks.

Asymmetric key Cryptography

- Asymmetric cryptography, also known as Public key cryptography, uses public and private keys to encrypt and decrypt data.
- The keys are simply large numbers that have been paired together but are not identical (asymmetric).
- One key in the pair can be shared with everyone; it is called the public key.
- The other key in the pair is kept secret; it is called the private key.

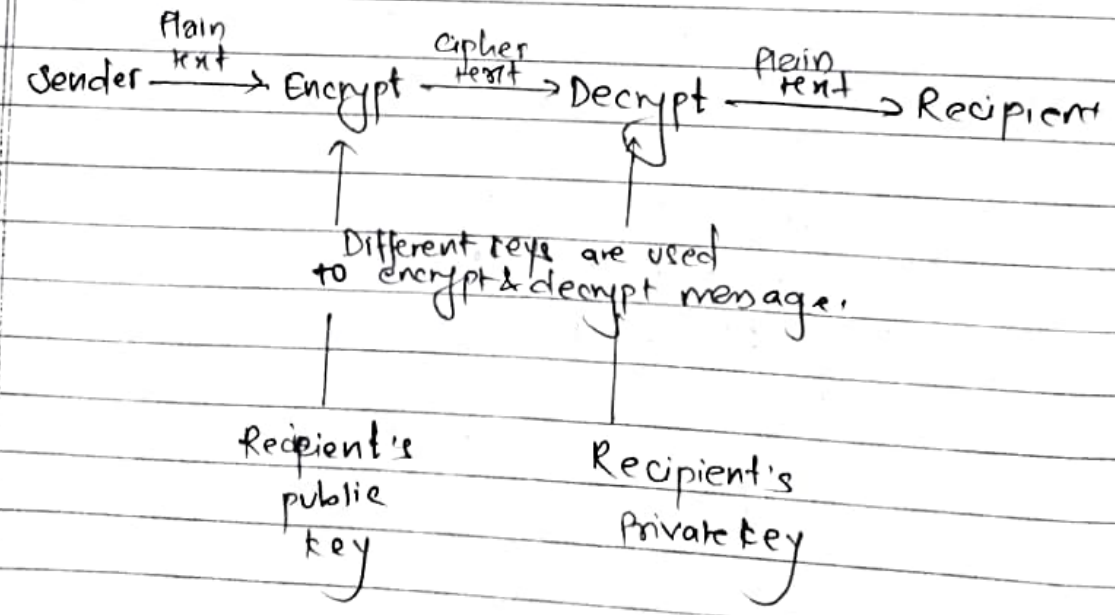


Fig: Asymmetric key cryptography.

Date
Page

Imp RSA Algorithm

- RSA is one of the first public-key cryptosystems and is widely used for secure data transmission.

- In such a cryptosystem, the encryption key is public and it is different from the decryption key which is kept secret.

- RSA stands for Ron Rivest, Adi Shamir and Leonard Adleman, who first publicly described it in 1978.

- RSA involves a public key and a private key. The public key can be known by everyone, and it is used for encrypting messages.

- The intention is that messages encrypted with the public key can only be decrypted by using the private key.

- The public key is represented by the integers n and e (although n is also used during the decryption). m represents the message.

n and e: and the private key by the

- A user of RSA creates and then publishes a public key based on two large prime numbers, along with an auxiliary value. The prime numbers must be kept secret.

- The RSA algorithm involves four steps: key generation, key distribution, encryption and decryption.

Key Generation:

The keys for RSA algorithm are generated in the following way:

1) Choose two different large random prime numbers p and q.

2) Calculate $n = p * q$. n is called modulus

3) Calculate the totient: $\Phi(n) = (p-1)(q-1)$.

4) ~~calculate~~ Choose an integer e such that $1 < e < \Phi(n)$, where e and $\Phi(n)$ donot share factors other than 1.
(e,n) is released as the public key

5) Computed to satisfy the relation:
$de \{mod\ \Phi(n)\} = 1$ or $d = (1 + k * \Phi(n))/e$
k is an integer which should be chosen in such a way that value of d should not be in fraction, $k < e$.

6) The public key is made of the modulus n and the encryption exponent e i.e. (e,n)

7) The private key is made of the modulus n and the decryption exponent d which must be kept secret i.e (d,n)

Example:

Pick two prime numbers: $p = 3, q = 5$

- $n = p * q = 3 * 5 = 15$
- $\Phi(n) = (p-1)(q-1) = (3-1)(5-1) = 2 * 4 = 8$
- Choose e satisfying $1 < e < \Phi(n)$.
  Let us choose $e = 3$, which donot share any common factors with 8 rather than 1.
- Compute d satisfying: $de \{mod\ \Phi(n)\} = 1$.
  So, $d * 3 \{mod\ 8\} = 1$
  Let us choose $d = 11$ which satisfies the relation

Q. If $p = 11$ & $q = 17$ calculate public key & private key by using RSA.

- Pick two prime numbers: $p = 11, q = 17$

$n = p * q = 11 \times 17 = 187$

- $\Phi(n) = (11-1)(17-1) = (10 * 16) = 160$
- Choose e satisfying $1 < e < \Phi(n)$
  Let us choose $e = 7$, which donot share any common factors with 160 rather than 1.
- Compute d satisfying: $de \{mod\ \Phi(n)\} = 1$
  so, $d * 3 \{mod\ 160\} = 1$
  Let us choose $d = 23$ which satisfies the relation.

public key $(e, n) = (7, 187)$

private key $(d, n) = (23, 187)$

- Encryption:

* After Bob obtains Alice's public key (e,n), he can send a message m to Alice by computing the cipher text c, using Alice's public key (e,n).

$$c = m^e \pmod n$$

* Bob then transmits c to Alice

- Decryption

* Alice can recover the original message m form c using her private key (d,n) by computing $m = c^d \pmod n$

Encryption example:

- Let us consider the message be 2.
- So, at encryption process, the sender uses the public key to encrypt the message. Resulting cipher text will be:

$$c = m^e \pmod n$$
$$= 2^3 \pmod{15}$$
$$= 8 \bmod 15$$
$$= 8$$

- At decryption process, the private key is used to decrypt the cipher text. Plain text is obtained as

$$m = c^d \pmod n$$
$$= 8^{11} \pmod{15}$$
$$= 2$$

Hence, the original msg 2 is obtained at receiver end after

decryption.

Q If p=11 q=17 calculate public key & private key by using RSA. Also show the encryption & Decription process if m=10.

For encryption,

~~Let us consider~~

The sender uses the public key to encrypt the message Resulting cipher text will be:

$$c = m \wedge e \pmod{n}$$
$$= 10 \wedge 7 \pmod{187}$$
$$= 175$$

At decryption process, the private key is used to decrypt the cipher text. Plain text is obtained as:

$$m = c \wedge d \pmod{n}$$
$$= 175 \wedge 23 \pmod{187}$$