MIT-WPU

॥ विश्वशान्तिर्ध्रुवं ध्रुवा ॥

Dr. Vishwanath Karad
MIT WORLD PEACE UNIVERSITY | PUNE
TECHNOLOGY, RESEARCH, SOCIAL INNOVATION & PARTNERSHIPS

CET4004B: Wireless and Mobile Device Security

SCHOOL OF COMPUTER ENGINEERING AND TECHNOLOGY

T. Y. B. TECH. COMPUTER SCIENCE AND ENGINEERING

CET4004B: Wireless and Mobile Device Security

Teaching Scheme
Theory: 3Hrs. / Week

Credits: 03 + 01 = 04
Practical: 2 Hrs./Week

Course Objectives:

1) Knowledge:

i. To understand wireless networks technologies and applications
ii. To study Ad-Hoc, sensor networks architecture, challenges and applications
iii. To understand basic security needs and issues in wireless networks
iv. To understand mobile device security architecture and security dynamics

2) Skills:

i. This course gives understanding of how to design and configure your own network

3) Attitude:

i. To deploy the network as well as provide various security aspects to the mobile device

Course Outcomes:

i. Compare different wired and wireless technologies
ii. Simulate and analyze wireless Ad-Hoc networks for different protocols
iii. Analyze the security threats in wireless sensor networks
iv. Configure or Program security needs in mobile devices

Module 4
Security in Wireless Networks

Disclaimer:

a. Information included in these slides came from multiple sources. We have tried our best to cite the sources. Please refer references to learn about the sources, when applicable.

b. The slides should be used only for preparing notes, academic purposes (e.g. in teaching a class), and should not be used for commercial purposes.

Points to be covered

- Security in Ad Hoc Wireless Networks
- Network Security Requirements
- Issues and Challenges in Security Provisioning
- Network Security Attacks and other attacks
- Key Management in Adhoc Wireless Networks
- Requirements of a Secure Routing Protocol for Ad Hoc Wireless Networks
- Overview of Wi-Fi security and Issues in Wi-Fi Security
- Access Point Security
- Authentication in Wireless networks
- Security in IPv4 and IPv6 Protocols

Security in Ad Hoc Wireless Networks

- In wireless ad hoc networks, basic network operations are carried out through the cooperation of all available nodes.
- Due to the inherent lack of a managed infrastructure, the nodes of an ad hoc network cannot be considered as trustworthy as in a dedicated infrastructure.
- Wireless ad hoc networks are thus vulnerable to various exposures threatening the basic network operations like routing and packet forwarding.
- Ad-hoc wireless networks are highly vulnerable to security attacks due to its unique characteristics.
- The security of ad hoc networks can be based on protection in the link or network layer.
- In some ad-hoc solutions, the link layer offers strong security services for protecting confidentiality and authenticity, in which case all of the security requirements need not be addressed in the network or upper layers.

Network Security Requirements

A security protocol should meet following requirements:

- Data confidentiality/ secrecy is concerned with ensuring that data is not exposed to unauthorized users.
- Data integrity means that unauthorized users should not be able to modify any data without the owner's permission.
- System availability means that nobody can disturb the system to have it unusable.
- Authentication is concerned with verifying the identity of a user.
- Non-repudiation means that the sender cannot deny having sent a message and the recipient cannot deny have received the message.

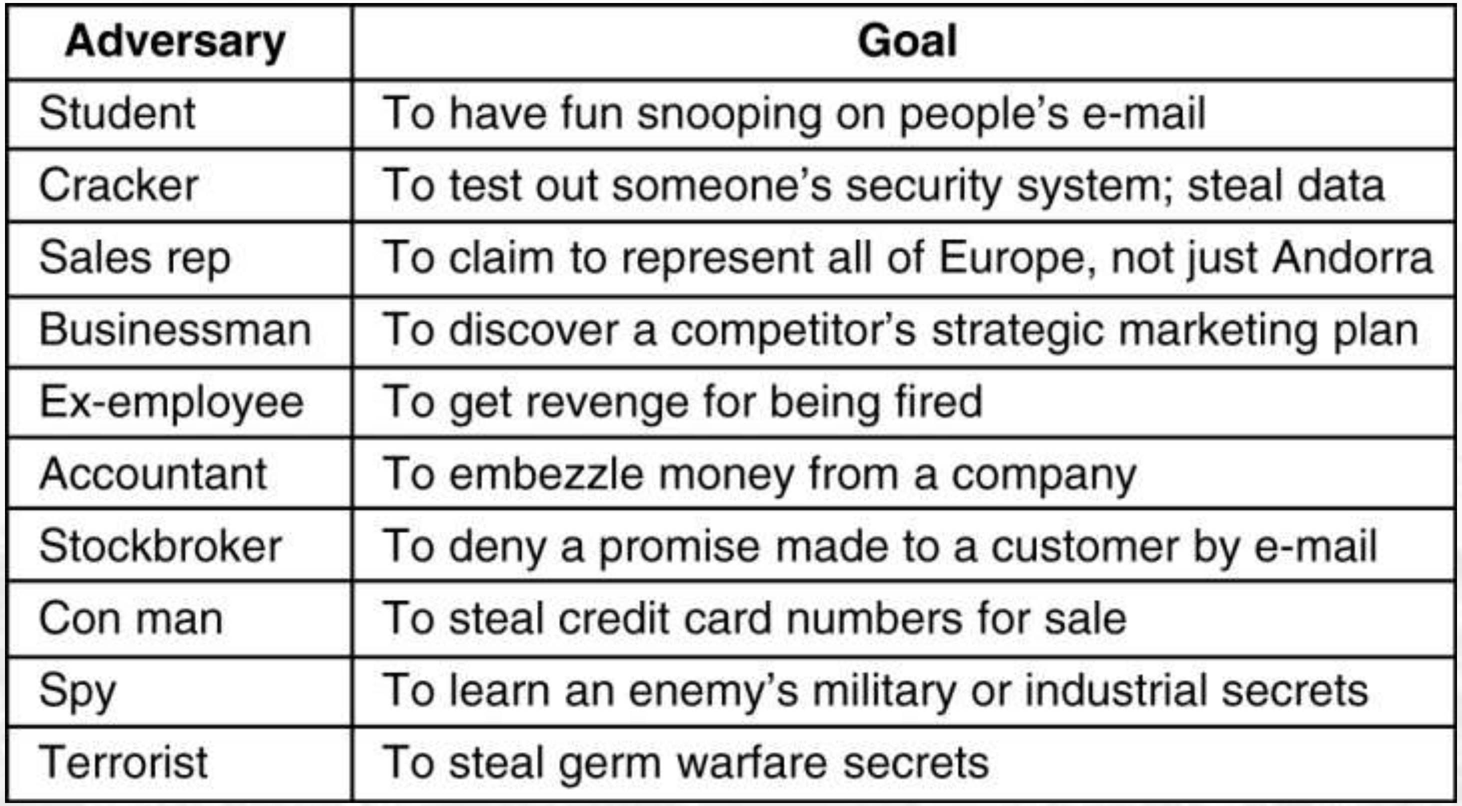
Issues and Challenges in Security Provisioning

Issues and challenges in security provisioning:

- Shared broadcast radio channel: The radio channel in ad hoc wireless networks is broadcast and is shared by all nodes in the network.
- Insecure operational environment: The operating environments where ad hoc wireless networks are used may not always be secure. For example, battlefields.
- Lack of central authority: There is no central monitor in ad hoc wireless networks.
- Lack of association: A node can join and leave the network at any point.
- Limited resource availability: Resources such as bandwidth, battery power, and computational power are scarce.
- Physical vulnerability: Nodes in these networks are usually compact and hand-held in nature.

Need for Security

- Some people who cause security problems and why.



Adversary	Goal
Student	To have fun snooping on people's e-mail
Cracker	To test out someone's security system; steal data
Sales rep	To claim to represent all of Europe, not just Andorra
Businessman	To discover a competitor's strategic marketing plan
Ex-employee	To get revenge for being fired
Accountant	To embezzle money from a company
Stockbroker	To deny a promise made to a customer by e-mail
Con man	To steal credit card numbers for sale
Spy	To learn an enemy's military or industrial secrets
Terrorist	To steal germ warfare secrets

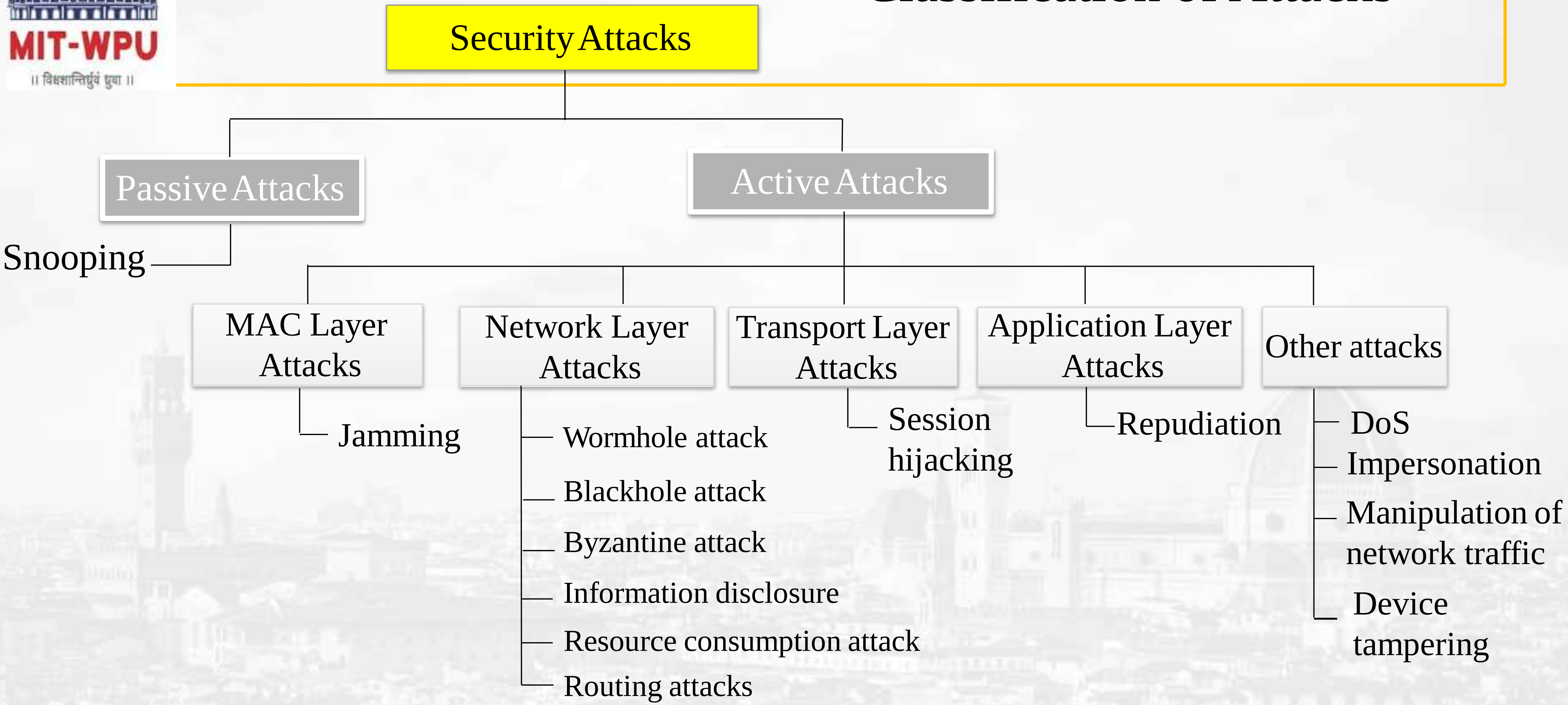
Security Threats

- ***threat***: a potential for violation of security

- Four types of security threats:
  - Interception refers to the situation that an unauthorized party has gained access to a service or data.
  - Interruption refers to the situation in which services or data become unavailable, unusable, or destroyed.
  - Modifications involve unauthorized changing of data or tampering with a service.
  - Fabrication refers to the situation in which additional data or activity are generated that would normally not exist.

- Interception – attack on confidentiality
- Interruption – attack on availability
- Modification – attack on integrity
- Fabrication – attack on authenticity

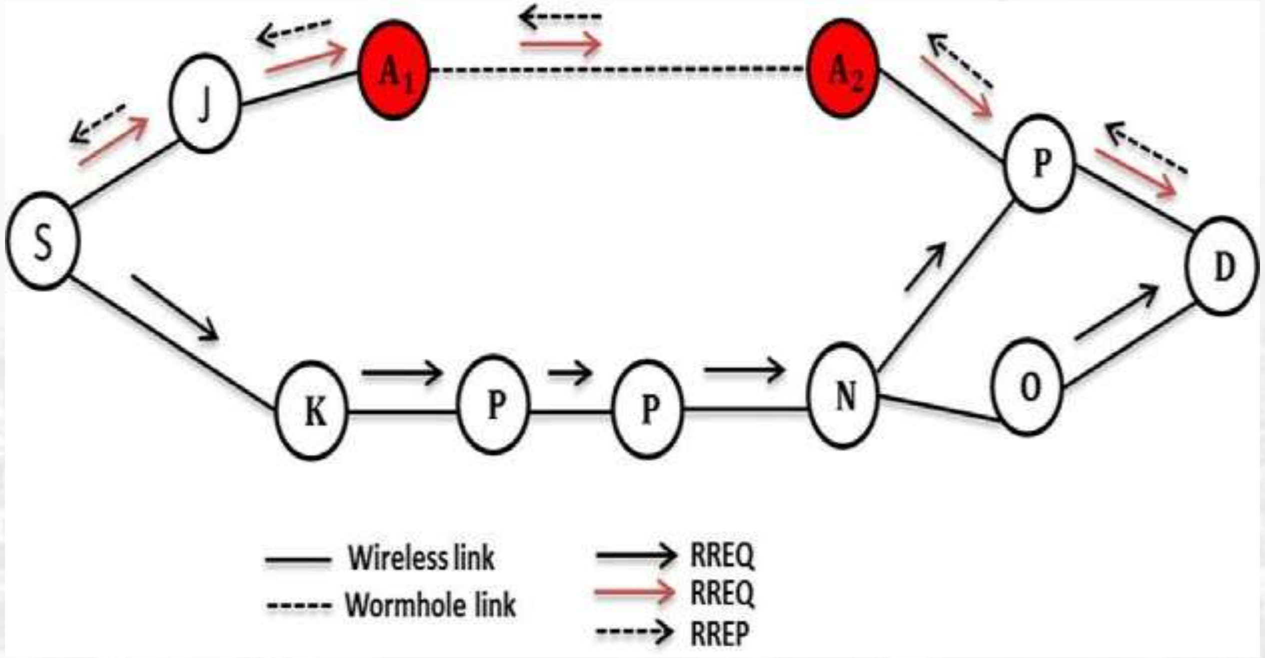
Classification of Attacks



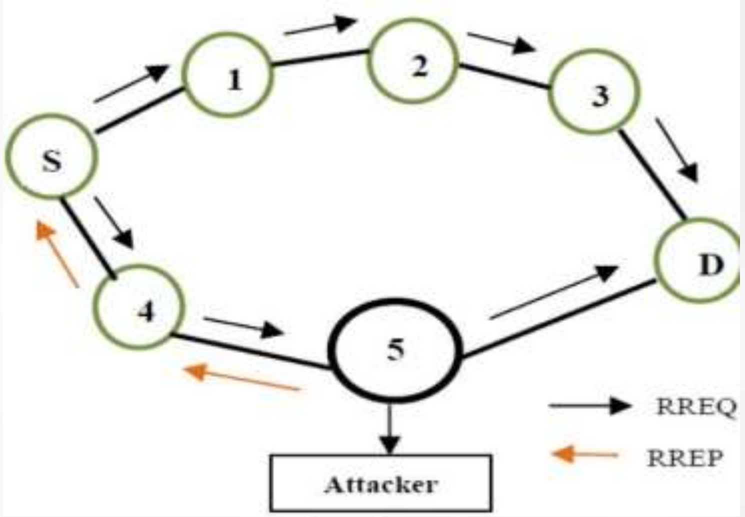
- Security Attacks
  - Passive Attacks
    - Snooping
  - Active Attacks
    - MAC Layer Attacks
      - Jamming
    - Network Layer Attacks
      - Wormhole attack
      - Blackhole attack
      - Byzantine attack
      - Information disclosure
      - Resource consumption attack
      - Routing attacks
    - Transport Layer Attacks
      - Session hijacking
    - Application Layer Attacks
      - Repudiation
    - Other attacks
      - DoS
      - Impersonation
      - Manipulation of network traffic
      - Device tampering

Network Security Attacks

- Network Layer Attacks:
  - Wormhole attack: an attacker receives packets at one location in the network and tunnels them to another location in the network.



- Blackhole attack: A malicious node could divert the packets.



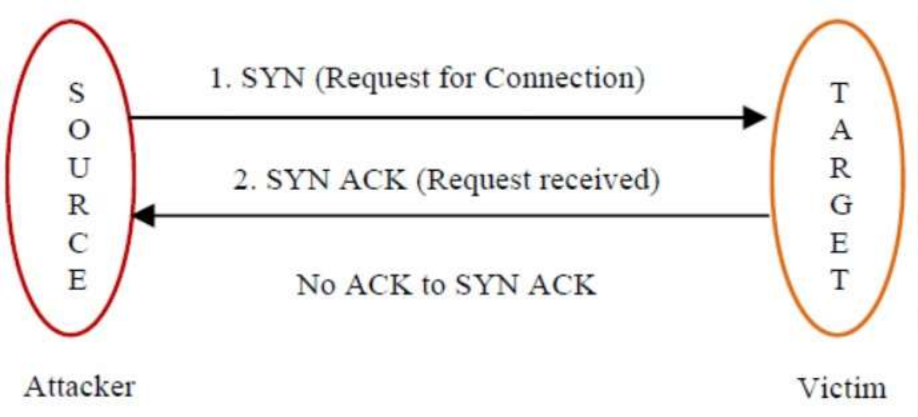
- Byzantine attack: A compromised intermediate node could create routing loops.
- Information disclosure: A compromised node may leak confidential information to unauthorized nodes in the network.
- Resource consumption attack: A malicious node tries to consume/waste away resources of other nodes present in the network.

- Routing attacks
  - **Routing table overflow**: An adversary node advertises routes to non-existent nodes.
  - **Routing table poisoning**: The compromised nodes send fictitious routing updates.
  - **Packet replication**: An adversary node replicates stale packets.
  - **Route cache poisoning**: Each node maintains a route cache that can be poisoned by a adversary node.
  - **Rushing attack**: On-demand routing protocols that use duplicate suppression during the route discovery process are vulnerable to this attack.

- Transport Layer Attacks
  - ❖ Session hijacking: An adversary takes control over a session between two nodes.

- Application Layer Attacks
  - ❖ Repudiation: Repudiation refers to the denial or attempted denial by a node involved in a communication.

- Other Attacks
  - Multi-layer attacks could occur in any layer of the network protocol stack.
    - Denial of service: An adversary attempts to prevent authorized users from accessing the service.
      - **Jamming:** Transmitting signals on the frequency of senders and receivers to hinder the communication.
      - **SYN flooding:** An adversary send a large number of SYN packets to a victim node.


S O U R C E
1. SYN (Request for Connection)
2. SYN ACK (Request received)
No ACK to SYN ACK
T A R G E T
Attacker
Victim

– **Distributed DoS attack:** Several adversaries attack a service at the same time.

- ❖ Impersonation: An adversary pretends to be other node.
- ❖ Device tampering: Mobile devices get damaged or stolen easily.

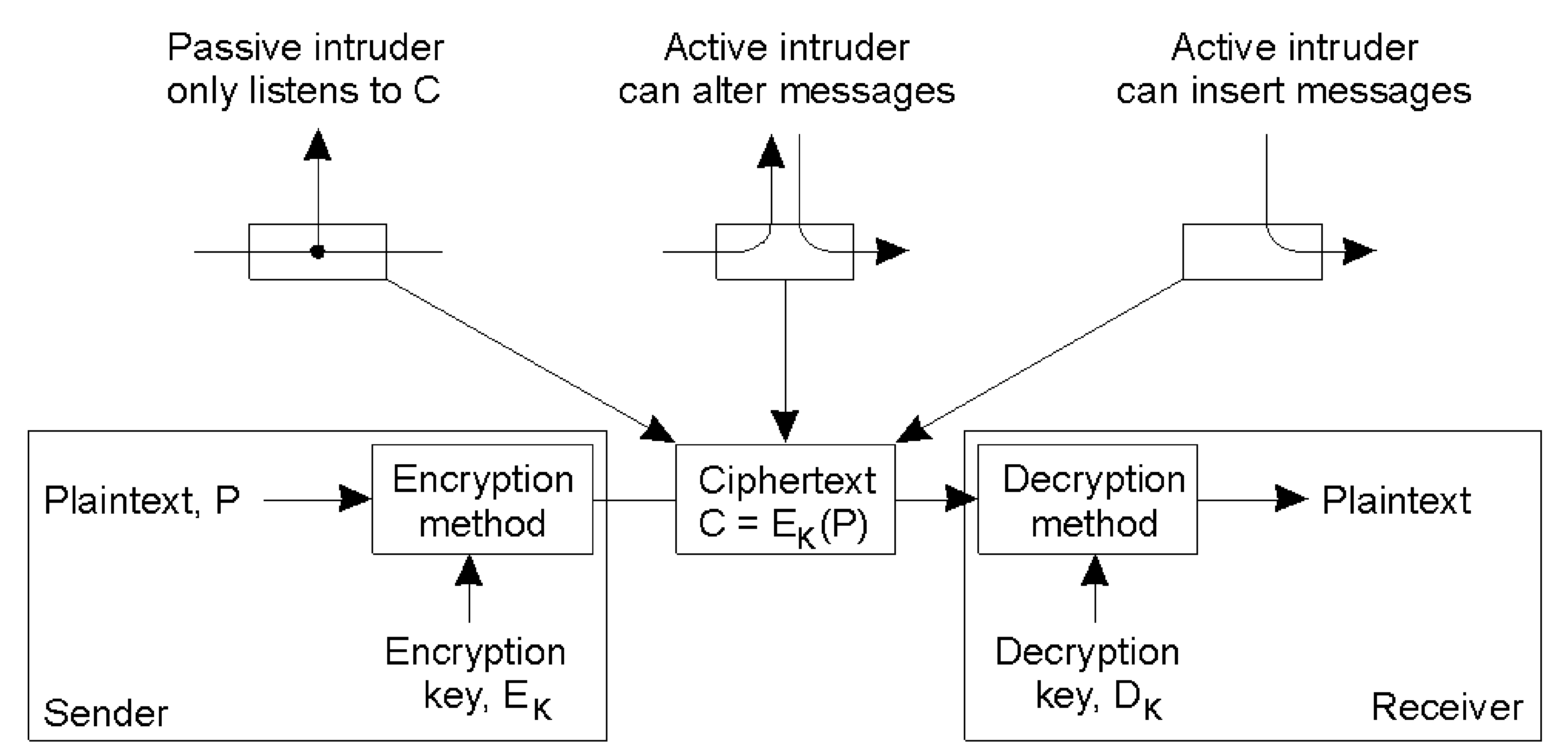
Key Management

Key Management

- Cryptography is one of the most common and reliable means to ensure security.
- The purpose of cryptography is to take a message or a file, called the **plaintext** (P), and encrypt it into the **ciphertext** (C) in such a way that only authorized people know how to convert it back to the plaintext.
- The secrecy depends on parameters to the algorithms called **keys**.
- The four main goals of cryptography are confidentiality, integrity, authentication, and non-repudiation.
- Usually, the encryption method E is made public, but let the encryption as a whole be parameterized by means of a key k (same for decryption).

- Three types of intruders:
  - Passive intruder only listens to messages.
  - Active intruder can alter messages.
  - Active intruder can insert messages.

Cryptography

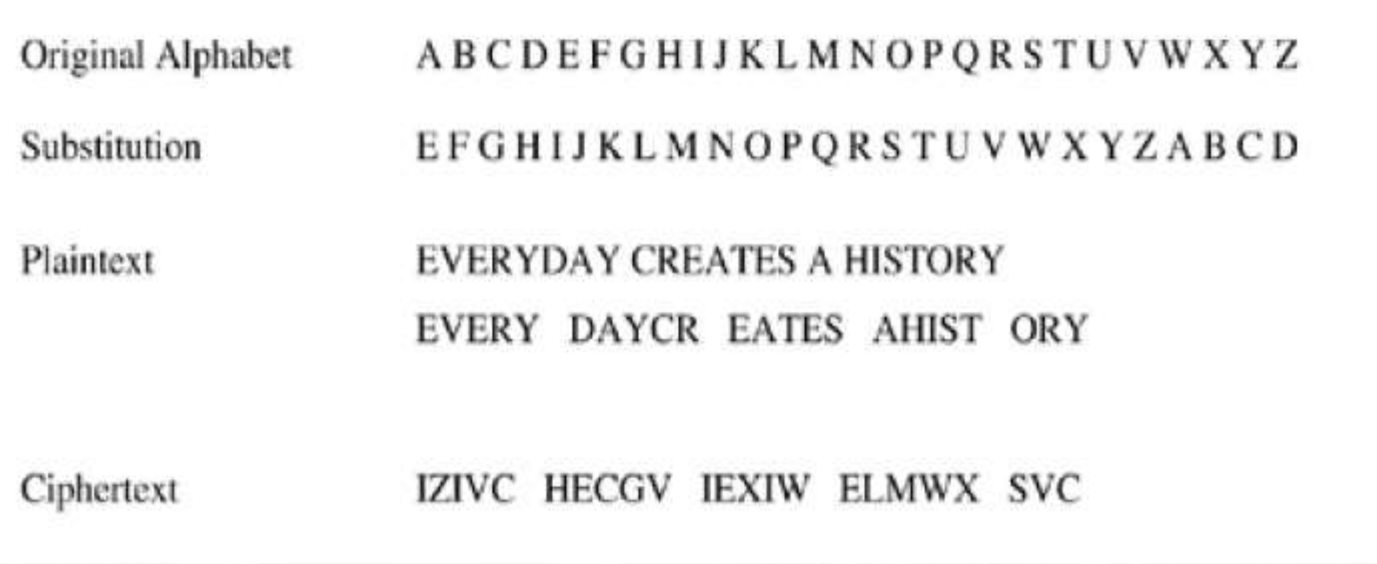


Cryptographic Algorithms

- There are two major kinds of cryptographic algorithms:
  - **Symmetric (secret-key) system**: Use a single key to (1) encrypt the plaintext and (2) decrypt the ciphertext. Requires that sender and receiver share the secret key.
  - **Asymmetric (public-key) system**: Use different keys for encryption and decryption, of which one is private, and the other public

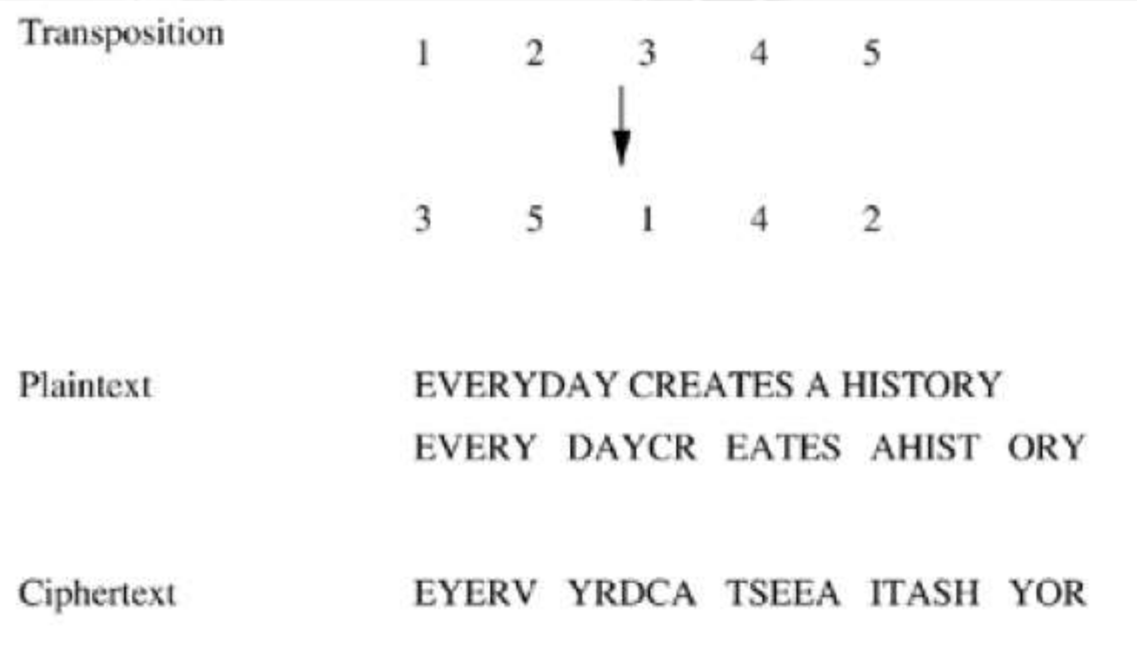
Encryption using Substitution and Transposition cipher

The encryption using substitution



Original Alphabet	A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
Substitution	E F G H I J K L M N O P Q R S T U V W X Y Z A B C D
Plaintext	EVERYDAY CREATES A HISTORY EVERY DAYCR EATES AHIST ORY
Ciphertext	IZIVC HECGV IEXIW ELMWX SVC

Transposition cipher



Transposition	1	2	3	4	5
			↓		
	3	5	1	4	2

Plaintext	EVERYDAY CREATES A HISTORY EVERY DAYCR EATES AHIST ORY
Ciphertext	EYERV YRDCA TSEEA ITASH YOR

Symmetric Cryptosystems

- **Substitute Cipher:** each letter or group of letter is replaced by another letter or group of letters
  - Caesar cipher: rotate the letter (a → D, b → E, c → F, z → C).
    - Example: attack → DWWDFN
  - Monoalphabetic substitution
    - Each letter replaced by different letter

      Plaintext: ABCDEFGHIJKLMNOPQRSTUVWXYZ

      Ciphertext: QWERTYUIOPASDFGHJKLZXCVBNM
    - Disadvantage: It does not smooth out frequencies in the cipher text.
  - Polyalphabatic cipher – use multiple cipher alphabets.

Secret-Key Cryptography

- Transposition cipher: reorder the letters, but don't disguise them.
  - Select a key MEGABUCK

    7 4 5 1 2 8 3 6

    p l e a s e t r

    a n s f e r o n

    e h u n d r e d

    → afnsedtoelnhesurndpaeerr

Plain text → cipher text

Asymmetric Key Algorithms

- Asymmetric key (or public key) algorithms use different keys at the sender and receiver ends for encryption and decryption, respectively.

- A very popular example of public key cryptography is the RSA system developed by Rivest, Shamir, and Adleman, which is based on the integer factorization problem.

- Digital signatures schemes are also based on public key encryption.

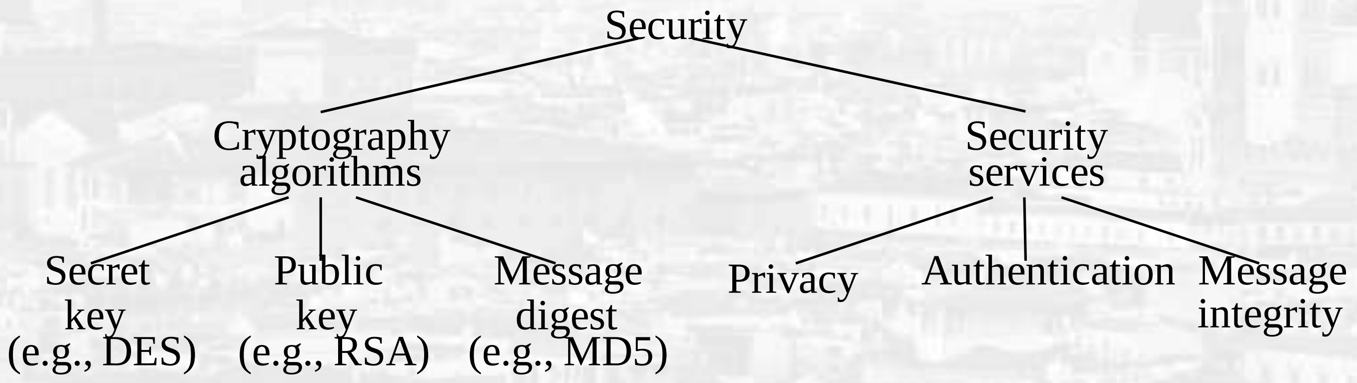
Hashing System

- **Hashing system**: Only encrypt data and produce a fixed length digest. There is no decryption; only comparison is possible.

Notation	Description
$K_{A,\,B}$	Secret key shared by A and B
K^{+}_{A}	Public key of A
	Private key of A

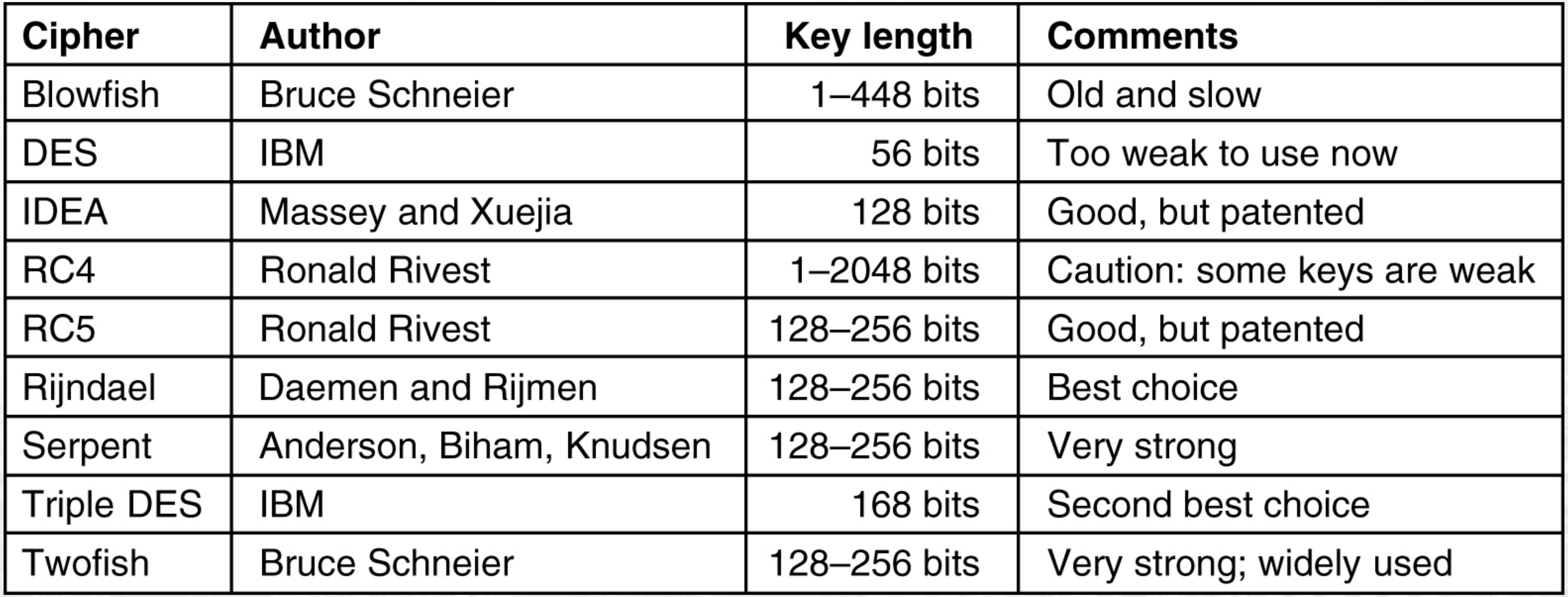
Cryptography Functions

- Cryptography functions
  - Secret key (symmetric cryptography, e.g., DES)
  - Public key (asymmetric cryptography, e.g., RSA)
  - Hashing (one-way function - message digest, e.g., MD5)
- Security services
  - Privacy (Secrecy): preventing unauthorized release of information
  - Authentication: verifying identity of the remote participant
  - Integrity: making sure message has not been altered



Cryptanalysis

- Some common symmetric-key cryptographic algorithms.

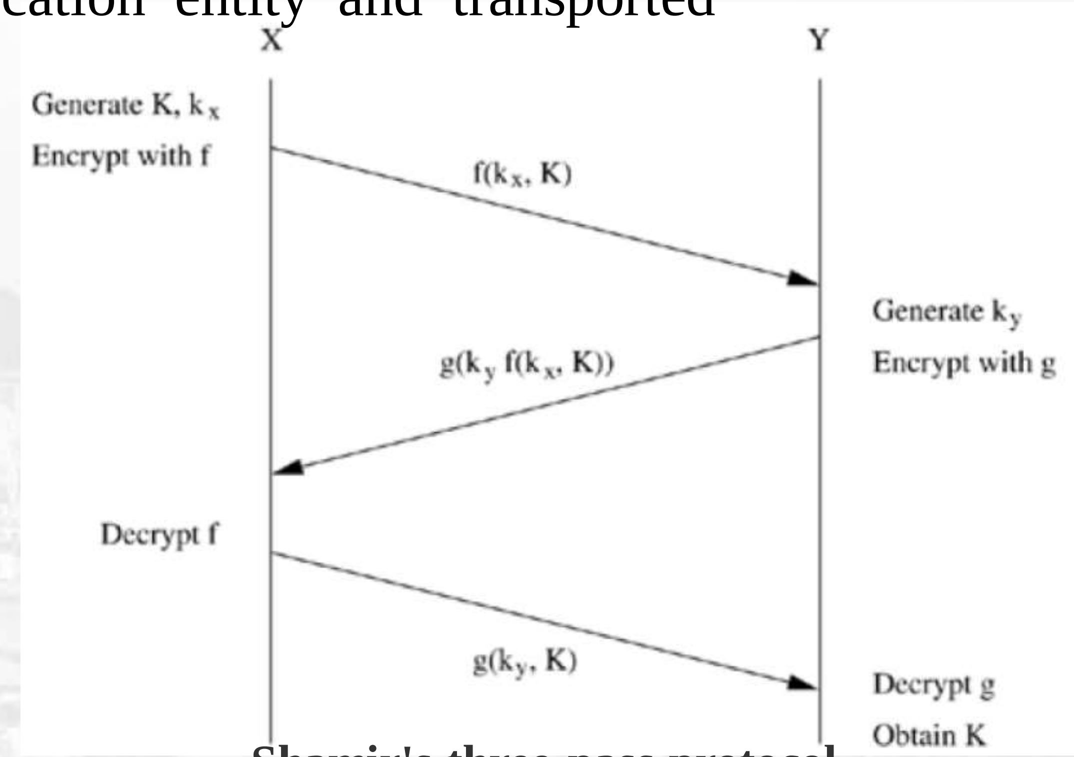


Cipher	Author	Key length	Comments
Blowfish	Bruce Schneier	1–448 bits	Old and slow
DES	IBM	56 bits	Too weak to use now
IDEA	Massey and Xuejia	128 bits	Good, but patented
RC4	Ronald Rivest	1–2048 bits	Caution: some keys are weak
RC5	Ronald Rivest	128–256 bits	Good, but patented
Rijndael	Daemen and Rijmen	128–256 bits	Best choice
Serpent	Anderson, Biham, Knudsen	128–256 bits	Very strong
Triple DES	IBM	168 bits	Second best choice
Twofish	Bruce Schneier	128–256 bits	Very strong; widely used

Key Management Approaches

- The primary goal of key management is to share a secret (some information) among a specified set of participants.

- **Key predistribution**: Keys are distributed to all participants before the communication.
- **Key transport**: Keys are generated in one communication entity and transported to all participants.
  - The key transport method without prior knowledge of shared key is used in Shamir's three pass protocol.



Shamir's three-pass protocol

- **Key arbitration**: Keys are created and distributed by a central arbitrator to all participants.

- **Key agreement**: Participants agree on a secret key for the further communications.

- While keys are encrypted by key encryption keys (KEKs), data traffic is encrypted by traffic encryption keys (TEKs).

Key Management in Ad Hoc Wireless Networks

❖ Password-based Group Systems

- A long string is given as the password for users for one session.
- A strong key is derived from the weak passwords given by the participants.
- It could be for two-party or for the whole group with a leader.

❖ Threshold Cryptography

- Public key infrastructure (PKI) enables the easy distribution of keys and is a scalable method. Each node has a public/private key pair, and a certifying authority (CA) can be bind the keys to the particular node.
- A scheme based on threshold cryptography by which **n servers** exist out of which any **(t + 1) servers** can jointly perform any arbitration or authorization successfully, but **t server** cannot perform the same. So up to t compromised severs can be tolerated.
- $n > 3 \times t + 1$

- To sign a certificate, each server generates a partial signature using its private key and submits it to a combiner.

❖ **Self-Organized Public Key Management for Mobile Ad Hoc Networks**

❖ The users issue certificates to each other based on personal acquaintance.

  - A certificate is a binding between a node and its public key and issued for a specific period of time.

Secure Routing in Ad Hoc Wireless Networks

Secure Routing in Ad Hoc Wireless Networks

- Requirements of a secure routing protocol for ad hoc wireless networks
  - ❖ Detection of malicious nodes
  - ❖ Guarantee of correct route discovery
  - ❖ Confidentiality of network topology
  - ❖ Stability against attacks

Security-aware Routing Protocols
Proposed
for
Ad hoc Wireless Networks

Secure routing protocols

❖ Security-Aware ad hoc Routing protocol (SAR):

- SAR defines level of trust as a measure for routing establishment.

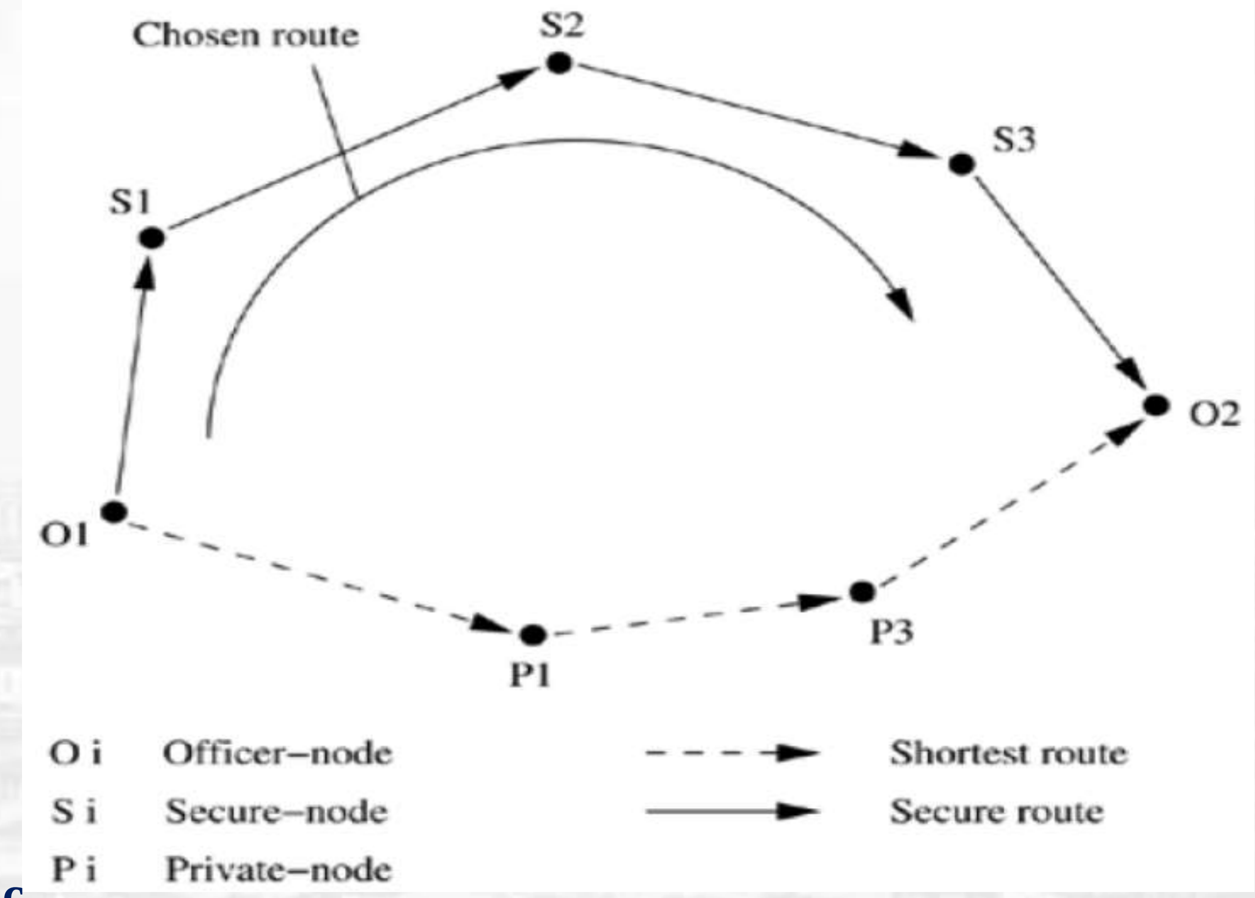


illustration of the level of trust metric

- The SAR can be implemented using AODV protocol.
- In SAR, a certain level of security is incorporated into the packet-forwarding mechanism.
- Each packet is associated with a security level.
- Each intermediate node is also associated with a certain level of security.
- Nodes of equal levels of trust distribute a common key among themselves and with those nodes having higher levels of trust.
- The protocol requires different keys for different levels of security. This tends to increase the number of keys required when the number of security levels used increases.

❖ Secure Efficient Ad hoc Distance Vector (SEAD) Routing Protocol:

- Aim: to overcome DoS and resource consumption attracts.
- Uses a one-way hash function and does not involve any asymmetric cryptographic operation.

Distance vector routing:

- The metric used for routing is the distance measured in terms of hop-count.
- Also, triggered updates approach is used, in which each node broadcasts routing updates only if its routing table gets altered.
- The DSDV protocol for ad hoc wireless networks uses sequence number tags to prevent the formation of loops, to counter the count-to-infinity problem.

One-Way Hash Function

- A one-way hash function (H) generates a one-way hash chain (h1 , h2 , ...).
- The function H maps an input bit-string of any length to a fixed length bit-string,
- that is, $H : (0, 1)^* \rightarrow (0, 1)^p$, where p is the length in bits of the output bit-string.
- $h_i = H(h_{i-1})$ for $0 \leq i \leq n$
- The SEAD protocol, however, would not be able to overcome attacks where the attacker uses the same metric and sequence number which were used by the recent update message, and sends a new routing update.

Authenticated Routing for Ad hoc Networks (ARAN)

- It is based on cryptographic certificates and end-to-end route authentication process.

Issue of Certificate:

- Assumes that keys are generated a priori by the server and distributed to all nodes in the network.
- On joining the network, each node receives a certificate from the trusted server.

$$\boxed{T \rightarrow A:\ Cert_A = [IP_A, K_{A+}, t, e]\ K_{T-}}$$

- Where, IP_A → represent the IP address of node A, K_{A+} → the public key of node A,
- t → the time of creation of the certificate, e → the time of expiry of the certificate,
- K_{T-} → the private key of the server

End-to-end Route Authentication:

- The correct intended destination is reached by the packets sent from the source node.

S -→ broadcasts : = [RDP, IP_D, $Cert_S$, N_S, t] K_{S-}

RDP – Route Discovery Packet

- When a node receives an RDP packet from the source with a higher value of the source's nonce than that in the previously received RDP packets from the same source node, it makes a record of the neighbor from which it received the packet, encrypts the packet further with its own certificate, and broadcasts it further.

$$A \text{ -→ broadcasts : } = [[RDP, IP_D, Cert_S, N_S, t]\ K_{S-}]\ K_{A-}\ , Cert_A$$

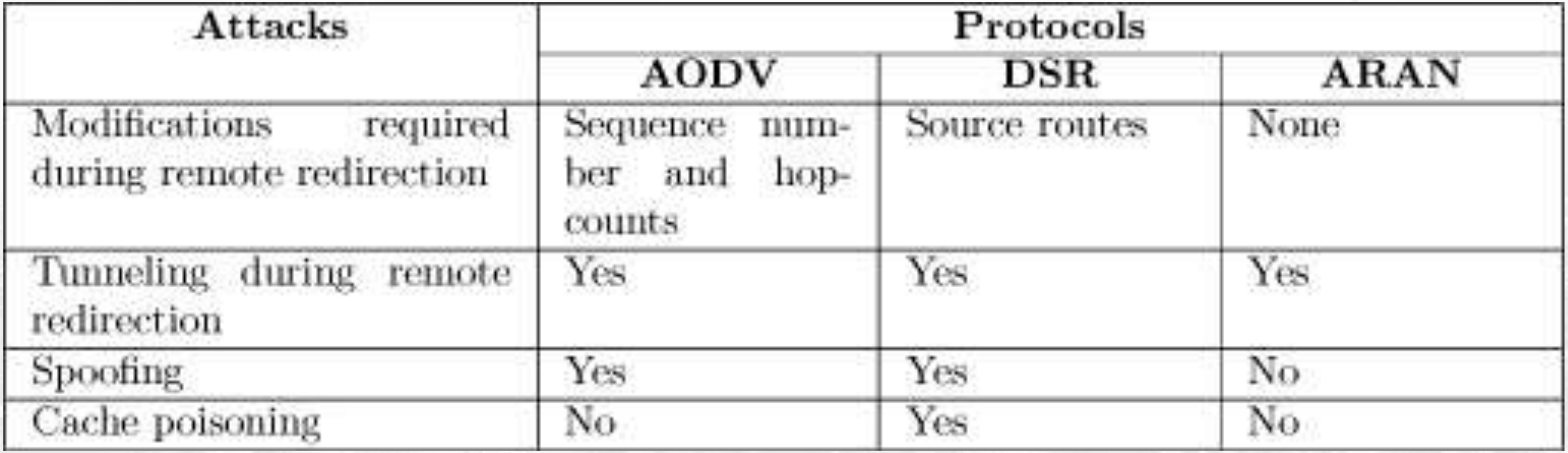
- Suppose an intermediate node B, on receiving an RDP packet from a node A, removes its neighbor's certificate, inserts its own certificate, and broadcasts the packet further.

- At final, destination node unicasts the REP packet to the source node along the reverse path.

$$D \text{ -→ } X: \ = [REP, IP_S, Cert_D, N_S, t]\ K_{D-}$$

Comparison of vulnerabilities of ARAN with DSR and AODV Protocols

- Table shows a comparison between the AODV, DSR, and ARAN protocols with respect to their security-related features.



Attacks	Protocols		
	AODV	DSR	ARAN
Modifications required during remote redirection	Sequence number and hop-counts	Source routes	None
Tunneling during remote redirection	Yes	Yes	Yes
Spoofing	Yes	Yes	No
Cache poisoning	No	Yes	No

Security-Aware AODV Protocol

- A malicious intermediate node could advertise that it has the shortest path to the destination, thereby redirecting all the packets through itself. This is known as a blackhole attack

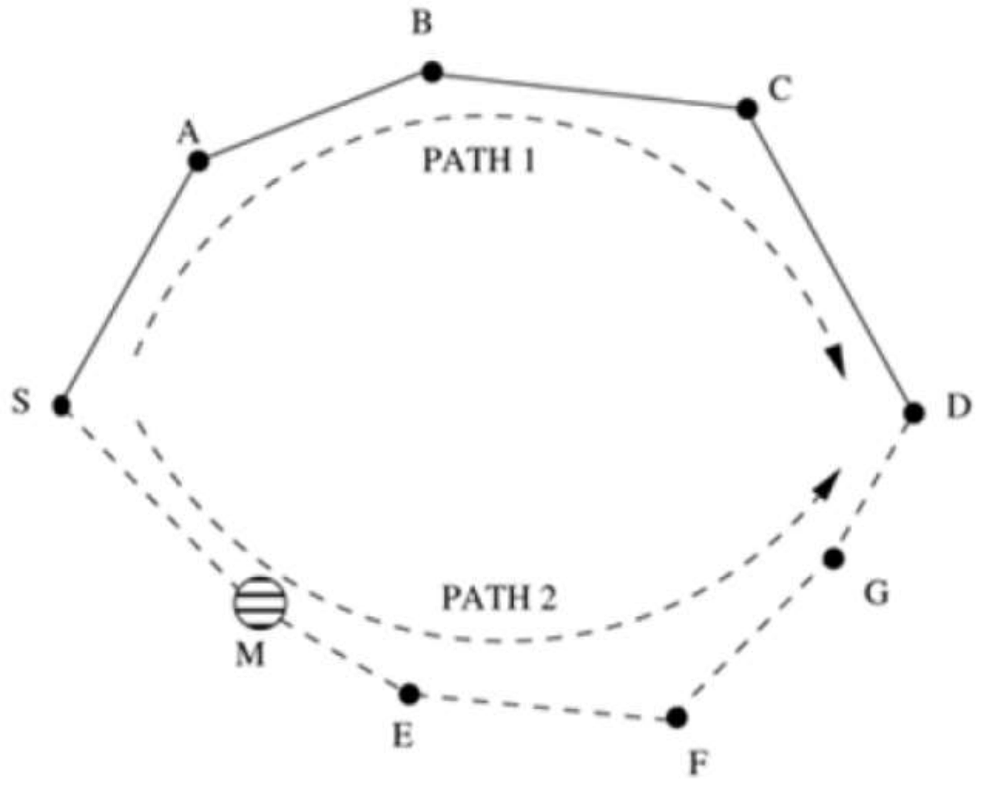
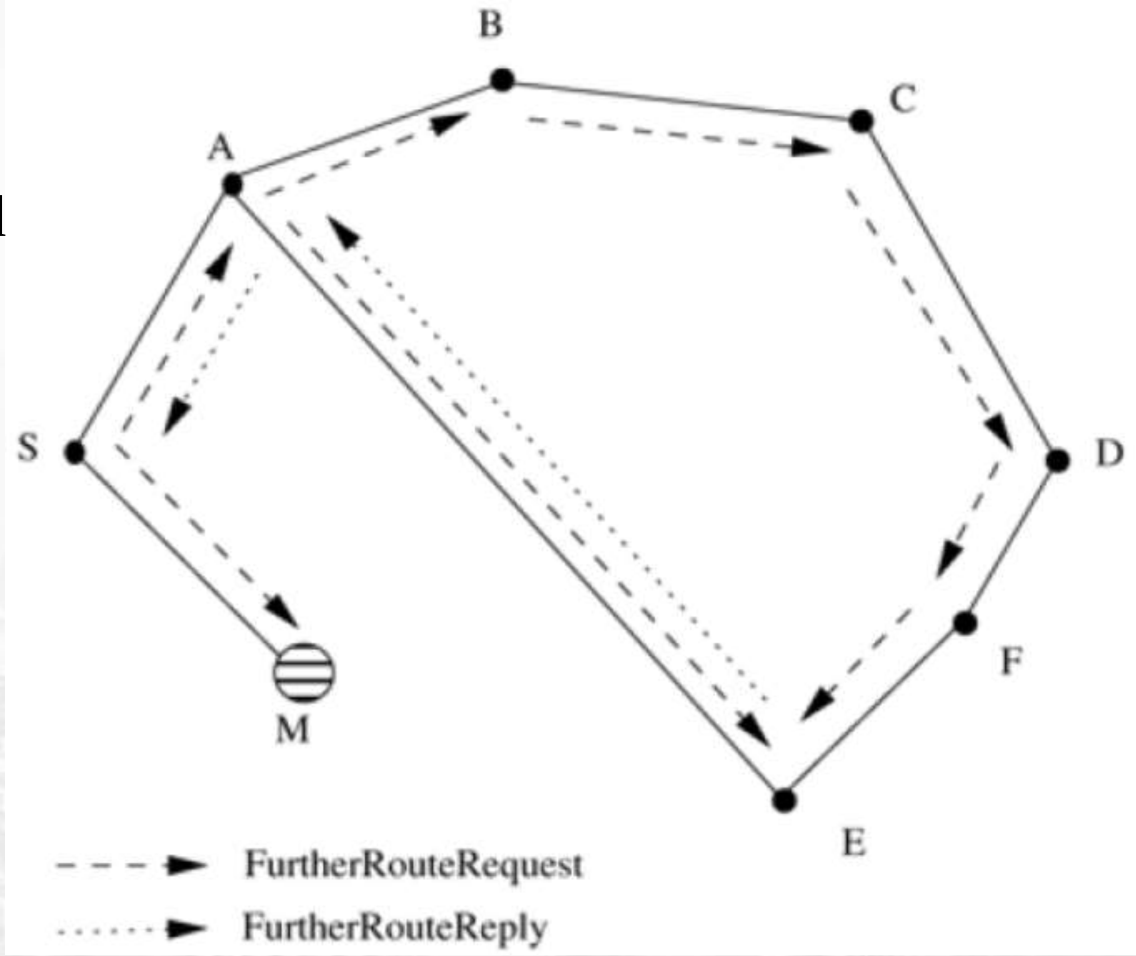


illustration of blackhole problem

Solutions for the Blackhole Problem:

- One solution is to restrict the intermediate nodes from originating RouteReply packets.
- Only the destination node would be permitted to initiate RouteReply packets.
- Another solution, as soon as the Route Replypacket is received from one of the intermediate nodes, another RouteRequest packet is sent from the source node to the neighbor node of the intermediate node in the path.
- This is to ensure that such a path exists from the intermediate node to the destination node.

- Node M is a malicious node which is not present in the routing list of node E.
- This protocol eliminates the blackhole attack caused by a single attacker.
- The disadvantage: control overhead of the routing protocol increases considerably.
- Also, if the malicious nodes work in a group, this protocol fails miserably.



Propagation of *FurtherRouteRequest* and *FurtherRouteReply*

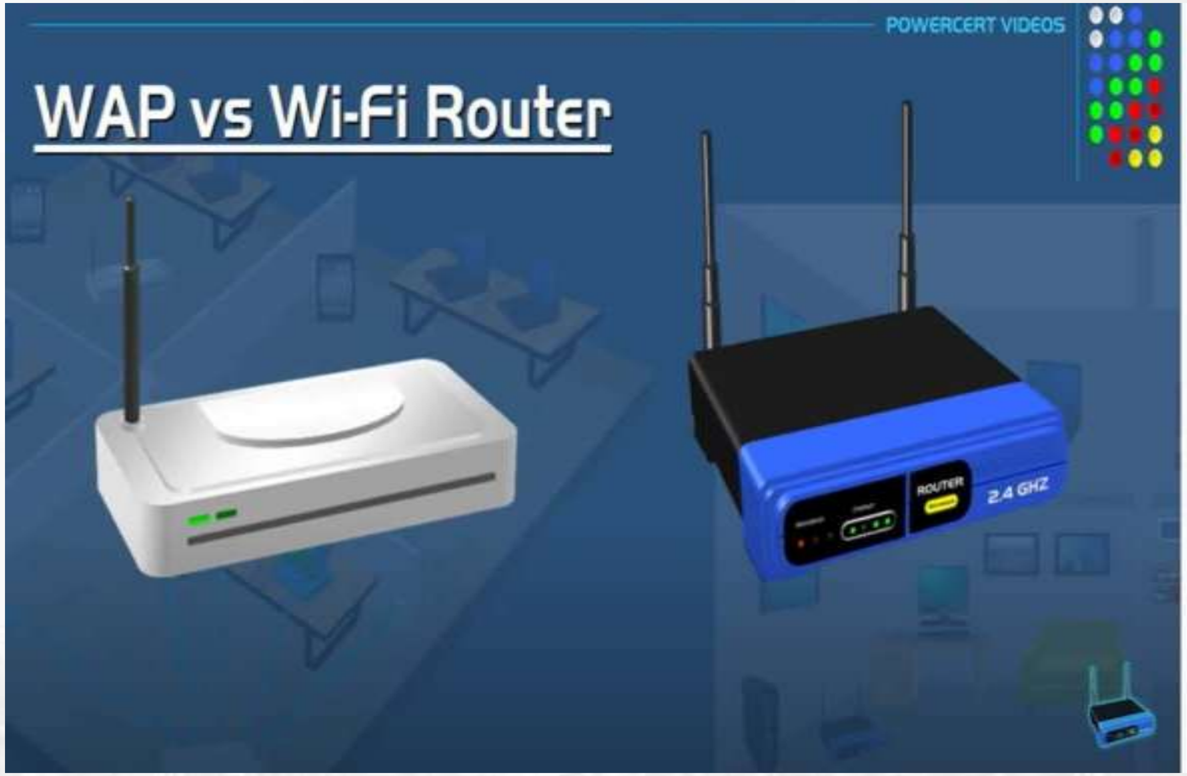
Wi-Fi Security and Access Point Security

Wi-Fi Security and Access Point Security

- Choice: the physical size of the network, the needs of the organization and the total number of Wi-Fi users.

- An AP is like an Ethernet hub.

- Wireless Router - Multi-function Device
  - Incorporates a switch, router, and wireless access point.
  - Provides routing, switching and wireless connectivity.
  - Wireless routers, are simple in design and used in home networks providing services such as NAT and DHCP



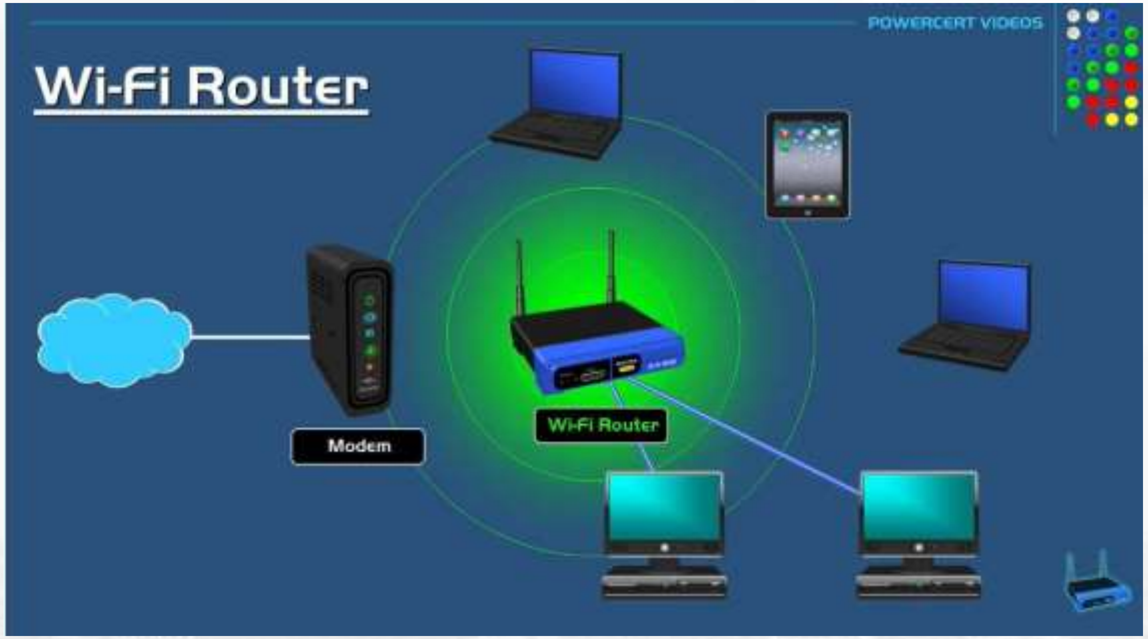
- AP functions
  - Acts as “base station” for wireless network
  - Acts as a bridge between wireless and wired networks
  - Can connect to wired network by a cable

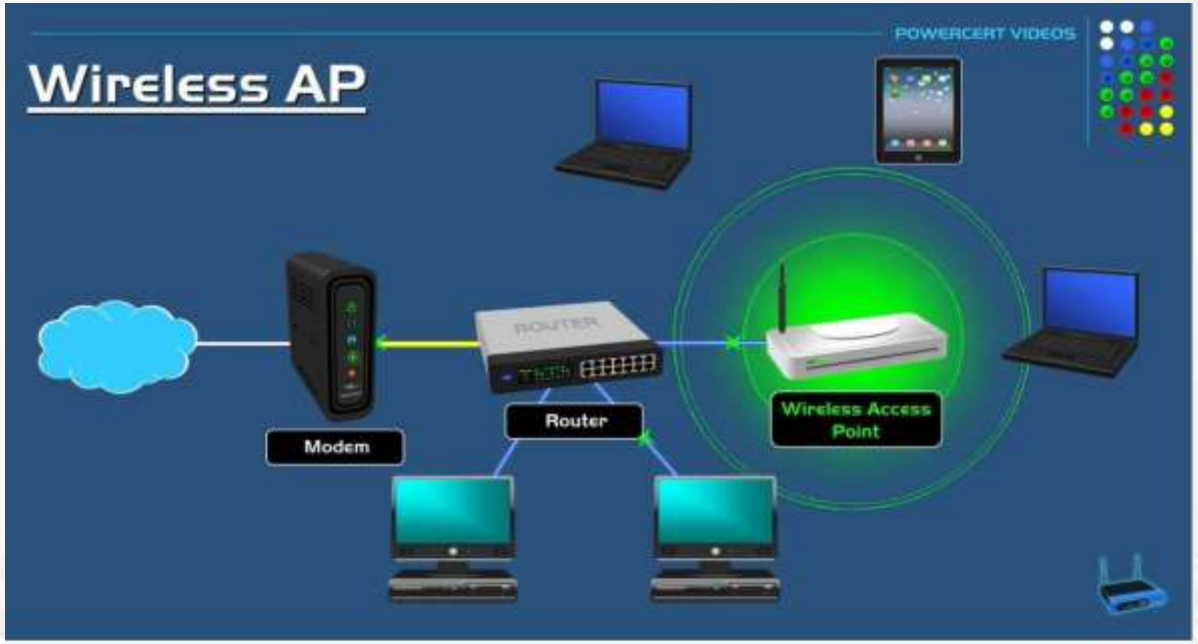
Wi-Fi Security

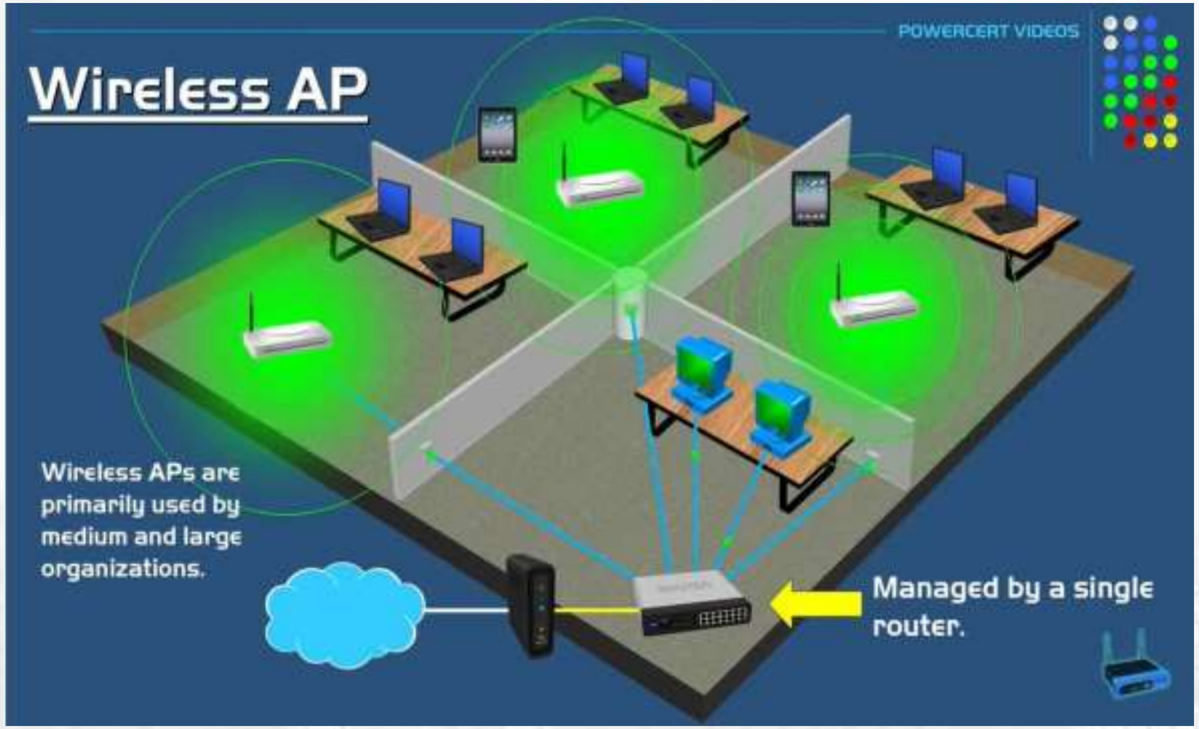
Wi-Fi Security is the protection of devices and networks connected in wireless environment

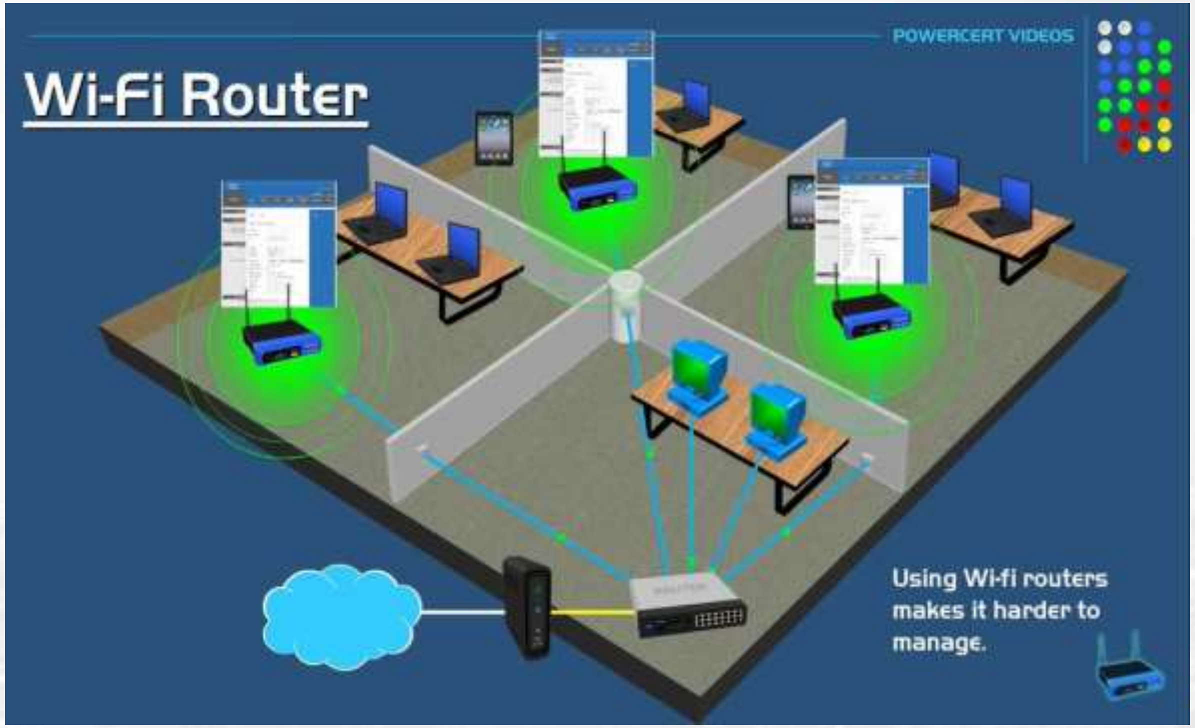
Four main types of infrastructure elements

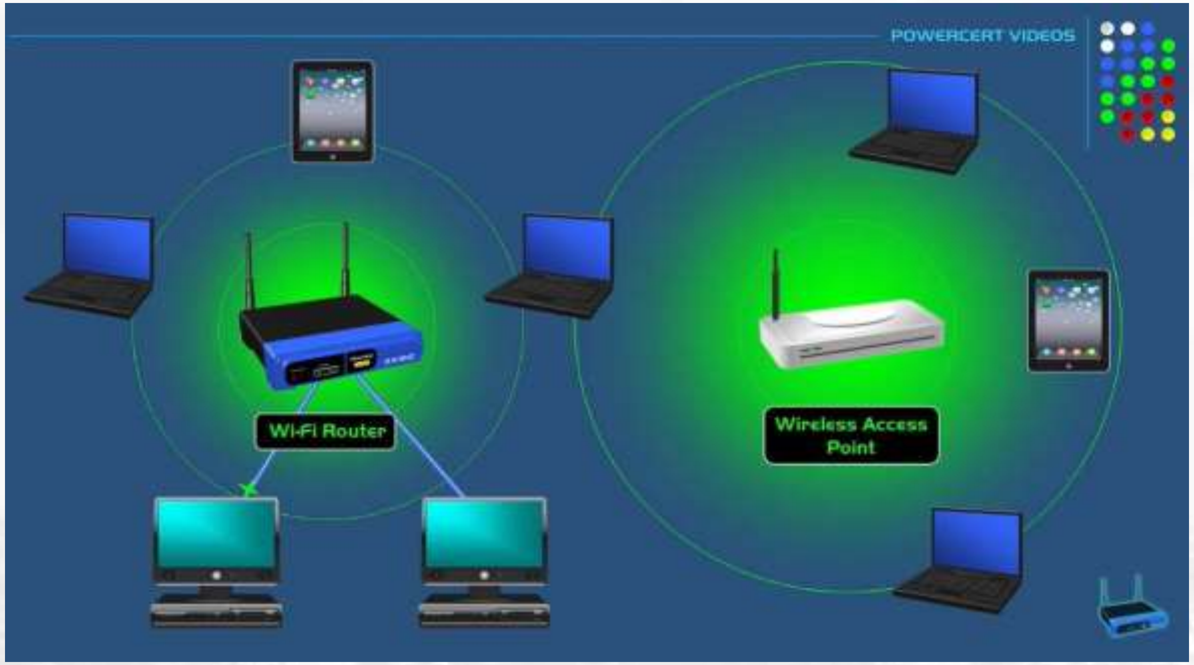
1. Authentication infrastructure
2. *Radio security*
3. *Packet filtering*
4. *Access to remote services (roaming)*

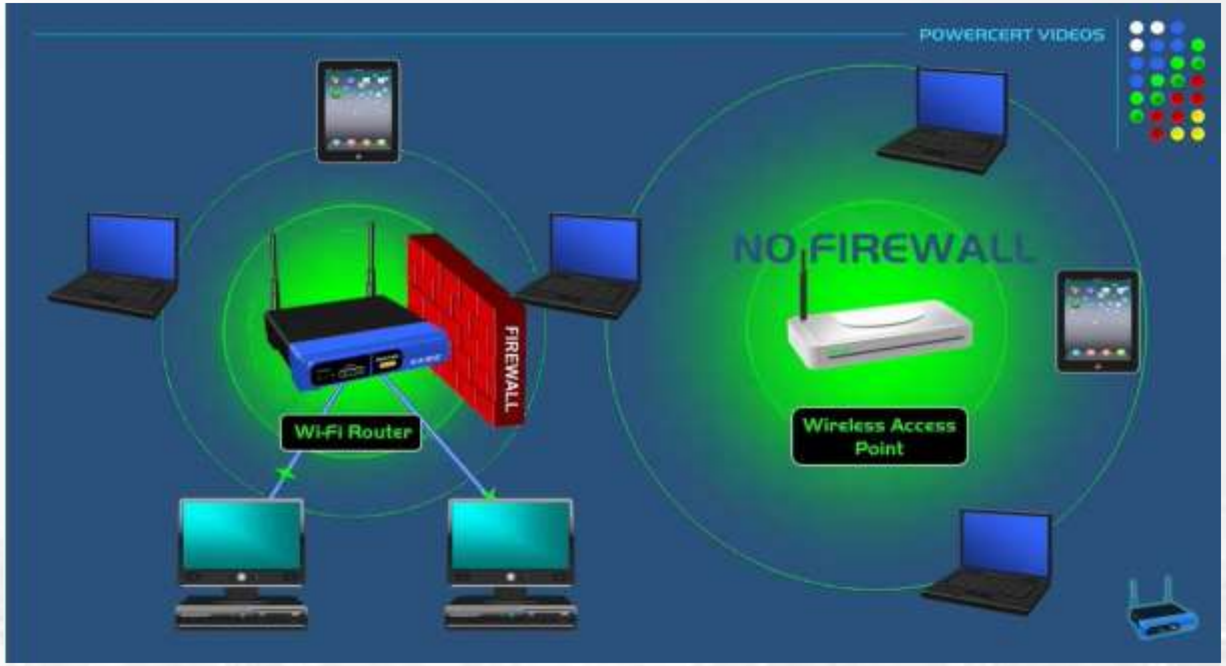

POWERCERT VIDEOS
Wi-Fi Router
Modem
Wi-Fi Router

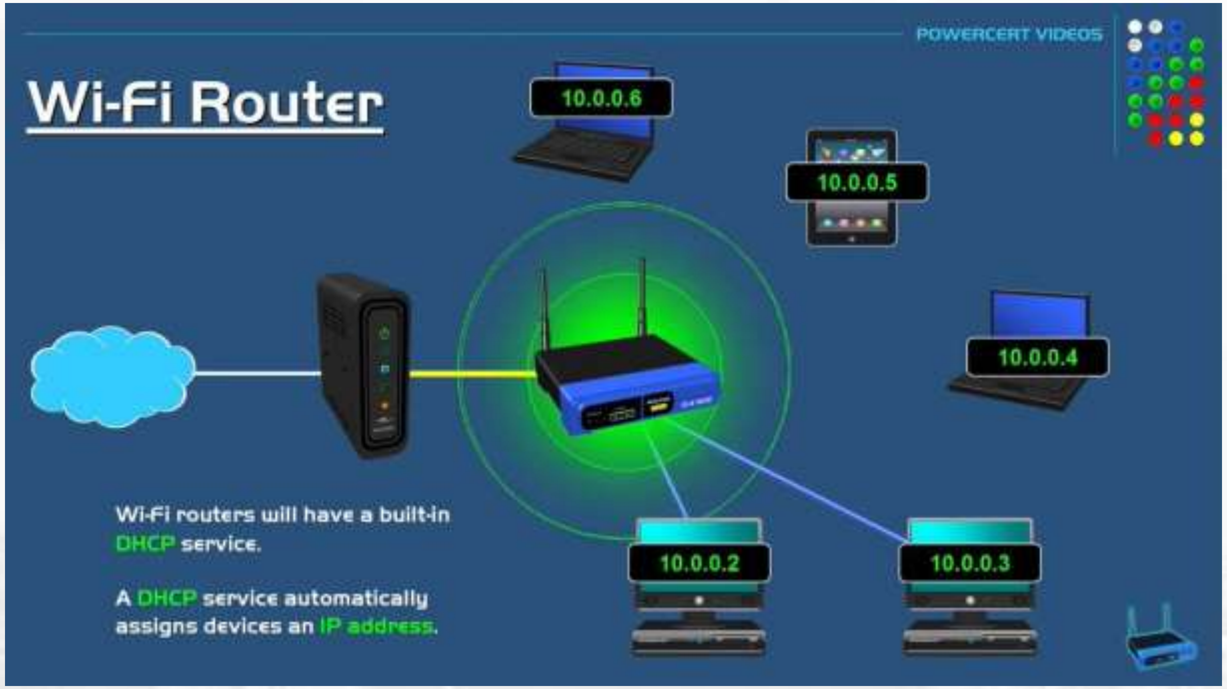

POWERCERT VIDEOS
Wireless AP
Modem
Router
ROUTER
Wireless Access Point


POWERCERT VIDEOS
Wireless AP
Wireless APs are primarily used by medium and large organizations.
Managed by a single router.


POWERCERT VIDEOS
Wi-Fi Router
Using Wi-fi routers makes it harder to manage.


POWERCERT VIDEOS
Wi-Fi Router
Wireless Access Point

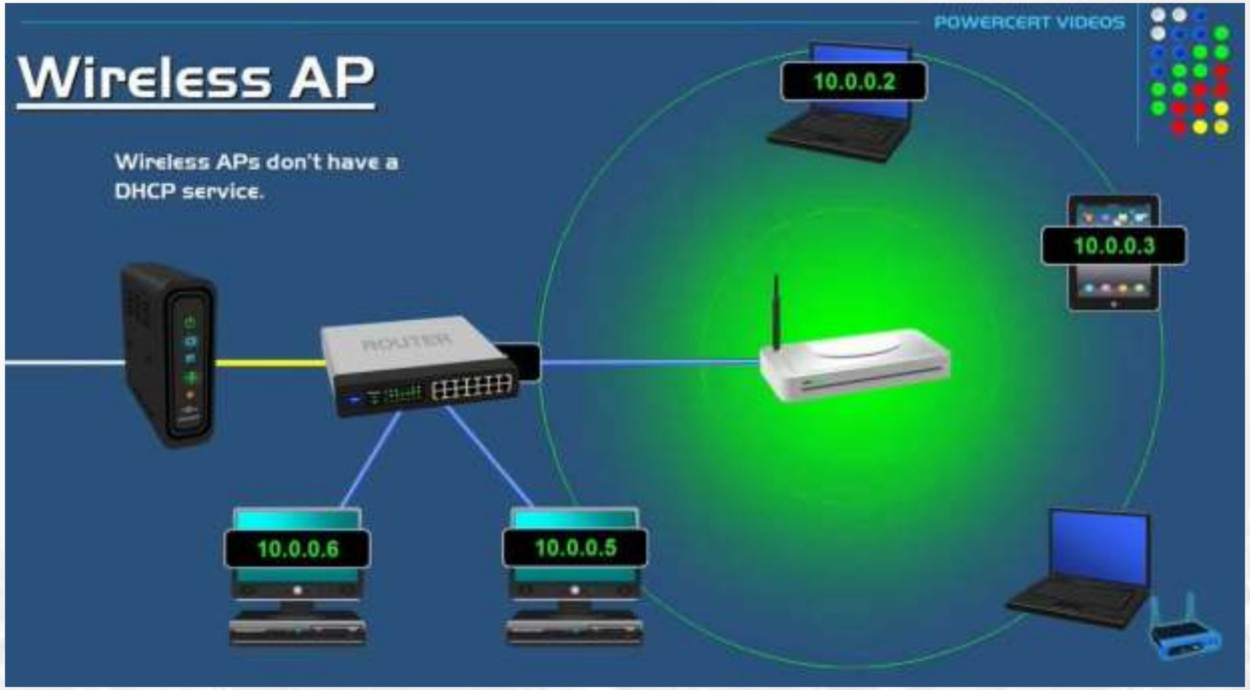

POWERCERT VIDEOS
NO FIREWALL
FIREWALL
Wi-Fi Router
Wireless Access Point



Wi-Fi Router

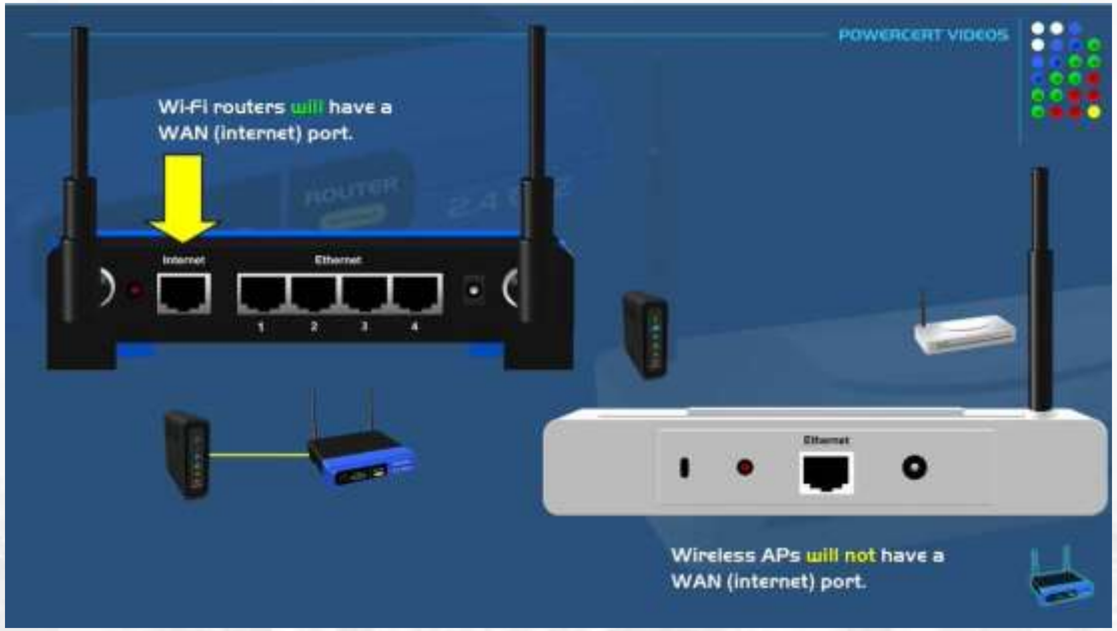
Wi-Fi routers will have a built-in DHCP service.

A DHCP service automatically assigns devices an IP address.



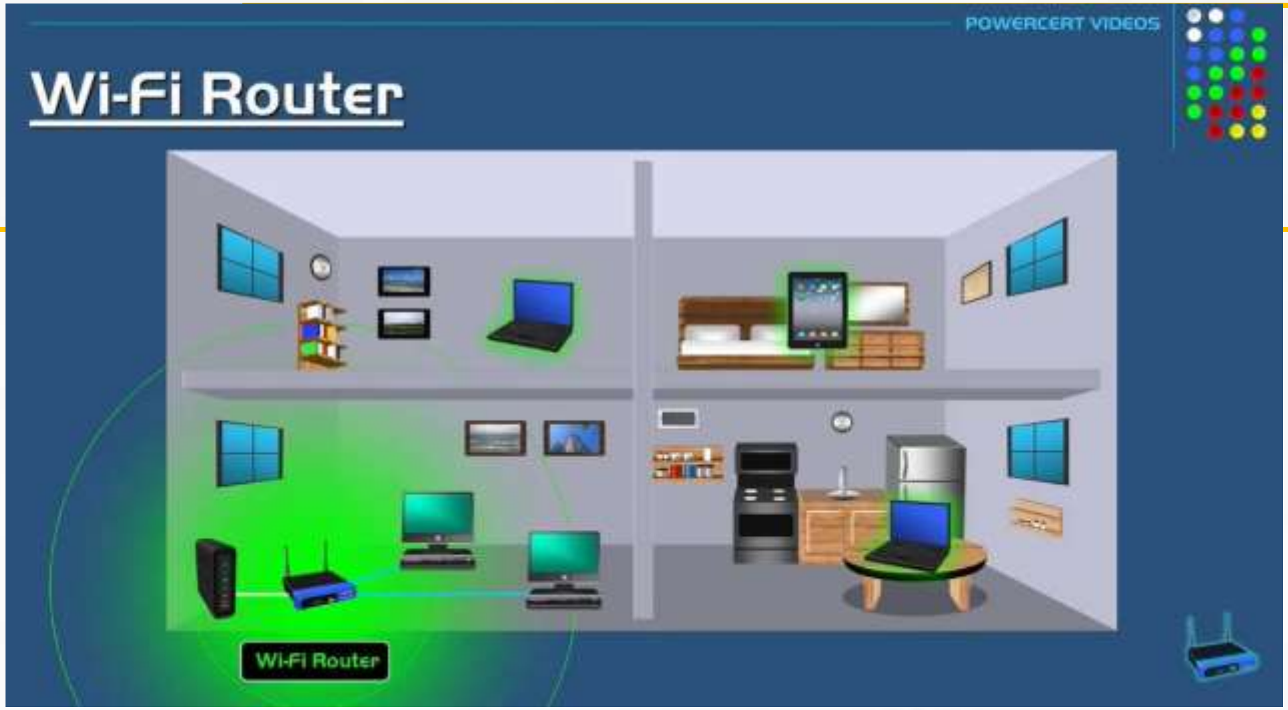
Wireless AP

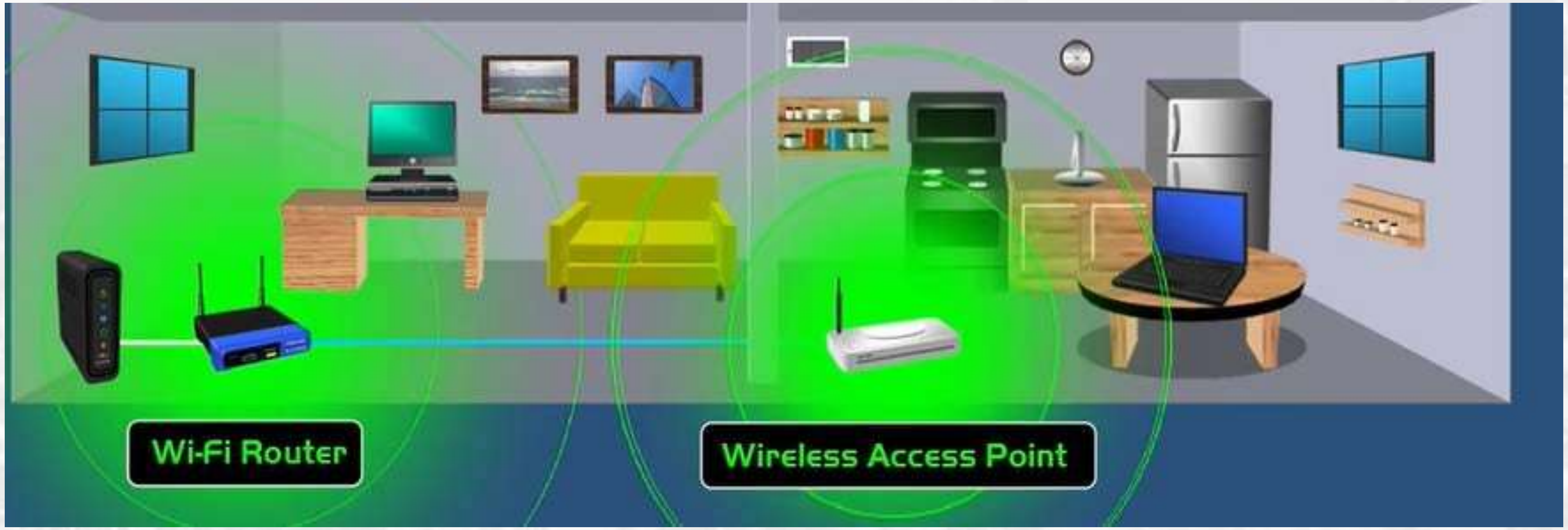
Wireless APs don't have a DHCP service.



Wi-Fi routers will have a WAN (internet) port.

Wireless APs will not have a WAN (internet) port.


POWERCERT VIDEOS
Wi-Fi Router
Wi-Fi Router


Wi-Fi Router
Wireless Access Point

Attacks on wireless networks

Attacks may cause

- Loss of proprietor information,
- Legal costs and recovery,
- A tarnished image and
- Loss of network services.

1. Passive attacks

- An attack is called passive when an unauthorized person obtains access to a resource without changing its content.
- Attacks may be passive eavesdropping or traffic analysis, sometimes called analysis of traffic flow.

Eavesdropping: The attacker listens to the transmissions in order to retrieve the content of messages.

For example, a person listens to the transmissions over a LAN network between two stations or listens to transmissions between a wireless phone and a base station.

Traffic analysis: The attacker obtains information by monitoring transmissions to detect types or classical models in the communication.

Attacks on wireless networks

2. Active attacks

An attack is called active when making unauthorized changes are made to messages and data flows or files.

1. ***Masquerade:*** The attacker impersonates an authorized user and obtains access to certain privileges.
2. ***Replay:*** The attacker monitors the transmissions (passive attack) and retransmits messages to a legitimate user.
3. ***Message modification:*** The attacker alters a legitimate message by deleting, adding, modifying or rearranging the contents.
4. ***Denial-of-service:*** The attacker prevents or prohibits normal usage of the management of the communication medium.

3. Denial-of-service attacks

Consists of making a large number of requests to the access point until it crashes.

Many denial-of-service attacks can be achieved using the ICMP

To flood a server, the easiest way is to send messages like ping messages asking it to return a reply.

Attacks on wireless networks

4. ***TCP attacks***

- The TCP protocol works with some port numbers which determine a socket address, i.e. a network access point.
- This socket address is formed by the concatenation of the IP address and the port number.
- Each application has a port number, for example, 80 for an HTTP application.
- An attacker can use a classical port to enter a computer or a company network.
- The user opens a TCP connection on a port that corresponds to an application to run.
- The hacker starts to use the same port disguised as that user and send the responses.

Attacks on wireless networks

5. ***Trojan attack***

- In a Trojan attack, the attacker introduces into the terminal station a program that makes it possible to memorize the login and the password.
- This information is sent to the outside by a message to an anonymous mailbox.
- Various techniques may be used for this, from a program that replaces the login manager to a hacker program that spies on what is happening in the terminal.
- This type of attack is fairly classic in wireless networks since a user can interfere with, via the access point, a PC and install spyware in it, allowing him/her to take the place of the user.

6. ***Dictionary attacks***

- Many chosen passwords are in the dictionary, so it is very easy for a machine to try them all.
- Simple solution to address this attack is to complicate passwords by adding capital letters, numbers and symbols like !, ?, &, etc.

Security in the IEEE 802.11 standard

IEEE 802.11 security mechanisms

A complete association with an access point requires the client to pass through three states

1) non-authenticated, non-associated;

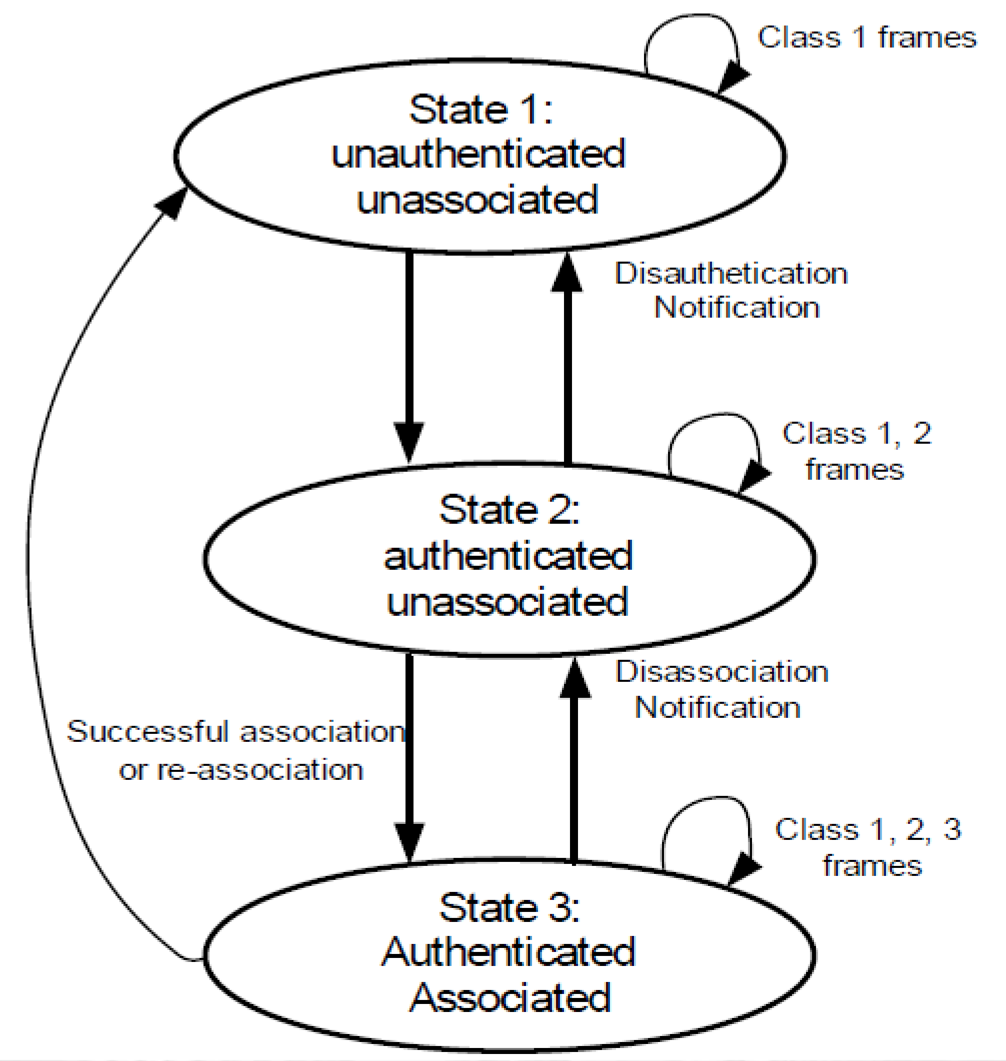
2) authenticated, non-associated;

3) authenticated, associated

Diagram describes the different states of a system and the transaction among these states.

- 802.11 exchanged frames may be of two types, **data** or **management frames**.
- To pass from one state to another, the WLAN station and the access point have to exchange management frames.

To authenticate a WLAN station in 802.11 wireless networks, a specific security mechanism, the WEP, has been defined.



The states of authentication in 802.11 for a WLAN station

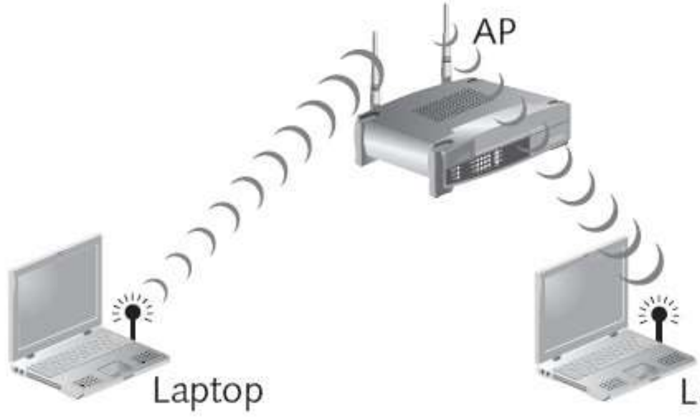
Wi-fi Security Protocol: WEP

- WEP stands for Wired Equivalent Privacy
- The fundamental goal of WEP is to prevent eavesdropping, which is confidentiality.
- The second goal is to allow authorized access to a wireless network, which is availability.
- The third goal is to prevent the tampering of any wireless communication, which is integrity.
- The WEP protocol is based on RSA Securities' RC4 stream cipher.
- Version1: 40-bit encryption key and 24-bit initialization vector, which equals 64 bits
- Version2: 104-bit encryption key and 24-bit initialization vector, which equals 128 bits.

WEP (Wired Equivalent Privacy)

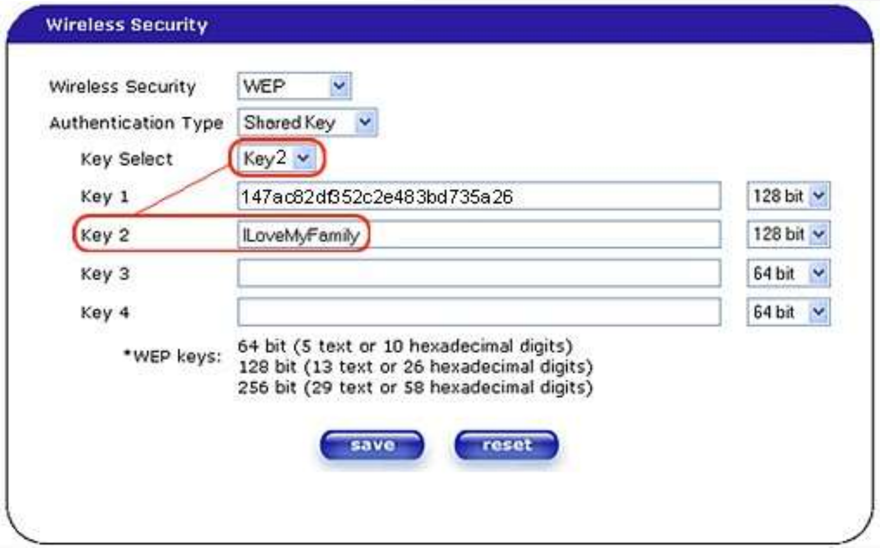
1. *Access control*
2. SSID (Service Set ID)
3. *The ACL (Access Control List)*
4. *Confidentiality*
5. *Authentication*
6. *Data integrity*

Key 1	2e3f4	Default key
Key 2	9u761	
Key 3	243yt	
Key 4	mju8e	



Key 1	2e3f4	
Key 2	9u761	
Key 3	243yt	
Key 4	mju8e	Default key

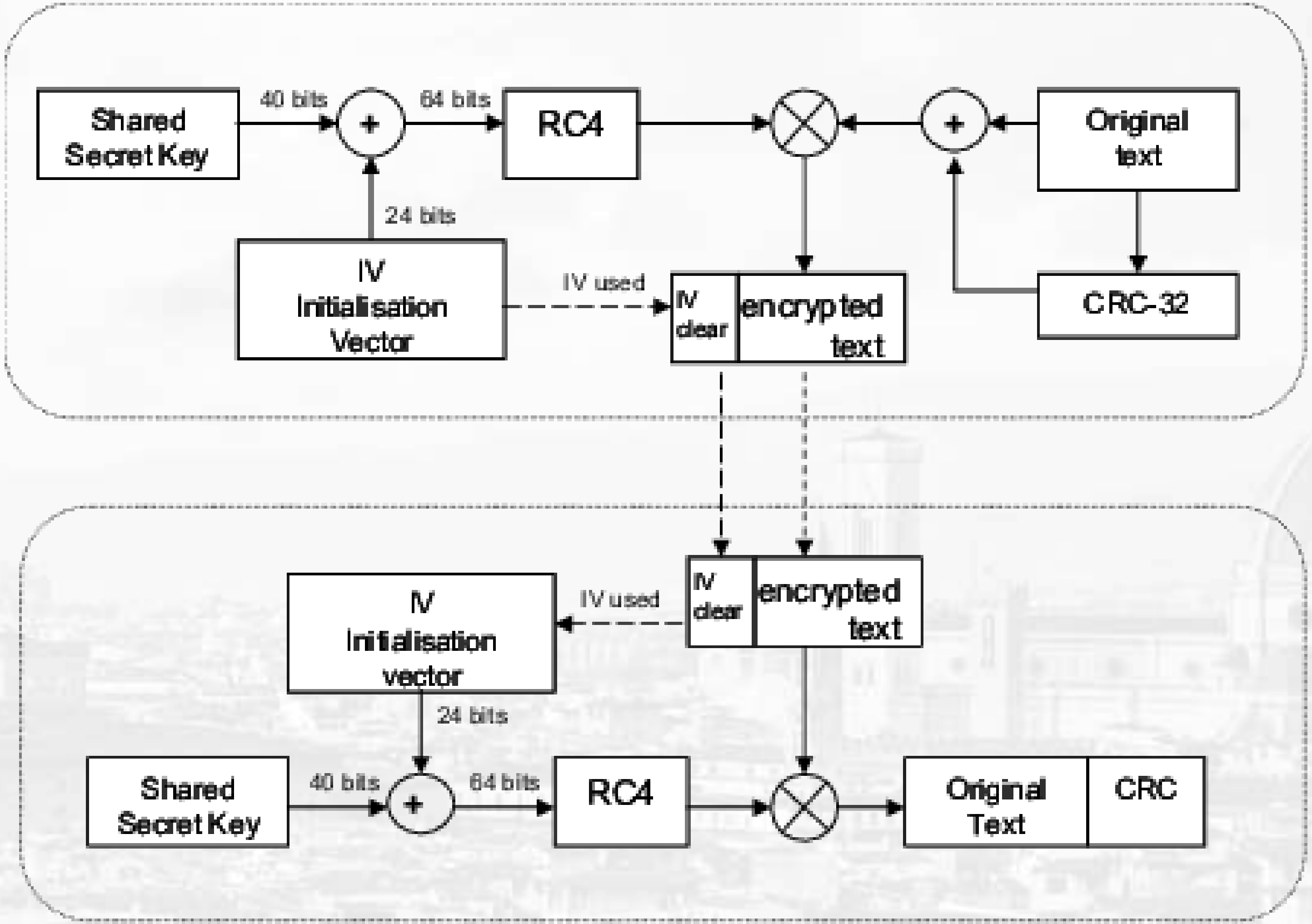
Key 1	2e3f4	
Key 2	9u761	Default key
Key 3	243yt	
Key 4	mju8e	



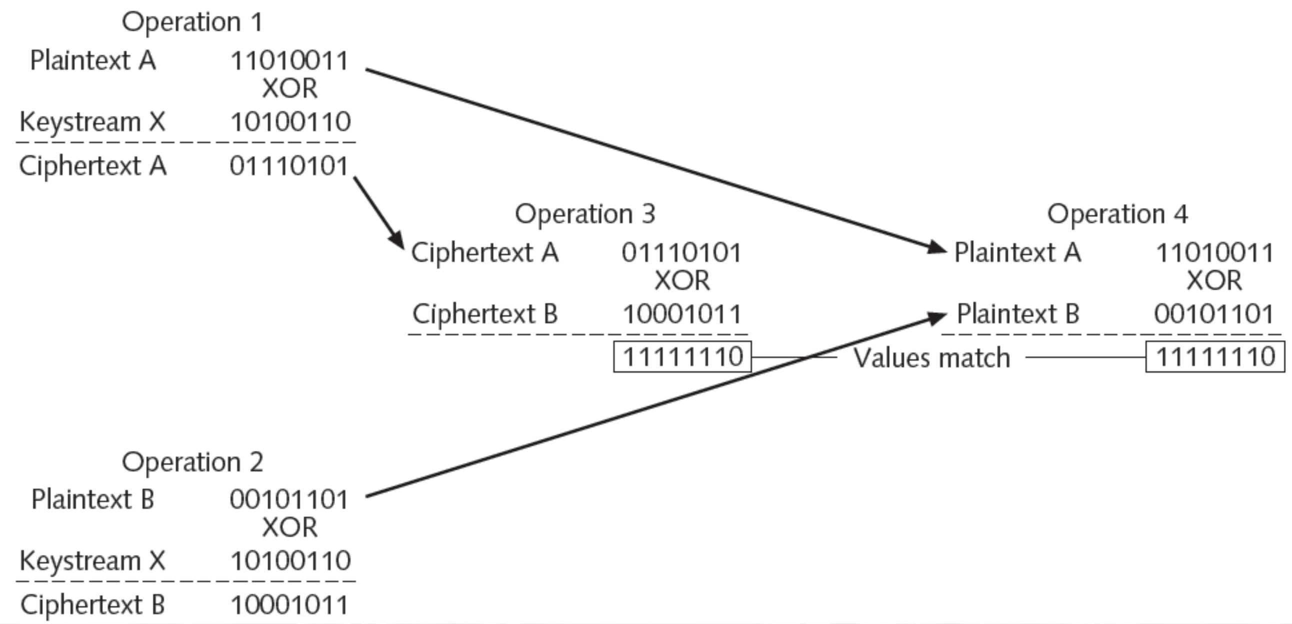
Wireless Security

Wireless Security	WEP	
Authentication Type	Shared Key	
Key Select	Key2	
Key 1	147ac82df352c2e483bd735a26	128 bit
Key 2	ILoveMyFamily	128 bit
Key 3		64 bit
Key 4		64 bit

*WEP keys: 64 bit (5 text or 10 hexadecimal digits)
128 bit (13 text or 26 hexadecimal digits)
256 bit (29 text or 58 hexadecimal digits)


Shared Secret Key
40 bits
64 bits
RC4
Original text
24 bits
IV Initialisation Vector
IV used
IV clear
encrypted text
CRC-32
IV clear
encrypted text
IV Initialisation vector
IV used
24 bits
Shared Secret Key
40 bits
64 bits
RC4
Original Text
CRC

- WEP vulnerabilities
  - Violates cardinal rule of cryptography: avoid a detectable pattern
  - Attackers can see duplication when IVs start repeating
- Keystream attack (or IV attack)
  - Attacker identifies two packets derived from same IV
  - Uses XOR to discover plaintext



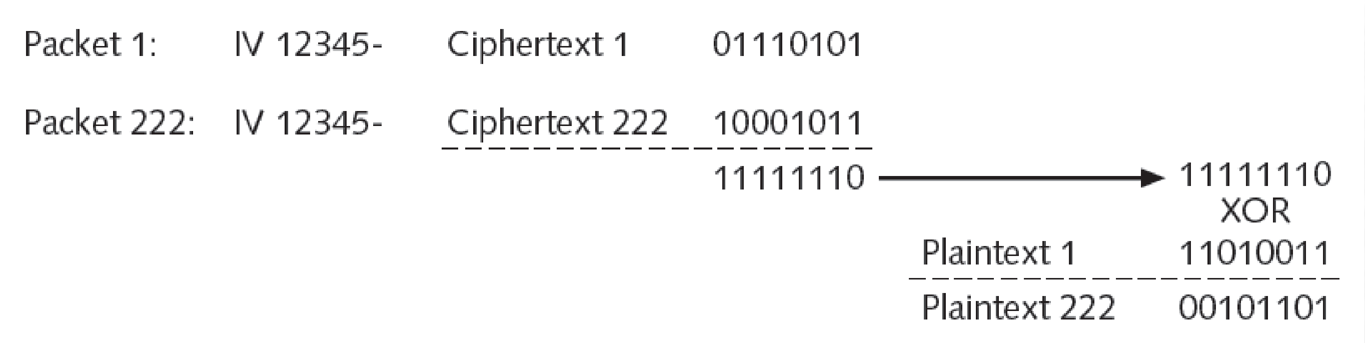
Operation 1
Plaintext A 11010011
XOR
Keystream X 10100110
Ciphertext A 01110101

Operation 2
Plaintext B 00101101
XOR
Keystream X 10100110
Ciphertext B 10001011

Operation 3
Ciphertext A 01110101
XOR
Ciphertext B 10001011
11111110

Operation 4
Plaintext A 11010011
XOR
Plaintext B 00101101
11111110

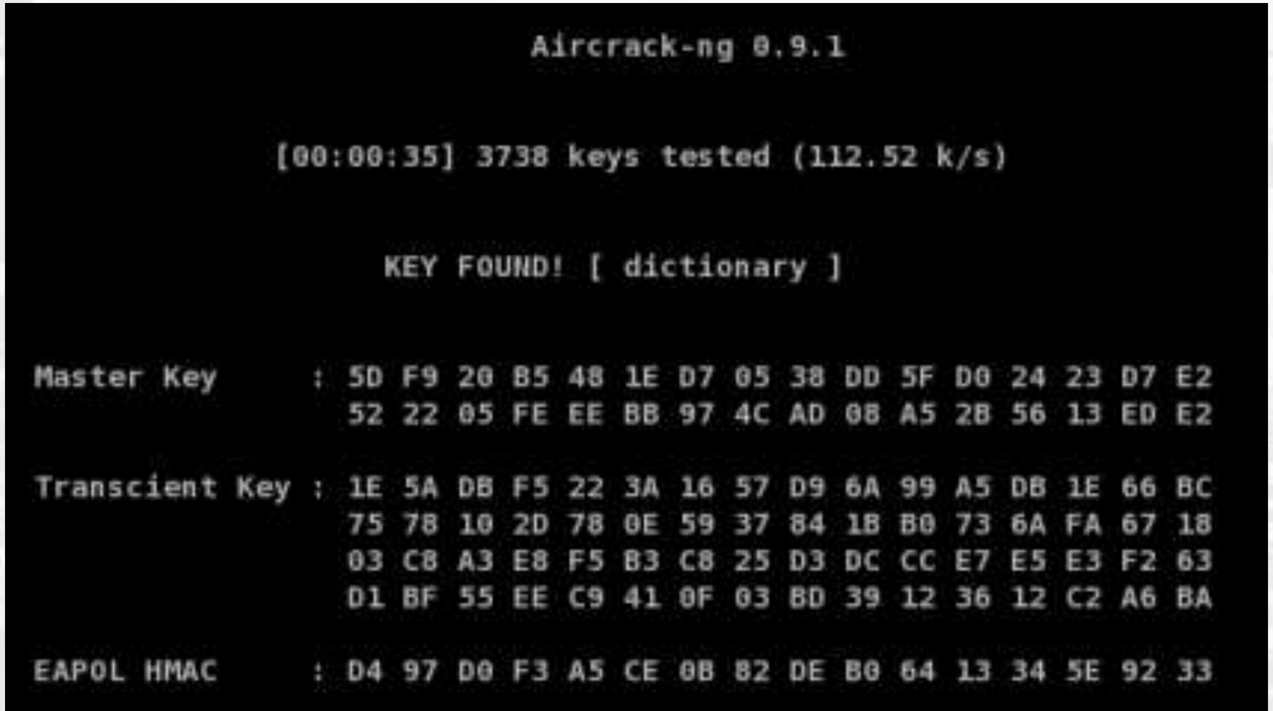
Values match



Packet 1: IV 12345- Ciphertext 1 01110101
Packet 222: IV 12345- Ciphertext 222 10001011
11111110

11111110
XOR
Plaintext 1 11010011
Plaintext 222 00101101

- With the right equipment, WEP can be cracked in just a few minutes
  - You need a support wireless card
  - Kismet
  - Aircrack-ng



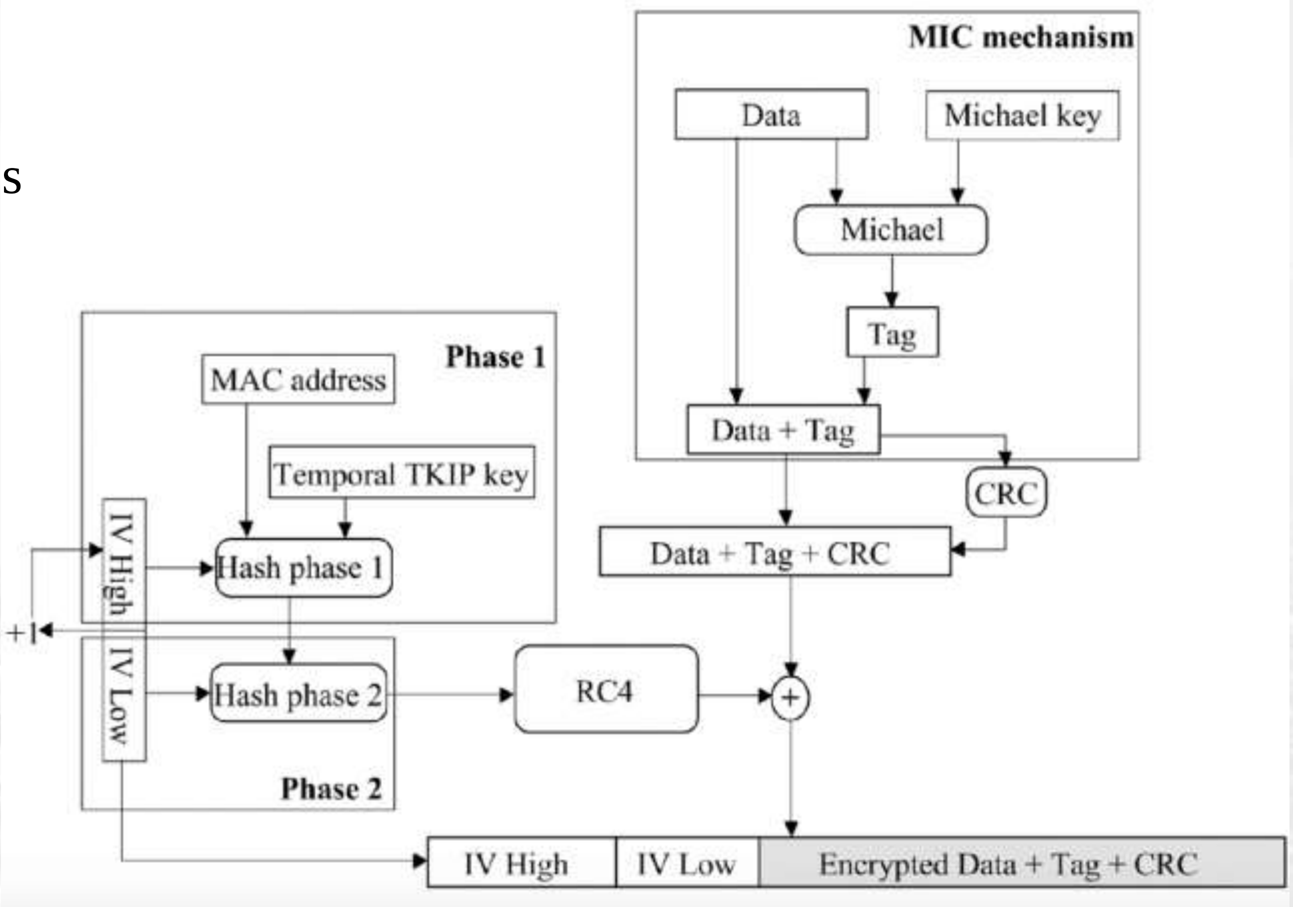
```
                         Aircrack-ng 0.9.1


                 [00:00:35] 3738 keys tested (112.52 k/s)


                     KEY FOUND! [ dictionary ]


 Master Key     : 5D F9 20 B5 48 1E D7 05 38 DD 5F D0 24 23 D7 E2
                  52 22 05 FE EE BB 97 4C AD 08 A5 2B 56 13 ED E2

 Transcient Key : 1E 5A DB F5 22 3A 16 57 D9 6A 99 A5 DB 1E 66 BC
                  75 78 10 2D 78 0E 59 37 84 1B B0 73 6A FA 67 18
                  03 C8 A3 E8 F5 B3 C8 25 D3 DC CC E7 E5 E3 F2 63
                  D1 BF 55 EE C9 41 0F 03 BD 39 12 36 12 C2 A6 BA

 EAPOL HMAC     : D4 97 D0 F3 A5 CE 0B 82 DE B0 64 13 34 5E 92 33
```

- Wireless Security Solutions
  - Unified approach to WLAN security was needed
    - IEEE and Wi-Fi Alliance began developing security solutions
  - Resulting standards used today
    - IEEE 802.11i
    - WPA, WAP2 and WPA3

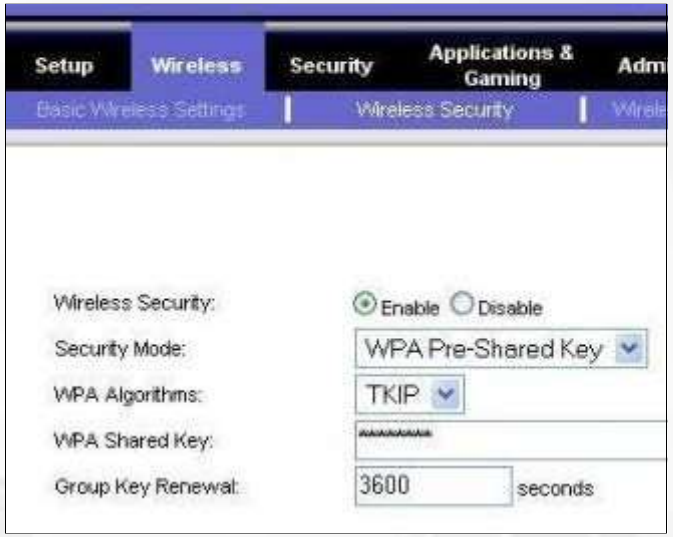
Wi-fi Security Protocol: WAP

- Wi-Fi Protected Access (WAP)

- Introduced in 2003 by the Wi-Fi Alliance
- A subset of IEEE 802.11i
- Design goal: protect present and future wireless devices
- Temporal Key Integrity Protocol (TKIP) Encryption
  - Used in WPA
  - Uses longer 128 bit key than WEP
  - Dynamically generated for each new packet



- ❖ Prescription-shared Key (PSK) Authentication
  - After AP configured, client device must have same key value entered
  - Key is shared prior to communication taking place
  - Uses a passphrase to generate encryption key
  - Key must be entered into both the access point and all wireless devices
  - Not used for encryption
    - Instead, it serves as the starting point (seed) for mathematically generating the encryption keys



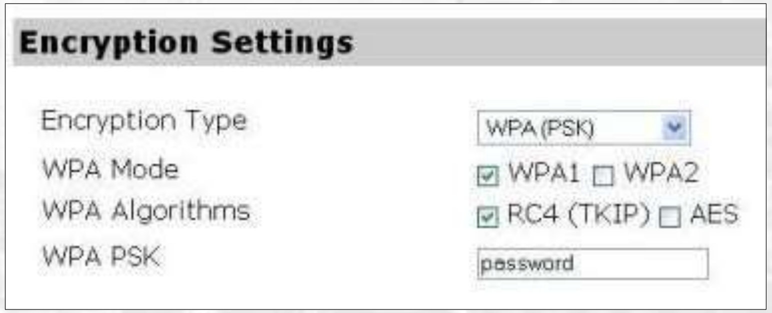
Wireless Security: ● Enable ○ Disable

Security Mode: WPA Pre-Shared Key

WPA Algorithms: TKIP

WPA Shared Key: ********

Group Key Renewal: 3600 seconds



Encryption Settings

Encryption Type: WPA (PSK)

WPA Mode: ☑ WPA1 □ WPA2

WPA Algorithms: ☑ RC4 (TKIP) □ AES

WPA PSK: password

- Vulnerabilities in WPA
  - Key management
    - Key sharing is done manually without security protection
    - Keys must be changed on a regular basis
    - Key must be disclosed to guest users
  - Passphrases
    - PSK passphrases of fewer than 20 characters subject to cracking

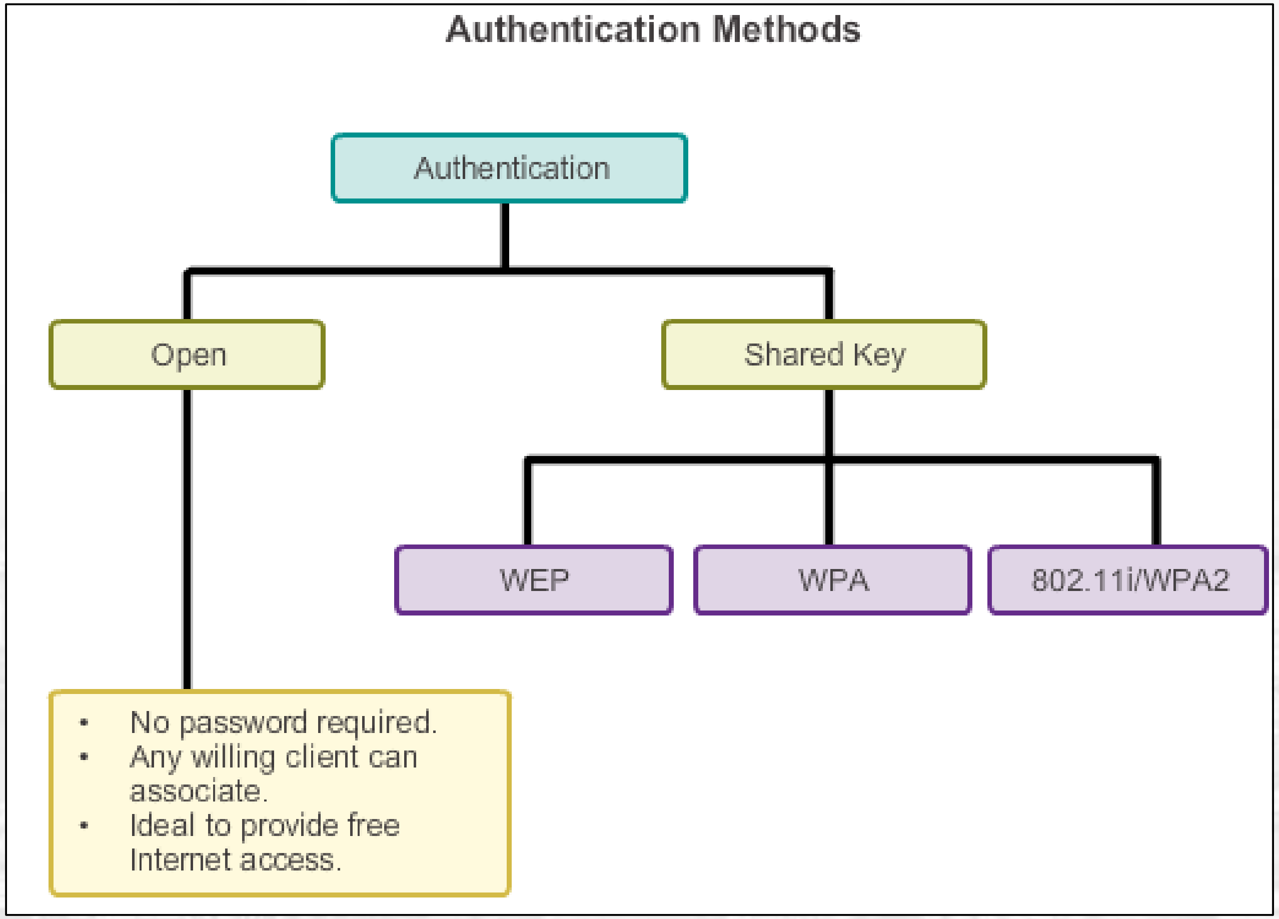
- With the right equipment, WEP can be cracked in just a few minutes
  - You need a support wireless card
  - Kismet
  - Aircrack-ng

Wi-Fi Protected Access 2 (WPA2)

- Second generation of WPA known as WPA2
  - Introduced in 2004
  - Based on final IEEE 802.11i standard
  - Uses Advanced Encryption Standard (AES)
  - Supports both PSK (Personal) and IEEE 802.1x (Enterprise) authentication
- AES-CCMP Encryption
  - Encryption protocol standard for WPA2
  - CCM is algorithm providing data privacy
  - CBC-MAC component of CCMP provides data integrity and authentication

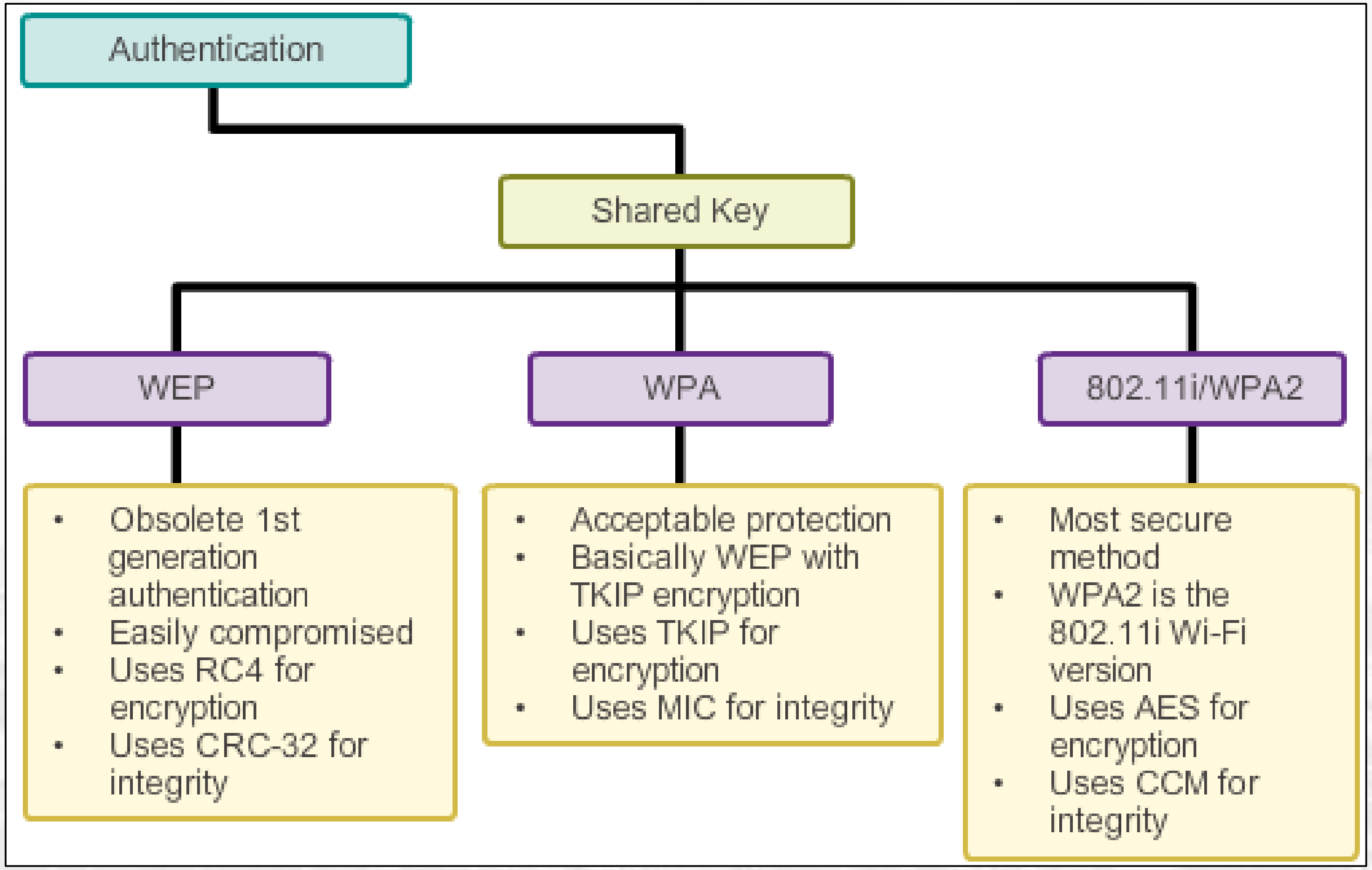
Wireless Security Overview

- Use authentication and encryption to secure a wireless network.



- No password required.
- Any willing client can associate.
- Ideal to provide free Internet access.

Shared Key Authentication Methods



Authentication

Shared Key

WEP

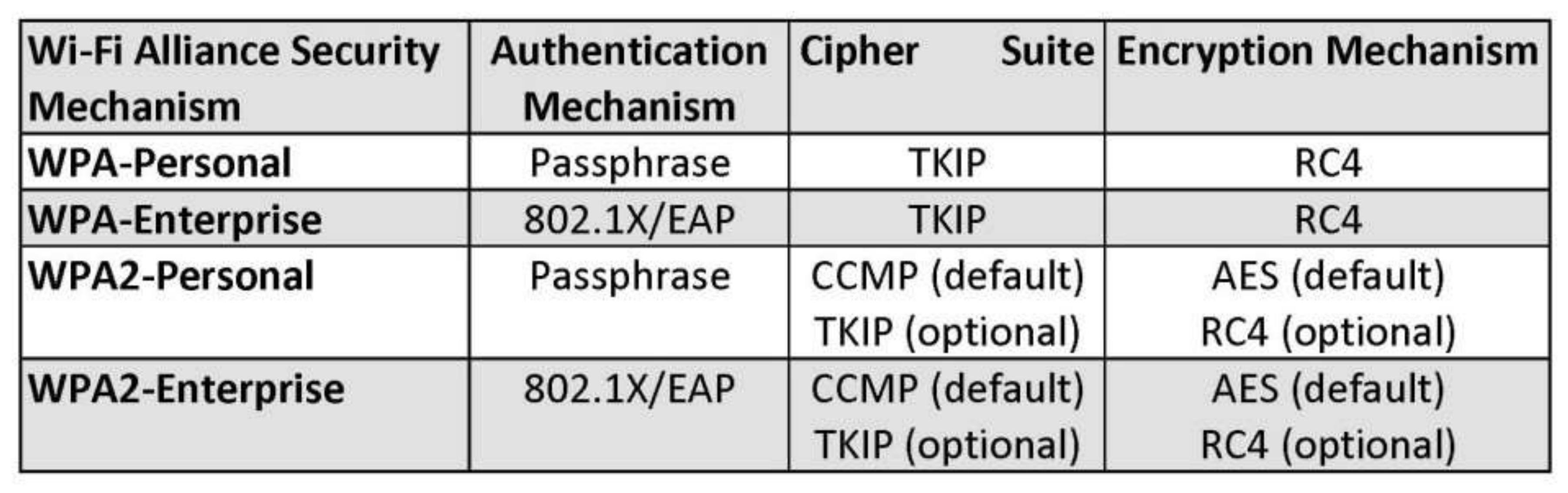
- Obsolete 1st generation authentication
- Easily compromised
- Uses RC4 for encryption
- Uses CRC-32 for integrity

WPA

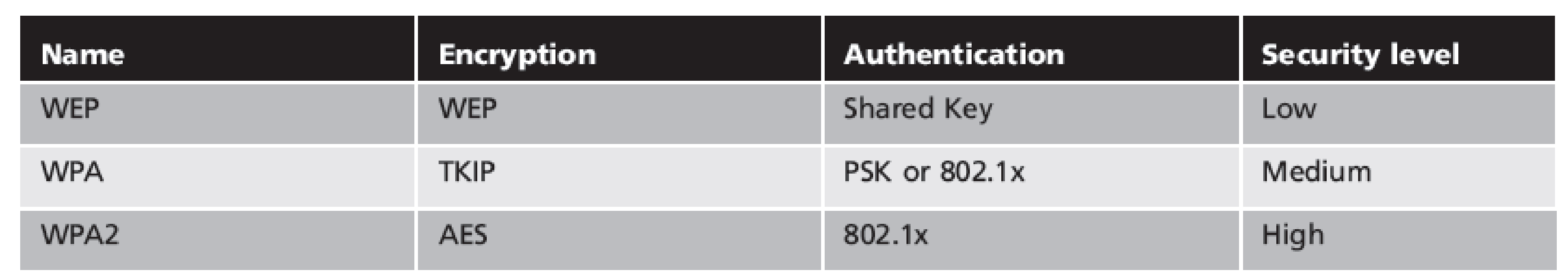
- Acceptable protection
- Basically WEP with TKIP encryption
- Uses TKIP for encryption
- Uses MIC for integrity

802.11i/WPA2

- Most secure method
- WPA2 is the 802.11i Wi-Fi version
- Uses AES for encryption
- Uses CCM for integrity

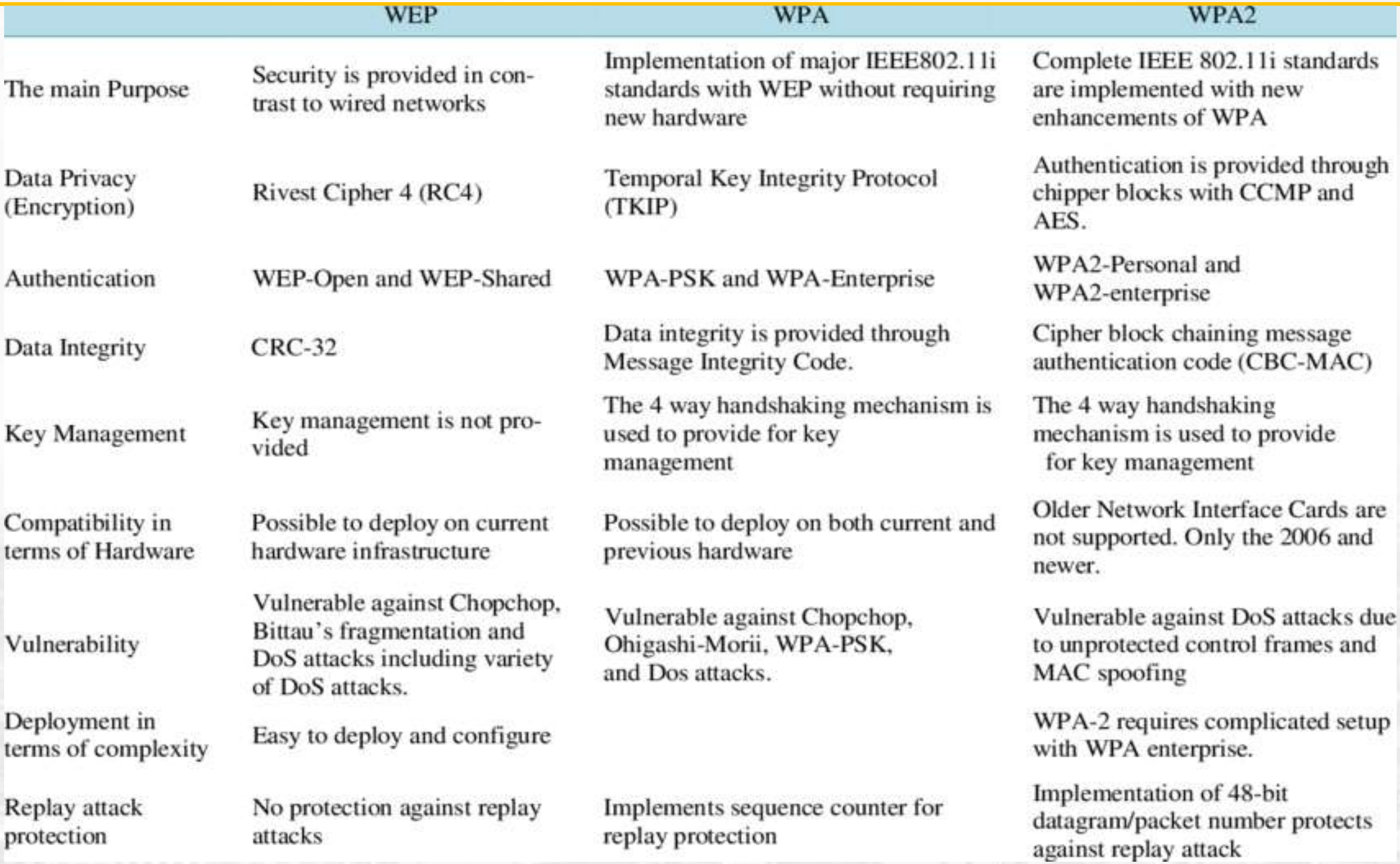


Wi-Fi Alliance Security Mechanism	Authentication Mechanism	Cipher Suite	Encryption Mechanism
WPA-Personal	Passphrase	TKIP	RC4
WPA-Enterprise	802.1X/EAP	TKIP	RC4
WPA2-Personal	Passphrase	CCMP (default) TKIP (optional)	AES (default) RC4 (optional)
WPA2-Enterprise	802.1X/EAP	CCMP (default) TKIP (optional)	AES (default) RC4 (optional)



Name	Encryption	Authentication	Security level
WEP	WEP	Shared Key	Low
WPA	TKIP	PSK or 802.1x	Medium
WPA2	AES	802.1x	High

Comparison



	WEP	WPA	WPA2
The main Purpose	Security is provided in contrast to wired networks	Implementation of major IEEE802.11i standards with WEP without requiring new hardware	Complete IEEE 802.11i standards are implemented with new enhancements of WPA
Data Privacy (Encryption)	Rivest Cipher 4 (RC4)	Temporal Key Integrity Protocol (TKIP)	Authentication is provided through chipper blocks with CCMP and AES.
Authentication	WEP-Open and WEP-Shared	WPA-PSK and WPA-Enterprise	WPA2-Personal and WPA2-enterprise
Data Integrity	CRC-32	Data integrity is provided through Message Integrity Code.	Cipher block chaining message authentication code (CBC-MAC)
Key Management	Key management is not provided	The 4 way handshaking mechanism is used to provide for key management	The 4 way handshaking mechanism is used to provide for key management
Compatibility in terms of Hardware	Possible to deploy on current hardware infrastructure	Possible to deploy on both current and previous hardware	Older Network Interface Cards are not supported. Only the 2006 and newer.
Vulnerability	Vulnerable against Chopchop, Bittau's fragmentation and DoS attacks including variety of DoS attacks.	Vulnerable against Chopchop, Ohigashi-Morii, WPA-PSK, and Dos attacks.	Vulnerable against DoS attacks due to unprotected control frames and MAC spoofing
Deployment in terms of complexity	Easy to deploy and configure		WPA-2 requires complicated setup with WPA enterprise.
Replay attack protection	No protection against replay attacks	Implements sequence counter for replay protection	Implementation of 48-bit datagram/packet number protects against replay attack

	WEP	WPA	WPA2	WPA3
Brief description	Ensure wired-like privacy in wireless	Based on 802.11i without requirement for new hardware	All mandatory 802.11i features and a new hardware	Announced by Wi-Fi Alliance
Encryption	RC4	TKIP + RC4	CCMP/AES	GCMP-256
Authentication	WEP-Open WEP-Shared	WPA-PSK WPA-Enterprise	WPA2-Personal WPA2-Enterprise	WPA3-Personal WPA3-Enterprise
Data integrity	CRC-32	MIC algorithm	Cipher Block Chaining Message Authentication Code (based on AES)	256-bit Broadcast/Multicast Integrity Protocol Galois Message Authentication Code (BIP-GMAC-256)
Key management	none	4-way handshake	4-way handshake	Elliptic Curve Diffie-Hellman (ECDH) exchange and Elliptic Curve Digital Signature Algorithm (ECDSA)

Security in IPV4 and IPv6 protocols

Learning Resources

Text books

1. C. Siva Ram Murthy, B.S. Manoj, “Adhoc Wireless Networks Architectures and Protocols”, PHI, ISBN - 9788131706885, 2007.
2. Nekoley Elenkov, “Android Security internals”, No Starch Press, ISBN-10: 1-59327-581-1 ISBN-13: 978-1-59327-581

Reference Books

1. KiaMakki, Peter Reiher, “Mobile and Wireless Network Security and Privacy “, Springer, ISBN 978-0-387-71057-0, 2007.
2. Hakima Chaouchi, Maryline Laurent-Maknavicius , “Wiress and Mobile Networks Security”, Wiley publication, ISBN 978-1-84821-117-9
3. Noureddine Boudriga, “Security of Mobile Communications”, ISBN 9780849379413, 2010.
4. Kitsos, Paris; Zhang, Yan, “RFID Security Techniques, Protocols and System-On-Chip Design”, ISBN 978-0-387-76481-8, 2008.
5. Johny Cache, Joshua Wright and Vincent Liu,” Hacking Wireless Exposed: Wireless Security Secrets & Solutions “, second edition, McGraw Hill, ISBN: 978-0-07-166662-6, 2010
6. Tim Speed, Darla Nykamp,Mari Heiser,Joseph Anderson,Jaya Nampalli, "Mobile Security: How to Secure, Privatize, and Recover Your Devices", Copyright © 2013 Packt Publishing, ISBN 978-1-84969-360-8

Learning Resources

Web Resources:

i. http://whatis.techtarget.com/definition/mobile-security

ii. http://techgenix.com/security/mobile-wireless-security/

Weblinks

i. https://en.wikipedia.org/wiki/Mobile_security

MOOCs:

i. https://www.ntnu.edu/studies/courses/TTM4137#tab=omEmnet
ii. http://nptel.ac.in/courses/106105160/37
iii. https://www.eccouncil.org/
iv. https://www.csoonline.com/article/2122635/mobile-security/wireless-security--the-basics.html

THANK
YOU FOR
LISTENING
ANY
QUESTION ?