Wi-Fi Technology Fundamentals

Module-4

Security in Wi-Fi

Session-4a

Various Wi-Fi Security Protocols

Recap …..

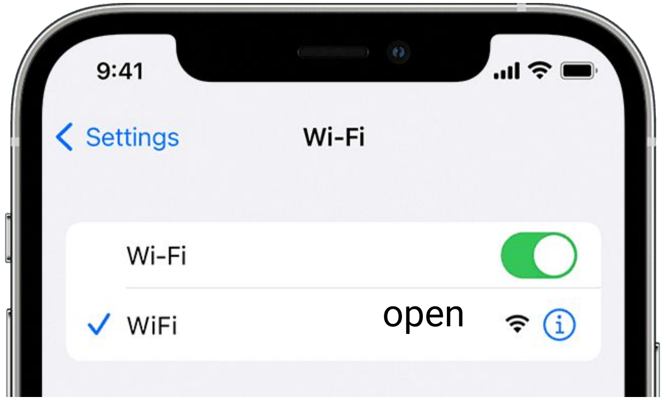
Module 3: WLAN MAC Layer

- Basic AP Management and Control Functions
  - Beaconing, BSSID, Scanning, Basic Service Set and its Capabilities
- MAC Framing, Headers and Key Functions
  - MAC headers and key functions, Management/Control/Data Frames
- Carrier Sense and Medium Access
  - Physical/Virtual Carrier Sensing, DCF, Random Backoff, Interframe Spacing, EDCA Parameters
- Data Transfer and Aggregation
  - Data Transfer Mechanism, Aggregation, Admission Control

Module 4: Security in Wi-Fi

- Various Wi-Fi Security Protocols
  - Security Basics, WEP, WPA/WPA2, Enterprise/Personal
- Basics of Authentication and Encryption
  - EAP Methods, TKIP/CCMP, 802.1X connection, Key Generations, 4-way Handshake
- Attacks and Vulnerabilities
  - DoS Attacks, Man in the Middle Attacks, Cracking Security Keys, PMF
- Seamless connectivity/Open Roaming
  - Open Roaming Technology, Wi-Fi to Cellular Handover, EAP-SIM/AKA

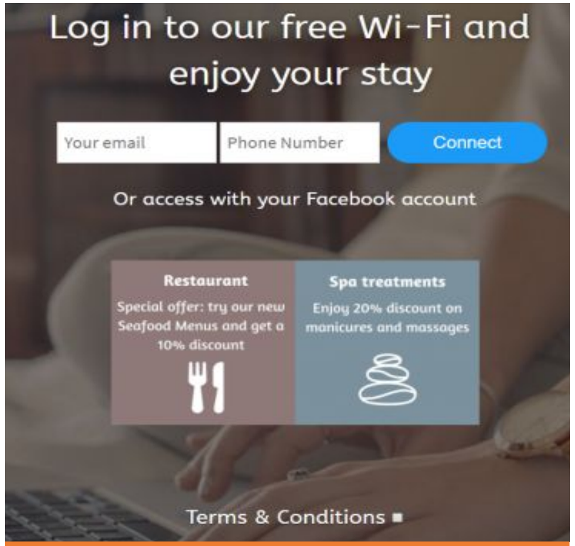
Methods we use to connect to a WiFi Network



Wi-Fi

✓ WiFi open

Connect to Open Networks



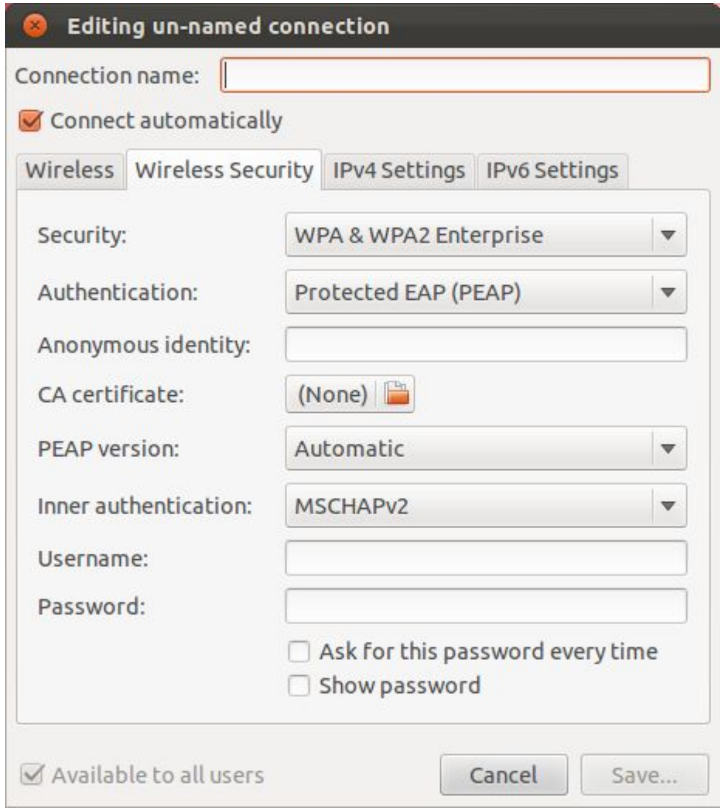
Log in to our free Wi-Fi and enjoy your stay

Your email | Phone Number | Connect

Or access with your Facebook account

Restaurant
Special offer: try our new Seafood Menus and get a 10% discount
Spa treatments
Enjoy 20% discount on manicures and massages
Terms & Conditions

Connect to Hotel Wi-Fi



Editing un-named connection

Connection name:

☑ Connect automatically

Security: WPA & WPA2 Enterprise

Authentication: Protected EAP (PEAP)

Anonymous identity:

CA certificate: (None)

PEAP version: Automatic

Inner authentication: MSCHAPv2

Username:

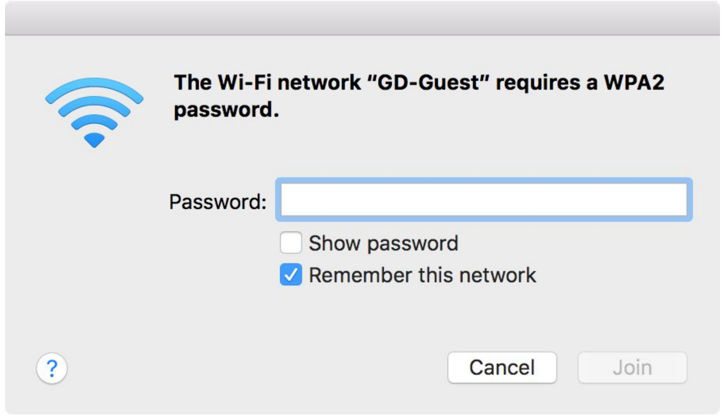
Password:

□ Ask for this password every time

□ Show password

☑ Available to all users

Connect to Office Wi-Fi



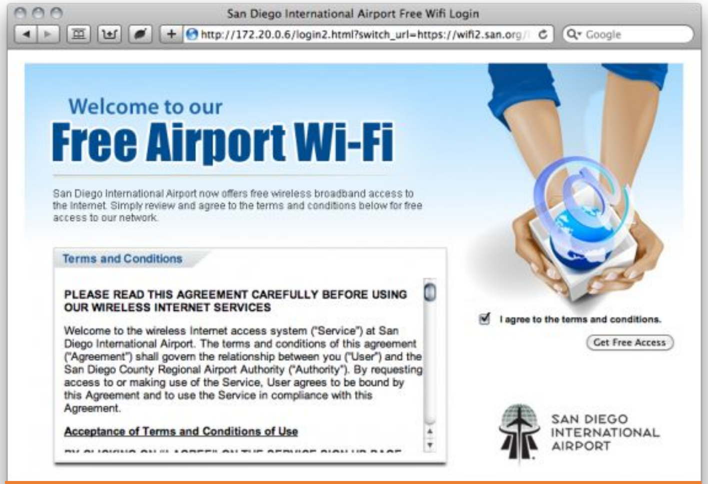
The Wi-Fi network "GD-Guest" requires a WPA2 password.

Password:

□ Show password

☑ Remember this network

Connect to WiFi at Home



San Diego International Airport Free Wifi Login

http://172.20.0.6/login2.html?switch_url=https://wifi2.san.org/

Welcome to our

Free Airport Wi-Fi

San Diego International Airport now offers free wireless broadband access to the Internet. Simply review and agree to the terms and conditions below for free access to our network.

Terms and Conditions

PLEASE READ THIS AGREEMENT CAREFULLY BEFORE USING OUR WIRELESS INTERNET SERVICES

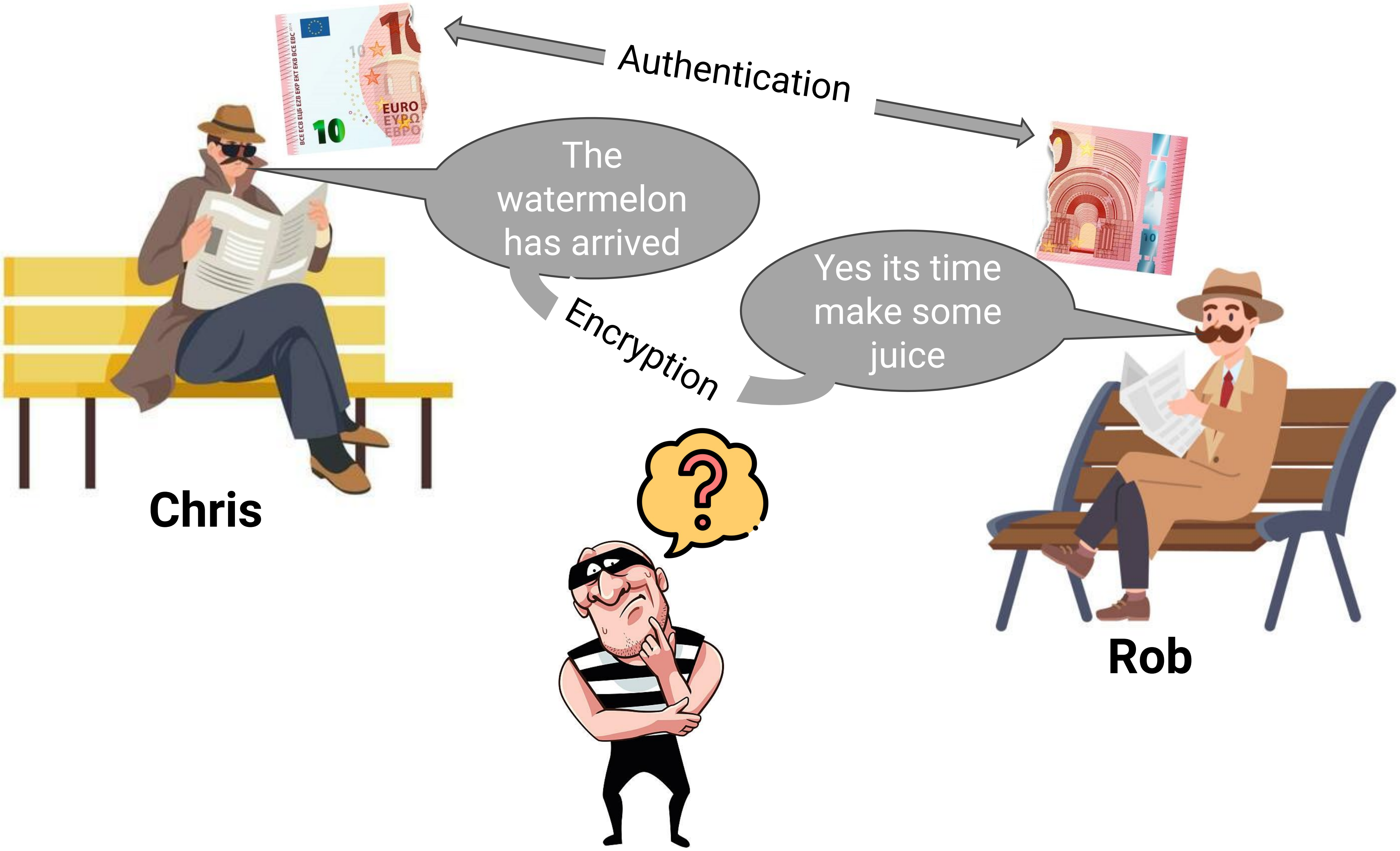
Welcome to the wireless Internet access system ("Service") at San Diego International Airport. The terms and conditions of this agreement ("Agreement") shall govern the relationship between you ("User") and the San Diego County Regional Airport Authority ("Authority"). By requesting access to or making use of the Service, User agrees to be bound by this Agreement and to use the Service in compliance with this Agreement.

Acceptance of Terms and Conditions of Use

☑ I agree to the terms and conditions.

Connect to Airport Wi-Fi

How can we secure a communication?

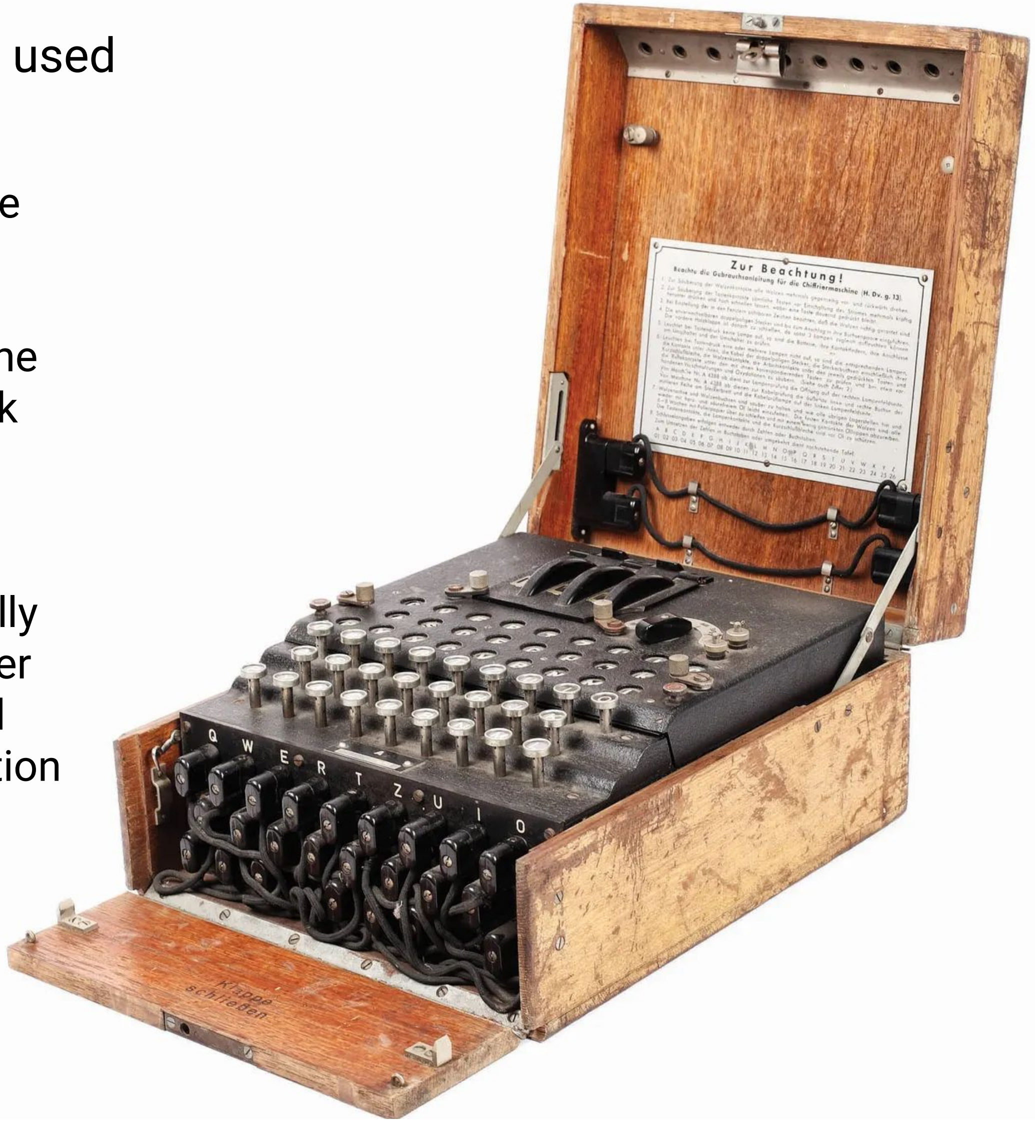


Enigma Machine Example

The idea of encryption dates back years ago. In World War II, Nazis used Enigma Machines to communicate secretly in the warfare

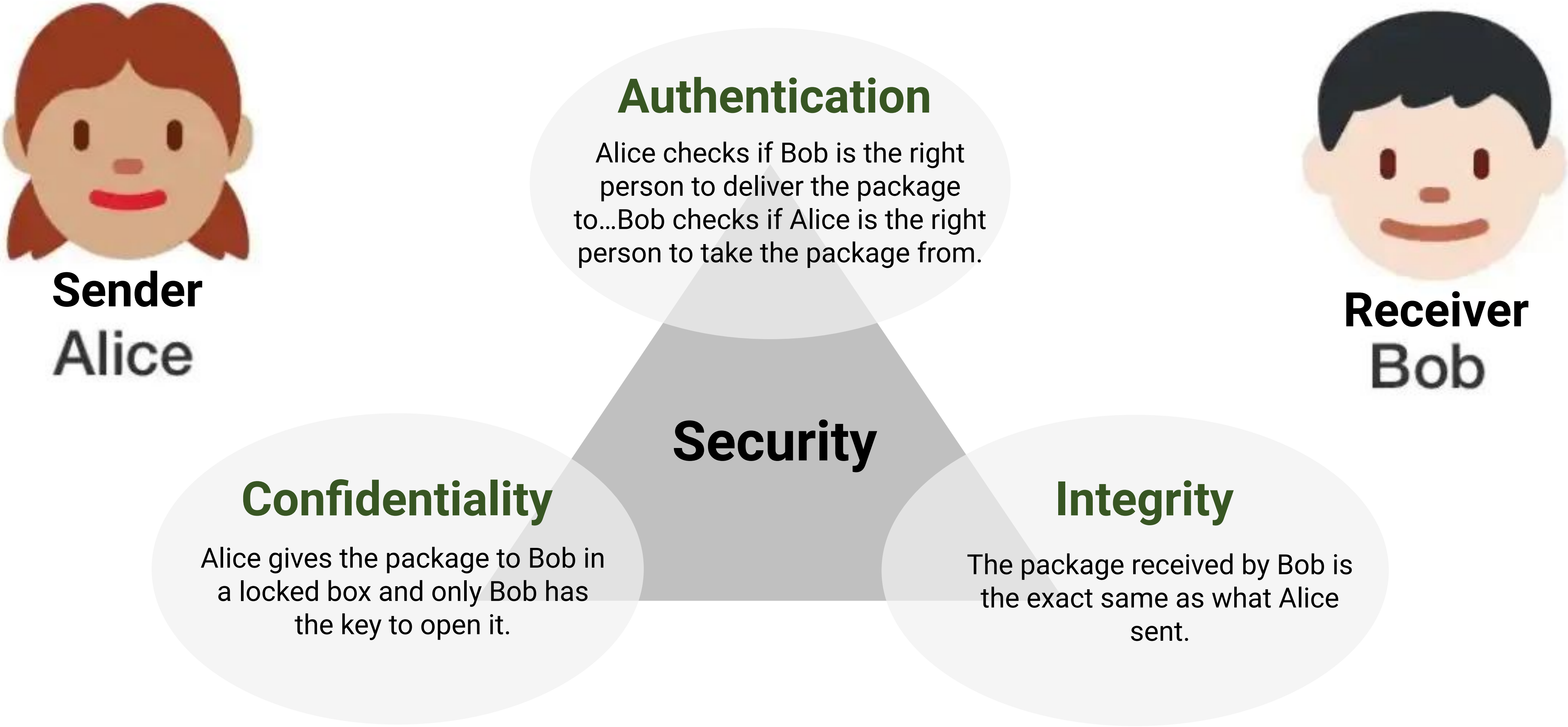
The Enigma has an electromechanical rotor mechanism that scrambles the 26 letters of the alphabet. In typical use, one person enters text on the Enigma's keyboard and another person writes down which of the 26 lights above the keyboard illuminated at each key press. If plain text is entered, the illuminated letters are the ciphertext. Entering ciphertext transforms it back into readable plaintext. The rotor mechanism changes the electrical connections between the keys and the lights with each keypress.

The security of the system depends on machine settings that were generally changed daily, based on secret key lists distributed in advance, and on other settings that were changed for each message. The receiving station would have to know and use the exact settings employed by the transmitting station to successfully decrypt a message.



Source : https://en.wikipedia.org/wiki/Enigma_machine

The Three pillars of WiFi Security



Sender
Alice

Receiver
Bob

Security

Authentication

Alice checks if Bob is the right person to deliver the package to…Bob checks if Alice is the right person to take the package from.

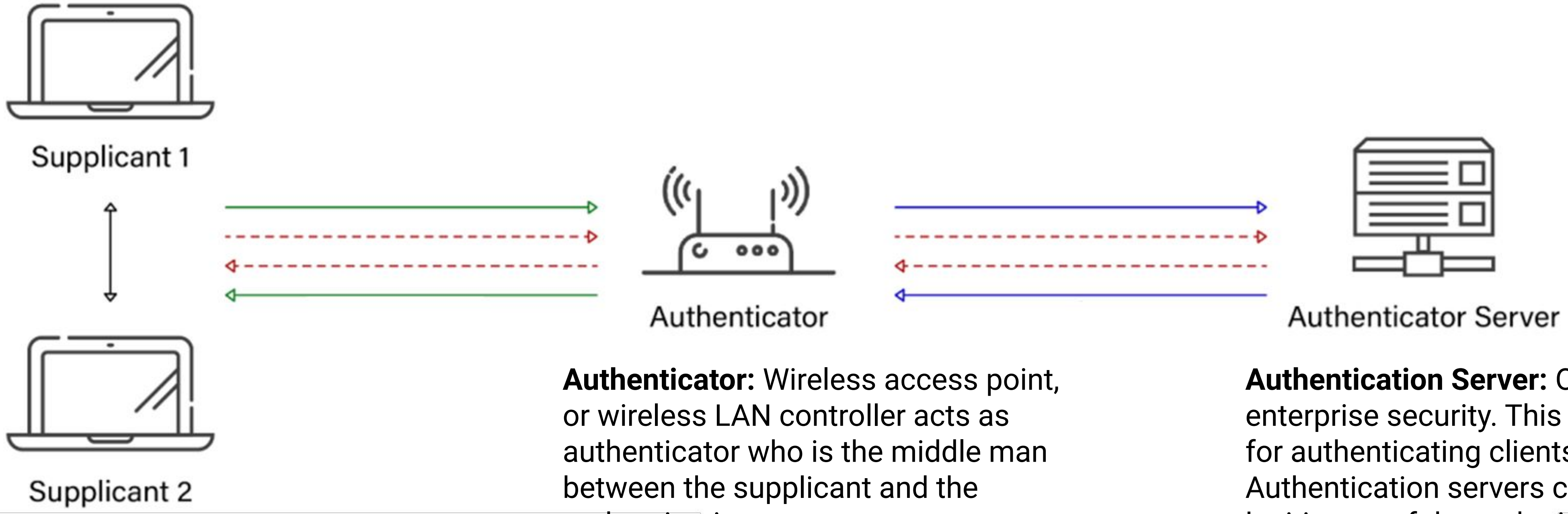
Confidentiality

Alice gives the package to Bob in a locked box and only Bob has the key to open it.

Integrity

The package received by Bob is the exact same as what Alice sent.

The Three Enforcers of WiFi Security

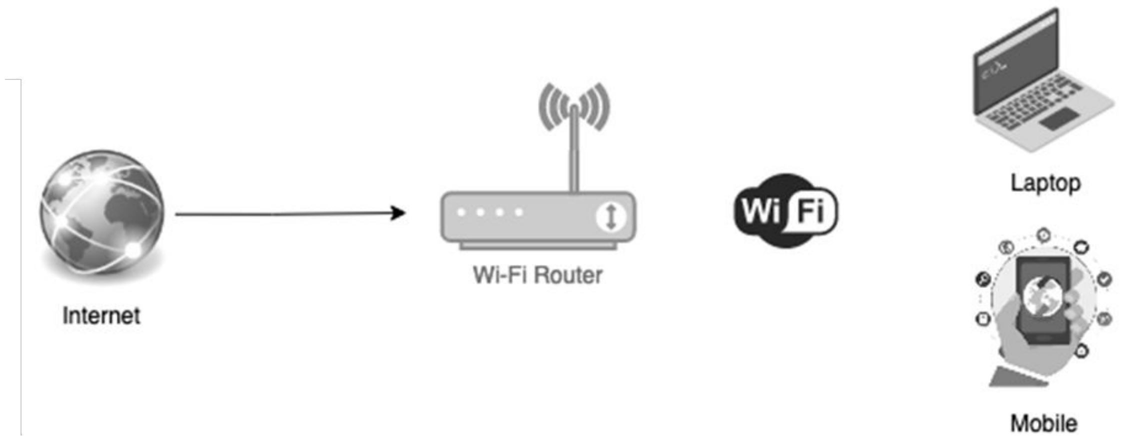


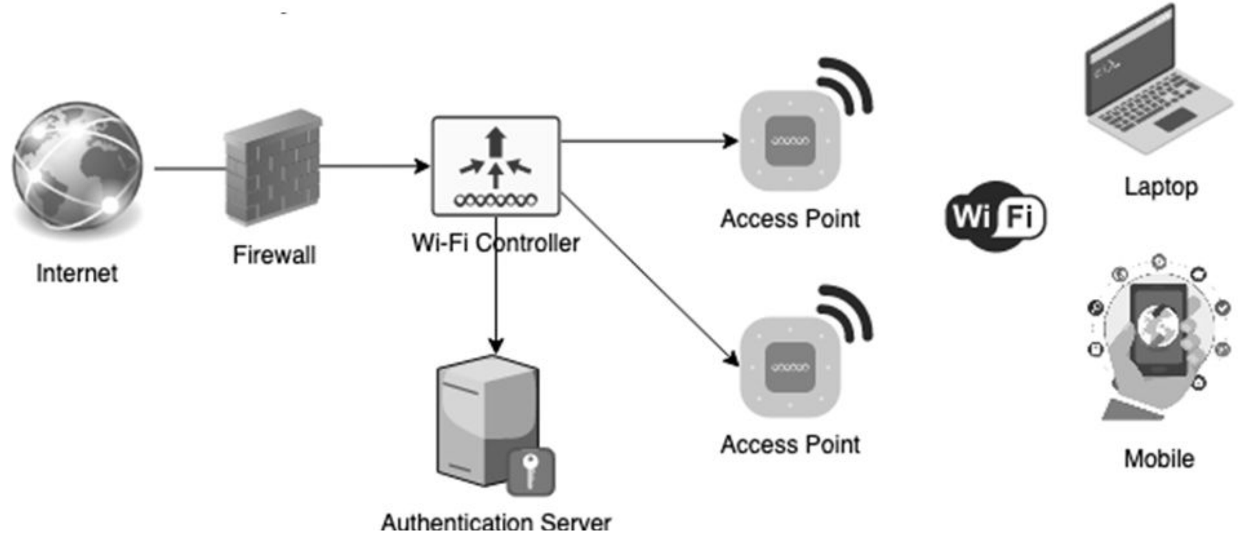
Supplicant: This is the application running on the endpoint or the client's device. It exchanges messages with the authenticator for authentication and encryption

Authenticator: Wireless access point, or wireless LAN controller acts as authenticator who is the middle man between the supplicant and the authentication server.

Authentication Server: Only used for enterprise security. This is responsible for authenticating clients. Authentication servers check the legitimacy of the endpoint and report back to the authenticator with approval or denial.

Personal Vs Enterprise Security





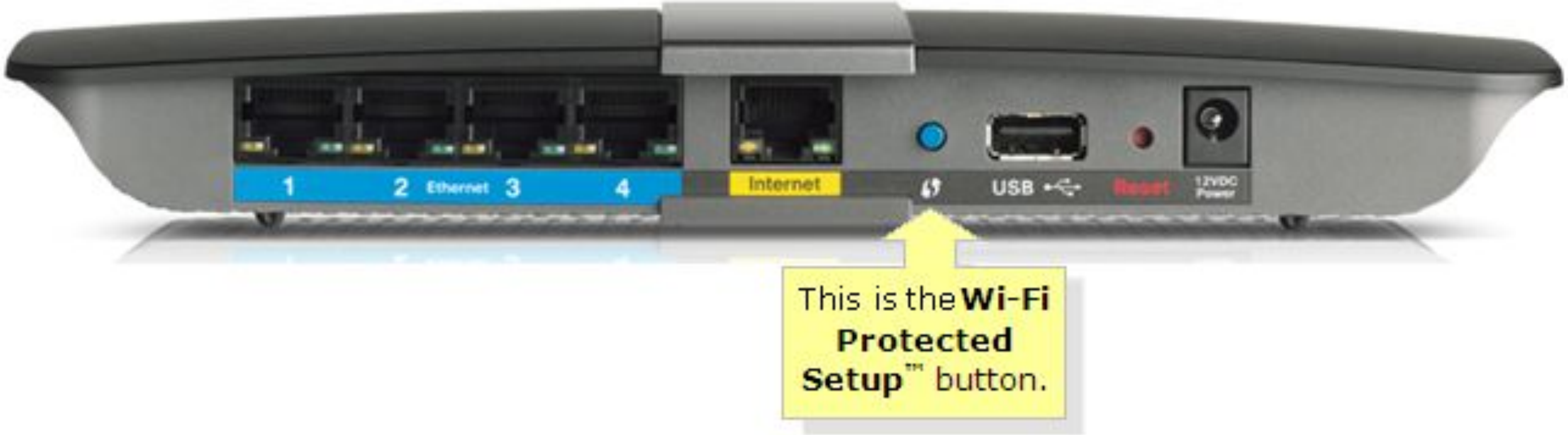
Personal Security

- Uses Pre Shared Keys (PSK)
- All security handshakes relating to Authentication are only between the Router and the Station.
- The security keys are manually entered in both the router and the station.

Enterprise Security

- Uses 802.1X/EAP
- The authentication aspect is handles by the authentication server on the enterprise network with the APs acting as relays.
- Usually the authentication is tied up with other IT systems like Active Directory services, authorization and accounting operations.
- Authentication is user based and there is no need to manually enter any security keys in the AP or the station.
- Is easily extensible to large scale deployments.

Wi-Fi Protected Setup (WPS)

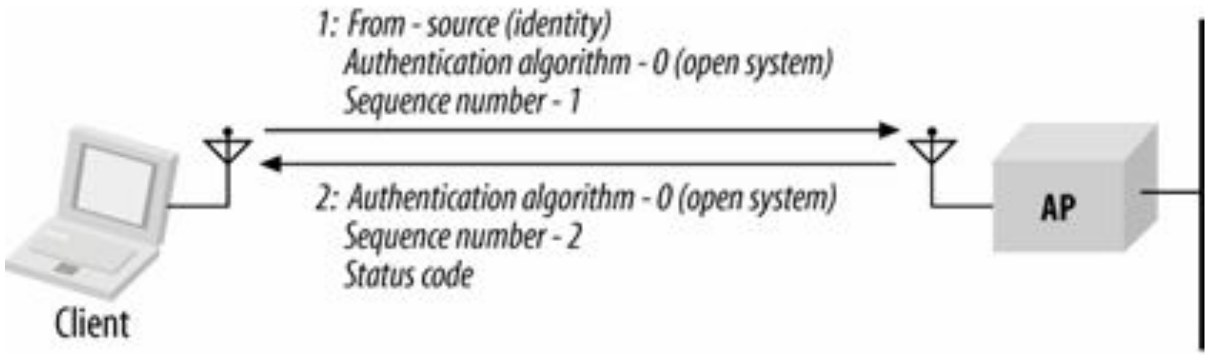


This is the **Wi-Fi Protected Setup**™ button.

Base 802.11 Security: Open and Shared Key Authentication

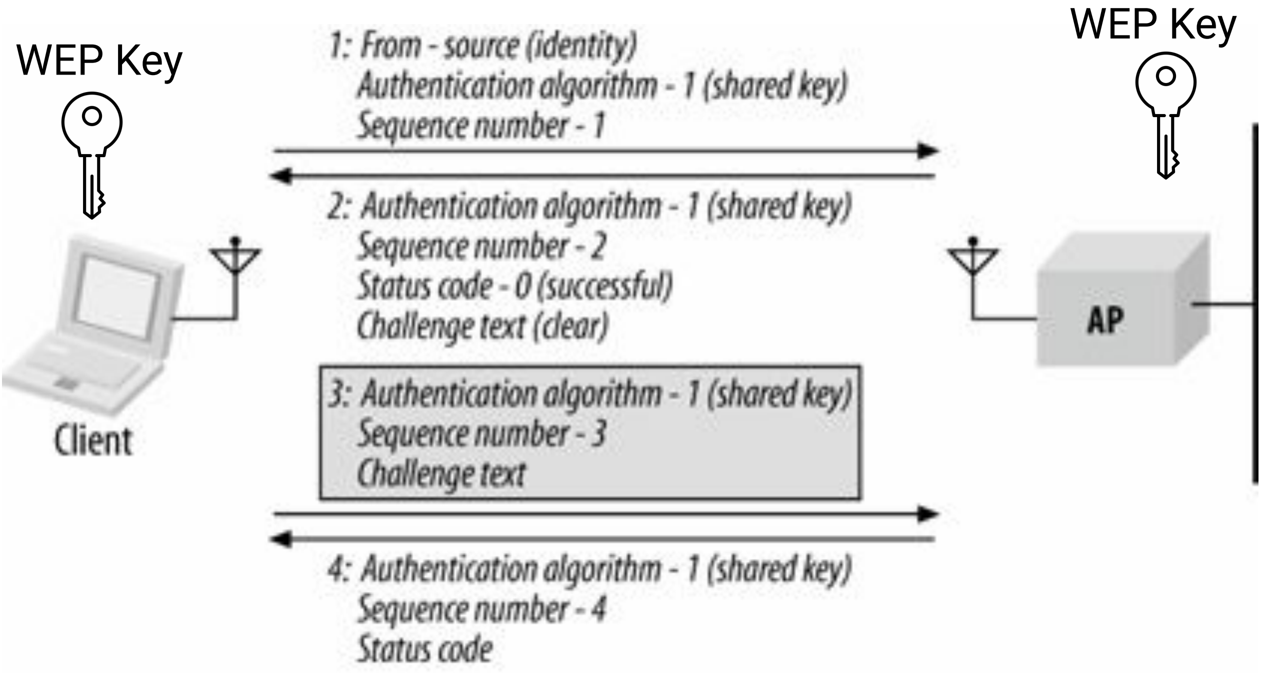
Open System authentication

The client sends an authentication request to the AP indicating that the Authentication Method will OPEN (no encryption of data)
The AP will Acknowledge and after successful association the data is transferred in plain text.


1: From - source (identity)
Authentication algorithm - 0 (open system)
Sequence number - 1
2: Authentication algorithm - 0 (open system)
Sequence number - 2
Status code
Client
AP

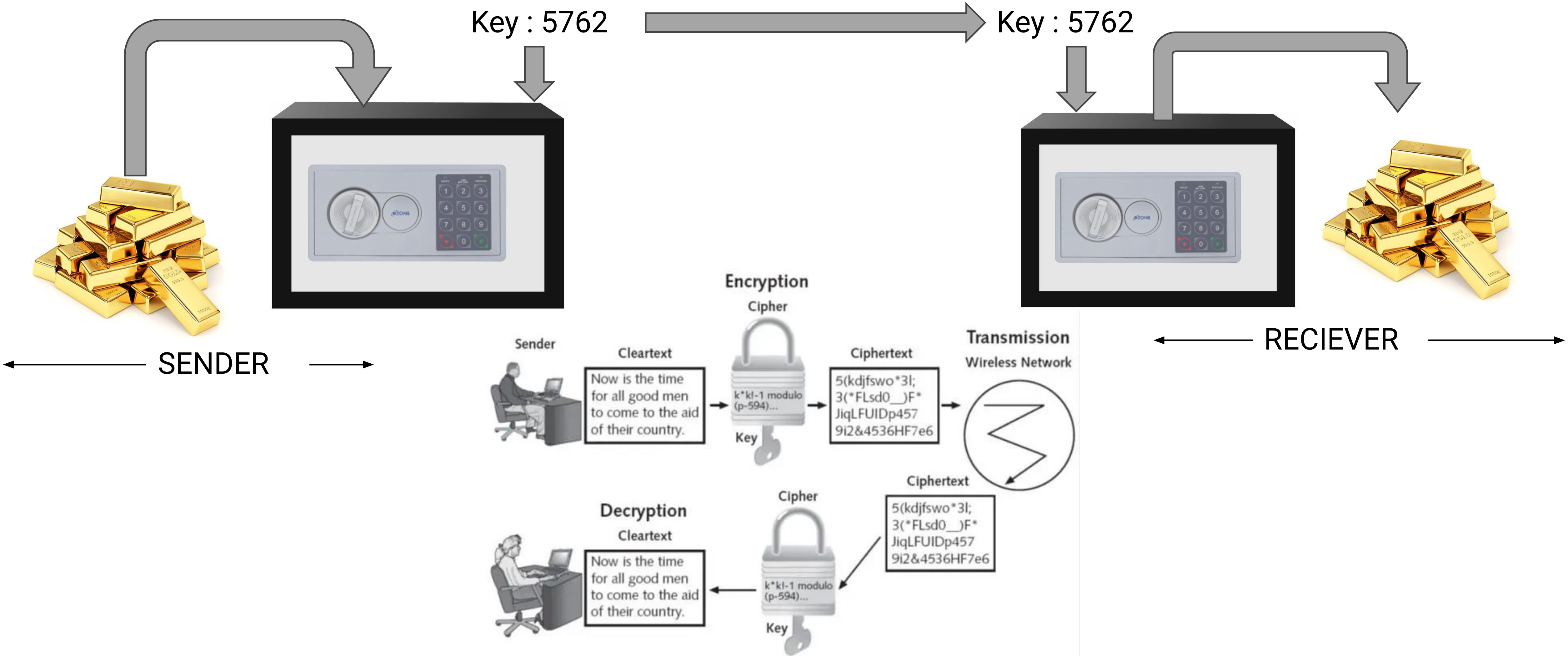
Shared key authentication – Uses WEP

- Client sends Authentication request with Auth Algorithm set to 1 to indicate share key authentication
- AP responds with a text
- Station encrypts the text using the WEP key and sends it back
- AP decrypts and returns an authentication management frame


WEP Key
WEP Key
1: From - source (identity)
Authentication algorithm - 1 (shared key)
Sequence number - 1
2: Authentication algorithm - 1 (shared key)
Sequence number - 2
Status code - 0 (successful)
Challenge text (clear)
3: Authentication algorithm - 1 (shared key)
Sequence number - 3
Challenge text
4: Authentication algorithm - 1 (shared key)
Sequence number - 4
Status code
Client
AP

What is a KEY?

- A key is a sequence of bits/numbers that allows the user to encrypt and decrypt information.
- A key normally used for providing authentication and confidentiality.



Key : 5762

Key : 5762

SENDER

RECIEVER

Encryption

Sender

Cleartext

Now is the time for all good men to come to the aid of their country.

Cipher

k*k!-1 modulo (p-594)...

Key

Ciphertext

5(kdjfswo*3l; 3(*FLsd0__)F* JiqLFUIDp457 9i2&4536HF7e6

Transmission

Wireless Network

Ciphertext

5(kdjfswo*3l; 3(*FLsd0__)F* JiqLFUIDp457 9i2&4536HF7e6

Cipher

k*k!-1 modulo (p-594)...

Key

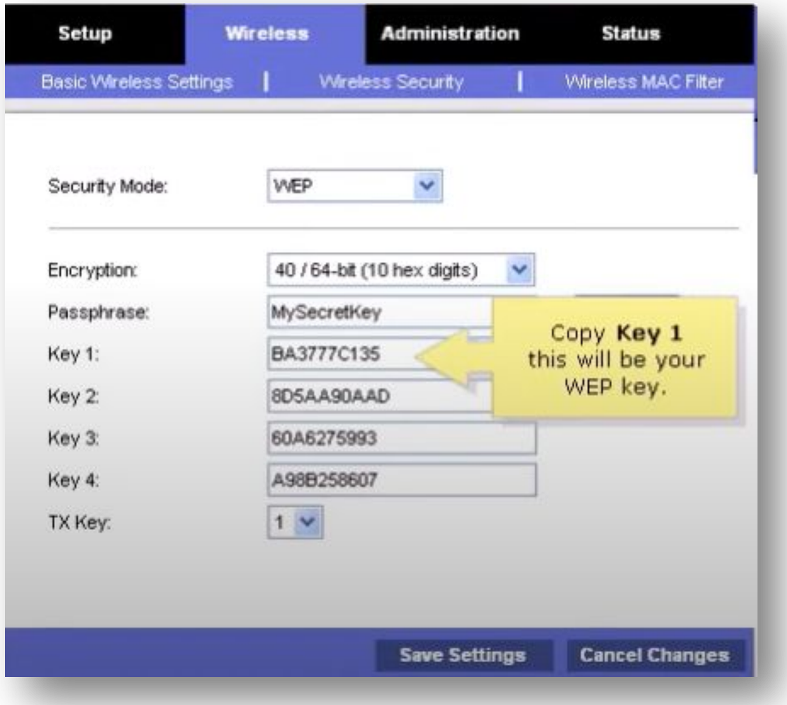
Decryption

Cleartext

Now is the time for all good men to come to the aid of their country.

Wired Equivalent Privacy (WEP)

- Introduced in the base standard to provide data confidentiality (encryption)
- Uses Encryption Keys to encrypt the data.
- A key is a sequence of bit
- Key length can be 40 or 104 bit long represented by 10 or 26 hex digits:
  - 64 bit (24 bit IV + 40 bit Key)
  - 128 bit (24 bit IV + 104 bit Key)
- IV (Initialization vector) is a random stream of 24 bits that is changed for each packet transmission and its primary purpose is to ensure that two packets don't have the same key stream.


Setup
Wireless
Administration
Status
Basic Wireless Settings | Wireless Security | Wireless MAC Filter
Save Settings
Cancel Changes

Security Mode: WEP

Encryption: 40 / 64-bit (10 hex digits)

Passphrase: MySecretKey

Key 1: BA3777C135

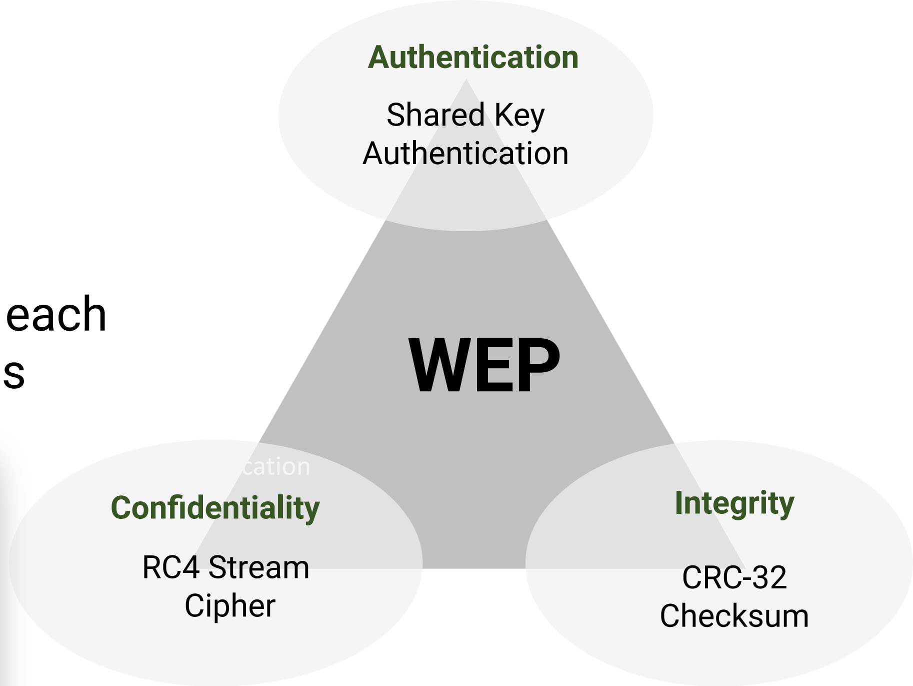
Key 2: 8D5AA90AAD

Key 3: 60A6275993

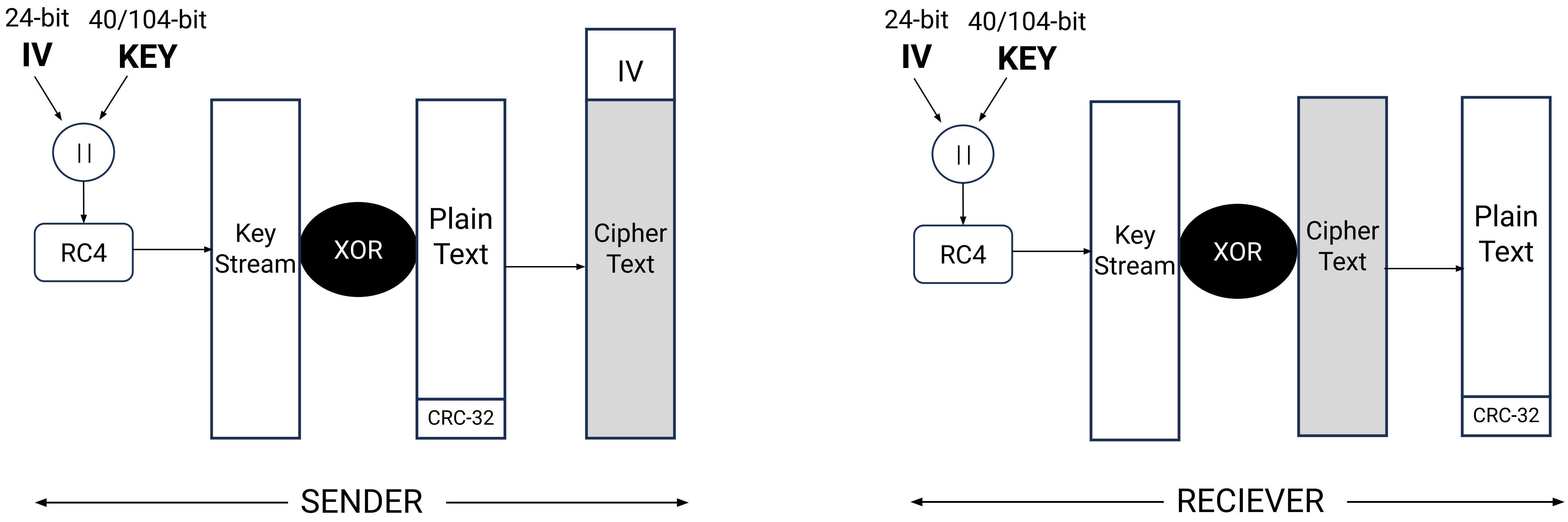
Key 4: A98B258607

TX Key: 1

Copy **Key 1** this will be your WEP key.



WEP Encryption and Decryption Procedure



WEP Flaws

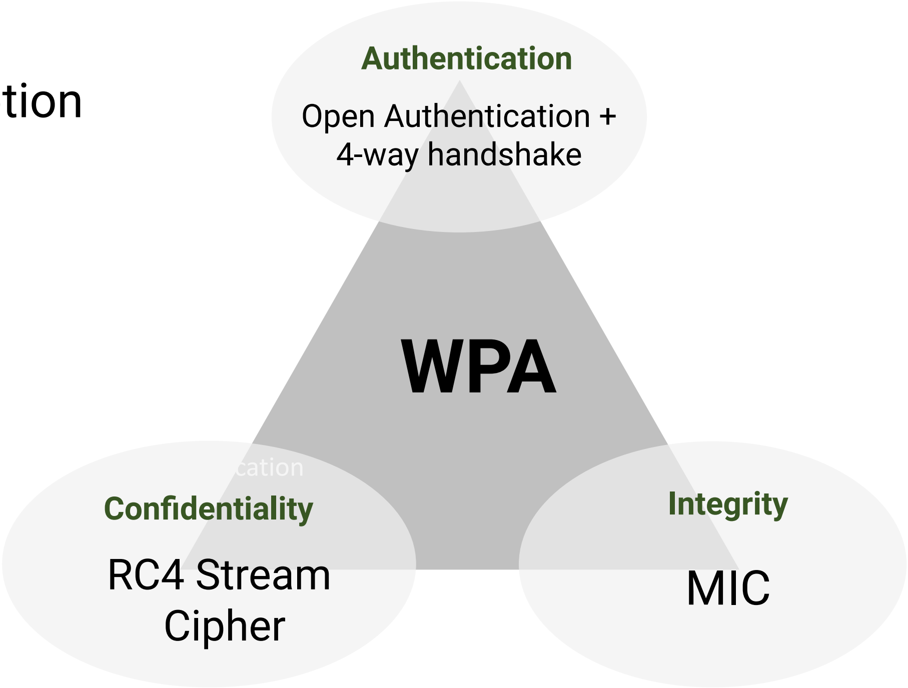
- Weak encryption: WEP uses a stream cipher called RC4, which is relatively weak and easy to crack.
- Key reuse: WEP reuses the same encryption key for all packets, which makes it easier for attackers to crack the key.
- Initialization vector (IV) gets reused for multiple packets over time, which can also be exploited by attackers.

Wi-Fi Protected Access (WPA) - Personal

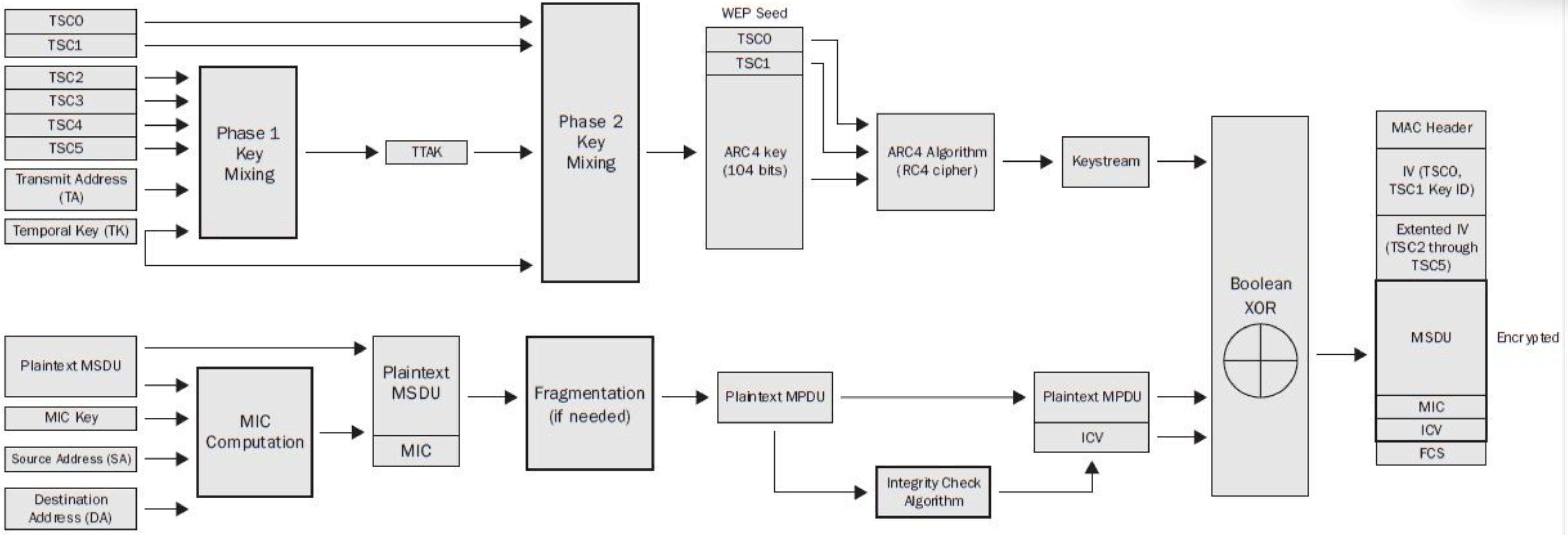
- Intended to provide better security over WEP
- Released as an intermediate solution and as a patchwork to overcome WEP weak securities
- Based on PSK and 802.1x/EAP based auth
- Uses TKIP (Temporal Key Integrity Protocol) based on RC4
- Uses 48-bit IV, 64-bit key for authentication and 128-bit key for encryption
- Firmware upgrade is enough to use WPA instead of WEP
- User can enter a 8-64 bit ASCII value as the key.

Improvements over WEP

- Unique per packet encryption keys are generated.
- 48-bit Initialization Vector (IV) instead of 24 bit IV which removes the chance of repetition of IV.
- Used Transmitter MAC as a part of the key to make the key unique for each Tx/Rx pair.
- MIC (Message Integrity Check): MIC verifies the integrity of data packets to prevent attackers from modifying them and is more robust than CRC-32



WPA Encryption Procedure

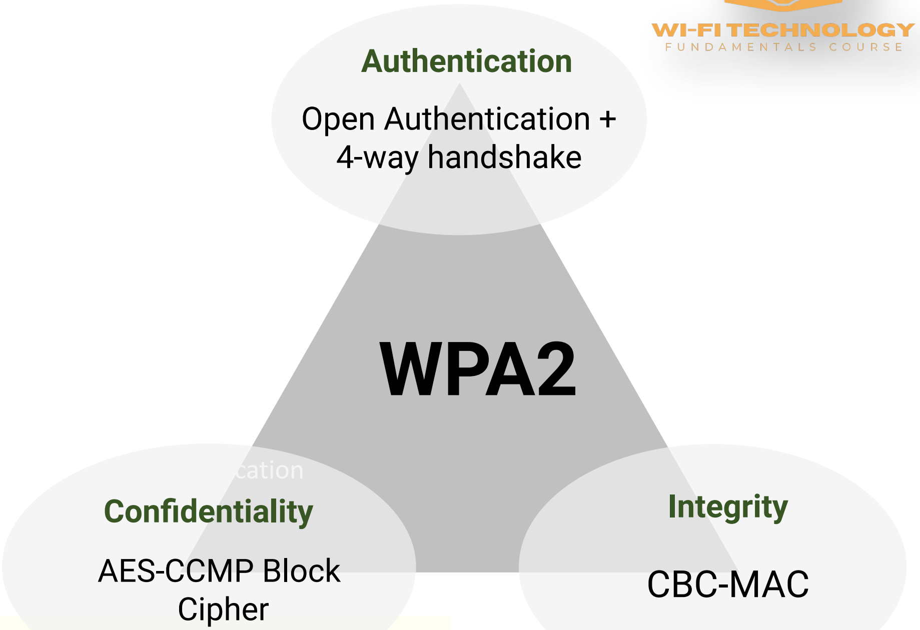


- TKIP use 2 phase key mixing process.
- 48-bit TKIP Sequence Counter (TSC) is generated & broken into 6 octets (TSC0-TSC5)
- Phase 1 key mixing us 128-bit temporal key (TK) with TSC2-TSC5 as well as Transmit Address (TA)
- Output of phase 1 is known as TKIP-mixed transmit address & key (TTAK)
- Phase 2 key mixing combines, TTAK with TSC0-TSC1 with 128 bit TK.
- Output of the phase 2 is known as “WEP seed”
- WEP seed is then run through ARC4 algorithm & key stream is created.
- WEP seed is represented as WEP Initialization Vector(IV) & 104 bit WEP keys.
- Extend IV created by TSC2-5 of key mixing phase2
- IV & Extended IV (8 byte in total) called TKIP header.

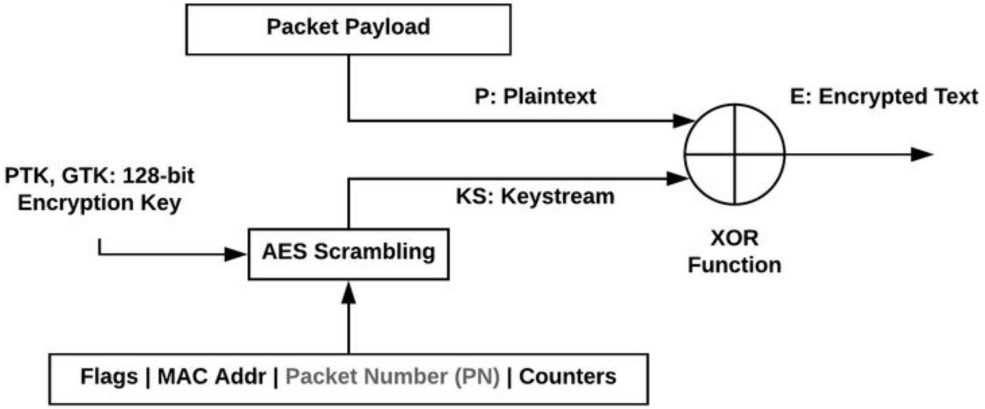
- TKIP uses Message Integrity Code(MIC) also named as “Michael”
- MIC is computed using Destination Address (DA), Source Address (SA), MSDU priority and plaintext Data.
- TKIP MIC does not replace WEP ICV (32bit), but augments it.
- WEP ICV helps prevent false detection of MIC failures that would cause TKIP countermeasure to be invoked.
- MPDU+MIC+ICV used to perform XOR with Keystream to generated encrypted payload.
- Frame Check Sequence(FCS) is calculated over all of the header & entire frame body resulting 32bit CRC placed in FCS field.
- Before MIC verification, receiving STA check FCS, ICV & TSC of all MPDU

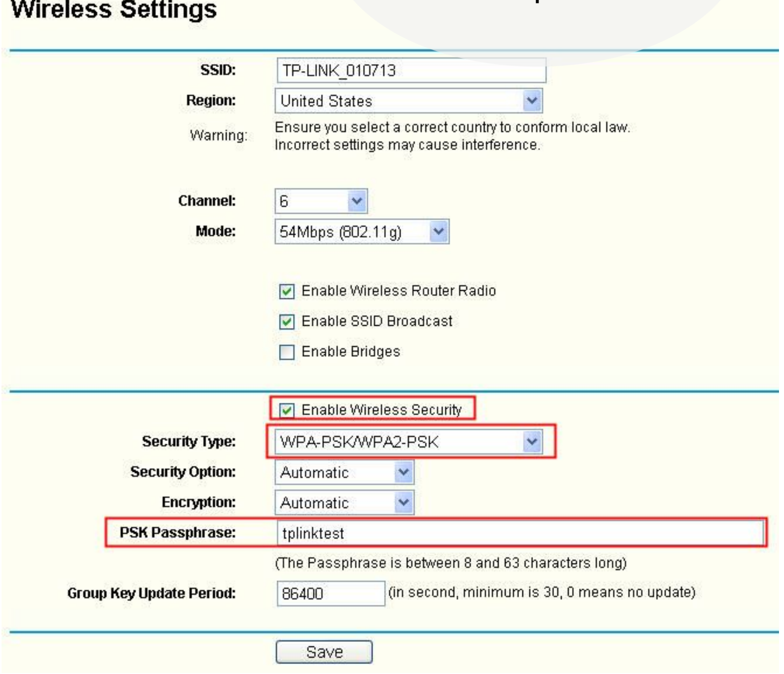
Wi-Fi Protected Access2 (WPA2) - Personal

- Uses Advanced Encryption Standard (AES) for encryption
- Unlike WPA, this needs hardware support
- Uses 128-bit key for data encryption
- CBC-MAC (Cipher Block Chaining Message Authentication Code) mode is used to calculate the MIC
- Packet Number is used to prevent replay attacks
- CCM use new temporal key for each session
- APs can support WPA+WPA2 modes for backward compatibility



WPA2 Encryption Procedure





Wireless Settings

SSID: TP-LINK_010713

Region: United States

Warning: Ensure you select a correct country to conform local law.
Incorrect settings may cause interference.

Channel: 6

Mode: 54Mbps (802.11g)

☑ Enable Wireless Router Radio

☑ Enable SSID Broadcast

☐ Enable Bridges

☑ Enable Wireless Security

Security Type: WPA-PSK/WPA2-PSK

Security Option: Automatic

Encryption: Automatic

PSK Passphrase: tplinktest

(The Passphrase is between 8 and 63 characters long)

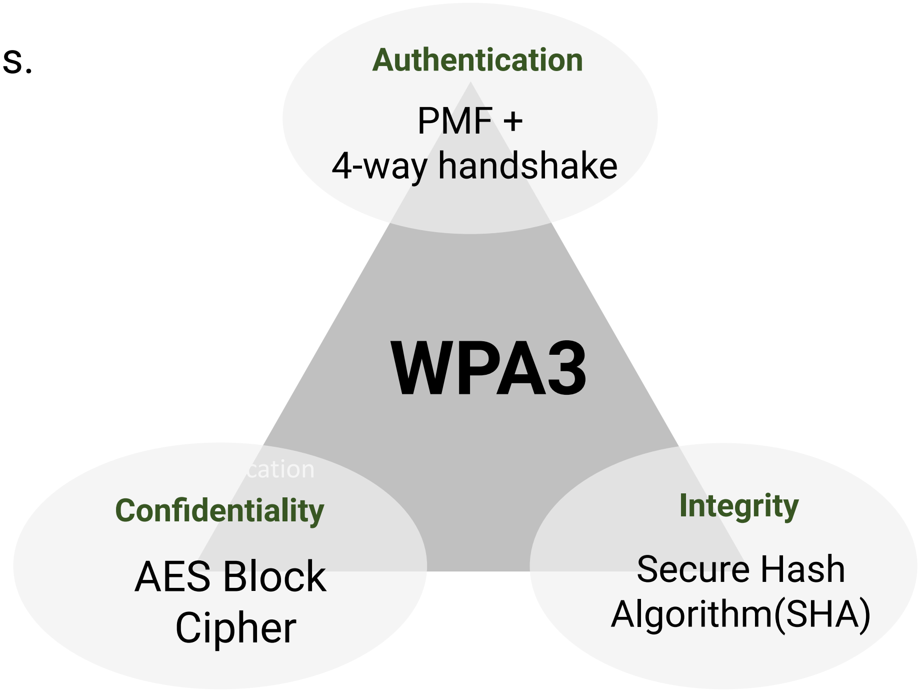
Group Key Update Period: 86400 (in second, minimum is 30, 0 means no update)

Wi-Fi Protocol Access3 (WPA3) - Personal:

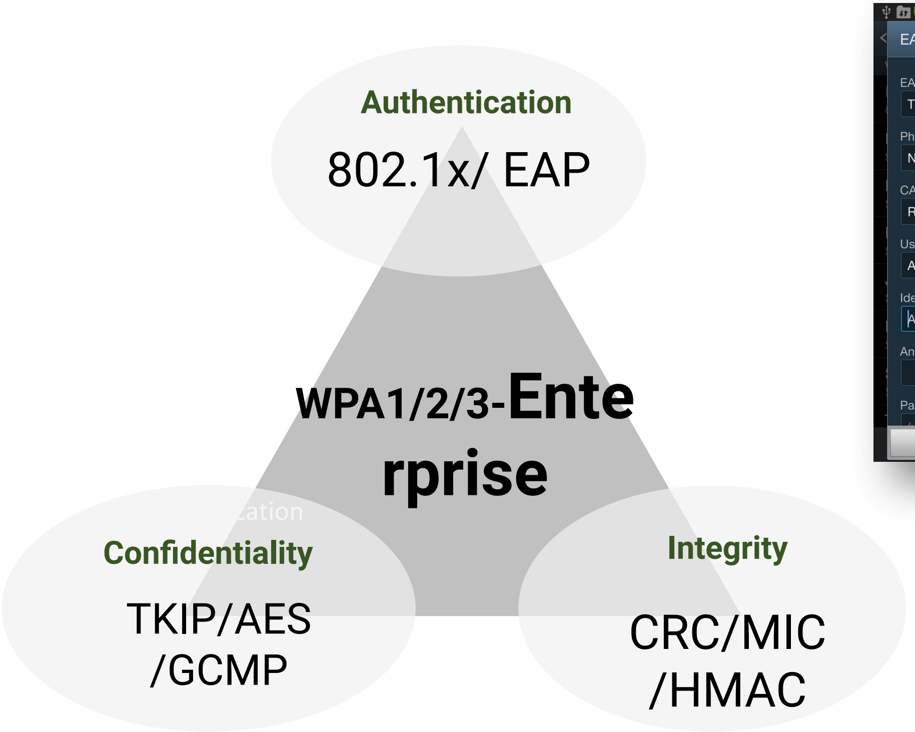
- Uses GCMP (Galois/Counter Mode Protocol)
- Uses 128/192/256-bit keys for data encryption
- 384-bit Hashed-based Message Authentication Code (HMAC)
- 256-bit Broadcast/Multicast Integrity Protocol (BIP-GMAC-256)
- A unique session key is generated for every individual session a user initiates.
- Enhanced open security with OWE

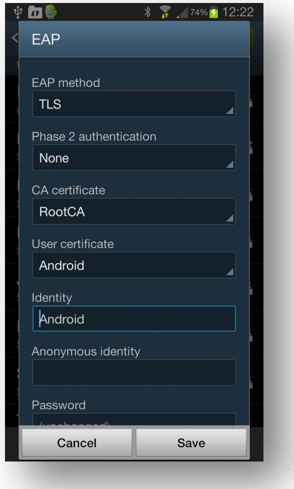
Key features of WPA3 include the following:

- Mandates PMF (Protected Management Frames) for protecting Management frames from other users
- Replaces PSK (Pre-Shared Key) with SAE (Simultaneous Authentication of Equals) which is more secure to offline dictionary attacks
- Transition mode is a mixed mode that enables the use of WPA2 to connect clients that don't support WPA3.



From Personal to Enterprise Security





EAP

EAP method: TLS

Phase 2 authentication: None

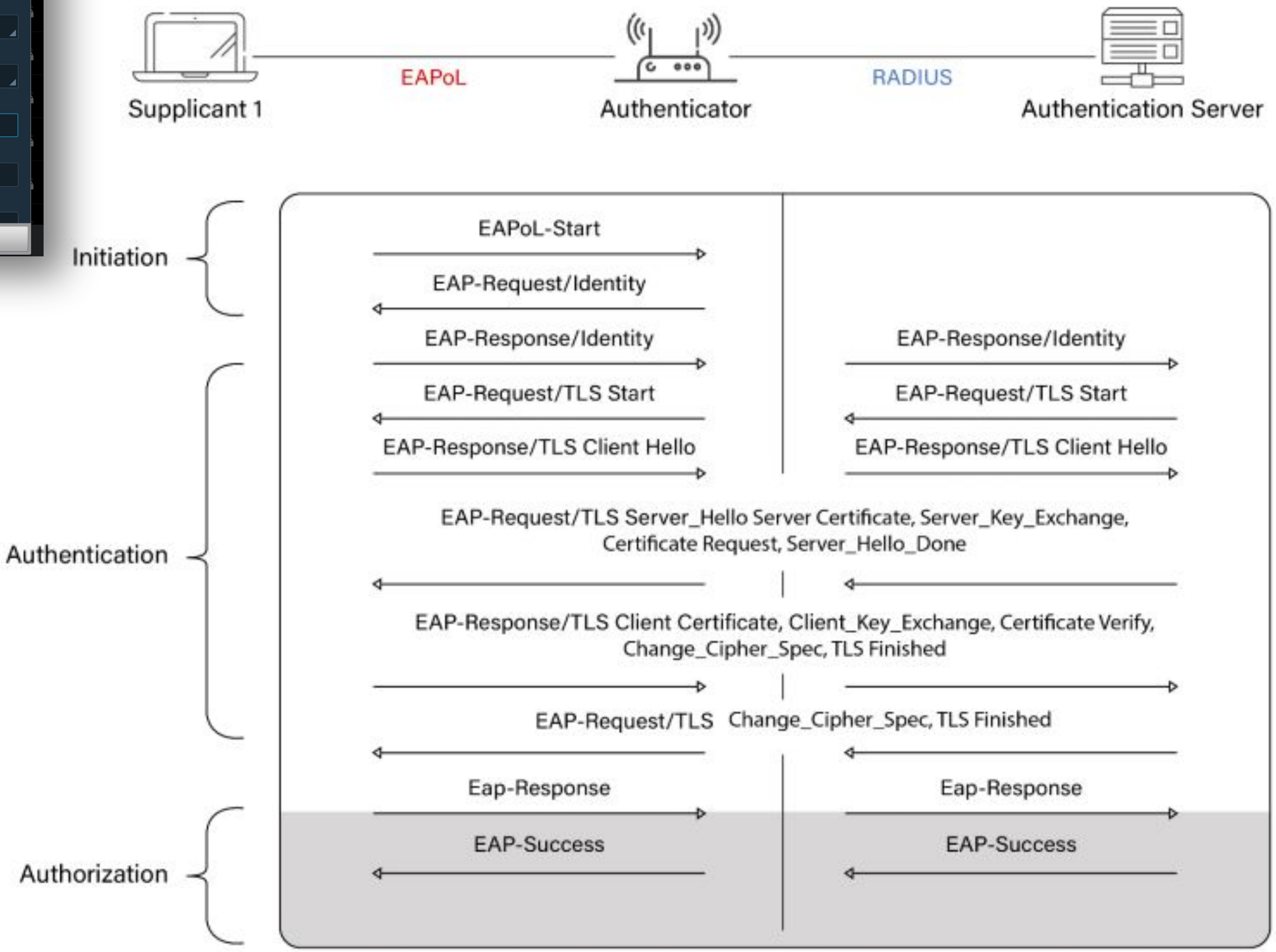
CA certificate: RootCA

User certificate: Android

Identity: Android

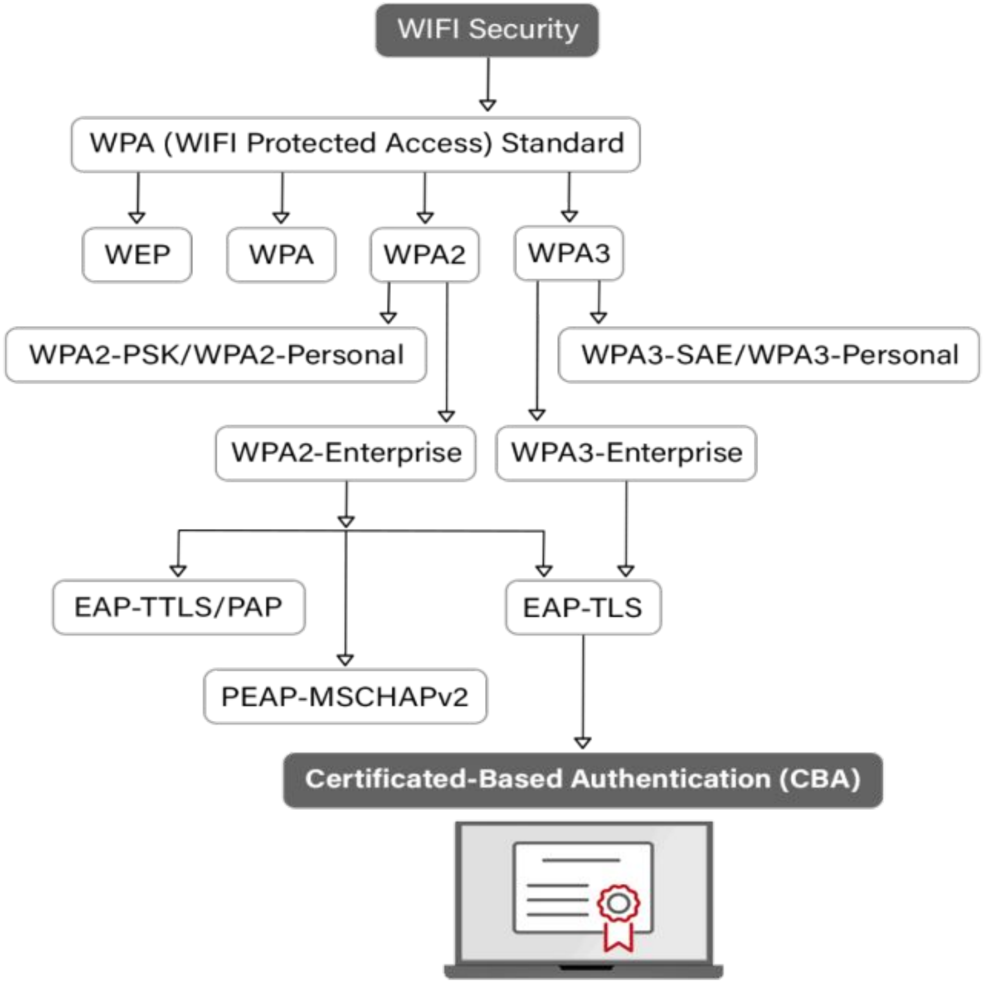
Anonymous identity:

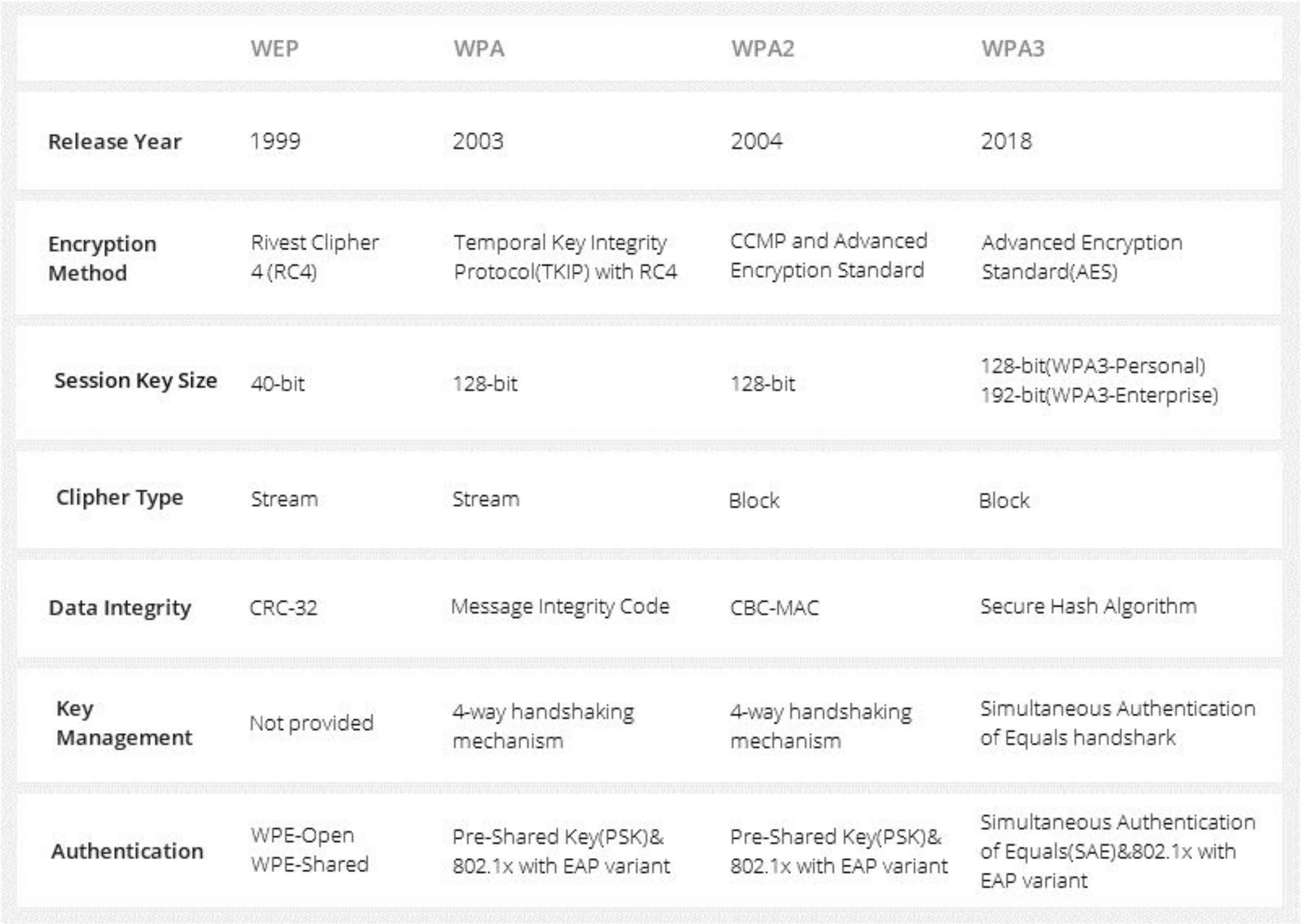
Password: (unchanged)


Supplicant 1
EAPoL
Authenticator
RADIUS
Authentication Server
Initiation
Authentication
Authorization
EAPoL-Start
EAP-Request/Identity
EAP-Response/Identity
EAP-Response/Identity
EAP-Request/TLS Start
EAP-Request/TLS Start
EAP-Response/TLS Client Hello
EAP-Response/TLS Client Hello
EAP-Request/TLS Server_Hello Server Certificate, Server_Key_Exchange, Certificate Request, Server_Hello_Done
EAP-Response/TLS Client Certificate, Client_Key_Exchange, Certificate Verify, Change_Cipher_Spec, TLS Finished
EAP-Request/TLS Change_Cipher_Spec, TLS Finished
Eap-Response
Eap-Response
EAP-Success
EAP-Success

- The authentication aspect is handles by the authentication server on the enterprise network with the APs acting as relays.
- Usually the authentication is tied up with other IT systems like Active Directory services, authorization and accounting operations.
- Authentication is user based and there is no need to manually enter any security keys in the AP or the station.
- Is easily extensible to large scale deployments.

Summary of various authentication/encryption methods





	WEP	WPA	WPA2	WPA3
Release Year	1999	2003	2004	2018
Encryption Method	Rivest Clipher 4 (RC4)	Temporal Key Integrity Protocol(TKIP) with RC4	CCMP and Advanced Encryption Standard	Advanced Encryption Standard(AES)

Session Key Size	40-bit	128-bit	128-bit	128-bit(WPA3-Personal)
				192-bit(WPA3-Enterprise)

Clipher Type	Stream	Stream	Block	Block
Data Integrity	CRC-32	Message Integrity Code	CBC-MAC	Secure Hash Algorithm
Key Management	Not provided	4-way handshaking mechanism	4-way handshaking mechanism	Simultaneous Authentication of Equals handshark
Authentication	WPE-Open WPE-Shared	Pre-Shared Key(PSK)& 802.1x with EAP variant	Pre-Shared Key(PSK)& 802.1x with EAP variant	Simultaneous Authentication of Equals(SAE)&802.1x with EAP variant

Simple TIPs on How to Secure your Home Wi-Fi Network

- Update your routers to use the latest encryption mechanisms
- Change your router default settings, username and passwords
- Use a strong security Key and change the key frequently
- Turn OFF WPS and any UPnP features
- Turn ON firewall settings on your router
- Select the safest possible location in the house for the Physical location of the router.
- Setup a separate Guest Network with very restricted access.
- Turn on Access Control Lists where you can enter only certain devices MAC addresses as allowed devices.
- Log Out of router admin mode
- Update router firmware regularly

References

WEP Explained
https://www.youtube.com/watch?v=6cKgoA3Qj60

TKIP Encryption Method
https://mrncciew.com/2014/09/13/cwsp-tkip-encryption-method/

WPA3 Basics
https://www.techtarget.com/searchsecurity/definition/WPA3

Next-Gen Wi-Fi Security - WPA3 Explained
https://www.youtube.com/watch?v=aPoe4WtX2mU

Q&A

?
QUIZ!
TIME

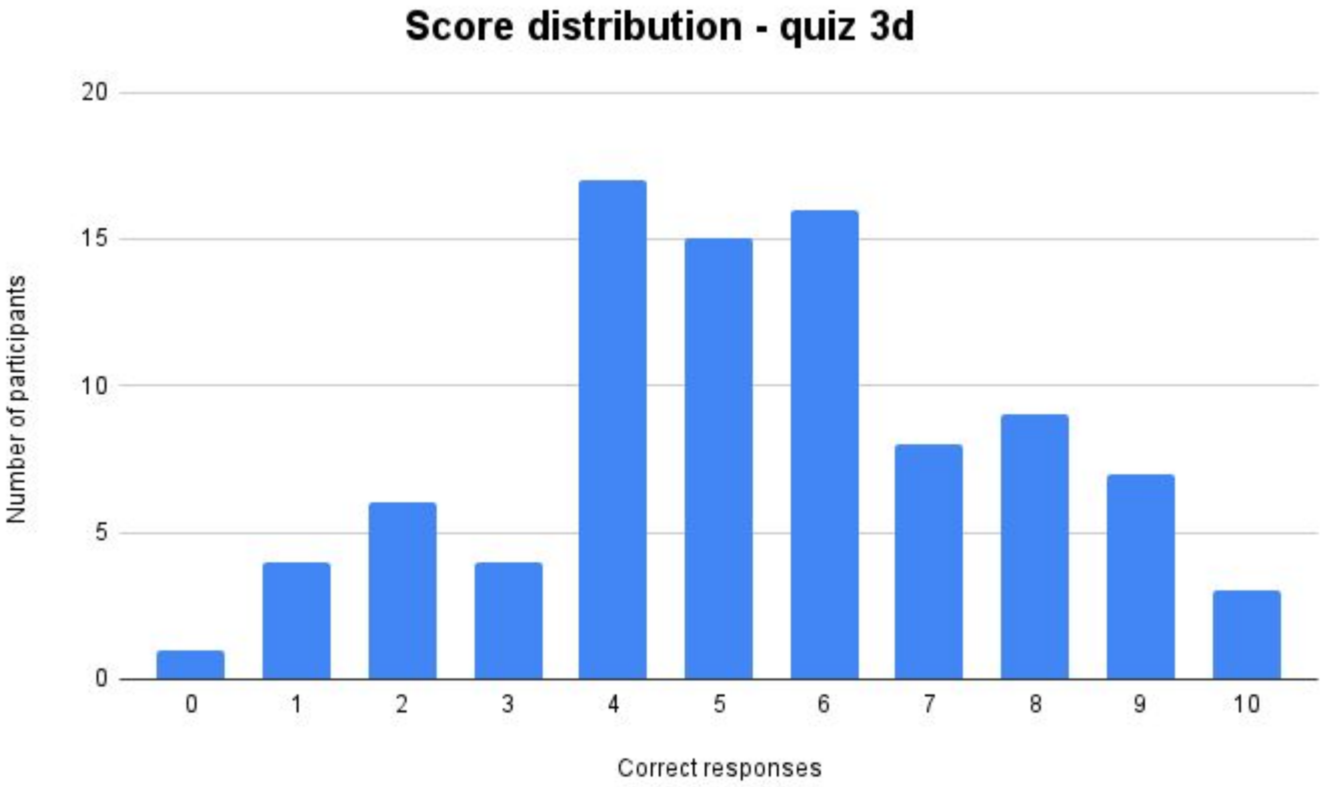
Quiz 3d Results

Winner

Dummu Sneha

INDIA

Number of participants - 90


Score distribution - quiz 3d
Number of participants
Correct responses