Wi-Fi Security: WPA (Wi-Fi Protected Access)

1. WEP
2. WPA
3. WPA2
4. WPA3

1. WEP (Wired Equivalent Privacy)

The Goal of WEP

WEP was the **first Wi-Fi security protocol**, released in 1997.
Its goal was simple:

> “Make wireless communication as secure as wired communication.”

That’s why it’s called
WEP — Wired Equivalent Privacy.

How WEP Works

Each device on the Wi-Fi network shares the **same static key** (e.g., 40 or 104 bits).

- When a message is sent:

1. A small random number called an **Initialization Vector (IV)** is added to the secret key: this changes the key slightly for each packet.
2. The combined key (**Key + IV**) is used by the **RC4** encryption algorithm: to scramble (encrypt) the message.
3. A simple **checksum (CRC)** is attached: to detect transmission errors (not real security).

The Problem with WEP

Weakness Description:

1. Static key The same key is reused for all sessions.
2. Short IV (24-bit) Quickly repeats → attackers can find patterns.
3. Weak RC4 usage RC4’s key scheduling leaks info about the key.
4. Integrity check (CRC) Not cryptographically secure — easy to modify packets.

Result:
Attackers can capture enough packets and derive the key in minutes.

2. WPA (Wi-Fi Protected Access)

The Core Idea of WPA

We need a way for **the router (Access Point)** and **the client (Laptop/Phone)** to:

1. **Authenticate** each other (make sure both are legitimate), and
2. **Encrypt all traffic** over the air — so eavesdroppers see only gibberish.

> ✅ WPA = Secure authentication + encrypted communication for Wi-Fi

2. WPA (2003 – Temporary Fix)

How WPA Works

Step 1. Authentication

- You enter the **Wi-Fi password** (Pre-Shared Key, PSK).
- The router and your device use that password to **prove** they both know the key
  without sending it over the air (using a **4-way handshake**).

Step 2. Key Generation

- Both sides derive a **session key** from the shared password and random nonces.
- Even if many devices share the same Wi-Fi password, each gets its **own session key**.

Step 3. Encryption

- Uses **RC4** cipher + **TKIP (Temporal Key Integrity Protocol)** to vary keys per packet.
- Improved integrity via **MIC (Message Integrity Check)**.

> WPA improved WEP but still relied on the weak RC4 cipher — a temporary solution.

3. WPA2 (2004 – The Standard)

What Changed

WPA2 replaced RC4/TKIP with a **stronger AES-based system** called **CCMP** (Counter Mode with CBC-MAC Protocol).

Feature	WPA	WPA2
Encryption	RC4 + TKIP	AES + CCMP
Integrity	MIC	CBC-MAC
Hardware	Works with old hardware	Needs AES-capable hardware
Security	Medium	Strong

✅ WPA2 = AES-level encryption + modern key management.

WPA2 Handshake Recap

The **4-Way Handshake** is still used in WPA2
to generate the **Pairwise Transient Key (PTK)**.

```
Client ↔️ Access Point
 1. AP sends nonce (ANonce)
 2. Client responds with SNonce + MIC
 3. Both derive same session key (PTK)
 4. AP confirms → secure AES channel
```

Session Key Example

```
PSK       = “MyHomeWiFi123!”
ANonce    = A1B2C3D4E5F6
SNonce    = 9A8B7C6D5E4F
AP_MAC    = 11:22:33:44:55:66
CL_MAC    = AA:BB:CC:DD:EE:FF

PTK = HMAC–SHA1(
  key = PSK,
  data = ANonce || SNonce || AP_MAC || CL_MAC
)
= 5F3A1C9E92B7F58D1E28D3F91A67B1AF6C3E9B7C
```

> The PTK is a unique session key derived for each device connection: When you reconnect → a new PTK is generated.

4. WPA3 (2018 – The Modern Standard)

WPA3 replaces the old PSK method with SAE (Simultaneous Authentication of Equals), a Diffie–Hellman–based handshake that prevents offline password guessing.

How WPA3-SAE Works

1. Both sides choose random secrets
2. Exchange public values (DH-style)
3. Compute the same shared secret using their private values
4. Use that secret as the session key
5. Mutual authentication ensures both sides are legitimate

```
Client:  a → g^a mod p
AP:      b → g^b mod p
Shared Key = (g^b)^a = (g^a)^b mod p
```

> WPA3 provides forward secrecy and offline attack resistance.

The WPA Family

Version	Year	Key Algorithm	Improvement
WEP	1997	RC4 (static key)	Weak, easily cracked
WPA (TKIP)	2003	RC4 + TKIP	Temporary fix using dynamic keys
WPA2 (AES-CCMP)	2004	AES	Strong encryption, industry standard
WPA3 (SAE)	2018	Diffie–Hellman (SAE)	Resistant to offline password attacks