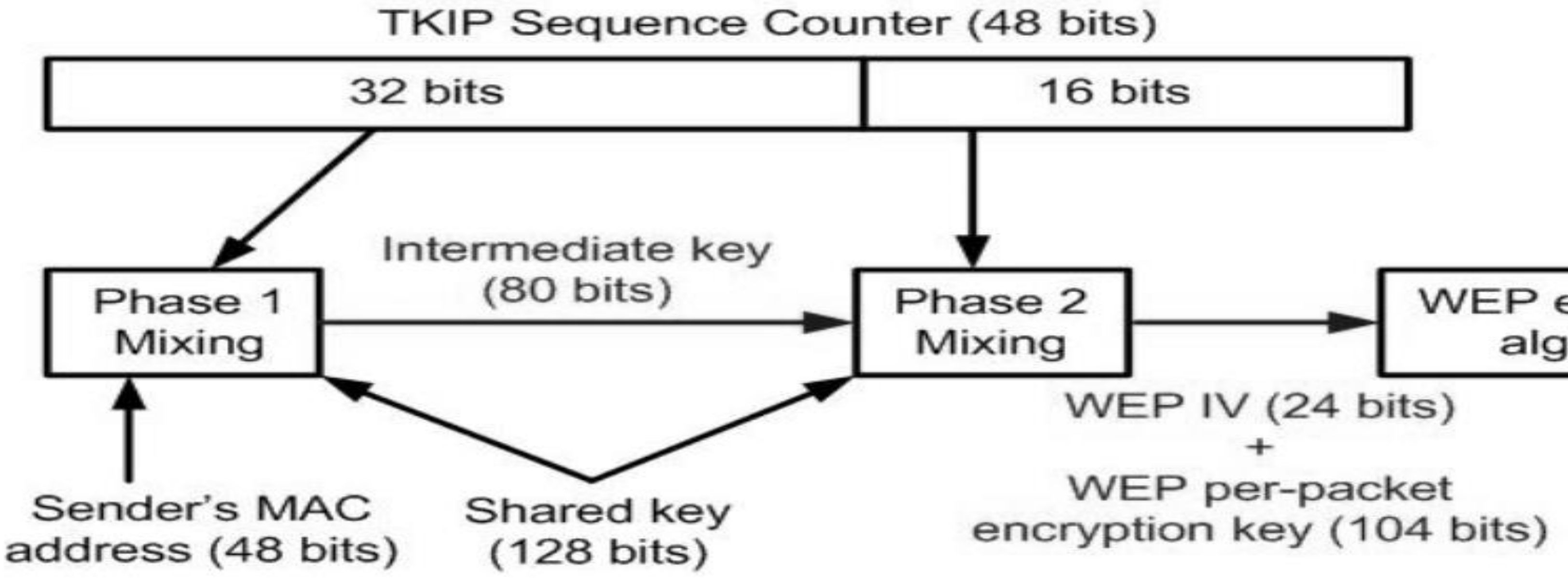
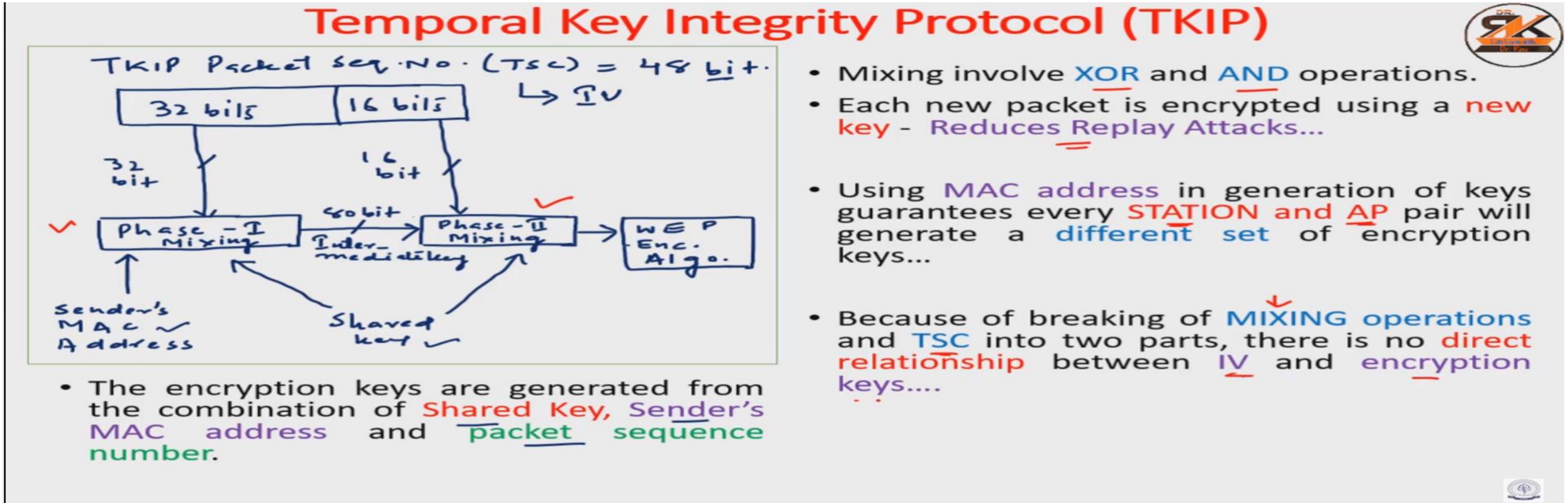
WPA :- Wi-Fi Protected Access

Known as **Wi-Fi Protected Access**.WPA became available in 2003.

- It is more secure than WEP.
- It Uses TKIP (Temporal Key Integrity Protocol).
- The keys used by WPA are 256-bit

WPA, just like WEP, after being put through proof-of-concept and applied public demonstrations turned out to be pretty vulnerable to intrusion.


TKIP Sequence Counter (48 bits)
32 bits
16 bits
Intermediate key (80 bits)
Phase 1 Mixing
Phase 2 Mixing
WEP encryption algorithm
WEP IV (24 bits) + WEP per-packet encryption key (104 bits)
Sender's MAC address (48 bits)
Shared key (128 bits)

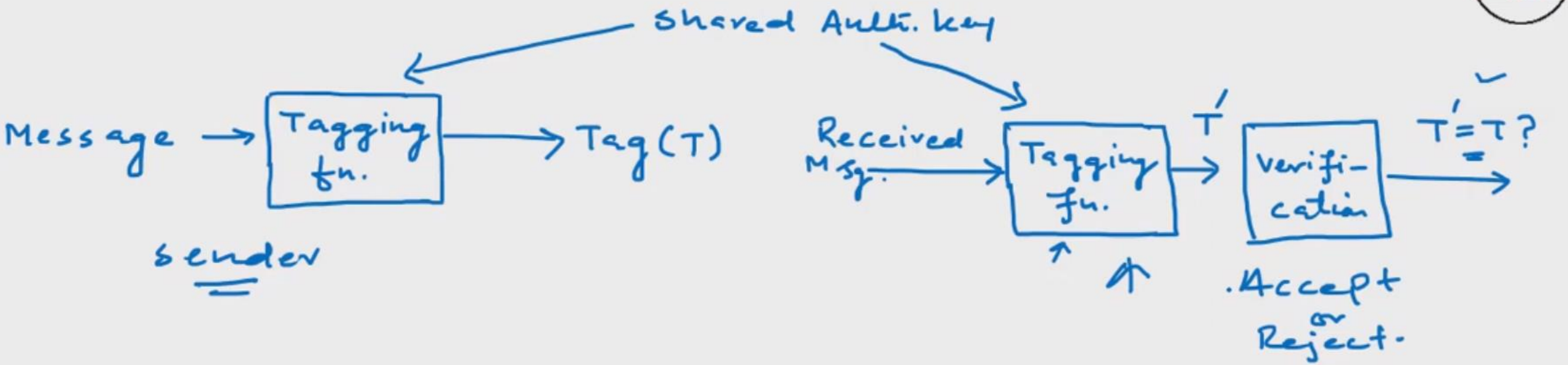


Temporal Key Integrity Protocol (TKIP)

- The encryption keys are generated from the combination of Shared Key, Sender's MAC address and packet sequence number.

- Mixing involve XOR and AND operations.
- Each new packet is encrypted using a new key - Reduces Replay Attacks...
- Using MAC address in generation of keys guarantees every STATION and AP pair will generate a different set of encryption keys...
- Because of breaking of MIXING operations and TSC into two parts, there is no direct relationship between IV and encryption keys....

Message Integrity Code (MIC)



- The message is partitioned into 32 bit chunks…

- In each iteration, one chunk is mixed with key using XORs, Bit Swaps and Additions.

- 64 bit O/P serves as MIC……………….. Defeats message forgery attacks