Name: Aswath S

College: Vellore Institute of Technology, Vellore

Reg.No: 21BEC2188

Wi-Fi Training Program 2025

Module 6

Question 4:

Why is WEP considered insecure compared to WPA2 or WPA3?

Solution:

Reason	Explanation
Weak Encryption (RC4)	WEP uses the RC4 stream cipher with very short keys (40 or 104 bits). RC4 itself has flaws, and WEP's implementation made it worse.
Short Initialization Vector (IV)	WEP uses a 24-bit IV, which is too short. It repeats quickly, making it easy for attackers to find patterns and crack the key.
No Strong Key Management	WEP keys are usually manually entered and rarely changed, so once the key is cracked, an attacker has long-term access.
Easily Crackable Tools	There are free tools (like Aircrack-ng) that can crack WEP passwords in minutes by capturing just a few thousand packets.
No Strong Integrity Check	WEP uses a simple CRC-32 checksum to check data integrity, which attackers can manipulate without detection.
No Protection Against Replay Attacks	Attackers can capture and replay old packets because WEP doesn't defend against it properly.