



Automotive Cyber Security Syllabus



1-Month Crash Course – Automotive Cyber Security Basics (4 Weeks)

Week 1 – Cybersecurity & Automotive Basics

- ❖ Cybersecurity overview, CIA triad
- ❖ Automotive ECUs & in-vehicle networks (CAN, LIN, FlexRay, Ethernet)
- ❖ Attack surfaces in vehicles
- ❖ Lab: Capture & analyze CAN traffic with Wireshark/PCAN

Week 2 – Cryptography & Secure Communication

- ❖ AES, RSA, ECC, Hashing (SHA2/3) basics
- ❖ Secure Onboard Communication (SecOC) overview
- ❖ UDS Security Access (Seed/Key)
- ❖ Lab: Implement simple AES encryption on CAN messages

Week 3 – ECU Security Foundations

- ❖ Secure Boot basics
- ❖ Firmware integrity validation
- ❖ OTA (Over-the-Air) update security basics
- ❖ Lab: Demonstration of Secure Boot validation flow

Week 4 – Case Studies & Compliance Intro

- ❖ Jeep Cherokee Hack, Tesla Hack overview
- ❖ ISO/SAE 21434 introduction
- ❖ Lab: Perform simple replay attack demo & mitigation

 **Outcome:** Crash knowledge for awareness + hands-on exposure.