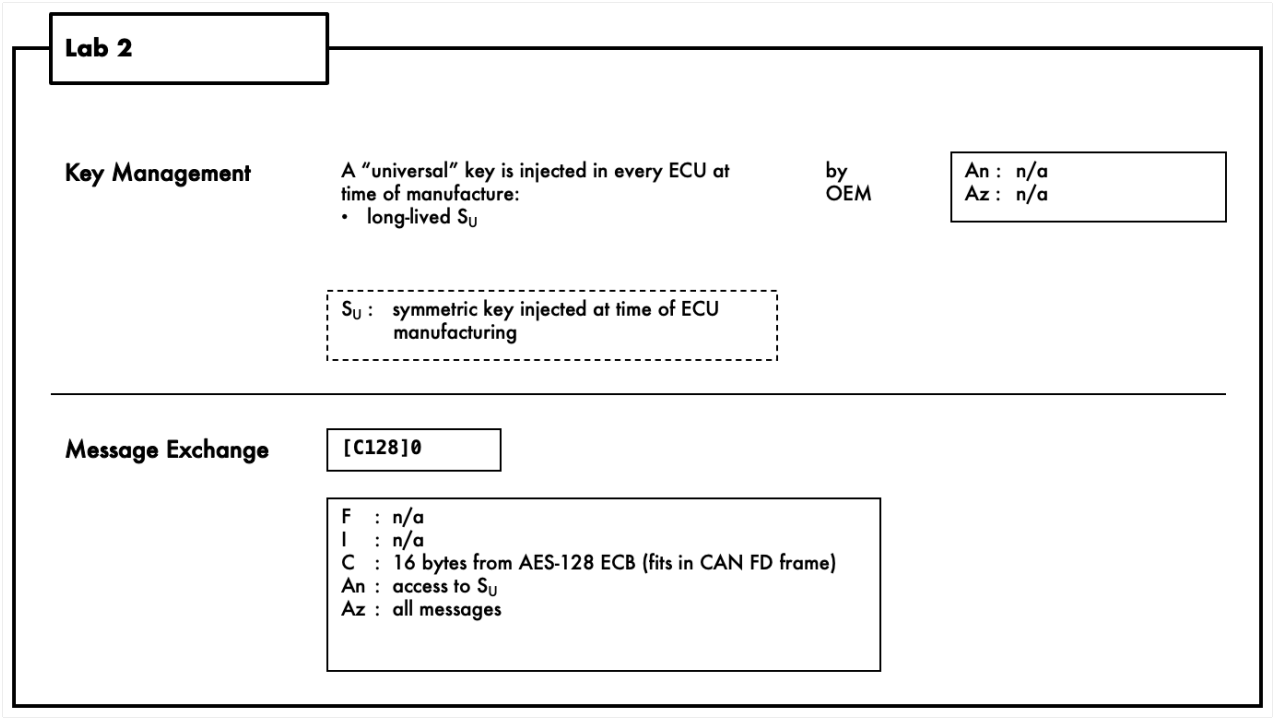


**Scenario** : Say your PoC convinced the product engineering team to to try to secure the messages, and their response was to use AES-ECB to encrypt every message on the bus. To do this required the use of CAN FD to send 16 bytes (128 bits) of encrypted data, where before we were only sending 8 bytes of plaintext data.
You can imagine someone saying "Wow! This must be really secure. There is 128 bits of encrypted data on the bus."
While you appreciate the change of heart to add security, you disagree that the system is secure. You know that this is a clear example of how *cryptography does not equate to security*.

**Exercise 1** : Review the network security framework, above. Comment on the risk added to this system through the use of $S_U$.

**Exercise 2** : [ATTACK] Create a PoC to allow driver assistance operations at any speed *without needing to exfiltrate* $S_U$. This can be a simple and noisy attack. You can assume that if half the time the vehicle thinks it is going less than the assistance threshold then assist will be available.
(note: Engine Speed and PTO Speed should appear as normal. That is, they ramp-up and down smoothly while Ground Speed is being attacked.)

**Exercise 3** : [ATTACK] Create a PoC that is less noisy on the bus by using MitM.
(hint: you still do not need $S_U$.)

**Exercise 4** : Say you did have $S_U$, comment on how it would change, if at all, your attack in Exercise 3.