- There are limitations to AI usage
- Some attacks can be go many routes to infer different information about certain users within the system

- Symmetric Ciphers' biggest issue
    - We still have not discussed the biggest issue regarding symmetric ciphers: how do we exchange the key?
- Message Authentication:
    - Protects against active attacks
    - Verifies that messages are authentic and not altered
    - Can be used with conventional encryption
    - No one can read the message, but it is still open to alterations
    - we use a signature that is generated by us, a hash value that is attached to the message.
        - one verifies (signature)
        - encryption for those that should not be seeing it
        - Shown in figure 2.3 in the reading.
    - IMEI is like a UID for phones which is used to access networks… network identifies you as a verified user with IMEI
- Hash Requirements: Continue here on 2/21