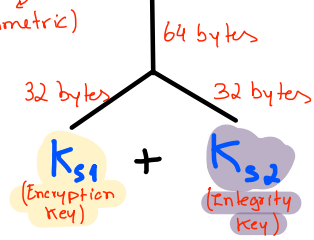


Session Communication: Encryption

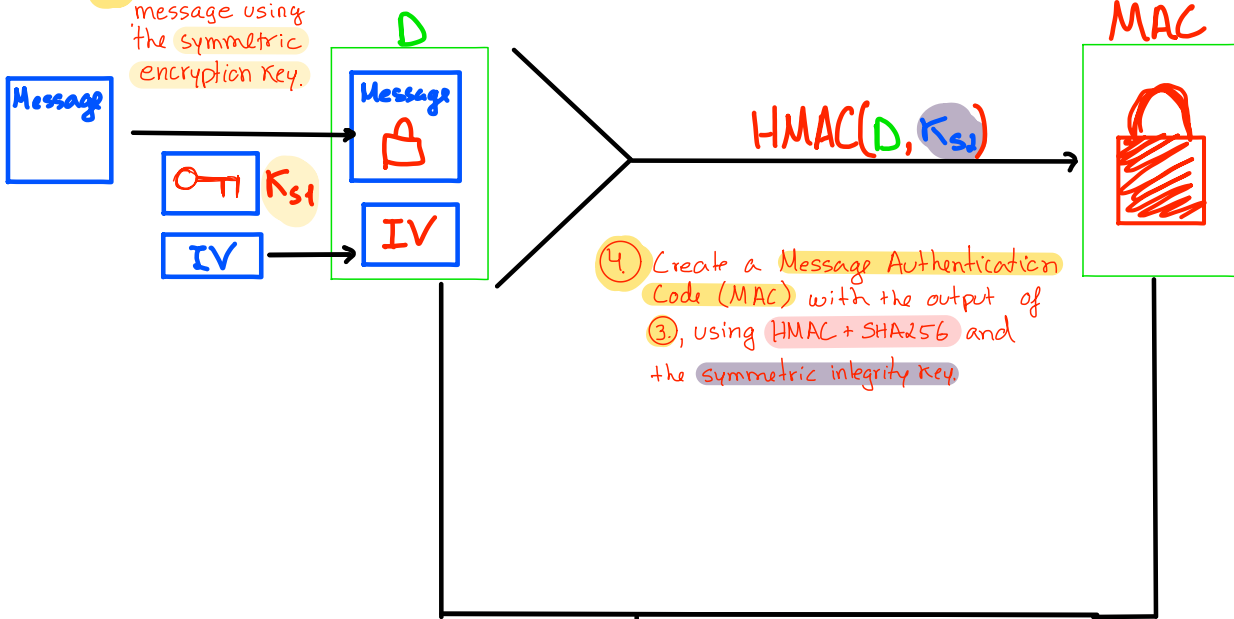
$S = K_s = \text{secret}$
(session key)
(symmetric)



① Use the **ECDH secret** agreed when creating session

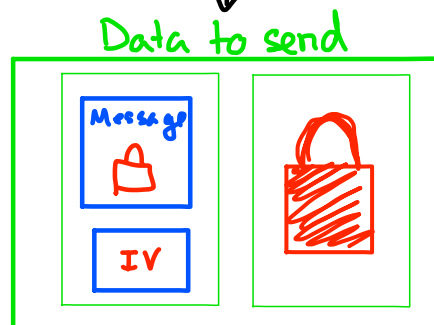
② Divide in 2 32-byte **symmetric keys**

③ Encrypt the message using the **symmetric encryption key**.



④ Create a **Message Authentication Code (MAC)** with the output of ③, using **HMAC + SHA256** and the **symmetric integrity key**.

⑤ **Concatenate** all the data to send.



⑥ **Send it** through an **insecure channel**