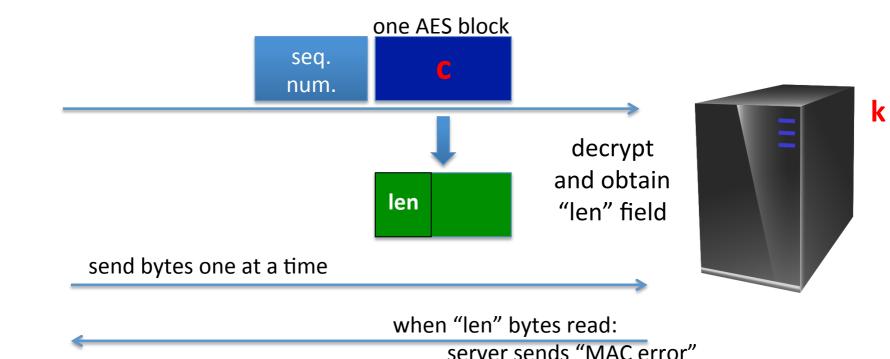
Attacker has <u>one</u> ciphertext block c = AES(k, m) and it wants m



attacker learns 32 LSB bits of m!!