CS 338

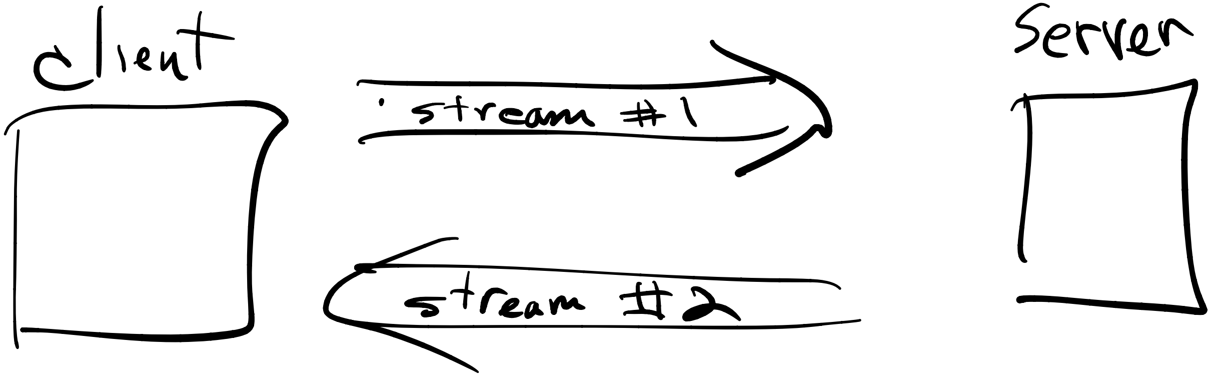
M, 22 Sep 2025

+

W, 24 Sep 2025

ACK

TCP connection 2 one-way streams



ACK

Every TCP packet has

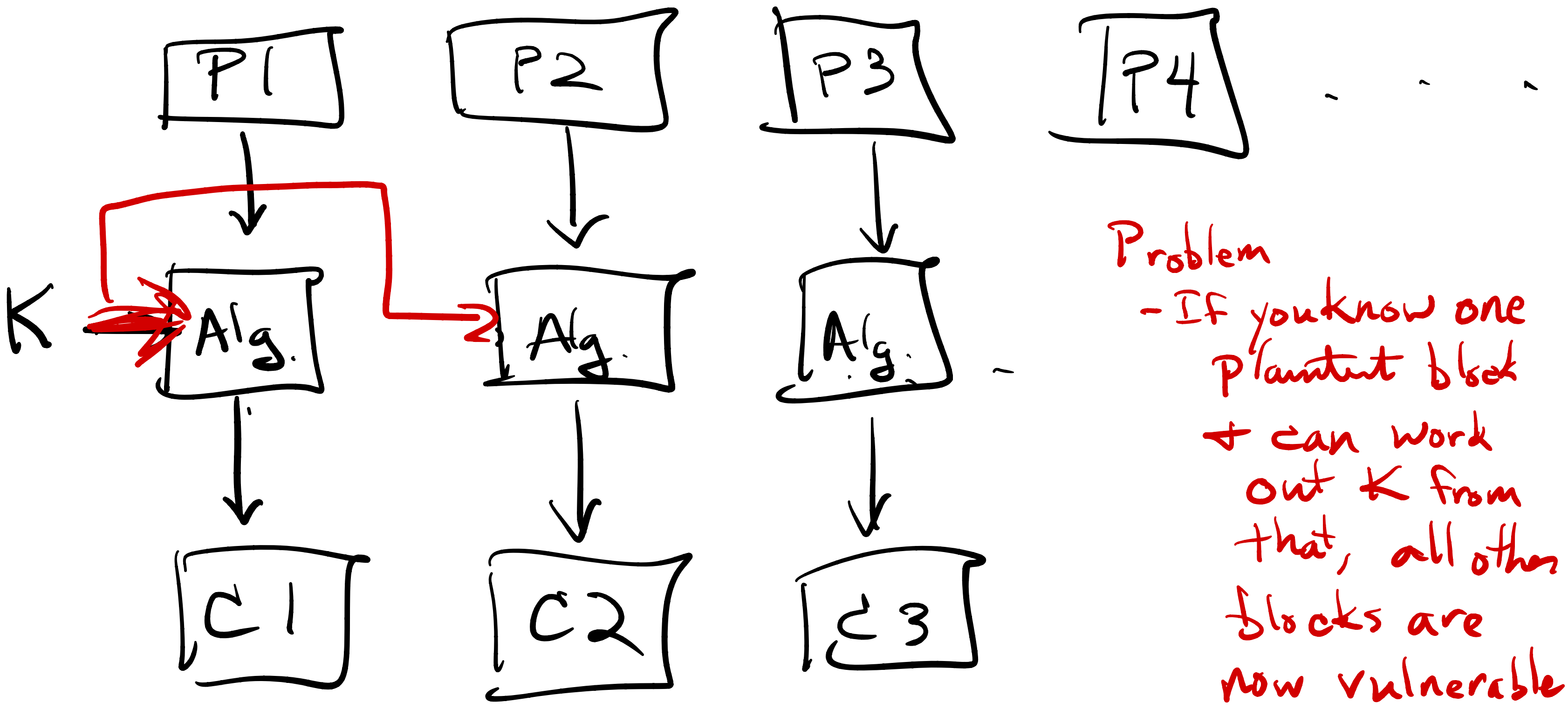
Seq # : "how many bytes of payload have I sent you so far"

ACK : "how many bytes in order have I seen from you"

Electronic Code Book (ECB)

Bad

plaintext in blocks



ciphertext

Problem

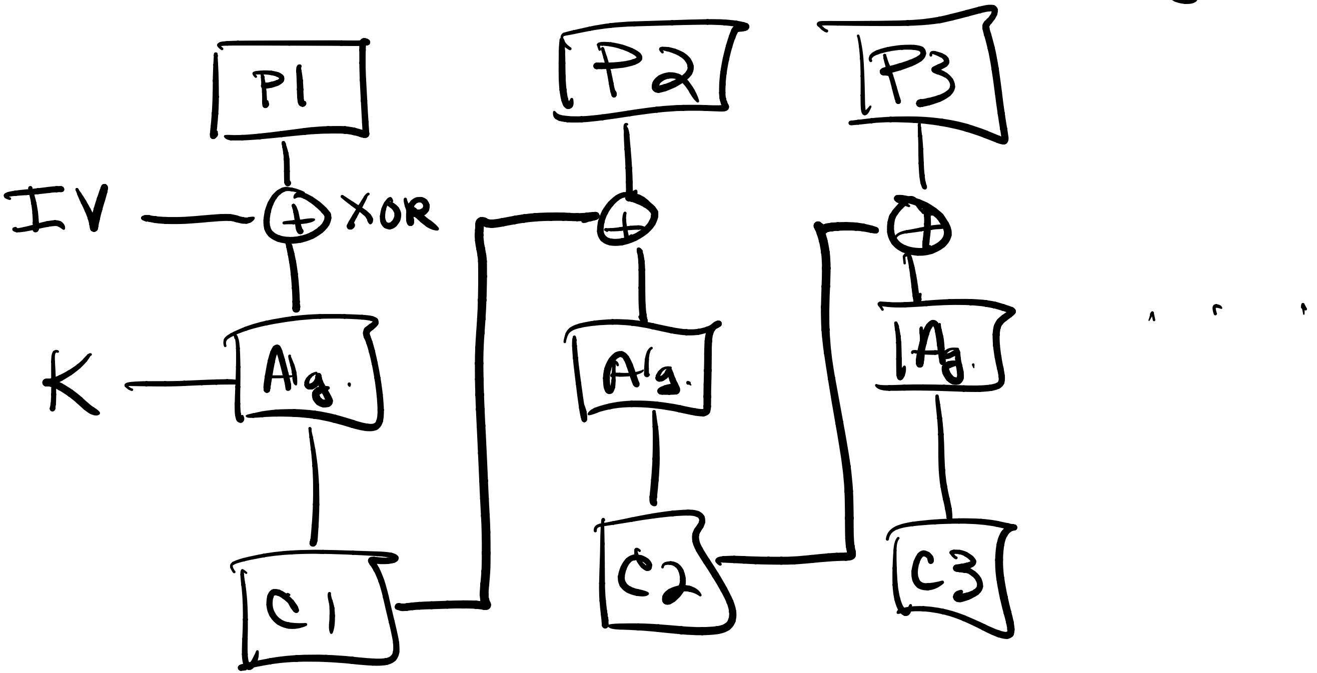
- If you know one plaintext block + can work out K from that, all other blocks are now vulnerable

AES blocks are 128 bits

cont'd

if any P_j and P_k are the same, cracking one of C_j or C_k cracks the other

Alternately: CBC Cipher Block Chaining
(Good)



AES = Advanced Encryption Standard

Rijndael (won a contest)