

(pure) Encryption Modes

a.k.a. how to encrypt long messages

ECB - Electronic Code Book

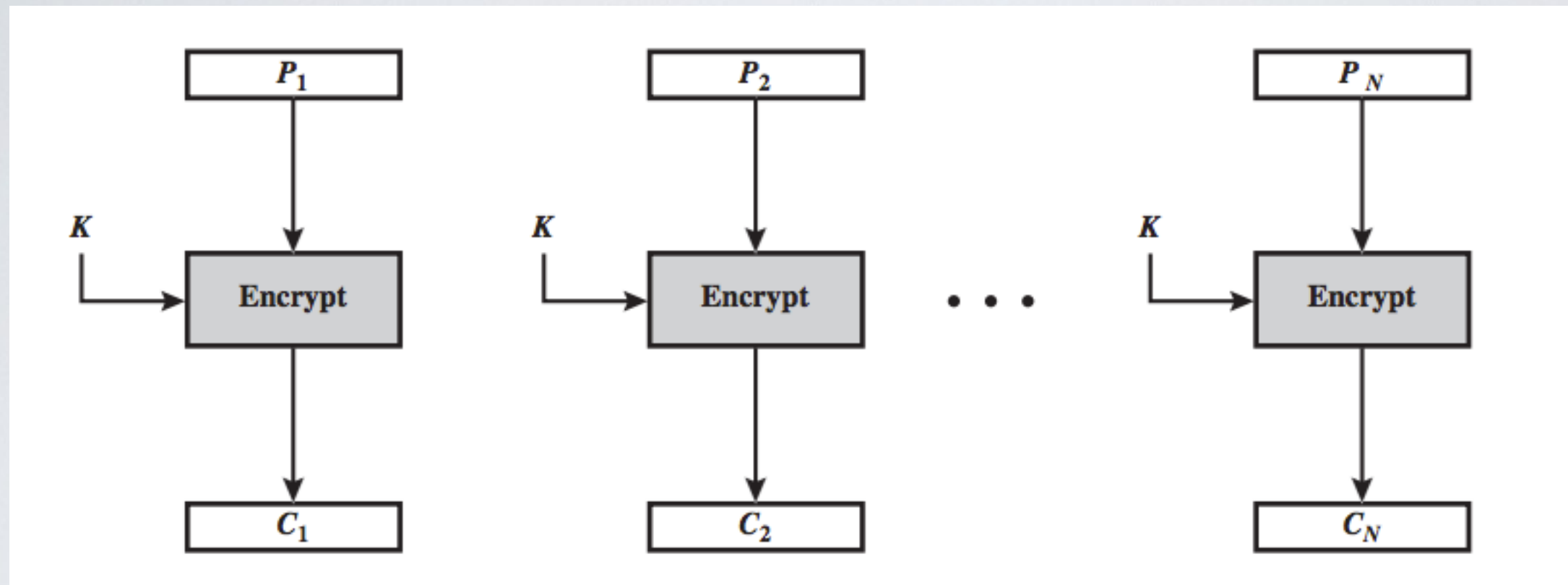
CBC - Cipher Block Chaining

CFB - Cipher Feedback

OFB - Output Feedback

CTR - Counter

ECB - Electronic Code Book



Each plaintext block is encrypted independently with the key

✓ Block can be encrypted in parallel

⦿ The same block is encrypted to the same ciphertext