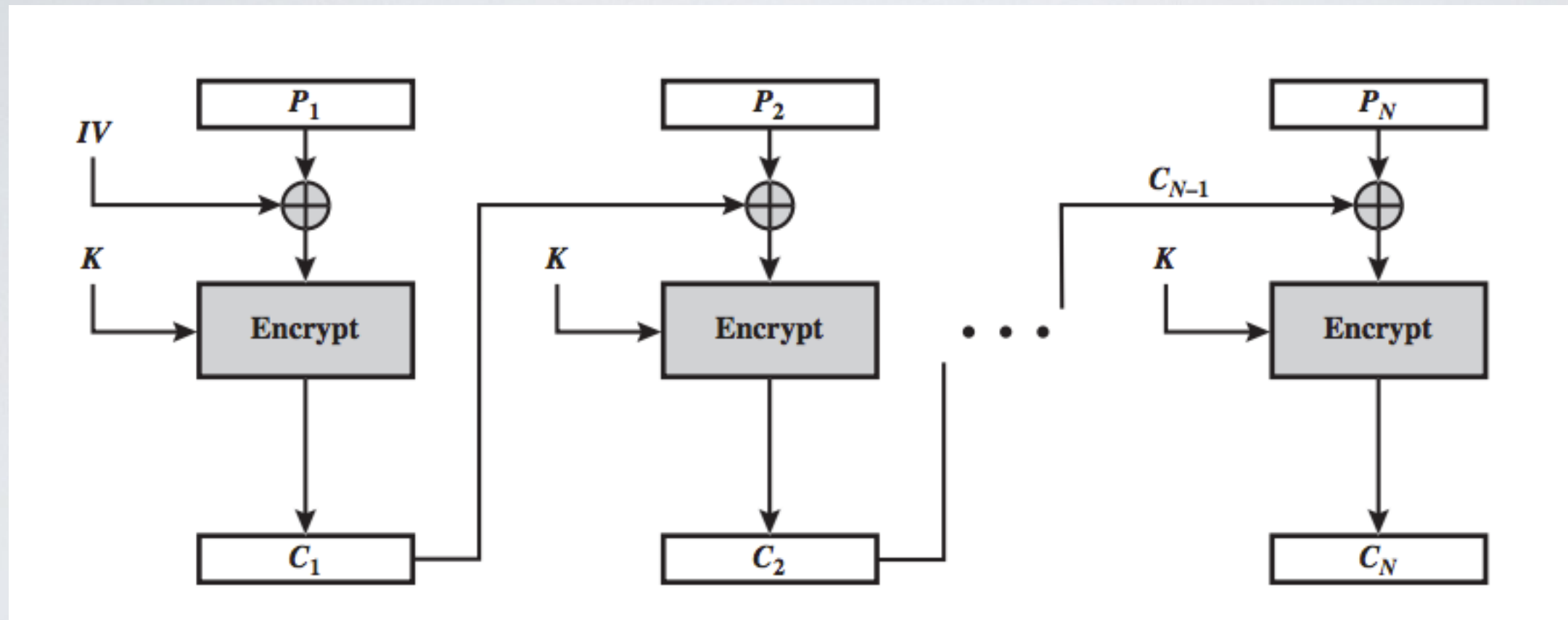


CBC - Cipher Block Chaining



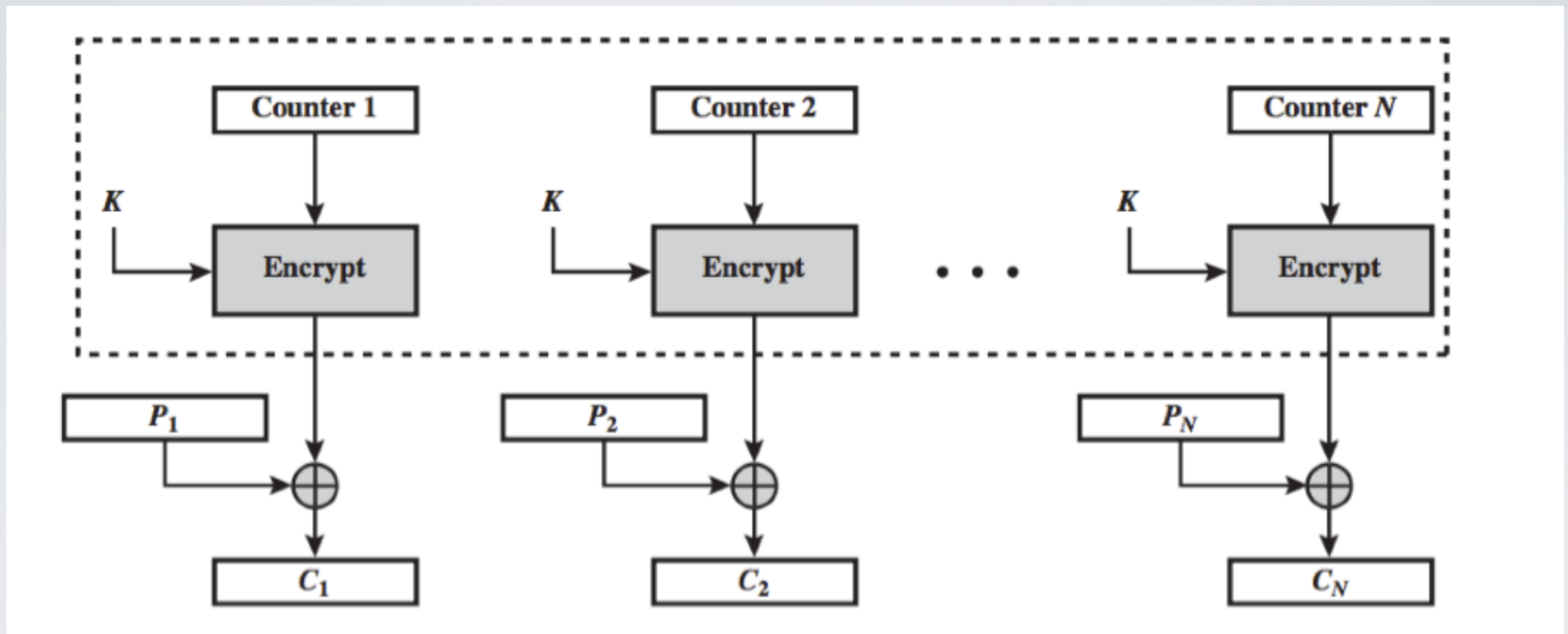
Introduce some randomness using the previous ciphertext block

✓ Repeating plaintext blocks are not exposed in the ciphertext

⦿ No parallelism

➡ The Initialization Vector should not be known by the opponent and must be sent separately (ECB mode for instance)

CTR - Counter



Introduce some randomness using a counter

✓ High entropy and parallelism

⦿ Sensitive to key-reused attack

➡ Popular usage : IPsec (coming soon in this course)