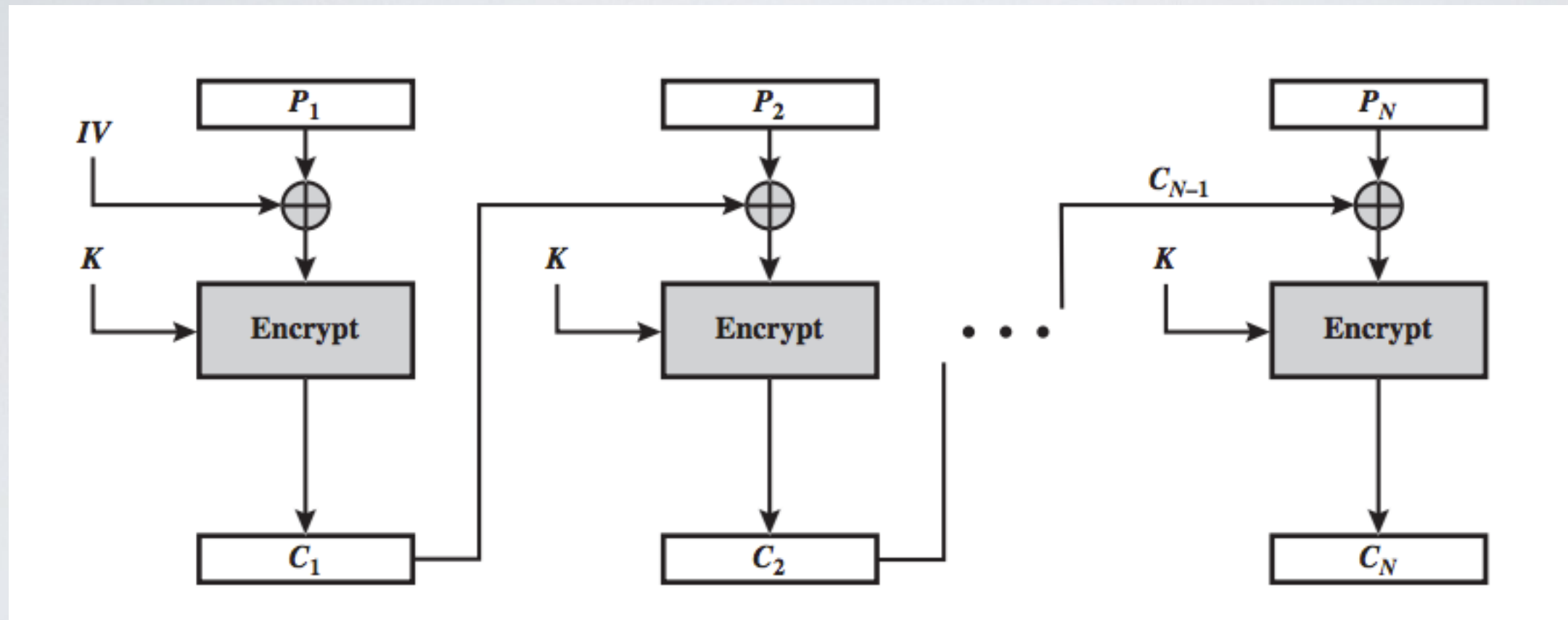


CBC - Cipher Block Chaining



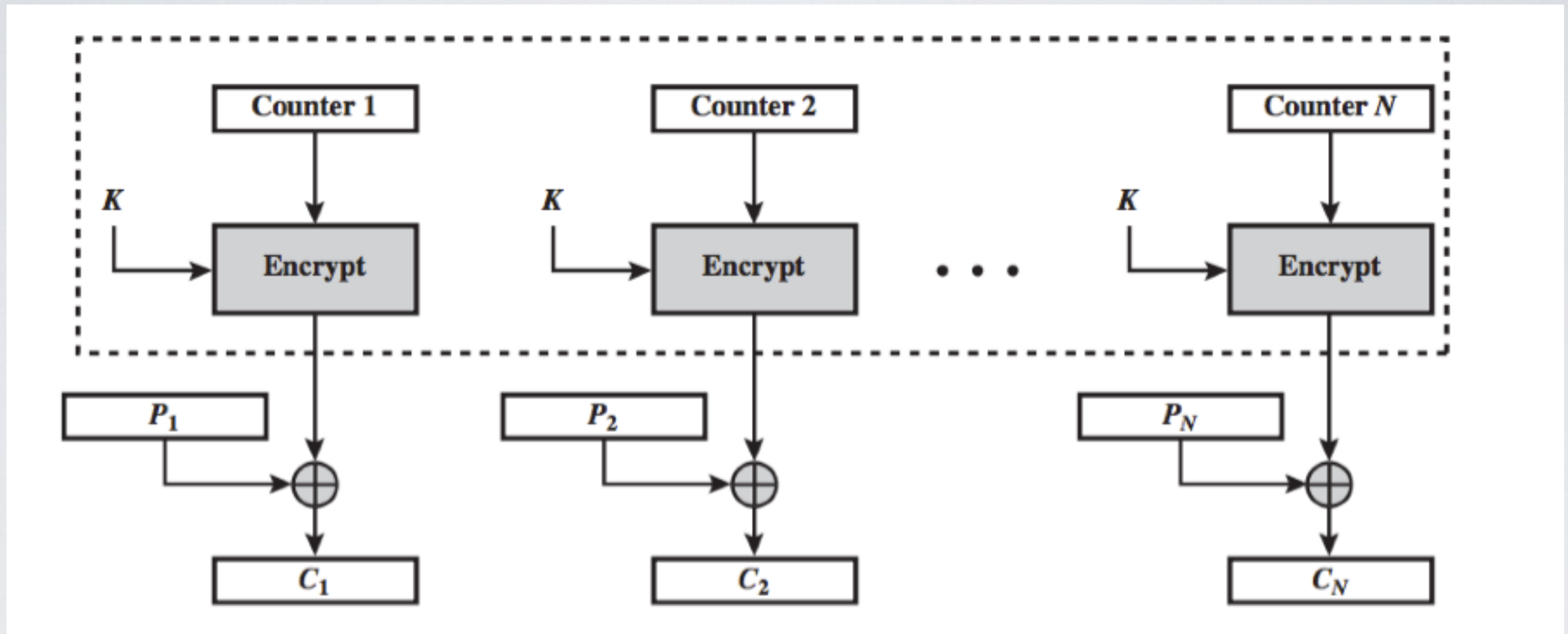
Introduce some randomness using the previous ciphertext block

✓ Repeating plaintext blocks are not exposed in the ciphertext

⦿ No parallelism

➡ The Initialization Vector should be known by the recipient

CTR - Counter



Introduce some randomness using a counter

- ✓ High entropy and parallelism
- Sensitive to key-reused attack