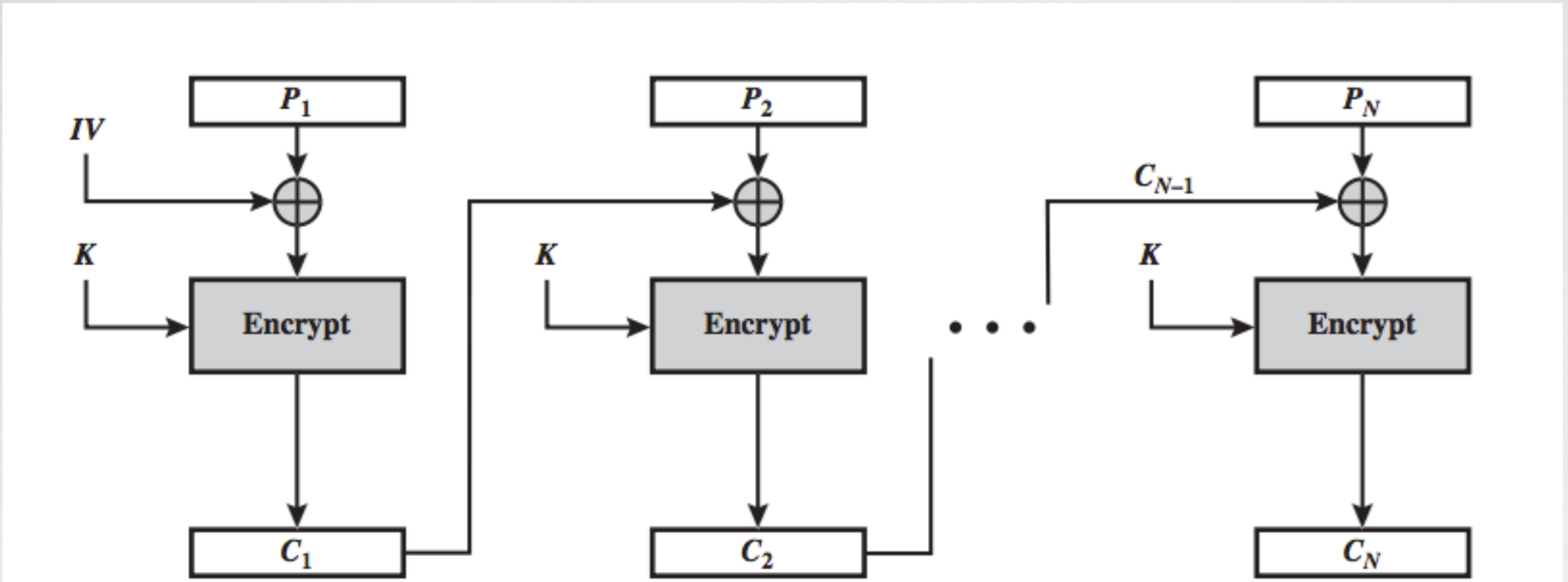
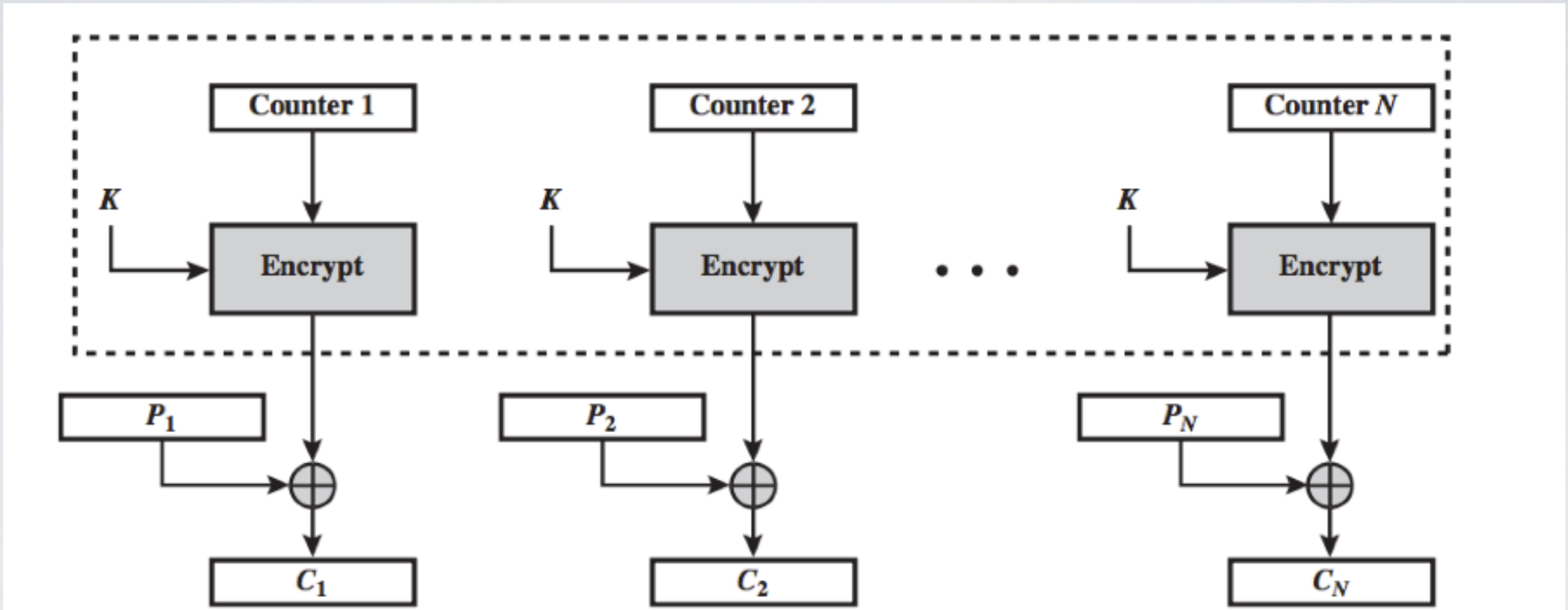
CBC - Cipher Block Chaining (a.k.a Chaining Mode)



Introduce some <u>randomness</u> 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 Mode



Introduce some randomness using a counter

- ✓ High entropy and parallelism
- ◉ Behaves as a stream cipher - sensitive to key-reused attack