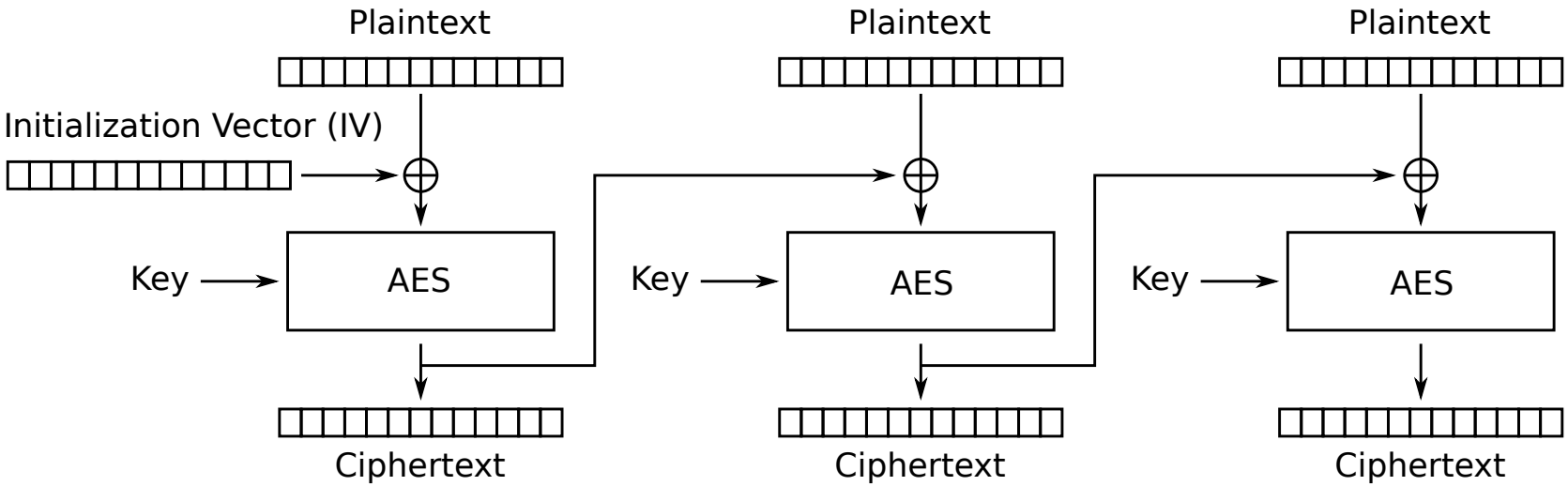
Modes of Operation: CBC

Cipher Block Chaining (CBC):



CBC ist sicher ... wenn,

- IVs zufällig gewählt werden (je nach Anwendung)
- nicht zu viele Daten verschlüsselt werden
  (Limit bei 128 bit Blockgröße: $\approx 2^{68}$ Bytes)
- **nichts über den Klartext bekannt ist**