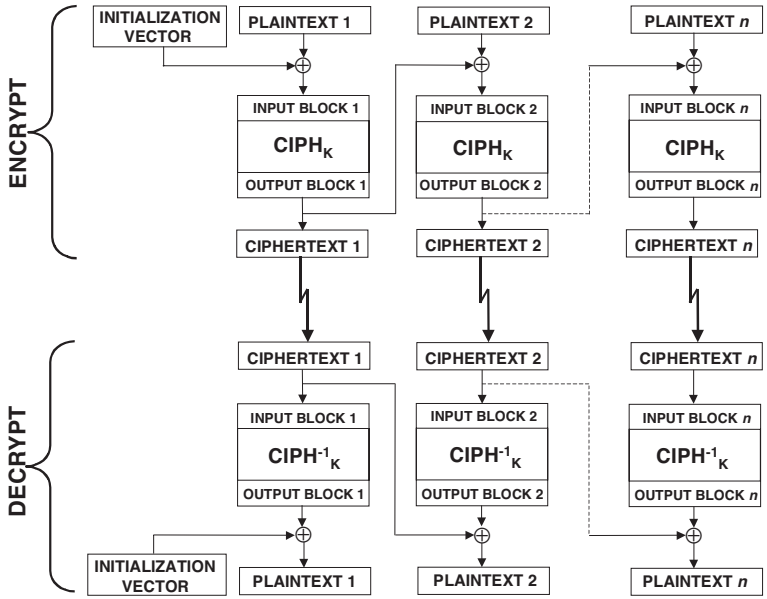
Block Cipher Modes



Five Confidentiality Modes

- Five confidentiality modes: ECB, CBC, CFB, OFB, and CTR
- ECB: Electronic Codebook
- CBC: Cipher Block Chaining
- CFB: Cipher Feedback
- OFB: Output Feedback
- CTR: Counter

Advanced Modes

- Authentication Mode: CMAC stands for cipher-based message authentication code
- Authenticated Encryption Mode: CCM combines the counter mode for confidentiality with the cipher block chaining technique for authentication
- High-Throughput Authenticated Encryption Mode: GCM (Galois Counter Mode) combines the counter mode for confidentiality with an authentication mechanism that is based on a universal hash function
- Confidentiality Mode Designed for Storage Devices: XTS-AES mode was designed to protect the confidentiality of data on block-oriented storage devices without providing authentication
- Methods for Key Wrapping: AES Key Wrap (KW) mode, AES Key Wrap With Padding (KWP) mode, Triple DES Key Wrap (TKW) mode