

AES (Encryption/Decryption)

Product Features (Brief)

- Latest NIST FIPS-197 compatible AES Encryption and Decryption.
- Support all AES key sizes (128, 192 and 256-bits).
- Compile as Encryptor, Decryptor, Encryptor/Decryptor or Encryptor + Decryptor in duplex mode.
- Supports all modes (ECB, CBC 128, OFB and CTR) of AES defined in SP800-38A.
- Very high performance implementation results.

Applications

- Wireless Networking: IEEE 802.11, 802.15, 802.16 and 3GPP-LTE
- Internet Security: IPSec, SSL, TSL protocols
- Electronic Financial Transactions using ANSI x9.53
- Secure Communications
- Power line networks
- Encrypted Data Storage Security: IEEE P1619
- Digital Rights Management
- Secure Video Surveillance Systems
- Secure RFID