

# AES

Powered by original computing algorithm "DMNA" based on mathematical methods

## 1 Abstract

TMC's AES encryption / decryption IP core is validated by "NIST CAVP".

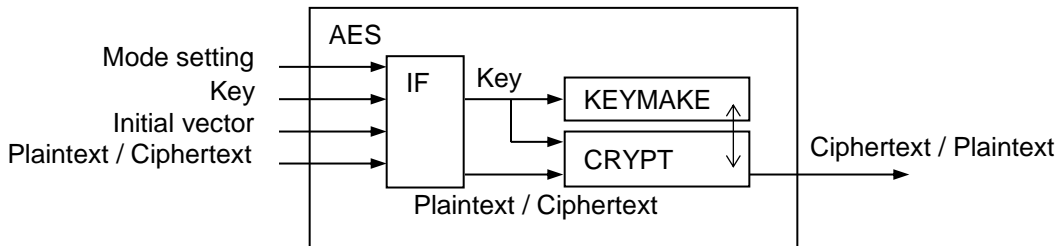
It processes at high speed, so it can be used high-speed LAN systems and other fields.

## 2 Features

Super high speed operation

- Process one round in one clock
- Processing power 1 Gbps(Operating frequency is 100 MHz)
- Implementable on FPGA

## 3 Block Diagram



## 4 Specifications

Cryptographic Standards	Compliant with NIST FIPS PUB 197
Certification	NIST AES Algorithm Validation Cert. #3875
Encryption Mode	ECB/CBC/OFB/CFB1/CFB8/CFB128 (CTR mode : optional)
Bit Length	Plaintext: 128 bits, Ciphertext: 128 bits, Key length: 128/192/256 bits
Throughput	1 round/clock (Ex.) 1Gbps at key length:128bit, frequency:100 MHz. *The maximum operating frequency depends on process technology / FPGA etc..

**Note** Specifications are subject to change without notice

### Contact Information

7F, Gotanda NN Bldg., 2-12-19, Nishi-gotanda, Shinagawa-ku, Tokyo 141-0031

**Techno Mathematical Co., Ltd.**

TEL: +81-3-3492-3633

Email: info-sales@tmath.co.jp

FAX: +81-3-3492-3631

URL: <https://www.tmath.co.jp>