File Encryption/Decryption With AES in Python

Presenter: MohammadReza Vafazadeh

Teacher: Dr. Fazlollah Adibnia

What is AES?

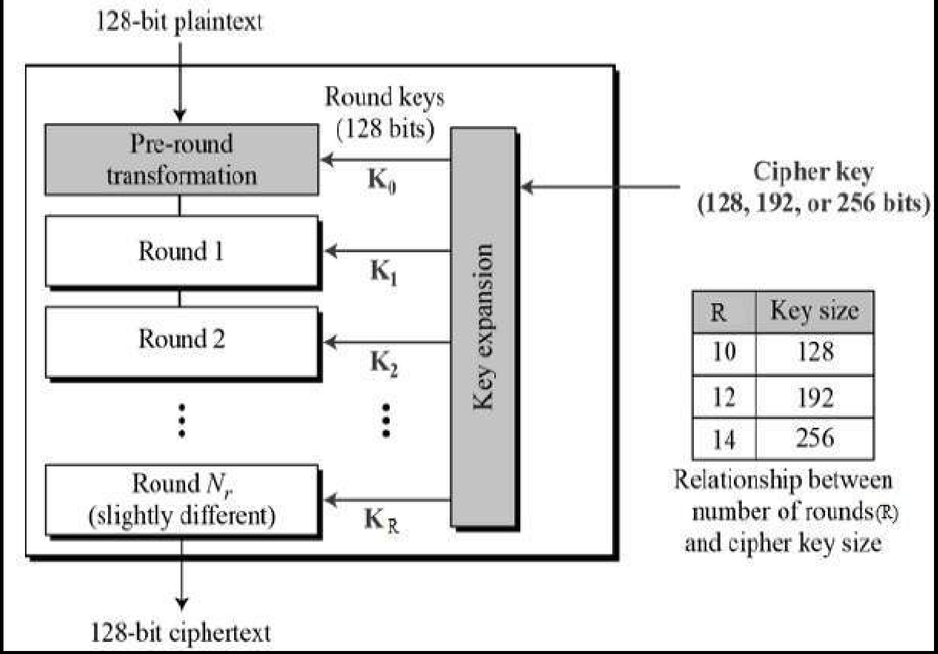
- Advanced Encryption Standard
- Established by the U.S. National Institute of Standards and Technology (NIST)
- Created in 2001

Why AES?

- Best public crypt analysis
- Key sizes: 128, 192 or 256 bit (16, 24 or 64 Byte)
- Block Size: 128 bit
- Fast (Fastest Encryption Algorithm)
- Secure

How AES Works?

- Create R sub-keys from main key
- Execute R round depends on key length

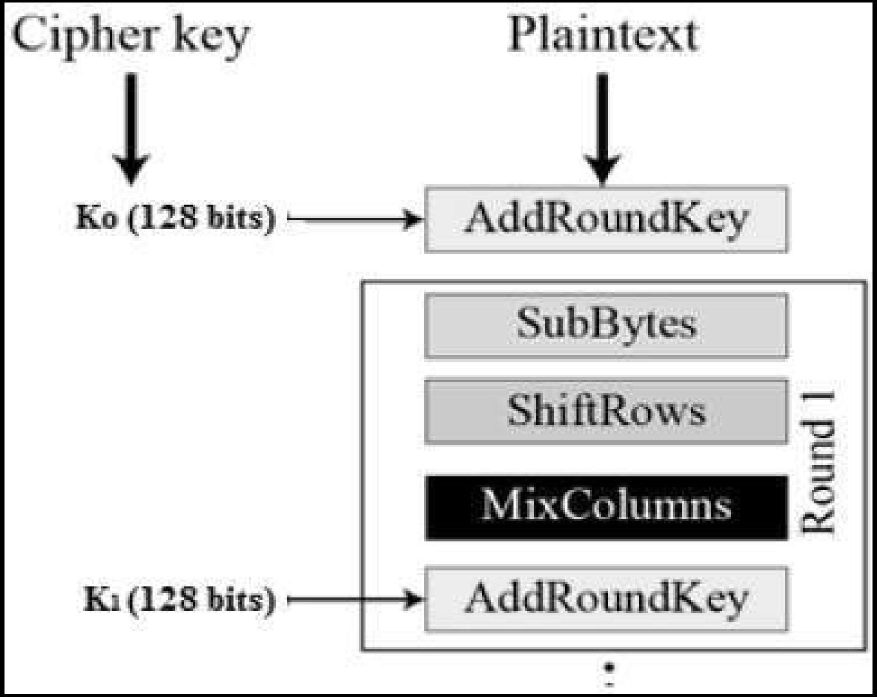


R	Key size
10	128
12	192
14	256

Relationship between number of rounds(R) and cipher key size

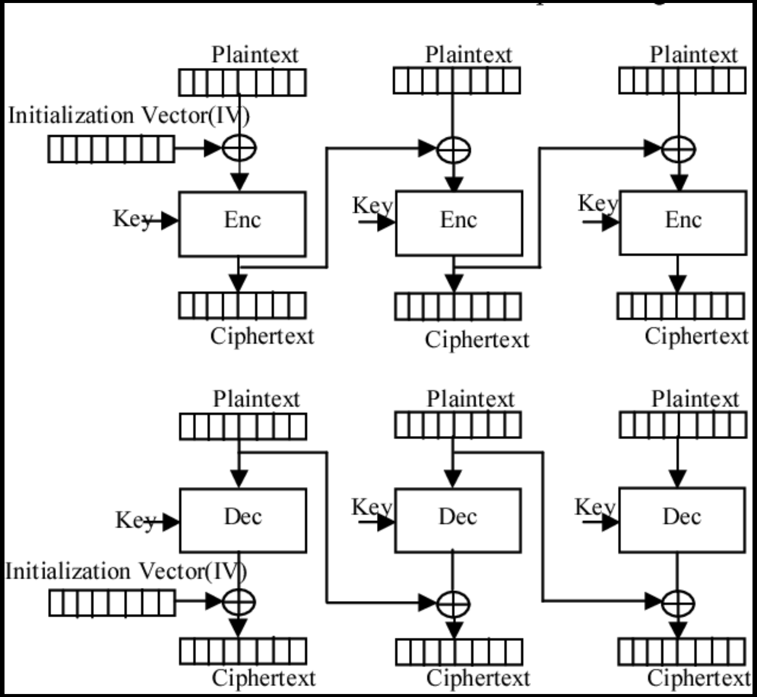
How AES Works? (Continue)

- Create RoundKey for next round
- Execute round functions



Mode in encryption

- OFB (output FeedBack)
- CBC (Block cipher mode of operation)
- PGP (Pretty Good Privacy)
- CFB (Cipher FeedBack)
- CTR (Counter)
- OPENPGP



Code Architecture / Encryption

- Get key and hash it with sha256 (Why?)
- Read file in all bits
- Send file bits to AES module
- Write data in file

Code Architecture / Decryption

- Get the key and hash it with sha256
- Read the file in bits
- Send data to AES module
- Write data in output file

Thanks for your patience

MohammadReza Vafazadeh