AES Extension from 128-bits to 192-bits & 256-bits

MSCS\_630L\_231\_16S

Security Algorithms & Protocols

Created By

Dixita Sharegar

Saranya Radhakrishnan

# Introduction

AES i.e. Advanced Encryption Standard is a specification by NIST to encrypt and decrypt electronic data established by the National Institute of Standards and Technology. It is a block cipher which uses a block length of 128 bits. AES allows for 3 different key lengths 128,192 and 256. AES is symmetric i.e. it uses the same secret key for encryption & decryption, both sender & receiver should share this key. All key lengths are considered good enough to protect classified information up to the “Top Secret” level.

AES 128 bit encryption was accomplished in the previous lab work for this course, which serves as a base for the subsequent decryption techniques implemented as mentioned in this paper.