IMPROVED ADVANCED ENCRYPTION STANDARD (AES) ALGORITHM WITH ADDED ADDROUNDKEY

ABSTRACT

The Advanced Encryption Standard (AES) is a widely-used symmetric encryption algorithm that provides secure and efficient data encryption. However, there is always a need to improve the security of cryptographic algorithms to meet the increasing demands of secure communication and data protection. In this project a Modified AES Encryption algorithm is proposed using an additional AddRoundKey operation. The additional AddRoundKey operation is applied before the MixColumns operation, which can provide an additional level of diffusion and improve the security of the encryption.

The modified AES encryption algorithm is tested against standard AES encryption algorithm using a variety of test vectors. Test results shows that the modified AES algorithm has better Avalanche effect compared to the standard AES algorithm. The modified AES algorithm provides improved diffusion and confusion properties than standard AES encryption algorithm, which can make it more secure against certain types of attacks.

Keywords: Standard AES , Modified AES, AddRoundKey, Avalanche effect, Diffusion, confusion.

GUIDE:

T. MUKTHAR AHAMED

BY

D.LOKESH (1011902017)

G.DEVENDRA(1011902008)

K.MADHUSUDHAN(1011902018)

K.SASIREKHA(1011902030)

L.PRAVEEN KUMAR(1012002905)