ADVANCED ENCRYPTION STANDARD with user interface

The Advanced Encryption Standard (AES) is a symmetric block cipher chosen by the U.S. government to protect classified information. AES is implemented in software and hardware throughout the world to encrypt sensitive data. It is essential for government computer security, cybersecurity and electronic data protection.

Features of AES:

1. Block encryption implementation
2. 128-bit group encryption with 128,192 and 256-bit key lengths
3. Symmetric algorithm requiring only one encryption and decryption key
4. Data security for 20-30 years
5. Worldwide access
6. No royalties
7. Easy overall implementation

History of AES:

1998-15 proposals to NIST for a better cipher

2001-Rijndael from Belgium chosen as AES

AES does not use Feistel structure

Secure and flexible.

Process of AES:

1. Initial round key addition
   ADD round key-each byte of the state is combined with a byte of the round key using bitwise xor
2. SUB BYTES: a non-linear substitution step where each byte is replaced with another according to a lookup table
3. Shift-rows: a transposition step where the last three rows of the state are shifted cyclically certain number of steps
4. Mix columns- a linear mixing operation which operates on the columns of the state combining the four bytes in each column which is done by Galois multiplication.

5. Key expansion: Round keys are derived from the cipher key using the AES key schedule. AES requires a separate 128-bit round key block for each round plus one more
   Steps involved in Key expansion:
   1.One-byte circular left shift
   2. byte substitution using forward S-box
   3.XOR with Round constant

Keying restrictions:

No weak or semi-weak keys have been identified for AES algorithm and there is no restriction for key selection.

THE SOURCE CODE OF THE PROJECT IS :

https://github.com/sreecharan05/Cryptography-project

USER INTERFACE:

After entering the values and getting encrypted text:

For encryption:

For decryption:

TEAM members:

M. SREE CHARAN SAI(AM.EN.U4CSE19232)

P. CHETHAN SAI KUMAR REDDY(AM.EN.U4CSE19242)

K. KARTHIK VISWANADH(AM.EN.U4CSE19269)

M.GOWTHAM(AM.EN.U4CSE19234)