AES Encryption

Enter Plain Text to Encrypt -

Кожен день є новим початком. Подолайте свої страхи, вірте в себе і рухайтеся вперед. Ваш успіх чекає вас.

The String which is to be encrypted using AES

Select Mode ECB

AES works in 2 modes - CBC and ECB mode.
CBC (Cipher Block Chaining) requires Initialization Vector(IV) to make each message unique.Using IV we randomize the encryption of similar blocks. So any identical plain text blocks will be encrypted into disimmilar cipher text blocks
ECB(Electronic Code Book) encryption mode does not need the IV for encryption. The input plain text will be divided into blocks and each block will be encrypted with the key provided and hence identical plain text blocks are encrypted into identical cipher text blocks.

Key Size in Bits 128

The input can be of 128 bit or 192 bit or 256 bit
So if key size is 128 then "aesEncryptionKey" is a valid secret key because it has 16

Enter Initialization Vector -

Select Mode ECB

AES works in 2 modes - CBC and ECB mode.
CBC (Cipher Block Chaining) requires Initialization Vector(IV) to make each message unique.Using IV we randomize the encryption
blocks. So any identical plain text blocks will be encrypted into disimmilar cipher text blocks
ECB(Electronic Code Book) encryption mode does not need the IV for encryption. The input plain text will be divided into blocks and
block will be encrypted with the key provided and hence identical plain text blocks are encrypted into identical cipher text blocks.

Key Size in Bits 128

The input can be of 128 bit or 192 bit or 256 bit
So if key size is 128 then "aesEncryptionKey" is a valid secret key because it has 16 characters i.e 16*8=128 bits

Enter Initialization Vector -

The initialization vector is needed in case of CBC mode
The initialization vector size should be 128 bit
So if initialization vector size is 128 then **"encryptionIntVec"** is a valid initialization vector because it has 16 characters i.e 16*8=128 bi

Enter Secret Key - aesEncryptionKey

As AES is a symmetric algorithm the same secret key can be used for both encryption and decryption. The expected secret ke
have specified in the key size dropdown
So if key size is 128 then **"aesEncryptionKey"** is a valid secret key because it has 16 characters i.e 16*8=128 bits

Output Text Format Base64

Specify if output format should be in Base64 encoded format or Hex Encoded format.

Encrypt

```
knJh0zpJ5kYobaxBUPNvcdYDtt+NCrFBH0qFupdpBx5L7eFZ36jNpjGwIQFsBxBu8GRfWnsYtwwrGxhtl+iozDCqFKNiaqs1YHIkYnjSBCMvvCJ3qF1TgdaTramQeDrzUyUQKZpLk2QrPTDQxQ5a4KzCrb+M1o4aSArlR9
```

AES Decryption

Enter Encrypted Text to Decrypt -

```
wwrGxhtI+iozDCqFKNiaqs1YHlkYnjSBCMvvCJ3qF1TgdaTramQeDrzUyUQKZpLk2QrPTDQx
Q5a4KzCrb+M1o4aSArIR9Ih7SzeHhBNQsGv7r9EMBxw2GqIYWwLBgPVWU4QDWsaQ9Pnc
0Ug+J/gt3vLQwENlYcT21VHlHOp/JyUcB6H6t9SyatJ
```

The AES Encrypted String which we want to decrypt

Input Text Format Base64

Specify if input format is in Base64 encoded format or Hex Encoded format.

Select Mode ECB

AES works in 2 modes - CBC and ECB mode.
CBC (Cipher Block Chaining) requires Initialization Vector(IV) to make each message unique.Using IV we randomize the encryption of similar blocks. So any identical plain text blocks will be encrypted into disimmilar cipher text blocks
ECB(Electronic Code Book) encryption mode does not need the IV for encryption. The input plain text will be divided into blocks and each block will be encrypted with the key provided and hence identical plain text blocks are encrypted into identical cipher text blocks.

Key Size in Bits 128

The input can be of 128 bit or 192 bit or 256 bit
So if key size is 128 then "aesEncryptionKey" is a valid secret key because it has 16 characters i.e 16*8=128 bits

Enter Initialization Vector -

The initialization vector is needed in case of CBC mode
The initialization vector size should be 128 bit
So if initialization vector size is 128 then **"encryptionIntVec"** is a valid initialization vector because it has 16 characters i.e 16*8=128 bits

Enter Secret Key - aesEncryptionKey

As AES is a symmetric algorithm the same secret key can be used for both encryption and decryption. The expected secret key size we have specified in the key size dropdown
So if key size is 128 then **"aesEncryptionKey"** is a valid secret key because it has 16 characters i.e 16*8=128 bits

Decrypt

```
Кожен день є новим початком. Подолайте свої страхи, вірте в себе і рухайтеся вперед. Ваш успіх чекає вас.
```