

Jere Mike C. Hipos

BSIT 4-1

ACTIVITY TITLE: " CIA Triad Application (Hands-on)"

A. CONFIDENTIALITY TEST – BASIC DATA ENCRYPTION

Tool: Online AES Encryption/Decryption tool

<https://www.devglan.com/online-tools/aes-encryption-decryption>

AES Encryption

Enter Plain Text to Encrypt

You can't see the future if you don't take a risk

Select Cipher Mode of Encryption

ECB

Select Padding

PKCS5Padding

Key Size in Bits

128

Enter Secret Key

EMIKHPOS198765

Output Text Format

Base64

Encrypt

AES Encrypted Output

oXqUQINASmX4GxoFC7b2MN3QJMLFb2xTJBxUKJmZBvwmvutZhbyqyOvDR84IZR5A
ZHnm9D+8xehHmPMci7IQ==

AES Decryption

AES Encrypted Text

oXqUQINASmX4GxoFC7b2MN3QJMLFb2xTJBxUKJmZBvwmvutZhbyqyOvDR84IZR5A
ZHnm9D+8xehHmPMci7IQ==

Select Cipher Mode of Decryption

ECB

Select Padding

PKCS5Padding

Key Size in Bits

128

Enter Secret Key used for Encryption

EMIKHPOS198765

Output Text Format

Plain-Text

Decrypt

AES Decrypted Output

You can't see the future if you don't take a risk

AES Encryption

Enter Plain Text to Encrypt

Kids who've never seen peace and kids who've never seen war have different values

Select Cipher Mode of Encryption

CBC

Select Padding

PKCS5Padding

Enter IV (Optional)

Enter initialization vector

Key Size in Bits

128

Enter Secret Key

EMIKHPOS098765

Output Text Format

Base64

Encrypt

AES Encrypted Output

MhJp20/SGnrXt59wAxShJE9w9j+HL6vOZv8ECu3z+ShryAnfNSSD6DF6oGUPwQnUJu
5ZVPVslmTY4u6LHfPdsAVG48auAqomOrOyDOvbnQLBEyTJUcETXt9iNR

AES Decryption

AES Encrypted Text

MhJp20/SGnrXt59wAxShJE9w9j+HL6vOZv8ECu3z+ShryAnfNSSD6DF6oGUPwQnUJu
5ZVPVslmTY4u6LHfPdsAVG48auAqomOrOyDOvbnQLBEyTJUcETXt9iNR

Select Cipher Mode of Decryption

CBC

Select Padding

PKCS5Padding

Enter IV Used During Encryption(Optional)

Enter initialization vector

Key Size in Bits

128

Enter Secret Key used for Encryption

EMIKHPOS098765

Output Text Format

Plain-Text

Decrypt

AES Decrypted Output

Kids who've never seen peace and kids who've never seen war have different values

AES Encryption

Enter Plain Text to Encrypt

A man dies when he's forgotten

Select Cipher Mode of Encryption

ECB

Select Padding

PKCS5Padding

Key Size in Bits

128

Enter Secret Key

EMIKHPOS#09876

Output Text Format

Base64

Encrypt

AES Encrypted Output

BeTK+PmXmqwez9UzYJwgoF+UzzB2WeB0vR78VEsDPA=

AES Decryption

AES Encrypted Text

BeTK+PmXmqwez9UzYJwgoF+UzzB2WeB0vR78VEsDPA=

Select Cipher Mode of Decryption

ECB

Select Padding

PKCS5Padding

Key Size in Bits

128

Enter Secret Key used for Encryption

EMIKHPOS#09876

Output Text Format

Plain-Text

Decrypt

AES Decrypted Output

A man dies when he's forgotten