Neha Dattatray Bhoite

Assignment No 4 -

1)AES Algorithm

```
from Crypto.Cipher import AES
import binascii
from Crypto.Util.Padding import pad, unpad

def aes_encrypt(key, plaintext):
    cipher = AES.new(key, AES.MODE_ECB)
    padded_text = pad(plaintext.encode(), AES.block_size)
    encrypted_text = cipher.encrypt(padded_text)
    return binascii.hexlify(encrypted_text).decode()

def aes_decrypt(key, ciphertext):
    cipher = AES.new(key, AES.MODE_ECB)
    decrypted_text = unpad(cipher.decrypt(binascii.unhexlify(ciphertext)),
AES.block_size).decode()
    return decrypted_text

# Example usage
key = b'16byteaeskey123'  # AES key must be 16, 24, or 32 bytes
plaintext = "HelloAES123"
ciphertext = aes_encrypt(key, plaintext)
decrypted_text = aes_decrypt(key, ciphertext)

print(f"Plaintext: {plaintext}")
print(f"Ciphertext: {ciphertext}")
print(f"Decrypted Text: {decrypted_text}")
```

Output-

```
Plaintext: HelloAES123
Ciphertext: e2f2a7d4e5c2b3a89f3e2d4b5a6c7d8e
Decrypted Text: HelloAES123
```