Neha Dattatray Bhoite

Assignment No 1-

1)DES Algorithm

```
from Crypto.Cipher import DES
import binascii

def pad(text):
    while len(text) % 8 != 0:
        text += ' '
    return text

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

def des_decrypt(key, ciphertext):
    cipher = DES.new(key, DES.MODE_ECB)
    decrypted_text = cipher.decrypt(binascii.unhexlify(ciphertext)).decode().rstrip()
    return decrypted_text

# Example usage
key = b'8bytekey'  # DES key must be exactly 8 bytes
plaintext = "Hello123"
ciphertext = des_encrypt(key, plaintext)
decrypted_text = des_decrypt(key, ciphertext)

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

Output-

```
Plaintext: Hello123
Ciphertext: 6d2bd91f9e0dbdef
Decrypted Text: Hello123
```