Practical.no - 2

Title - Implement Advanced Encryption Standard to encrypt and decrypt data.

```
from Crypto.Cipher import AES
from Crypto.Util.Padding import pad, unpad
from Crypto.Random import get_random_bytes
import base64
def encrypt(plaintext, key):
    cipher = AES.new(key, AES.MODE_ECB)
    padtext = pad(plaintext, AES.block_size)
    ctext = cipher.encrypt(padtext)
    encodedctext= base64.b64encode(ctext)
    return encodedctext
def decrypt(ciphertext, key):
    cipher = AES.new(key, AES.MODE_ECB)
    decodedctext = base64.b64decode(ciphertext)
    padded_plaintext = cipher.decrypt(decodedctext)
    plaintext = unpad(padded_plaintext, AES.block_size)
    return plaintext
key = get_random_bytes(16)
plaintext = input("Enter the plaintext: ").encode()
enc= encrypt(plaintext, key)
print("The encrypted data is:", enc)
decrypted = decrypt(enc, key)
print("The decrypted data is:", decrypted.decode('utf-8'))
```

Output -

```
Enter the plaintext: Hello World
The encrypted data is: b'0/AJNf6qPnTOO0vwFoEd0A=='
The decrypted data is: Hello World
```