CRYPTOGRAPHY AND COMPUTER NETWORKS

Name: NADDUNURI SANJAY

Hall Ticket: 2303A51LA4

Batch: 30

Assignment-6:

```
from cryptography.fernet import Fernet
import base64
import hashlib
def generate_key(secret: str) -> bytes:
    if not secret:
        raise ValueError("Secret key cannot be empty.")
    if len(secret) not in (16, 24, 32):
        raise ValueError("Secret key must be 16, 24, or 32 characters long.")
    hashed_key = hashlib.sha256(secret.encode()).digest()
    fernet_key = base64.urlsafe_b64encode(hashed_key)
    return fernet_key
def encrypt_message(key: bytes, plaintext: str) -> str:
    if not plaintext:
        raise ValueError("Plaintext message cannot be empty.")
    f = Fernet(key)
    ciphertext = f.encrypt(plaintext.encode())
    return ciphertext.decode()
def main():
    plaintext = input("Enter a plaintext message: ")
    secret = input("Enter a secret key (16, 24, or 32 characters): ")
    try:
        key = generate_key(secret)
        ciphertext = encrypt_message(key, plaintext)
        print("\n--- Encryption Result ---")
        print(f"Plaintext : {plaintext}")
        print(f"Ciphertext: {ciphertext}")
    except ValueError as e:
        print(f"Error: {e}")
if __name__ == "__main__":
    main()
```

OUTPUT:

```
Enter a plaintext message: varshu
Enter a secret key (16, 24, or 32 characters): mattepallivarshu

--- Encryption Result ---
Plaintext : varshu
Ciphertext: gAAAAABowAWvw1TTucu1xeQDEJA8E9EJ51LXl5ZPJ1pL7EM0PMy5Cxn61Tf1gE7FhJvvS-olHJxA0JDZa7UPhGM5j-qU__hqA==
```