1 Challenge 1: Two-Time Pad

1.1 Problem Understanding

This problem requires us to find the flag using the 2 given cipher texts, which are of the flag and a normal english sentence, also we know that the encryption algorithm is XOR

1.2 Given Data

- `ciphertext1.enc`
- `ciphertext2.enc`
- `encrypt.py`

1.3 Approach

- Using the cipher texts, if we XOR them, we will get s = m1 $\oplus$ m2
- Now using the fact that we know the starting few characters of the flag, (i.e., cs409{) we can XOR this with the starting 6 characters of s to get the first 6 characters of the message.
- Now using this, if we have any incomplete words, we can check and round it down to one word considering the fact that both the message and flag consist of meaningful words and symbols.
- So, using this method recursively to find a few characters of the message and then complete any incomplete words and then mapping this to the flag and so on, we can achieve our goal

1.4 Outputs and Flag

```
b'Crypta'
b'cs409{one_time'
b'Cryptanalysis freq'
b'cs409{one_time_pad_key_re'
b'Cryptanalysis frequently invo'
b'cs409{one_time_pad_key_reuse_compr'
b'Cryptanalysis frequently involves statistical att'
b'cs409{one_time_pad_key_reuse_compromises_security!!!'
b'Cryptanalysis frequently involves statistical attacks'

Flag: cs409{one_time_pad_key_reuse_compromises_security!!!}
```

1.5 Implementation

Listing 1: Python script to solve Challenge 1

```python
from Crypto.Util.strxor import strxor
from Crypto.Random import get_random_bytes

with open("ciphertext1.enc", "rb") as f:
    Cipher_Flag = f.read()
with open("ciphertext2.enc", "rb") as f:
    Cipher_Message = f.read()

M1_XOR_M2 = strxor(Cipher_Flag, Cipher_Message)
def Helper(a):
    n = len(a)
    extra = b"0"*(l - n)
    var = a + extra
    print(strxor(var, M1_XOR_M2)[0:n])

l = 53 # This is the length of the flag and message
flag = b"cs409{"
n = len(flag)
extra = b"0"*(l - n)
flag = flag + extra
print(strxor(flag, M1_XOR_M2)[0:n])

# Here we get that the first 6 characters of the MSG are: Crypta
# The possible words relevant are: Cryptanalysis, Cryptanalytic, Cryptanalyst
# So, lets assume that the first few characters of the message are: " Cryptanalysis "
message = b"Crypta" + b"nalysis "
n = len(message)
extra = b"0"*(l - n)
message = message + extra
print(strxor(M1_XOR_M2, message)[0:n])

flag = b"cs409{one_time_pad"
Helper(flag)

message = b"Cryptanalysis frequently "
Helper(message)

flag = b"cs409{one_time_pad_key_reuse_"
Helper(flag)

message = b"Cryptanalysis frequently involves "
Helper(message)

flag = b"cs409{one_time_pad_key_reuse_compromises_security"
Helper(flag)

message = b"Cryptanalysis frequently involves statistical attack"
Helper(message)

flag = b"cs409{one_time_pad_key_reuse_compromises_security!!!}"
Helper(flag)
# Message: "Cryptanalysis frequently involves statistical attacks"
```