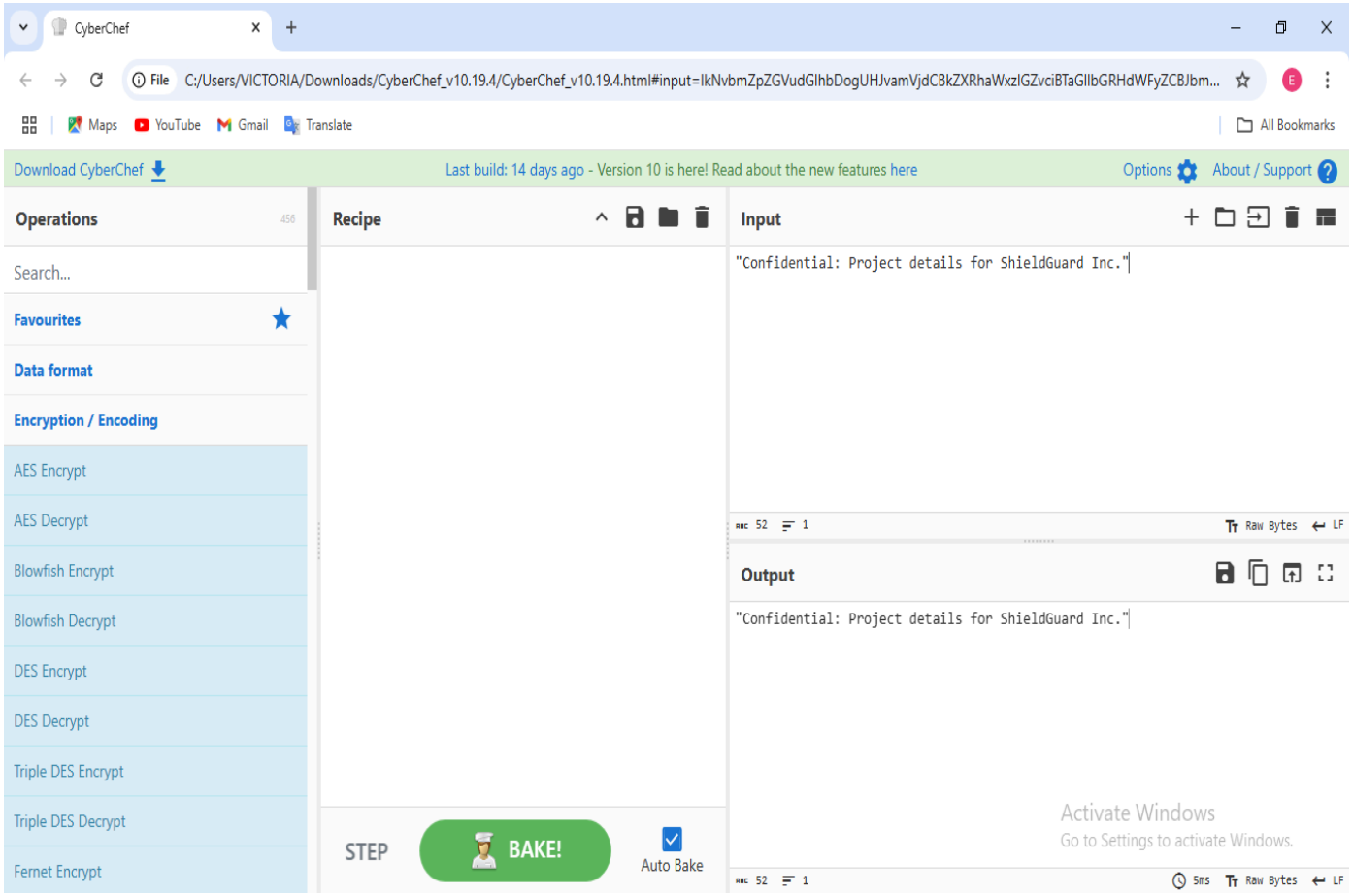
## Demonstration Of The Process Of Encrypting and Decrypting of Message Using CyberChef

### Introduction
I accessed the CyberChef website through the link provided on this project.

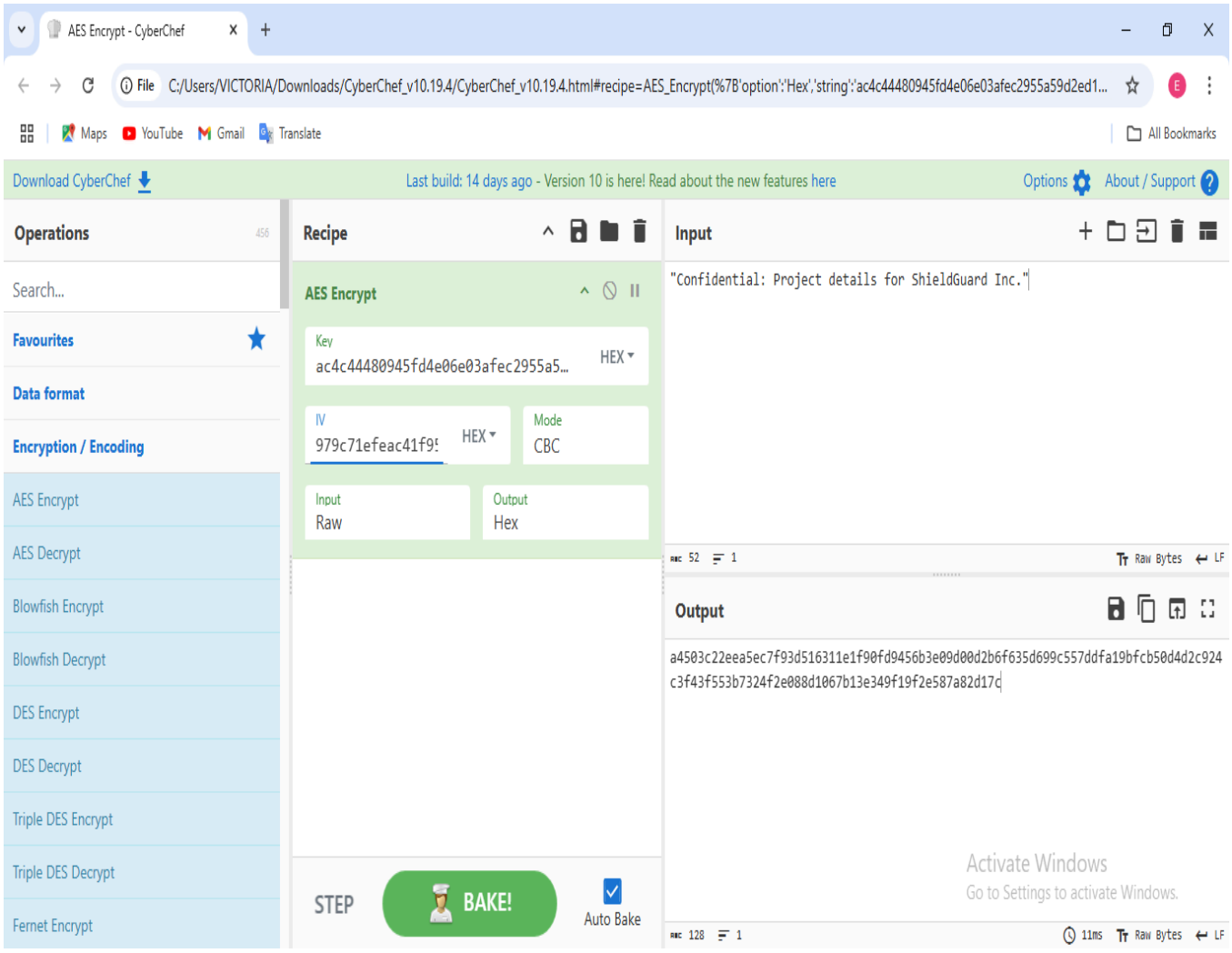
### Plaintext Message:
"Confidential: Project details for ShieldGuard Inc."




### Encryption Algorithm
I made use of AES(Advanced Encryption Standard).

### Encryption parameter used:
**Key:** ac4c44480945fd4e06e03afec2955a59d2ed156bb4dadcf0473c07239ef58d4a
**IV:** 979c71efeac41f952bb6892262fd0efb
**Block mode:** CBC

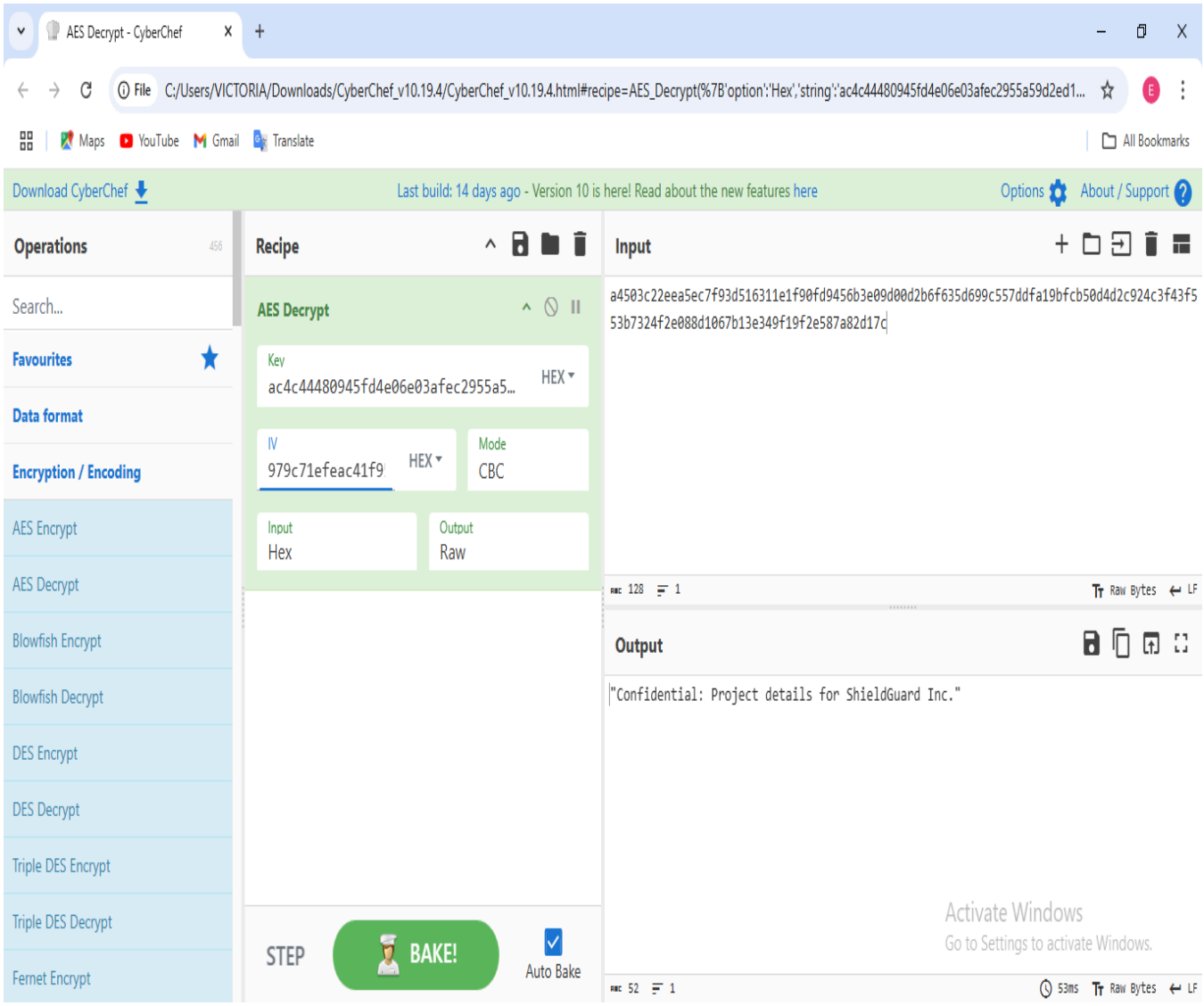
### Message Encryption
I encrypt the message using CyberChef.




**Secure key:** ac4c44480945fd4e06e03afec2955a59d2ed156bb4dadcf0473c07239ef58d4a
**Ciphertext:**
a4503c22eea5ec7f93d516311e1f90fd9456b3e09d00d2b6f635d699c557ddfa19bfcb50d4d2c924
c3f43f553b7324f2e088d1067b13e349f19f2e587a82d17c

**Sharing of Ciphertext and Key:**
This is by securely storing and transmitting the key alongside the ciphertext.

**Decryption**
I used CyberChef to decrypt the Ciphertext using the same key
The decrypted output matches the original plaintext.




**Record Observation**

The challenge is that one can easily omit a letter from the KEY or IV which can alter the whole encryption and decryption process.

**Importance of Key Management**

Key management is crucial in cryptography because it ensures the secure handling of encryption keys, which are essential for protecting sensitive data. Proper key management involves generating, storing, distributing, and destroying keys securely to prevent unauthorized access and maintain data integrity.