

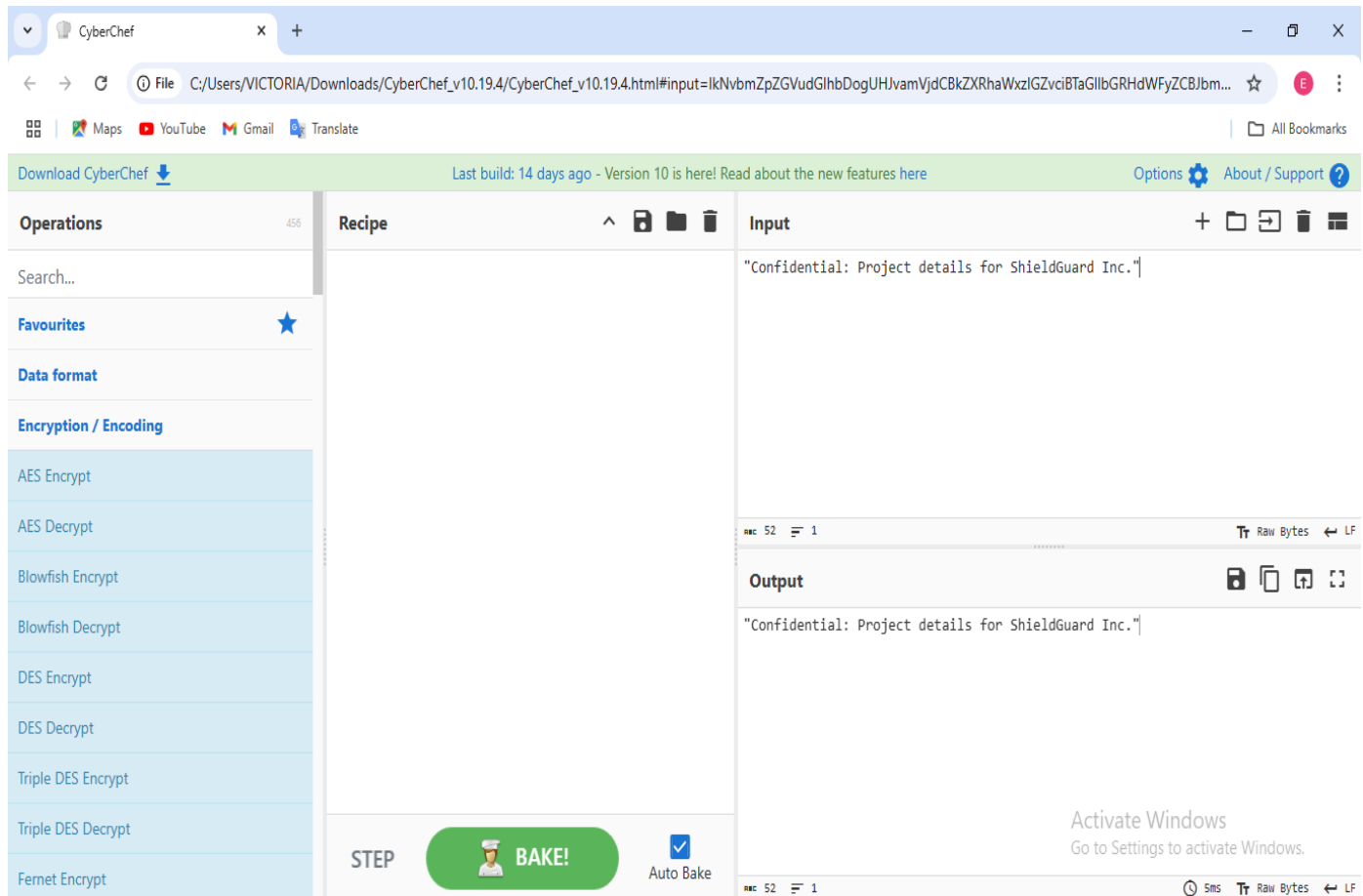
Demonstration Of The Process Of Encrypting and Decrypting of Message Using CyberChef

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: 979c71efead41f952bb6892262fd0efb

Block mode: CBC

Message Encryption

I encrypt the message using CyberChef.

The screenshot shows the CyberChef web application interface. The browser address bar indicates the URL: `C:/Users/VICTORIA/Downloads/CyberChef_v10.19.4/CyberChef_v10.19.4.html#recipe=AES_Encrypt(%7B'option':'Hex','string':'ac4c44480945fd4e06e03afec2955a59d2ed1...`. The interface is divided into several sections:

- Operations:** A sidebar on the left with a search bar and a list of operations including AES Encrypt, AES Decrypt, Blowfish Encrypt, Blowfish Decrypt, DES Encrypt, DES Decrypt, Triple DES Encrypt, Triple DES Decrypt, and Fernet Encrypt.
- Recipe:** The central area showing the selected 'AES Encrypt' operation. It includes fields for 'Key' (set to `ac4c44480945fd4e06e03afec2955a5...`), 'IV' (set to `979c71efeac41f9!`), and 'Mode' (set to 'CBC'). There are also 'Input' (Raw) and 'Output' (Hex) dropdowns.
- Input:** The rightmost section showing the input text: `"Confidential: Project details for ShieldGuard Inc."`.
- Output:** The bottom right section showing the resulting ciphertext: `a4503c22eea5ec7f93d516311e1f90fd9456b3e09d00d2b6f635d699c557ddfa19bfc50d4d2c924c3f43f553b7324f2e088d1067b13e349f19f2e587a82d17c`.
- Footer:** A 'STEP' indicator with a 'BAKE!' button and an 'Auto Bake' checkbox.

Secure key: `ac4c44480945fd4e06e03afec2955a59d2ed156bb4dadcf0473c07239ef58d4a`

Ciphertext:

`a4503c22eea5ec7f93d516311e1f90fd9456b3e09d00d2b6f635d699c557ddfa19bfc50d4d2c924c3f43f553b7324f2e088d1067b13e349f19f2e587a82d17c`

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.

The screenshot shows the CyberChef web application in a browser. The address bar indicates the URL: `C:/Users/VICTORIA/Downloads/CyberChef_v10.19.4/CyberChef_v10.19.4.html#recipe=AES_Decrypt(%7B'option':'Hex','string':'ac4c44480945fd4e06e03afec2955a59d2ed1...`

The interface is divided into several sections:

- Operations:** A sidebar on the left with a search bar and a list of operations including AES Encrypt, AES Decrypt, Blowfish Encrypt, Blowfish Decrypt, DES Encrypt, DES Decrypt, Triple DES Encrypt, Triple DES Decrypt, and Fernet Encrypt.
- Recipe:** The central panel shows the 'AES Decrypt' recipe selected. It includes input fields for:
 - Key:** `ac4c44480945fd4e06e03afec2955a5...` (HEX)
 - IV:** `979c71efeac41f9` (HEX)
 - Mode:** `CBC`
 - Input:** `Hex`
 - Output:** `Raw`
- Input:** The top right panel contains a long hexadecimal string: `a4503c22eea5ec7f93d516311e1f90fd9456b3e09d00d2b6f635d699c557ddfa19bfc50d4d2c924c3f43f553b7324f2e088d1067b13e349f19f2e587a82d17c`
- Output:** The bottom right panel displays the decrypted result: `"Confidential: Project details for ShieldGuard Inc."`

At the bottom of the Recipe panel, there is a 'STEP' indicator, a 'BAKE!' button with a chef icon, and an 'Auto Bake' checkbox which is checked.

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.