Assignment 1: Exploring Cybersecurity Tools for AES Encryption and Decryption

Chaitanya Bharathi Institute of Technology
Department of Information Technology
Class: V Semester IT1
Name: D Chandana
Roll No: 160123737012

Abstract

This assignment explores the use of AES encryption and decryption using two tools: Google Colab (Python implementation) and CyberChef (web-based tool). The problem addressed is secure text and file-level encryption, which is a crucial requirement in cybersecurity for ensuring confidentiality of data during storage and transmission.

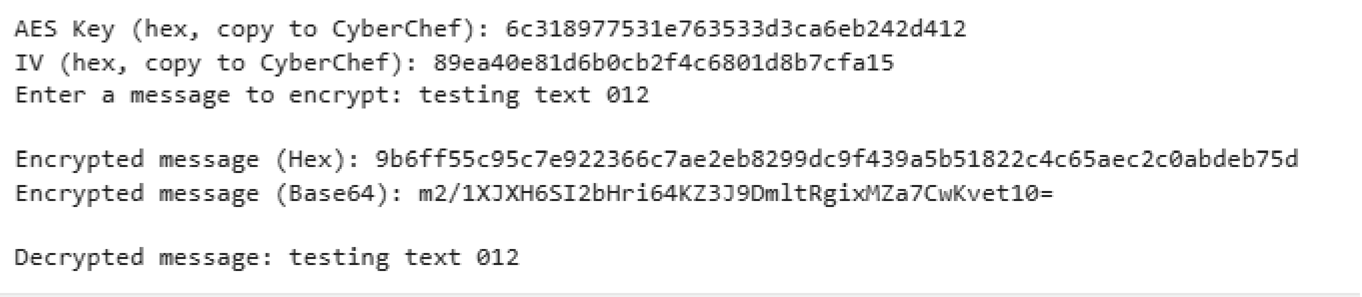
The solution involves implementing AES-256-CBC encryption in Colab for both text and files, exporting the encrypted data, and then cross-verifying decryption results in CyberChef using the same key and IV values. This demonstrates interoperability between coding-based implementations and professional cryptographic tools.

Problem Addressed

The main challenge is to securely encrypt and decrypt sensitive text and files, while ensuring compatibility across different environments. Many real-world cybersecurity scenarios demand that data encrypted in one platform should be correctly decrypted in another, making this an important use case for secure communication and digital forensics.

Results and Demonstration

1. Text Encryption and Decryption in Colab

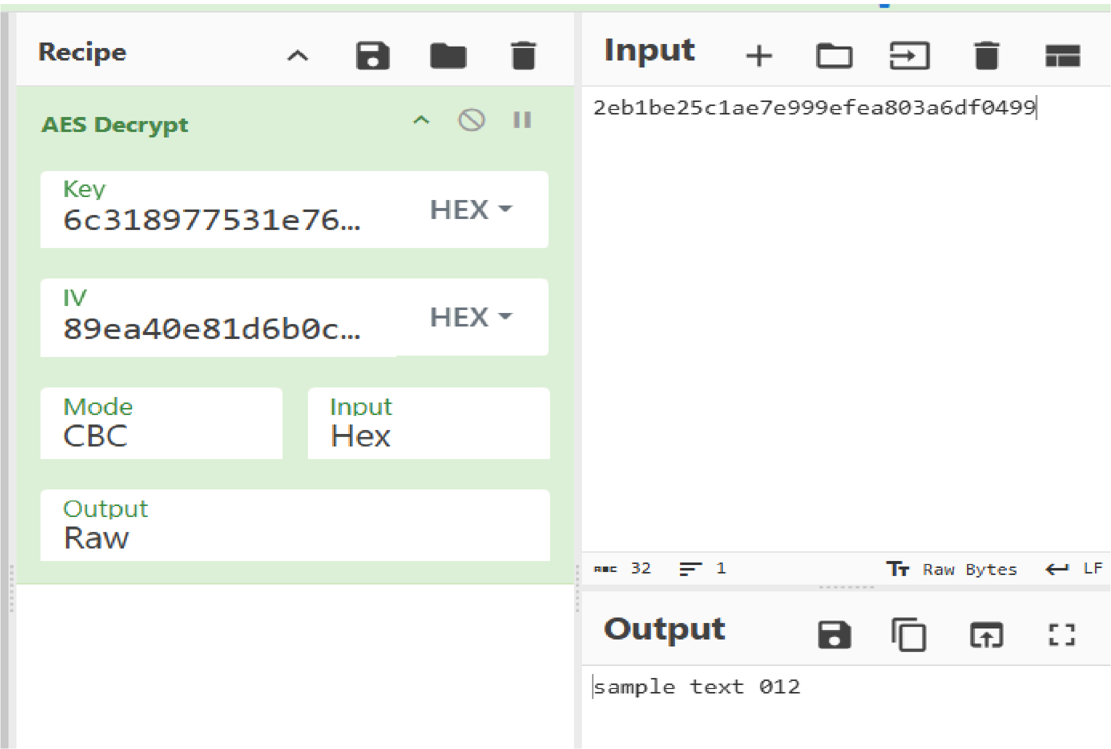


```
AES Key (hex, copy to CyberChef): 6c318977531e763533d3ca6eb242d412
IV (hex, copy to CyberChef): 89ea40e81d6b0cb2f4c6801d8b7cfa15
Enter a message to encrypt: testing text 012

Encrypted message (Hex): 9b6ff55c95c7e922366c7ae2eb8299dc9f439a5b51822c4c65aec2c0abdeb75d
Encrypted message (Base64): m2/1XJXH6SI2bHri64KZ3J9DmltRgixMZa7CwKvet10=

Decrypted message: testing text 012
```

2. Text Decryption in CyberChef



Key 6c318977531e76... HEX

IV 89ea40e81d6b0c... HEX

Mode CBC

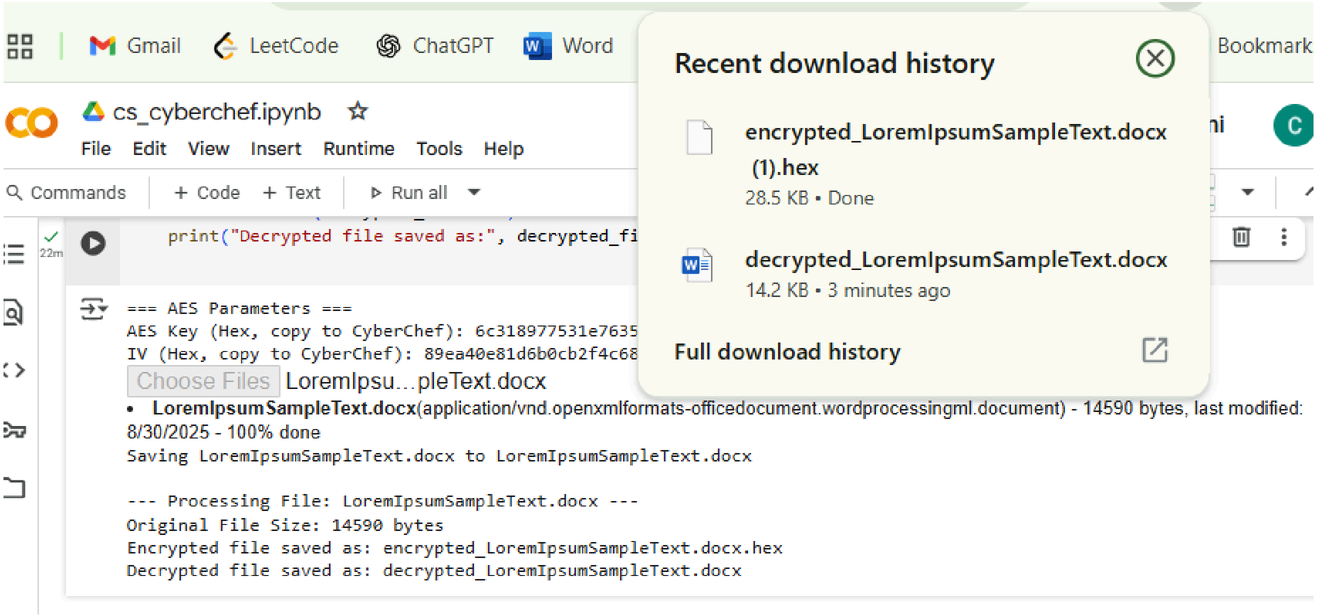
Input Hex

Output Raw

```
2eb1be25c1ae7e999efea803a6df0499
```

```
sample text 012
```

3. File Encryption and Decryption in Colab



encrypted_LoremIpsumSampleText.docx (1).hex
28.5 KB • Done

decrypted_LoremIpsumSampleText.docx
14.2 KB • 3 minutes ago

```
print("Decrypted file saved as:", decrypted_fi
```

```
=== AES Parameters ===
AES Key (Hex, copy to CyberChef): 6c318977531e7635
IV (Hex, copy to CyberChef): 89ea40e81d6b0cb2f4c68
Choose Files LoremIpsu...pleText.docx
• LoremIpsumSampleText.docx(application/vnd.openxmlformats-officedocument.wordprocessingml.document) - 14590 bytes, last modified: 8/30/2025 - 100% done
Saving LoremIpsumSampleText.docx to LoremIpsumSampleText.docx

--- Processing File: LoremIpsumSampleText.docx ---
Original File Size: 14590 bytes
Encrypted file saved as: encrypted_LoremIpsumSampleText.docx.hex
Decrypted file saved as: decrypted_LoremIpsumSampleText.docx
```

Conclusion

The experiment demonstrates that AES-256-CBC encryption performed in Google Colab can be successfully decrypted in CyberChef by using the correct key and IV. This validates the compatibility and reliability of AES as a secure encryption method. The solution highlights how cybersecurity professionals can integrate coding platforms with cryptographic tools for secure data handling in practical applications.