МІНІСТЕРСТВО ОБОРОНИ УКРАЇНИ

ВІЙСЬКОВИЙ ІНСТИТУТ ТЕЛЕКОМУНІКАЦІЙ ТА ІНФОРМАТИЗАЦІЇ

КАФЕДРА КІБЕРЗАХИСТУ

**ЗВІТ**

про виконання практичної роботи:

з дисципліни «Прикладна криптологія»

**Тема № 2**. Електронна комунікаційна мережа об’єкта кіберзахисту як джерело ознак кіберінциденту.

**Заняття № 3/18**. Реалізація алгоритму шифрування DES

**РОБОТА З WEB-ДОДАТКОМ CYBERCHEF.IO**

**Виконав:** курсант навчальної групи 314

солдат \_\_\_\_\_\_\_\_\_\_\_\_\_ ФЕДОРЯКА В.О

21.04.2024

**Перевiрив:** викладач кафедри № 33

капітан \_\_\_\_\_\_\_\_\_\_\_\_Прийма О.О.

Київ – 2024

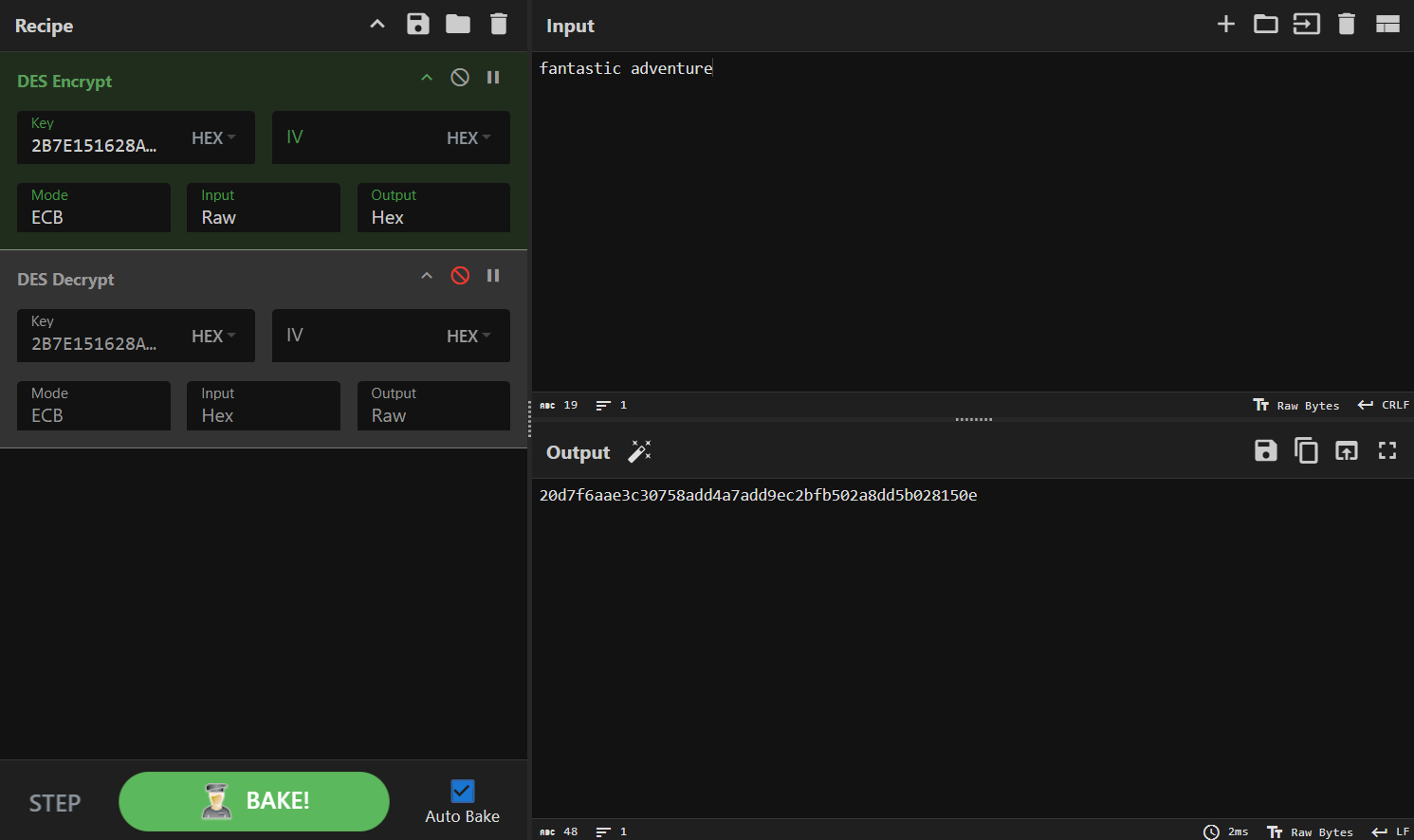
1. Виконати цикл шифрування алгоритмом DES у режимі ECB

Дані шифрування:

Ключ - 2B7E151628AED2A6 в HEX форматі.

Відкритий текст – [fantastic adventure](https://github.com/Phant0m-2604/fantastic-adventure)

Шифротекст - 20d7f6aae3c30758add4a7add9ec2bfb502a8dd5b028150e в HEX форматі.

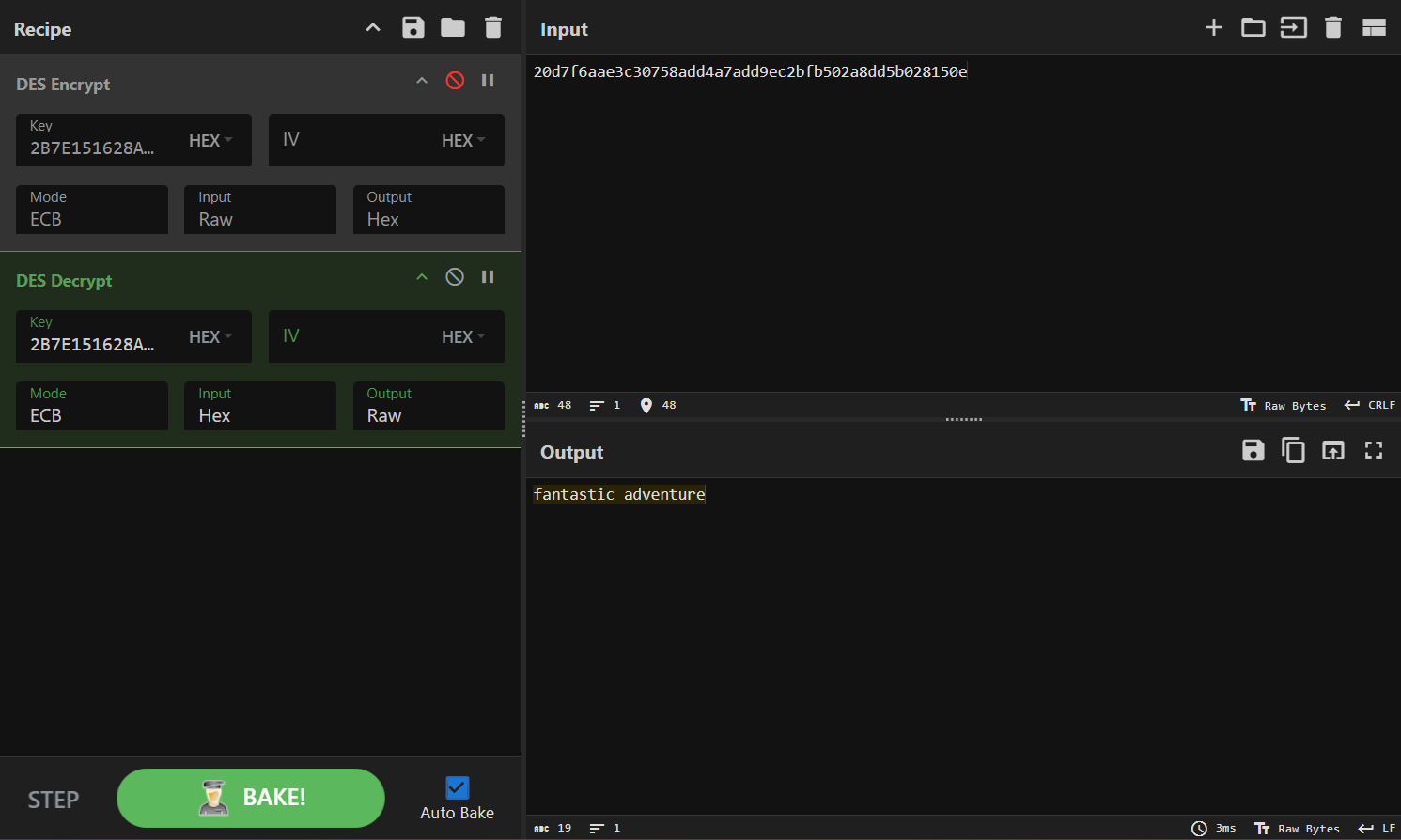


Дані розшифрування:

Ключ - 2B7E151628AED2A6 в HEX форматі.

Шифротекст - 20d7f6aae3c30758add4a7add9ec2bfb502a8dd5b028150e

Відкритий текст - [fantastic adventure](https://github.com/Phant0m-2604/fantastic-adventure)



1. Виконати цикл шифрування алгоритмом DES у режимі CBC

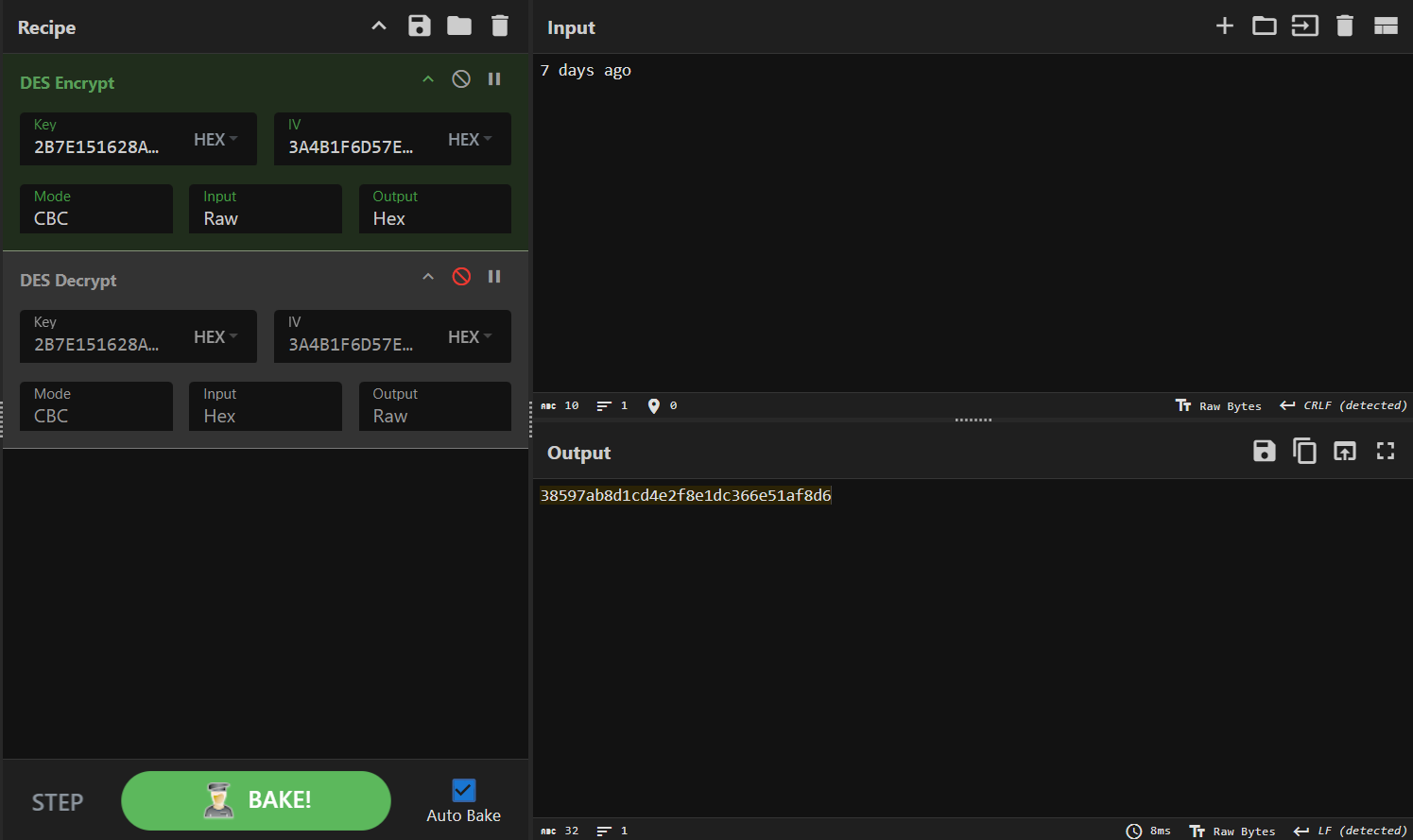
Дані шифрування:

Ключ - 2B7E151628AED2A6 в HEX форматі.

Вектор ініціалізації (IV) - 3A4B1F6D57E92C8F в HEX форматі.

Відкритий текст – 7 days ago

Шифротекст - 38597ab8d1cd4e2f8e1dc366e51af8d6 в HEX форматі.



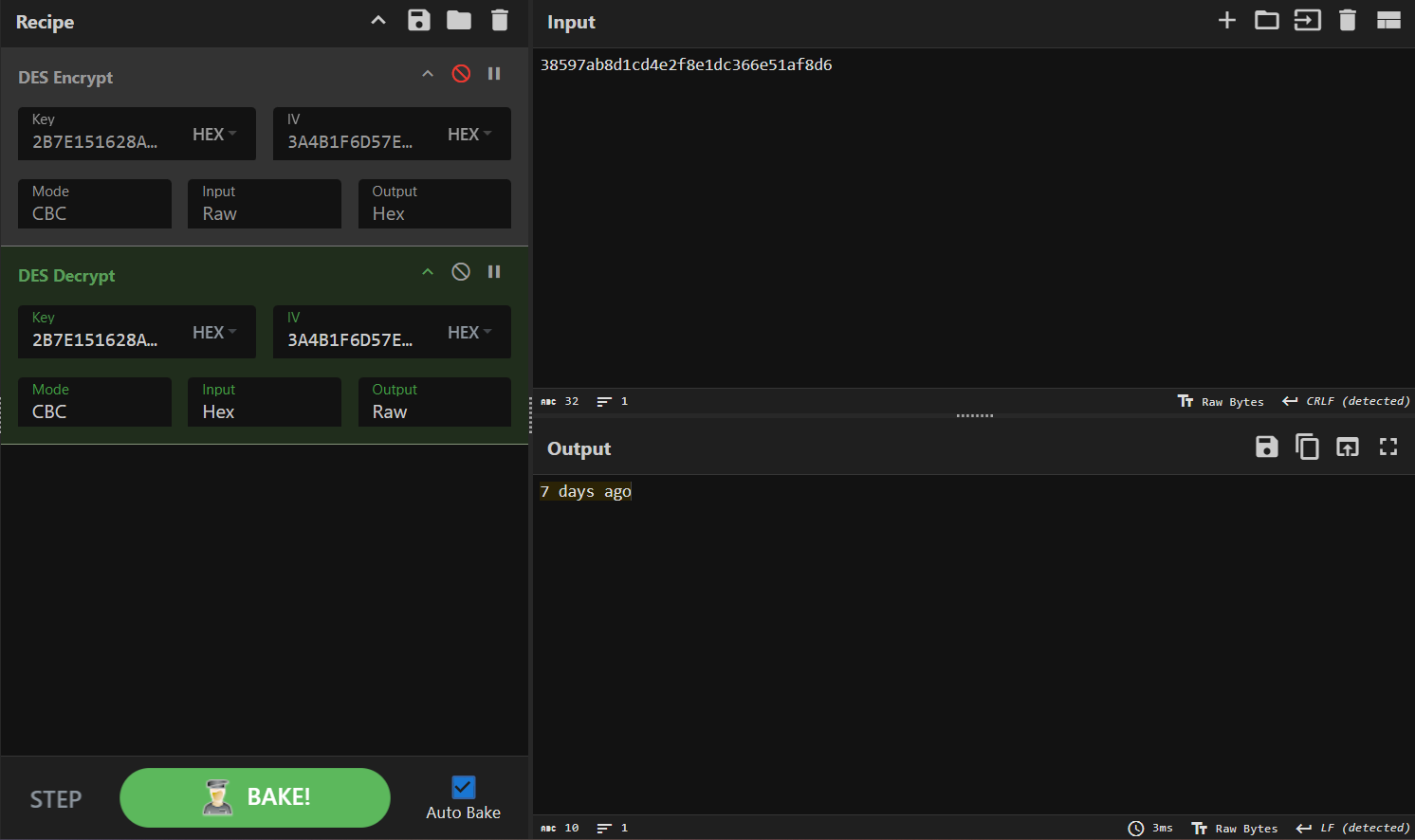
Дані розшифрування:

Ключ - 2B7E151628AED2A6 в HEX форматі.

Вектор ініціалізації (IV) - 3A4B1F6D57E92C8F в HEX форматі.

Шифротекст - 38597ab8d1cd4e2f8e1dc366e51af8d6 в HEX форматі.

Відкритий текст - 7 days ago



1. Виконати цикл шифрування алгоритмом DES у режимі CFB

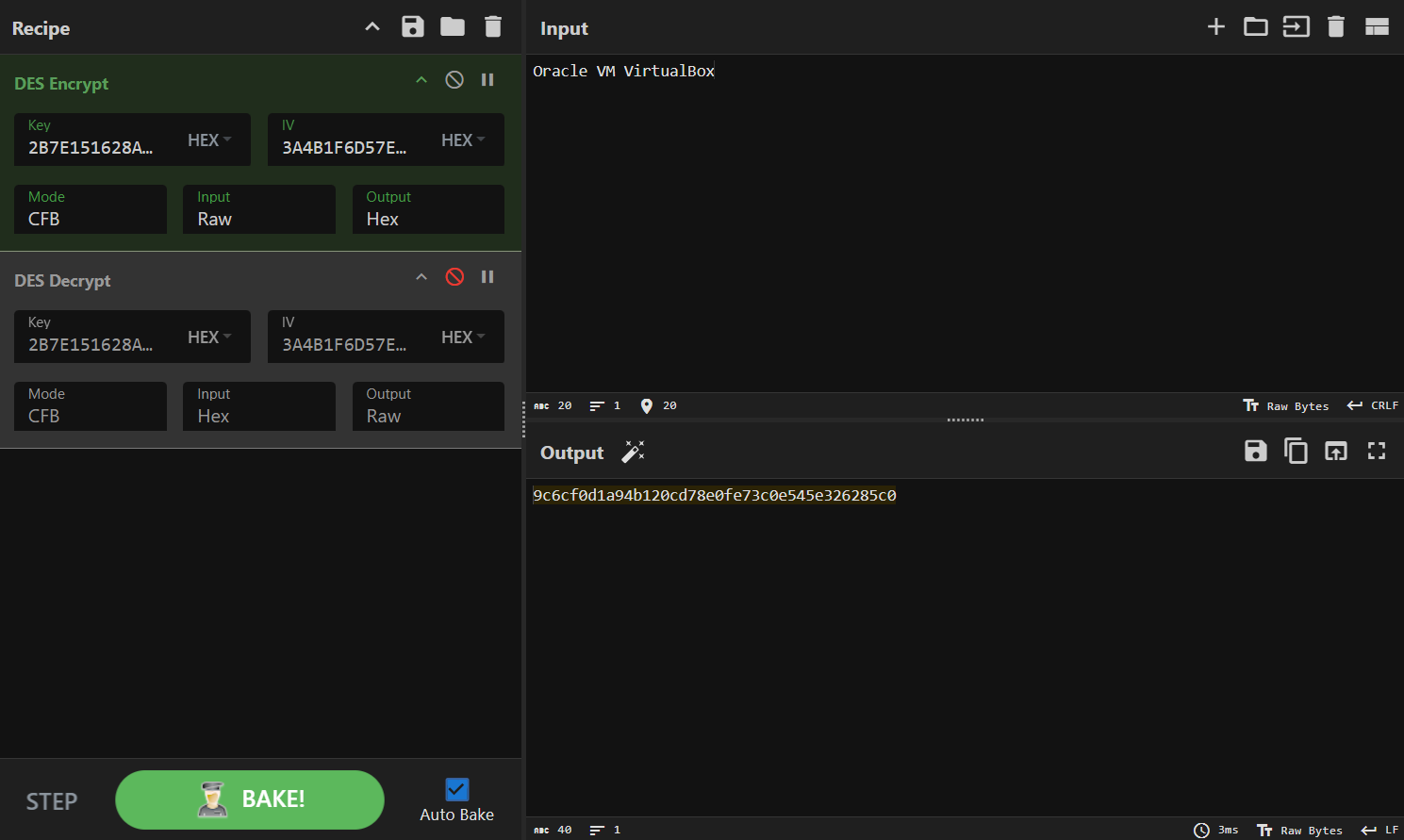
Дані шифрування:

Ключ - 2B7E151628AED2A6 в HEX форматі.

Вектор ініціалізації (IV) - 3A4B1F6D57E92C8F в HEX форматі.

Відкритий текст - Oracle VM VirtualBox

Шифротекст - 9c6cf0d1a94b120cd78e0fe73c0e545e326285c0 в HEX форматі.



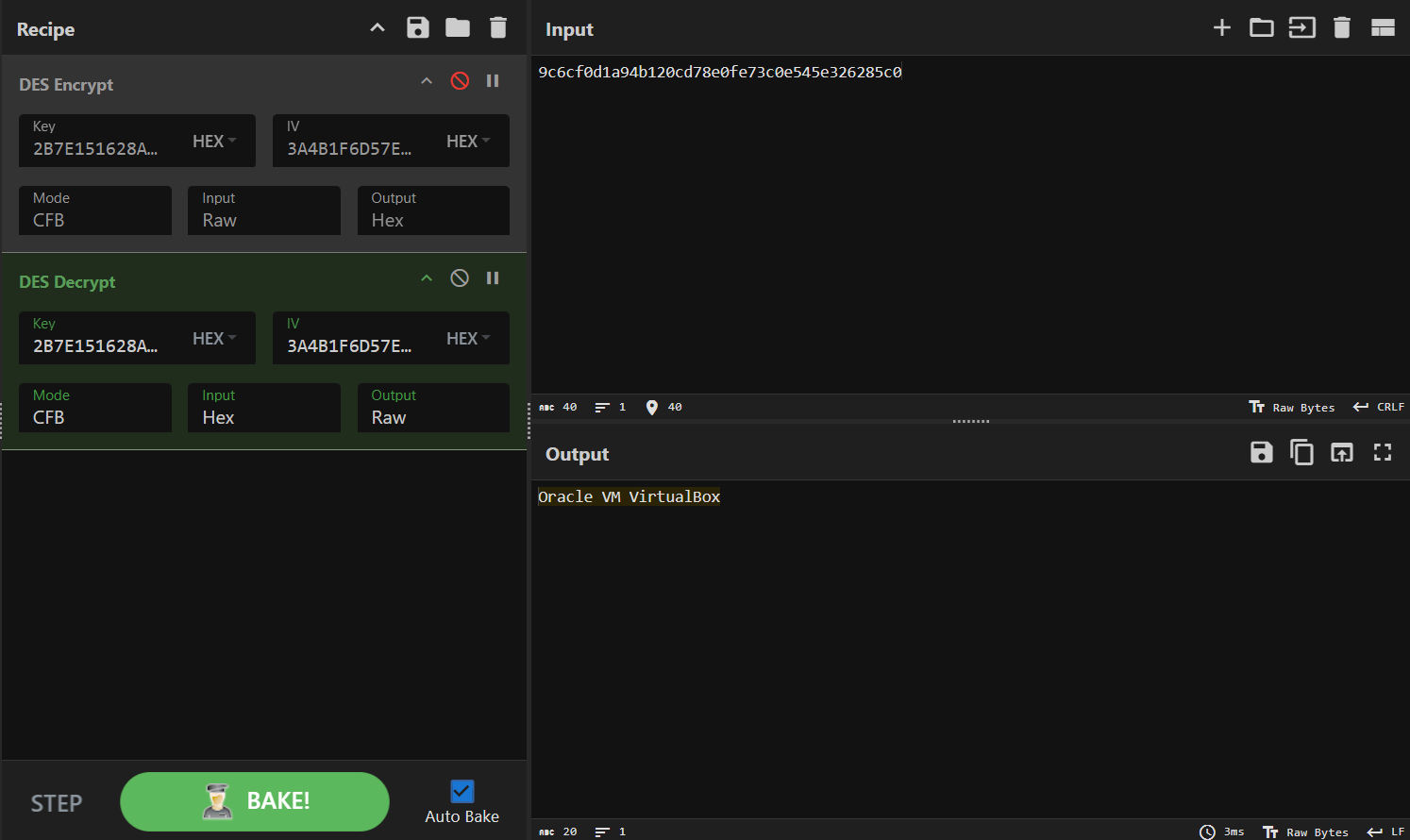
Дані розшифрування:

Ключ - 2B7E151628AED2A6 в HEX форматі.

Вектор ініціалізації (IV) - 3A4B1F6D57E92C8F в HEX форматі.

Шифротекст - 9c6cf0d1a94b120cd78e0fe73c0e545e326285c0 в HEX форматі.

Відкритий текст - Oracle VM VirtualBox



**Висновок:**

Після проведення експериментів з DES у режимах CFB, CBC та ECB, я зробив кілька висновків:

1. **ECB**:
   * Цей режим простий у реалізації та розумінні, але не забезпечує високого рівня безпеки.
   * Дані, які мають однакове значення, під час шифрування у тому ж самому блоку, отримують однаковий шифротекст, що може викликати проблеми з конфіденційністю.
2. **CBC**:
   * Режим CBC використовує попередній блок шифротексту для шифрування наступного блоку, що робить його стійким до атак на патерни та підсаджування даних.
   * Він забезпечує високий рівень конфіденційності, оскільки навіть однакові блоки даних будуть мати різний шифротекст.
3. **CFB**:
   * У режимі CFB кожен блок шифрується, а потім використовується для шифрування наступного блоку даних.
   * Він дозволяє передавати блоки будь-якого розміру, що може бути корисним у певних сценаріях.

Загалом, режими CBC і CFB забезпечують вищий рівень безпеки порівняно з ECB, оскільки вони уникнуть багатьох проблем, пов'язаних з патернами у шифрованому тексті та можливістю атак. Режим CBC, зокрема, виявився найбільш ефективним для забезпечення конфіденційності даних.