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

молодший сержант \_\_\_\_\_\_І.КОСТЕНКО

21.04.2024

**Перевiрив:** викладач кафедри № 33

капітан \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_О.ПРИЙМА

Київ – 2024

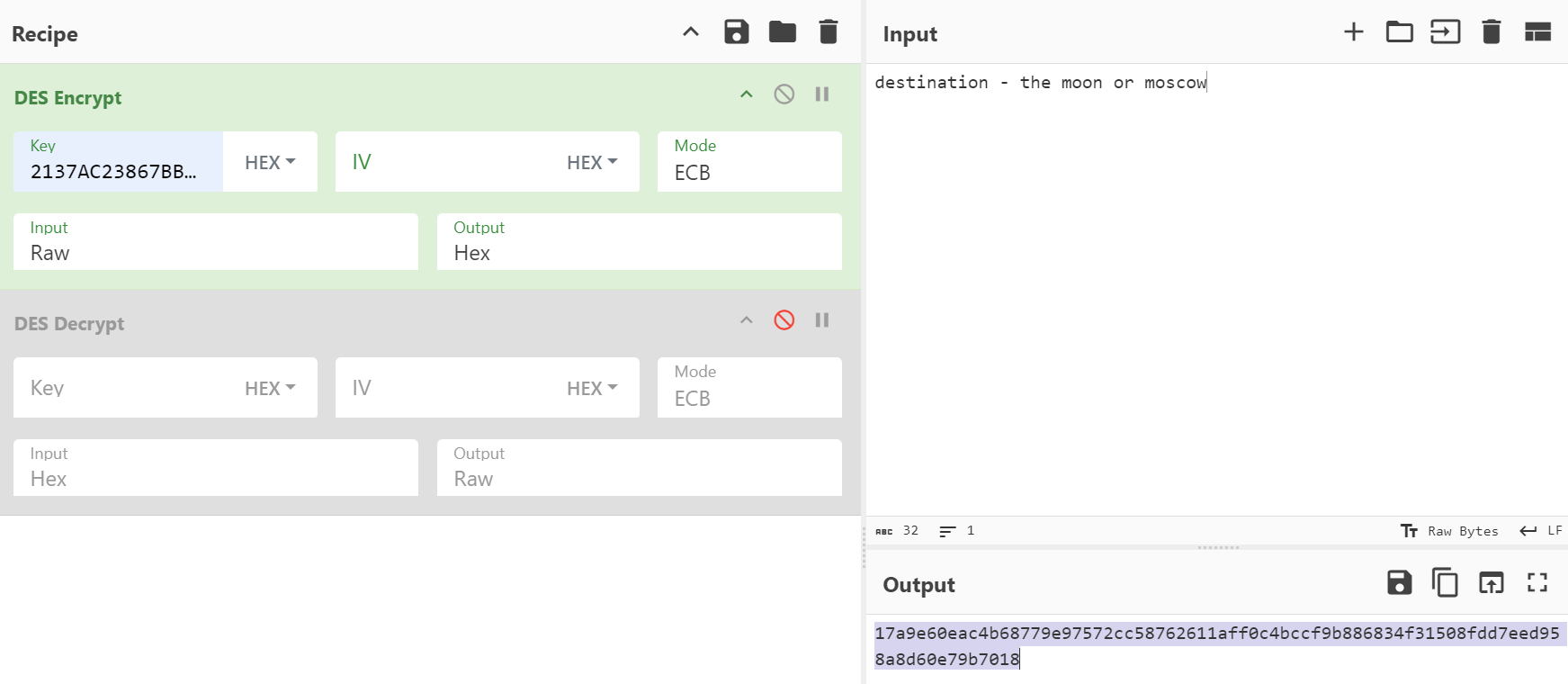
1. Шифрування алгоритмом DES у режимі ECB

Дані шифрування:

Ключ - 7232688AC2082133 (HEX format)

Відкритий текст – “destination - the moon or moscow”

Шифротекст “654095acaaf0774ff34d22dfde80b52db5fc156d6a562cb32cdee64a1faebbe2f585e2512d4058c0”

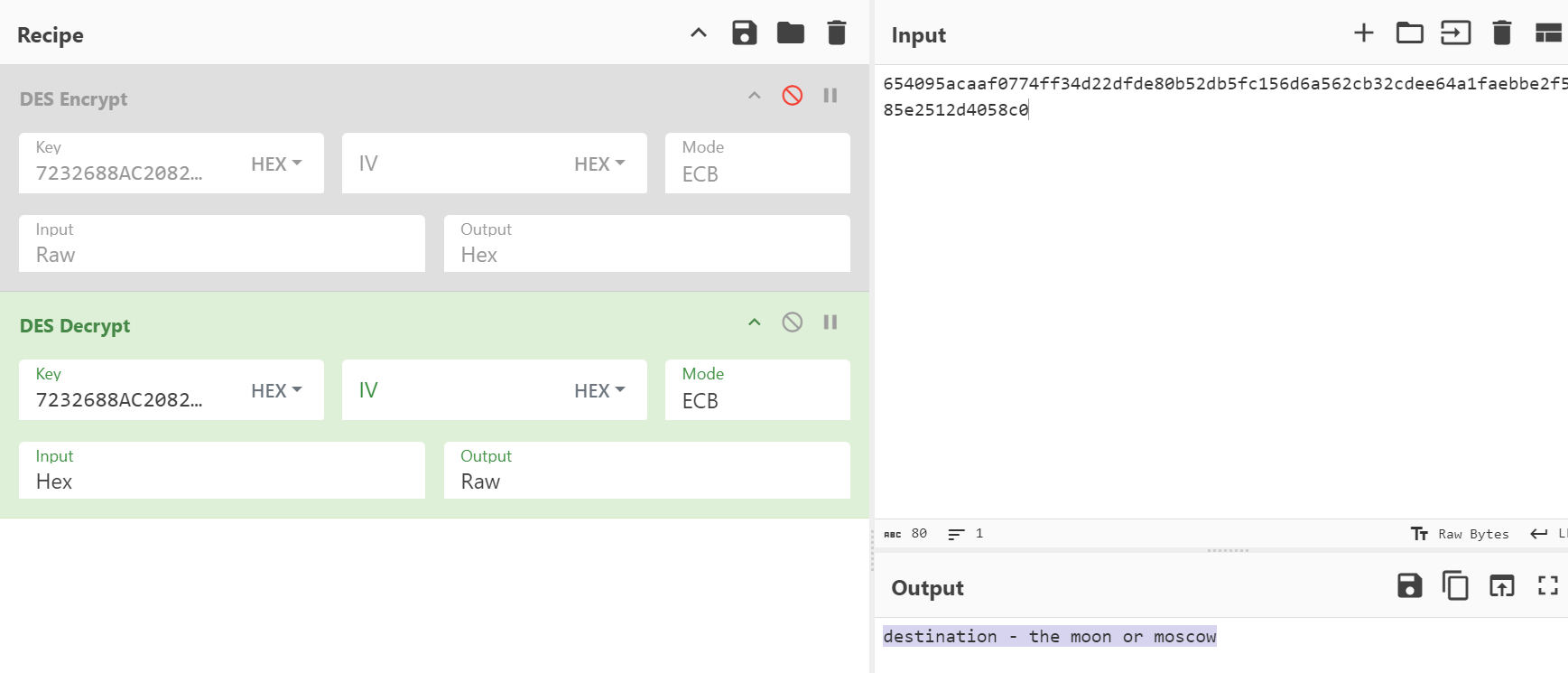


Дані розшифрування:

Ключ - 7232688AC2082133 (HEX format)

Шифротекст “654095acaaf0774ff34d22dfde80b52db5fc156d6a562cb32cdee64a1faebbe2f585e2512d4058c0”

Відкритий текст – “destination - the moon or moscow”



1. Шифрування алгоритмом DES у режимі CBC

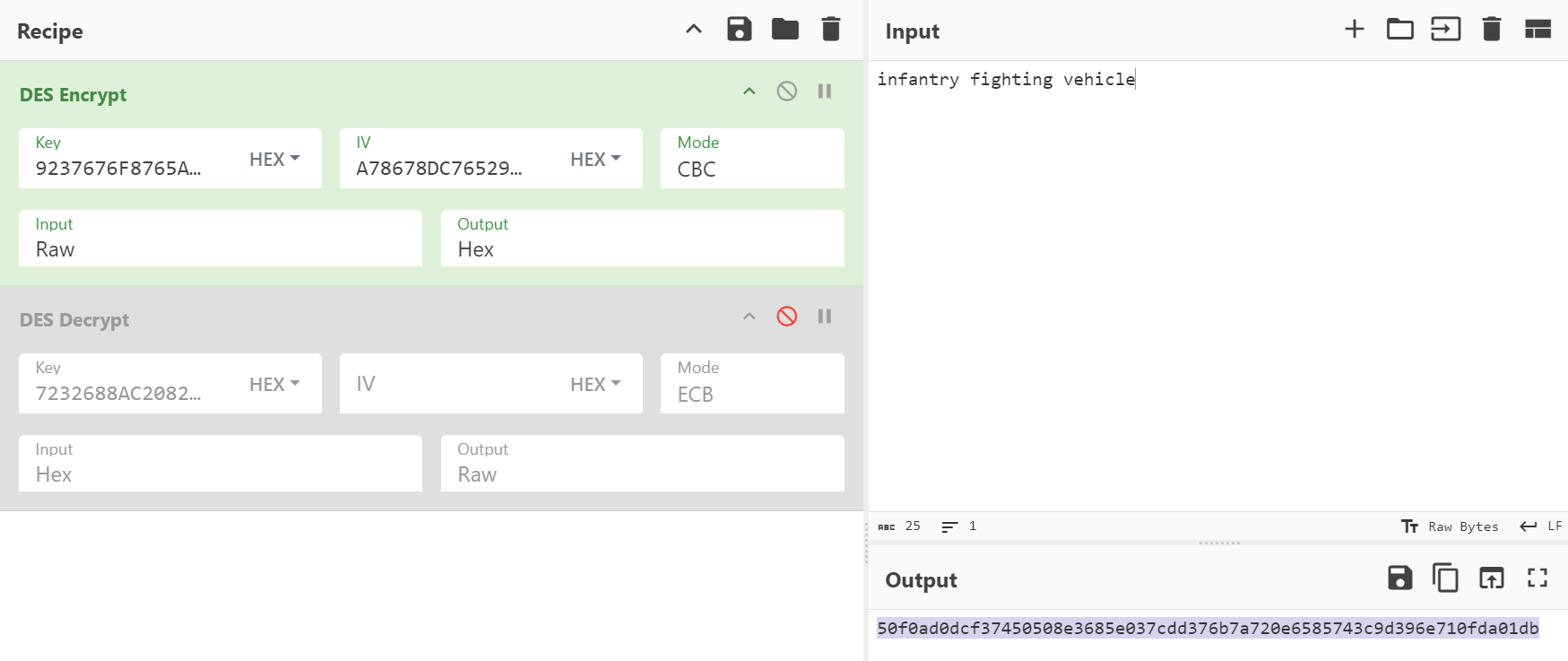
Дані шифрування:

Ключ - 9237676F8765AC6 (HEX format)

Вектор ініціалізації (IV) - A78678DC7652917(HEX format)

Відкритий текст – “infantry fighting vehicle”

Шифротекст “50f0ad0dcf37450508e3685e037cdd376b7a720e6585743c9d396e710fda01db”



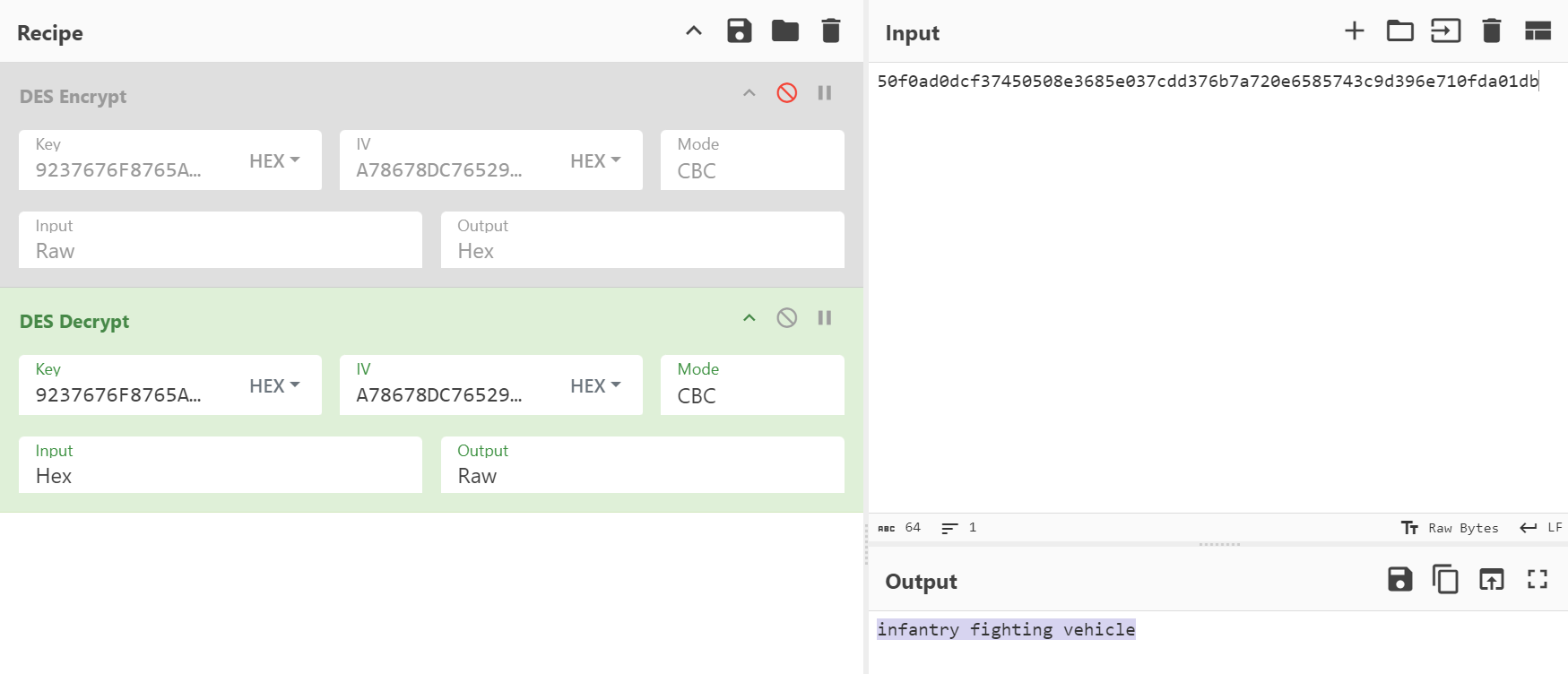
Дані розшифрування:

Ключ - 9237676F8765AC6 (HEX format)

Вектор ініціалізації (IV) - A78678DC7652917(HEX format)

Шифротекст “50f0ad0dcf37450508e3685e037cdd376b7a720e6585743c9d396e710fda01db”

Відкритий текст - “infantry fighting vehicle”



1. Шифрування алгоритмом DES у режимі CFB

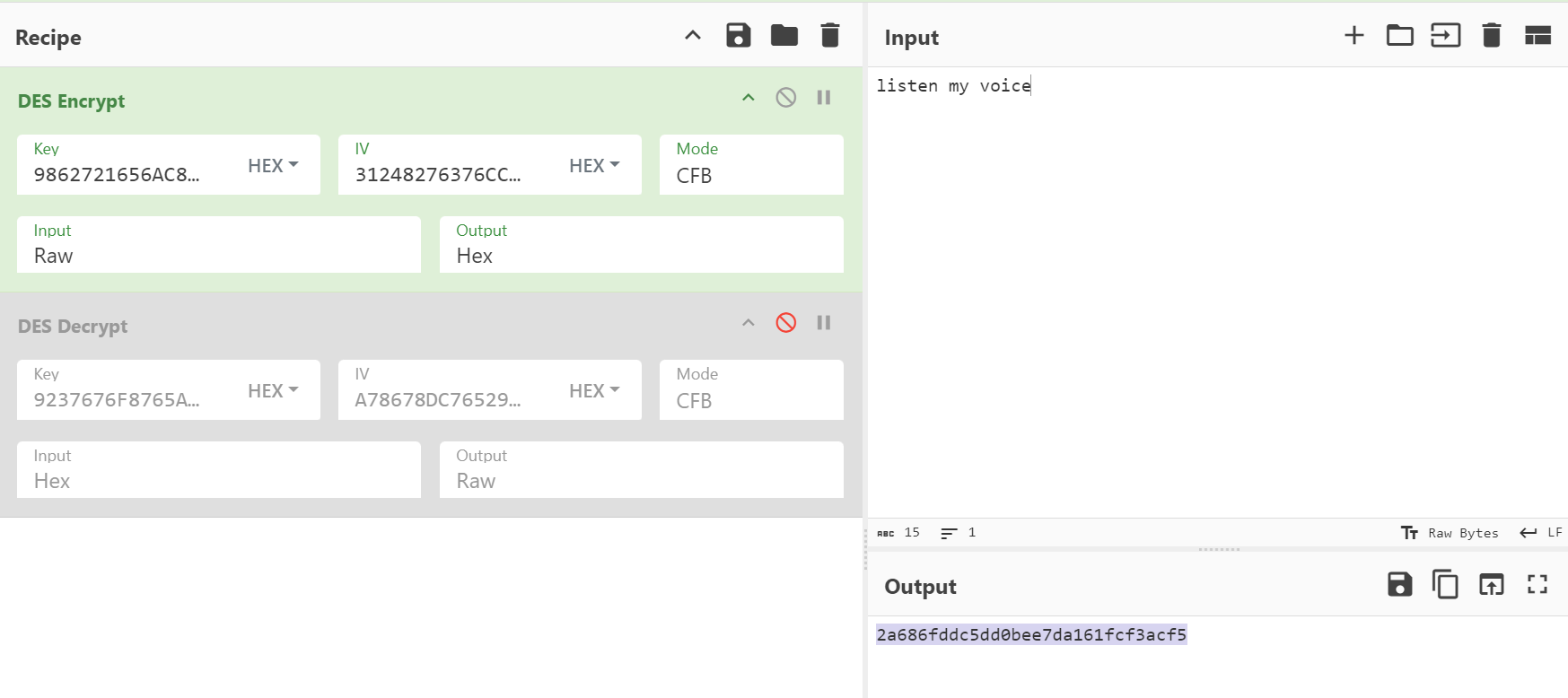
Дані шифрування:

Ключ - 9862721656АС87576 (HEX format)

Вектор ініціалізації (IV) - 31248276376СС973 (HEX format)

Відкритий текст – “listen my voice”

Шифротекст – “2a686fddc5dd0bee7da161fcf3acf5”.



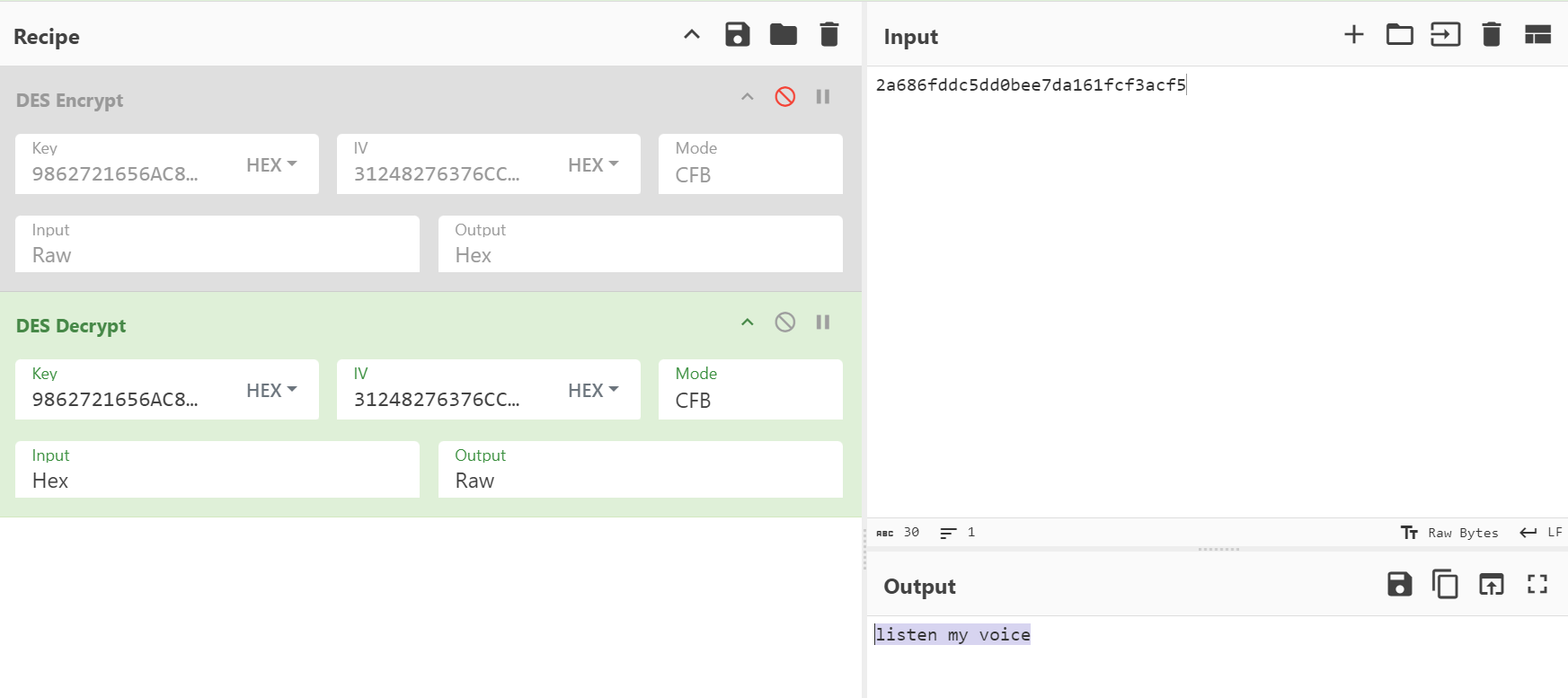
Дані розшифрування:

Ключ - 9862721656АС87576 (HEX format)

Вектор ініціалізації (IV) - 31248276376СС973 (HEX format)

Шифротекст - “2a686fddc5dd0bee7da161fcf3acf5”

Відкритий текст - “listen my voice”



**Висновок**

**1. ECB (Electronic Codebook):**

**Принцип роботи: Повідомлення розбивається на блоки однакового розміру, які потім шифруються незалежно один від одного з використанням одного ключа.**

**Переваги: Простота реалізації, висока швидкість шифрування.**

**Недоліки: Не є безпечним для деяких типів даних через однаковий шифрувальний блок, який призводить до можливості атак на шаблони.**

**2. CBC (Cipher Block Chaining):**

**Принцип роботи: Кожен блок даних під час шифрування залежить від попереднього зашифрованого блоку, що додає випадковість та запобігає атакам на шаблони.**

**Переваги: Більш безпечний за ECB через випадковий вектор ініціалізації, краща захищеність від атак на шаблони.**

**Недоліки: Частіше потребує додаткових обчислень та пам'яті, оскільки потрібно зберігати попередні блоки.**

**3. CFB (Cipher Feedback):**

**Принцип роботи: Використовується як взаємодія поточного шифрованого блоку з наступним блоком даних, а не з попереднім, як у CBC.**

**Переваги: Можливість шифрування блоків різного розміру, висока стійкість до помилок передачі.**

**Недоліки: Погане розпаралелювання процесу шифрування, також може знадобитися додатковий час на реалізацію.**

Загалом, CBC і CFB надають кращий рівень безпеки порівняно з ECB через додаткові механізми вектора ініціалізації та зв'язку між блоками даних. CBC частіше використовується в практичних застосуваннях, оскільки він забезпечує кращий рівень конфіденційності та цілісності даних, ніж ECB і CFB.