МІНІСТЕРСТВО ОБОРОНИ УКРАЇНИ

ВІЙСЬКОВИЙ ІНСТИТУТ ТЕЛЕКОМУНІКАЦІЙ ТА ІНФОРМАТИЗАЦІЇ

КАФЕДРА КІБЕРЗБЕЗПЕКИ

**ЗВІТ**

про виконання практичної роботи:

з дисципліни «Прикладна криптологія»

**РЕЖИМИ РОБОТИ ШИФРУ DES**

Дата 20.04.2024

**Виконав:** курсант 314 навчальної групи

старший солдат\_\_\_\_\_\_\_\_\_\_\_КОКУРА І.В.

**Перевiрив:** старший викладач кафедри 33

капітан\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ПРИЙМА О.О.

Шифр DES має 5 режимів роботи:

1. ECB;

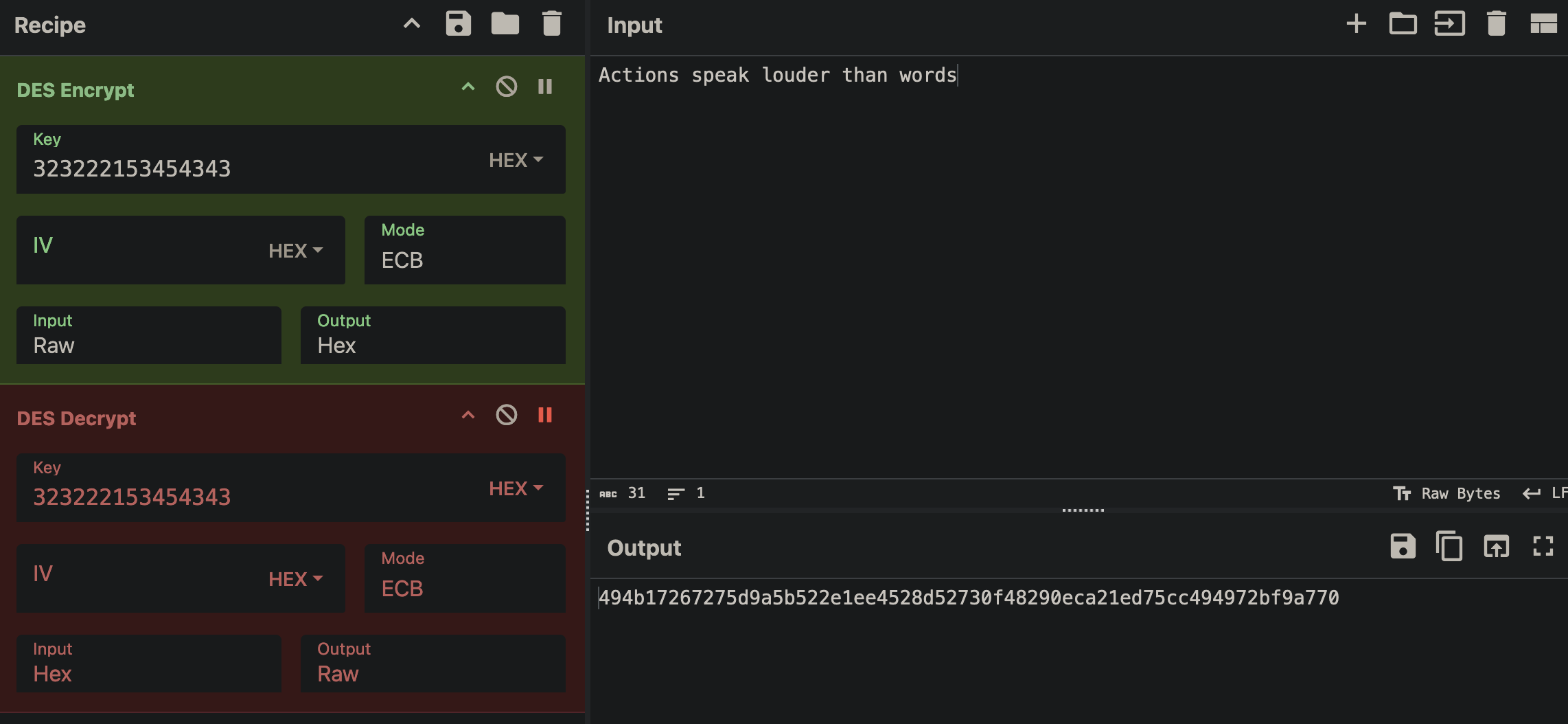
2. CTR;

3. OFB;

4. CFB;

5. CBC.

1. Шифрування в режимі ECB:



Дешифрування в режимі ECB:

A screenshot of a computer

Description automatically generated

2. Шифрування в режимі CTR:

A screenshot of a computer

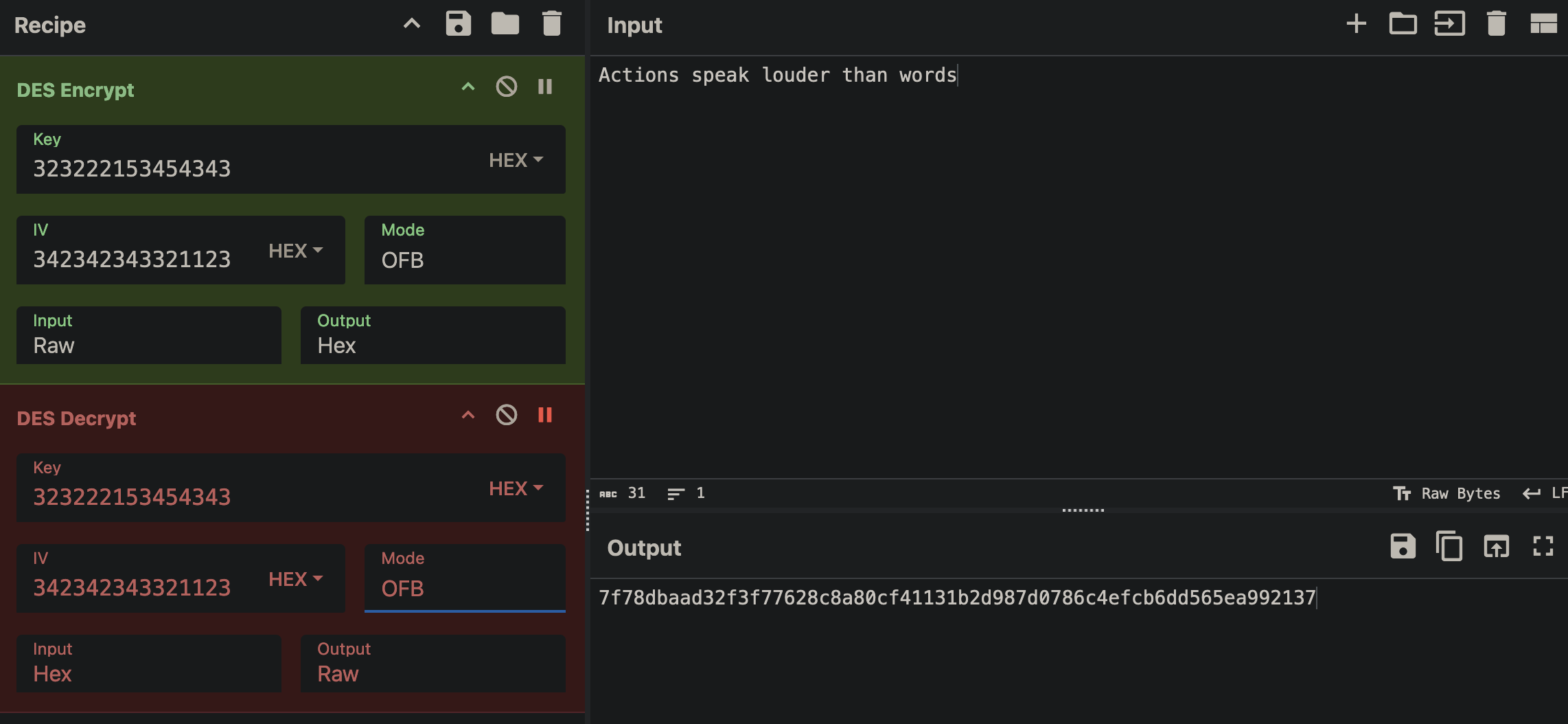
Description automatically generated

Дешифрування в режимі CTR:

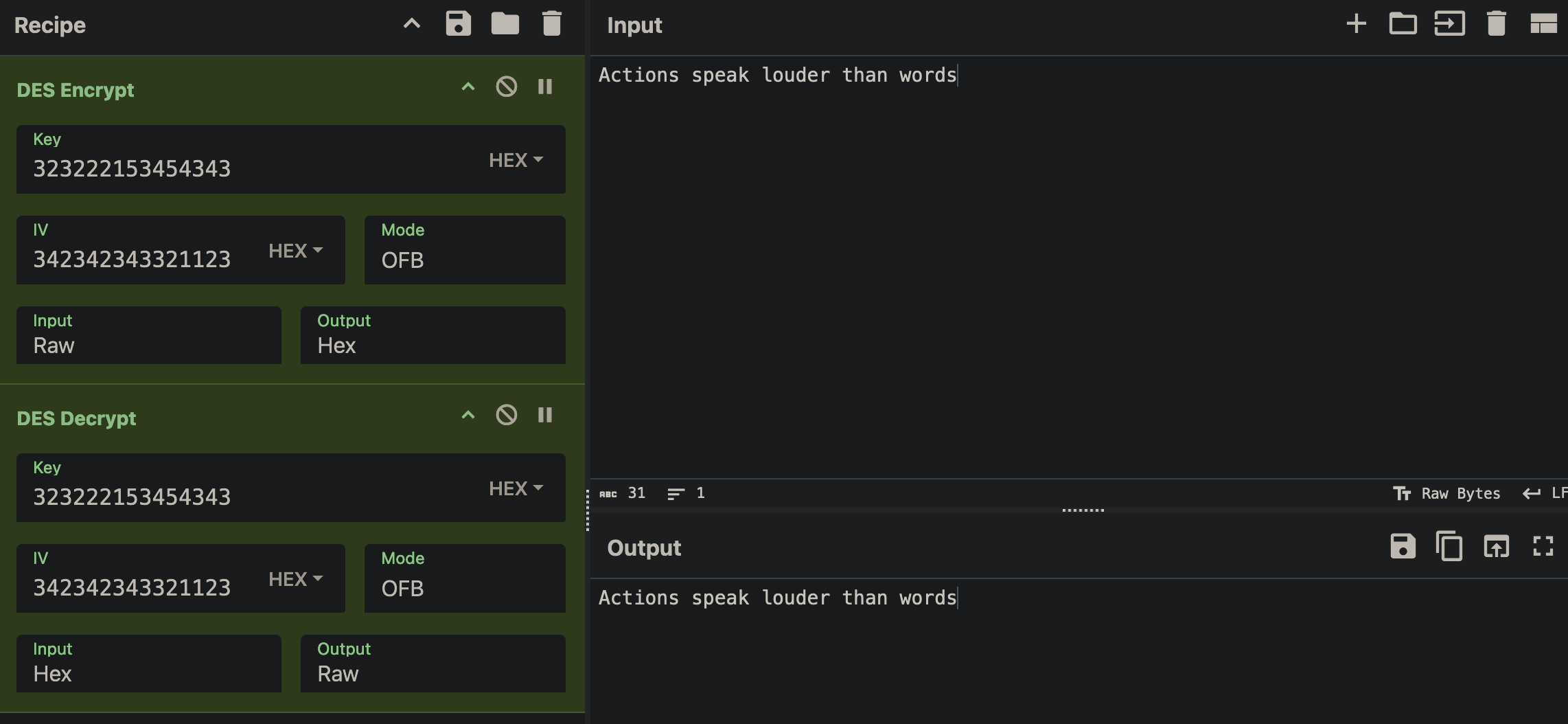
A screenshot of a computer

Description automatically generated

3. Шифрування в режимі OFB:



Дешифрування в режимі OFB:



4. Шифрування в режимі CFB:

A screenshot of a computer

Description automatically generated

Дешифрування в режимі CFB:

A screenshot of a computer

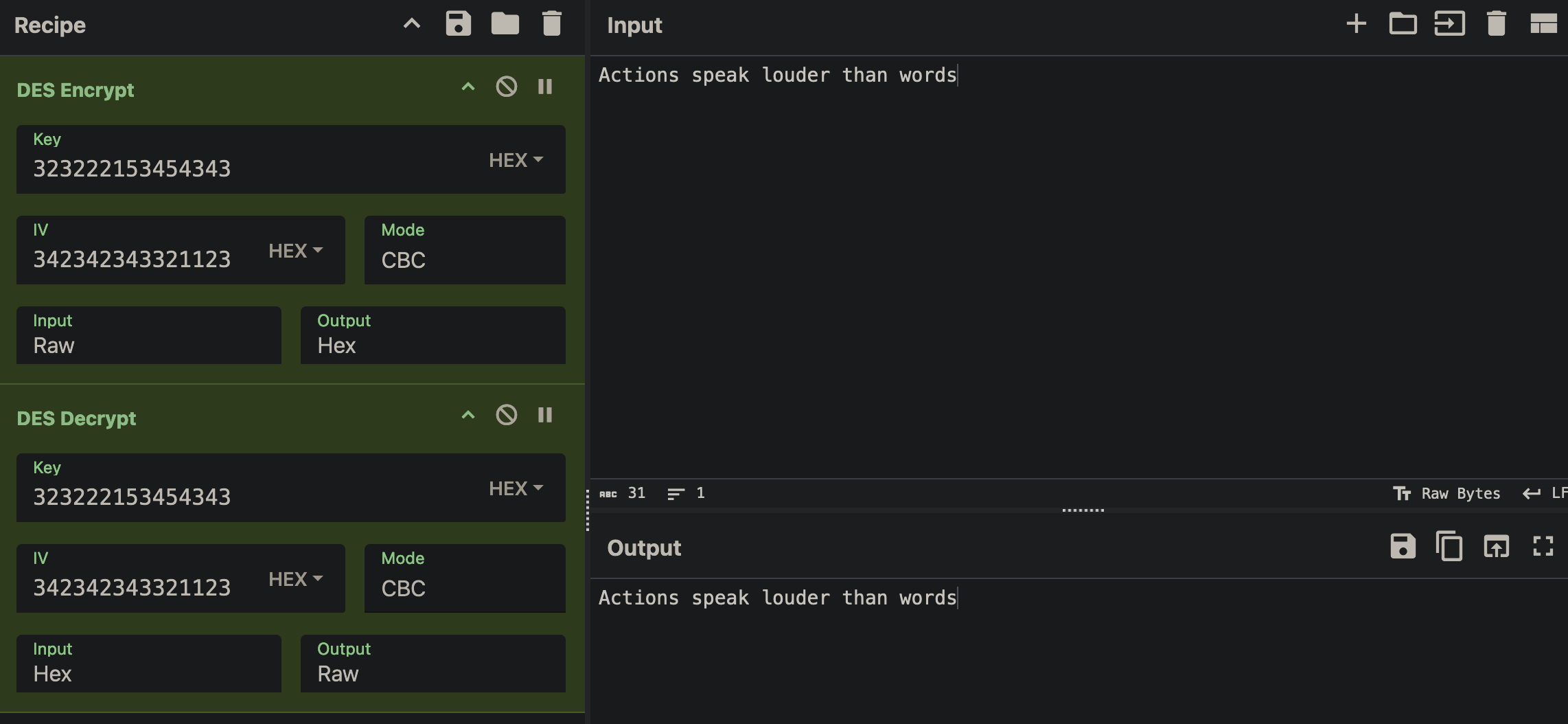
Description automatically generated

5. Шифрування в режимі CBC:

A screenshot of a computer

Description automatically generated

Дешифрування в режимі CBC:



DES (Data Encryption Standard) має п'ять режимів роботи, які дозволяють застосовувати шифрування для різних сценаріїв:

1. ECB (Electronic Codebook): Кожен блок даних шифрується незалежно один від одного. Це простий режим, але не надійний для деяких типів даних, оскільки ідентичні блоки введення можуть виводити ідентичні блоки виведення.
2. CBC (Cipher Block Chaining): Кожен блок даних комбінується з попереднім шифрованим блоком перед шифруванням. Це унеможливлює однаковість блоків виведення і додає безпеки, оскільки помилки в одному блоку не поширюються на всі наступні.
3. CFB (Cipher Feedback): Дані шифруються блоками, але виведення шифру передається назад для генерації наступного блоку. Це дозволяє шифрувати невеликі порції даних і підтримує використання змінної довжини блоку.
4. OFB (Output Feedback): Режим, схожий на CFB, але виведення шифру використовується як псевдовипадковий ключ для шифрування наступного блоку. Це дозволяє зберігати синхронізацію між відправником і отримувачем навіть при помилках передачі даних.
5. CTR (Counter): Використовується замість шифрування блоків для шифрування послідовності псевдовипадкових чисел, які потім комбінуються з вхідними даними. Це дозволяє паралельно шифрувати та розшифровувати дані, підвищуючи швидкість обробки.