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

старший солдат \_\_\_\_\_\_\_А.НАЗАРЕНКО

21.04.2024

**Перевiрив:** викладач кафедри № 33

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

Київ – 2024

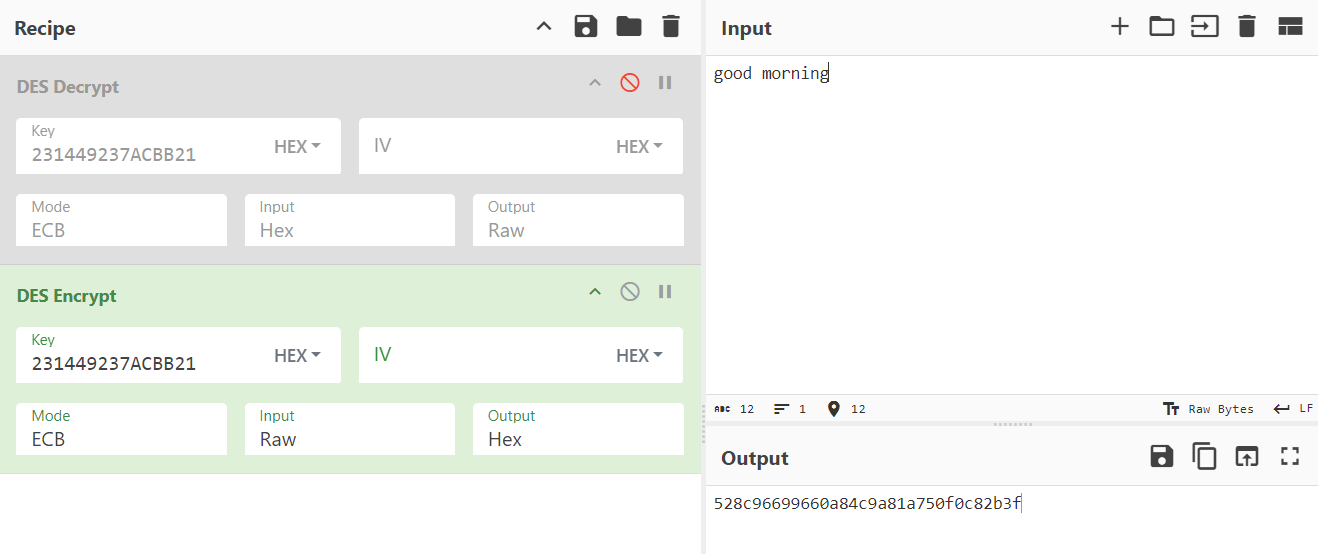
1. Виконати цикл шифрування алгоритмом DES у режимі ECB

Дані шифрування:

Ключ - 231449237ACBB21 (HEX format)

Відкритий текст – “good morning”

Шифротекст “528c96699660a84c9a81a750f0c82b3f”

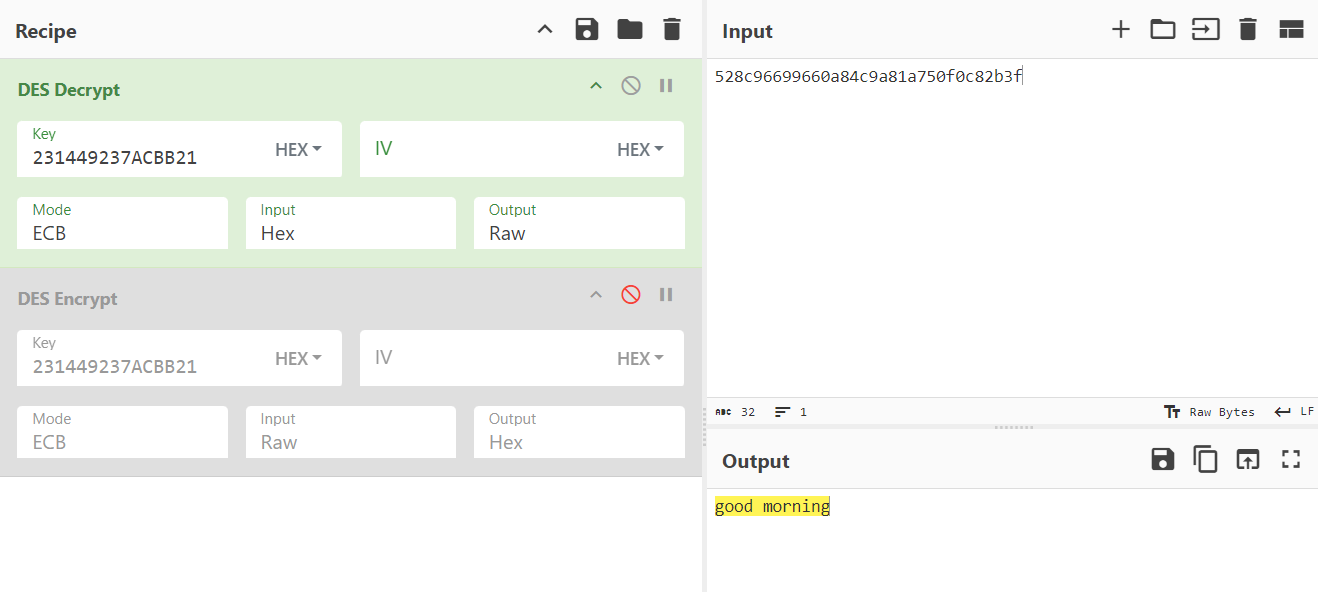


Дані розшифрування:

Ключ - 231449237ACBB21 (HEX format)

Шифротекст “528c96699660a84c9a81a750f0c82b3f”

Відкритий текст – “good morning”



1. Шифрування алгоритмом DES у режимі CBC

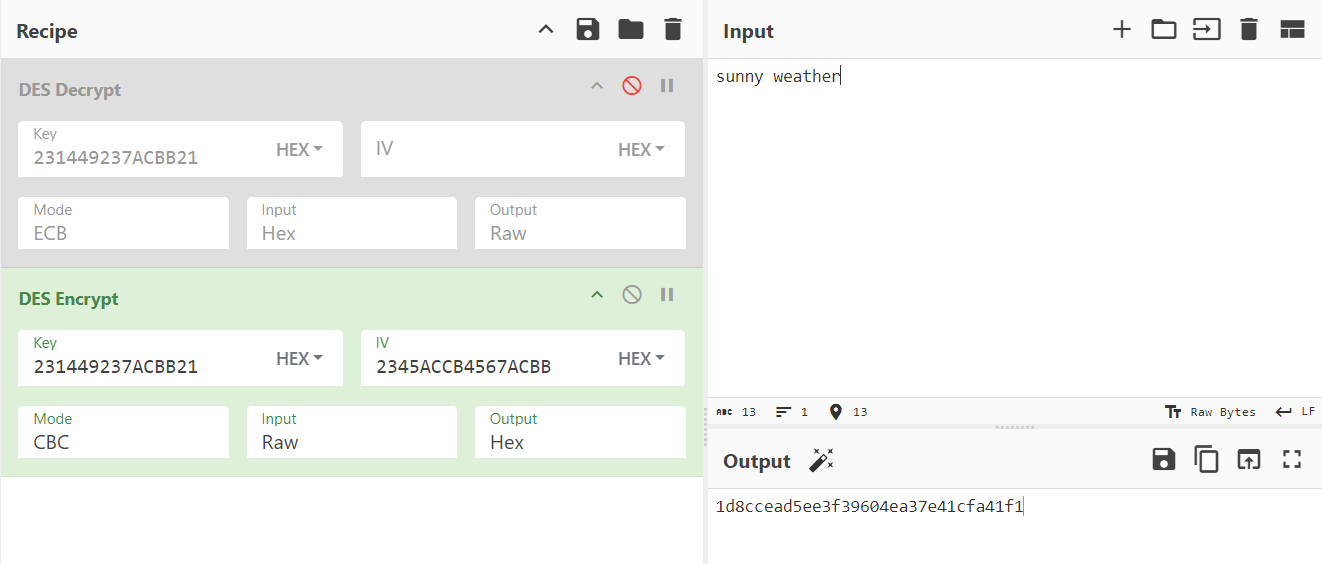
Дані шифрування:

Ключ - 231449237ACBB21 (HEX format)

Вектор ініціалізації (IV) - 2345ACCB4567ACBB в HEX форматі.

Відкритий текст - sunny weather

Шифротекст - 1d8ccead5ee3f39604ea37e41cfa41f1 в HEX форматі.



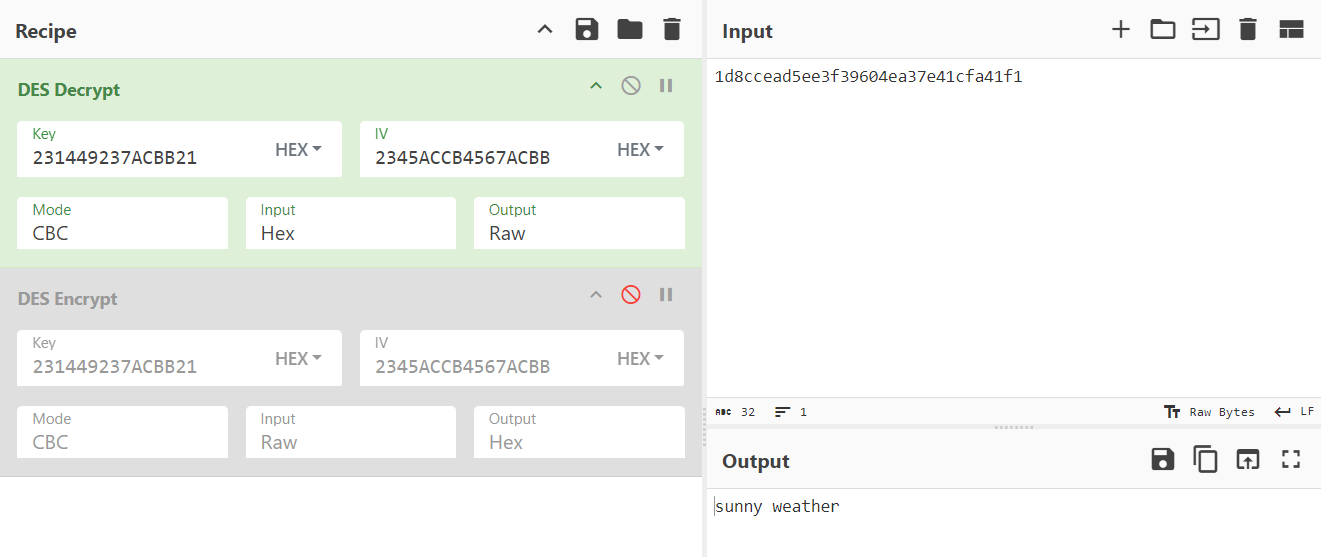
Дані розшифрування:

Ключ - 231449237ACBB21 в HEX форматі.

Вектор ініціалізації (IV) - 2345ACCB4567ACBB в HEX форматі.

Шифротекст - 1d8ccead5ee3f39604ea37e41cfa41f1 в HEX форматі.

Відкритий текст - sunny weather



1. Виконати цикл шифрування алгоритмом DES у режимі CFB

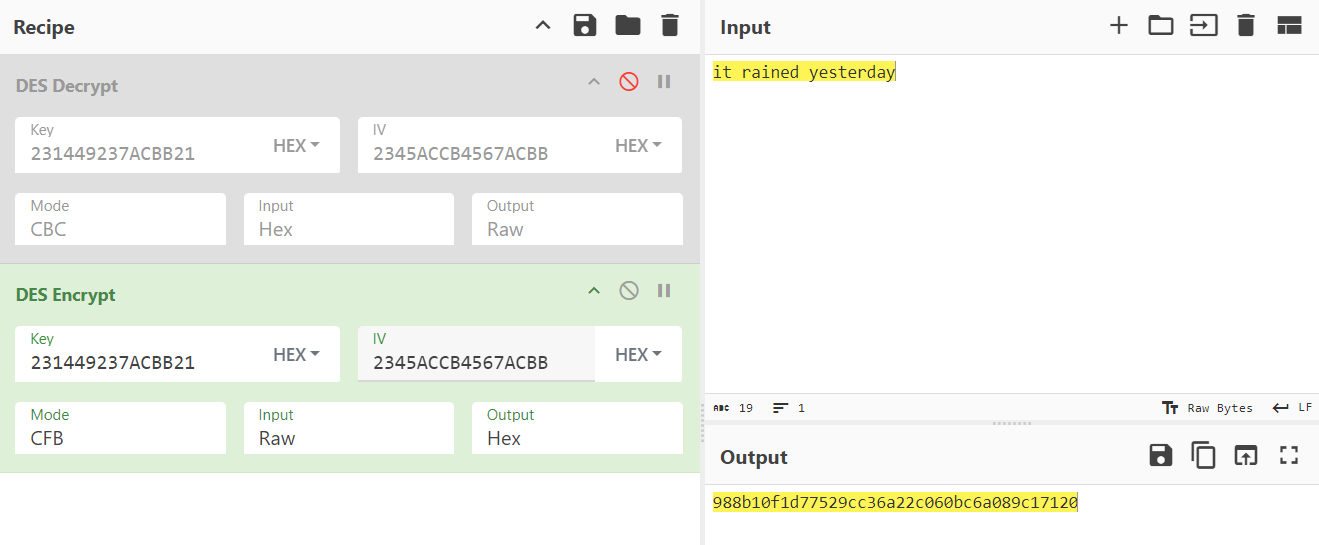
Дані шифрування:

Ключ - 231449237ACBB21 в HEX форматі.

Вектор ініціалізації (IV) - 2345ACCB4567ACBB в HEX форматі.

Відкритий текст - it rained yesterday

Шифротекст - 988b10f1d77529cc36a22c060bc6a089c17120 в HEX форматі.



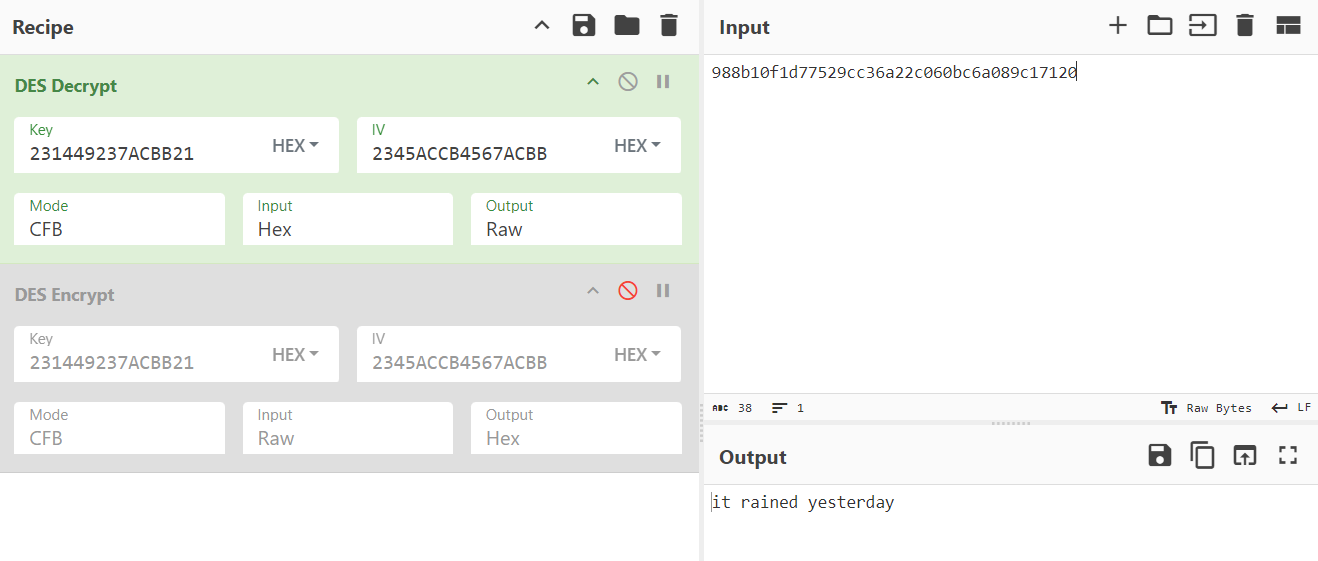
Дані розшифрування:

Ключ - 231449237ACBB21 в HEX форматі.

Вектор ініціалізації (IV) - 2345ACCB4567ACBB в HEX форматі.

Шифротекст - 988b10f1d77529cc36a22c060bc6a089c17120 в HEX форматі.

Відкритий текст - it rained yesterday



**Висновок:**

1. **ECB (Electronic Codebook):**
2. **Принцип роботи : в цьому режимі блок даних шифрується незалежно один від одного. Кожен блок тексту відкритого тексту шифрується одним і тим самим ключем, що робить його простим і ефективним для реалізації.**

**Переваги : простота і швидкість реалізації, оскільки блоки можуть оброблятися паралельно. Він також відповідає простим вимогам щодо виправлення помилок, оскільки один блок не впливає на інші.**

**Недоліки : ЕCB не допускає приховування структури даних, тому що однакові блоки відкритого тексту будуть шифруватися в однаковий шифртекст, що може розголошувати інформацію про самі дані.**

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

**Принцип роботи : у цьому режимі кожен блок відкритого тексту XOR-ується з попереднім шифрованим блоком перед шифруванням, що ускладнює відновлення вихідного тексту без наявності ключа.**

**Переваги : криптографічна сильність, оскільки кожен блок даних залежить від попереднього. Це дозволяє позбутися від дублювання шифртексту, що властиво ECB.**

**Недоліки : CBC не може шифрувати паралельно, оскільки кожен блок залежить від попереднього. Це може зробити його менш ефективним для деяких додатків.**

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

**Принцип роботи : у цьому режимі використовується зсувний реєстр, який використовується для генерації псевдовипадкових бітів, які потім XOR-уються з блоками відкритого тексту перед шифруванням.**

**Переваги : можливість шифрування в режимі потоку, що дозволяє передавати довільні обсяги даних без розділення на блоки. Також дозволяє передавати дані в реальному часі.**

**Недоліки : вимагає більше обчислень, оскільки потрібно обробляти кожен біт окремо. Крім того, помилки передачі можуть суттєво вплинути на розшифрування наступних блоків.**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.