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 \_\_\_\_\_\_\_\_\_\_\_\_\_Бондар В.Е.

21.04.2024

**Перевiрив:** викладач кафедри № 33

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

Київ – 2024

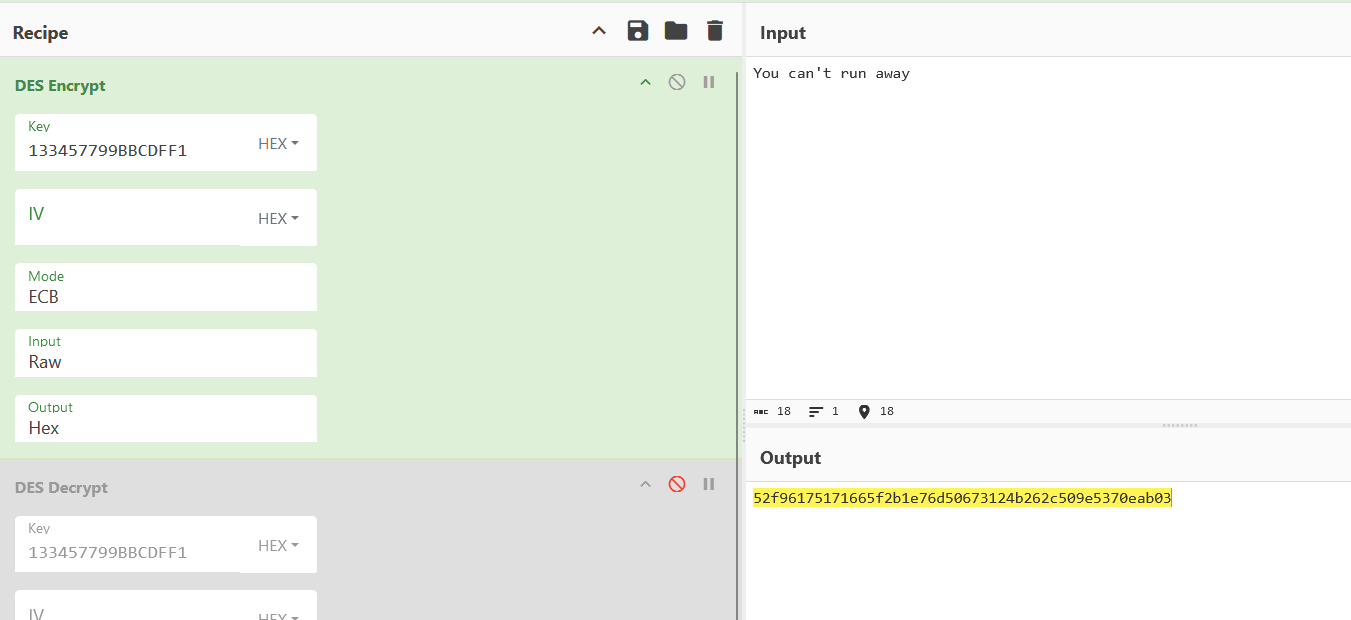
1. Виконати цикл шифрування алгоритмом DES у режимі ECB

Дані шифрування:

Ключ - 133457799BBCDFF1 в HEX форматі.

Відкритий текст - You can't run away

Шифротекст - 52f96175171665f2b1e76d50673124b262c509e5370eab03 в HEX форматі.

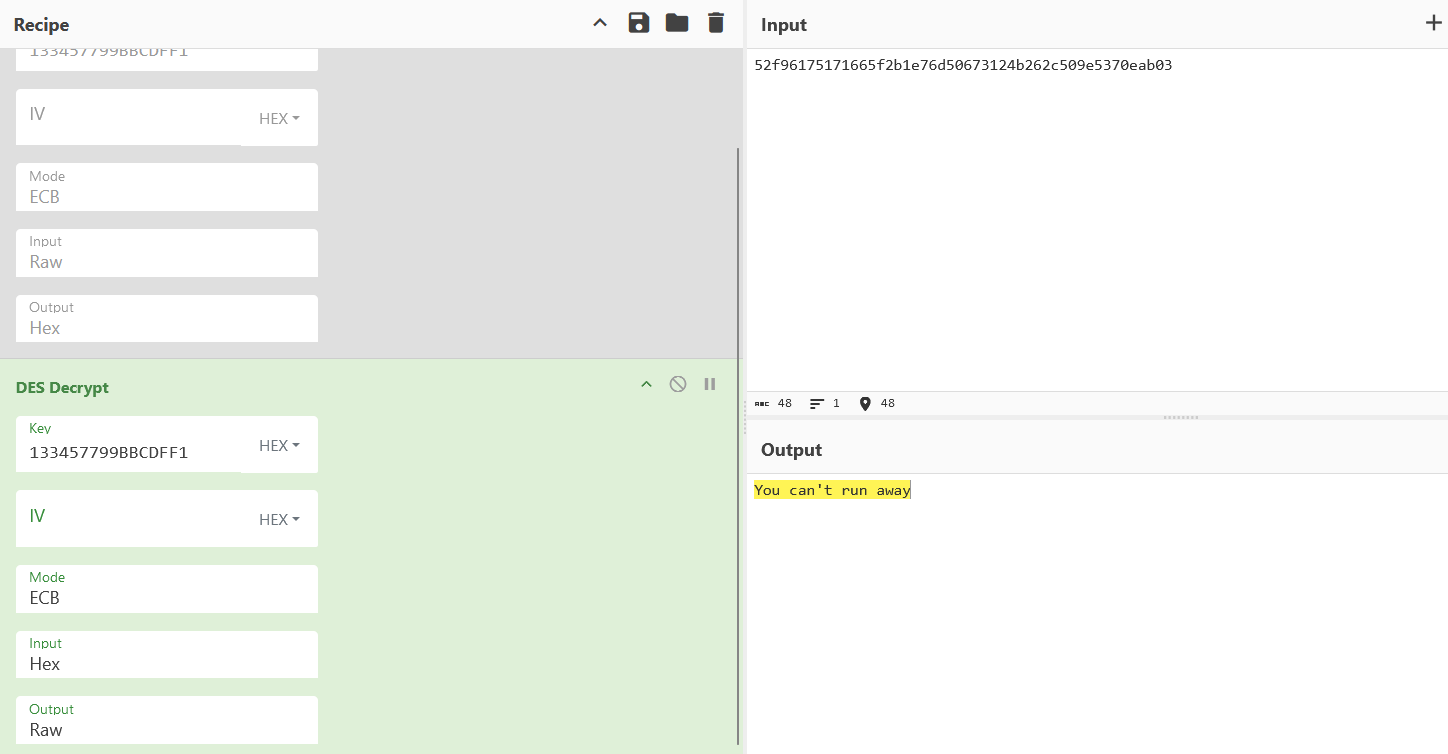


Дані розшифрування:

Ключ - 133457799BBCDFF1 в HEX форматі.

Шифротекст - 52f96175171665f2b1e76d50673124b262c509e5370eab03

Відкритий текст - You can't run away



1. Виконати цикл шифрування алгоритмом DES у режимі CBC

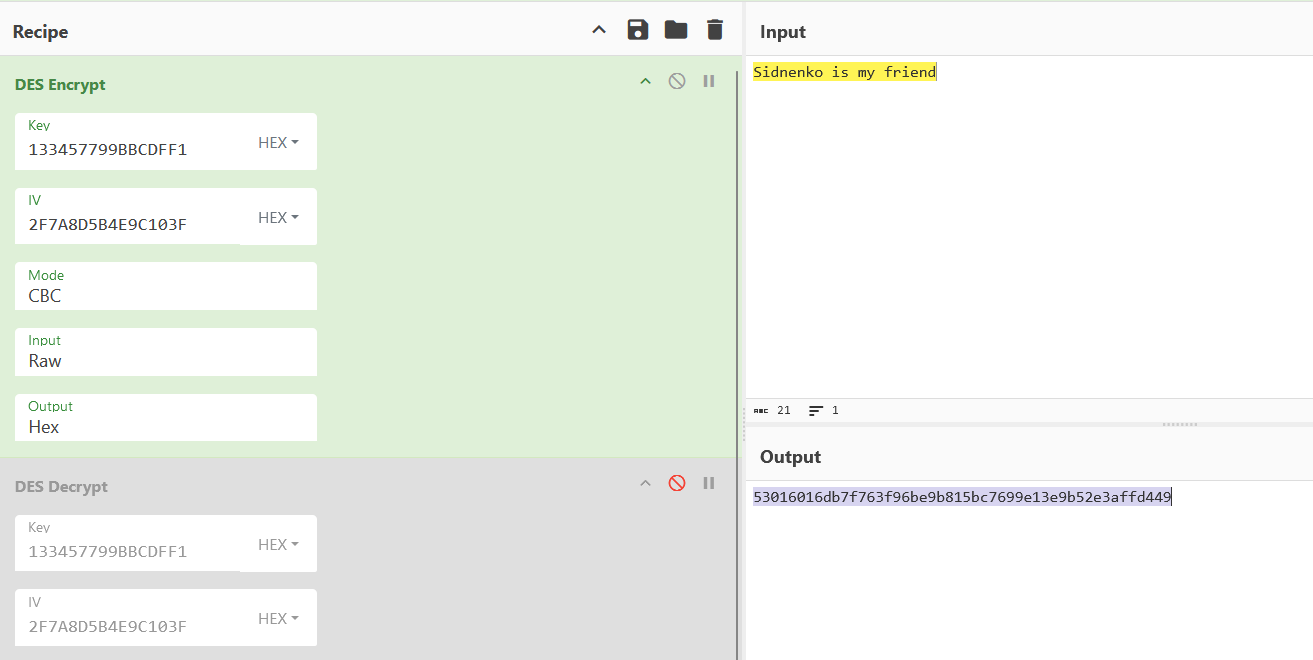
Дані шифрування:

Ключ - 133457799BBCDFF1 в HEX форматі.

Вектор ініціалізації (IV) - 2F7A8D5B4E9C103F в HEX форматі.

Відкритий текст - Sidnenko is my friend

Шифротекст - 53016016db7f763f96be9b815bc7699e13e9b52e3affd449 в HEX форматі.



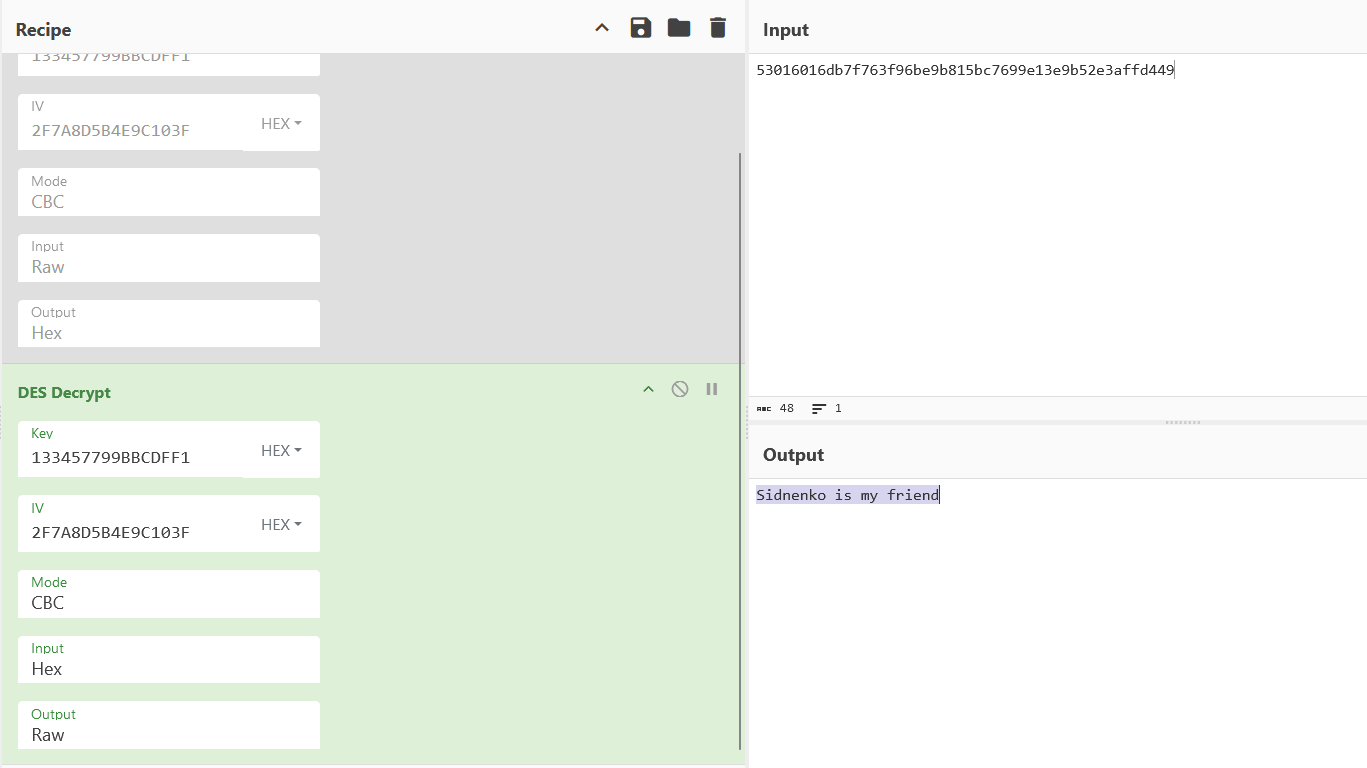
Дані розшифрування:

Ключ - 133457799BBCDFF1 в HEX форматі.

Вектор ініціалізації (IV) - 2F7A8D5B4E9C103F в HEX форматі.

Шифротекст - 53016016db7f763f96be9b815bc7699e13e9b52e3affd449 в HEX форматі.

Відкритий текст - Sidnenko is my friend



1. Виконати цикл шифрування алгоритмом DES у режимі CFB

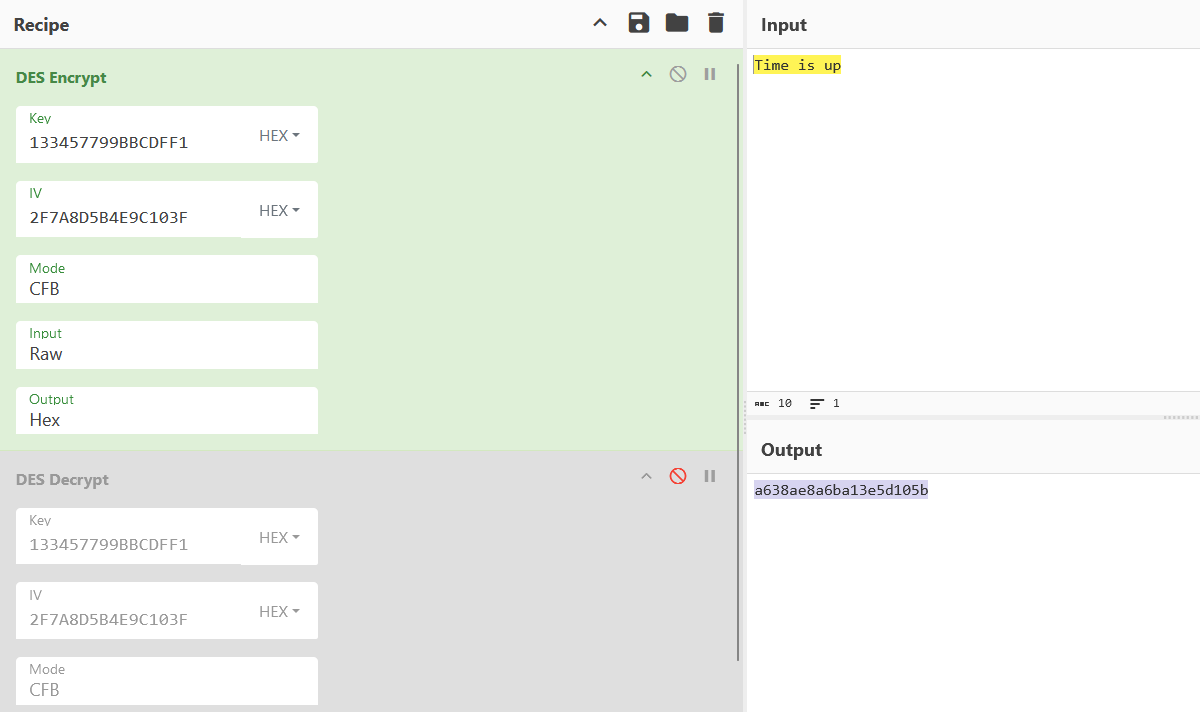
Дані шифрування:

Ключ - 133457799BBCDFF1 в HEX форматі.

Вектор ініціалізації (IV) - 2F7A8D5B4E9C103F в HEX форматі.

Відкритий текст - Time is up

Шифротекст - a638ae8a6ba13e5d105b в HEX форматі.



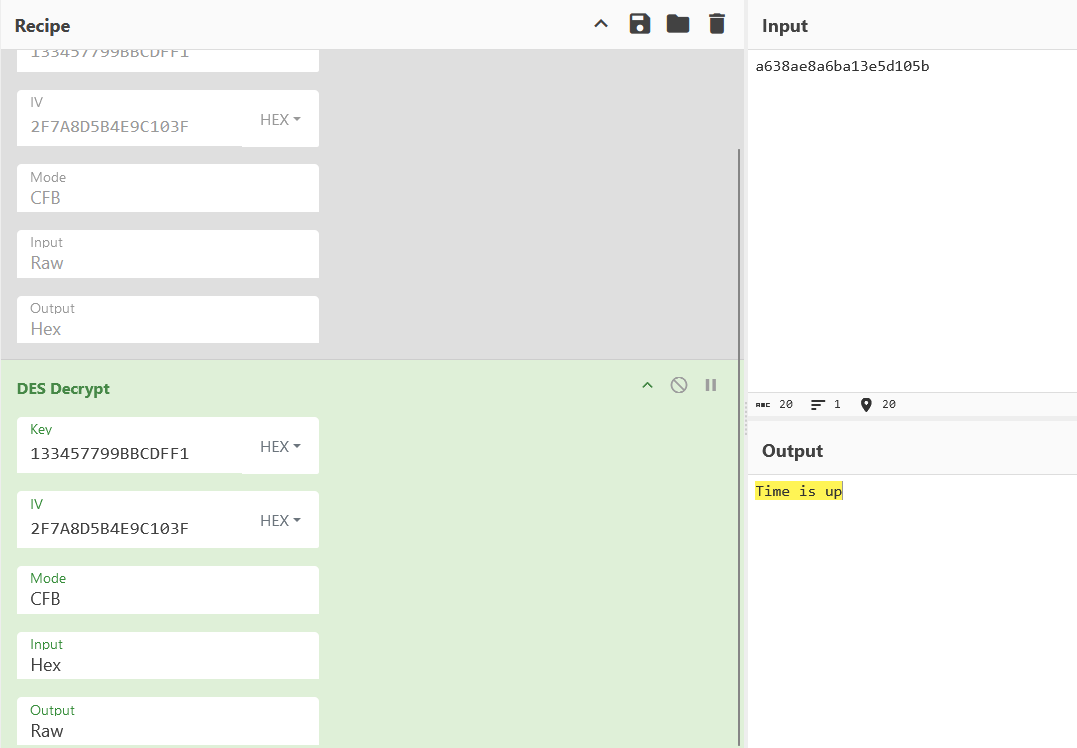
Дані розшифрування:

Ключ - 133457799BBCDFF1 в HEX форматі.

Вектор ініціалізації (IV) - 2F7A8D5B4E9C103F в HEX форматі.

Шифротекст - a638ae8a6ba13e5d105b в HEX форматі.

Відкритий текст - Time is up



**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.