МІНІСТЕРСТВО ОБОРОНИ УКРАЇНИ

ВІЙСЬКОВИЙ ІНСТИТУТ ТЕЛЕКОМУНІКАЦІЙ ТА ІНФОРМАТИЗАЦІЇ

КАФЕДРА КІБЕРЗАХИСТУ

**ЗВІТ**

про виконання практичної роботи:

з дисципліни «Прикладна криптологія»

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

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

**Виконав:** курсант навчальної групи 314

солдат \_\_\_\_\_\_\_\_\_\_\_\_\_Петренко К.В.

20.04.2024

**Перевiрив:** викладач кафедри № 33

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

Київ – 2024

1. Виконати цикл шифрування алгоритмом DES у режимі ECB

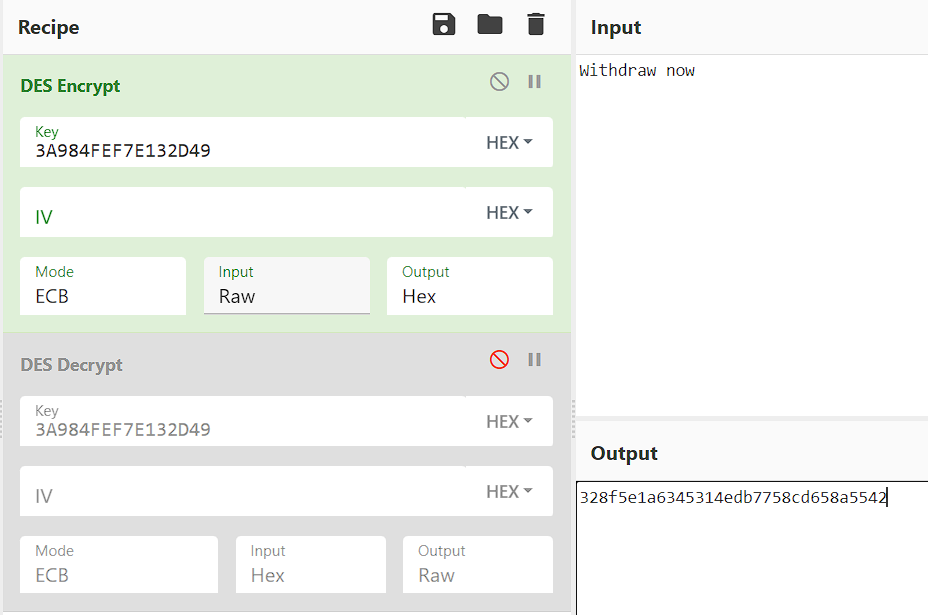
Кожен блок даних шифрується незалежно один від одного. Це простий та швидкий режим, але не надійний для деяких типів даних, оскільки ідентичні блоки введення можуть виводити ідентичні

Дані шифрування:

Ключ - 3A984FEF7E132D49 в HEX форматі.

Відкритий текст - Withdraw now

Шифротекст - 328f5e1a6345314edb7758cd658a5542 в HEX форматі.

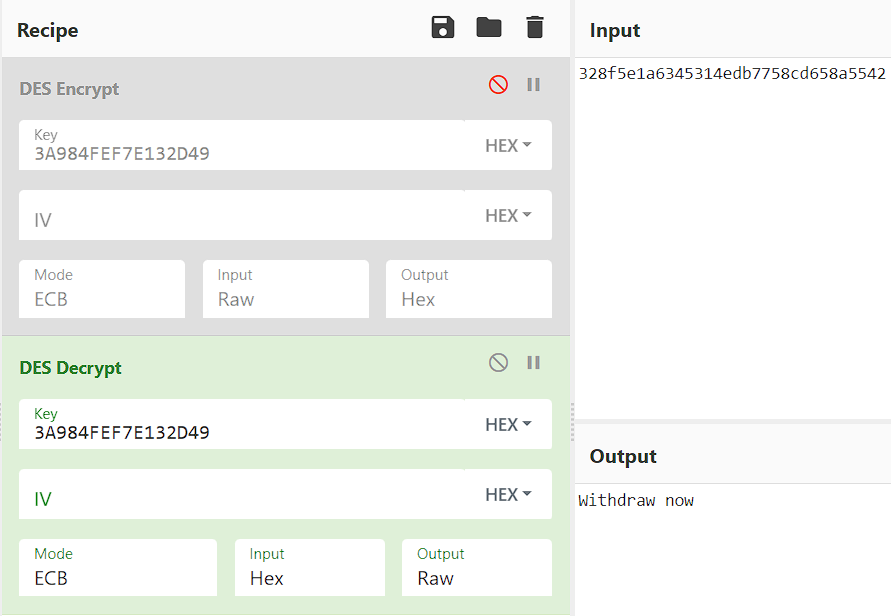


Дані розшифрування:

Ключ - 3A984FEF7E132D49 в HEX форматі.

Шифротекст - 328f5e1a6345314edb7758cd658a5542

Розшифрований текст - Withdraw now



1. Виконати цикл шифрування алгоритмом DES у режимі CBC

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.

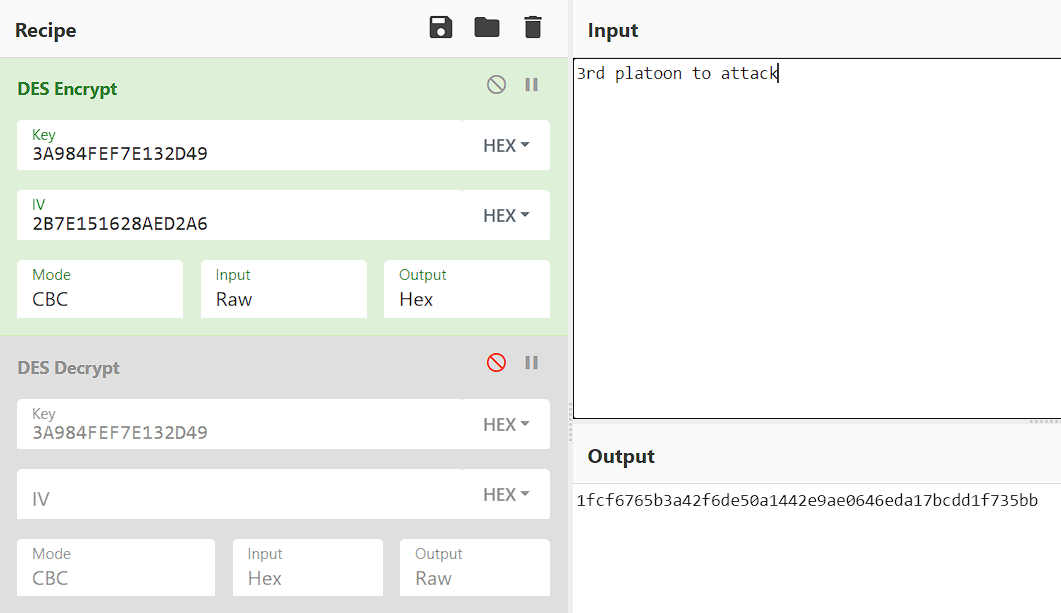
Дані шифрування:

Ключ - 3A984FEF7E132D49 в HEX форматі.

Вектор ініціалізації (IV) - 2B7E151628AED2A6 в HEX форматі.

Відкритий текст - 3rd platoon to attack

Шифротекст - 1fcf6765b3a42f6de50a1442e9ae0646eda17bcdd1f735bb в HEX форматі.



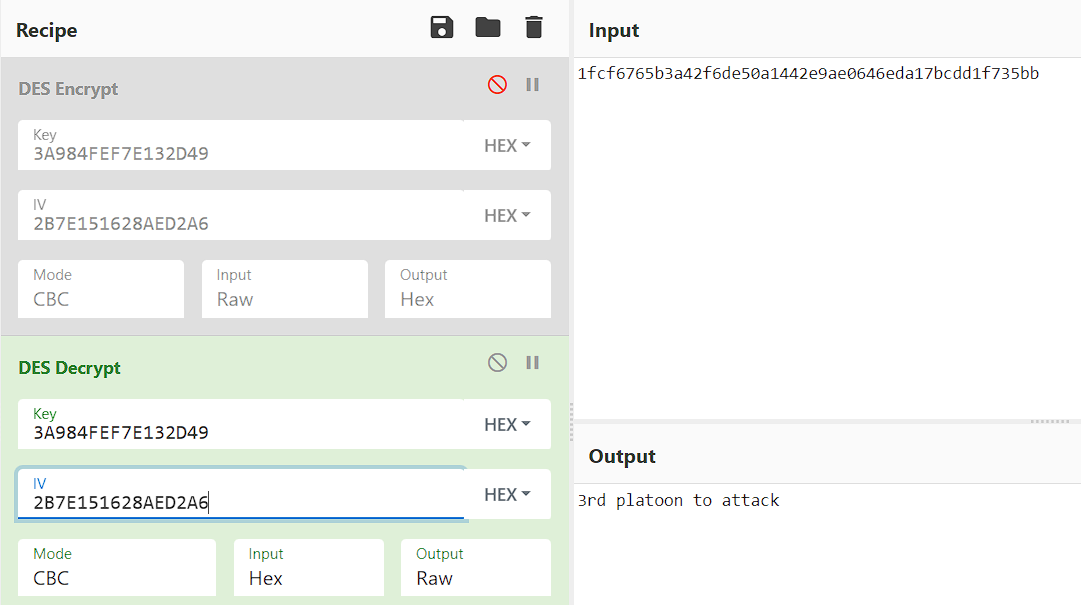
Дані розшифрування:

Ключ - 3A984FEF7E132D49 в HEX форматі.

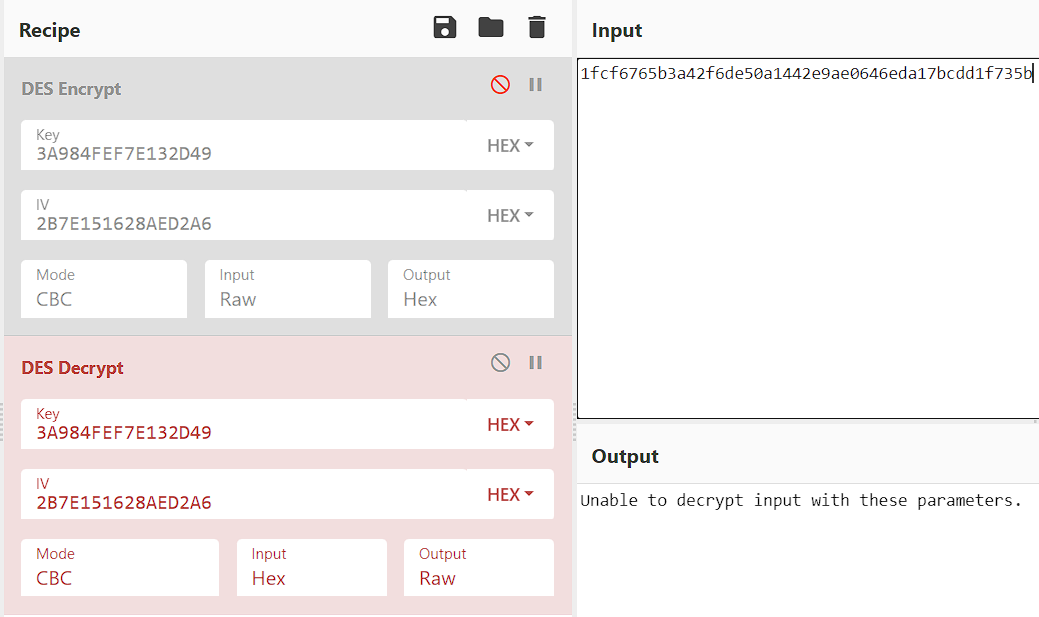
Вектор ініціалізації (IV) - 2B7E151628AED2A6 в HEX форматі.

Шифротекст - 1fcf6765b3a42f6de50a1442e9ae0646eda17bcdd1f735bb в HEX форматі.

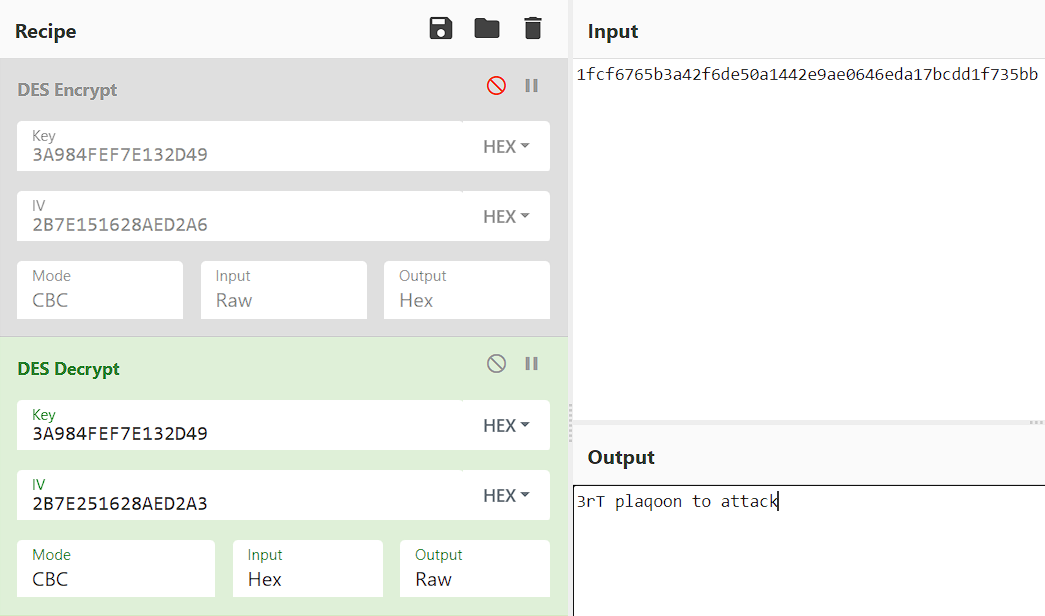
Розшифрований текст - 3rd platoon to attack



1. Якщо змінити хоч один символ в шифротексті чи в ключі, то виб’є помилку.



1. Але якщо змінити чи видалити 1 символ у векторі ініціалізації, то повідомлення залишиться читабельним.



1. Виконати цикл шифрування алгоритмом DES у режимі CFB

Дані шифруються блоками, але виведення шифру передається назад для генерації наступного блоку. Це дозволяє шифрувати невеликі порції даних і підтримує використання змінної довжини блоку.

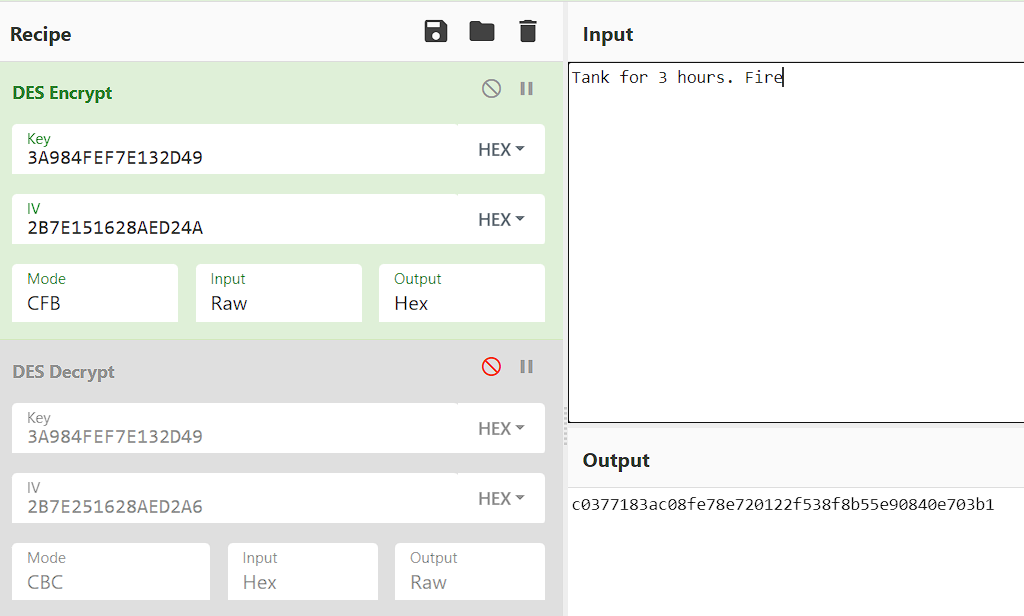
Дані шифрування:

Ключ - 3A984FEF7E132D49 в HEX форматі.

Вектор ініціалізації (IV) - 2B7E151628AED24A в HEX форматі.

Відкритий текст - Tank for 3 hours. Fire

Шифротекст - c0377183ac08fe78e720122f538f8b55e90840e703b1 в HEX форматі.



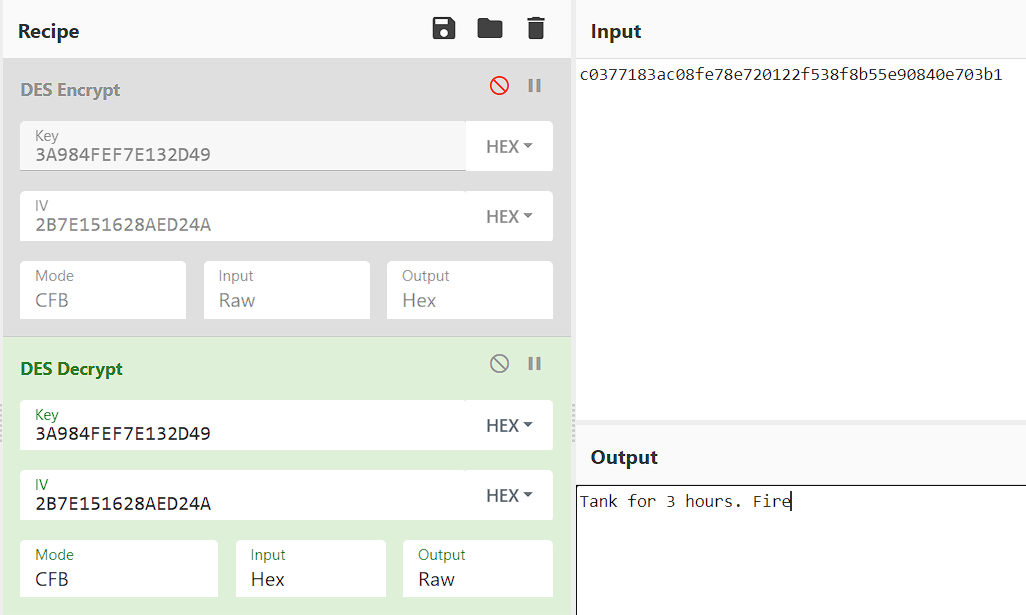
Дані розшифрування:

Ключ - 3A984FEF7E132D49 в HEX форматі.

Вектор ініціалізації (IV) - 2B7E151628AED24A в HEX форматі.

Шифротекст - c0377183ac08fe78e720122f538f8b55e90840e703b1 в HEX форматі.

Розшифрований текст - Tank for 3 hours. Fire



**Висновок:** У ході виконання завдання ми ознайомились і практично відпрацювали цикл шифрування алгоритмом DES за допомогою сайту cyberchef.io, розглянули його інтерфейс та з використанням реалізованого на цьому сайті функціоналу відпрацювали шифрування у режимах ECB, CBC, CFB, провели тестування на помилки шляхом викривленя параметрів розшифрування та виявили закономірності.