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

сержант \_\_\_\_\_\_\_\_\_\_\_\_\_Коханевич Є.Ю

20.04.2024

**Перевiрив:** викладач кафедри № 33

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

Київ – 2024

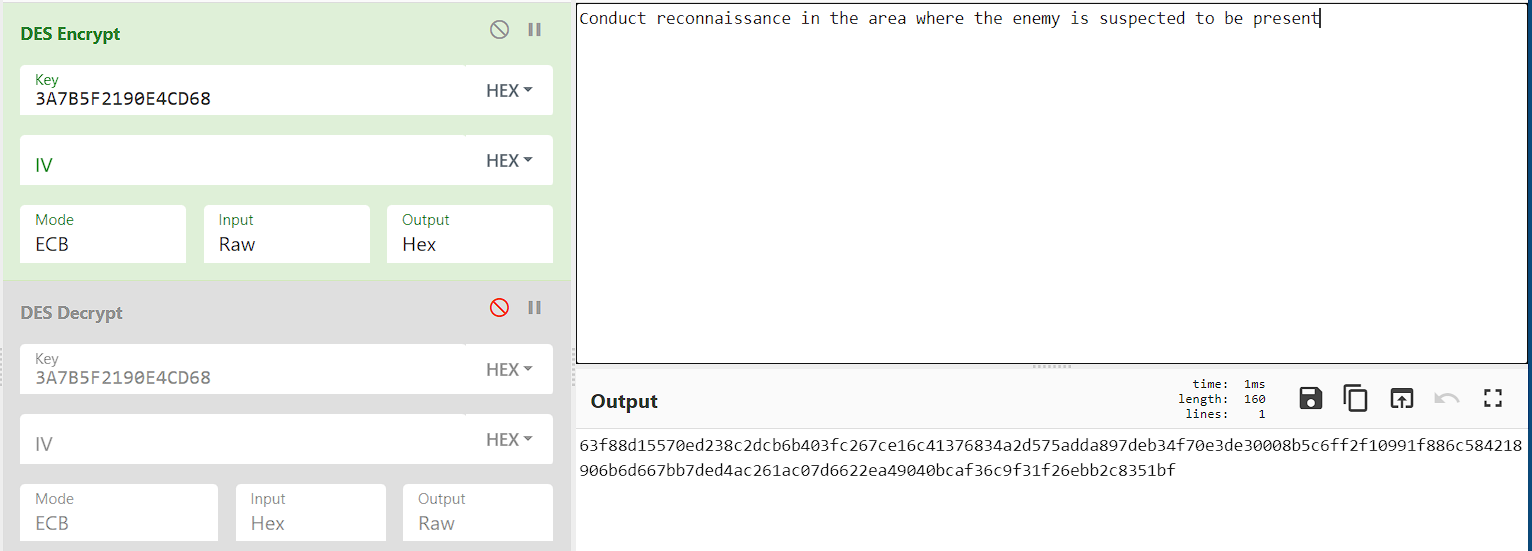
1. Виконати цикл шифрування алгоритмом DES у режимі ECB

Дані шифрування:

Ключ - 3A7B5F2190E4CD68 в HEX форматі.

Відкритий текст - Conduct reconnaissance in the area where the enemy is suspected to be present

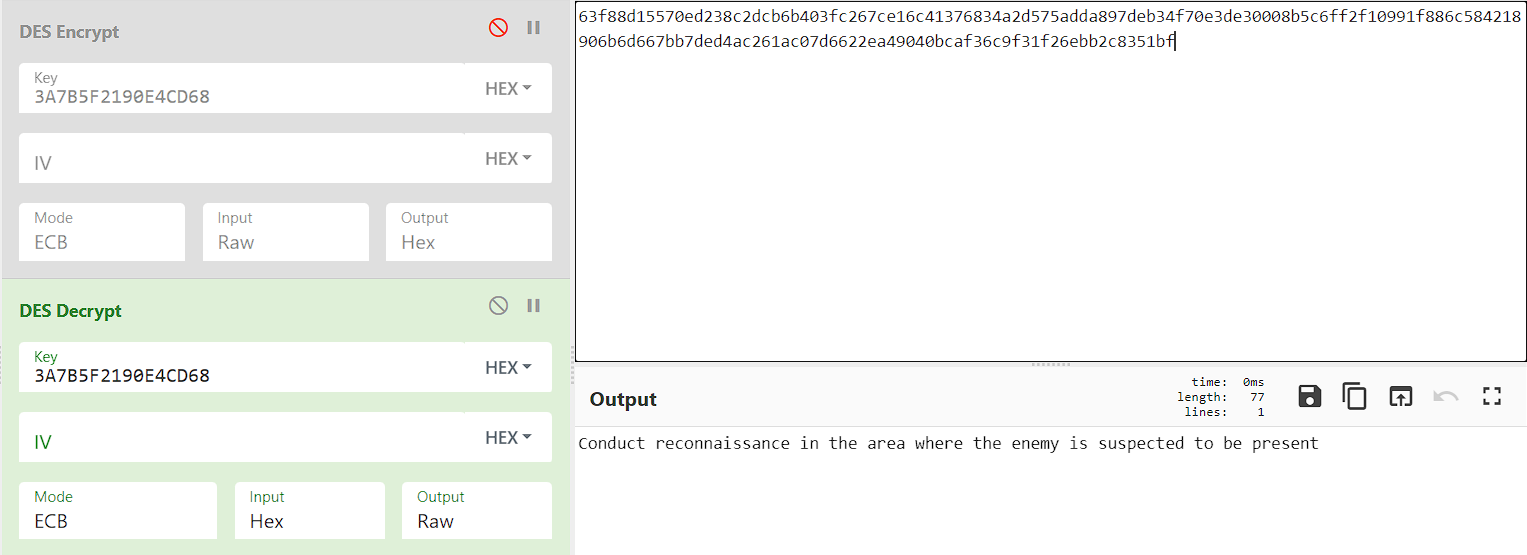
Шифротекст: 63f88d15570ed238c2dcb6b403fc267ce16c41376834a2d575adda897deb34f70e3de30008b5c6ff2f10991f886c584218906b6d667bb7ded4ac261ac07d6622ea49040bcaf36c9f31f26ebb2c8351bf в HEX форматі.



Ключ - 3A7B5F2190E4CD68 в HEX форматі.

Шифротекст: 63f88d15570ed238c2dcb6b403fc267ce16c41376834a2d575adda897deb34f70e3de30008b5c6ff2f10991f886c584218906b6d667bb7ded4ac261ac07d6622ea49040bcaf36c9f31f26ebb2c8351bf в HEX форматі.

Розшифрований текст - Conduct reconnaissance in the area where the enemy is suspected to be present



1. Виконати цикл шифрування алгоритмом DES у режимі CBC

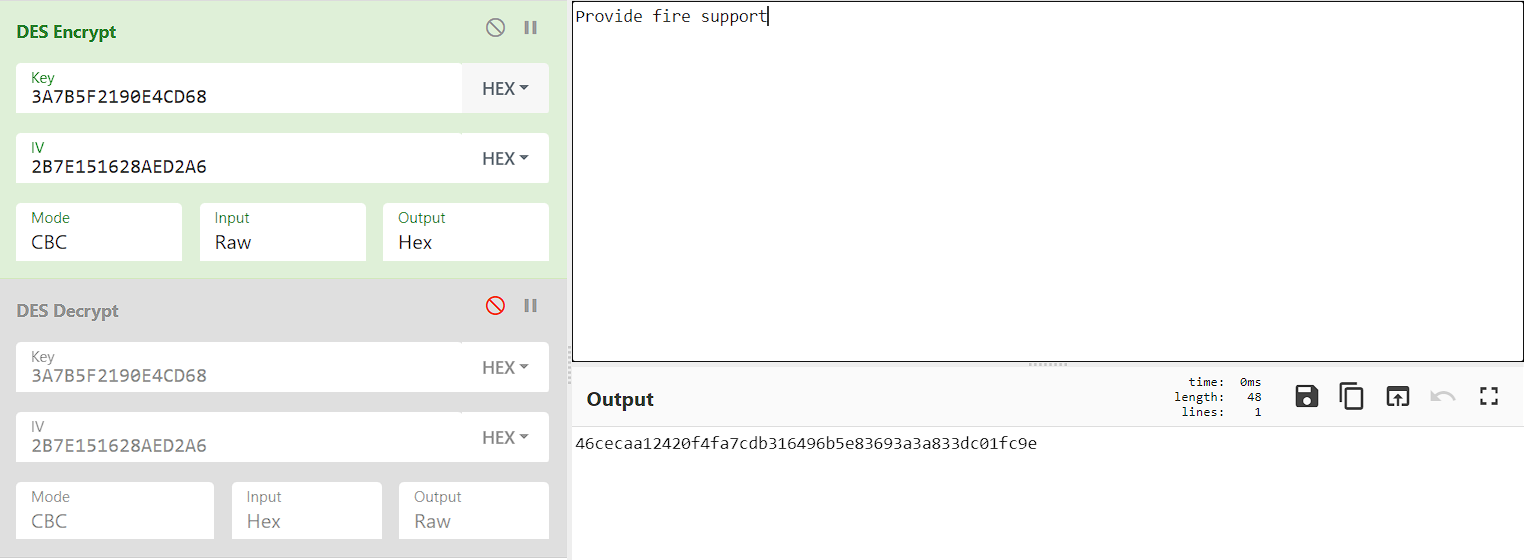
Дані шифрування:

Ключ - 3A7B5F2190E4CD68 в HEX форматі.

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

Відкритий текст - Provide fire support

Шифротекст - 46cecaa12420f4fa7cdb316496b5e83693a3a833dc01fc9e в HEX форматі.



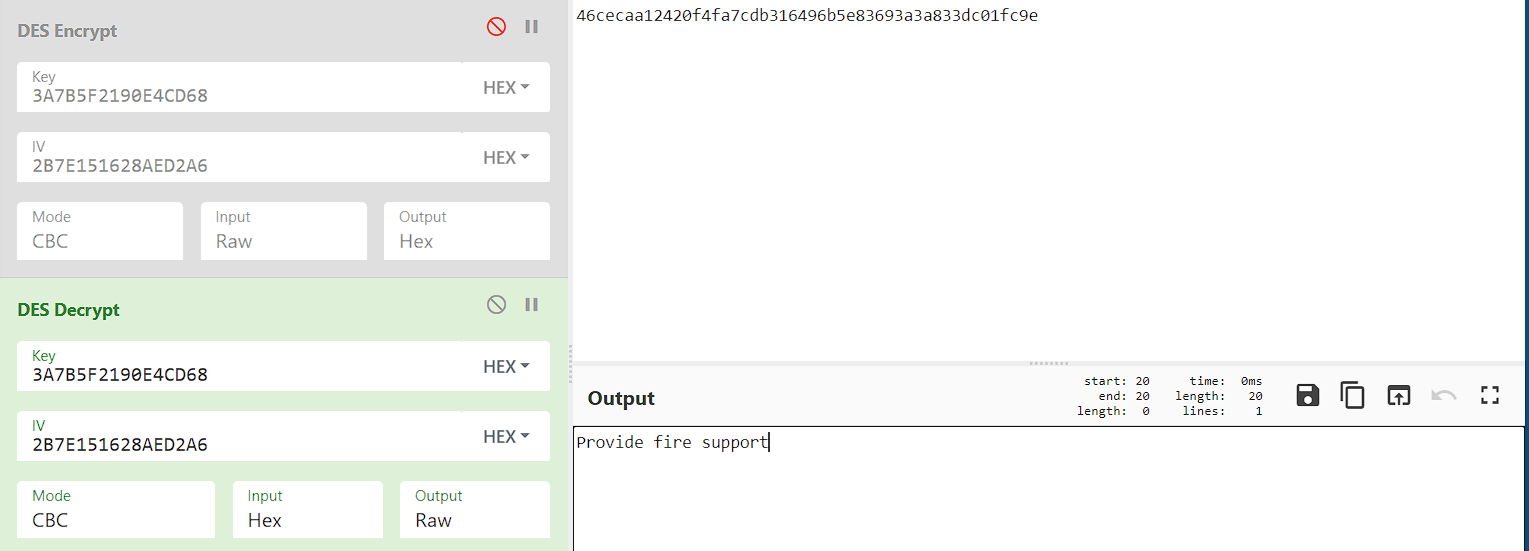
Дані розшифрування:

Ключ - 3A7B5F2190E4CD68 в HEX форматі.

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

Шифротекст - 46cecaa12420f4fa7cdb316496b5e83693a3a833dc01fc9e в HEX форматі.

Розшифрований текст - Provide fire support



1. Виконати цикл шифрування алгоритмом DES у режимі CFB

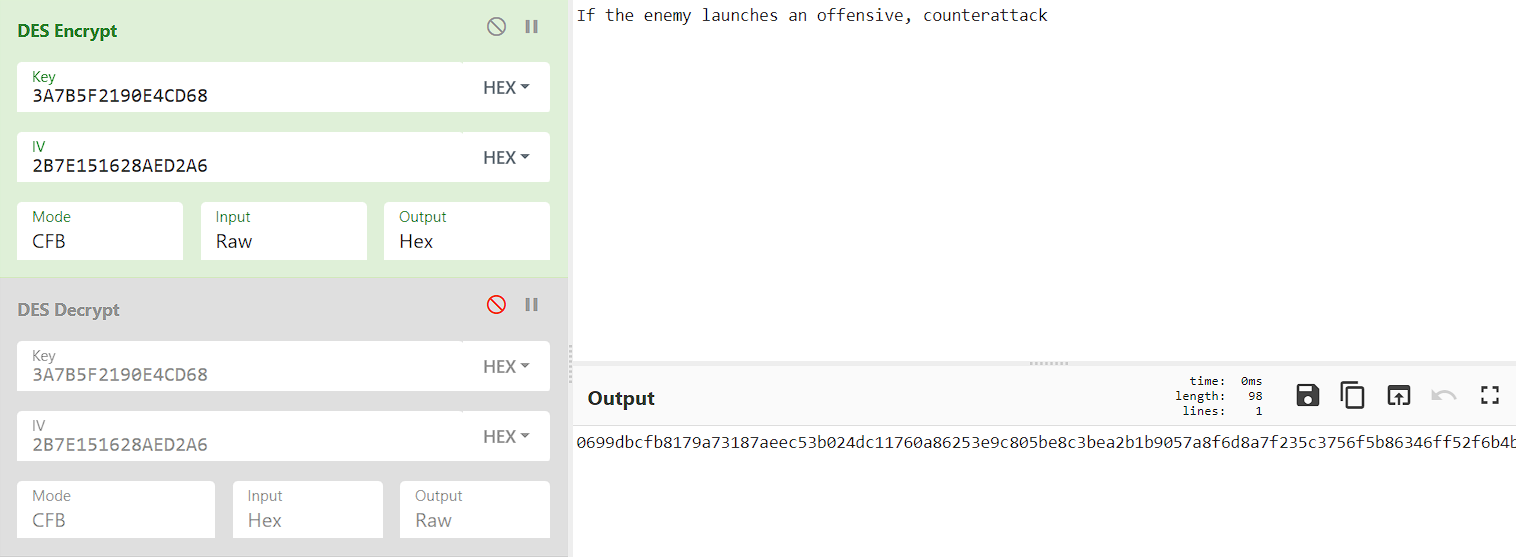
Дані шифрування:

Ключ - 3A7B5F2190E4CD68 в HEX форматі.

Вектор ініціалізації (IV) - 2B7E151628AED2A65 в HEX форматі.

Відкритий текст - If the enemy launches an offensive, counterattack

Шифротекст - 0699dbcfb8179a73187aeec53b024dc11760a86253e9c805be8c3bea2b1b9057a8f6d8a7f235c3756f5b86346ff52f6b4b в HEX форматі.



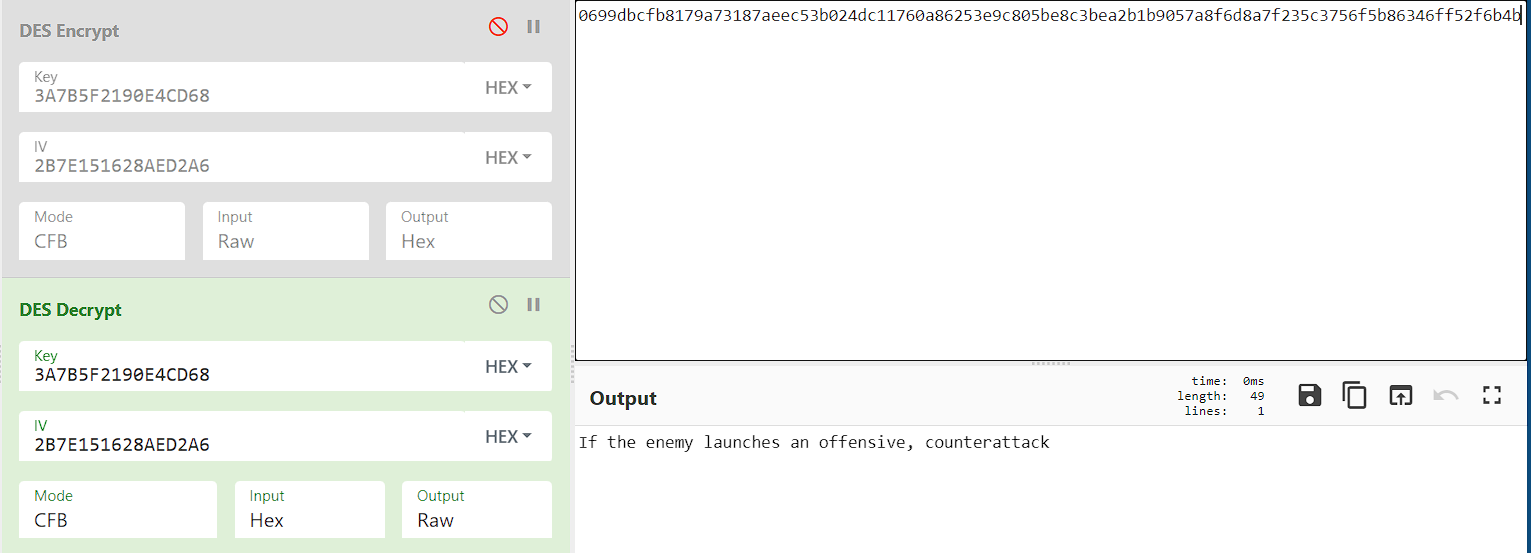
Дані розшифрування:

Ключ - 3A7B5F2190E4CD68 в HEX форматі.

Вектор ініціалізації (IV) - 2B7E151628AED2A65 в HEX форматі.

Шифротекст - 0699dbcfb8179a73187aeec53b024dc11760a86253e9c805be8c3bea2b1b9057a8f6d8a7f235c3756f5b86346ff52f6b4b в HEX форматі.

Розшифрований текст - If the enemy launches an offensive, counterattack



**Висновок:** У ході виконання завдання ми ознайомились і практично відпрацювали цикл шифрування алгоритмом DES за допомогою сайту cyberchef.io, розглянули його інтерфейс та за допомогою реалізованого на цьому сайті функціоналу відпрацювали шифрування у режимах ECB, CBC, CFB.