МІНІСТЕРСТВО ОБОРОНИ УКРАЇНИ

ВІЙСЬКОВИЙ ІНСТИТУТ ТЕЛЕКОМУНІКАЦІЙ ТА ІНФОРМАТИЗАЦІЇ

КАФЕДРА КІБЕРЗАХИСТУ

**ЗВІТ**

про виконання практичної роботи:

з дисципліни «Прикладна криптологія»

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

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

**Виконав:** курсант навчальної групи 314

ст. солдат \_\_\_\_\_\_\_\_\_\_\_\_\_Буховцев Г.І 21.04.2024

**Перевiрив:** викладач кафедри № 33

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

Київ – 2024

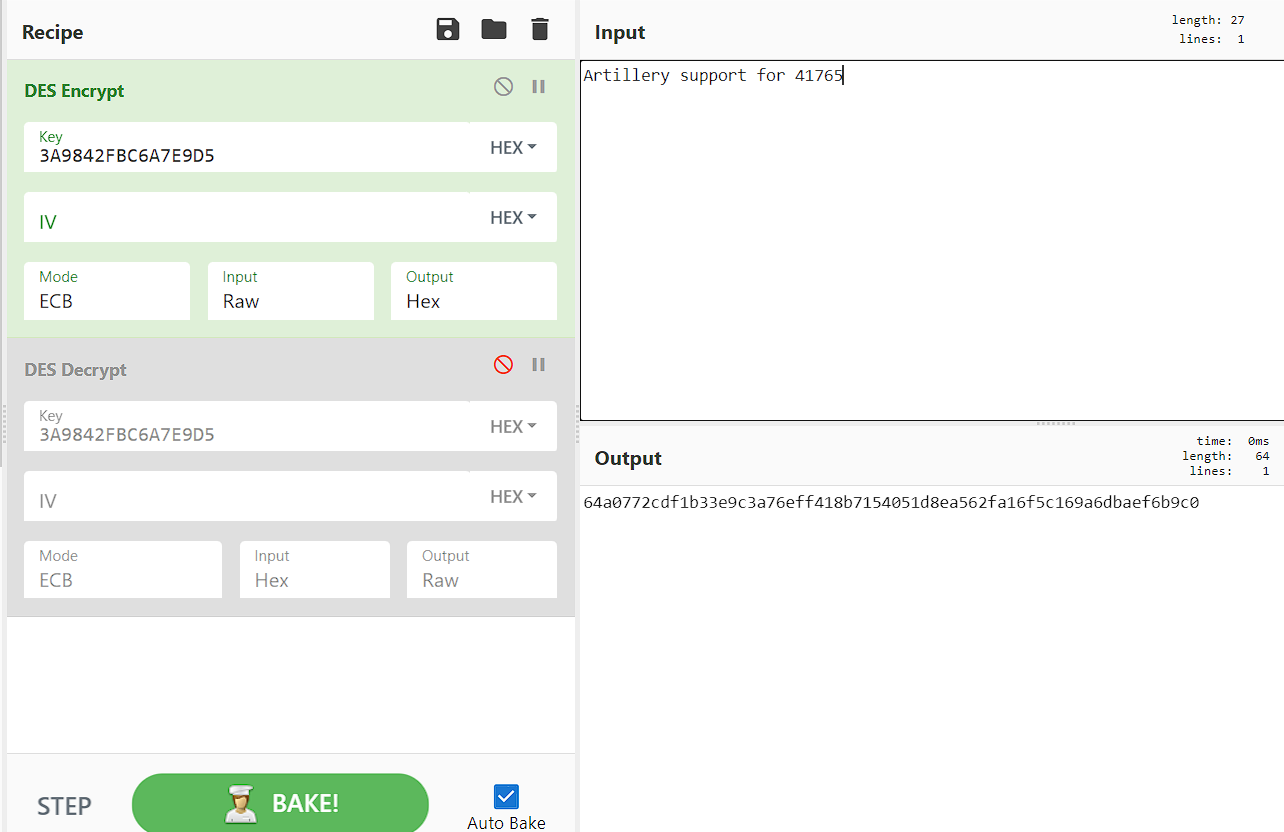
1. Виконати цикл шифрування алгоритмом DES у режимі ECB

Дані шифрування:

Ключ - 3A9842FBC6A7E9D5 в HEX форматі.

Відкритий текст - Artillery support for 41765

Шифротекст - 64a0772cdf1b33e9c3a76eff418b7154051d8ea562fa16f5c169a6dbaef6b9c0 в HEX форматі.

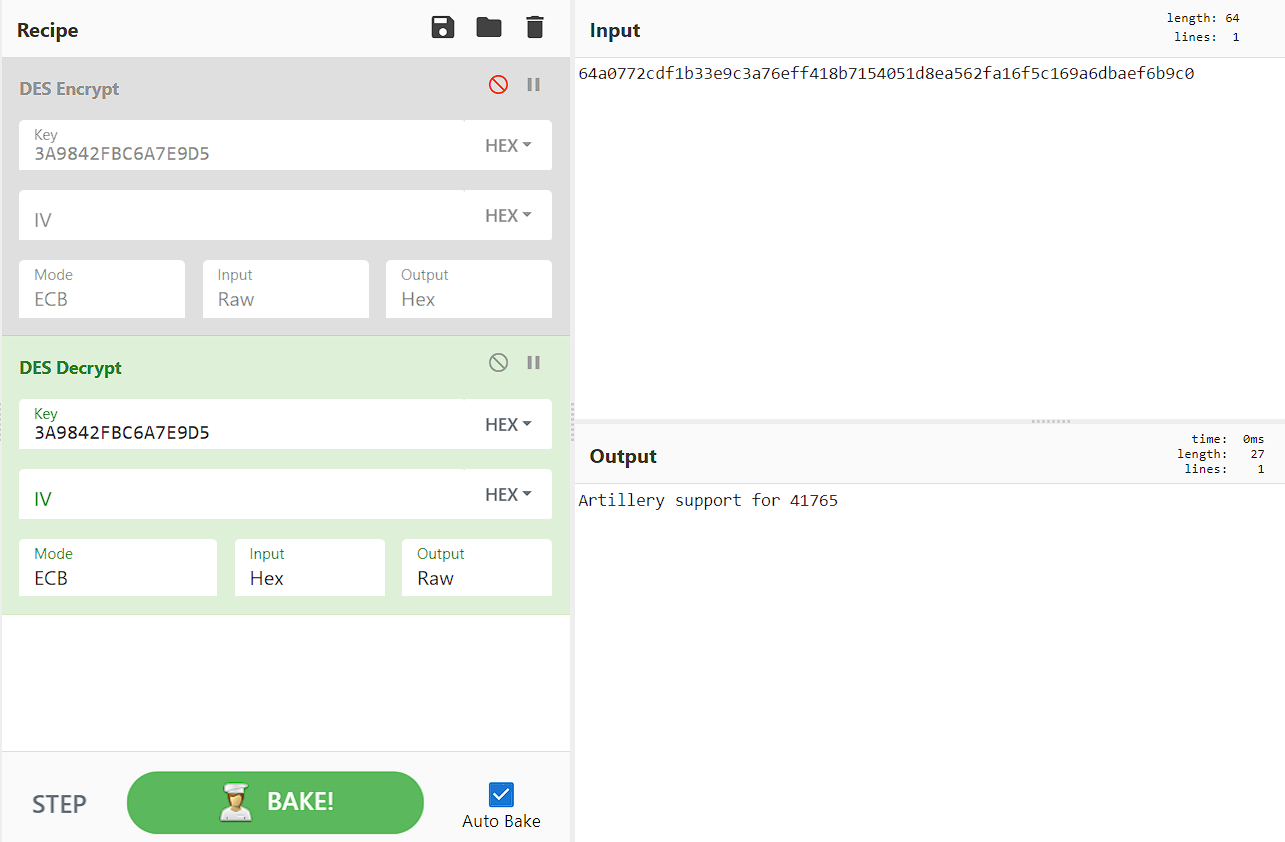


Дані розшифрування:

Ключ - 3A9842FBC6A7E9D5 в HEX форматі.

Шифротекст - 64a0772cdf1b33e9c3a76eff418b7154051d8ea562fa16f5c169a6dbaef6b9c0

Розшифрований текст - Artillery support for 41765



1. Виконати цикл шифрування алгоритмом DES у режимі CBC

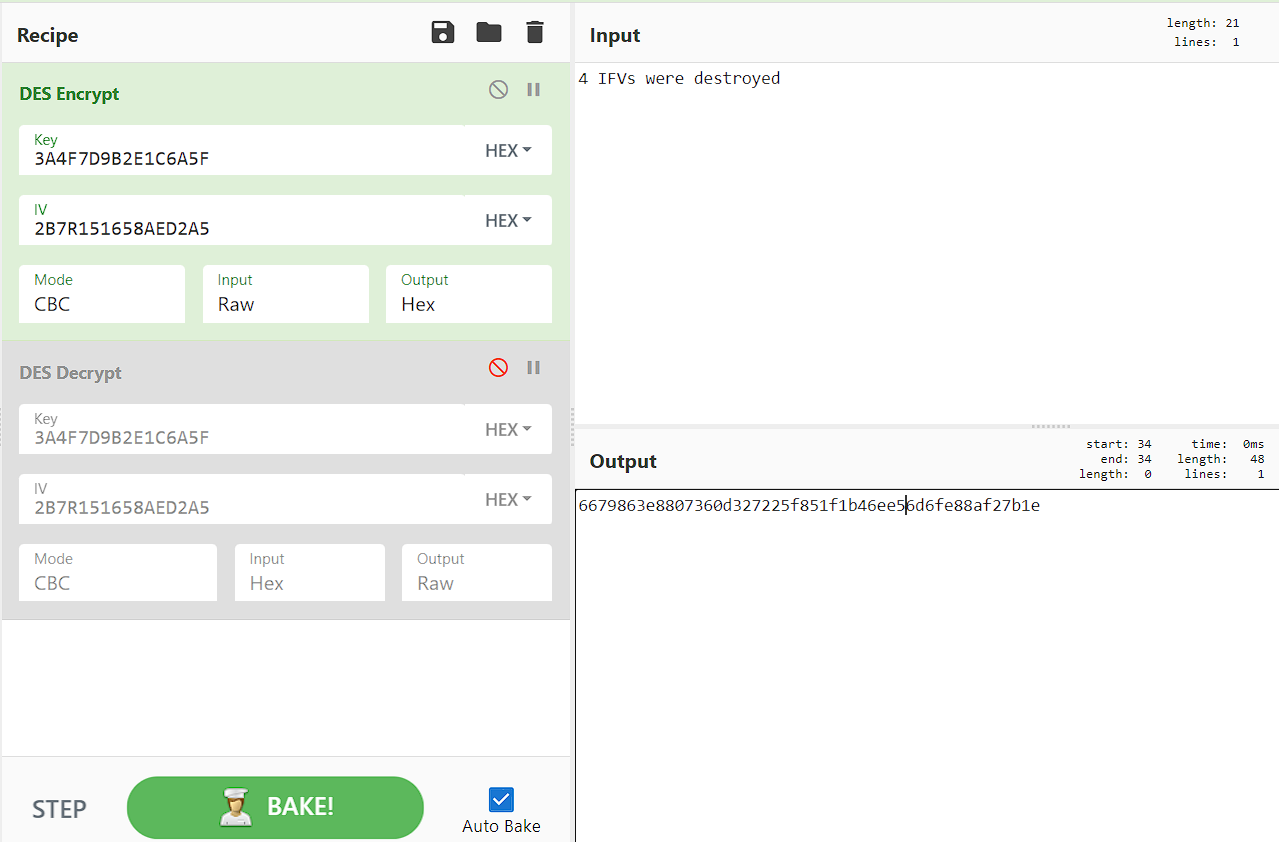
Дані шифрування:

Ключ - 3A4F7D9B2E1C6A5F в HEX форматі.

Вектор ініціалізації (IV) - 2B7R151658AED2A5 в HEX форматі.

Відкритий текст - 4 IFVs were destroyed

Шифротекст - 6679863e8807360d327225f851f1b46ee56d6fe88af27b1e в HEX форматі.



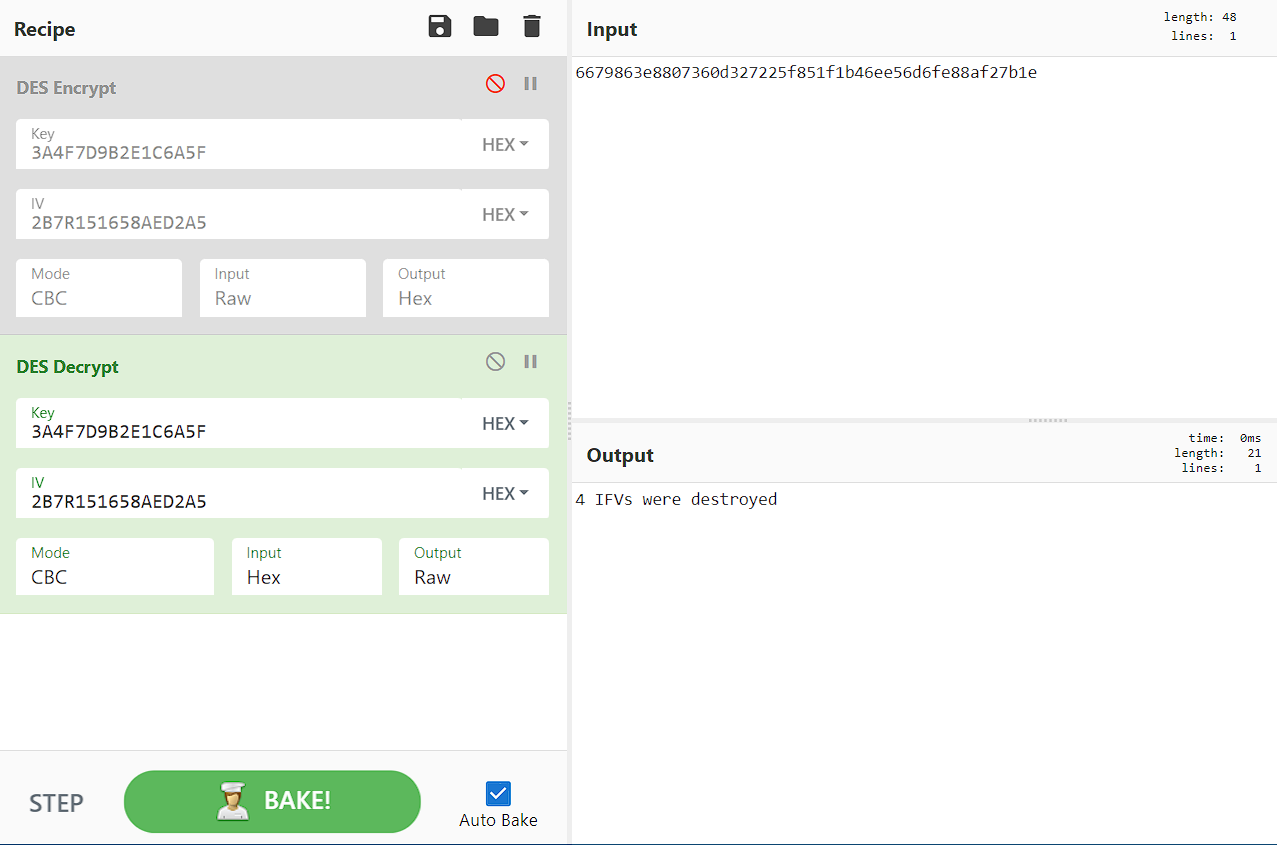
Дані розшифрування:

Ключ - 3A4F7D9B2E1C6A5F в HEX форматі.

Вектор ініціалізації (IV) - 2B7R151658AED2A5 в HEX форматі.

Шифротекст - 6679863e8807360d327225f851f1b46ee56d6fe88af27b1e в HEX форматі.

Розшифрований текст - 4 IFVs were destroyed



1. Виконати цикл шифрування алгоритмом DES у режимі CFB

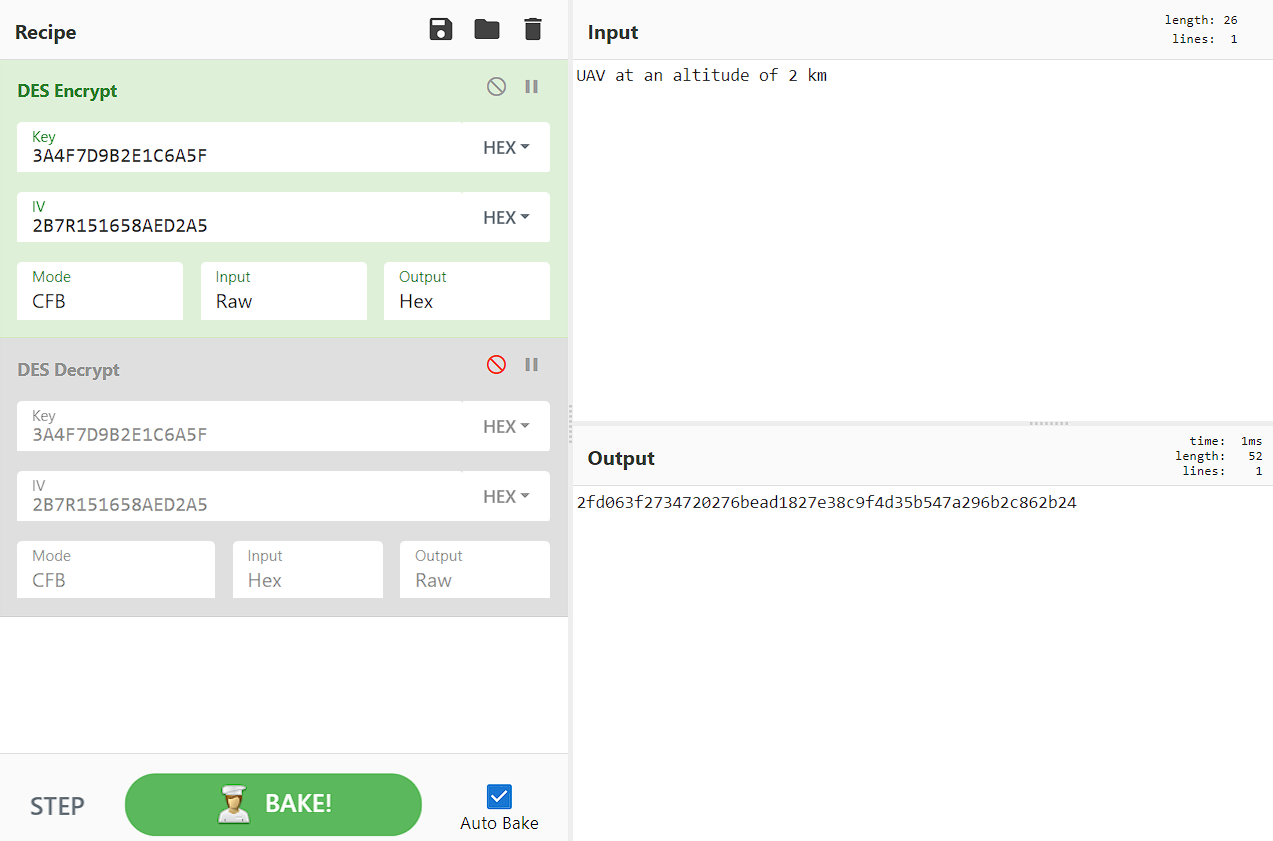
Дані шифрування:

Ключ - 3A4F7D9B2E1C6A5F в HEX форматі.

Вектор ініціалізації (IV) - 2B7R151658AED2A5 в HEX форматі.

Відкритий текст - UAV at an altitude of 2 km

Шифротекст - 2fd063f2734720276bead1827e38c9f4d35b547a296b2c862b24 в HEX форматі.



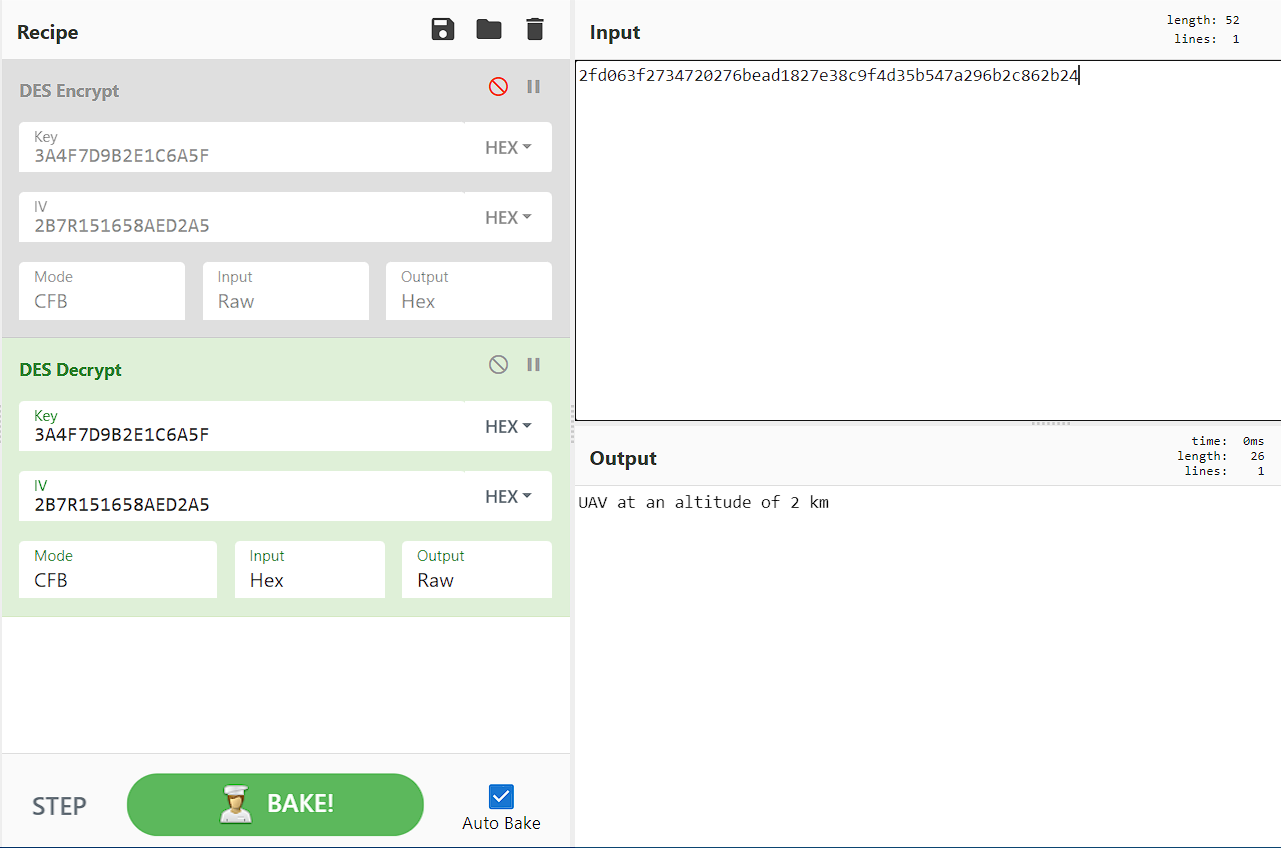
Дані розшифрування:

Ключ - 3A4F7D9B2E1C6A5F в HEX форматі.

Вектор ініціалізації (IV) - 2B7R151658AED2A5 в HEX форматі.

Шифротекст - 2fd063f2734720276bead1827e38c9f4d35b547a296b2c862b24 в HEX форматі.

Розшифрований текст - UAV at an altitude of 2 km



**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.