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

солдат \_\_\_\_\_\_\_\_\_\_\_\_\_Янковський О.О 20.04.2024

**Перевiрив:** викладач кафедри № 33

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

Київ – 2024

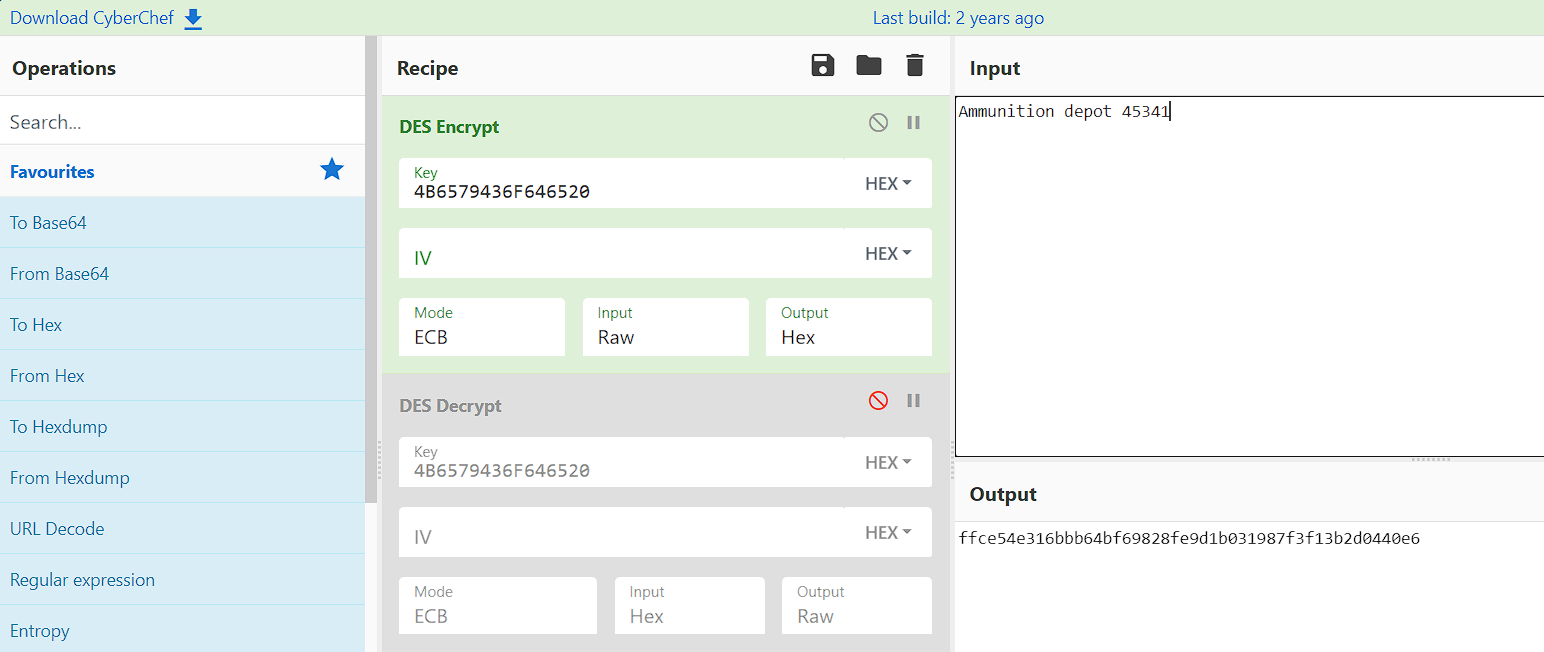
1. Виконати цикл шифрування алгоритмом DES у режимі ECB

Дані шифрування:

Ключ - 4B6579436F646520 в HEX форматі.

Відкритий текст - Ammunition depot 45341

Шифротекст - ffce54e316bbb64bf69828fe9d1b031987f3f13b2d0440e6 в HEX форматі.

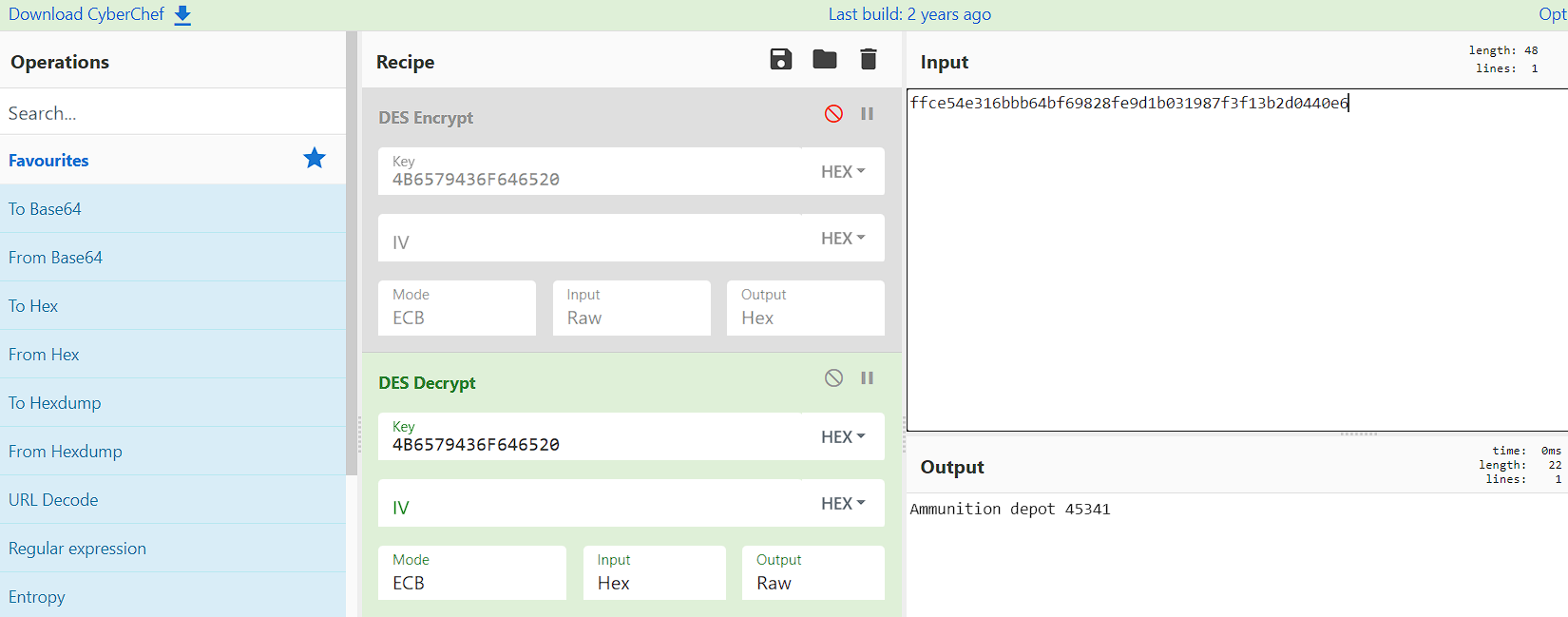


Дані розшифрування:

Ключ - 4B6579436F646520 в HEX форматі.

Шифротекст - ffce54e316bbb64bf69828fe9d1b031987f3f13b2d0440e6

Відкритий текст - Ammunition depot 45341



1. Виконати цикл шифрування алгоритмом DES у режимі CBC

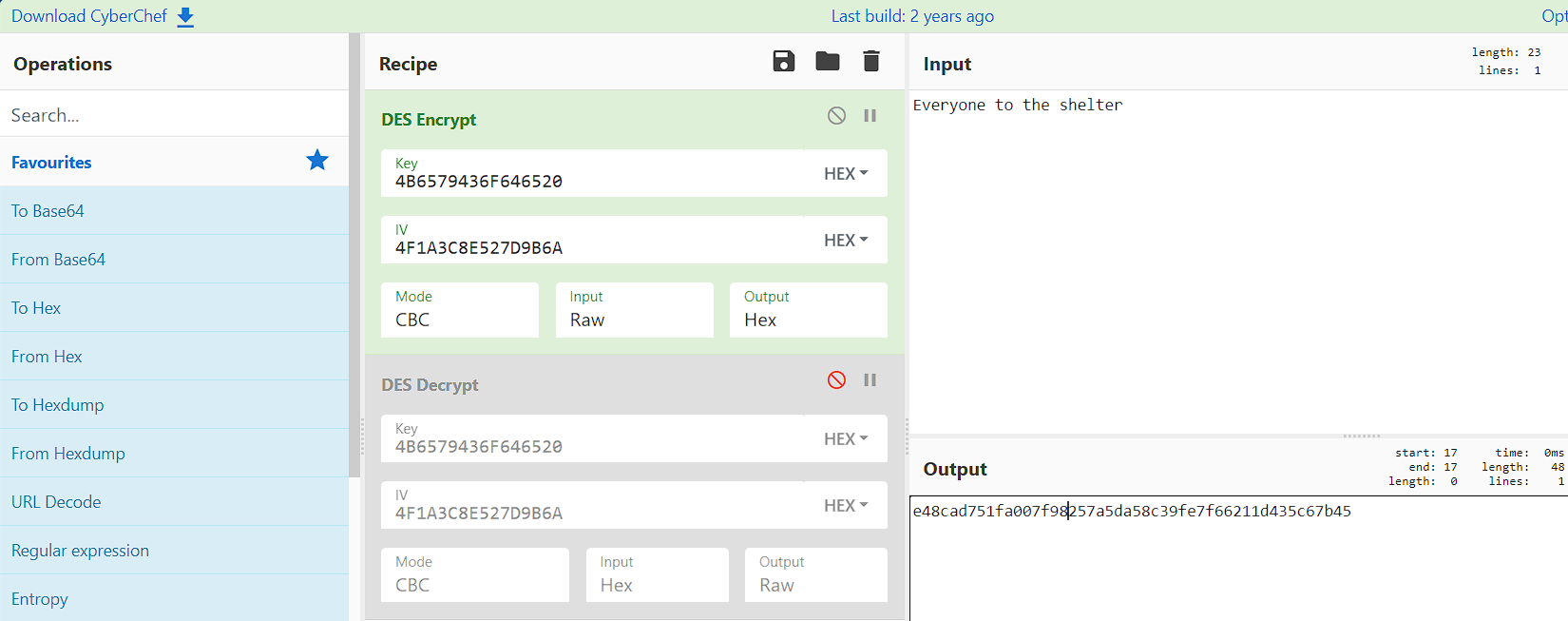
Дані шифрування:

Ключ - 4B6579436F646520 в HEX форматі.

Вектор ініціалізації (IV) - 4F1A3C8E527D9B6A в HEX форматі.

Відкритий текст - Everyone to the shelter

Шифротекст - e48cad751fa007f98257a5da58c39fe7f66211d435c67b45 в HEX форматі.



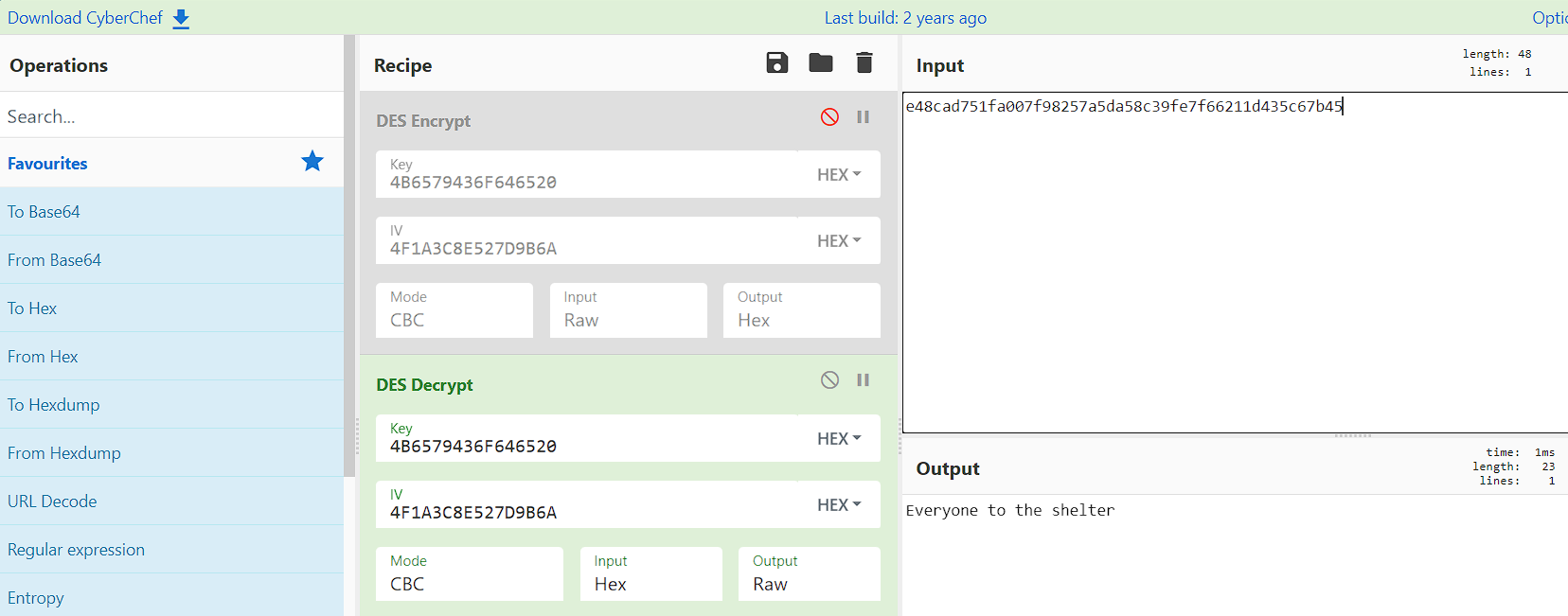
Дані розшифрування:

Ключ - 4B6579436F646520 в HEX форматі.

Вектор ініціалізації (IV) - 4F1A3C8E527D9B6A в HEX форматі.

Шифротекст - e48cad751fa007f98257a5da58c39fe7f66211d435c67b45 в HEX форматі.

Відкритий текст - Everyone to the shelter



1. Виконати цикл шифрування алгоритмом DES у режимі CFB

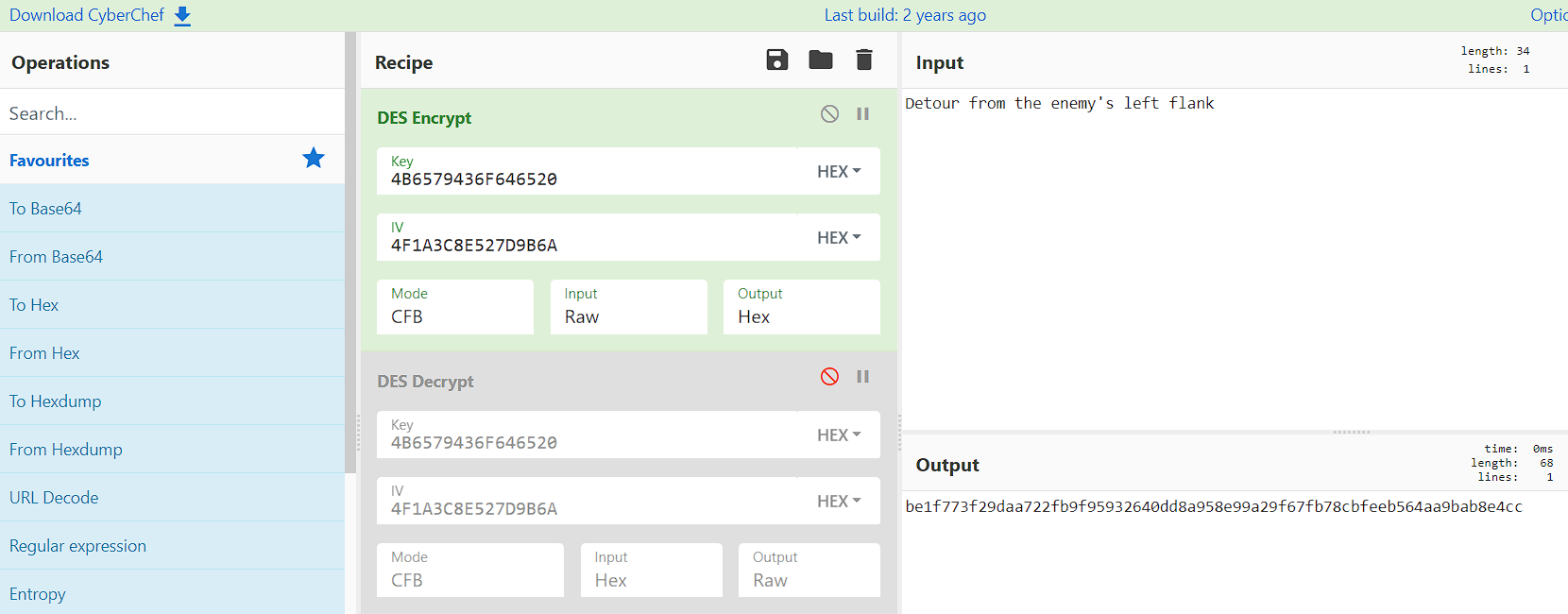
Дані шифрування:

Ключ - 4B6579436F646520 в HEX форматі.

Вектор ініціалізації (IV) - 4F1A3C8E527D9B6A в HEX форматі.

Відкритий текст - Detour from the enemy's left flank

Шифротекст - be1f773f29daa722fb9f95932640dd8a958e99a29f67fb78cbfeeb564aa9bab8e4cc в HEX форматі.

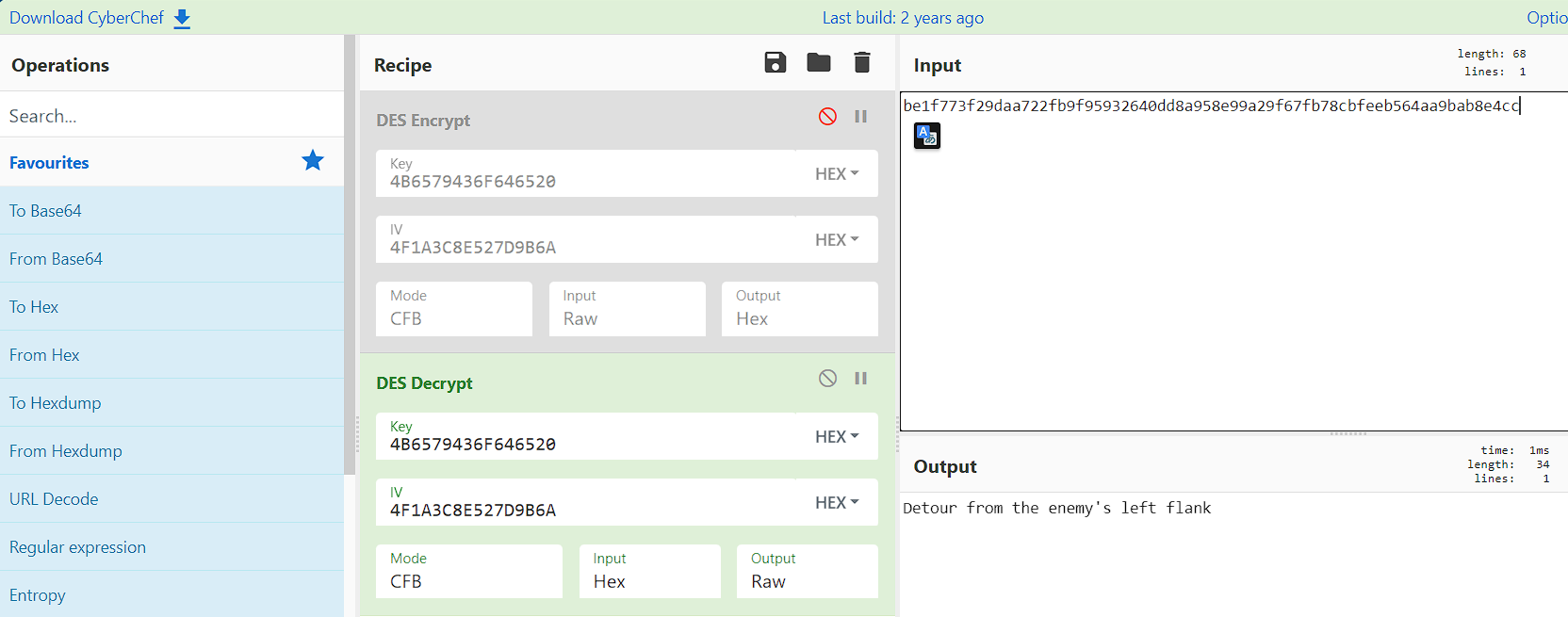


Дані розшифрування:

Ключ - 4B6579436F646520 в HEX форматі.

Вектор ініціалізації (IV) - 4F1A3C8E527D9B6A в HEX форматі.

Шифротекст - be1f773f29daa722fb9f95932640dd8a958e99a29f67fb78cbfeeb564aa9bab8e4cc в HEX форматі.



**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.