МІНІСТЕРСТВО ОБОРОНИ УКРАЇНИ

ВІЙСЬКОВИЙ ІНСТИТУТ ТЕЛЕКОМУНІКАЦІЙ ТА ІНФОРМАТИЗАЦІЇ

КАФЕДРА КІБЕРЗАХИСТУ

ЗВІТ

про виконання практичної роботи:

з дисципліни «Прикладна криптологія»

Заняття № 3/19. Дослідження криптостійкості DES

РОБОТА З WEB-ДОДАТКОМ CYBERCHEF.IO

Виконав: курсант навчальної групи 314

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

24.04.2024

Перевiрив: викладач кафедри № 33

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

Київ – 2024



Висновок:Після аналізу таблиці можна зробити кілька висновків:

Заміна першої та останньої букв у текстах впливає на кінцевий шифротекст у залежності від типу шифрування і режиму. Наприклад, у режимі ECB заміна першої букви у відкритому тексті призведе до повної зміни блока шифрування, тому весь блок шифрування буде різним. У

режимах CBC, CFB, OFB та CTR зміна першої букви вплине лише на відповідний блок шифрування.

Отже, таблиця демонструє різні результати шифрування в різних режимах та різницю у величині шифртексту в залежності від режиму шифрування та довжини відкритого тексту.