МІНІСТЕРСТВО ОБОРОНИ УКРАЇНИ

ВІЙСЬКОВИЙ ІНСТИТУТ ТЕЛЕКОМУНІКАЦІЙ ТА ІНФОРМАТИЗАЦІЇ

КАФЕДРА КІБЕРЗАХИСТУ

**ЗВІТ**

про виконання практичної роботи:

з дисципліни «Прикладна криптологія»

Дата 20.04.2024

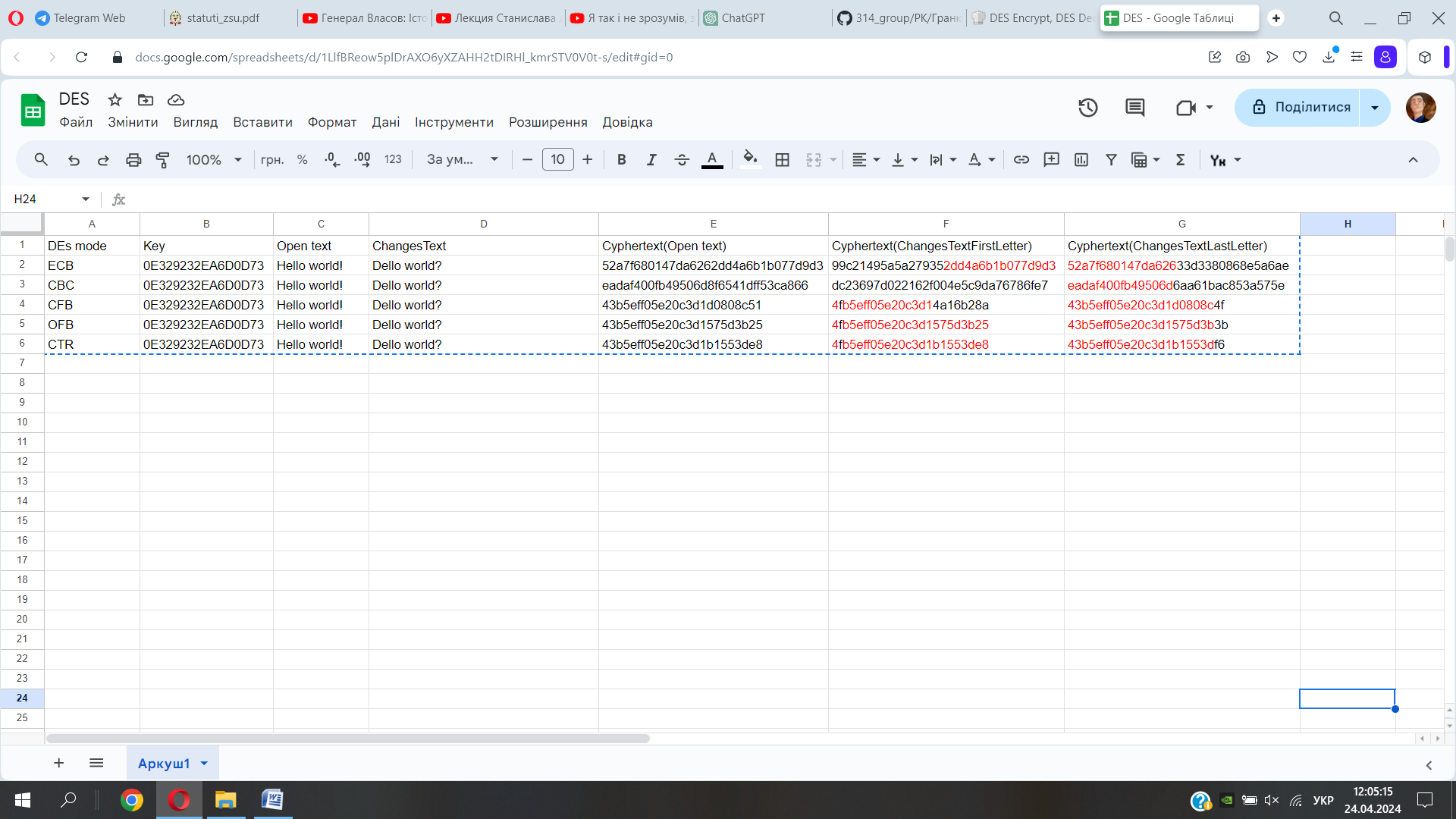
**Виконав:** курсант навчальної групи 314

солдат \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ ГРАНКІН П.Т.

**Перевiрив:**старший викладач кафедри № 33

капітан\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ ПРИЙМА О.О.

Київ – 2024



На малюнку червоний текст у рядку означає одинакові символи шифротексту зі зміненою першою або останньою літерою та шифротексту з відкритим текстом.

Висновок:

1) ECB – при зміні першої літери відкритого тексту у шифротексті змінюються перші 16 символів, якщо змінити останню літеру відкритого тексту, відповідно, зміняться 16 останніх символів шифротексту. Це відбувається тому що в ECB використовується блокова шифрація по 16 бітів. Тобто ECB також можна визначити якщо шифротекст кратний 16-ти.

2) CBC - У режимі CBC кожен блок відкритого тексту спочатку комбінується з попереднім шифрованим блоком перед шифруванням. Це призводить до того, що зміна навіть одного біта в вхідному тексті вплине на всі наступні блоки шифротексту. Це робить CBC більш стійким до атак, які використовують шаблони.

3) CFB та OFB - У цих режимах блоки шифруються незалежно один від одного, але є зміщення (feedback), що додається до наступного блоку для створення шифротексту. Таким чином, зміни в відкритому тексті можуть розповсюджуватися далі в шифротексті, але не впливають на розшифрування попередніх блоків. Вони менш схильні до падіння в пастку шаблонів, якщо відбуваються невеликі зміни в відкритому тексті.

4) CTR - У режимі CTR кожен блок шифрується шляхом комбінування його зі значенням лічильника, що інкрементується для кожного блоку. Це дозволяє паралельне шифрування та розшифрування, а також надає можливість використання криптографічно стійкого псевдовипадкового числа як лічильника. Як результат, зміни в відкритому тексті впливають тільки на конкретні блоки шифротексту, але можуть змінювати його в несподіваний спосіб через використання лічильника.