**МІНІСТЕРСТВО ОБОРОНИ УКРАЇНИ**

**ВІЙСЬКОВИЙ ІНСТИТУТ ТЕЛЕКОМУНІКАЦІЙ ТА ІНФОРМАТИЗАЦІЇ**

КАФЕДРА КІБЕРБЕЗПЕКИ

**ЗВІТ**

про виконання практичної роботи:

з дисципліни «Прикладна криптологія 2»

**СТАНДАРТ ШИФРУВАННЯ ДАНИХ DES**

**Виконав:** курсант 314 навчальної групи

ст. солдат \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Є.КОНДРАТЕНКО

.04.2024

**Перевiрив:** викладач кафедри № 33

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

.04.2024

Київ – 2024

**Стандарт шифрування даних (DES)** — це блоковий шифр із довжиною 56-бітного ключа, який відіграв значну роль у безпеці даних .Стандарт шифрування даних (DES) був визнаний вразливим до дуже потужних атак, тому популярність DES дещо знизилася.

DES — це блоковий шифр, який шифрує дані в блоках розміром 64 бітикожен, що означає, що 64 біти звичайного тексту надходять як вхідні дані для DES, який створює 64 біти зашифрованого тексту. Для шифрування та [дешифрування](https://www.geeksforgeeks.org/difference-between-encryption-and-decryption/)використовуються той самий алгоритм і ключ з незначними відмінностями. Довжина ключа становить 56 біт. 

**1. Electronic Code Book (ЕСВ)**

**Режим електронна кодова книга**

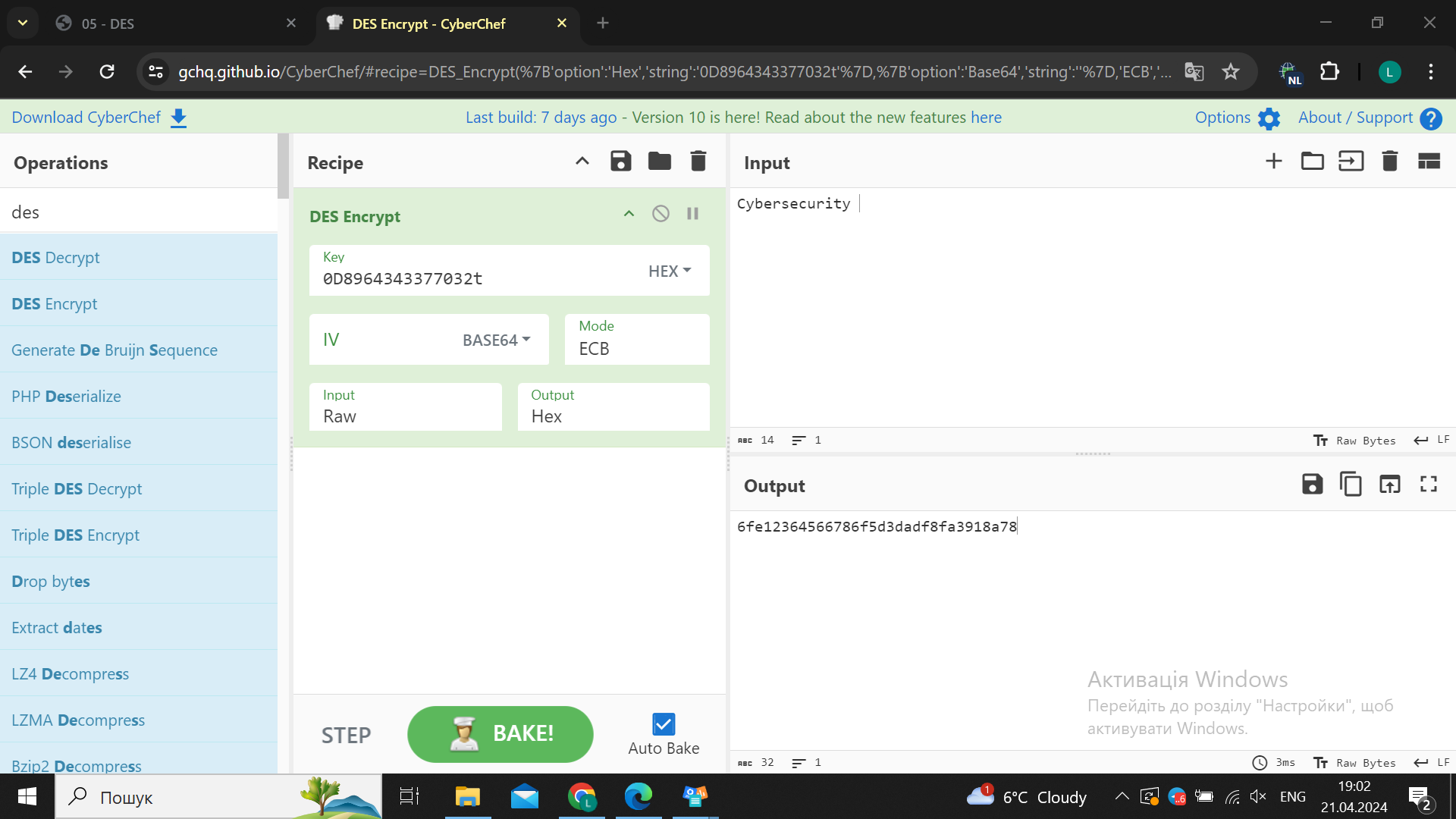
Звичайне використання DES як блокового шифру. Текст, що шифрується, розбивається на блоки, при цьому, кожен блок шифрується окремо, не взаємодіючи з іншими блоками.

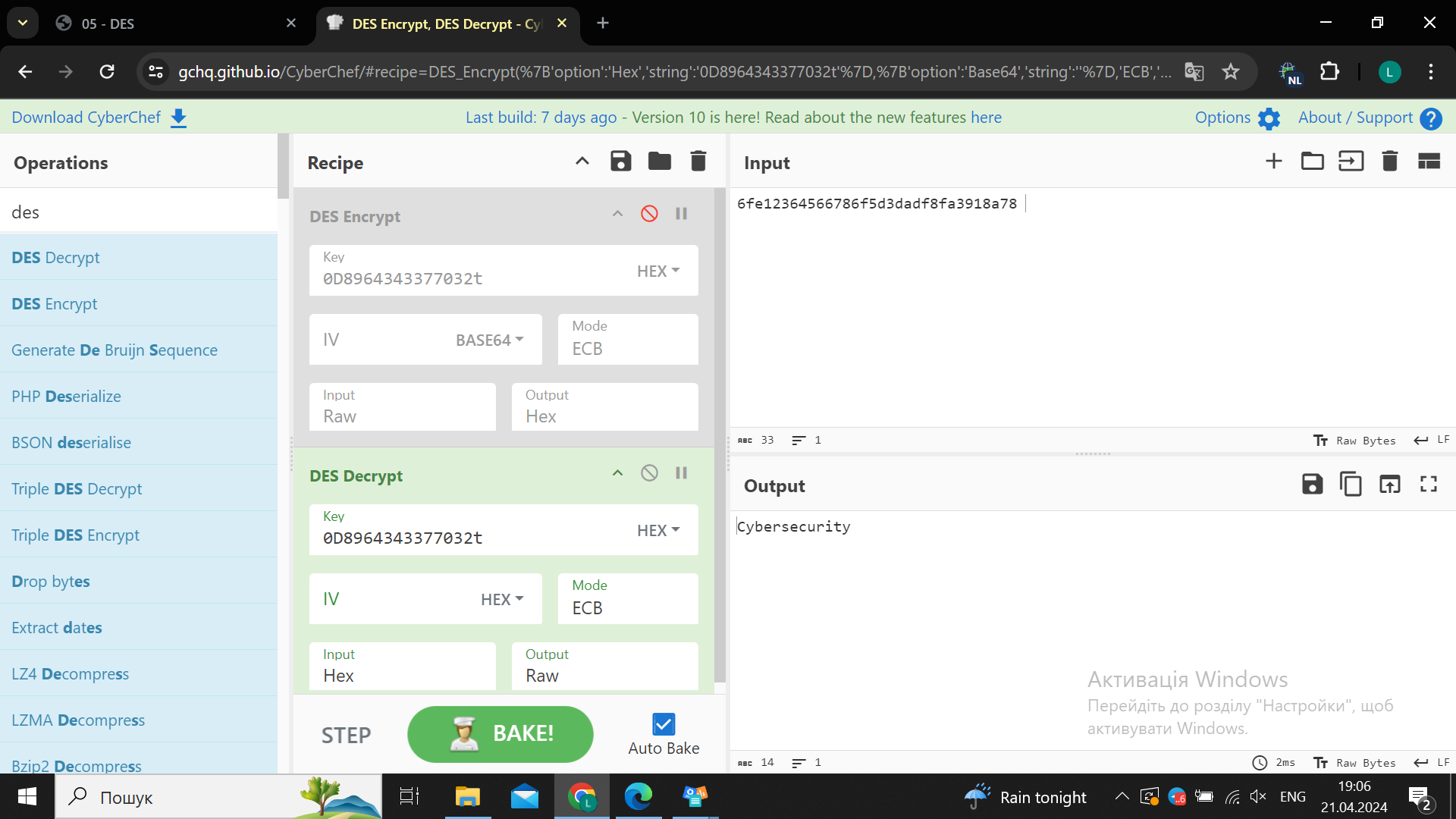
**KEY(HEX):** 0D8964343377032t

**ВТ:** *Cybersecurity*

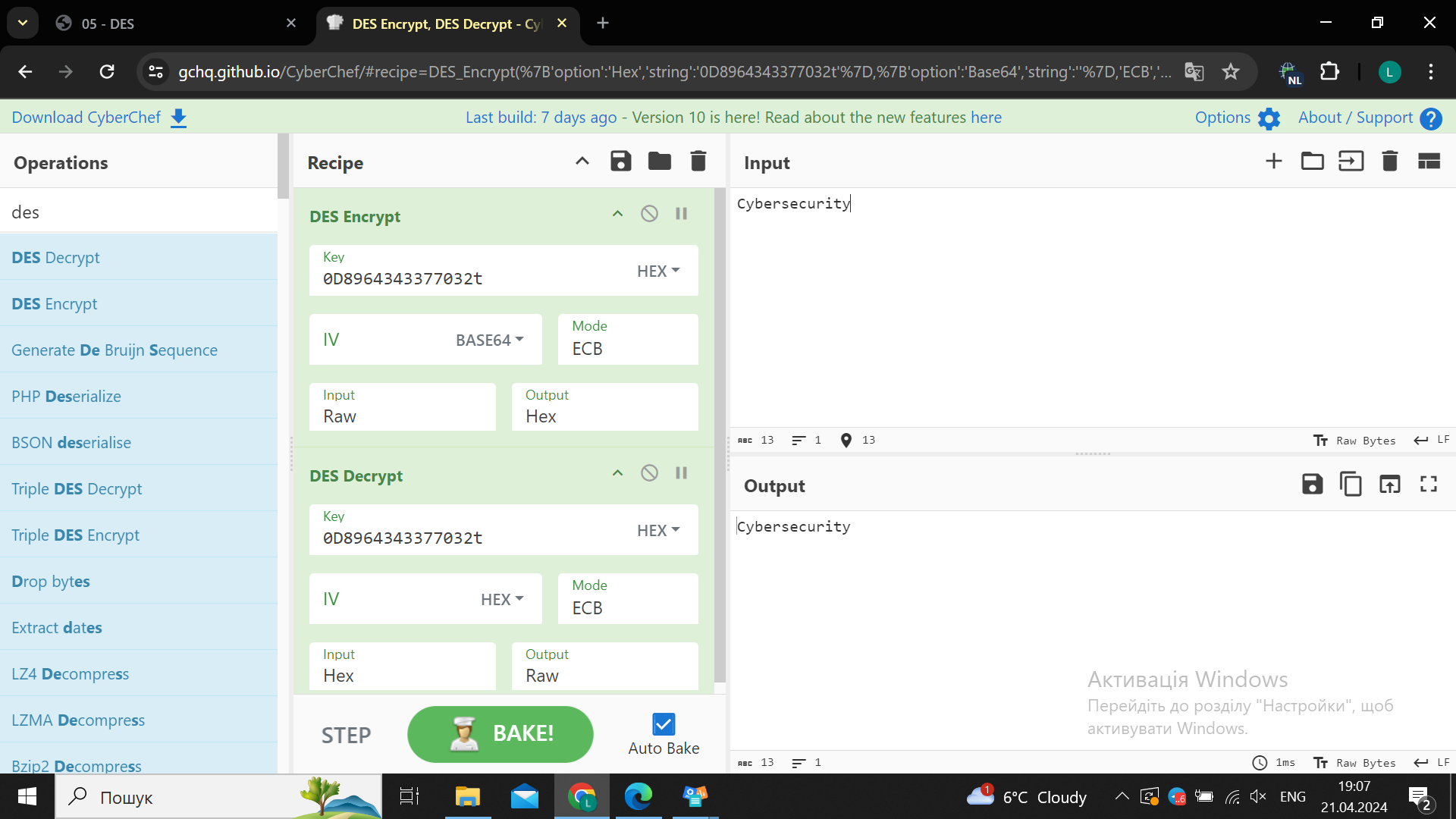
**ШТ:** 6fe12364566786f5d3dadf8fa3918a78

***ENCRYPT:***

***DECRYPT:***



***IN BLOCK:***



**2.Cipher Block Chaining ( СВС )**

**Режим зчеплення блоків**

В цьому режимі кожен блок відкритого тексту з'єднується з попереднім блоком перед шифруванням.

Переваги режиму CBC включають високий рівень безпеки, особливо при правильному виборі випадкового IV. Однак цей режим не підтримує паралельне шифрування/розшифрування блоків, оскільки кожен блок залежить від попереднього. Також він вимагає, щоб кожен блок був унікальним для досягнення надійного шифрування.

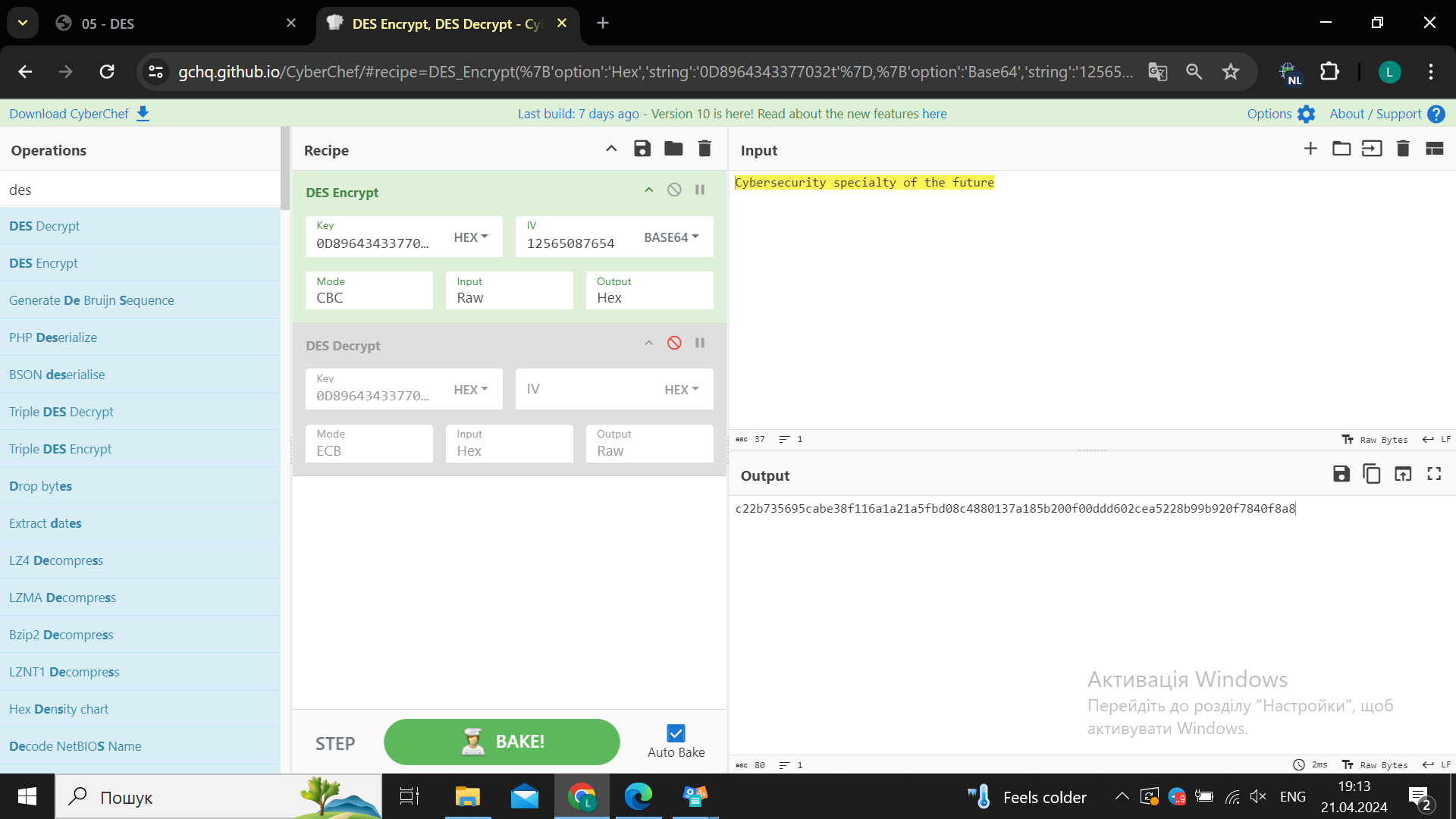
**KEY(HEX):** 0D8964343377032t

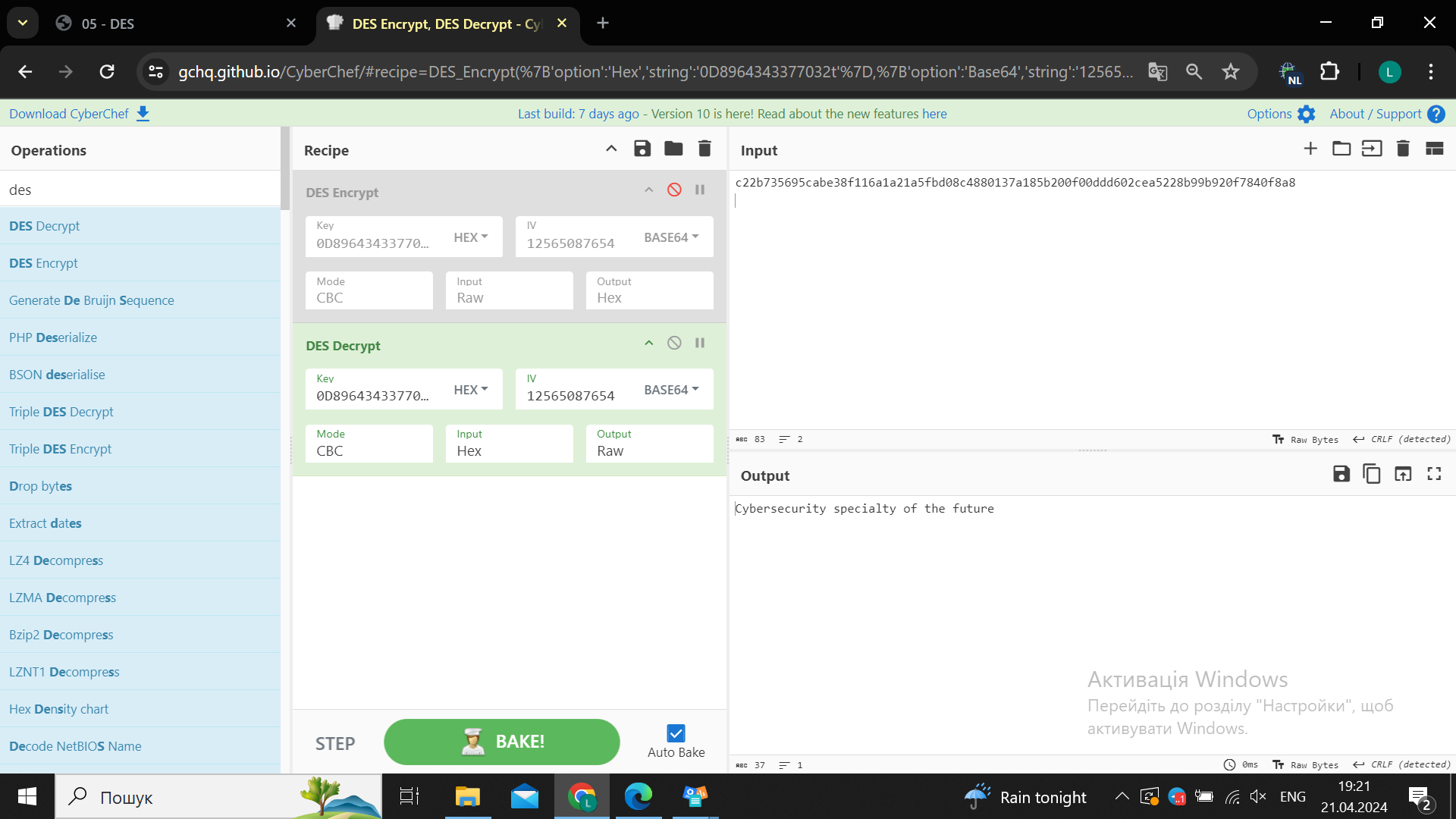
**IV(BASE64)** 12565087654

**ВТ:** *Cybersecurity* specialty of the future

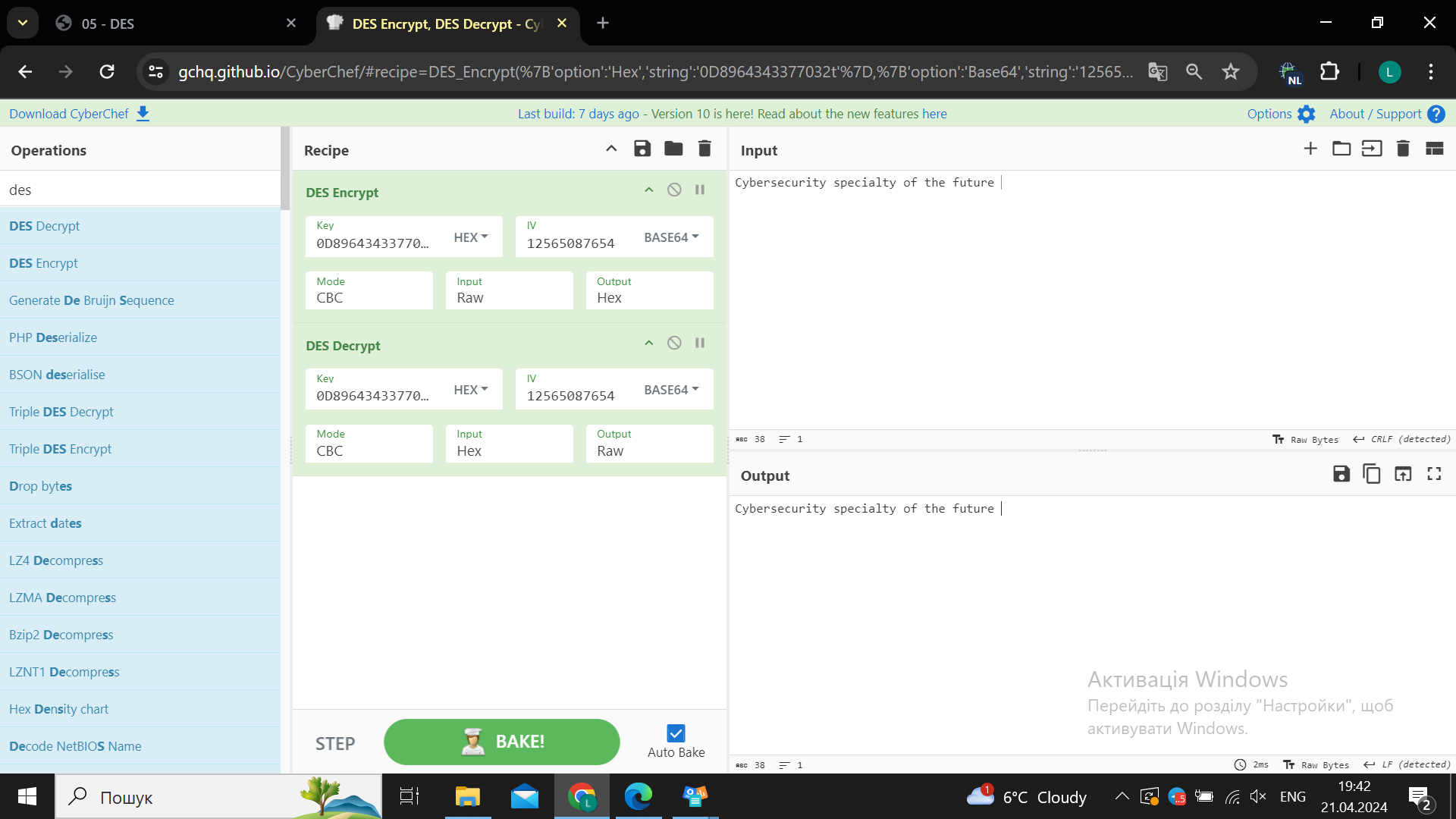
**ШТ:c22b735695cabe38f116a1a21a5fbd08c4880137a185b200f00ddd602cea5228b99b920f7840f8a8**

***ENCRYPT:***

 ***DECRYPT:***



***IN BLOCK:***



**3. Cipher Feed Back (CFB)**

**Режим зворотного зв'язку за шифротекстом**

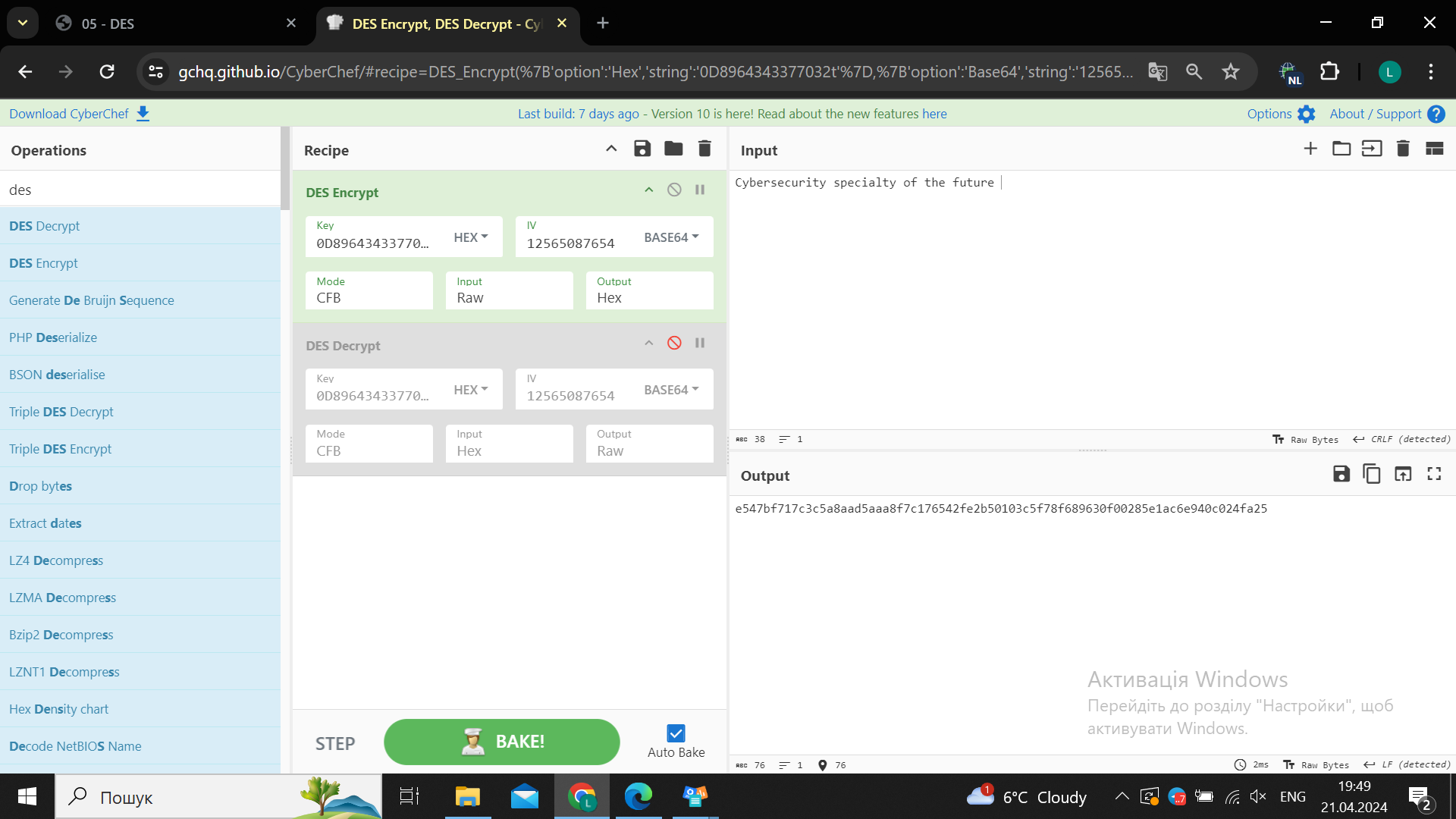
особливість полягає в тому, що кожен блок відкритого тексту комбінується з попереднім зашифрованим блоком перед тим, як він буде зашифрований. Однак він не підтримує паралельне шифрування/розшифрування блоків, оскільки кожен блок залежить від попереднього. Також вимагає, щоб кожен блок був унікальним для досягнення надійного шифрування.

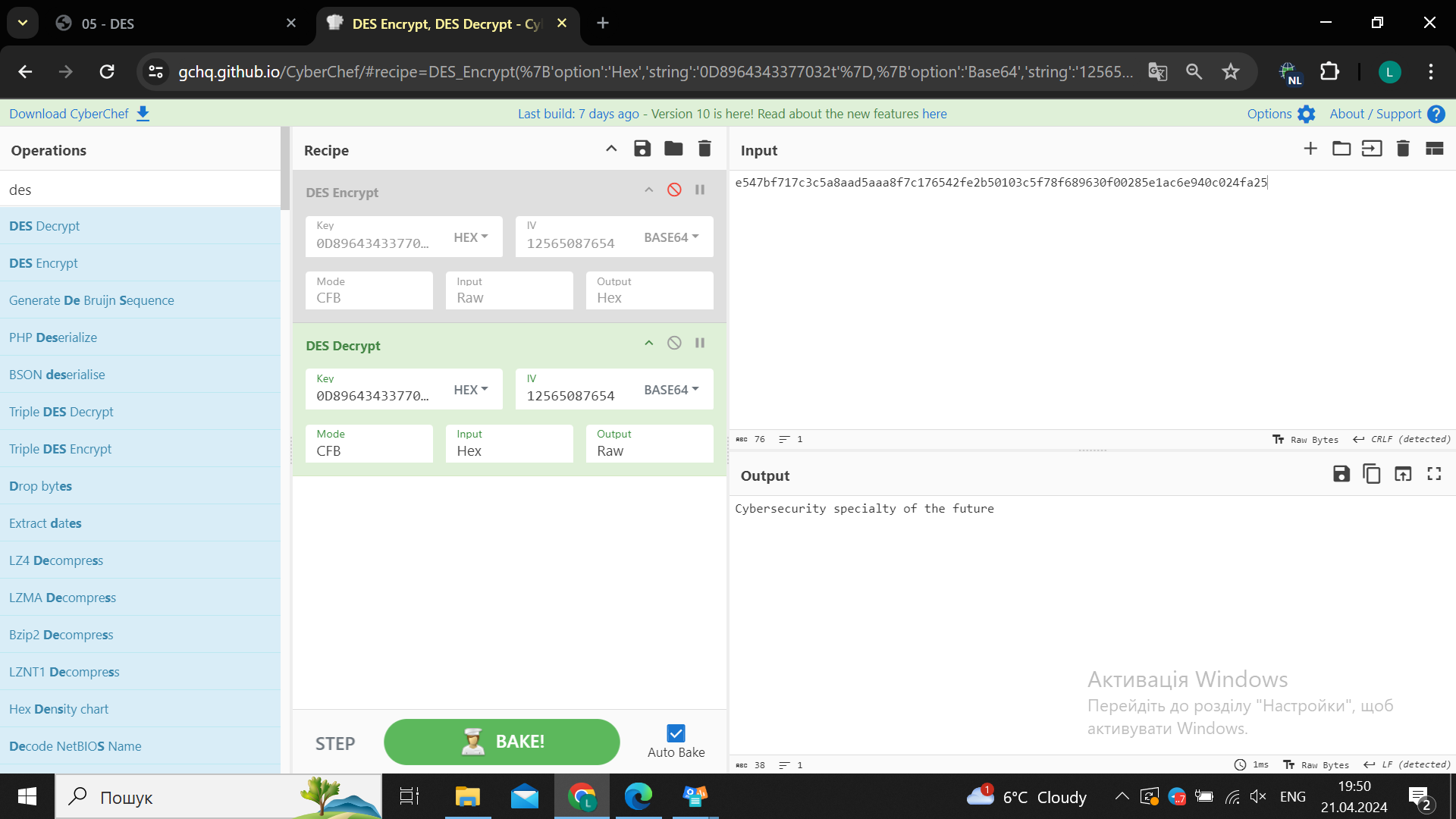
**KEY(HEX):** 0D8964343377032t

**ВТ:** *Cybersecurity* specialty of the future

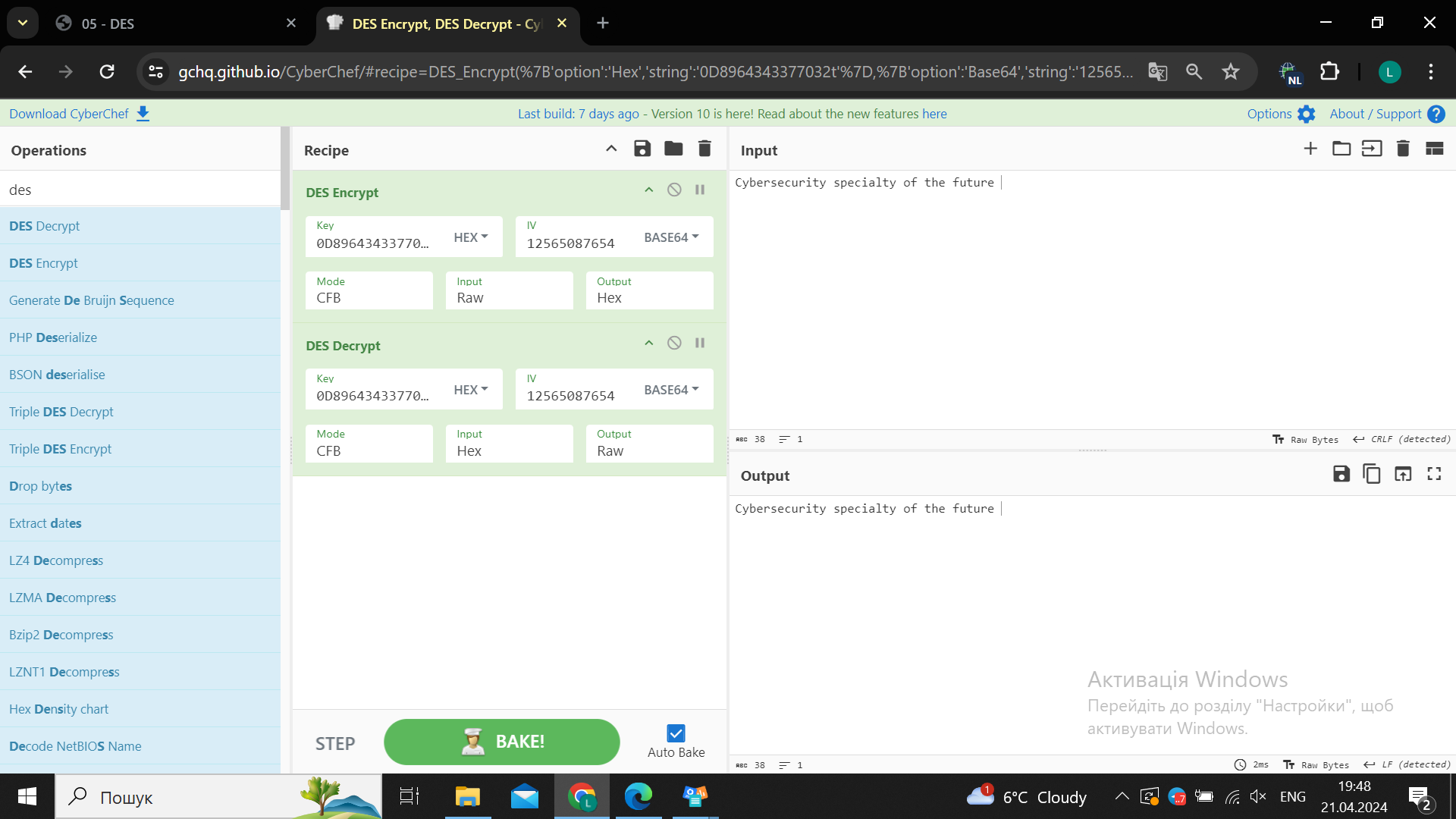
**ШТ:*e547bf717c3c5a8aad5aaa8f7c176542fe2b50103c5f78f689630f00285e1ac6e940c024fa25***

***ENCRYPT:***



***DECRYPT:***

***IN BLOCK:***



**3. Output Feed Back (OFB )**

**Режим зворотного зв'язку після виходу**

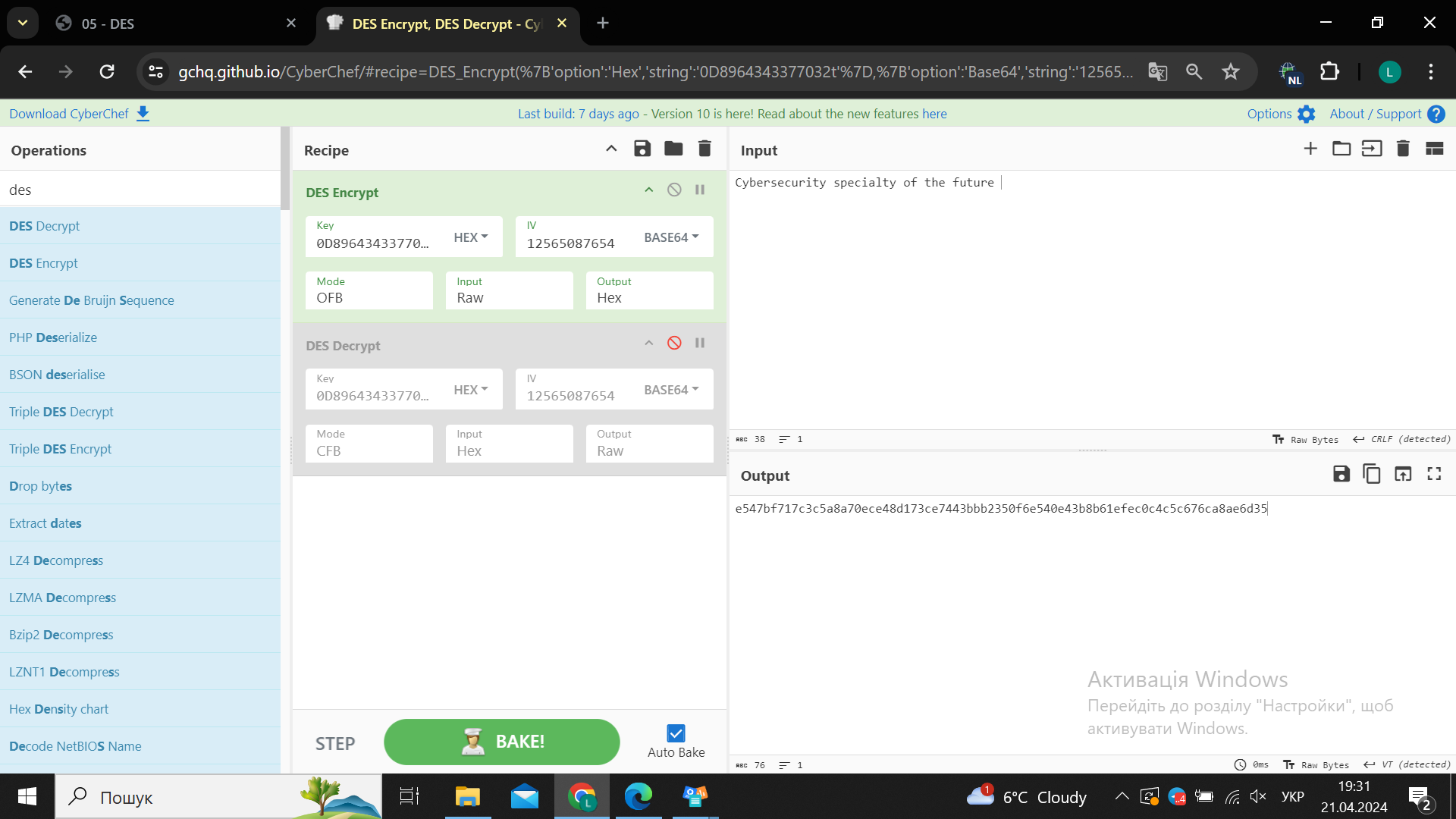
У цьому режимі блок шифртексту генерується не шляхом простого зашифрування відкритого тексту, а шляхом шифрування псевдовипадкового потоку бітів, що називається рекурсивною послідовністю, а потім змішується з відкритим текстом, щоб отримати шифртекст.

Основна перевага режиму OFB полягає в тому, що він не вимагає обертання блоків в процесі декодування, що дозволяє ефективно застосовувати його для потокового шифрування. Він також дозволяє паралельну роботу для шифрування та розшифрування даних. Однак, важливо зазначити, що якщо тільки один біт псевдовипадкової послідовності втрачений або змінений, це може призвести до зміни або втрати відповідного біта у відкритому тексті, що може призвести до помилок у даних при декодуванні.

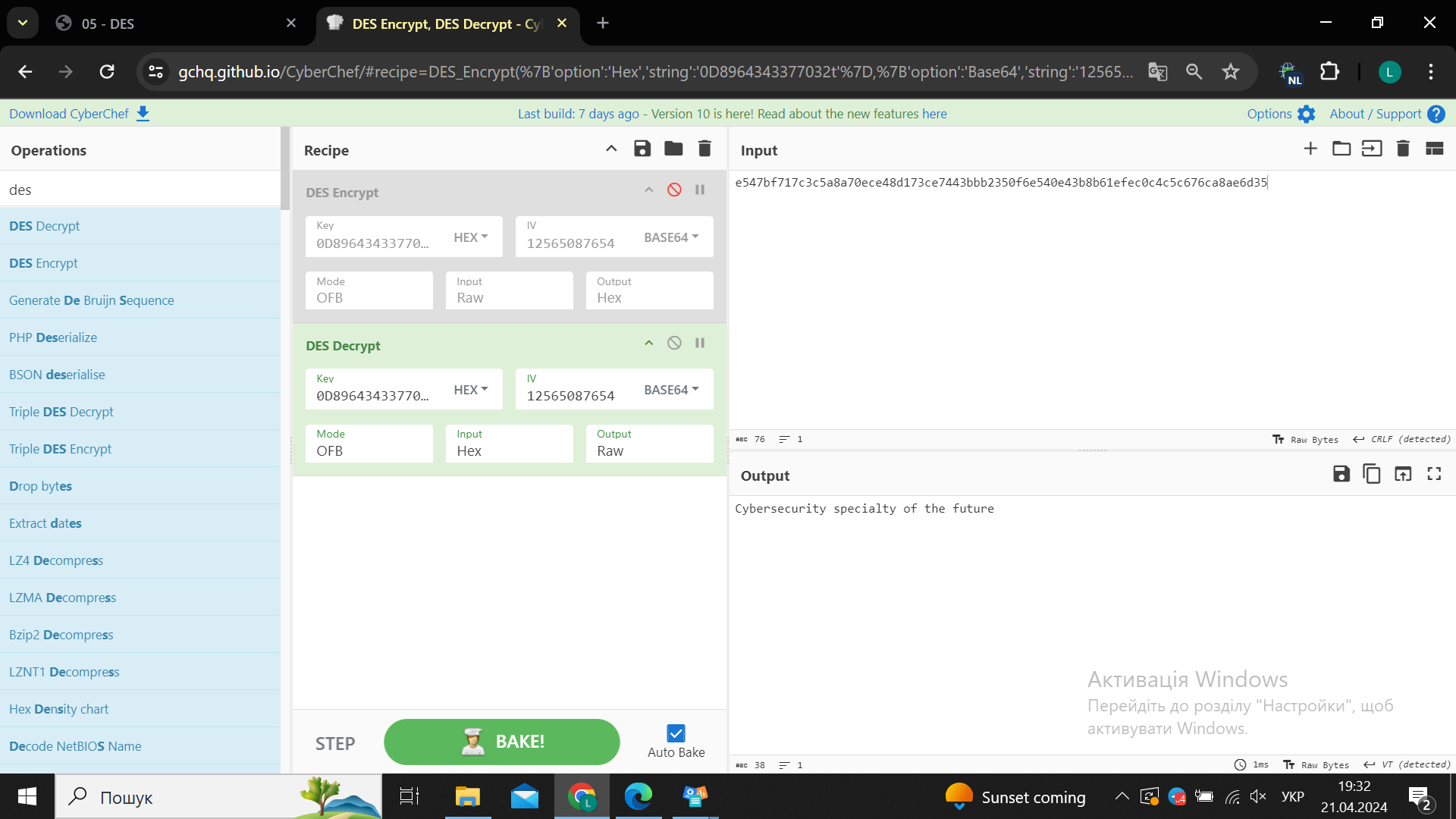
**KEY(HEX):** 0D8964343377032t

**ВТ:** *Cybersecurity* specialty of the future

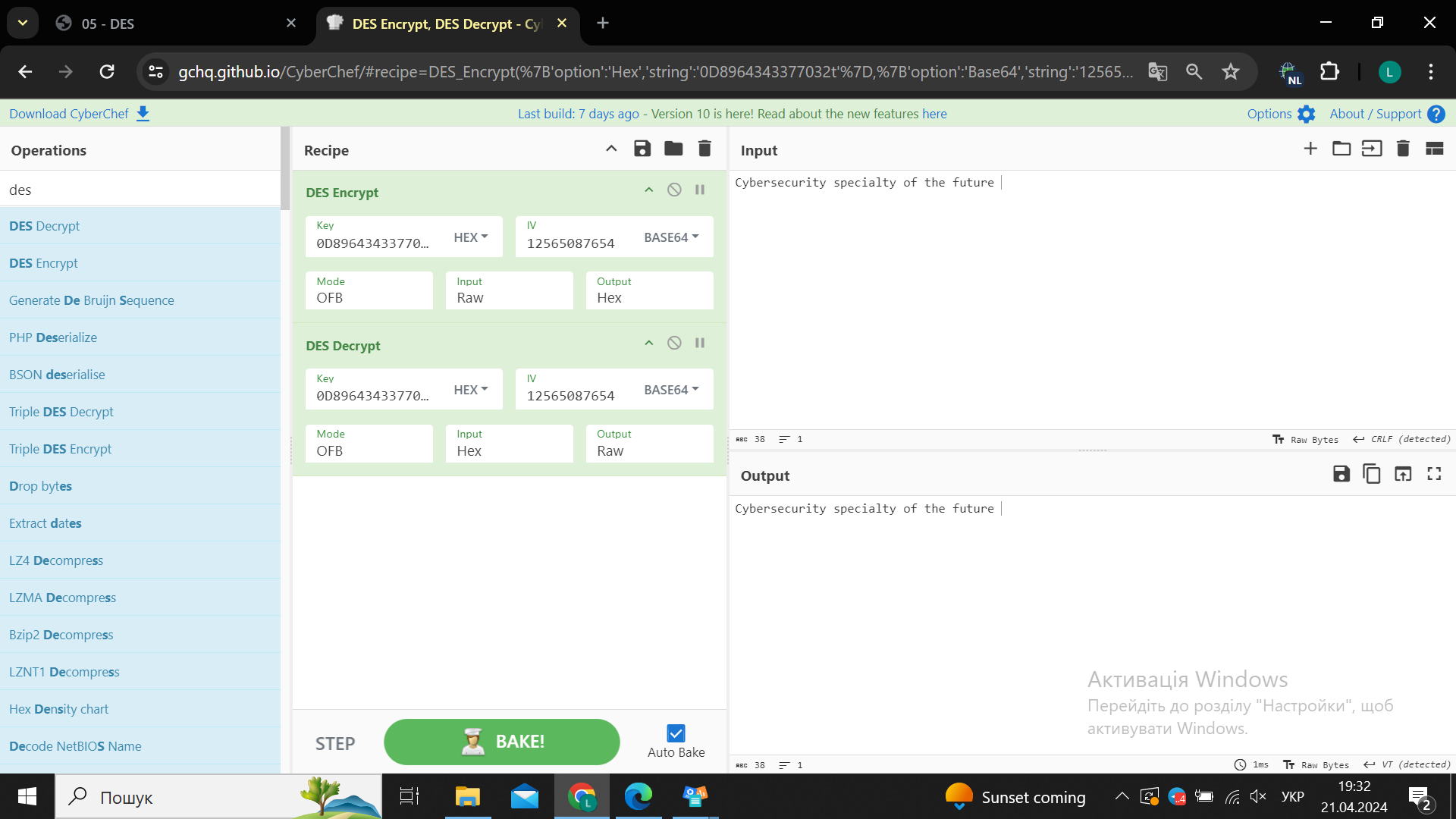
**ШТ:e547bf717c3c5a8a70ece48d173ce7443bbb2350f6e540e43b8b61efec0c4c5c676ca8ae6d35**

***ENCRYPT:***

***DECRYPT:***



***IN BLOCK:***



**4. MODE Cipher Feedback Mode (CFB)  
Режим**  **обратной связи шифра**

У цьому режимі кожен блок шифротексту використовується для згенерування ключа, який потім використовується для шифрування наступного блоку даних. Це дозволяє шифрувати дані неблоковими порціями і може бути корисним для потокового шифрування.

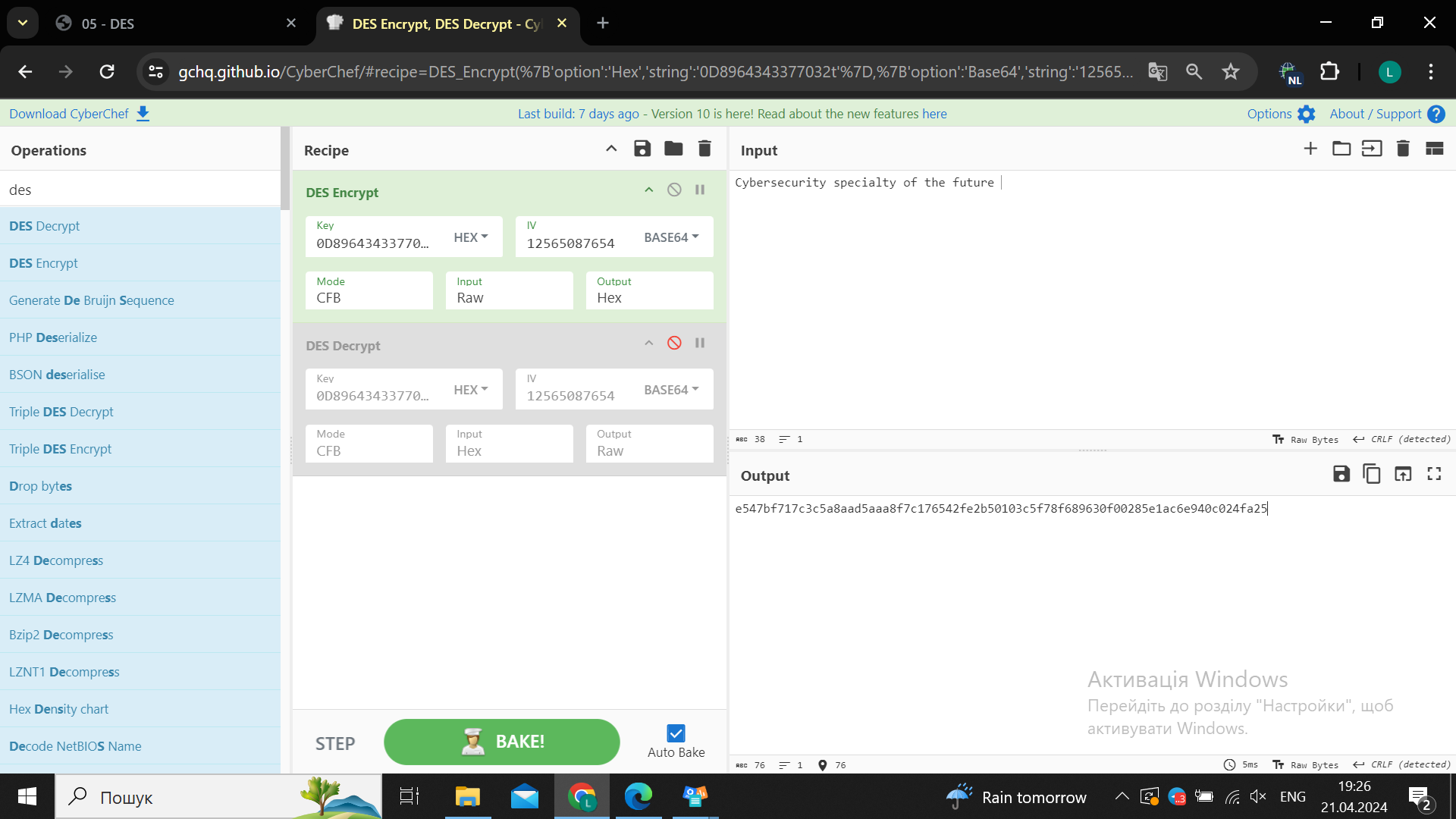
**KEY(HEX):** *0D8964343377032t*

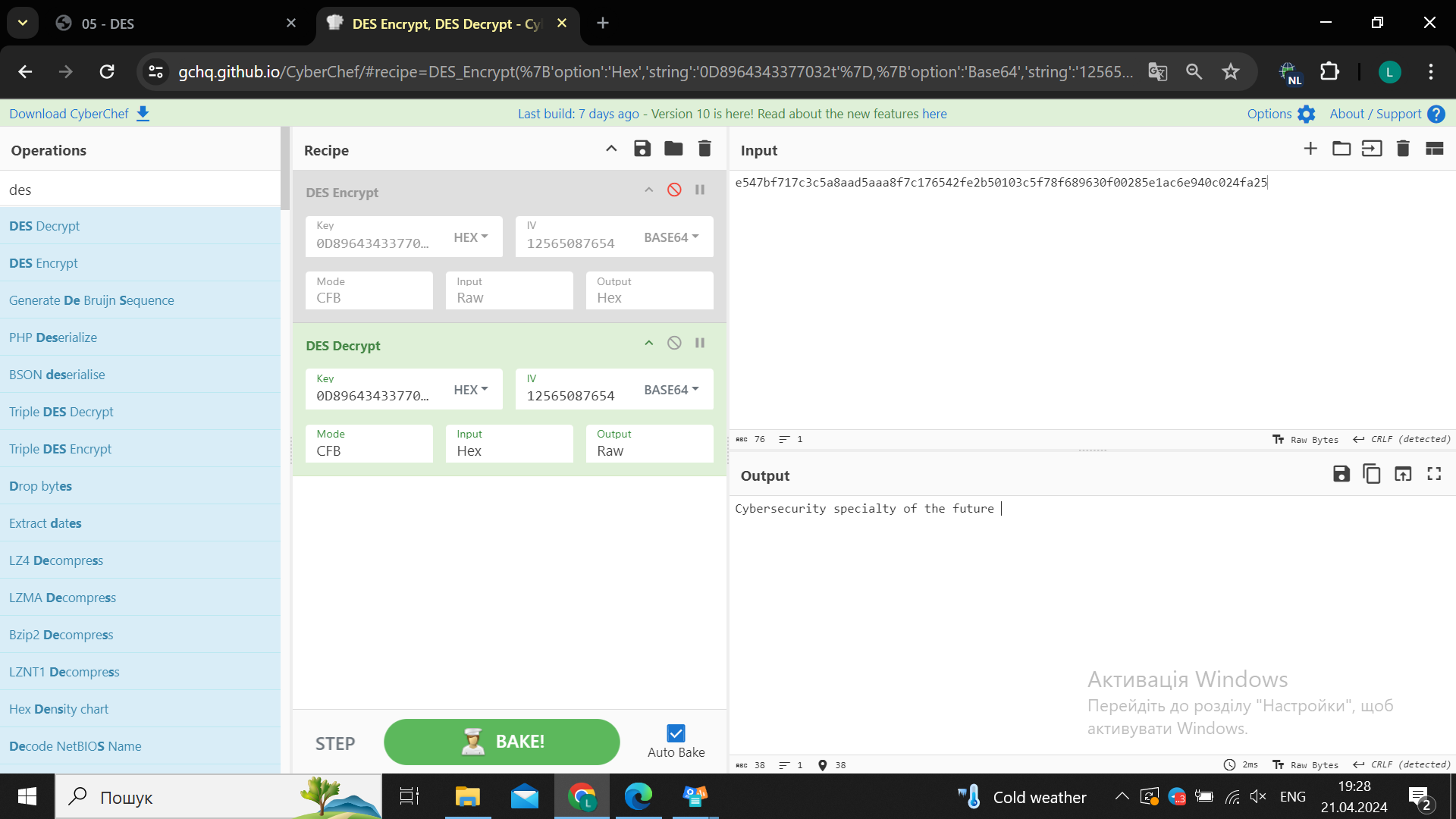
**IV(BASE64): 12565087654**

**ВТ:** Cybersecurity specialty of the future

***Шифрований текст: e547bf717c3c5a8aad5aaa8f7c176542fe2b50103c5f78f689630f00285e1ac6e940c024fa25***

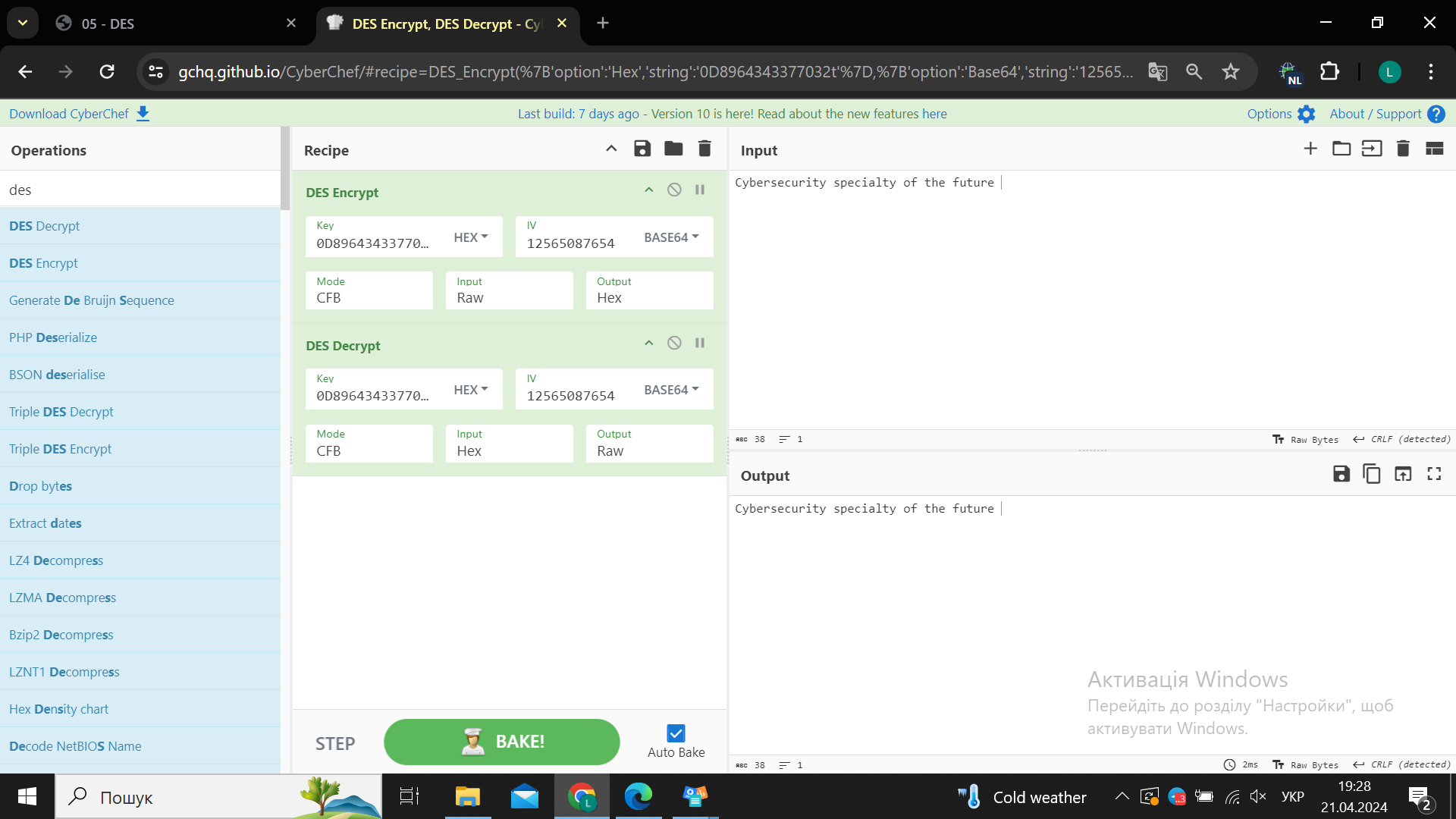
***ENCRYPT:***





***DECRYPT:***

***IN BLOCK:***



***5.MODE* Counter Mode( *CTR)***

**Режим лічильника**

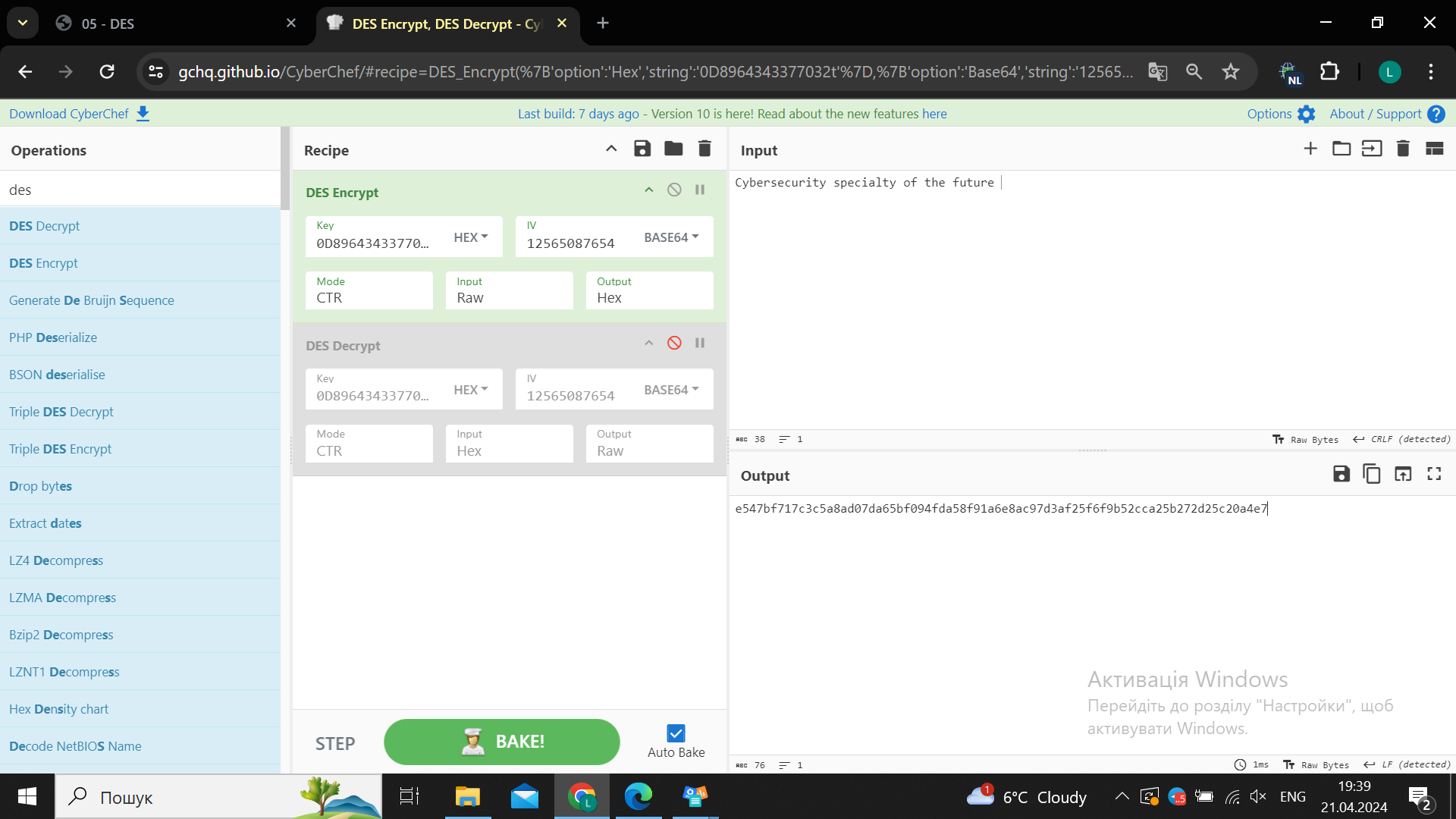
Режим лічильника (CTR) є типовим режимом роботи блочного шифру з використанням алгоритму блочного шифру. У цій версії ми надаємо можливість обробки Advanced Encryption Standard (AES), довжина ключа шифру для AES має бути 128/192/256 біт. Іншим обмеженням є те, що наш робочий режим працює з одиницями фіксованого розміру (128 біт на 1 блок), але текст у реальному світі має різну довжину. Отже, останній блок тексту, наданий цьому примітиву, повинен бути доповнений до 128 біт перед шифруванням або дешифруванням.

**KEY(HEX):** *0D8964343377032t*

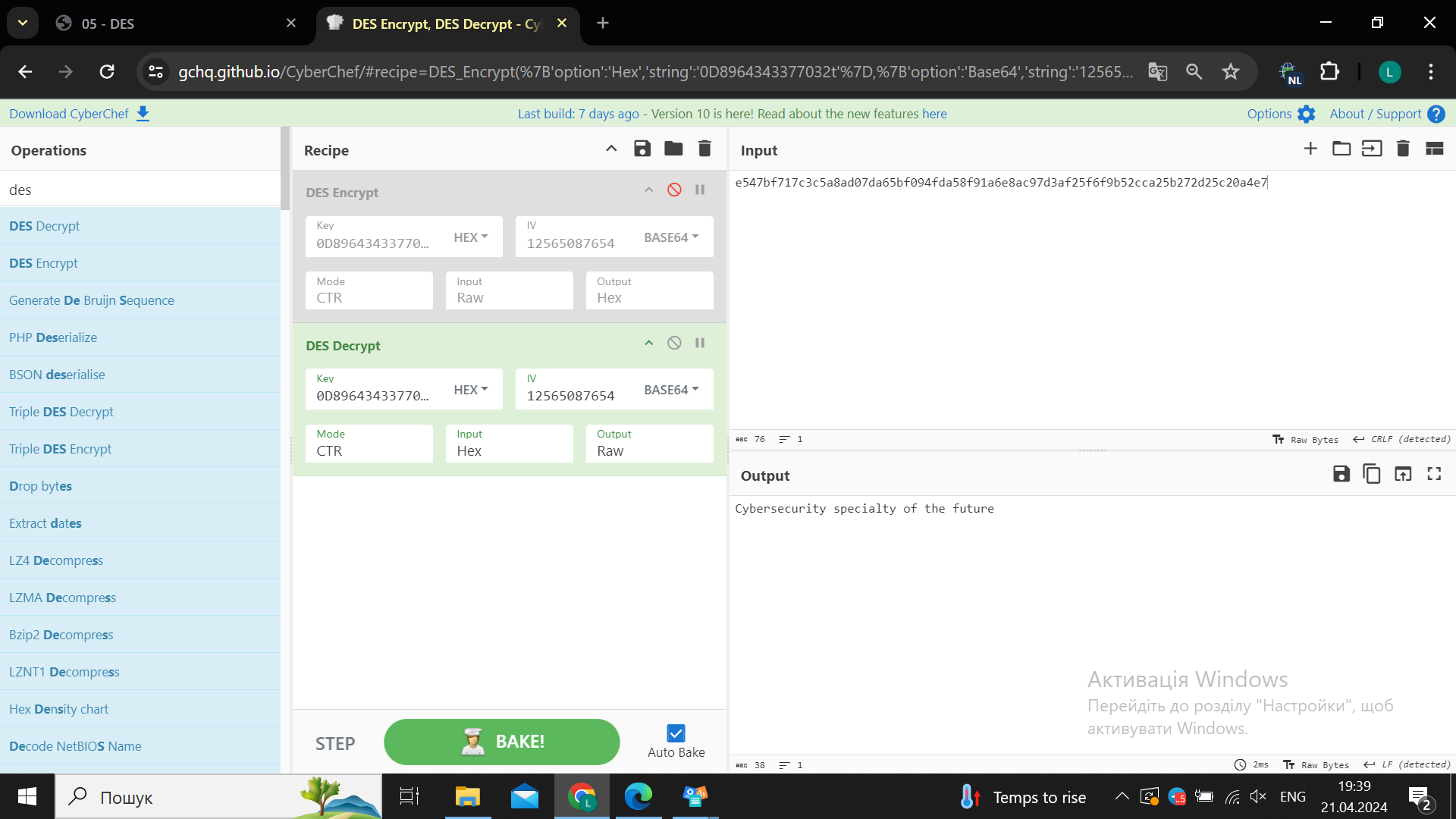
**ВТ:*Cybersecurity specialty of the future***

***ШТ: e547bf717c3c5a8ad07da65bf094fda58f91a6e8ac97d3af25f6f9b52cca25b272d25c20a4e7***

***ENCRYPT:***



***DECRYPT:***



***IN BLOCK:***

