**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

старший солдат \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Р.ДІДКОВСЬКИЙ

.04.2024

**Перевiрив:** викладач кафедри № 33

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

.04.2024

Київ – 2024

1. **РЕЖИМИ РОБОТИ АЛГОРИТМУ DES**

**DES** (*Data Encryption Standard*) — це симетричний алгоритм шифрування певних даних, стандарт шифрування.

Для DES рекомендовано декілька режимів:

• **ECB** (electronic code book) – режим «електронної кодової книги» (проста заміна);

• **CBC** (cipher block chaining) – режим зчеплення блоків;

• **CFB** (cipher feed back) - режим зворотного зв'язку за шифротекстом;

• **OFB** (output feed back) – режим зворотного зв'язку по виходу;

• **CM** (counter Mode) — режим лічильника.

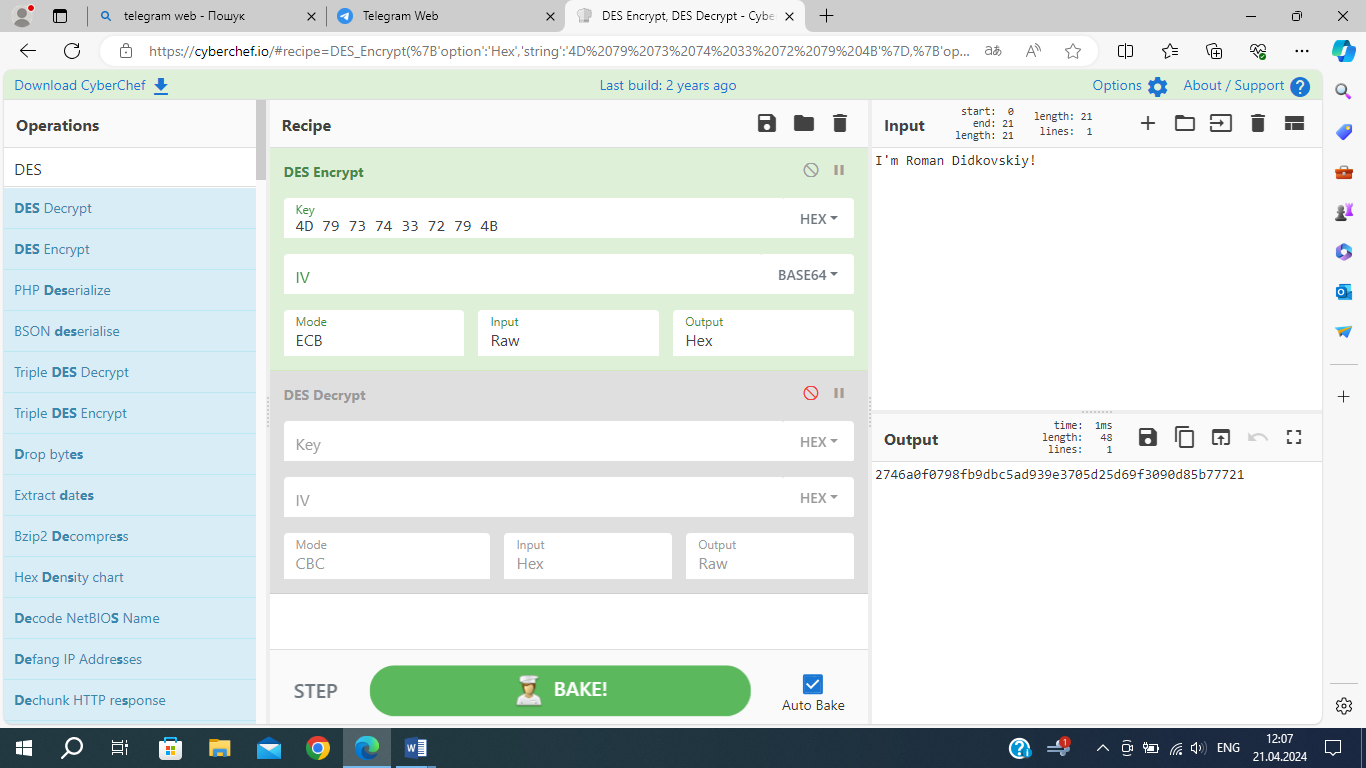
1. **АНАЛІЗ РОБОТИ РЕЖИМІВ**
2. **MODE ECB**

**KEY(HEX):** 4D 79 73 74 33 72 79 4B

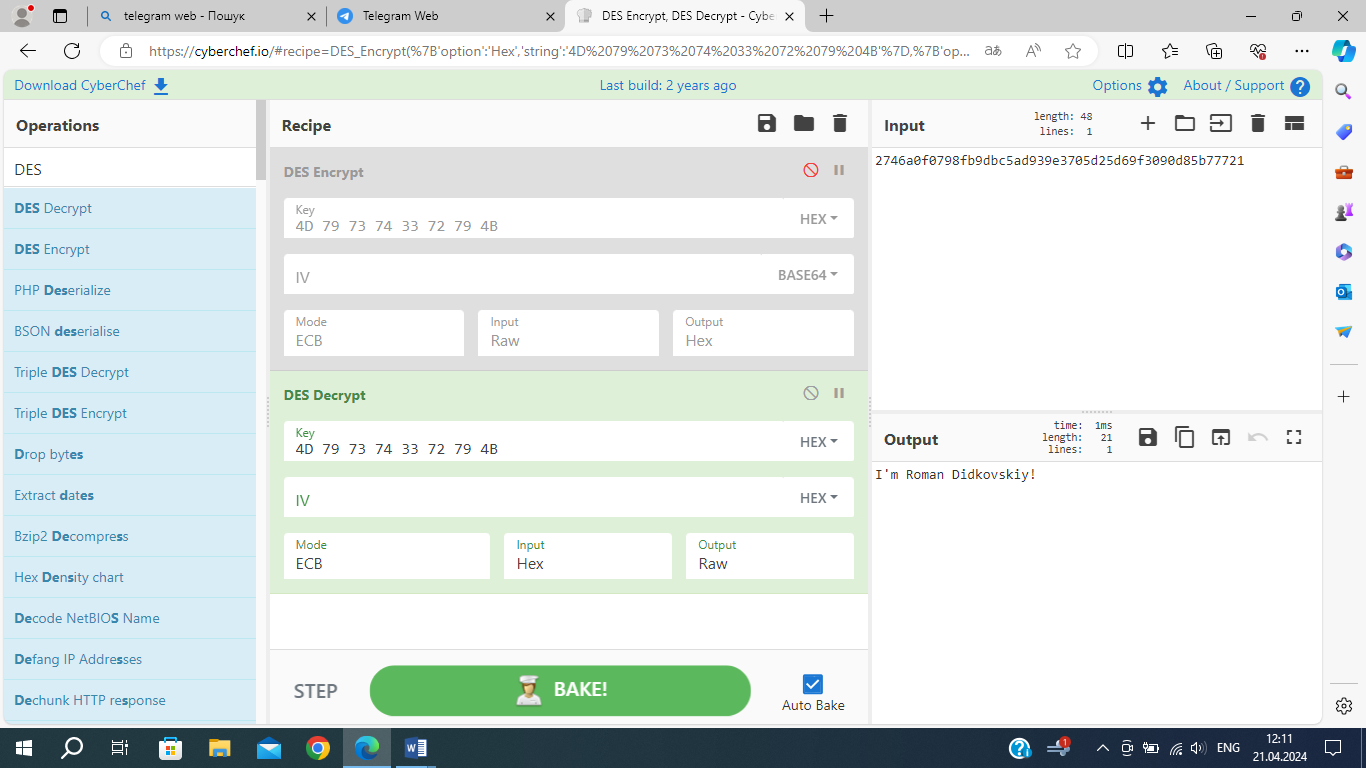
**Відкритий текст:** I'm Roman Didkovskiy!

**Шифрований текст:** 2746a0f0798fb9dbc5ad939e3705d25d69f3090d85b77721

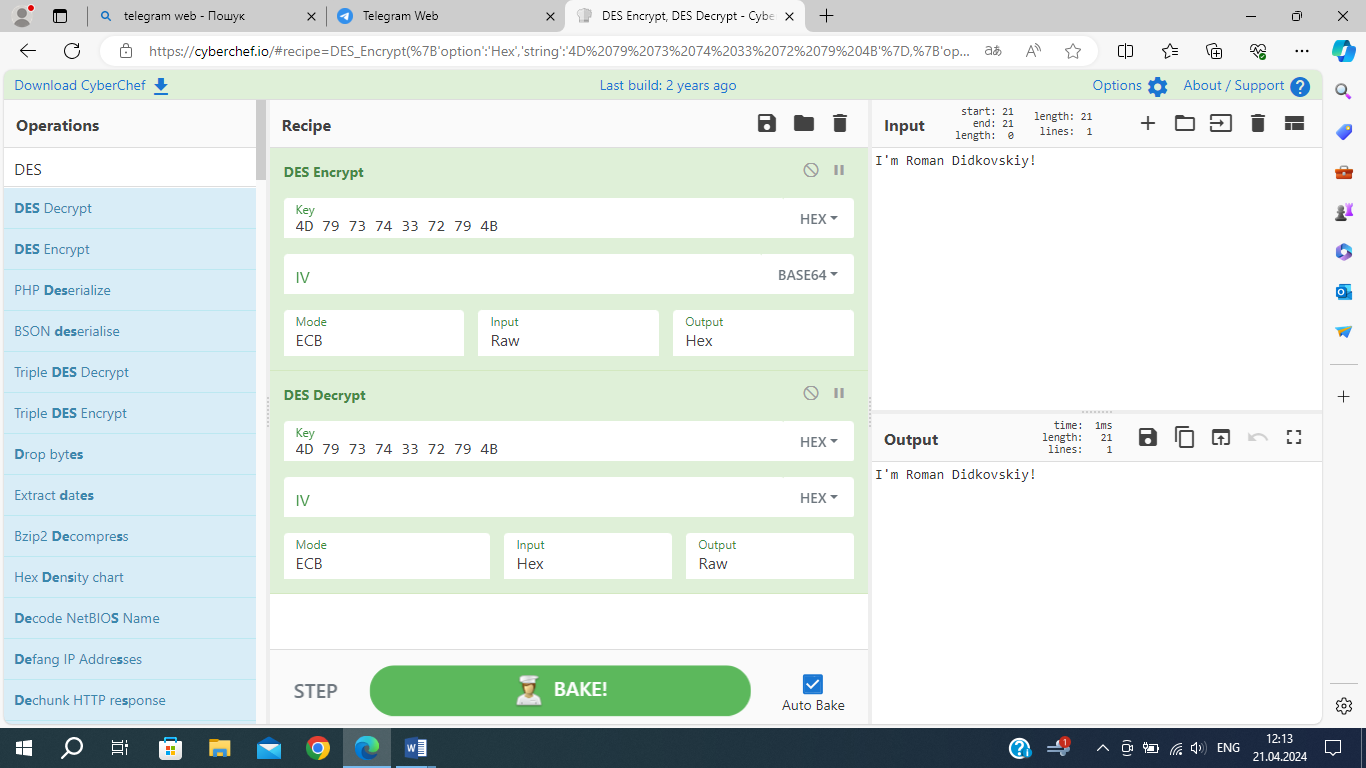
**ENCRYPT:**



**DECRYPT:**



**IN BLOCK:**



У цьому режимі блоки даних шифруються незалежно один від одного. Один і той же блок відкритого тексту завжди шифрується в один і той же шифротекст, що може призвести до недоліків у безпеці, особливо якщо вхідні дані мають певну регулярність.

1. **MODE CBC**

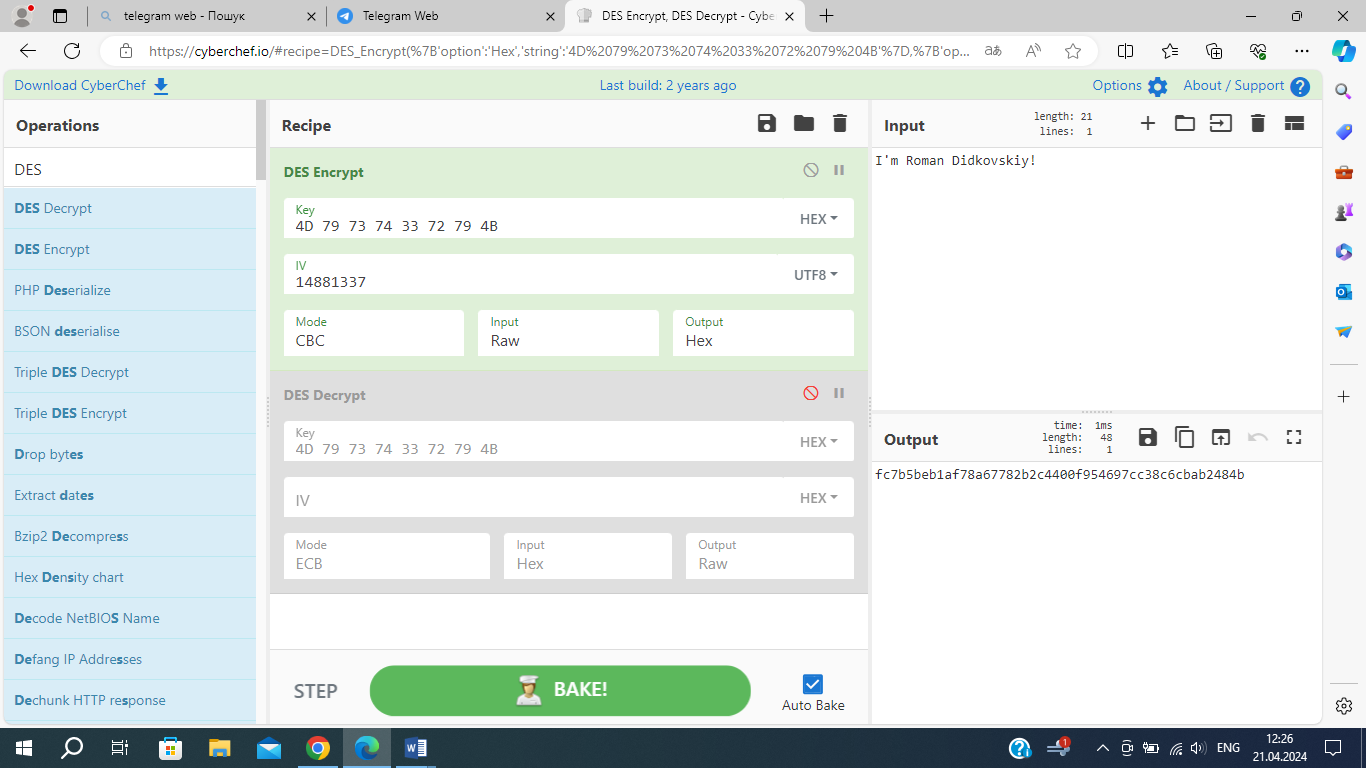
**KEY(HEX):** 4D 79 73 74 33 72 79 4B

**IV(UTF-8):** *14881337*

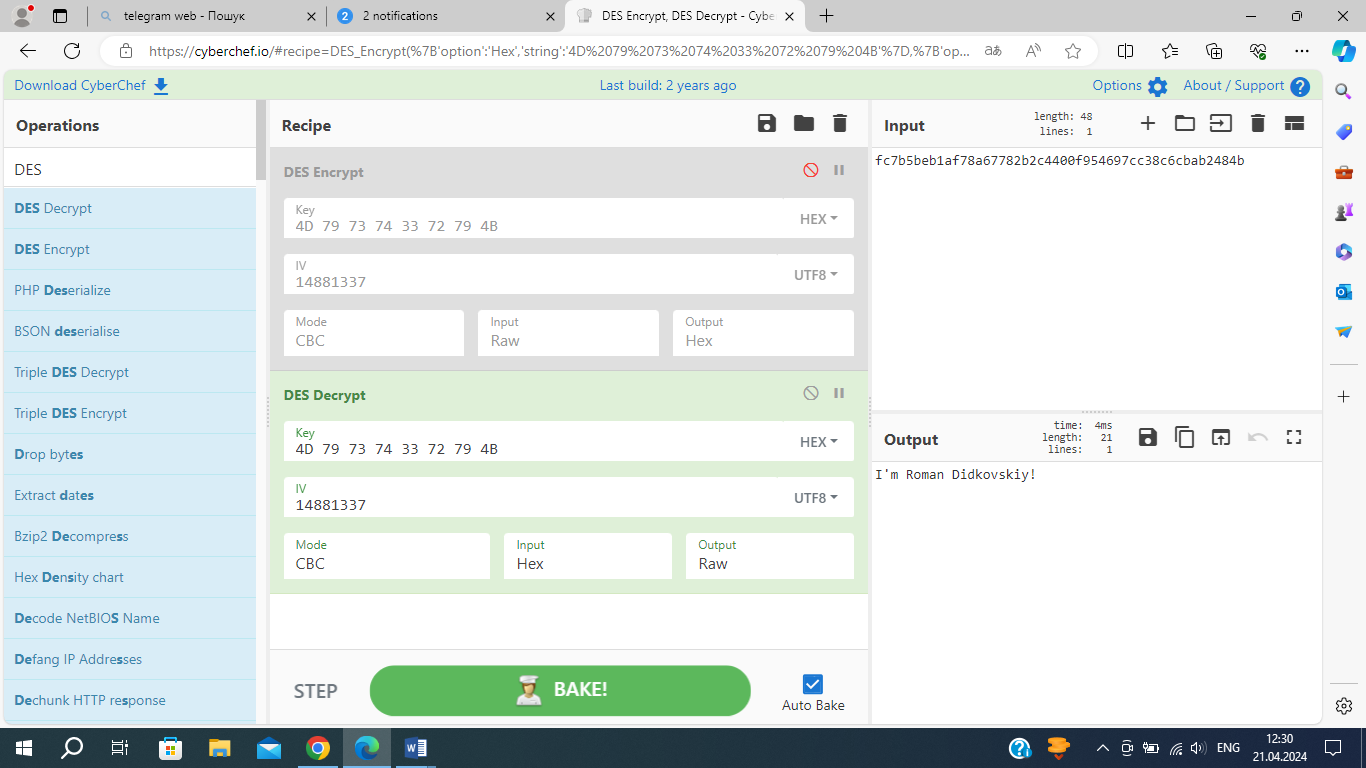
**Відкритий текст:** I'm Roman Didkovskiy!

**Шифрований текст:** fc7b5beb1af78a67782b2c4400f954697cc38c6cbab2484b

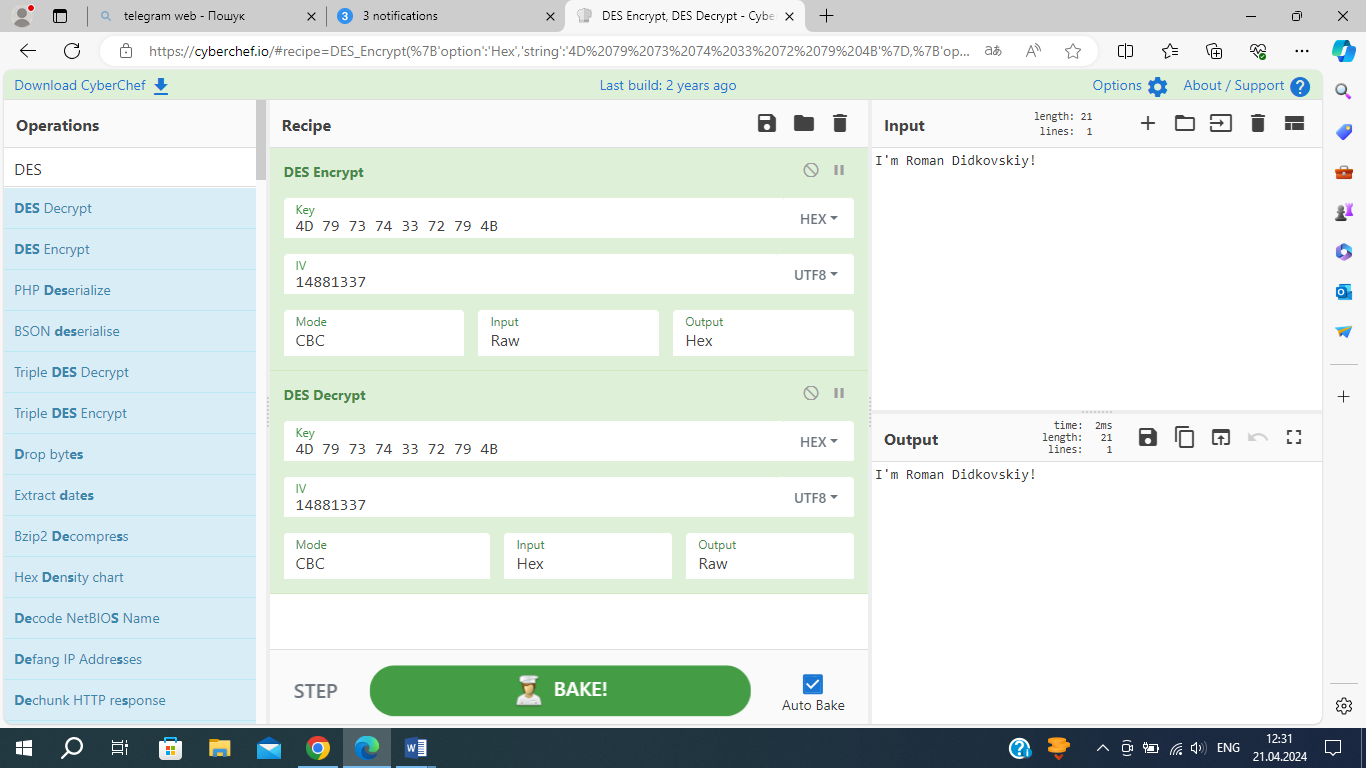
**ENCRYPT:**



**DECRYPT:**



**IN BLOCK:**



У цьому режимі кожен блок відкритого тексту комбінується з попереднім блоком шифротексту перед шифруванням, що робить шифротекст менш передбачуваним і додає додатковий рівень безпеки.

У DES і в багатьох інших шифрах з блоцьним шифруванням (наприклад, AES) використовується **ініціалізаційний вектор (IV)**, що є параметром, який вводиться в алгоритм разом із ключем.

**IV** - це випадкове значення, яке додається до відкритого тексту перед шифруванням. Воно використовується для того, щоб кожне повідомлення мало унікальний шифротекст, навіть якщо відкритий текст повторюється або має однакову частину.

**IV** зазвичай має ту ж довжину, що й **розмір блоку шифру (в DES це 64 біти)**, і воно має бути вибрано випадковим чином для кожного блоку даних. Крім того, **IV** не потрібно зберігати разом з шифрованим текстом, оскільки воно передається разом із шифрованим текстом (наприклад, у якості частини заголовка).

Ініціалізаційний вектор важливий для забезпечення безпеки криптографічних операцій, оскільки неправильне використання **IV** може призвести до певних атак на криптосистему, таких як атака на вибране шифрування. Відтак, правильне генерування та управління **IV** є важливою складовою безпечного застосування шифрувальних алгоритмів.

1. **MODE CFB**

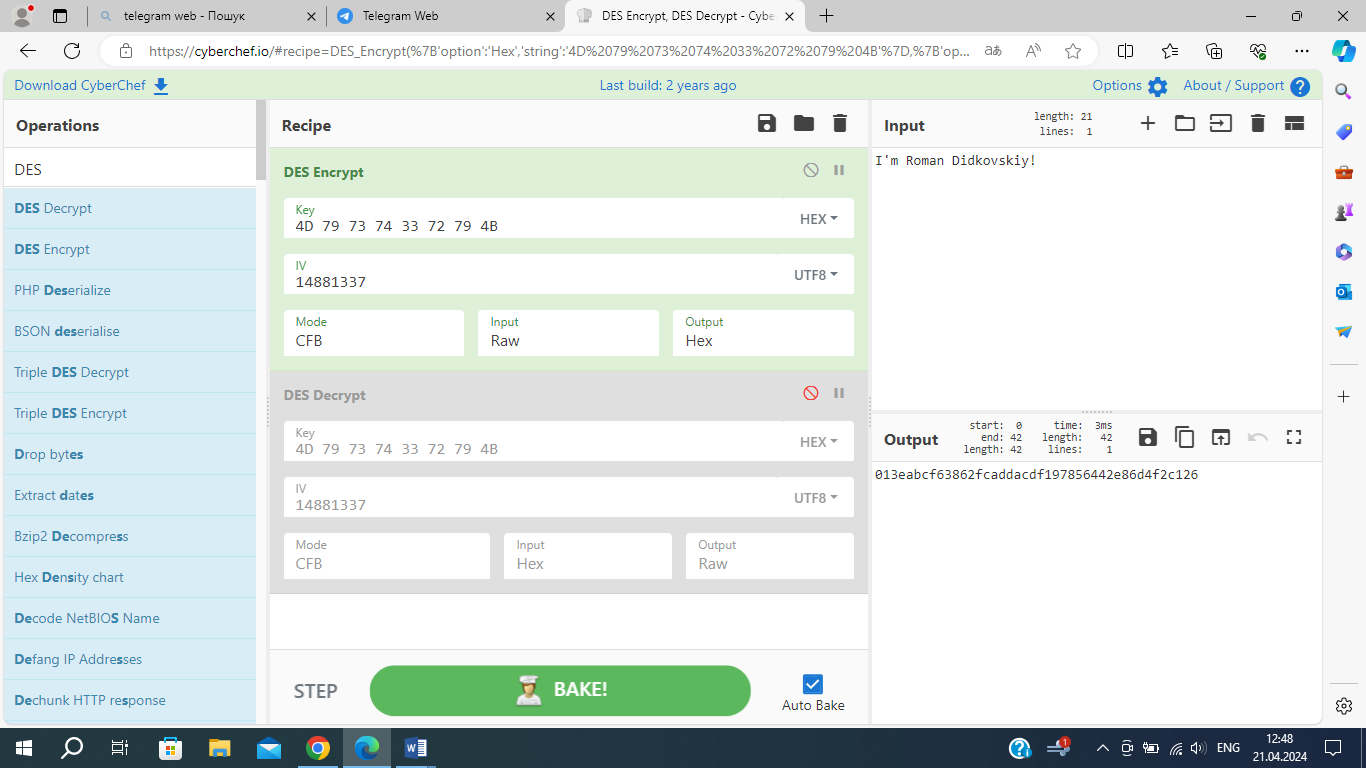
**KEY(HEX):** 4D 79 73 74 33 72 79 4B

**IV(UTF-8):** *14881337*

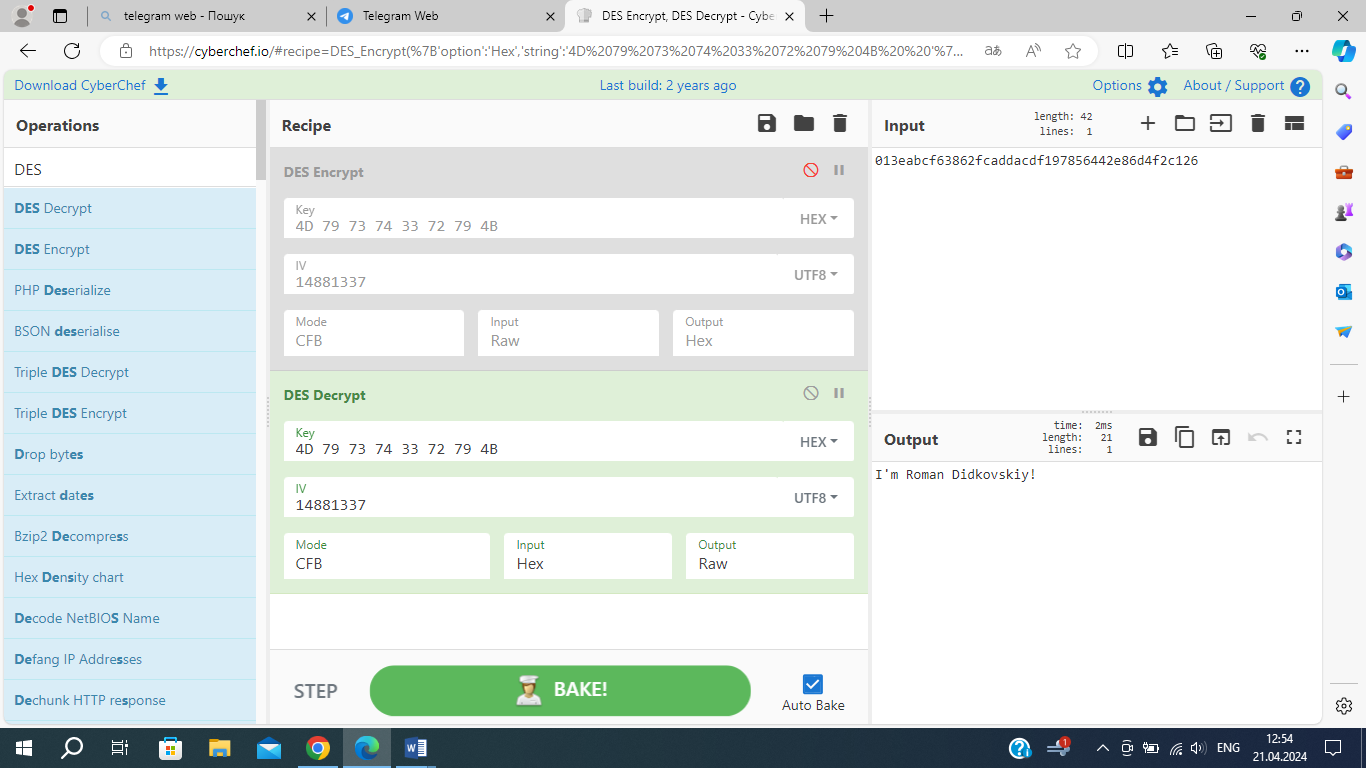
**Відкритий текст:** I'm Roman Didkovskiy!

**Шифрований текст:** 013eabcf63862fcaddacdf197856442e86d4f2c126

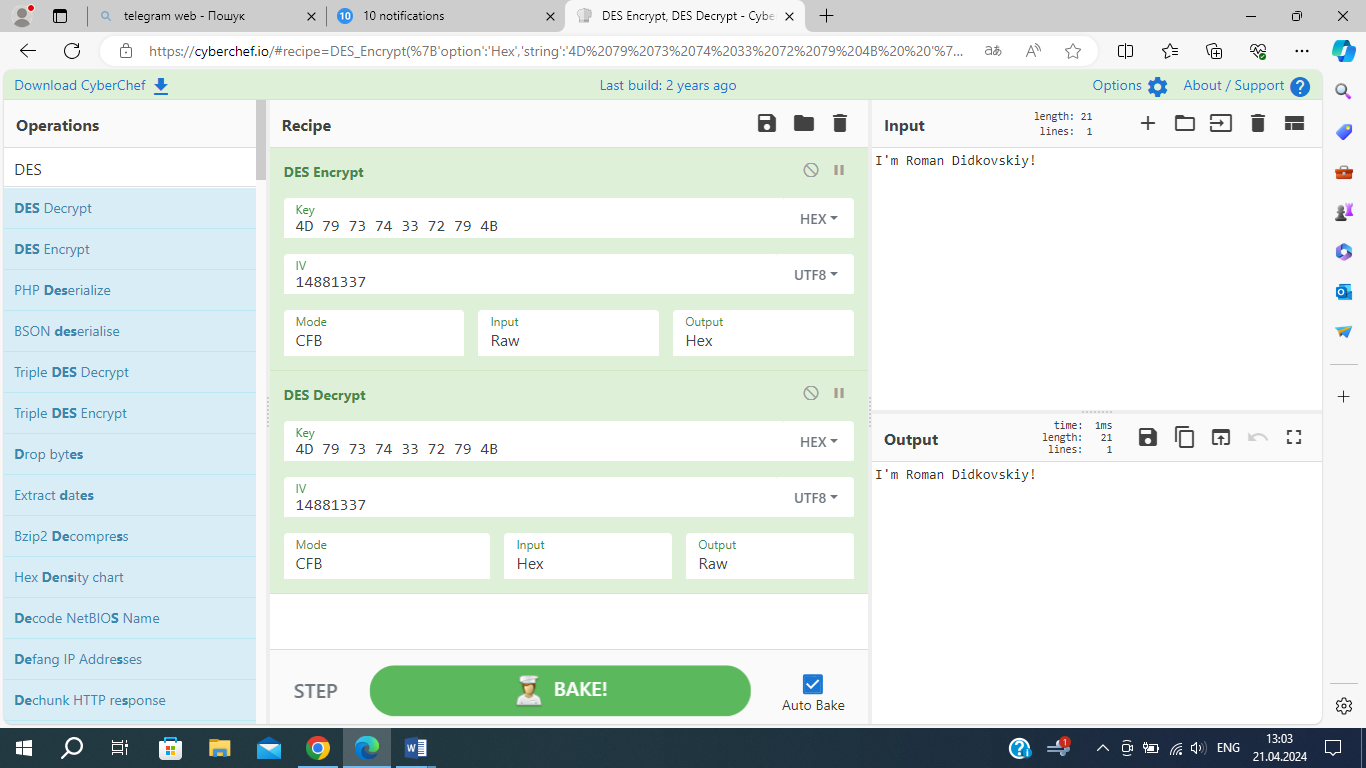
**ENCRYPT:**



**DECRYPT:**



**IN BLOCK:**



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.

1. **MODE OFB**

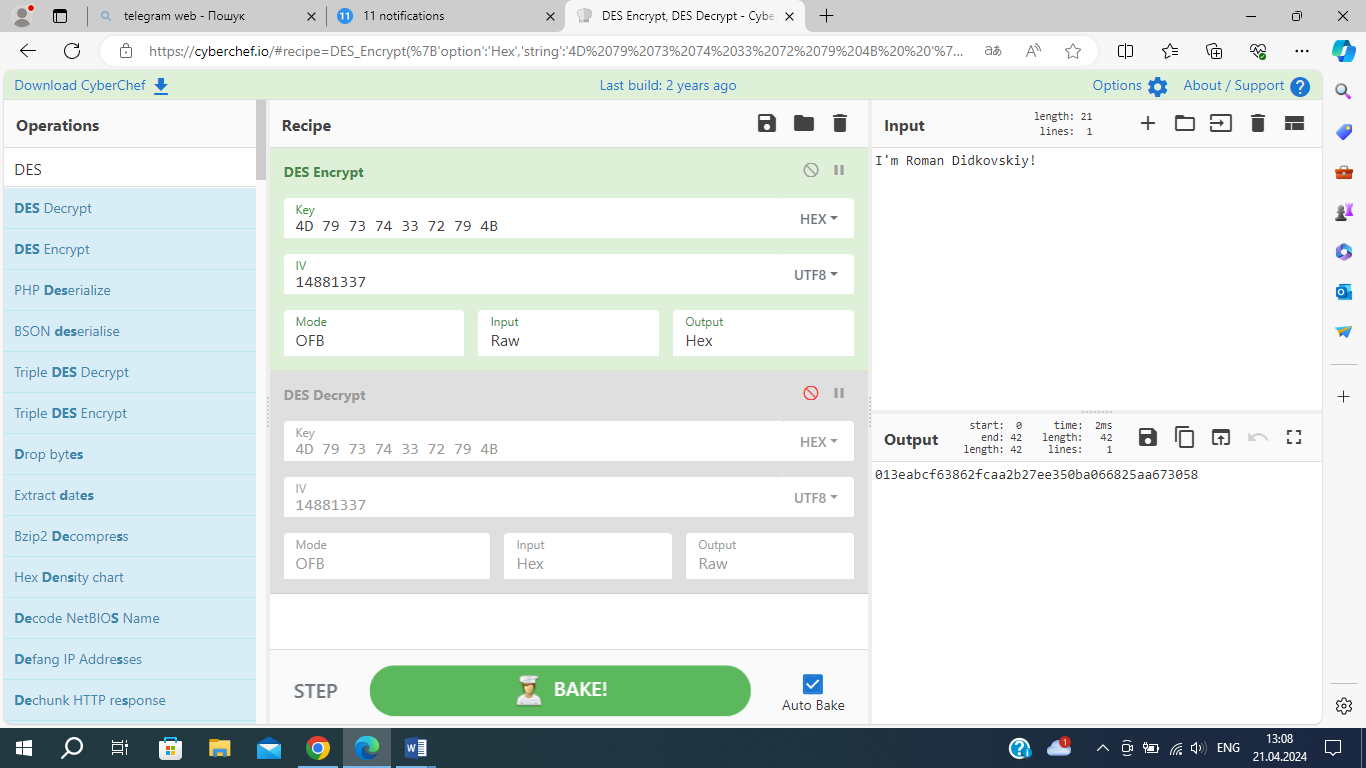
**KEY(HEX):** 4D 79 73 74 33 72 79 4B

**IV(UTF-8):** *14881337*

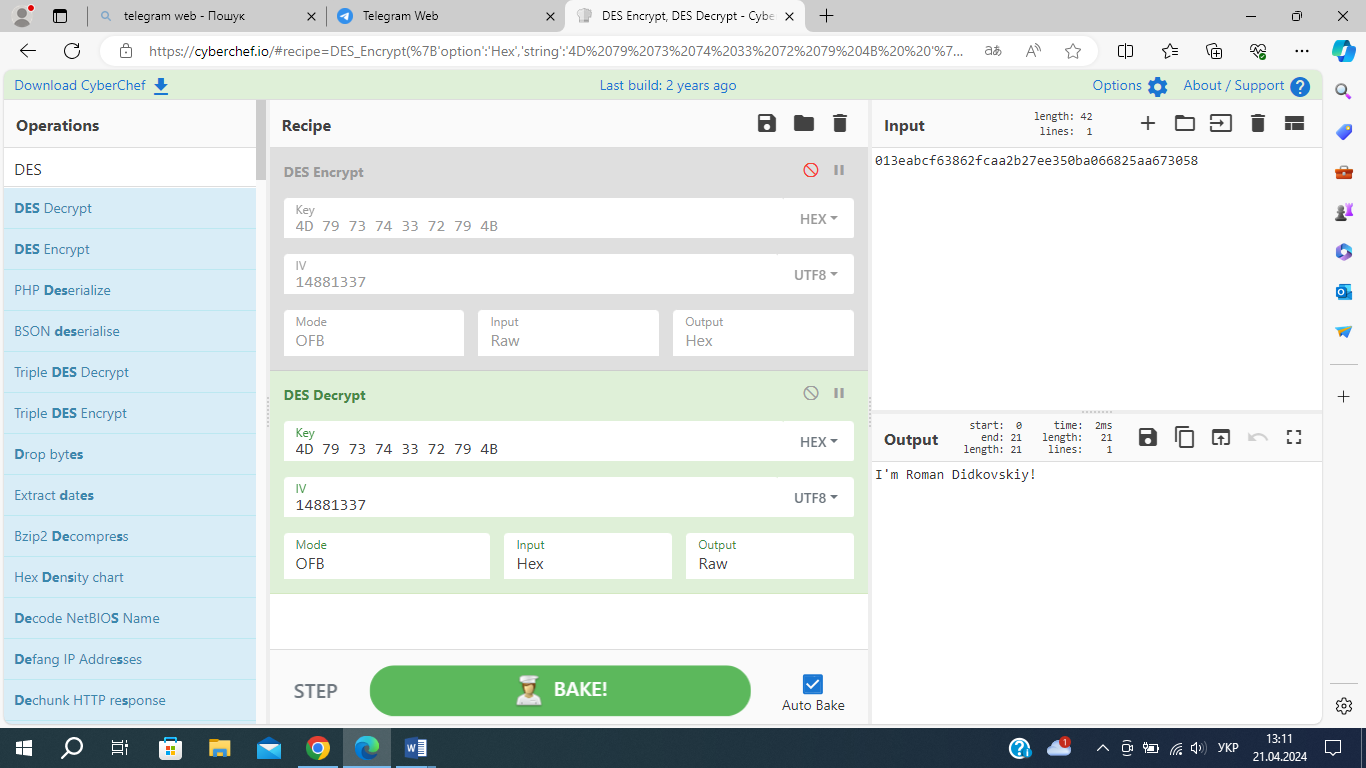
**Відкритий текст:** I'm Roman Didkovskiy!

**Шифрований текст:** 013eabcf63862fcaa2b27ee350ba066825aa673058

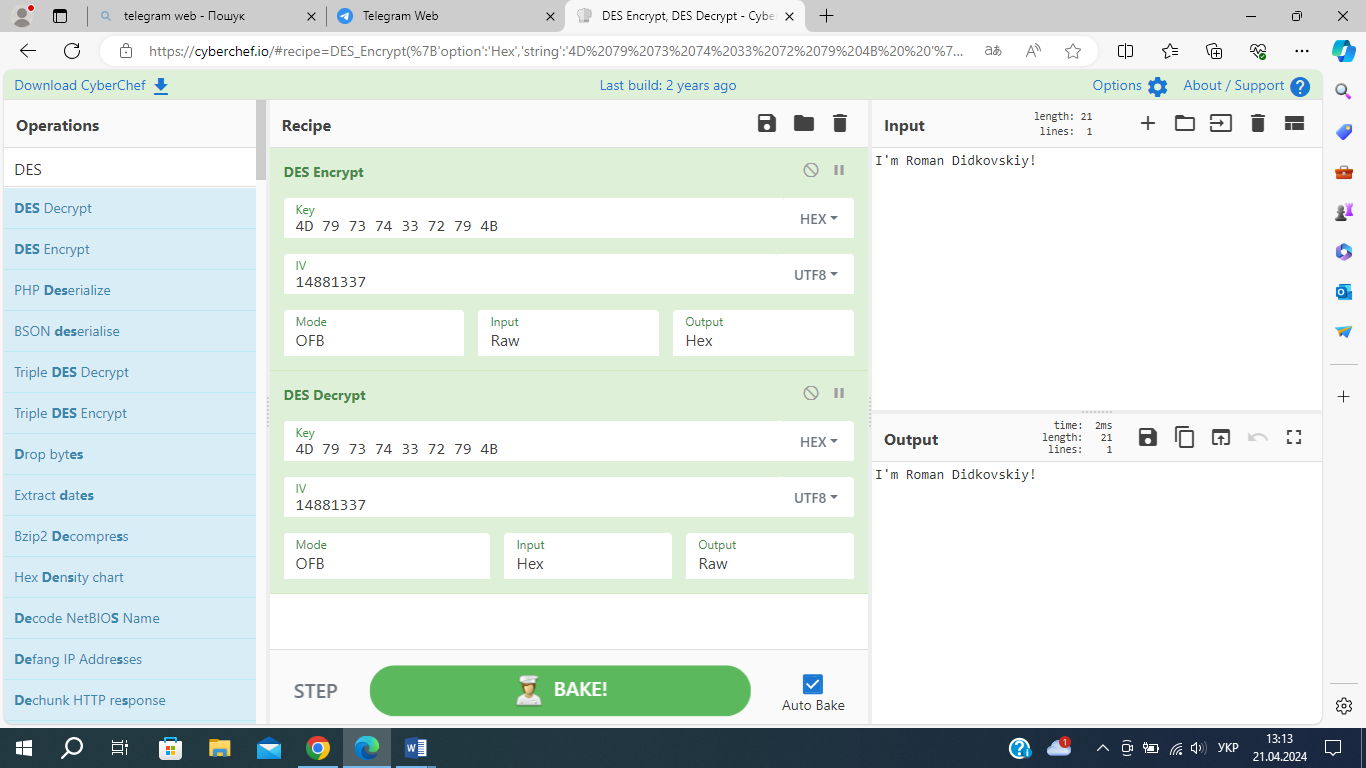
**ENCRYPT:**



**DECRYPT:**



**IN BLOCK:**



У цьому режимі блоки генеруються за допомогою шифруючої функції і потім використовуються для зміни відкритого тексту, а не для шифрування його безпосередньо. Це робить його добре підходящим для потокового шифрування.

1. **MODE CTR**

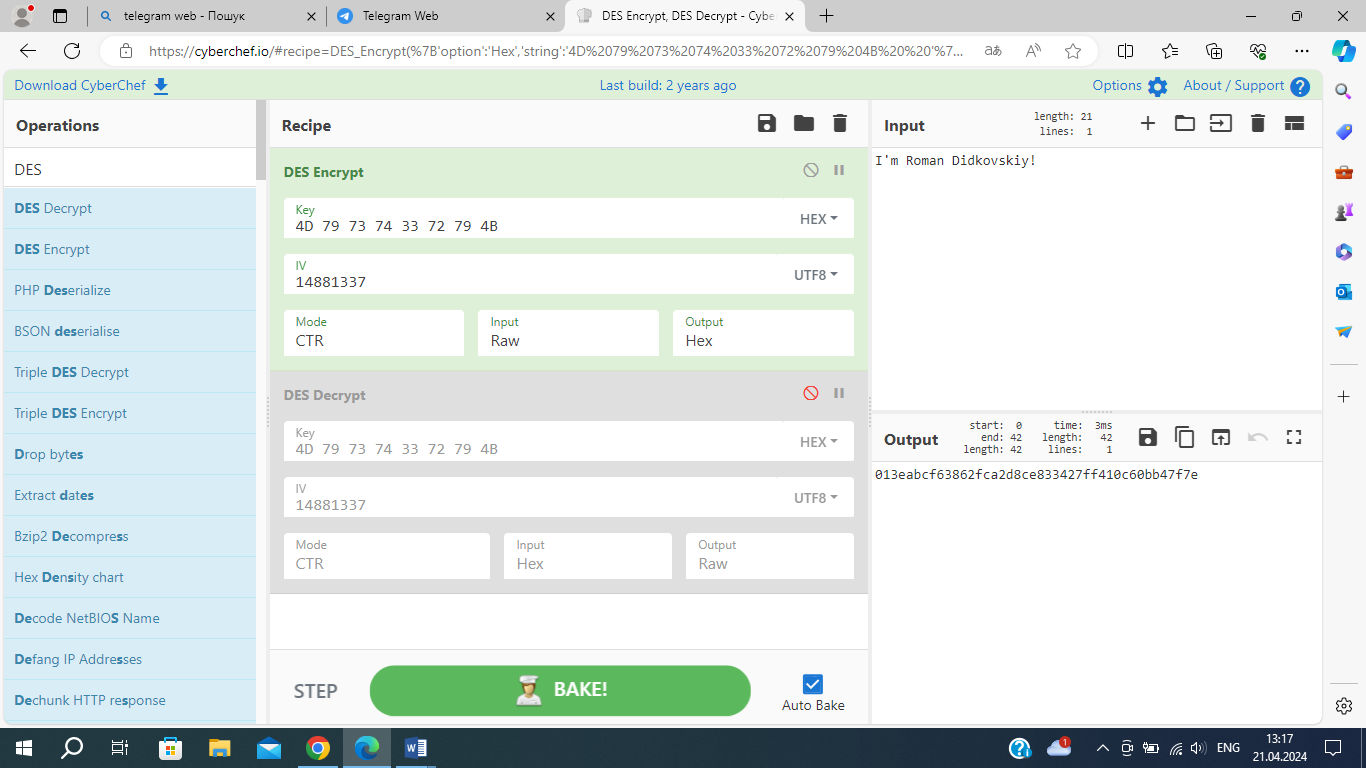
**KEY(HEX):** 4D 79 73 74 33 72 79 4B

**IV(UTF-8):** *14881337*

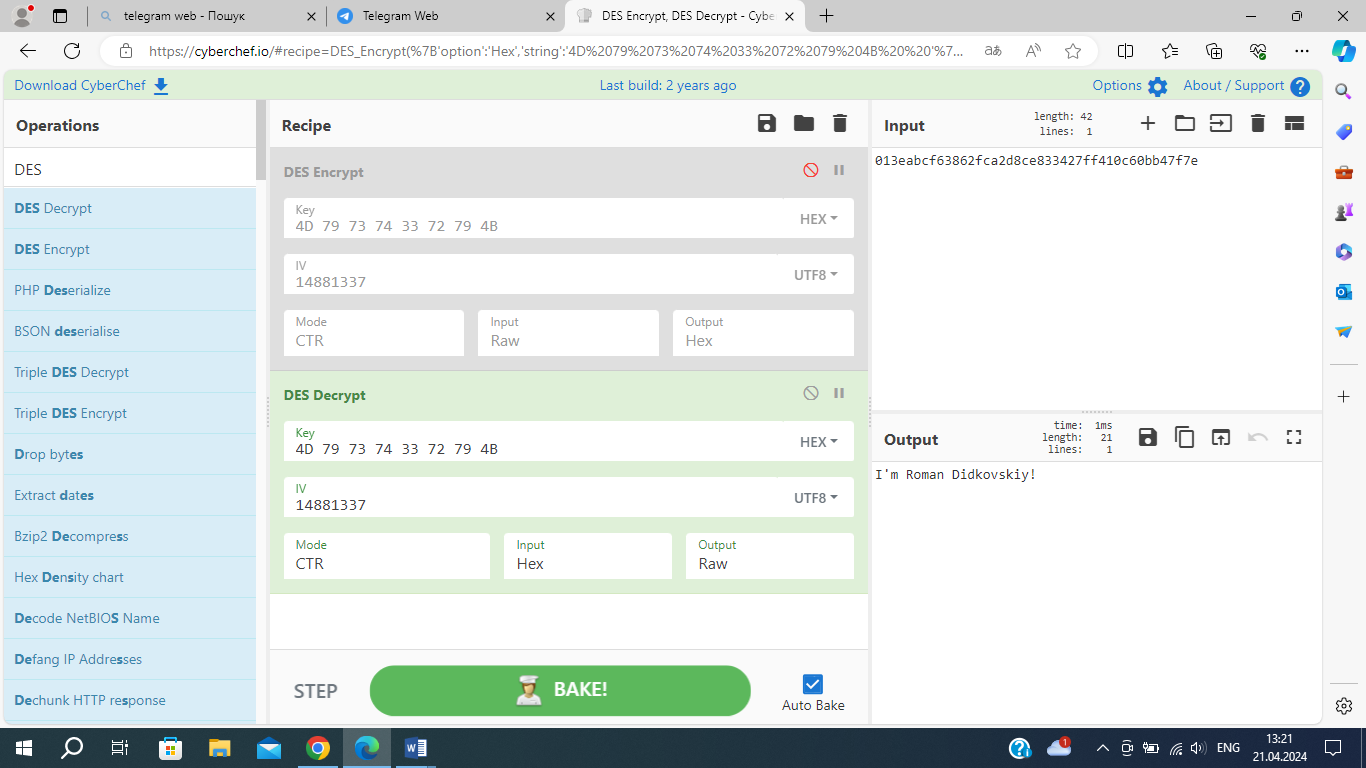
**Відкритий текст:** I'm Roman Didkovskiy!

**Шифрований текст:** 013eabcf63862fca2d8ce833427ff410c60bb47f7e

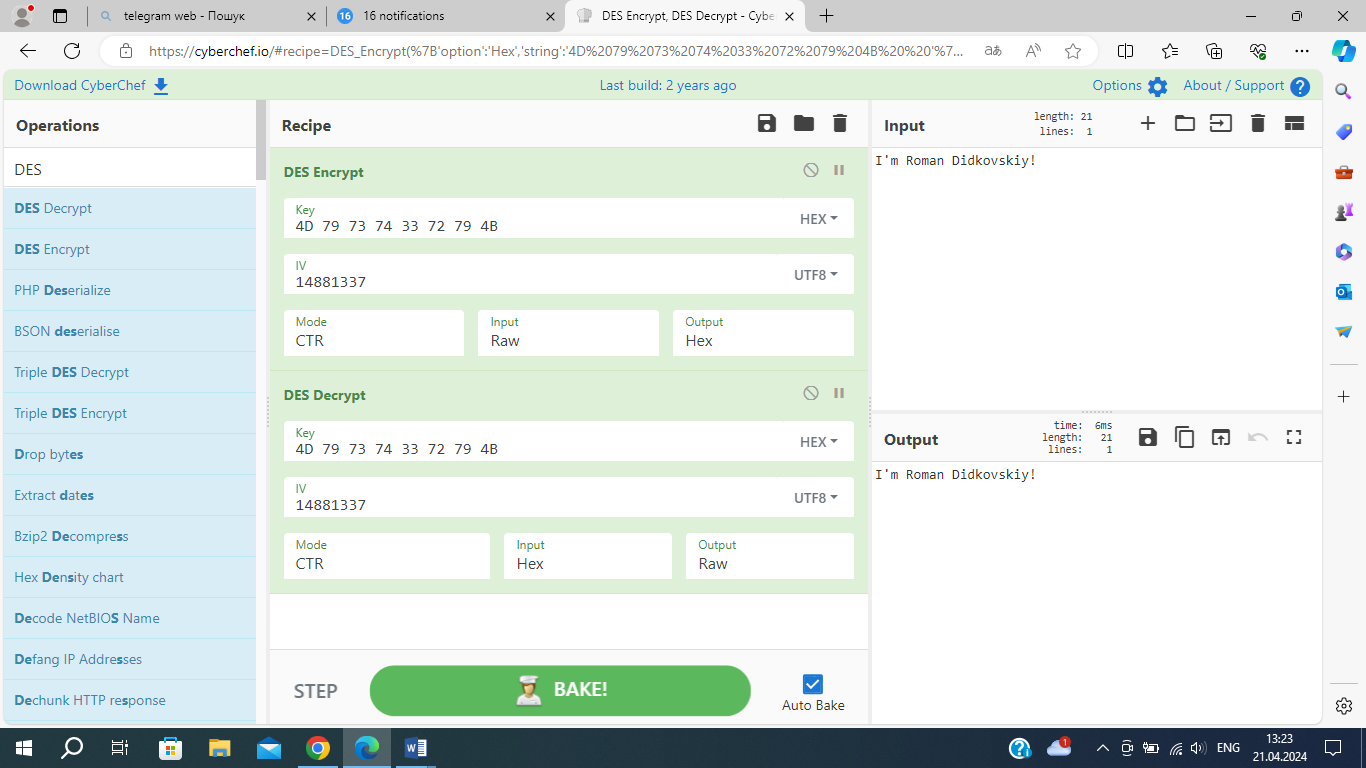
**ENCRYPT:**



**DECRYPT:**



**IN BLOCK:**



У цьому режимі блоки згенеровані за допомогою функції рахунку, яка змінюється кожен раз для кожного блоку. Це дозволяє паралельне шифрування та розшифрування, що робить його ефективним для застосувань, які вимагають високої швидкості.

**Отже**, кожен з цих режимів має свої переваги та недоліки, і вибір конкретного режиму залежить від конкретних вимог до безпеки та функціональності вашого застосунку.

**ВИСНОВКИ:**

Режими роботи DES є важливою складовою для ефективного та безпечного застосування цього шифру. Кожен режим має свої особливості та застосування, які впливають на безпеку та функціональність системи шифрування. **ECB (Electronic Codebook)** простий у реалізації, але його використання може призвести до повторюваності шифротексту та недоліків у безпеці. **CBC (Cipher Block Chaining)** забезпечує кращий рівень захисту, оскільки кожен блок залежить від попередніх, що ускладнює атаки. **CFB (Cipher Feedback)** та **OFB (Output Feedback)** використовуються для потокового шифрування, дозволяючи обробку даних меншими блоками і надаючи додатковий рівень конфіденційності. Режим **CTR (Counter)** надає можливість паралельного шифрування, що дозволяє підвищити продуктивність у деяких випадках. Обираючи режим роботи DES, важливо враховувати конкретні потреби системи та забезпечити відповідний рівень захисту даних.