**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 \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ О.ЛУТЧЕНКО

.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**

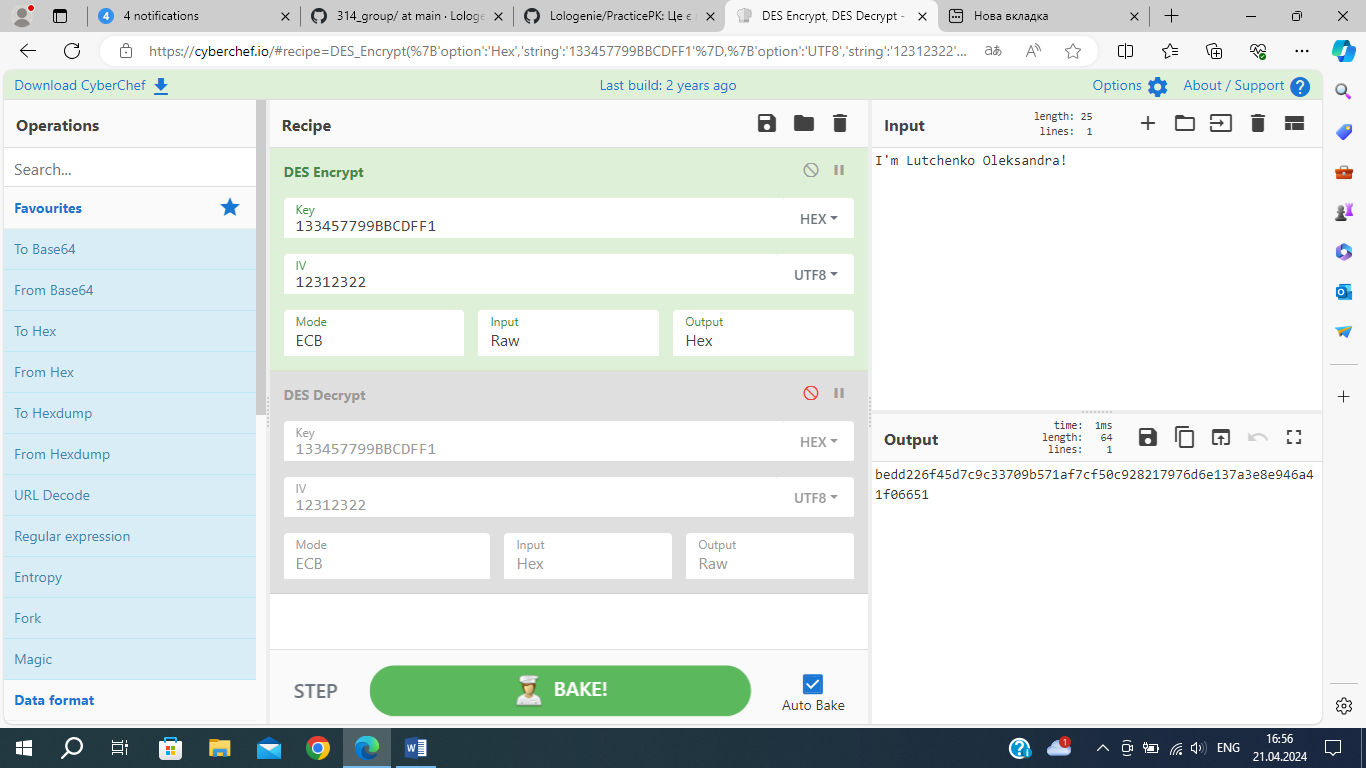
**KEY(HEX):** 133457799BBCDFF1

**Відкритий текст:** I'm Lutchenko Oleksandra!

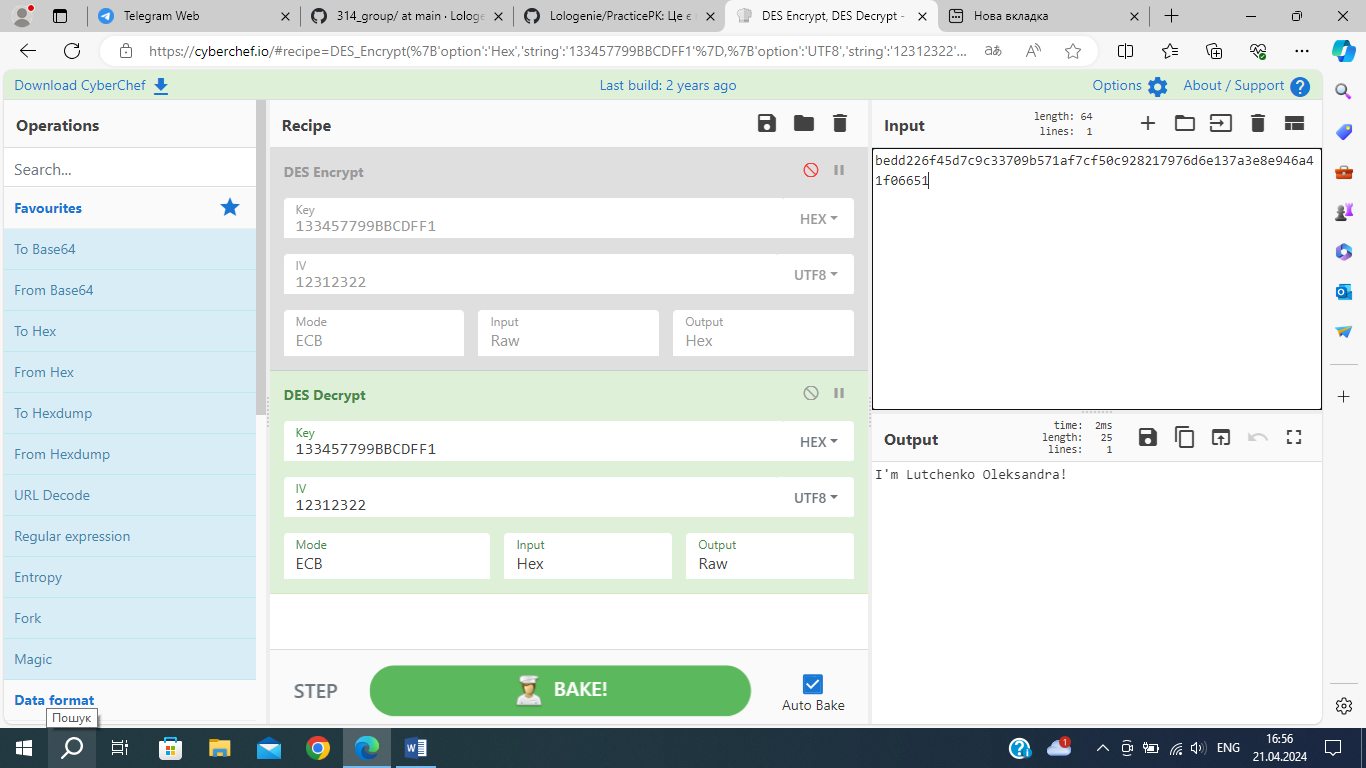
**Шифрований текст:**

bedd226f45d7c9c33709b571af7cf50c928217976d6e137a3e8e946a41f06651

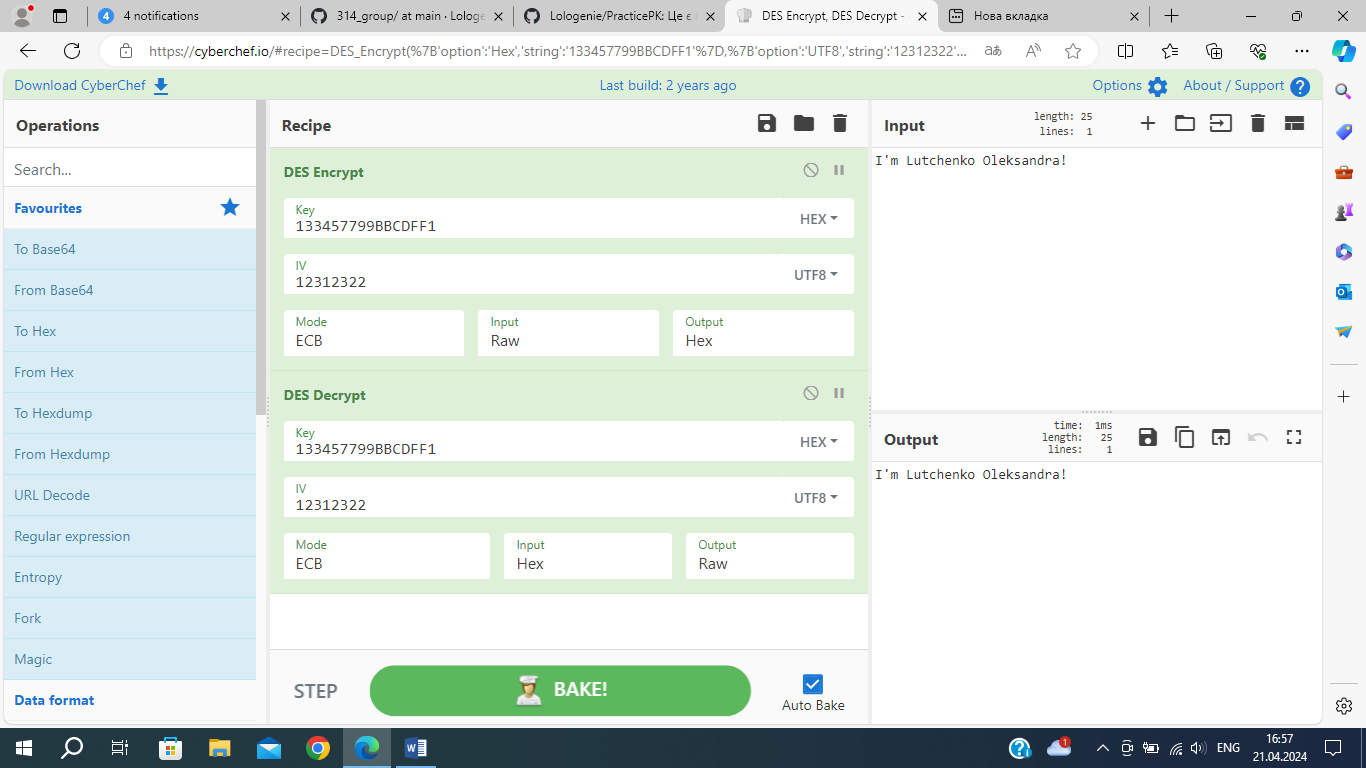
**ENCRYPT:**



**DECRYPT:**



**IN BLOCK:**



1. **MODE CBC**

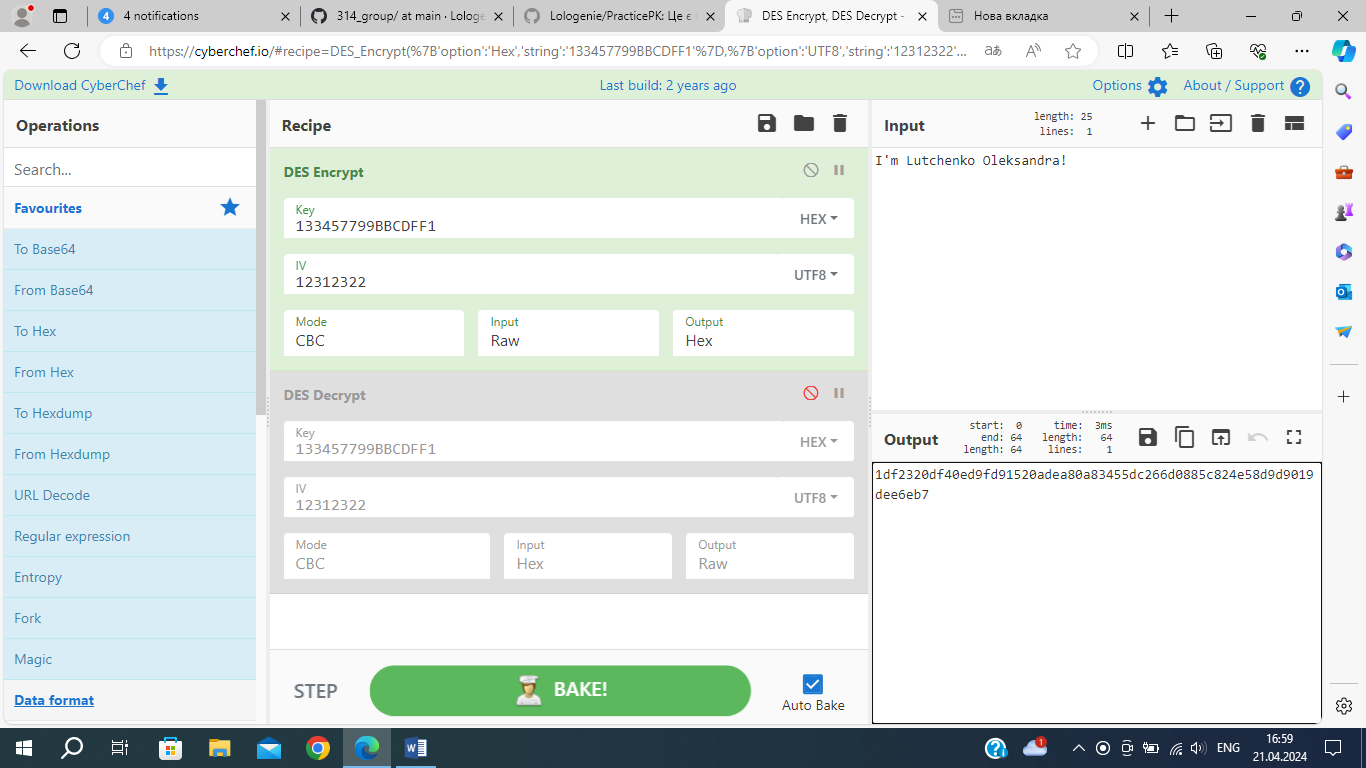
**KEY(HEX):** 133457799BBCDFF1

**IV(UTF-8):** 12312322

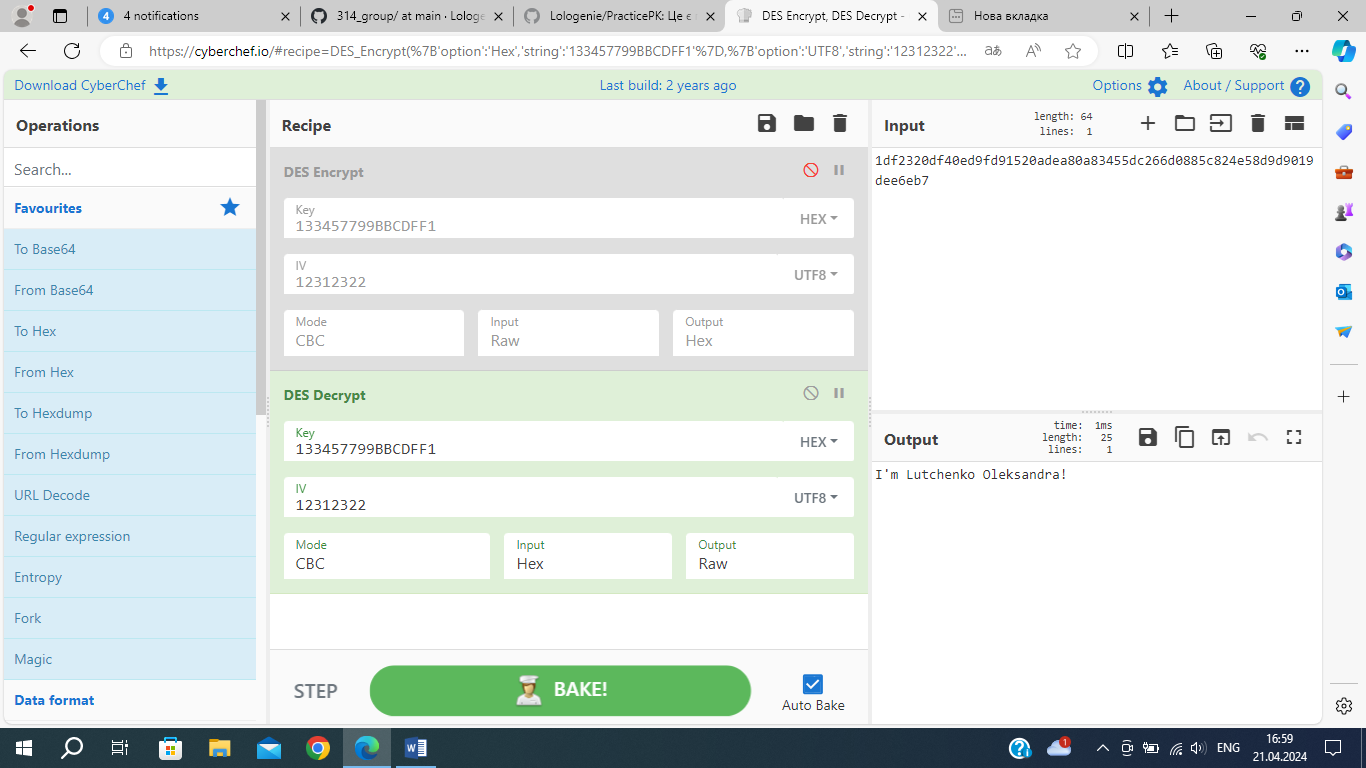
**Відкритий текст:** I'm Lutchenko Oleksandra!

**Шифрований текст:** 1df2320df40ed9fd91520adea80a83455dc266d0885c824e58d9d9019dee6eb7

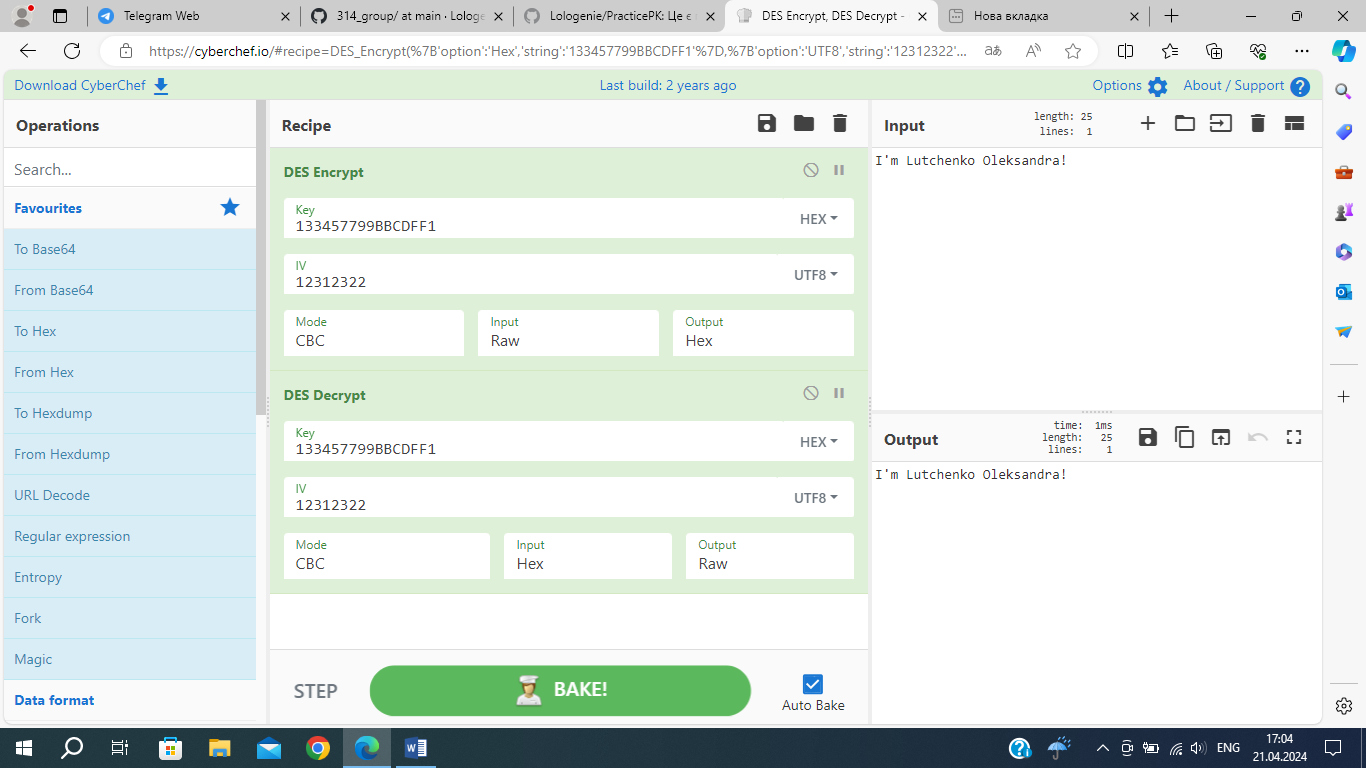
**ENCRYPT:**



**DECRYPT:**



**IN BLOCK:**



1. **MODE CFB**

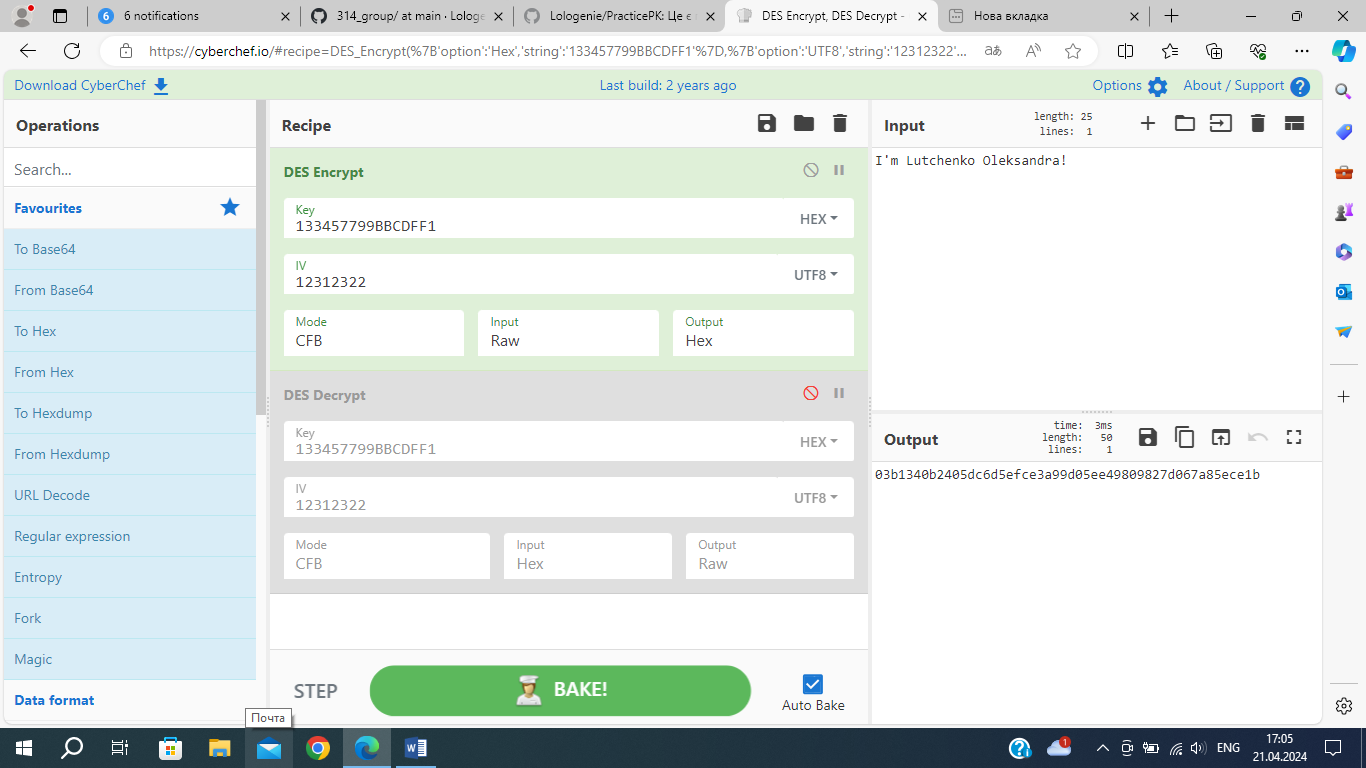
**KEY(HEX):** 133457799BBCDFF1

**IV(UTF-8):** 12312322

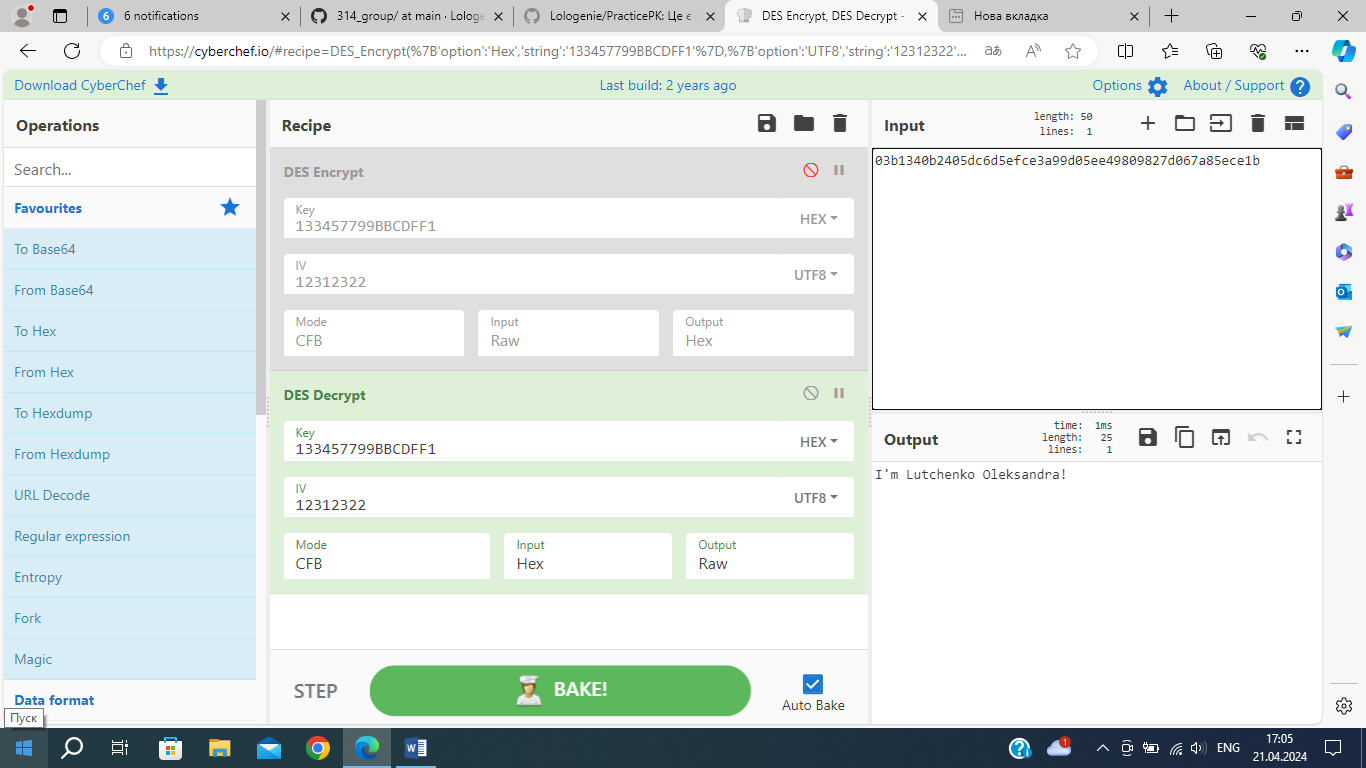
**Відкритий текст:** I'm Lutchenko Oleksandra!

**Шифрований текст:**

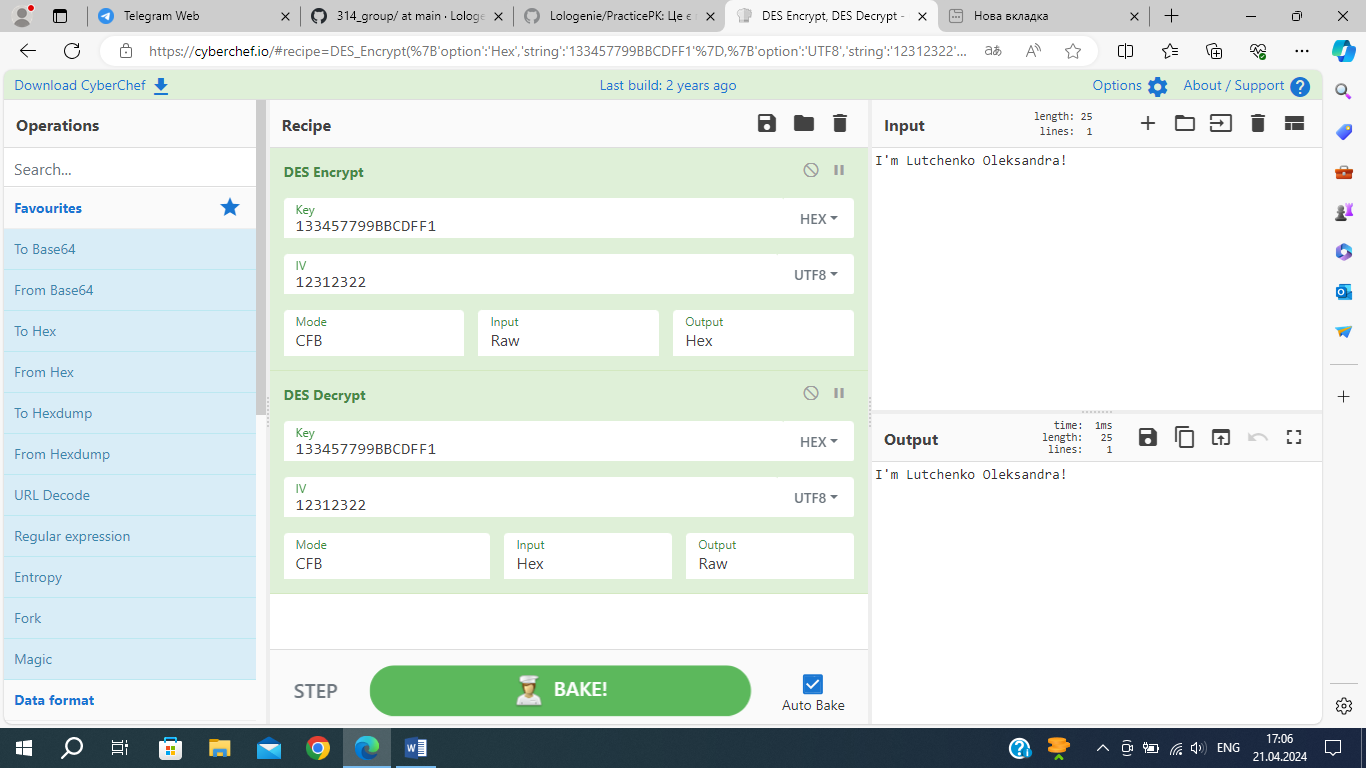
**ENCRYPT:**



**DECRYPT:**



**IN BLOCK:**



1. **MODE OFB**

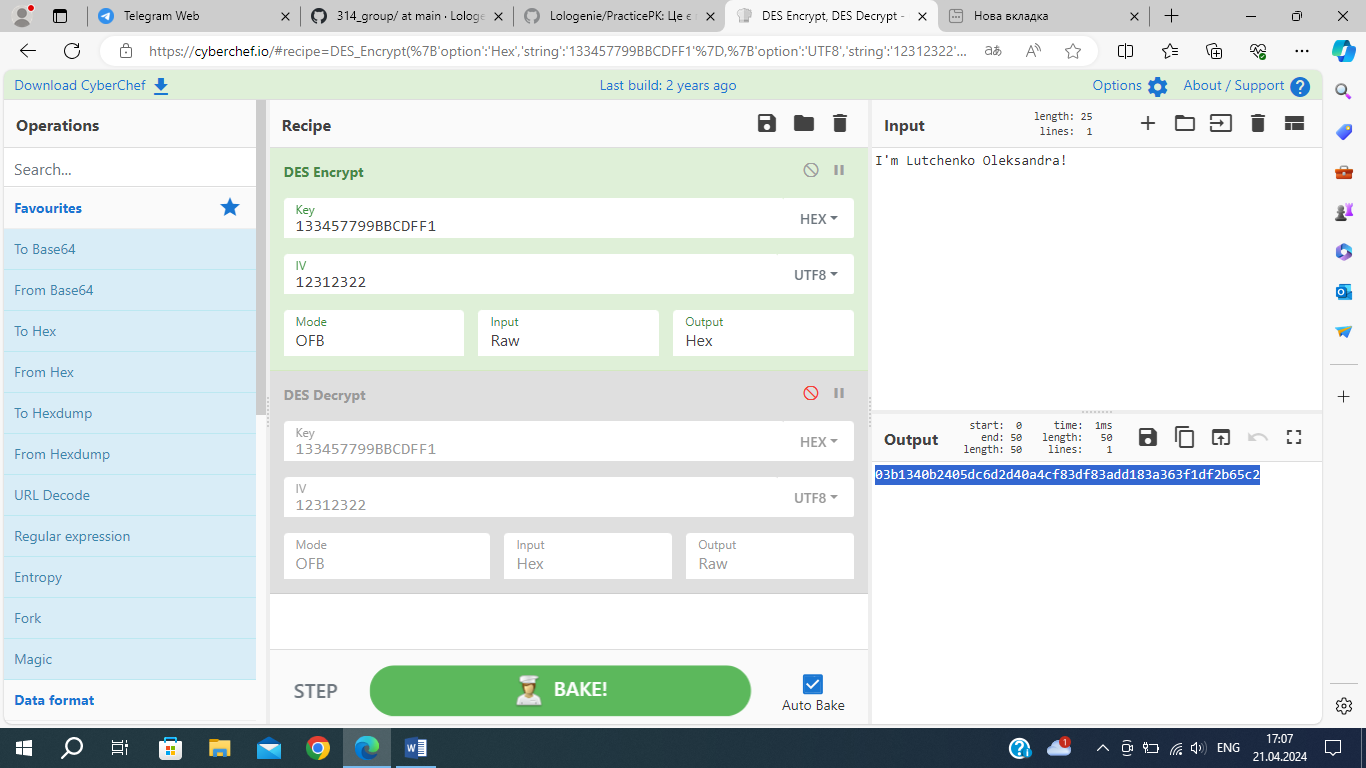
**KEY(HEX):** 133457799BBCDFF1

**IV(UTF-8):** 12312322

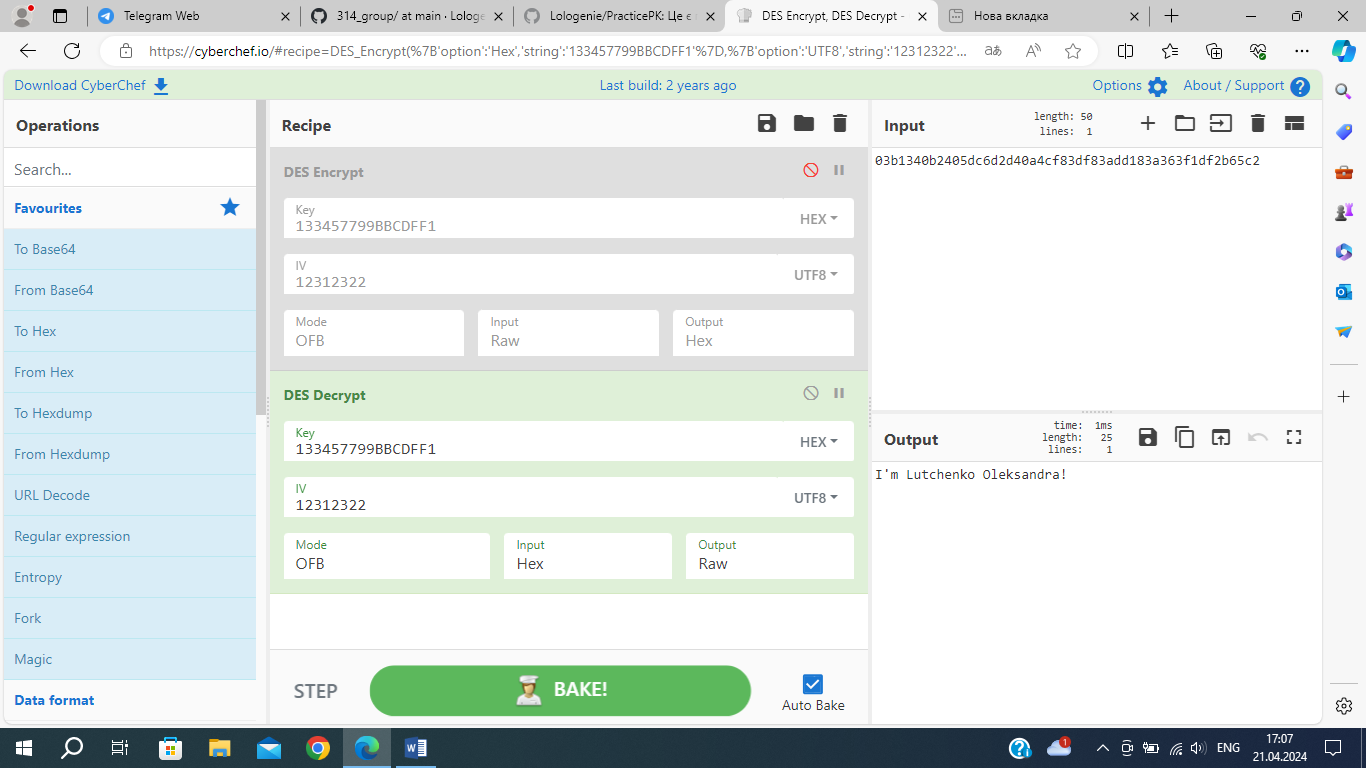
**Відкритий текст:** I'm Lutchenko Oleksandra!

**Шифрований текст:** 03b1340b2405dc6d2d40a4cf83df83add183a363f1df2b65c2

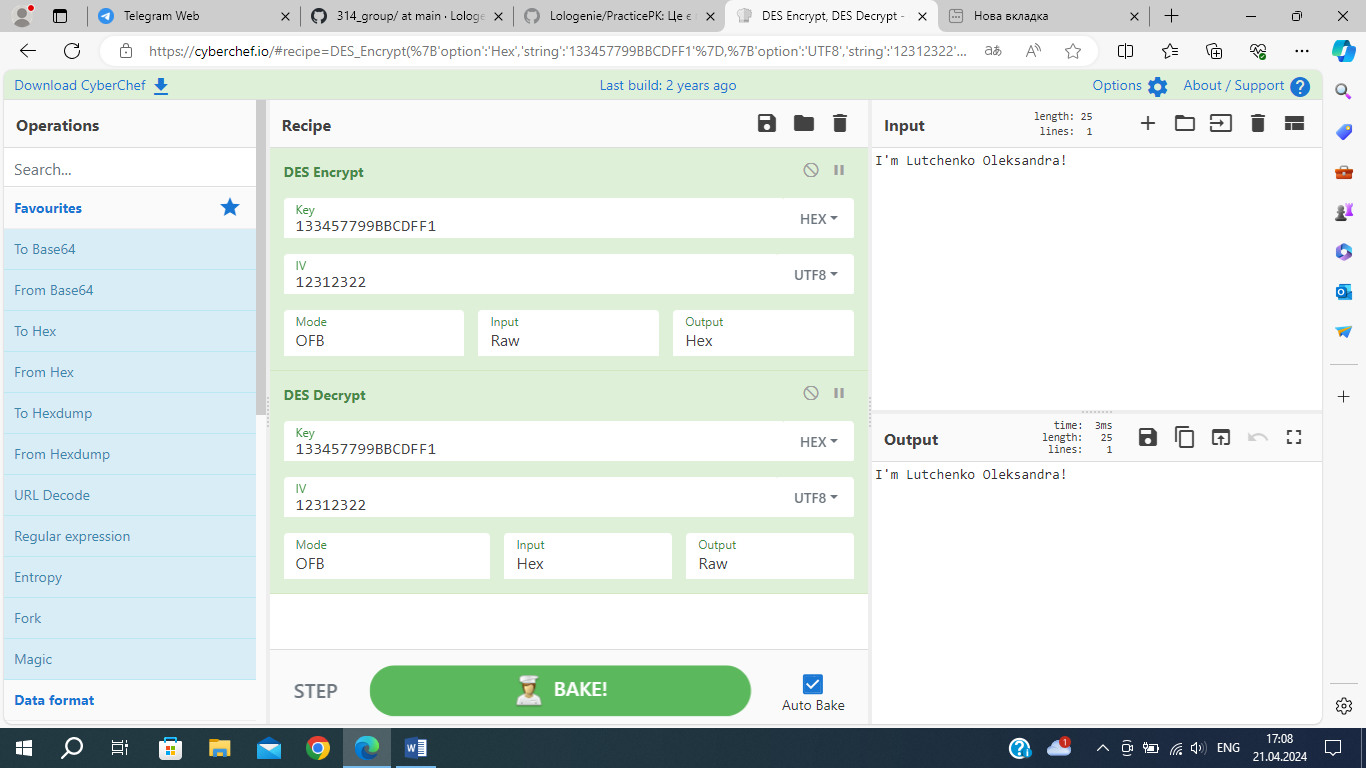
**ENCRYPT:**



**DECRYPT:**



**IN BLOCK:**



1. **MODE CTR**

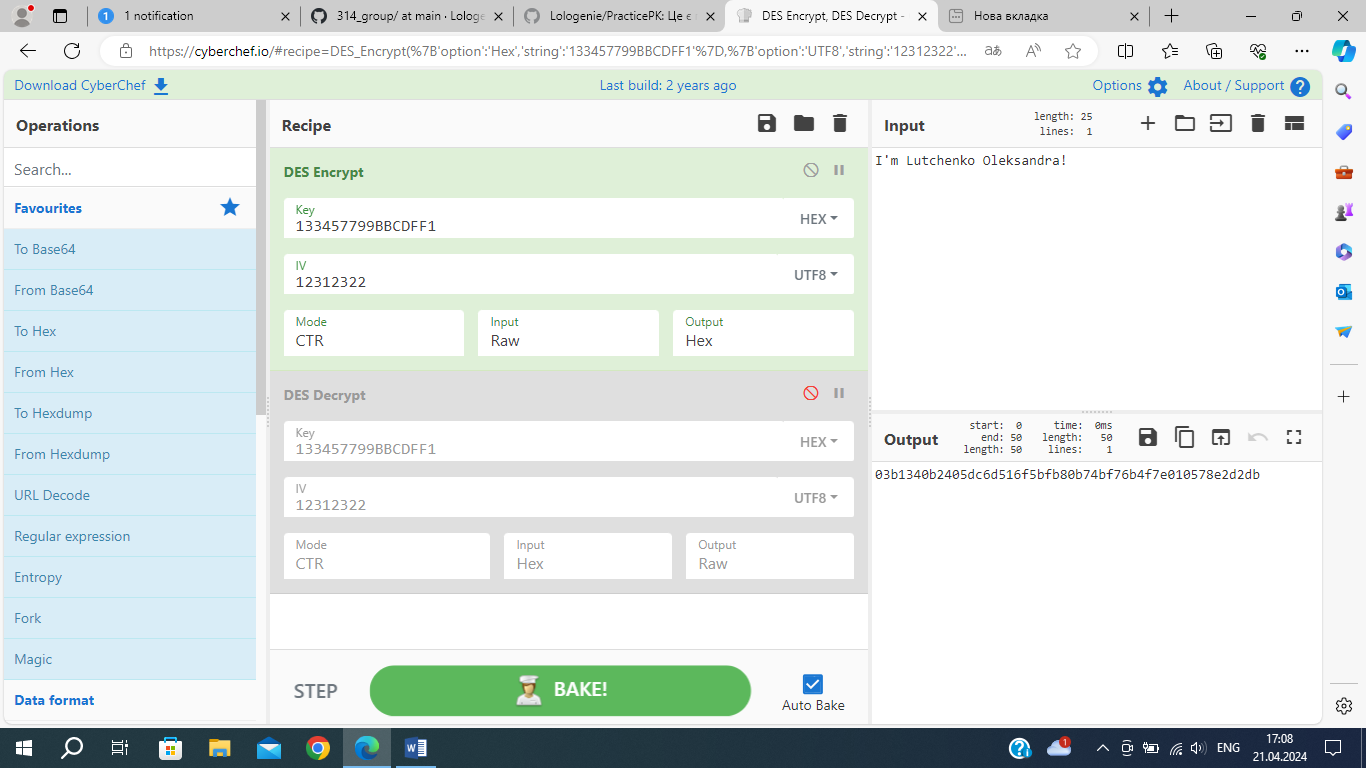
**KEY(HEX):** 133457799BBCDFF1

**IV(UTF-8):** 12312322

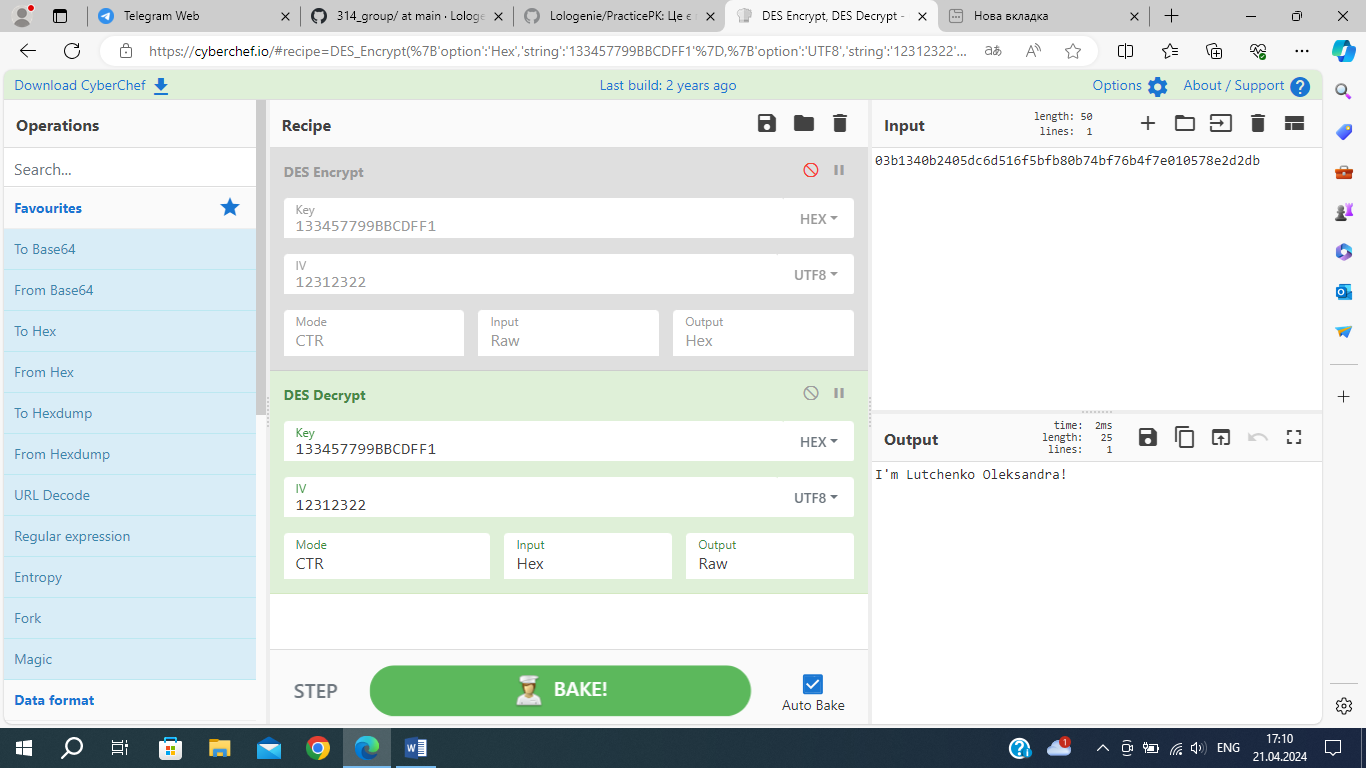
**Відкритий текст:** I'm Lutchenko Oleksandra!

**Шифрований текст:** 03b1340b2405dc6d516f5bfb80b74bf76b4f7e010578e2d2db

**ENCRYPT:**



**DECRYPT:**



**IN BLOCK:**

