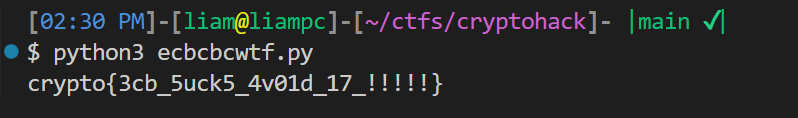
**ECBCBCWTF**

יש לCBC ולECB אותו מפתח, מכיוון שפענוח CBC עובד כך שהוא קודם מפענח ואז עושה XOR עם הIV (על מנת לבטל את הפעולה ההפוכה), ומכיוון שהIV מידע פומבי, ניתן לפענח את הבלוק הראשון ע"י:

*עכשיו יש לנו את הבלוק הראשון בplaintext, אבל הוא גם מהווה את הIV של הבלוק שאחריו.*

*לכן נוכל להמשיך לבצע את אותו התהליך.*

**