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:

$$D_{ECB}(C[1])\oplus IV = (P[1]\oplus IV)\oplus IV = P[1]$$

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

לכן נוכל להמשיך לבצע את אותו התהליך.

```
[02:30 PM]-[liam@liampc]-[~/ctfs/cryptohack]- |main ✓|
$ python3 ecbcbcwtf.py
crypto{3cb_5uck5_4v01d_17_!!!!!}
```