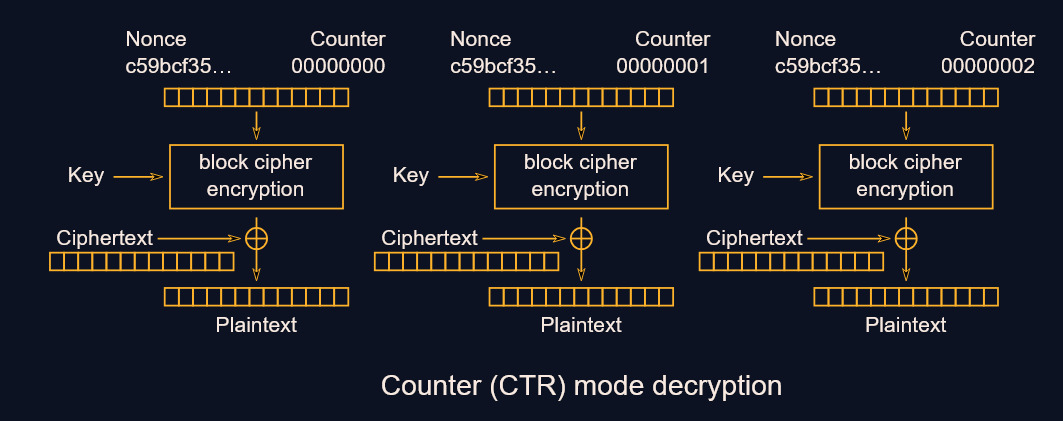
**Stream of Consciousness**

אז יש לנו AES-CTR



מה שמעניין כאן זה שכל החוזק של הצופן מתבסס על כך שהCounter משתנה, כי אחרת MITM יכול להדליף את הCiphertext (שהוא למעשה Counter+Nonce מה שלא ישתנה לעולם אם הCounter לא ישתנה)

וברגע שהוא מודלף ניתן לפענח כל Ciphertext

המחשה טובה לזה היא זו, כעת הקוד מבצע את הדבר הזה:

A computer screen with white text

AI-generated content may be incorrect.

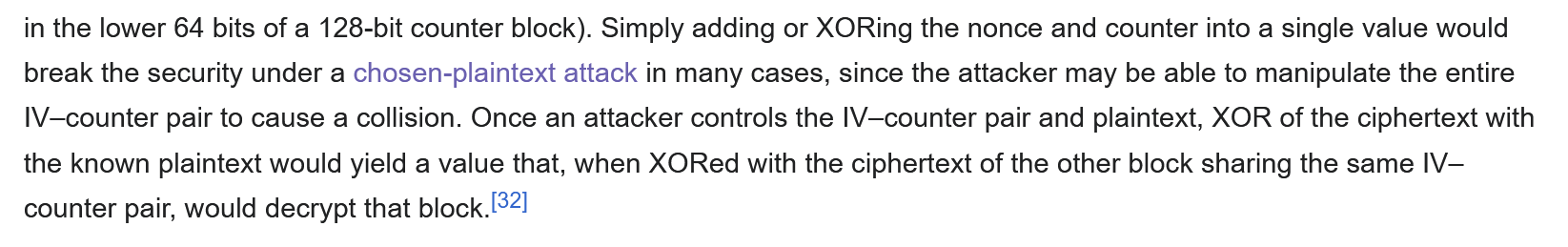
אך הוא אמור לבצע את הדבר הזה:

A screen shot of a computer code

AI-generated content may be incorrect.

למעשה יש פה חולשתיות דומה לזו של ECB – כל pt מתאים לאותו ct. ועדיין, אני יכול רק להצפין, כלומר יש לי את כל הct-ים אבל אפילו לא pt אחד. במידה וכן היה לי pt היה אפשר לנצח בקלות ע"י שכן ctr לא משתנה מה שמשאיר את זה קבוע כמו שכתבתי קודם, ואז נוכל פשוט לפענח הכל ע"י .

אבל נראה שאין לי דרך פיזבילית להשיג זוג ולכן אצטרך למצוא דרך אחרת לנצל את החולשתיות.

**

*זה יכול להיות ממש ממש מעניין, מה שמתבצע זה שרשור ולא חיבור של ערך הnonce והctr. שומר לי בראש.*

*אני יכול להדליף 7 בתים מהcounter אם פשוט אשתמש בסטרינג crypto{ שאני יודע שאמור להיות שם, אבל לא ברור איך אני אגלה מה מהם זה הוא. בכל מקרה שווה לנסות.*

*זה לא לגמרי כיוון שאני אוהב, קראתי בתיעוד של פייתון (לוקאלית) ומצאתי משהו מגניב יותר*

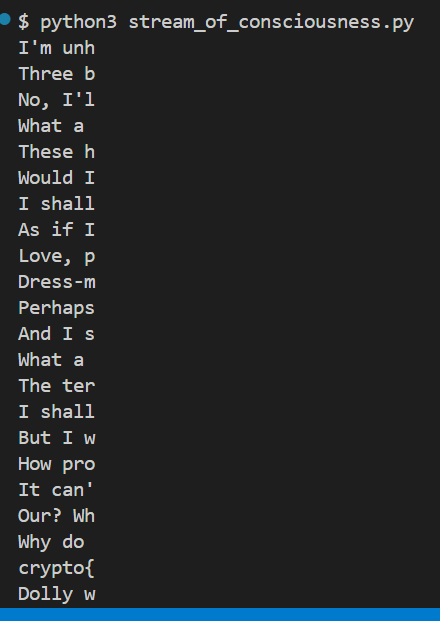
*A black screen with white text

AI-generated content may be incorrect.*

*אז בעצם, 128 זה ביטים, counter value אף פעם לא עולה כי תמיד יוצרים חדש והוא נשאר 1 שזה הinitial\_value והprefix=postfix=empty string?*

*נשמע חולשתי, למעשה אני יודע בדיוק איך הבלוק הזה נראה – 31 אפסים ו1 בסוף.*

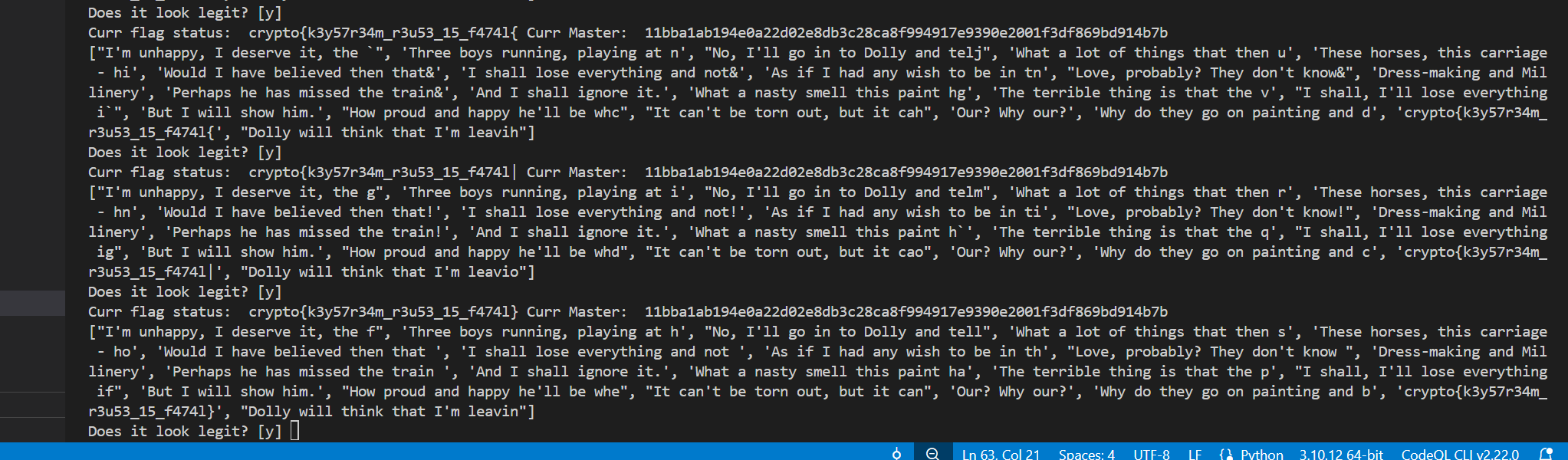
*לא כיוון שעזר לי, חזרתי לנסות להדליף את ההתחלה והצלחתי*

**

*באמת בגלל שיש לי מושג לגבי קצת מהplaintext אני יכול להדליף את ההתחלה של כל המשפטים*

*ואז זה הכה בי – ברוט פורס מוזר יכול לעבוד כאן. אני רק צריך להוסיף בתים למה שכבר מצאתי ולבדוק שכל שאר המשפטים נשארים ascii.*

*פסט פורווד של כמעט שעה להשמשה הכי מצחיקה ומציקה בעולם*

**

*כן. ליטרלי ככה.*

*דגמתי מספיק CTs כדי שיהיה ברור מתי המשפטים הגיוניים, התחלתי עם להדליף בזכות crypto{ 7 בתים ואז ניסיתי בית אחר בסוף בכל פעם, במידה והתוצאה של המפתח הנוכחי (כלומר כמות הבתים הנכונים שאספתי + הבית שאני מנסה עכשיו) XOR הCT מביא PT הגיוני אני ממשיך ומוסיף את הבית הנוכחי, החולשה היא עדיין העובדה שאני לא צריך לדעת את המפתח כדי להבין את הערך שכל הStream מוצפן איתו.*

*מעייף, בטוח יש דרך יותר טובה, אבל עכשיו אני רמה 12 בקריפטוהאק*

*crypto{k3y57r34m\_r3u53\_15\_f474l}*