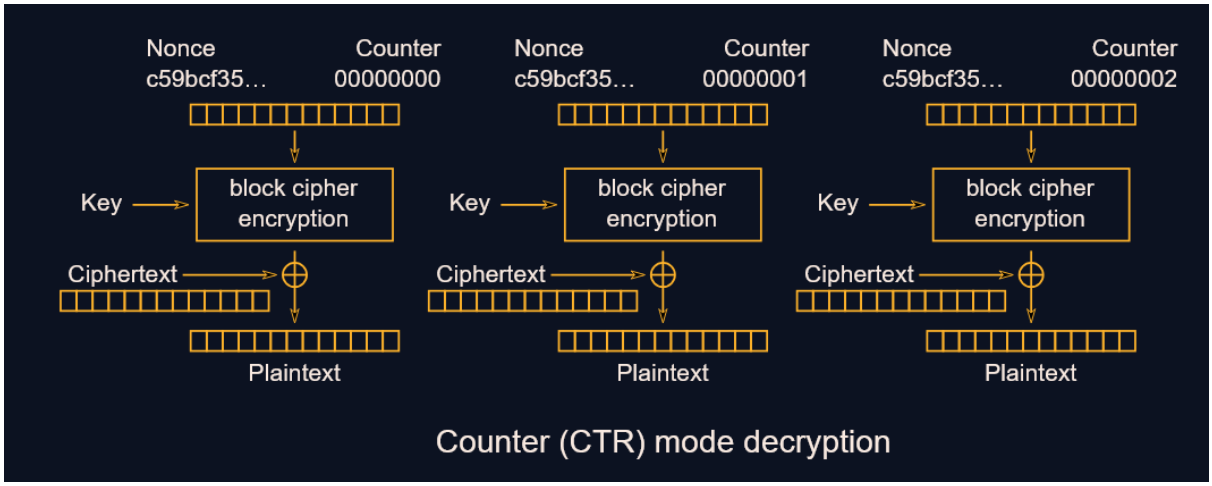
Stream of Consciousness

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:

```
>>> cipher = AES.new(KEY, AES.MODE_CTR, counter=Counter.new(128))
>>> cipher.encrypt(b"Hello")
b'w\x03A<\xd5'
>>> cipher = AES.new(KEY, AES.MODE_CTR, counter=Counter.new(128))
>>> cipher.encrypt(b"Hello")
b'w\x03A<\xd5'
>>> cipher = AES.new(KEY, AES.MODE_CTR, counter=Counter.new(128))
>>> cipher.encrypt(b"Hello")
b'w\x03A<\xd5'
>>> |
```

אך הוא אמור לבצע את הדבר הזה:

```
>>> cipher.encrypt(b"Hello")
b'w\x03A<\xd5'
>>> cipher.encrypt(b"Hello")
b'\xa8\x92X\x120'
>>> cipher.encrypt(b"Hello")
b'[}\xa2\xf8\xa7'
```

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 $pt \oplus ct = AES_{CTR}(nonce + ctr)$ שכן ctr לא משתנה מה שמשאיר את זה קבוע כמו שכתבתי קודם, ואז נוכל פשוט לפענח הכל ע"י $AES_{CTR}(nonce + ctr) \oplus ct = pt$.

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

in the lower 64 bits of a 128-bit counter block). Simply adding or XORing the nonce and counter into a single value would break the security under a chosen-plaintext attack in many cases, since the attacker may be able to manipulate the entire IV–counter pair to cause a collision. Once an attacker controls the IV–counter pair and plaintext, XOR of the ciphertext with the known plaintext would yield a value that, when XORed with the ciphertext of the other block sharing the same IV–counter pair, would decrypt that block.[32]

זה יכול להיות ממש ממש מעניין, מה שמתבצע זה שרשור ולא חיבור של ערך ה*nonce* ו*ctr*. שומר לי בראש.

אני יכול להדליף 7 בתים מה*counter* 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

```
Each call to the function returns the next counter block.
Each counter block is made up by three parts:

+------+--------------+-------+
|prefix| counter value|postfix|
+------+--------------+-------+

The counter value is incremented by 1 at each call.
```

אז בעצם, 128 זה ביטים, *counter value* אף פעם לא עולה כי תמיד יוצרים חדש והוא נשאר 1 שזה ה*initial_value* ו*prefix=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

```
$ python3 stream_of_consciousness.py
I'm unh
Three b
No, I'l
What a
These h
Would I
I shall
As if I
Love, p
Dress-m
Perhaps
And I s
What a
The ter
I shall
But I w
How pro
It can'
Our? Wh
Why do
crypto{
Dolly w
```

באמת בגלל שיש לי מושג לגבי קצת מה*plaintext* 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

```
Does it look legit? [y]
Curr flag status:  crypto{k3y57r34m_r3u53_15_f4741{ Curr Master:  11bba1ab194e0a22d02e8db3c28ca8f994917e9390e2001f3df869bd914b7b
["I'm unhappy, I deserve it, the `", 'Three boys running, playing at n', "No, I'll go in to Dolly and telj", 'What a lot of things that then u', 'These horses, this carriage
 - hi', 'Would I have believed then that&', 'I shall lose everything and not&', 'As if I had any wish to be in tn', "Love, probably? They don't know&", 'Dress-making and Mil
linery', 'Perhaps he has missed the train&', 'And I shall ignore it.', 'What a nasty smell this paint hg', 'The terrible thing is that the v', "I shall, I'll lose everything
 i`", 'But I will show him.', "How proud and happy he'll be whc", "It can't be torn out, but it cah", 'Our? Why our?', 'Why do they go on painting and d', 'crypto{k3y57r34m_
r3u53_15_f4741{', "Dolly will think that I'm leavih"]
Does it look legit? [y]
Curr flag status:  crypto{k3y57r34m_r3u53_15_f4741| Curr Master:  11bba1ab194e0a22d02e8db3c28ca8f994917e9390e2001f3df869bd914b7b
["I'm unhappy, I deserve it, the g", 'Three boys running, playing at i', "No, I'll go in to Dolly and telm", 'What a lot of things that then r', 'These horses, this carriage
 - hn', 'Would I have believed then that!', 'I shall lose everything and not!', 'As if I had any wish to be in ti', "Love, probably? They don't know!", 'Dress-making and Mil
linery', 'Perhaps he has missed the train!', 'And I shall ignore it.', 'What a nasty smell this paint h`', 'The terrible thing is that the q', "I shall, I'll lose everything
 ig", 'But I will show him.', "How proud and happy he'll be whd", "It can't be torn out, but it cao", 'Our? Why our?', 'Why do they go on painting and c', 'crypto{k3y57r34m_
r3u53_15_f4741|', "Dolly will think that I'm leavio"]
Does it look legit? [y]
Curr flag status:  crypto{k3y57r34m_r3u53_15_f4741} Curr Master:  11bba1ab194e0a22d02e8db3c28ca8f994917e9390e2001f3df869bd914b7b
["I'm unhappy, I deserve it, the f", 'Three boys running, playing at h', "No, I'll go in to Dolly and tell", 'What a lot of things that then s', 'These horses, this carriage
 - ho', 'Would I have believed then that ', 'I shall lose everything and not ', 'As if I had any wish to be in th', "Love, probably? They don't know ", 'Dress-making and Mil
linery', 'Perhaps he has missed the train ', 'And I shall ignore it.', 'What a nasty smell this paint ha', 'The terrible thing is that the p', "I shall, I'll lose everything
 if", 'But I will show him.', "How proud and happy he'll be whe", "It can't be torn out, but it can", 'Our? Why our?', 'Why do they go on painting and b', 'crypto{k3y57r34m_
r3u53_15_f4741}', "Dolly will think that I'm leavin"]
Does it look legit? [y]
```

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 ה*Stream* מוצפן איתו.

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

crypto{k3y57r34m_r3u53_15_f474l}