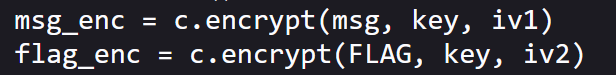
**Dancing Queen**

קיבלנו קוד פייתוני המממש את ChaCha20, בנוסף הנתונים:

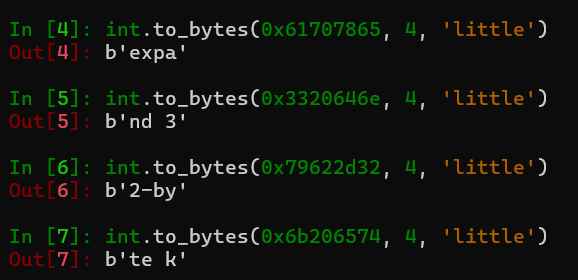
* מפתח רנדומלי בגודל 32 בתים
* צמד של Pt-Ct
* הCt של הדגל

לא מכיר ChaCha20 אבל הדבר הראשון שצץ זה שמשתמשים בself.\_counter במימוש של encrypt, אבל הוא גם מוגדר שם ומאותחל ל1. כלומר בקריאות הבאות:



המונה נשאר זהה ומהווה דפוס בהצפנה שאולי נוכל להשתמש בו.

לאחר סרטון קצר של Computerphile הבנתי שזה לא באג שהCounter מתאפס, זה בהגדרה. חשבתי בהתחלה גם שהסטרינג הקבוע הוא בendianess שגוי אבל נראה שמפרשים אותו כlittle endian



חשבתי שמצאתי את החולשה כשראיתי שמבצעים רק 10 סיבובי ChaCha על כל בלוק, אבל בפועל אלו 10 איטרציות שמבצעות 8 (ולא 4) רבעי-סיבוב ולכן כן יש 20 סיבובים.

לאחר עוד זמן צללתי לRFC של ChaCha להבין מה דה פאק זה רוצה ממני – ואז הבנתי, בRFC יש את הפסודו-קוד הבא:

A screen shot of a computer code

AI-generated content may be incorrect.

במימוש של חברנו יש את הקוד הבא:

A computer screen with white text

AI-generated content may be incorrect.

לכאורה קשה לראות את ההבדל, שניהם פועלים על בלוק, מאתחלים את הState בצורה נכונה (וידאתי), מבצעים 20 סיבובי ChaCha (10 סיבובים כפולים), ובסוף מבצעים XOR (כמו שיש בפסודו-קוד [הזה](https://datatracker.ietf.org/doc/html/rfc8439#section-2.4.1))

אבל שימו לב שלאחר כל טיפול בבלוק, המימוש של ChaCha20 בRFC מעדכן את הInitial State ושלנו לא!

נוכל לבדוק את זה 😊 [הם היו נדיבים וסיפקו לנו דוגמא](https://datatracker.ietf.org/doc/html/rfc8439#section-2.4.2)

אולי אפשר פשוט לשחזר? – [משהו כזה](https://crypto.stackexchange.com/questions/77628/is-the-chacha20-block-function-reversible-using-known-plaintext), התחלתי לקרוא את התגובה הראשונה ועצרתי, הבנתי שכנראה יש כאן משהו. בסך הכל קצת Xor,Add,Rotate – אין סיבה שלא נוכל לשחזר את זה!

אז הרעיון הכללי יהיה כזה:

1. נשתמש בצמד Pt-Ct שלנו כדי לשחזר את רצף המפתחות
2. משם ניקח את 64 הבתים הראשונים כדי לבנות את הState הראשונה מחדש
3. מכיוון שהיא פשוט מקיימת , נפעיל את שנממש בהקדם
4. מהinitial\_state נשחזר את המפתח
5. נקרא לdecrypt וננצח!

אחרי Poc קצר כתבתי את הפונקציות הבאות:

A screen shot of a computer code

AI-generated content may be incorrect.

A black background with white text

AI-generated content may be incorrect.

וזה אשכרה עבד!

עכשיו ננצח

