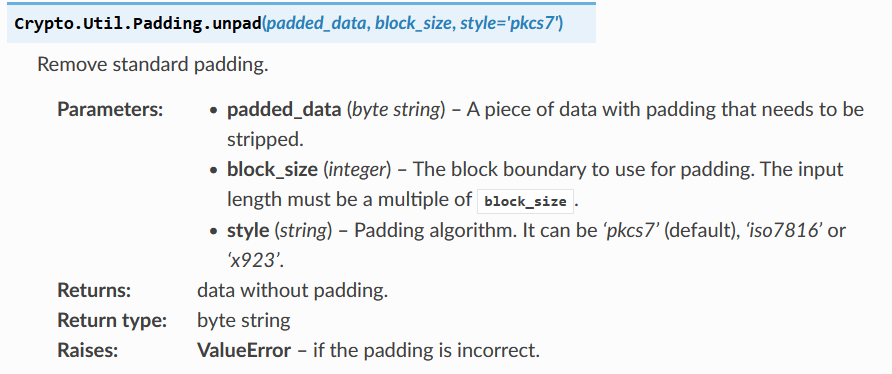
**Pad Thai**

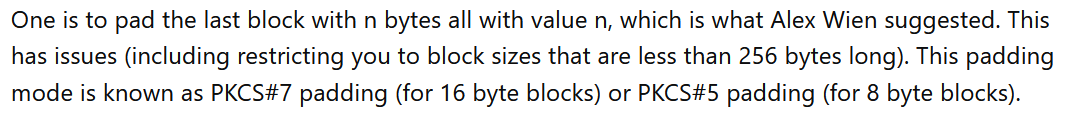
אין פה הרבה קוד, מתחילים עם מפתח קבוע מגונרט רנדומלית, הודעה רנדומלית שתופסת בלוק אחד בדיוק ו-IV רנדומלי שאינו קבוע 😊 כלומר החולשה היא לא בקינפוג הAES

יש לנו יכולת לקרוא לget\_ct שמביאה לנו את ההודעה עם IV שונה בכל פעם, לcheck\_message שתבדוק אם ההודעה שהכנסנו זהה להודעה הסודית ואם כן תביא לנו דגל ולcheck\_padding.

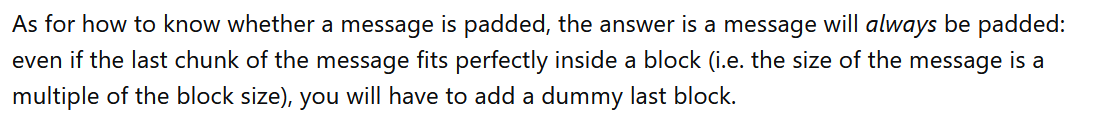
המעניינת היא כמובן check\_padding, ספציפית מתבצע unpad(plaintext, 16) ואם הpadding נכון חוזר True, אחרת False.



אז פונקציית הunpad מקבלת 3 פרמטרים, המידע, גודל הבלוק וסוג הפדינג. נראה שהכל נכון אז נצטרך לקרוא על pkcs7 padding.



אז מסתבר שpkcs#7 זה פשוט למלא את שאר הבלוק עם בתים שהערך שלהם זה הגודל שמשלים אותו ל16.



זה מגניב – תמיד יהיה padding למרות שבמקרה הזה ההודעה שלנו בגודל בלוק בלבד.

לאחר קצת מחשבה עלה לי כיוון מעניין, יש לי שליטה על הIV שמשומש בפענוח ואני יודע (ובדקתי עם אתגר קודם) שAES מבצע Decrypt ואז XOR עם הIV, משהו מגניב שאני יכול לעשות זה brute-force מוזר לפי סכמת הפדינג.

משהו בסגנון של:

* נוריד את בלוק הפדינג ונשאר עם 2 בלוקים בלבד, IV וCT
* נשנה את הבית האחרון בIV כל פעם עד שunpad מחזירה true, במקרה הזה אני יודע שמתקיים ומכיוון שXOR אסוציאטיבי אני יכול לקבוע ש
* לאחר שיש לי את הערך הזה אני יכול לחשב ולקבל , ולבצע והפעם יתקיים (הנקודה היא שאחרי שעשינו ברוט-פורס כדי לגלות את הערך שיביא ל1, אפשר בזמן קבוע לחשב מה צריך לעשות כדי שהבית הPT יהפוך ל2)
* ואז נעשה ברוט-פורס על הבית ה14 בIV כדי לגלות מה יביא את הבית ה14 בPT להיות 2...

וככה נבצע שוב ושוב, הסיבוכיות תהיה 😊

מכאן כדי לגלות את ההודעה נצטרך רק לפתור 16 משוואות בסגנון של

ולאחר התפסטנות כהוגן על מימוש יעיל בפייתון וכל מני הסרות חלודה, הבנתי שקרתה פדיחה. הרצתי את השרת לוקאלית ואני קולט שהצפנו 32 בתים (כי message.encode(‘ascii’)), מה שאומר שלא מספיק לי להדליף בלוק אחד. יתרה מכך – שיחקתי עם זה קצת והצלחתי להדליף בלוק אחד, עכשיו צריך להבין איך מכלילים את המתקפה לn בלוקים.

ואז נזכרתי שאני לא מהנדס ביטים אלא עושה קריפטו, בסוף – אין הבדל בין אם הIV המשומש הוא הבלוק ה0 או ה1, לבלוק השני הIV הוא הבלוק ה1, אני יכול לעשות בדיוק אותו דבר עליו כמו שעשיתי לIV המקורי (שהוא הIV לבלוק הראשון)

עכשיו רק נותר לחכות להצלחה

A screen shot of a computer

AI-generated content may be incorrect.

בזמן הזה אני אבהיר את המשוואה שיש בסוף.

נניח שהIV באינדקס 15 הוא 0x4, כדי שהpadding יהיה נכון צריך להתקיים (בבלוק עם פדינג מגדול 1)

אנחנו יודעים את IV ואת ה0x1 כמובן, אז מה נשאר לעשות כדי להדליף את הבלוק?

ברוט-פורס על ערך x כלשהו שעבורו נבצע כדי שנהפוך את הפדינג של הבלוק לפדינג בגודל 1 (הדרך שהאלגוריתם של הפדינג מגלה כמה גדול הפדינג זה לקרוא את הערך שבבית הזה ולכן הוא יחשוב שהפדינג הוא 1, בלי תלות בכמה הפדינג באמת)

ברגע שנמצא את זה נוכל לשחזר את בקלות ע"י

כמובן שאת זה נכליל לn כללי כדי להדליף את כל הבלוק, כדי להדליף כמה בלוקים פשוט חוזרים על זה ככמות הבלוקים ומשנים את IV בהתאם.

A screenshot of a computer program

AI-generated content may be incorrect.