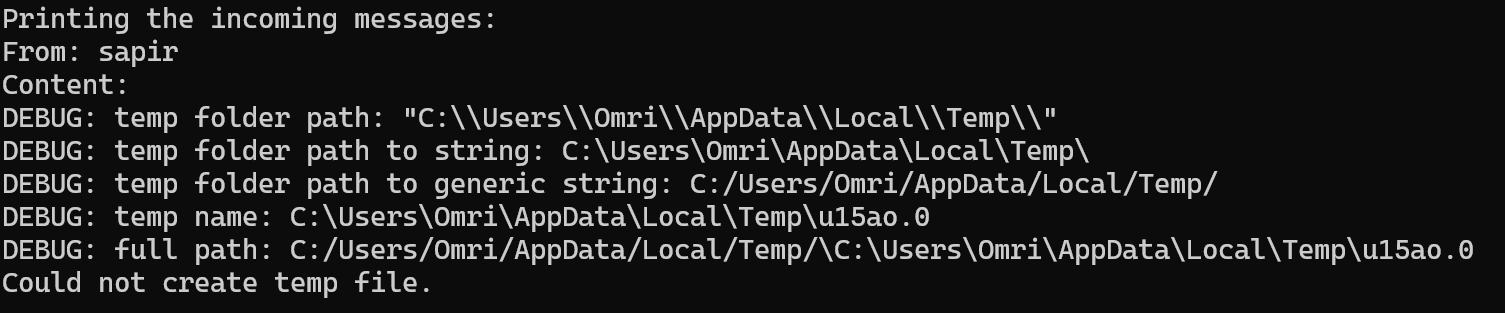
**מעקב פרויקט בדפנסיבי**

**שרת בפייתון**

1. ~~להתחיל Template לשרת בסיסי רצח, שמתחיל בפונק' main.~~
2. ~~לעשות שהוא יעבוד~~ **~~בריבוי משתמשים~~** ~~ע"י threads או selector.~~
3. ~~גרסת השרת תהיה 1~~ (אם אני לא משתמש בSQL).
4. ~~לקרוא מקובץ, להיעזר בדרישות ובפונק' שכבר עשיתי בממן 14, לשים לב לדרישה אם הקובץ לא קיים.~~
5. ~~ליצור מחלקה לבסיס נתונים, עם פונק' בסיסיות – לפי מה שדרוש.~~
6. עשיתי מחלקה של בקשה, שמקבלת בקשה ומפרסרת אותה:  
   א' לוודא שעשיתי כמו שצריך ושהנתונים נאספים בתצורה הנכונה (אולי צריך להמיר חלק למספר / מחרוזת או משהו בסגנון? או בכלל לא להמיר? לעבור בדיוק על איך עשיתי ב14 ולתקן בהכול!!!! (גם בrequest וגם בmessage).  
   ב' ~~לכתוב פונק' שממשיכה לפרסר כמו שצריך את הmessages~~
7. ~~לכתוב פונקציות המשך לכל אחת מסוגי הבקשות שם, לפי מה שעשיתי בTODO, שממש עושות כל אחד מהדברים כמו שדרוש.~~
8. ~~לעשות את הכנ"ל רק עם ההודעות^^^^^^^~~
9. ~~להוסיף בדיקה שהusername הוא לפי הפורמט איפה שהוא.~~
10. להוסיף בדיקה שכל המספרים הם תקינים, לפי מה שעשיתי בממ"ן 14.
11. לוודא האם כדאי לי לשמור את השם משתמש בבסיס נתונים כTEXT או varchar(255).
12. להוסיף מחלקה של response (או מחלקות ויורשות וכו?) ולהתחיל להכין את התגובות בחזרה, **לוודא** שאני שולח את הכול כמו שצריך, עם padding של \0 לstr שקטן מ255 (למשל שם משתמש).
13. לעשות Unit test לדברים האלו איכשהו.
14. **רועי** מתעקש שצריך לוודא שמה שאנחנו מקבלים בפורמט little endian??????? לבדוק האם סוג המערכת הוא big endian ולהמיר את הכול במידה וכן..........
15. משהו משתבש בחלק של פייתון כאשר אני מעביר את המפתח הסימטרי שמוצפן בעזרת הציבורי של לקוח אחר. זה ממש מעביר בתים אחרים.. **לדבג ולתקן.**
16. **לכתוב תיעוד להכול**
17. לעבור על כל הקוד ולוודא שלא כתוב שורות סרק ושעשיתי הכול כמו שצריך.
18. לוודא שבכל תקלה בצד שרת פשוט להחזיר general error **ולא** להקריס את השרת (אלא אם זו תקלה ממש בתחילת ריצת השרת).

**Client בCPP**

1. ~~להתחיל להכין את המחלקות במבנה דומה לשרת, ובהשראה למה שעשיתי ל-14.~~
2. ~~להכין את הממשק הכללי והלולאה הכללית, עם כל הפונק' הדרושות.~~
3. ~~להתחיל לעבוד על ההצפנה!~~
4. ~~כשאני מכין את הבקשה מסוג הודעה, לזכור להוסיף~~ **~~גם~~** ~~לגודל של שpayload~~ **~~וגם~~** ~~לשל הmessage content size את הגודל של ההודעה!~~
5. ~~כשאני בונה את הקוד שמקבל את רשימת הלקוחות, ליצור וקטור זמני שמכיל את הclass של clientlistresponse~~ **~~או~~** ~~שאולי עדיף בעצם לעשות רק לattributes של זה, בלי כל הversion,request וכו... – קיצר לעבוד על זה.~~
6. ~~לכל החלק של ההתחברות עם הרשת ובדיקת קובץ וכו – לעבור שם~~ **~~כמו~~** ~~שצריך- לסדר את הפונקציות, מתי אני מתחבר לרשת, להוסיף ניהול שגיאות, ולהעביר את~~ **~~כל~~** ~~הנתונים כמו שצריך.~~
7. **~~לכתוב פונק' שמוודאת קובץ server.info תקין כמו שצריך~~**~~. לעבור על זה עם אפרת.~~
8. **~~אולי~~** ~~חשוב לשמור את השם משתמש והid כmap בעצם?~~
9. **~~רועי~~** ~~מתעקש שצריך לוודא שמה שאנחנו מקבלים בפורמט little endian??????? לבדוק האם סוג המערכת הוא big endian ולהמיר את הכול במידה וכן..........~~
10. לעבור על כל הTODOS
11. לעשות את הפונקציה הזאת של verify שמוודאת שמה שהתקבל הוא באמת מספרים? האם זה רלוונטי? **כמו שעשיתי בממן 14, לא זוכר בכלל מה הסיבה**.
12. ~~לשנות את הסדר של הדברים ככה שאני~~ **~~מתחבר~~** ~~באמצעות הסוקט~~ **~~רק~~** ~~אחרי שהיוזר הכניס קלט כמו שצריך (או במקרה אחר, רק אחרי שכבר ליטרלי הכנסתי את כל הדברים כמו יוזרניים וכו...)~~
13. ~~לשנות את clienthandler ככה שתשמור את הclientid אחרת, כרגע זה שמור בצורה הזויה וגם לא נכונה. אולי עדיף פשוט כמחרוזת...~~
14. ~~להבין מה לעשות עם הפונקציה של send, שבחלק הייתי צריך ליצור פוינטר חדש ממש לסוג הספציפי, זה לא אמור פשוט לעבוד לבד עם ירושה...?~~
15. להוסיף אופציה שאם רשימת הלקוחות **בזיכרון** ריקה לא להמשיך הלאה באף אחד מהשלבים שבהם צריך שם של לקוח ספציפי. **גם** לעשות פונק' שבודקת את כמות הלקוחות בזיכרון **וגם** להשתמש בה.
16. ~~צריך להצפין עוד איזה חלק בהודעות ולא הבנתי נכון את המשימה??? לול~~
17. לשנות את הגודל המקסימלי של קובץ וטקסט ל4bytes **פחות** הmessage header!!!!
18. ~~משום מה, כאשר מבקשים טקסט אז הוא מחכה ל-2 שורות (בשליחת קובץ טקסט). להבין למה ולתקן.~~
19. ~~למה לעזאזל המפתח הסימטרי לא עובד???~~
20. ~~בעיה מוזרה שכאשר אני מנסה לשלוח בקשת 152 שליחת מפתח סימטרי, הוא שולח קוד בקשה בהקסא, ואז גם המספר מתפרש אחרת בפייתון, והכול מתחרבש כולל המפתח. לדעתי זה משהו עם הבנאי של message ואיך שזה קורא לrequest. לעבור על זה!!!~~
21. **~~משהו משתבש בתהליך של ההצפנה והפענוח. לדבג ולהבין האם הpublic key נשלח, נשמר ומפורש כמו שהוא נוצר. אם לא, בגדול- אני לא מבין איפה הבעיה בפענוח. אולי משהו משתבש בטקסט המוצפן עצמו??~~**
22. ~~לוודא שכשאני מחזיר הודעות מהשרת, להוסיף בPAYLOAD את הגודל של~~ **~~כל~~** ~~ההודעות ביחד, ואז בלקוח לוודא שזה הכמות שאני קורא (במקום מה שאני עושה כרגע שזה לוודא שאני סיימתי לקרוא, סתם מיותר...)~~
23. האם אני ממיר את הid לשטות הזו של hexa ובחזרה בכל גישה לקובץ me.info???
24. לוודא שכל סוג של הודעה שאני שולח מדפיסה הודעה אחרת (נגיד מפתח סימטרי תדפיס נשלח מפתח סימטרי ללקוח X וכנ"ל לטקסט וקובץ וכו.........)
25. לוודא שכאשר אני מקבל את המספרים בresponse, כאשר אני ממיר אותם (מבחינת endianness) inplace זה **באמת** עושה את זה, בגדול עדיף פשוט לשמור במשתנה זמני ולשלוח אותו.
26. לוודא שכאשר אני שולח קובץ, זה שומר כמו שצריך במיקום הנכון ומדפיס את **המיקום** ולא את תוכן הקובץ (זה מה שמבקשים, נראה לי?)
27. **לוודא עם רועי** שכשאני שולח קובץ אז לקרוא כבינארי (צריך?) ולא לשמור על הסוג קובץ המקורי כאשר אני יוצר שם זמני. והאם יש הנחיות לשם זמני? ובכללי מה דרוש לזה ~~~~
28. לעדכן את כל מה שרלוונטי ואז ליצור שוב פעם בשם client2 ולדבג!
29. להוסיף חתימות לכל הפונקציות בcpp בקובץ hpp.
30. להוסיף תיעוד להכול!!!!!!

**הצפנה כללי**

-**כל ההצפנות והפענוחים קורים אצל הCPP, אז בקיצור – להתחיל CPP!!!!**  
**החלפת הודעות**

1. לקוח A מבקש מהשרת את המפתח **הציבורי** של לקוח B. - **בקשה רגילה 602.**
2. לקוח A שולח הודעה (דרך השרת) ללקוח B מסוג "בקשת מפתח הצפנה סימטרי". ההודעה מוצפנת ע"י המפתח הציבורי של B. – **בקשת הודעה 603 -> בקשת מפתח סימטרי 1.**
3. השרת מקבל את ההודעה ושומר אותה. – **שומר את הבקשה בDB, כרגיל.**
4. לוקח B מושך מהשרת את ההודעות הממתינות לו. – **בקשת שליפת הודעות 604.**
5. לקוח B מפענח את ההודעה באמצעות המפתח **הפרטי** שלו. – **קורה אצל הלקוח.**
6. לקוח B מבקש מהשרת את המפתח **הציבורי** של לקוח A. – **בקשה 602.**
7. לקוח B שולח **תשובה** מסוג "מפתח הצפנה סימטרי" ללקוח A. התשובה מוצפנת ע"י המפתח הציבורי של A. – **בקשת הודעה 603 -> שליחת מפתח סימטרי 2.**
8. השרת מקבל את ההודעה ושומר אותה. – **כרגיל.**
9. לקוח A מושך מהשרת את ההודעות הממתינות לו. – **בקשה 604.**
10. לקוח A מפענח את ההודעה באמצעות המפתח **הפרטי** שלו. – **קורה אצל לקוח A.**
11. כעת, לקוח A ולקוח B יכולים לשוחח באמצעות מפתח הצפנה **סימטרי**. – **להעמיק עוד.**

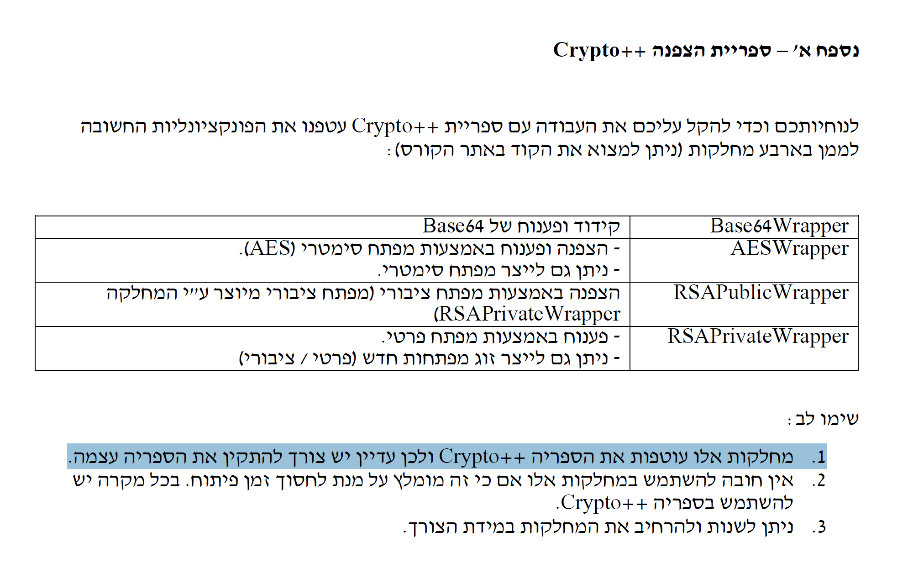
**גודל כל אחד מסוגי המפתחות:**

מפתח סימטרי = 128 סיביות (bits), כלומר – 16 בתים.  
מפתח א-סימטרי = 1024 סיביות, כלומר – 128 בתים.

מפתח ציבורי = 160 בתים.

תמונה שמכילה טקסט, צילום מסך, גופן, מסמך

התיאור נוצר באופן אוטומטימפתח פרטי = **לא רלוונטי?**



**חולשות אפשריות:**

שרת

* קלט שמגיע בגדלים שונים
* קלט שמגיע בפורמט אחר ומנסים לפענח אותו
* קלט שמגיע קצר מדי ולא בודקים את זה
* Payload/message\_content שמגיע עם size לפני, ולא מוודאים שה-size והגודל ממש של הפיילואד שווים.

לקוח

* הגבלתם את הגודל של הpayload? כדי למנוע מצב של עומס או DOS? (אין דרישה כזאת במטלה אם אני לא טועה) - לא. dos בא בחינם למסמך חולשות. **חולשה טובה לפרוטטוקול.!!**