שאלה 1 (75%)

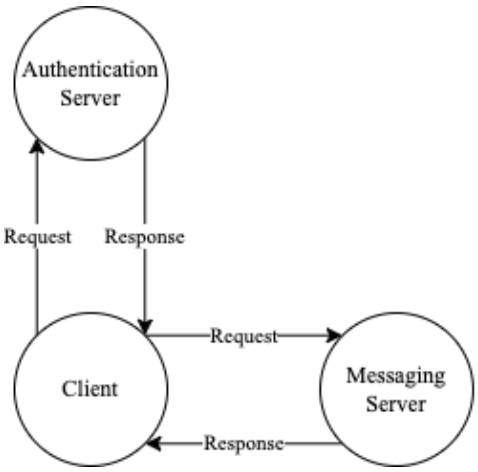
בתרגיל זה תממשו מערכת העברת מסרים המבוססת על פרוטוקול Kerberos. המערכת תכלול קוד שרת אימות (המהווה Key Distribution Center), וקוד שרת-לקוח המשתמשים במפתח משותף על מנת להעביר הודעות. הקוד ייכתב בשפת Python או ++C או Java.

חשוב! קראו היטב את כל המטלה לפני תחילת העבודה. וודאו שאתם מבינים היטב את פרוטוקול התקשורת ואת המבנה של תוכנת השרת והלקוח.

ארכיטקטורה

ארכיטקטורת התוכנה מבוססת על שרת-לקוח. הלקוח יוצר קשר ביוזמתו עם שרת האימות, אשר מאמת את זהות הלקוח. לאחר אימות מוצלח, הלקוח מקבל מפתח סימטרי לתקשורת עם שרת ההודעות. לאחר מכן, הלקוח מעביר לשרת ההודעות את המפתח הסימטרי, אחריו יוכל לשלוח הודעות מוצפנות לשרת ההודעות. תפקיד שרת ההודעות הוא לקבל הודעות מלקוחות ולהדפיס אותן למסך.

הנכם נדרשים לתמוך בשרת הודעות בודד. **בונוס (5 נק'), רשות:** הוסיפו תמיכה במספר רב של שרתים.



הפרוטוקול במבט על

Client --> Auth Server:	ID_s, Nonce
Auth Server --> Client:	$E_{K_c}(K_{c,s}$, Nonce), Ticket
Client -->Msg Server:	Ticket, Authenticator
Msg Server -->Client:	KeyAck
Client --> Msg Server:	$E_{K_{c,s}}$(Message)
Msg Server -->Client:	MsgAck

פרטי הפרוטוקול מוגדרים בהמשך.

שרת האימות

תפקיד שרת האימות הוא לנהל את רשימת הלקוחות הרשומים לשירות ולאפשר להם לשלוח הודעות שונות לשרת ההודעות.

א. השרת יתמוך בריבוי משתמשים ע"י חוטים (threads).
ב. גרסת הפרוטוקול היא **24** (גרסה זו מופיעה בהודעות התקשורת).

פורט

השרת יקרא את מספר הפורט <u>מתוך קובץ טקסט</u> בצורה הבאה:

- שם הקובץ: port.info
- מיקום הקובץ: באותה תיקיה של קבצי הקוד של השרת
- תוכן הקובץ: מספר פורט
  לדוגמא:
  1234

קובץ פרטי שרת הודעות (ללא בונוס)

יישמר כאשר קיים במערכת שרת אחד בלבד (ללא בונוס). שרת האימות ישמור ויקרא את פרטי שרת ההודעות מתוך קובץ טקסט. הקובץ יישמר גם אצל שרת האימות וגם אצל שרת ההודעות. מבנה הקובץ:

- שם הקובץ: msg.info
- מיקום הקובץ: בתיקיה של קובץ ההרצה/סקריפט
- תוכן הקובץ:
  שורה ראשונה: כתובת שרת ההודעות: כתובת IP + נקודתיים + מספר פורט
  שורה שניה: שם השרת (מחרוזת עד 255 תווים)
  שורה שלישית: מזהה ייחודי בייצוג ASCII כאשר כל שני תווים מייצגים ערך hex בעל 8 סיביות.
  שורה רביעית: מפתח סימטרי ארוך טווח עבור שרת ההודעות (משותף עם שרת האימות) בפורמט בסיס 64.
  לדוגמא:

```
127.0.0.1:1235
Printer 20
64f3f63985f04beb81a0e43321880182
MIGdMA0GCSqGSIb3DQEBA…
```

שרת האימות יתעלם מכתובת ה-IP של שרת ההודעות (אינו צריך לתקשר איתו ישירות).

נתונים

השרת ישמור את נתוני הלקוחות הרשומים לשירות בזיכרון (RAM) ובקבצים.

מידע על הלקוחות ישמר בקובץ בשם clients. מבנה כל שורה בקובץ:

ID:Name:PasswordHash:LastSeen

כאשר:

שם	סוג	הערות
ID	16 בתים (128 ביט)	מזהה ייחודי עבור כל לקוח. אינדקס
Name	מחרוזת (255 תוים)	מחרוזת ASCII המייצגת שם משתמש. **כולל תו מסיים!** (null terminated)
PasswordHash	32 בתים	תמצית SHA-256 של סיסמת הלקוח. **מהווה מפתח סימטרי ארוך טווח עבור הלקוח**
LastSeen	תאריך ושעה	הזמן בו התקבלה בקשה אחרונה מלקוח

במקרה והשרת נפל, תהיה לו אפשרות לעלות מחדש ולטעון את רשימת הלקוחות הרשומים מהקובץ. לקוחות רשומים יוכלו להמשיך לשלוח בקשות מבלי לבצע רישום מחדש.

אופן פעולת שרת האימות

1. קורא את הפורט מתוך הקובץ port.info. (אם הקובץ לא קיים, להוציא אזהרה ולעבוד על פורט ברירת מחדל 1256. לא להגיע לנפילה עם Traceback במידה והקובץ לא זמין.)
2. קורא את פרטי שרת ההודעות מתוך הקובץ msg.info.
3. השרת בודק את קובץ הלקוחות, אם כבר קיים, וטוען נתוני לקוחות שנרשמו בהפעלות קודמות.
4. ממתין לבקשות מלקוחות בלולאה אין סופית.
5. בעת קבלת בקשה מפענח את הבקשה בהתאם לפרוטוקול:

א. בקשה לרישום: במידה ושם הלקוח המבוקש כבר קיים, שרת האימות יחזיר שגיאה. אחרת, השרת ייצר UUID[1] חדש עבור הלקוח, ישמור את הנתונים בזיכרון ובקובץ ויחזיר תשובת הצלחה.

ב. בקשה למפתח: שרת האימות ייצור מפתח AES, יצפין אותו בעזרת המפתח של הלקוח וישלח בתגובה יחד עם Ticket שמיועד לשרת ההודעות.

בונוס (5 נק'), רשות:

ג. בקשה לרישום של שרת.

ד. בקשת לרשימת שרתי הודעות: השרת יחזיר את רשימת השרתים לפי הפרוטוקול.

לקוח

תוכנת הלקוח תדע לתקשר מול שרת האימות ושרת ההודעות. תוכנת הלקוח תדע:

(1) להירשם לשרת האימות (במידה ולא רשום מהפעלה קודמת).

(2) לבקש מפתח סימטרי לתקשורת עם שרת ההודעות.

[1] בתרגיל זה נעשה שימוש במזהה ייחודי גלובלי (UUID). לקריאה נוספת:
https://en.wikipedia.org/wiki/Universally_unique_identifier

(3) לתקשר עם שרת ההודעות.

גרסת הלקוח תהיה **24**.

כתובות השרתים והפורטים

- שם הקובץ: srv.info
- מיקום הקובץ: בתיקיה של קובץ ההרצה/סקריפט
- תוכן הקובץ:
  שורה ראשונה: כתובת שרת האימות: כתובת IP + נקודתיים + מספר פורט
  שורה שניה (ללא בונוס): כתובת שרת ההודעות: כתובת IP + נקודתיים + מספר פורט
- <u>דוגמא</u>:
  127.0.0.1:1234
  127.0.0.1:1235

קובץ פרטי לקוח

שם ומזהה ייחודי: הלקוח ישמור ויקרא את השם והמזהה הייחודי שלו מתוך קובץ טקסט בצורה הבאה:

- שם הקובץ: me.info
- מיקום הקובץ: בתיקיה של קובץ ההרצה/סקריפט
- תוכן הקובץ:
  שורה ראשונה: שם הלקוח (מחרוזת עד 255 תווים)
  שורה שניה: מזהה ייחודי בייצוג ASCII כאשר כל שני תווים מייצגים ערך hex בעל 8 סיביות.
  לדוגמא:

```
Michael Jackson
64f3f63985f04beb81a0e43321880182
```

שרת ההודעות

השרת מקבל הודעות מוצפנות מלקוחות ומדפיס אותן למסך (stdout). מערכת זו מדמה שרת הדפסה אמיתי מבוסס Kerberos.

א. השרת יתמוך בריבוי משתמשים ע"י חוטים (threads).
ב. גרסת השרת תהיה **24** (גרסה זו מופיעה בהודעות תקשורת מטעם השרת).

קובץ פרטי שרת הודעות

מוגדר מעלה. הקובץ זהה עבור שרת האימות ושרת ההודעות.

אופן פעולת שרת ההודעות

1. קורא את פרטי השרת מתוך הקובץ msg.info.
2. ממתין לבקשות מלקוחות בלולאה אין סופית.
3. בעת קבלת בקשה מפענח את הבקשה בהתאם לפרוטוקול:

א. קבלת מפתח: השרת מקבל Ticket, מפענח אותו עם המפתח הסימטרי ארוך הטווח שלו ושומר את המפתח עבור הלקוח.
ב. הדפסת הודעה: השרת מפענח את ההודעה עם המפתח הסימטרי ומדפיס את ההודעה.

שגיאה מצד השרת

בכל מקרה של שגיאה הלקוח ידפיס למסך הודעה: "server responded with an error".

פעולות אפשריות

בקשת רישום

1. במידה והקובץ me.info לא קיים, הלקוח יקלוט שם משתמש וישלח בקשת רישום לשרת האימות.
2. הלקוח ישמור בקובץ בשם me.info את השם והמזהה הייחודי שיקבל מהשרת.
3. במידה והקובץ כן קיים, הלקוח יקרא את הנתונים מהקובץ להתחברות חוזרת.
   שימו לב! במידה והקובץ כבר קיים הלקוח לא יירשם שנית.

בקשת רשימת שרתי הודעות (בונוס 5 נק')

הלקוח ישלח בקשת רשימת שרתי הודעות לשרת האימות. יפענח את התשובה וידפיס למסך את שמות השרתים.

קבלת מפתח AES לשרת הודעות

לאחר שהלקוח מבקש מפתח AES לשרת הודעות ספציפי, הוא מקבל מפתח מוצפן ו-Ticket. הלקוח פותח את המפתח בעזרת התמצית של הסיסמה שלו ושומר את מפתח ה-AES ואת ה-Ticket לשימוש עתידי עם שרת ההודעות.

שליחת מפתח AES לשרת ההודעות

הלקוח מייצר Authenticator באמצעות מפתח ה-AES שקיבל משרת האימות. הלקוח שולח את ה-Authenticator לשרת ההודעות יחד עם ה-Ticket.

שליחת הודעה לשרת ההודעות

הלקוח קולט הודעה לשליחה מהמשתמש. הלקוח מצפין את ההודעה בעזרת מפתח ה-AES ושולח אותה לשרת ההודעות.

פרוטוקול התקשורת

כללי

- הפרוטוקול הוא בינארי וממומש מעל TCP.
- כל השדות המספריים חייבים להיות עם ערכים גדולים מאפס (**Unsigned**) ומיוצגים כ- **Little endian**.
- המימוש צריך לבדוק את התקינות של כל שדה בפרוטוקול.
- פרוטוקול זה תומך **בבקשות** לשרת **ותשובות** ללקוח. בקשות או תשובות יכולות להכיל **"הודעה"**.
- הודעה עוברת בין לקוחות לשרת ההודעות.

זכרו! הפרוטוקול מחייב ולא ניתן לעשות בו שינויים. כפועל יוצא, כל שרת ולקוח הממשים את הפרוטוקול (ללא תלות בשפת התכנות) יכולים לעבוד אחד מול השני.

רישום למערכת

1. כל לקוח שמתחבר בפעם הראשונה נרשם בשירות מול שרת האימות עם שם (מחרוזת באורך מקסימלי של 255 בתים) וסיסמה.
2. שרת האימות שומר את תמצית הסיסמה ומחזיר ללקוח מזהה ייחודי שנוצר עבורו או שגיאה אם השם כבר קיים בבסיס הנתונים.

פרטי הפרוטוקול

בקשות

מבנה בקשה מהלקוח לשרת. השרת יפרש את התוכן (Payload) לפי קוד הבקשה.

בקשה לשרת

Request	שדה	גודל	משמעות
כותרת (Header)	Client ID	16 בתים (128 ביט)	מזהה ייחודי עבור כל לקוח
	Version	בית	מספר גרסת לקוח
	Code	2 בתים	קוד בקשה
	Payload size	4 בתים	גודל תוכן הבקשה
תוכן (Payload)	Payload	משתנה	תוכן הבקשה. משתנה בהתאם לבקשה

תוכן (Payload)

התוכן משתנה בהתאם לבקשה. לכל בקשה מבנה שונה.

קוד בקשה 1024 – רישום לקוח

שדה	גודל	משמעות
Name	255 בתים	מחרוזת ASCII המייצגת שם משתמש. **כולל תו מסיים!** (null terminated)
Password	255 בתים	מחרוזת ASCII המייצגת סיסמה. **כולל תו מסיים!** (null terminated)

שימו לב: השרת יתעלם מהשדה Client ID

קוד בקשה 1025 – רישום שרת **(בונוס, רשות)**

שדה	גודל	משמעות
Name	255 בתים	מחרוזת ASCII המייצגת שם משתמש. **כולל תו מסיים!** (null terminated)
מפתח סימטרי	32 בתים	מפתח AES סימטרי לשרת ההדפסה (מיועד לפענוח Ticket-ים)

קוד בקשה 1026 – בקשת רשימת שרתי הודעות **(בונוס, רשות)**

שדה payload לא קיים. שדה Payload size=0.

קוד בקשה 1027 – בקשת מפתח סימטרי

שדה	גודל	משמעות
Server ID	16 בתים	מזהה ייחודי עבור כל שרת הדפסה
Nonce	8 בתים	ערך אקראי שהלקוח יוצר

תשובות משרת האימות

Response	שדה	גודל	משמעות
כותרת (Header)	Version	בית	מספר גרסת שרת
	Code	2 בתים	קוד התשובה
	Payload size	4 בתים	גודל תוכן התשובה
תוכן (Payload)	Payload	משתנה	תוכן התשובה. משתנה בהתאם לתשובה

קוד תשובה 1600 – רישום הצליח

שדה	גודל	משמעות
Client ID	16 בתים	מזהה ייחודי של לקוח/שרת

קוד תשובה 1601 – רישום נכשל

קוד תשובה 1602 – רשימת שרתי הודעות **(בונוס, רשות)**

רשות: הוסיפו תמיכה במספר רב של שרתים. מחליף את קובץ פרטי שרת ההודעות אצל הלקוח ואצל שרת האימות.

שדה	גודל	משמעות
Server ID	16 בתים	מזהה ייחודי של שרת
Server name	255 בתים	מחרוזת ASCII המייצגת שם משתמש. **כולל תו מסיים!** (null terminated)
Server IP	4 בתים	כתובת ה-IP של השרת
Server port	2 בתים	הפורט של השרת

חשוב: הרשימה עשויה לכלול שרתים רבים. הם יופיעו אחד אחרי השני וניתן לחשב את מספרם ע"י הנוסחה:

Payload Size / (16+255+4+2)

קוד תשובה 1603 – שליחת מפתח סימטרי מוצפן

שדה	גודל	משמעות
Client ID	16 בתים	מזהה ייחודי של לקוח
Encrypted key		מפתח AES מוצפן ללקוח
Ticket		מוצפן לשרת ההודעות

מבנה המפתח המוצפן (שדה ה-Encrypted key):

שדה	גודל	משמעות
Encrypted key IV	16 בתים	
Nonce	8 בתים	ערך אקראי שנוצר ע"י הלקוח והתקבל בבקשת מפתח סימטרי. **מוצפן** באמצעות המפתח הסימטרי של הלקוח
AES key	32 בתים	מפתח הצפנה עבור הלקוח והשרת. **מוצפן** באמצעות המפתח הסימטרי של הלקוח

מבנה ה-Ticket:

שדה	גודל	משמעות
Version	בית	מספר גרסת שרת
Client ID	16 בתים	מזהה ייחודי עבור כל לקוח
Server ID	16 בתים	מזהה ייחודי עבור כל שרת
Creation time	8 בתים	Timestamp, זמן יצירת ה-Ticket
Ticket IV	16 בתים	
AES key	32 בתים	מפתח הצפנה עבור הלקוח והשרת. **מוצפן** באמצעות המפתח הסימטרי של שרת ההודעות
Expiration time	8 בתים	Timestamp, זמן תום התוקף של ה-Ticket. **מוצפן** באמצעות המפתח הסימטרי שרת ההודעות

בקשות לשרת ההודעות

קוד בקשה 1028 – שליחת מפתח סימטרי לשרת הודעות

שדה	גודל	משמעות
Authenticator		
Ticket		

מבנה ה-Authenticator :

שדה	גודל	משמעות
Authenticator IV	16 בתים	
Version	בית	מספר גירסת שרת. **מוצפן** באמצעות המפתח הסימטרי של שרת ההודעות
Client ID	16 בתים	מזהה ייחודי עבור כל לקוח. **מוצפן** באמצעות המפתח הסימטרי של שרת ההודעות
Server ID	16 בתים	מזהה ייחודי עבור כל שרת. **מוצפן** באמצעות המפתח הסימטרי של שרת ההודעות
Creation time	8 בתים	Timestamp, זמן יצירת ה-Auth. **מוצפן** באמצעות המפתח הסימטרי של שרת ההודעות

קוד בקשה 1029 – שליחת הודעה

שדה	גודל	משמעות
Message size	4 בתים	גודל ההודעה (לאחר הצפנה)
Message IV	16 בתים	
Message content	משתנה	תוכן ההודעה. **מוצפן** תחת מפתח סימטרי שנוצר ע״י שרת האימות.

קוד תשובה 1609 – שגיאה כללית בשרת שלא טופלה באחד המקרים הקודמים.

קוד תשובות משרת ההודעות

קוד תשובה 1604 – מאשר קבלת מפתח סימטרי

קוד תשובה 1605 – מאשר קבלת הודעה, תודה

קוד תשובה 1609 – שגיאה כללית בשרת שלא טופלה באחד המקרים הקודמים.

הצפנה

פרוטוקול התקשורת משתמש בהצפנה סימטרית על מנת להעביר מפתחות והודעות.

השתמשו ב-AES-CBC.

אורך המפתח **256 ביט**. נדרש לייצר IV אקראי בכל הצפנה.

דגשים לפיתוח

1. מומלץ לעבוד עם מערכת לניהול קוד (כדוגמת גיט[2])
2. עבדו באופן מודולרי ובדקו את עצמכם כל הזמן
   א. זהו את המחלקות והפונקציות החשובות
   ב. **בצד השרת:**
   כיתבו קוד לטיפול בבקשה אחת. הוסיפו תמיכה בריבוי לקוחות בשלב מאוחר יותר
   ג. **בצד הלקוח:**
   ממשו את הרכיבים הגדולים באופן בלתי תלוי בחלקים אחרים של המערכת (תקשורת, הצפנה, פרוטוקול וכו').
3. ממשו קוד לבדיקה כבר בשלבים מוקדמים של הפרויקט
   א. **בצד השרת:**
   השתמשו בהדפסות למסך או בכתיבה ללוג כדי לעקוב אחרי התקשורת. תוכלו גם לטעון את המודול לתוך ה- interpreter ולעבוד באופן דינמי.
   ב. **בצד הלקוח:**
   כיתבו פונקציות קטנות שבודקות חלקים נפרדים של המערכת. השתמשו בפונקציות הללו תוך כדי כתיבת הקוד עצמו.
4. כתיבת הקוד
   א. ממשו את התוכנה לפי עקרונות תכנות מונחה עצמים
   ב. שימו לב לייצוג ערכים בזיכרון כ- little-endian או big-endian
   ג. הקפידו על תיעוד של הקוד (comments)
   ד. תנו שמות משמעותיים למשתנים, פונקציות ומחלקות. המנעו ממספרי קסם!
   ה. הודעה יכולה להיות גדולה מאוד (בגודל דינמי). חשבו על הדרך הנכונה ביותר לקבל ולשלוח כמות מידע גדולה.
   ו. **אבטחת מידע** – חשבו לאורך כל הדרך על כתיבת קוד בטוח לפי העקרונות שלמדתם:
      - האם בדקתם את הקלט?
      - איך נעשה שימוש בזיכרון דינמי?
      - האם מתבצעת המרת טיפוסים (casting) וכו'..
   ז. בדקו שגיאות בכל בקשה ותשובה בשרת ובלקוח!
5. **לפני ההגשה**
   א. בדקו שהפרויקט מתקמפל ורץ בצורה תקינה ללא קריסות או תלויות בספריות שונות (למעט הספריות הנדרשות לתרגיל)
   ב. מומלץ לייצר תיקיה חדשה ולהעתיק לשם את הקבצים המיועדים לשליחה. לייצר פרויקט VS חדש, לקמפל ולהריץ
   ג. העבודה תיבדק על מ"ה חלונות עם Visual Studio Community 2022 עם גרסת C++ 17

[2] https://www.atlassian.com/git/tutorials/what-is-version-control

המלצות לקוד פייתון

1. השתמשו בפייתון **גרסה 3**
2. עשו שימוש בספריות פייתון הסטנדרטיות בלבד (פרט לספריית ההצפנה)!
3. תוכלו להיעזר בספריה **struct** על מנת לעבוד עם נתוני התקשורת בנוחות
4. השרת יפעל עם חבילת הצפנה PyCryptodome, ופרט לכך עם חבילות סטנדרטיות הכלולות במפרש.

המלצות לקוד C++

1. ממשו את הקוד בשפת C++ תואמת גרסה 11 ומעלה (לדוגמא פונקציות מסוג למדה, שימוש ב- auto וכו'..), בעזרת Visual Studio 2022.
2. עשו שימוש בספריות STL.
3. השתמשו בצד הלקוח בספריה **Crypto++**[3] (ראו דוגמת קוד באתר הקורס)
4. למימוש התקשורת עשו שימוש ב- winsock או בספריית boost

הגשה

פייתון

1. עליכם להגיש רק את קבצי הקוד (כלומר קבצי py.).
שימו לב! על התוכנית להטען ולרוץ בצורה תקינה (ללא צורך בתוספות קבצים וללא קריסות).
2. יש לכלול פונקציה ראשית בשם **main**. פונקציה זו תהיה הפונקציה הראשית של תוכנית השרת והיא תעבוד לפי אופן פעולת השרת המפורט לעיל.
טיפ:
תוכלו להשתמש במנגנון הבא כדי לאפשר עבודה אינטראקטיבית **וגם** הרצה של הקוד:

```
if __name__ == "__main__":
```

C++

1. עליכם להגיש רק את קבצי הקוד (כלומר קבצי h. ו- cpp.).
שימו לב! על התוכנית לרוץ בצורה תקינה (ללא צורך בתוספות קבצים, ללא קריסות)
2. עבודתכם תיבדק במערכת הפעלה חלונות, באמצעות Visual Studio ולכן מומלץ לעבוד עם סביבה זו.

וידאו עם דוגמת ריצה

עליכם להקליט וידאו ממסך המחשב, בו אתם פותחים **שלושה** חלונות cmd במקביל ומריצים את המערכת שפיתחתם. יש להפעיל קודם את השרתים ולאחר מכן גם את הלקוח. יש לעבור את תהליך הרישום של הלקוח, קבלה והעברה של ה-Ticket, כאשר ההודעות המתאימות מופיעות בחלונות הרלוונטיים, והעברת הודעה מוצפנת מהלקוח לשרת ההודעות. בוידאו צריך להיות פרט מזהה הכולל את השם או תעודת הזהות שלכם, והוא צריך להימשך 2-5 דקות.

[3] https://www.cryptopp.com/

שאלה 2 (25%)

עליכם לממש התקפת מילון לא-מקוונת נגד הפרוטוקול המתואר.

הנחיות:

- הנכם יכולים "לשלוף" ערכים מהתקשורת ולהשתמש בהם בתור קבועים בקוד (Hardcoded).
- אין צורך לממש Proxy או קוד שמבצע MITM.
- פרוטוקול הרישום (שאינו מוגן באמצעים קריפטוגרפיים) הוא Out-of-scope עבור שאלה זו ואין להשתמש בהודעות שלו לצורך התקיפה.

<u>יש להגיש מסמך</u> המסביר את ההתקפה והצעה לתיקון, בנוסף לקוד.

הגשה

מסמך word או pdf.

סרטון וידאו.

את כלל קבצי המערכת יש לארוז לקובץ zip.