# Assignment 2

## שאלה 1:

1. התוקף נקרא לו E יכול להאזין להודעות בין A ל-B, ולאחר שלב 3 כאשר A שולח הודעה ל-E, התוקף E ישלח לשרת את ההודעה הבאה: $E\text{->}S: \{A,E,\{N_B,K_{AB}\}_{KAS}\}_{KES}$ , עם השם שלו וההצפנה שלו.
ויקבל חזרה את ההודעה: $S\text{->}E: \{N_B,K_{AB}\}_{KES}$ , עם המפתח $K_{AB}$ שהוא צריך מוצפן עם המפתח $K_{ES}$ שהוא יכול לפתוח. כעת E מסוגל להאזין לתקשורת בין A ל-B.

2. היכולות הנדרשות מהתוקף E כדי להצליח במזימה שלו הן:
   א. דרך להאזין להודעות שעוברות בין A ל-B.
   ב. צריך להיות מזוהה עם השרת אמון ובעל מפתח משותף איתו.

3. ניתן לתקן את הפרוטוקול כדי להתמודד עם המתקפה מסעיף א' אנו נוסיף הודעה של מי הנמען בהודעה המוצפנת שיוצאת מ-A ל-B: $A\text{->}B: \{B,N_B,K_{AB}\}_{KAS}$ , בכדי שהשרת אמון כשיפתח את ההודעה ידע האם יש שם בעיה או להמשיך כרגיל.

## שאלה 2:

השינוי הנ"ל אינו בטוח, נתאר את ההתקפה שהתוקף יכול לעשות:

הרעיון הוא שהתוקף ישתמש ב-replay attack , ע"י כך שיקליט את כל השיחה בין הלקוח לשרת. לאחר מכן התוקף בעצמו יזום שיחה עם השרת ויסכימו על מפתחות סימטריים משלהם לתקשורת שזה שלבים 1 עד 6. לאחר מכן בשלב 7 התוקף במקום להגריל מחרוזת r ישלח את $Enc_{PKS}(PreMasterKey)$ שהקליט מהשיחה בין הלקוח לשרת, לאחר פעולה זאת השרת ישלח לתוקף את PreMasterKey ובכך התוקף יחשב את $K_{MAC},K_{ENC}$ עם ה-transcript שהקליט והKEY שקיבל הרגע. עכשיו E שמח כי הוא יכול להאזין לתקשורת המוצפנת בין הלקוח לשרת.

## שאלה 3:

1. פעולות שצריך לבצע בשביל לבדוק את הסרטיפיקט:

   א. פתיחת ההודעה עם המפתח הפומבי של השרת ובדיקה ש- $ID_x == ID_B$ , אם כן אז המפתח הפומבי לגיטימי.

   ב. פתיחת החלק השני עם המפתח הפומבי של השרת ובדיקה ש- $ID_x == ID_B$ , אם כן אז המפתח הפומבי לגיטימי ולכן ניתן לפתוח גם אותו עם המפתח הפומבי של השרת.

   ג. פתיחת החלק השני עם המפתח הפומבי $PUB_X$ שקיבלנו ולאחר מכן חילוץ של $ID_x$ עם המפתח הפומבי של השרת ובדיקה ש- $ID_x == ID_B$ , אם כן אז המפתח הפומבי.

   ד. פתיחת החלק השני עם המפתח הפומבי של השרת, לאחר מכן חילוץ של $ID_x$ עם המפתח $PUB_X$ שקיבלנו ולאחר מכן בדיקה ש- $ID_x == ID_B$ , אם כן אז המפתח הפומבי לגיטימי.

2. נתאר לכל סעיף האם בטוח או לא:

בתרגיל זה אף פרוטוקול לא בטוח, וסעיפים 1 ו-2 דומים בכל שלב לכן נרשום אותם פעם אחת פה ובכל סעיף נמשיך מהשלב השלישי:

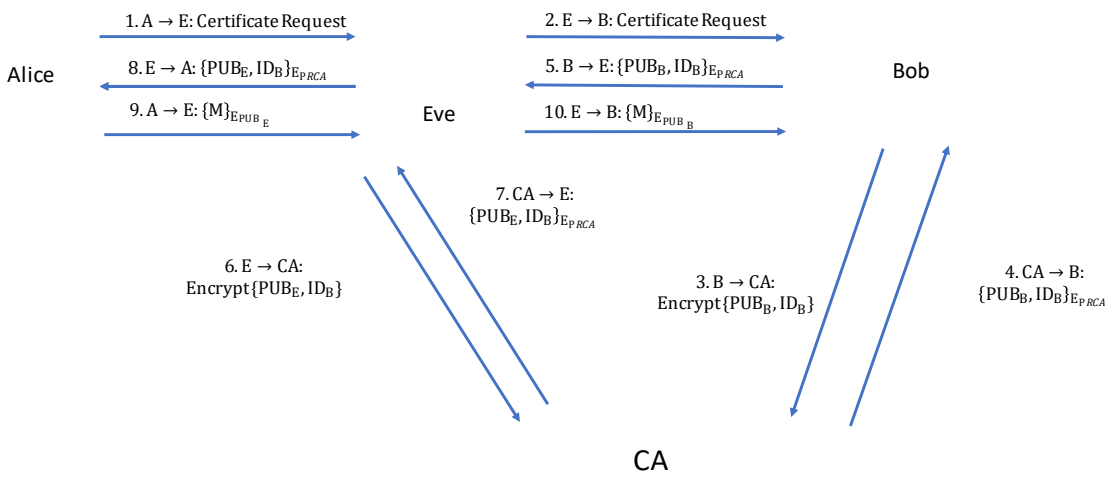
1) A תשלח בקשה ל-B לקבלת סרטיפיקט דרך Eve

2) B יבקש מ-CA את הסרטיפיקט שלו וישלח ל-A דרך Eve

**<u>הפרוטוקול לא בטוח</u>** –

3) Eve תשלח הודעה ל-CA עם $ID_B$ ומפתח פומבי משלה $PUB_E$ ותשלח ל-A את מה שהשרת הצפין

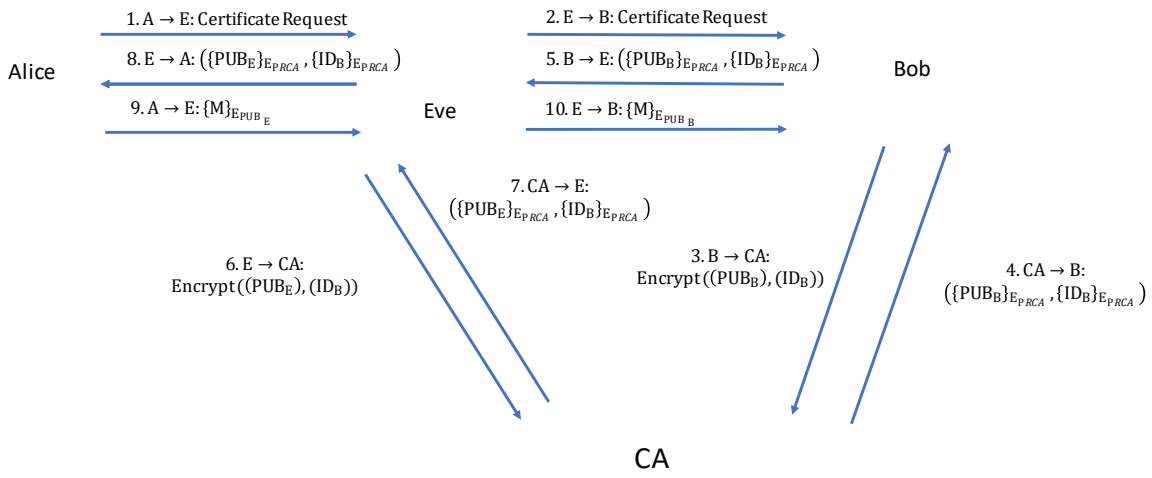
4) A תפתח את ההודעה עם המפתח הפומבי של CA תוודא שה-ID נכון ותשתמש במפתח הפומבי של Eve להצפנת ההודעות שלה עם B



## הפרוטוקול לא בטוח

3) Eve תשנה את החלק הראשון בהודעה למפתח הפומבי שהיא קיבלה מ-CA בחלק השני תשים את ה-ID המקורי של B שקיבל מהשרת ותשלח את זה ל-A

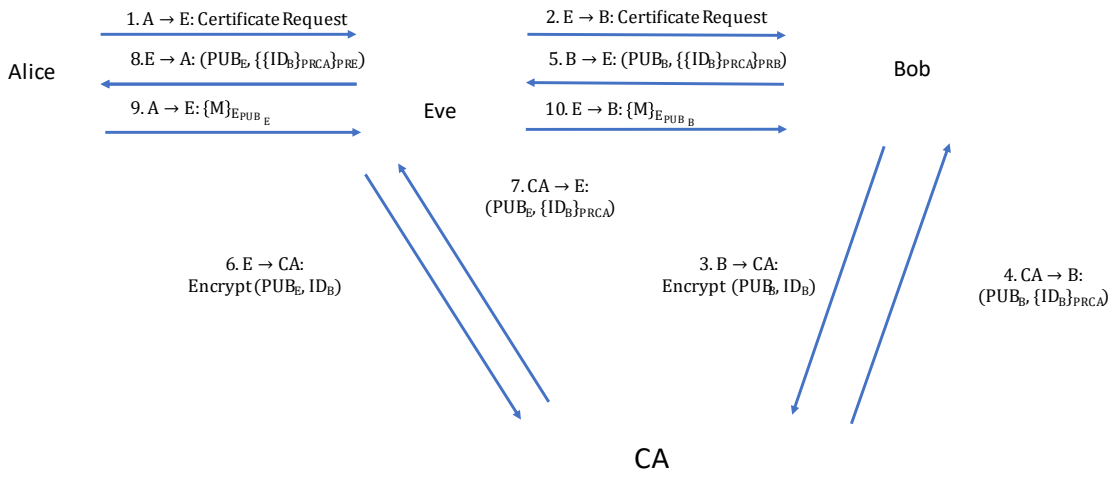
4) A תפתח את ההודעה עם המפתח הפומבי של CA תוודא שה-ID נכון ותשתמש במפתח הפומבי של Eve להצפנת ההודעות שלה עם B



## הפרוטוקול לא בטוח

3) Eve תשנה את החלק הראשון בהודעה למפתח הפומבי שהיא קיבלה מהשרת, והחלק השני היא תצפין בעזרת המפתח הפומבי שלה ותשלח את זה ל-A

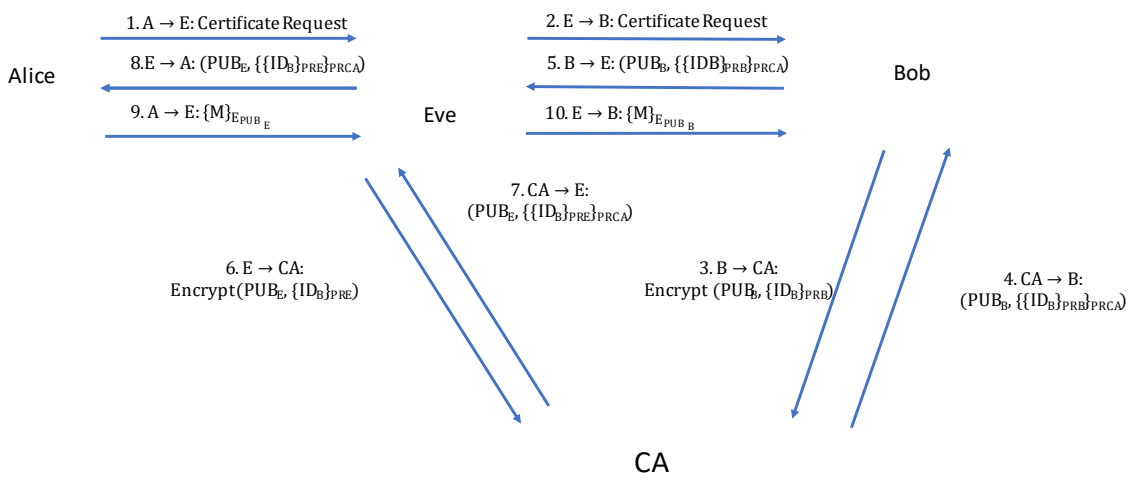
4) A תפתח את ההודעה עם הפומבי של Eve ואז עם הפומבי של CA תוודא שה-ID נכון ותשתמש במפתח הפומבי של Eve להצפנת ההודעות שלה עם B



**<u>הפרוטוקול לא בטוח</u>**

3) Eve תשנה את החלק הראשון בהודעה למפתח הפומבי שהיא קיבלה מהשרת, ובחלק השני היא היא תשים את ההצפנה שלה של $ID_B$ עם ההצפנה שקיבלה מ-CA ותשלח את זה ל-A

4) A תפתח את ההודעה עם הפומבי של CA ואז עם הפומבי שקיבלה בשדה הראשון תוודא שה-ID נכון ותשתמש במפתח הפומבי של Eve להצפנת ההודעות שלה עם B




<u>שאלה 4:</u>

<u>users</u> – alice, bob.  <u>gurus</u> - charlie

| | accounts | | | cv.txt | | | exam | | | solutions | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | R | W | A | R | W | A | R | W | A | R | W | A |
| alice | ★ | ★ | ★ | ★ | ★ | | | | | ★ | ★ | |
| bob | | | ★ | ★ | | | ★ | ★ | | | | |
| charlie | | | ★ | ★ | | | ★ | | | ★ | | |

שאלה 5:

staff – alex, benn, cloe.  gurus - cloe

| | manual.txt | report.txt | microedit | src/code.c | src/code/h |
|---|---|---|---|---|---|
| alex | R W | R W | R X | R | |
| benn | R | R | R W X | R W | |
| cloe | | R W | R | R | R |