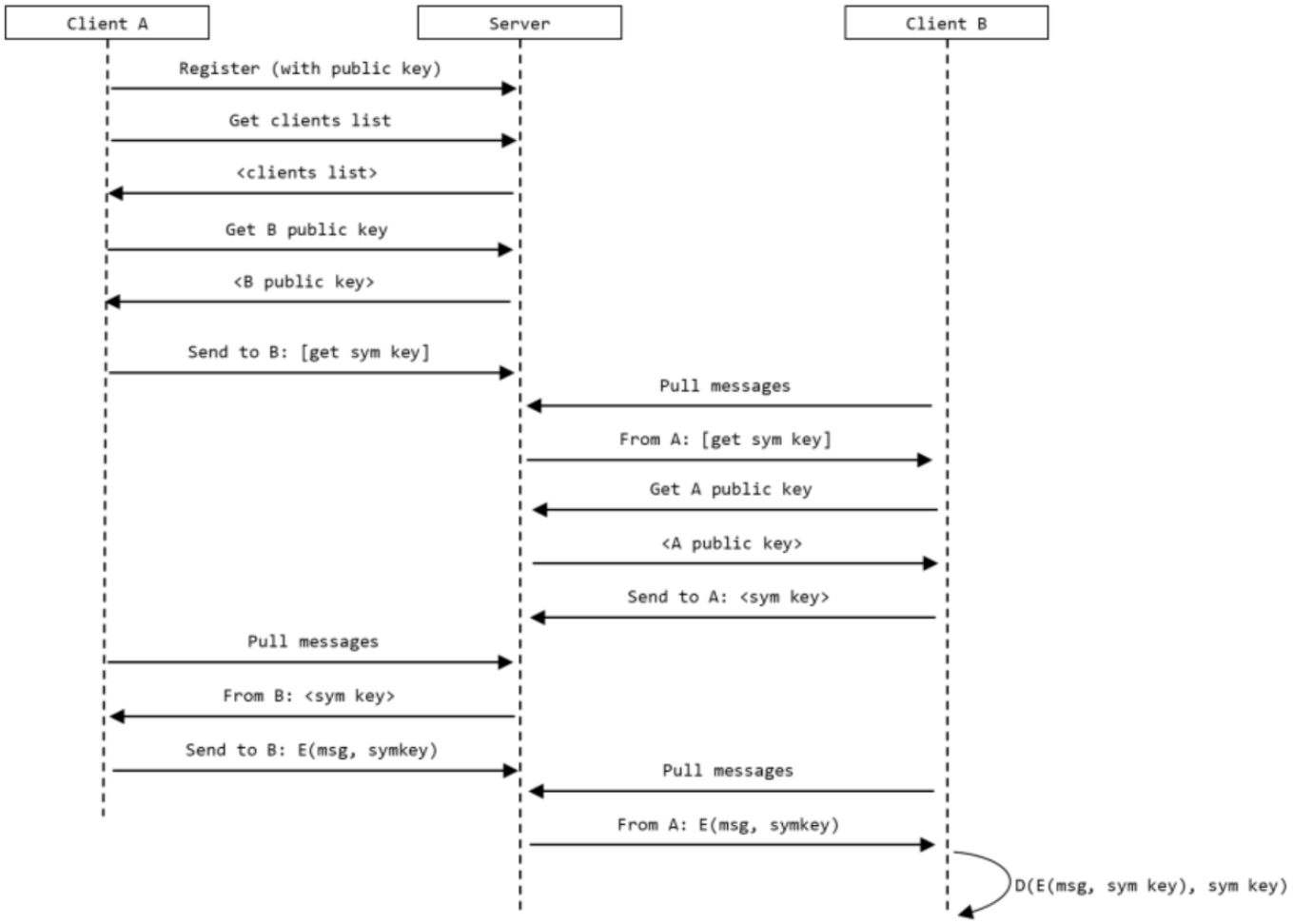
ממן 15 שאלה 2

בשאלה 1 מוצע פרוטוקול שיתוף מפתח הצפנה סימטרי לצורך החלפת הודעות בין 2 לקוחות. שיתוף המפתח מבוצע על פי מספר שלבים, שמכיל פעולות הצפנה ופיענוח בעזרת זוג מפתחות א-סימטרי (פרטי וציבורי) של כל לקוח.

<u>הפרוטוקול המוצע:</u>

1. לקוח **A** מבקש מהשרת את המפתח הציבורי של לקוח **B.**
2. לקוח **A** שולח הודעה (דרך השרת) ללקוח **B** מסוג "בקשת מפתח הצפנה **סימטרי**" ההודעה מוצפנת ע"י המפתח **הציבורי** של **B.**
3. השרת מקבל את ההודעה ושומר אותה.
4. לקוח **B** מושך מהשרת את ההודעות הממתינות לו.
5. לקוח **B** מפענח את ההודעה באמצעות המפתח **הפרטי.**
6. לקוח **B** מבקש מהשרת את המפתח **הציבורי** של לקוח **A.**
7. לקוח **B** שולח תשובה מסוג "מפתח הצפנה **סימטרי** "ללקוח **A** התשובה מוצפנת ע"י המפתח **הציבורי** של **A.**
8. השרת מקבל את ההודעה ושומר אותה.
9. לקוח **A** מושך מהשרת את ההודעות הממתינות לו.
10. לקוח **A**מפענח את ההודעה באמצעות המפתח **הפרטי.**
11. כעת, לקוח **A** ולקוח **B** יכולים לשוחח באמצעות מפתח הצפנה **סימטרי.**



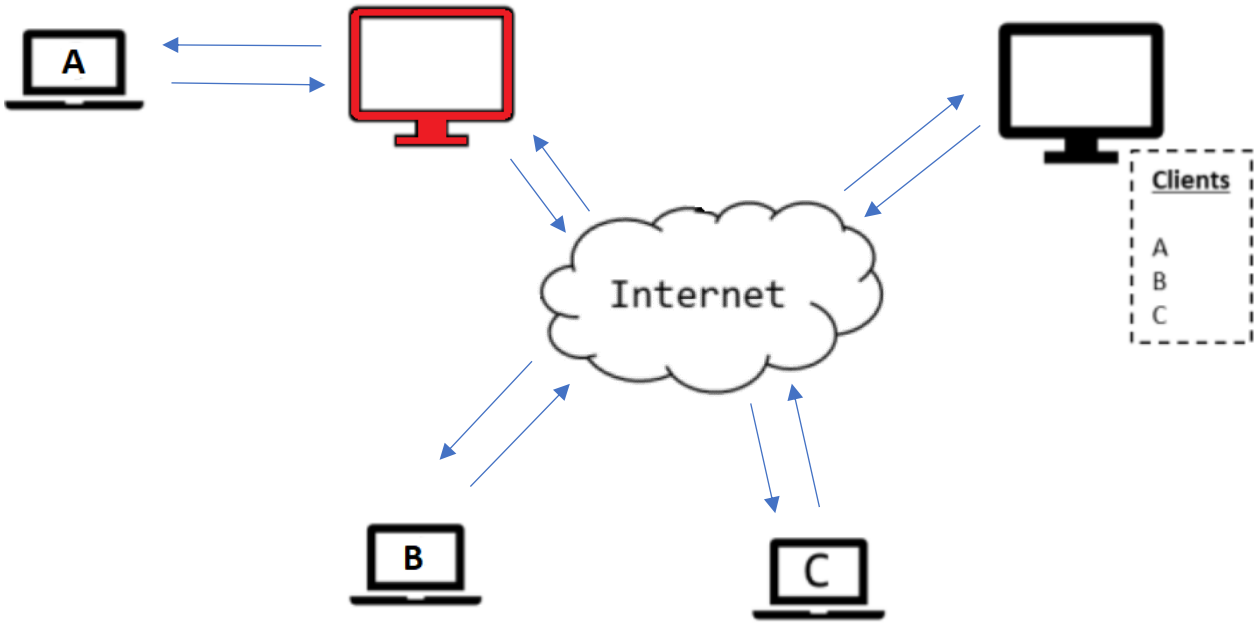
התקפה אפשרית: התקפת Man in the Middle

לקוח A אשר מבקש מהשרת את המפתח ציבורי של לקוח B, לצורך שליחת בקשת מפתח הצפנה סימטרי מקבל תשובה מהשרת.

אין בפרוטוקל שום שלב שמכיל מנגנון ווידוא על כך שהשרת הינו מחשב לגיטמי (מנגנון ווידוא certificate כמו ב-TLS\SSL) ולא איזשהו שרת זדוני.

אם כך, בתור מישהו חיצוני, אני יכול להתחזות לשרת זדוני ולתת שירות לזוג לקוחות אשר רוצה להחליף הודעות. התמקמות על תווך התקשורת בין לקוח A והשרת יהווה התקפת Man in the Middle.

השרת המתחזה אך ורק יספק את מפתחות ההצפנה הא-סימטריים **שלו** לזוג הלקוחות שרוצה לתקשר.



- נתייחס בהסבר הבא אל השרת הזדוני כאל שרת הביניים. המפתח הציבורי והפרטי של שרת הביניים ייקראו: מפתח ציבורי שקרי ו-פרטי שקרי בהתאמה.

תיאור ההתקפה

1. לקוח A מבקש להירשם למערכת. בקשה עוברת דרך שרת הביניים.
2. שרת הביניים שולח לשרת הראשי, בקשת רישום. הבקשה זהה לזו ש-A שלח, אך המפתח הציבורי הוא איננו של A, אלא של שרת הביניים, היינו המפתח הציבורי השקרי.
3. לקוח **A** מבקש מהשרת את המפתח הציבורי של לקוח **B.**
4. הבקשה מתקבלת אצל שרת הביניים. הוא מחזיר ללקוח A את המפתח הציבורי שקרי.
5. לקוח A שולח הודעה ללקוח B מסוג "בקשת מפתח הצפנה סימטרי". ההודעה מוצפנת ע"י המפתח הציבורי השקרי של שרת הביניים.
6. הבקשה מתקבל אצל שרת הביניים. הוא מפענח עם המפתח הפרטי השקרי ורואה שזו הודעת בקשת מפתח הצפנה סימטרי מלקוח B.
7. שרת הבניים מבקש את המפתח הפומבי של B, ואז מצפין איתו את הודעהת בקשת מפתח סימטרי ש-A שלח. בנוסף שרת הביניים שמר בעת הרישום את המפתח הציבורי של A.
8. השרת הראשי מקבל את ההודעה ושומר אותה.
9. לקוח B מושך מהשרת את ההודעות הממתינות לו.
10. B מפענח את ההודעה עם המפתח הפרטי שלו.

11. B מבקש מהשרת את המפתח הציבורי של A. ומקבל בחזרה את המפתח הציבורי השקרי.
12. B שולח תשובה מסוג "מפתח הצפנה סימטרי" ללקוח A. התשובה מוצפנת ע"י המפתח הציבורי השקרי.
13. השרת הראשי מקבל את ההודעה ושומר אותה.
14. לקוח A מבקש למשוך מהשרת הראשי את ההודעות הממתינות לו. הבקשה עוברת דרך שרת הביניים.
15. השרת הראשי מחזיר ל-A את ההודעות הממתינות לו. ההודעות מתקבלות קודם אצל שרת הביניים.
16. שרת הביניים מפענח את תשובת המפתח הסימטרי ע"י המפתח הפרטי השקרי שלו.
17. שרת הביניים מחזיר ל-A את תשובת המפתח הסימטרי, מוצפנת ע"י המפתח הציבורי של A.
18. A מפענח את ההודעה עם המפתח הפרטי שלו.
19. כעת, לקוח A ולקוח B יכולים לשוחח באמצעות מפתח הצפנה סימטרי.
20. שרת הביניים גם כן מחזיק במפתח הסימטרי ויכול לפענח הודעות בין A ל- B.

תיקון

על מנת למנוע התקפה מסוג כזה, ניתן להחליף את פרוטוקול החלפת המפתחות שמוצע במשימה בפרוטוקול החלפת מפתחות אמין יותר.

למשל, אפשר להשתמש ב-SSL. בפרוטוקול זה, השרת צריך להזדהות בפני הלקוח עם ה- SSL certificate שלו. ה-certificate הזה ייתן אינדיקציה לכך שהשרת אמין ושניתן להתחבר אליו ולתקשר איתו בצורה מאובטחת. לאחר שתהליך ההזדהות והאימות יבוצע, השרת והלקוח יחליפו מפתחות הצפנה כמתואר.