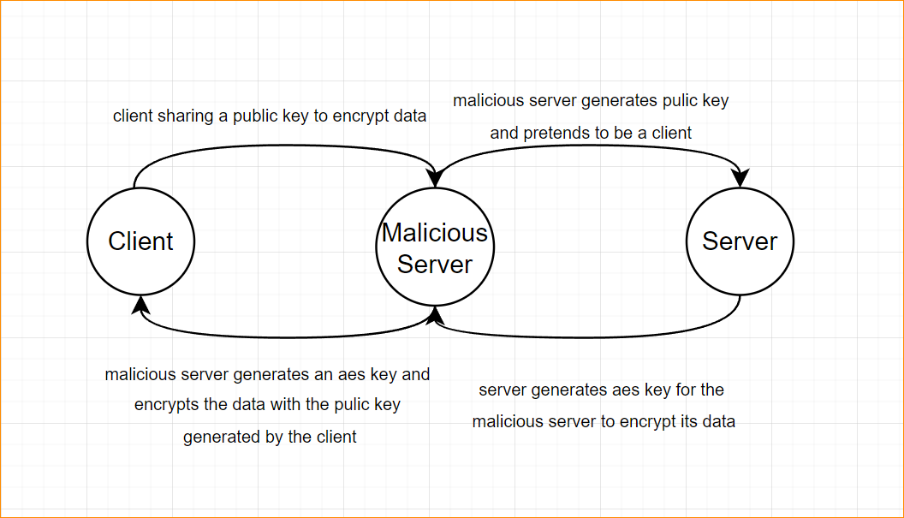
שאלה 2

MITM - man in the middle

התקפתman in the middle מתבצעת כאשר ישנו תוקף אקטיבי המאזין לתקשורת בין שני מחשבים באותו תווך בו הם משדרים, לשם הפשטה ההתקפה man in the middle תתבצע על קו תקשורת בו עוברים נתונים בין קליינט לשרת עבור המימוש נשים לב כי הנתונים בין הקליינט לשרת עוברים בחלקם מוצפנים כך שעצם האזנה לקו מאפשרת לדלות חלק מהנתונים כגון שם משתמש מזהה ייחודי שגיאות שהשרת מפיק ללקוח ושגיאות שהשרת מפיק עבור העברת קבצים לא תקינים ייחודי שכן הם נתונים שלא עוברים הצפנה עצם הידיעה כי השרת מפיק שגיאות התוקף יכול ליצור פקטות ייחודיות המכילות שגיאות ובכך בכל בקשה של הלקוח לשרת לשלוח לקליינט פקטה עם שגיאה כזאת או אחרת ובכך לגרום ללקוח לסיים את התוכנית שלו ללא הצלחה במימושים פחות טובים ניתן לגרום בכך לקריאות לתאי זיכרון שלא קיימים ובכך לגרום לקריסה ויציאה עם שגיאה

בעת התקפה man in the middle תוקף אקטיבי יכול להתחזות לשרת ובעת יצירת תקשורת בין הקליינט לשרת, התוקף יכול להזדהות עבור הלקוח בתור שרת לגיטימי ועבור השרת בתור לקוח לגיטימי כך שבעת החלפת המפתחות בין הלקוח לשרת הלקוח יחליף מפתחות עם התוקף והתוקף יחליף מפתחות עם השרת עבור השרת ועבור הלקוח נדמה כי התקשורת ביניהם מוצפנת אך עבור התוקף התקשורת לא מוצפנת ובכך התוקף יכול לראות ולשנות את תכולת הפקטות שעוברות דרכו



עבור ההתקפות על מנת לייעל את הפרוטוקול יש עדיפות לבצע החלפת מפתחות עוד בתחילת התקשורת עוד לפני שעובר מידע כלשהו על הקו כמו כן ניתן ליישם שרת שלישי שנמצא על תווך אחר עבור אותו שרת שלישי על מנת שיבוצע אימות עבור המידע העובר או שתתבצע החלפה של מפתחות נוספים או קבוצת ביטים רנדומלית שתתווסף לכל הודעה (salt) כך שעבור כל הצפנה עבור מפתחות זהים וקלט זהה יצא פלט שונה עבור ההצפנות ניתן לבצע הצפנה מרובת שלבים rolling code encryption כך שלתוקף יקח זמן לפענח כיצד ואיזה הצפנה בוצעה עם אותם המפתחות