TLS

Key agreement

1. הלקוח שולח הודעת client Hello לשרת עם הפרמטרים הבאים:
   * "Client Hello"
   * Client\_random – מספר באורך 32 בטים (bytes) רנדומליים
   * Cipher suites – כל סוגי ההצפנות הניתנות לביצוע ע"י הלקוח
2. השרת שולח ללקוח הודעת Server Hello עם הפרמטרים הבאים:
   * "Server Hello"
   * סוג ההצפנה בו יהיה שימוש בהמשך התקשורת, אשר נמצא ברשימת סוגי ההצפנה ששלח הלקוח בהודעתו הקודמת
   * server\_random - מספר באורך 32 בטים (bytes) רנדומליים
   * מפתח ציבורי של השרת
3. הלקוח בוחר מספר רנדומלי בשם pre\_master\_secret, מצפין אותו עם המפתח הפומבי של השרת ושולח את התוצאה.
4. לאחר העברת פרמטרים אלו, השרת והלוקח מחשבים את מפתח ההצפנה ואת וקטור האתחול. חישוב המפתח ווקטור האתחול נעשה ע"י ערך של פונקציית הגיבוב אשר נבחרה בידי השרת בעזרת הפרמטרים הבאים לפי סדר:
   * pre\_master\_secret
   * "master secret"
   * client\_random
   * server\_random

את תוצאת הגיבוב (digest) אנו חותכים לשני חלקים שווים, הראשון זהו מפתח ההצפנה, החלק השני הוא ווקטור האתחול

מרגע זה במצב: Encrypted communication

לאחר שנוצרו מפתח ההצפנה ווקטור האתחול, שני הצדדים מתקשרים ע"י ההצפנה הסימטרית שנבחרה ע"י השרת בשלבים הקודמים