**אימות חתימה ברשת ביטקוין**

הבטחת אמינות ואימות חתימות נעשית ברשת ביטקוין באמצעות קריפטוגרפיה.

מהי קריפטוגרפיה?

ביוונית משמעות המילה היא "כתיבה נסתרת" אבל הקריפטוגרפיה נועדה ליותר מהצפנה של כתב אלא גם על מנת לחתום באופן ייחודי בחתימה וירטואלית אותנטית ולאמת תוכן וזהויות משתמשים.

נוכל, אם כן, להגדיר 3 מטרות עבור אבטחת פרוטוקול ושימוש בקריפטוגרפיה:

1. להצפין את המסר הנשלח
2. לאמת זהות שולח ומקבל
3. לאשר אותנטיות מסמך ושלא נעשו שינויים

על מנת להבין את תשתיות הקריפטוגרפיה ולאחר מכן את שימוש מערכת הביטקוין באבטחה, נצטרך לסגור מספר מושגים בסיסיים של אבטחה.

*הצפנה א-סימטרית –* היא הצפנה העושה שימוש במפתחות שונים (פרטי וציבורי) להצפנה ולפענוחה. יש צורך להתאים מפתח שיחה זמני עבור כל שיחה כך שהצדדים יוכלו לפענח את מה שכתוב עם המפתחות הציבוריים והאישיים שלהם.

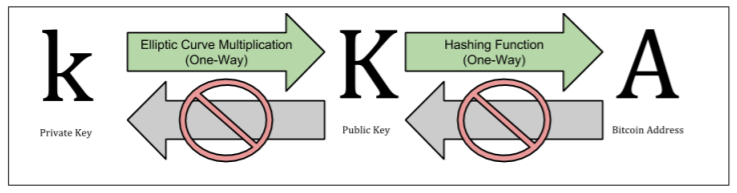
*כתובת ביטקוין* היא למעשה *מפתח ציבורי* המוצפן באמצעות פונקציית Hash חד כיוונית.

*מפתח ציבורי* – הוא מפתח הנוצר באמצעות פונקציה מתמטית (עקומות אליפטיות) חד כיוונית על *המפתח הפרטי*.

*מפתח פרטי* – הוא מספר שנוצר באופן רנדומלי **ככל שניתן** בגודל ומוצג בHEX. (ליצור מספר רנדומלי אמיתי זוהי משימה קשה ומסוכנת. רוב התוכנות והאפליקציות שנשתמש בהן על מנת להגריל מספר יתנו מספר צפוי מראש).

למעשה, ניתן לבחור לבד את המפתח הפרטי - למשל 11, או 123456789, אם כי הוא יהיה קל לניחוש.

המפתח הפרטי מוצג ע"י פונקציית Hash (SHA256) כדי להכניס את המספר לגודל הרצוי.



כיוון שהפונקציות הן חד כיווניות – **אין** דרך לחשב את המפתח הפרטי מתוך המפתח הציבורי.

כדי להבין איך מפיקים מפתח ציבורי מתוך המפתח הפרטי (המוגרל באופן רנדומלי) נצטרך להבין פונקציה חד כיוונית הנקראת "עקומות אליפטיות".

עקומה אליפטית היא פונקציה מהצורה . בפרט, ביטקוין משתמש בעקומה אליפטית מסוימת: או יותר נכון ובפרמטרים מסוימים.

כל הפרמטרים הרלוונטים לפונקציית ההצפנה של מפתחות ציבוריים בביטקוין נכללים בשם Secp256k1.

<https://en.bitcoin.it/wiki/Secp256k1>

*p* = FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFE FFFFFC2F= 2256 - 232 - 29 - 28 - 27 - 26 - 24 - 1

PGP – שיטת הצפנה המשתמשת ב- SHA1 על מנת

<http://vlib.eitan.ac.il/encryption1/Misc/Hadgamot.htm> (אתר בעברית להסבר על סוגי הצפנות שונים)