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.

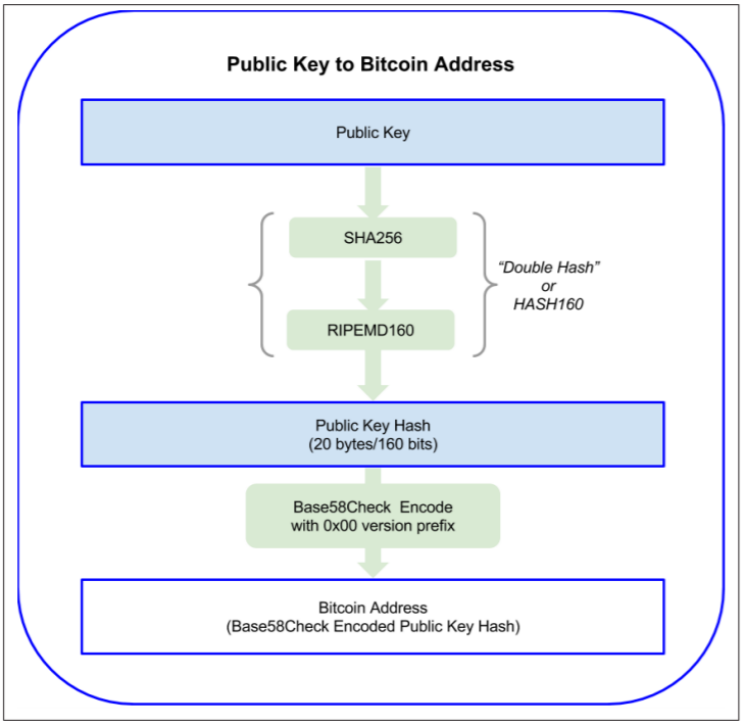
נוכל, אם כן, להגדיר 3 מטרות עבור אבטחת פרוטוקול ושימוש בקריפטוגרפיה:

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.

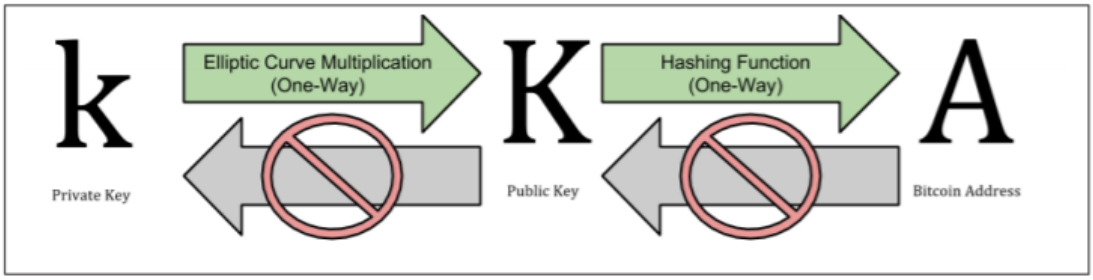


מפתח ציבורי – מורכב מקאורדינטות (x, y) על גרף העקומה האליפטית. המפתח נוצר באמצעות "הכפלה" חד כיוונית של *המפתח הפרטי* בנקודה קבועה על העקומה. (ומוצג באמצעות Hash160)

מפתח פרטי – הוא מספר שנוצר באופן רנדומלי **ככל שניתן** בגודל 2^{256} 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.

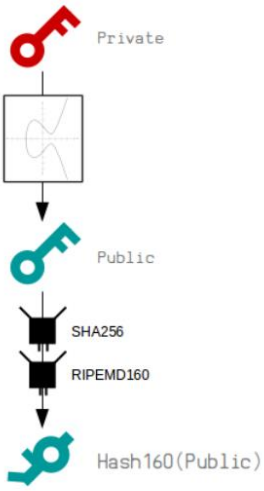
כדי להבין איך מפיקים מפתח ציבורי מתוך המפתח הפרטי (המוגרל באופן רנדומלי) נצטרך להבין פונקציה חד כיוונית הנקראת "עקומות אליפטיות".

עקומה אליפטית היא פונקציה מהצורה $y^2 = x^3 - p \cdot x - q$. בפרט, ביטקוין משתמש בעקומה אליפטית מסוימת: $y^2 = x^3 + 7$ או יותר נכון $y^2 \; mod \; p = x^3 + 7 \; mod \; p$ ובפרמטרים מסוימים.

המודולו נועד כדי לשבור את התבנית וכדי ליצור רצף נקודות שקשה מאוד לנבא.

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

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



בעצם, עבור מפתח פרטי k, ניתן ליצור מפתח ציבורי K בצורה הבאה: $K = k \cdot G$ כך ש*G* הוא נקודה קבועה על העקומה האליפטית המסוימת עבור כל רשת הביטקוין.

p = FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFE FFFFFC2F= $2^{256} - 2^{32} - 2^9 - 2^8 - 2^7 - 2^6 - 2^4 - 1$

(p = 115792089237316195423570985008687907853269984665640564039457584007908834671663)

G = 04 79BE667E F9DCBBAC 55A06295 CE870B07 029BFCDB 2DCE28D9 59F2815B 16F81798 483ADA77 26A3C465 5DA4FBFC 0E1108A8 FD17B448 A6855419 9C47D08F FB10D4B8

G = (55066263022277343669578718895168534326250603453777594175500187360389116729240L,

3267051002075881697808308513050704318447127338065924327593890433575733748242 4L)

מספר זה מייצג נקודה על העקומה האליפטית. הכפלה של נקודה זו בכל מספר שלם כלשהו, תיתן נקודה חדשה **על העקומה**. הכפלה זו היא חד כיוונית ולכן בהינתן תוצאה (מפתח ציבורי) והנקודה G, לא ניתן לגלות את המפתח הפרטי.

הכפלת קאורדינטה במספר X – היא פעולה של הוספת הנקודה לעצמה X פעמים. בכל הוספה, נמצא את הנקודה המקבילה לנקודה בה המשיק מהנקודה הראשונה חותך את העקומה:

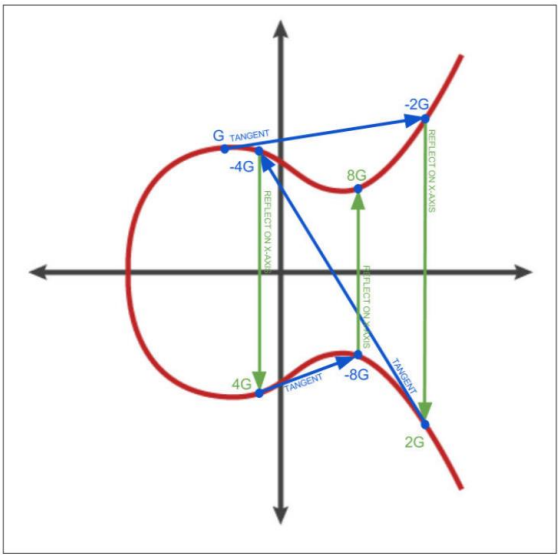


Figure 4-4. Elliptic Curve Cryptography: Visualizing the multiplication of a point G by an integer k on an elliptic curve

אפשר לראות בתמונה הכפלה בשלמים עד 8 של הנקודה G. נשים לב שבכל הפכלה צריך לחשב מחדש ואין חוקיות עבור מיקום נקודת ההכפלה הבאה. כמו כן, כל הכפלה שלילית היא תמונת מראה של ההכפלה החיובית.

אחרי מציאת נקודת המפתח הציבורי, הוא מקבל קידומת 04, לאחריה הקאורדינטות וזו כתובת המפתח הציבורי.

בחלק מההעברות מצורף המפתח הציבורי עצמו ולכן יש צורך לכווץ אותו בדרך הבאה:

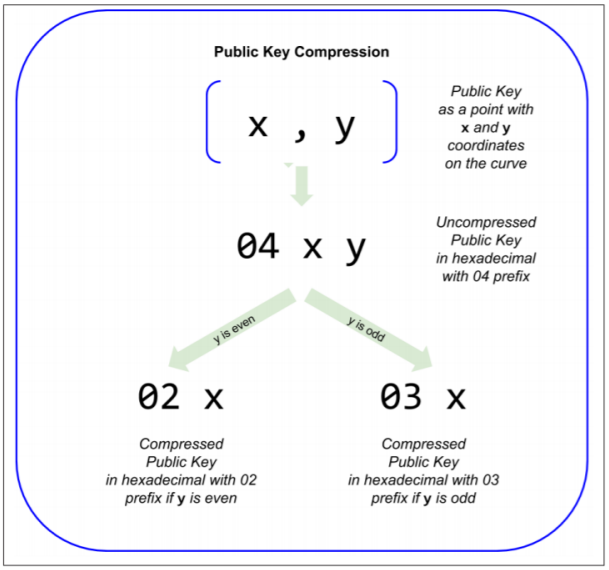


Figure 4-7. Public Key Compression

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

אחרי כיווץ המפתח מגבבים אותו באמצעות SHA256 כדי "להצפין" עד כמה שאפשר את המפתח הציבורי. את הגיבוב עצמו מגבבים באמצעות RIPEMD160

https://www.coindesk.com/math-behind-bitcoin (הסבר צעד אחר צעד על כתובת הביטקוין מתוך המפתח הפרטי)