

אליס רוצה להעביר הודעה חתומה דיגיטלית על ידה לבוב, כך שהוא יהיה בטוח שזה בא ממנה. ההודעה היא M. המפתח הפרטי של אליס הוא d, המפתח הציבורי שלה הוא: e. היא משתמשת בפונקציית האש ידועה h. ההודעה לא צריכה להיות מוצפנת.

הנה תיאור מפורט של תהליך יצירת החתימה הדיגיטלית על ידי אליס ואימותה על ידי בוב, שלב אחר שלב:

שלב 1: יצירת החתימה הדיגיטלית (על ידי אליס)

1. **חישוב ערך ההאש:** אליס לוקחת את ההודעה המקורית M ומעבירה אותה דרך פונקציית ההאש h התוצאה היא ערך האש (Hash Digest) ייחודי וקבוע באורכו:

$$H=h(M)$$

2. **הצפנת ההאש (חתימה):** אליס מצפינה את ערך ההאש H באמצעות המפתח הפרטי שלה d פעולת ההצפנה הזו מייצרת את החתימה הדיגיטלית, אותה נסמן כ-S:

$$S=\text{encrypt}(d) \text{ of } H$$

3. **שליחת המסר:** אליס מצרפת את החתימה S לצד ההודעה המקורית M, ושולחת לבוב את החבילה: M,S.

שלב 2: אימות החתימה (על ידי בוב)

כאשר בוב מקבל את החבילה M,S, הוא מבצע שתי פעולות במקביל כדי לוודא שההודעה אכן הגיעה מאליס ולא שונתה בדרך:

1. **חישוב האש עצמאי:** בוב לוקח את ההודעה M שקיבל, ומעביר אותה בדיוק באותה פונקציית האש h שבה השתמשה אליס. הוא מקבל ערך האש חדש, נסמן אותו כ H כלומר $H1=h(M)$

2. **פענוח החתימה הדיגיטלית:** בוב לוקח את החתימה הדיגיטלית S שקיבל, ומפענח אותה באמצעות המפתח הציבורי של אליס e. הפענוח משחזר את ערך ההאש המקורי שאליס הצפינה, נסמן אותו כ-H2

$$H2=S \text{ decrypt } (e)$$

שלב 3: ההשוואה וההכרעה

- בוב משווה בין שני הערכים שקיבל: הוא בודק האם $H1 == H2$
- אם הערכים זהים - החתימה תקפה. בוב יכול להיות בטוח ב-100% ש:

1. ההודעה הגיעה מאליס (רק המפתח הפרטי שלה d) יכול היה ליצור חתימה שמפוענחת בהצלחה בעזרת המפתח הציבורי שלה e).

2. ההודעה לא שונתה או זויפה בדרך (אם תו אחד היה משתנה, ערך ה-Hash שהיה מופק בשלב 2 היה שונה לחלוטין).

- **אם הערכים שונים $H1 \neq H2$ החתימה אינה תקפה.** בוב יודע שההודעה שונתה בדרך, או שהיא לא נחתמה על ידי אליס