מבוא לקריפטולוגיה - דף תרגילים מספר 4

1. (60%) להלן סכמת חתימה של **אונג-שנור-שמיר**:
נניח שאליס רוצה לחתום על מסמך.

<u>יצירת מפתחות החתימה:</u>
אליס בוחרת מספר אי-זוגי גדול n (אין צורך לדעת את הפרוק שלו) ומספר אקראי k שזר ל n. אליס מחשבת את $g\equiv-\left(k^{-1}\right)^2 \pmod{n}$.
המפתח הפומבי של אליס הוא (n,g) והמפתח הסודי הוא (n,k).

<u>חתימה:</u>
כדי לחתום על מסמך M אליס בוחרת מספר אקראי r שזר ל n ומחשבת:

$$S_1=2^{-1}(h(M)r^{-1}+r) \pmod{n}$$

$$S_2=2^{-1}k(h(M)r^{-1}-r) \pmod{n}$$

מגדירים $sig(M)=\left(S_1,S_2\right)$. שימו לב ש $h(M)$ הוא ערך hash של המסמך /M
<u>בדיקת החתימה</u>: $ver\left(M,\left(S_1,S_2\right)\right)=True \Leftrightarrow S_1^2+gS_2^2\equiv h(M) \pmod{n}$.

א. (20%) הוכיחו שבדיקת החתימה נכונה, כלומר,

$$S_1^2+gS_2^2\equiv h(M) \pmod{n} \Leftrightarrow sig(M)=\left(S_1,S_2\right)$$

ב. (40%) ממשו את סכמת החתימה בקוד. לשם כך כיתבו תוכנית המכילה את המרכיבים הבאים:

a. מחלקה OSSGenerator שהבנאי שלה מקבל את הגודל של n בבתים ומייצר זוג מפתחות חתימה שנשמרים כמשתני מחלקה private. המחלקה תכיל שתי שיטות נוספות:
   i. get_public_key שמחזירה אובייקט מפתח פומבי (ר' סעיף ב')
   ii. get_private_key שמחזירה אובייקט מפתח פרטי (ר' סעיף ג')

b. מחלקה OSSPubKey שהבנאי שלה מקבל שני מספרים שמהווים את המפתח הפומבי ושומרת אותם כמשתני מחלקה. המחלקה תכיל שיטה ver שמקבלת מסמך (מטיפוס bytes) וחתימה ובודקת אם החתימה נכונה.

c. מחלקה OSSPriKey שהבנאי שלה מקבל שני מספרים שמהווים את המפתח הפרטי ושומרת אותם כמשתני מחלקה. המחלקה תכיל שיטה sig שמקבלת מסמך m (מטיפוס bytes) וחותמת עליו. השיטה תחזיר את הזוג (S_1,S_2).

d. פונקציה main שמציגה בפני המשתמש 3 אפשרויות:
   i. יצירת מפתח הצפנה. המשתמש יתבקש להגיד את גודל המפתח. המפתחות יישמרו לשני קבצים private.key ו public.key.
   ii. חתימה על מסמך. המשתמש יתבקש לתת את שם הקובץ שבו נמצא המסמך. תשמש בקובץ private.key כדי ליצור חתימה ותשמור את המסמך ואת החתימה עליו בקובץ חדש עם סיומת sig.
   iii. בדיקת חתימה על מסמך. המשתמש יתבקש לתת את שם הקובץ בו נמצאים המסמך והחתימה ותשתמש בקובץ public.key כדי לבדוק את החתימה.

* לצורך חישוב $h(M)$ יש להשתמש ב sha256. מצורף הקובץ modular_funcs.py ובו פונקציות לחישובים מודולריים.

2. (40%) להלןווריאציה של סכמת הפצת המפתחות של Diffie-Hellman שיכולה לשמש לחתימה:

גורמים פומביים:

מספר ראשוני q

α מספר פרימיטיבי מודולו q

מפתח פרטי:

$X \in Z_q^*$

מפתח פומבי : Y המקיים:

$Y = \alpha^X \mod q$

חתימה על מסמך M:

1. מחשבים קודם את $h=h(M)$, כאשר h היא פונקצית hash. נדרוש כי $\gcd(h,q-1)=1$. אם לא, מצרפים את h ל M ומחשבים את $h=h(M||h)$. ממשיכים עד שמקבלים מספר שזר ל $q-1$.
2. מחשבים מספר Z כך ש $Zh \equiv X \mod (q-1)$. .
3. החתימה של M תהיה $s = \alpha^Z \mod q$.

בדיקת החתימה: החתימה קבילה אם ורק אם

$s^h = Y \mod q$.

א. הראו מדוע הבדיקה נכונה.

ב. תארו דרך פשוטה לזיוף חתימה על מסמך. יש שתי אפשרויות. מספיק להראות את אחד מהם:

1) נתונים מסמך M וחתימה תקינה s. באמצעות מידע פומבי בלבד יש לחתום על מסמך אחר 'M באמצעות חתימה 's כך שבדיקת החתימה תחזיר True

2) לא נתון מסמך חתום M אלא רק המפתח הפומבי. יש לחתום על מסמך אחר 'M באמצעות חתימה 's כך שבדיקת החתימה תחזיר True