מבוא לקריפטולוגיה - דף תרגילים מספר 4

1. (40%) אליס משתמשת בסכמת החתימה ECDSA (עקומים אליפטיים) כדי לחתום על מסמכים שאותם היא שולחת לבוב. לבוב יש את המפתח הפומבי של אליס והוא משתמש בו כדי לוודא שהחתימה של אליס אותנטית. הבעייה שבתוכנת החתימה של אליס יש כמה באגים.

   א. אחרי שאליס חותמת על מסמך M ומייצרת חתימה (r,s) התוכנה שולחת בטעות את החתימה (r,-s) (-s הוא בעצם n-s). האם בוב יאשר את החתימה? נמקו.

   ב. נניח שתיקנו את הבאג של סעיף א'. עכשיו אליס חותמת על שני מסמכים שונים M_1 ו M_2 ושולחת לבוב את המסמכים עם החתימות (r_1,s_1) ו (r_2,s_2) בהתאמה. בשל באג נוסף בתוכנה של אליס היא השתמשה באותו מספר אקראי k עבור שתי החתימות. הראו כיצד בוב יכול להשתמש בעובדה הזאת כדי לגלות את המפתח הפרטי של אליס.

2. (60%) בתרגיל זה תממשו חתימה דיגיטלית המבוססת על עקום אליפטי. מצורפים הקבצים:

   i) modular_funcs.py ובו פונקציות לאריתמטיקה מודולרית ושבו השתמשנו בתרגיל בשיעור

   ii) ecc.py ובו המחלקות שהשתמשנו בהן בשיעור (כולל התוספות שעשינו7 בשיעור). בנוסף יש בקובץ פונקציה read_ec_data שמקבלת שם של קובץ וקוראת ממנו נתוני עקום אליפטי.

   iii) ec_bitcoin ובו הנתונים של העקום האליפטי שבו משתמשים בביטקוין

   א. כיתבו תוכנית make_keys.py שמקבלת שקוראת מהקובץ ec_bitcoin.txt נתוני עקום אליפטי (של ביטקוין) ומייצרת זוג מפתחות: מפתח פומבי ומפתח סודי לחתימה דיגיטלית. את המפתח הפומבי היא תשמור לקובץ public_key.txt ואת המפתח הסודי היא תשמור לקובץ private_key.txt

   ב. כיתבו תוכנית sign_ecdsa.py שמקבלת מהמשתמש שם של קובץ טקסט *filename*.txt וחותמת על תוכן הקובץ באמצעות המפתח הסודי שנמצא בקובץ private_key.txt (ובאמצעות נתוני העקום שנמצאים בקובץ ec_bitcoin.txt). את התוצאה יש לשמור בקובץ *filename*_sig.txt. (למשל, אם שם הקובץ הוא alibaba.txt אז החתימה תישמר לקובץ alibaba_sig.txt.). שימו לב שכדי לחתום יש להפוך את תוכן הקובץ ל bytes להפוך את זה למספר.

   ג. כיתבו תוכנית verify_ecdsa.py שמקבלת מהמשתמש שם של קובץ *filename*.txt ובודקת באמצעות מפתח פומבי שנמצא בקובץ public_key.txt אם החתימה שבקובץ *filename*_sig.txt מתאימה לתוכן הקובץ *filename*.txt. אם כן, היא תוציא הודעה signature OK. אם לא, התוכנית תוציא הודעה signature failed.

מצורפים קבצים לדוגמה: קובץ טקסט לחתימה, קובצי מפתחות וקובץ חתימה