תרגיל רשות מעשי בקריפטוגרפיה –

Paillier cryptosystem & Naïve Electronic Voting

מערכת ההצפנה של Paillier היא מערכת הצפנה עם מפתח ציבורי שיתרונותיה שהיא עם בטיחות מוכחת ובנוסף היא הומומורפית: בהינתן המפתח הציבורי והצפנות של שתי הודעות m_1 ו- m_2 ניתן בצורה יעילה לחשב הצפנה של m_1+m_1. בתרגיל תממשו מערכת הצפנה זו ואפליקציה שנגזרת מתכונת ההומומורפיזם – מערכת בחירות אלקטרונית פשטנית.

התרגיל הוא תרגיל רשות ומשקלו 10% מהציון. תאריך ההגשה יפורסם בהמשך.

מטרות התרגיל:

- קריאה עצמית והבנה של חומר מתקדם .
- הבנת מושגים כמו בטיחות של מערכת הצפנה ותכונת ההומומורפיות.
- התנסות בתכנות של מערכת קריפטוגרפית בדגש על יעילות המימוש.
- תכנות כלי של בחירות אלקטרוניות חשאיות שימדוד את איכות המימוש של המערכת הקריפטוגרפית.

אופן הבדיקה:

את התוכנית יש לשלוח לבודק במייל ובנוסף יש לקבוע מועד לבדיקה פרונטאלית בה עליכם יהיה להריץ את התוכניות שתכתבו ולענות על שאלות הבנה כלליות כגון : על איזה קושי קריפטוגרפי המערכ ת מסתמכת ? מהי בטיחות סמנטית ? מהי תכונת ההומומורפיות ומה היא מאפשר ת. השאלות באות לבדוק האם באמת קראתם את החומר (מתוך הסריקות המצורפות) ואין מה להילחץ שכן עבודות סבירות יכולות רק לשפר את הציון הסופי.

בנוסף, יש לצרף דוח עם תיאור המימושים שלכם ושיקולים ומסקנות מהמימוש שעשיתם.

ניתן להתייעץ עם פרופ' עמוס ביימל בכל הקשור להבנה התיאורטית של מערכת ההצפנה. בכל הקשור למימוש ניתן להתייעץ עם הבודק. שאלות ניתן גם לשאול בפורום באתר הקורס.

שם הבודק: אילן אורלוב

דואר אלקטרוני: ilanorv@cs.bgu.ac.il

הנחיות:

1. קראו בעיון את הקובץ המצורף מתוך הספר של Katz&Lindell. ניתן לדלג על ההוכחה של משפט 11.34.
2. כתבו תוכנית שתפקידה לממש את אלגוריתמי ההצפנה, פענוח ויצירת המפתחות כפי שקראתם.

- הכתיבה תהיה בשפה java.
- השיקולים התכנותיים נשארים בידיים שלכם, בכל אופן, המחלקות המומלצות שיהיו הן MyPaillier שתייצג את הסכמה ובה יהיו שיטות ליצירת מפתחות , הצפנה ופענוח, PrivateKey – שתייצג מפתח פרטי ו- PublicKey שתייצג מפתח ציבורי.
- יש להשתמש בספריה java.math.BigInteger בכדי לעבוד עם מספרים גדולים באמת.
- כעת, המטרה היא שתממשו את המרכיבים של הפרוטוקול ותשוו את המימוש עם פונקציות הספרייה, לכן יש לאגד את כל הקריאות לפונקציות שאתם תממשו ובנוסף יש לאגד את הקריאות לפונקציות הספרייה המקבילות.
- יש לממש העלאה בחזקה מודולו מספר, כפי הנלמד בכיתה.
- יש לממש יצירת מספר ראשוני גדול (לטובת יצירת המפתחות) באופן הבא: הגרלת מספר ששקול לשלוש מודולו ארבע ושימוש באלגוריתם שנלמד בכיתה. ניתן ורצוי לשפר את האלגוריתם – הפעילו מחשבה ותקבלו ציון בונוס בהתאם.

- יש לממש את האלגוריתם למציאת gcd – אלגוריתם אוקלידס כפי שנלמד בכיתה.
- יש לממש אלגוריתם למציאת הופכי בשדה סופי.
- אורך המפתח צריך להיות לפחות 1024 ביטים.
- יש לממש מימוש מקביל שמשתמש בפונקציות ספרייה : קריאה להעלאה בחזקה מודולו מספר , יצירת מספר ראשוני גדול באמצעות הבנאי ב – BigInteger, האלגוריתם למצי את gcd והאלגוריתם למציאת הופכי בשדה סופי.

3. כתבו מערכת בחירות אלקטרוניות שתשתמש בתכונת ההומומורפיות של פונקצית ההצפנה. שימו לב, מערכת הבחירות שאתם הולכים לממש נאיבית למדי (כל משתתף שולח ה צפנה של הבחירה שלו ומניח שהמקבל /שופט לא יפענח את הבחירה שלו, אלא רק **אחרי** שיכפיל את כל הבחירות של השחקים האחרים).
   - הכתיבה תהיה בפרויקט שיצרתם בסעיף הקודם.
   - כמו מקודם, השיקולים התכנותיים נשארים בידיים שלכם , אך המחלקות המומלצות הן Voter שתייצג בוחר ו-VotingSystem שתייצג מערכת ספירת קולות.
   - יש להשתמש בספריה java.math.BigInteger בכדי לעבוד עם מספרים גדולים באמת.
   - במחלקה שתייצג מצביע יש לממש שיטה שמגרילה מספר באקראי בין אפס לאחד ואם המספר המתקבל גדול מחצי אז המצביע מחליט להצביע עבור אפשרות א' אחרת מחליט להצביע עבור אפשרות ב'.
   - במחלקה שתייצג מערכת בחירות יש ליצור מערך עם המצביעים שהו לכים להשתתף בפרוטוקול המאובטח להצבעה כפי שמפורט בדפים.
   - יש לממש שתי קריאות שונות לפונקצית ההצפנה והפענוח של תוצאות הבחירות:
     א. הצפנה ופענוח שבוחרים להשתמש במימושים שלכם מהחלק הקודם.
     ב. הצפנה ופענוח שבוחרים להשתמש בפונקציות הספרייה, כפי שתואר בחלק הקודם.
   - בדקו עד כמה הצלחתם לממש את הדברים בצורה יעילה . כלומר, בדקו על מספר אורכים שונים של מפתחות ועל מבחר של מספרי מצביעים בפרוטוקול מה היחס של זמן הריצה בין סט המימושים שלכם ו למימוש המשתמש בפונקציות הספרייה.

מקורות:

1. Jonathan Katz and Yehuda Lindell. Introduction to Modern Cryptography. Chapman & Hall/Crc Cryptography and Network Security Series, Pages 408—417, 2007.
2. Pascal Paillier. Public-Key Cryptosystems Based on Composite Degree Residuosity Classes, *EUROCRYPT' 99*, vol. 1592 of Lecture Notes in Computer Science, pp. 223 —238, Springer-Verlag, 1999.