ב"ה

בנית ישומים מאובטחים - תשפ"ב:

תרגיל תכנותי ב Java Crypto API

א. יצרו מפתח פרטי וציבורי עבור צד א' (עבור אלגוריתם RSA) באמצעות השימוש בתוכנית keytool

http://docs.oracle.com/javase/6/docs/technotes/tools/solaris/keytool.html

על המפתח הפרטי שנשמר ב Keystore המיוצר באמצעות Keytool להיות מוגן באופן האוטימלי האפשרי

ב. יצרו מפתח פרטי וציבורי עבור צד ב' (עבור אלגוריתם RSA) באמצעות השימוש בתוכנית keytool , על המפתח הפרטי שנשמר ב Keystore המיוצר באמצעות Keytool להיות מוגן באופן האוטימלי האפשרי

ג. כל אחד משני הצדדים יוצר באמצעות ה Keytool תעודה דיגיטלית מסוג Self-Signed Certificate ו"מעביר" אותה לצד השני. כל צד שמקבל את התעודה הדיגיטלית של עמיתו טוען אותה ל Keystore כ Trusted certificate.

כל הפעולות בשלבים א-ג יעשו באמצעות command line ויש לתעד את ה command lines בהם השתמשתם עבור כל אחד מהשלבים לעיל. את השלבים הבאים יש לעשות תוך שימוש ב keystores שיצרתם.

ד. בנו תוכנית להצפנת וחתימת קבצים.

- התוכנית קוראת קובץ גלוי, יוצרת קובץ חדש המכיל את תוכן הקובץ המקורי מוצפן
- התוכנית מחשבת חתימה דיגיטלית אסימטרית של תוכן הקובץ ושומרת אותו בקובץ קונפיגורציה המצורף לקובץ המקורי
- התוכנית מבצעת כתיבה של קובץ באופן מוצפן באמצעות שימוש ב CipherOutputStream
- את ה Cipher יש לאתחל לשימוש באלגוריתם AES במוד CTR או במוד CBC תוך שימוש ב IV אקראי
- את המפתח לאלגוריתם ההצפנה יש להגריל באופן אקראי תוך שימוש בפונקציה המתאימה
- את המפתח יש להצפין בהצפנה אסימטרית תוך שימוש באלגוריתם ה RSA
- את המפתח המוצפן כמו גם פרמטרים מוספים אפשר לשמור בקובץ הקונפיגורציה שיצורף לקובץ המוצפן (שבו תשמר גם החתימה הדיגיטלית של הקובץ המוצפן)
- את המפתח הציבורי שידרש להצפנת המפתח הסימטרי יש לקרוא מהתעודה הדיגיטלית שתקרא ה KeyStore המתאים
- את המפתח הפרטי שידרש לחתימה הדיגיטלית יש לקרוא מה KeyStore המתאים (את הסיסמא יש לקבל כפרמטר לתוכנית)

ה. בנו תוכנית לפיענוח ובדיקת חתימה דיגיטלית של קבצים מוצפנים וחתומים.

- התוכנית קוראת את הקובץ המוצפן מפענחת אותו ובודק את השלמות שלו

- את הפרמטרים לפענוח הקובץ ולבדיקת החתימה הדיגיטלית התוכנית המפענחת קוראת מקובץ קונפיגורציה שהוכן ע״י התוכנית המצפינה
- התוכנית מבצעת קריאה של קובץ באופן מוצפן באמצעות שימוש ב CipherInputStream
- התוכנית תבדוק את השלמות של הקובץ לאחר הפענוח שלו
- את המפתח הציבורי שידרש לבדיקת החתימה הדיגיטלית יש לקרוא מהתעודה הדיגיטלית שתקרא מה KeyStore המתאים
- את המפתח הפרטי שידרש לפענוח הקובץ יש לקרוא מה KeyStore המתאים (את הסיסמא יש לקבל כפרמטר לתוכנית)
- בהנחה שבדיקת השלמות של הקובץ (על פי החתימה דיגיטלית) תקינה, התוכנית תיצור קובץ פלט עם התוכן הגלוי שפוענח (אם בדיקת התוכן נכשלה התוכנית תכתוב למסך ולקובץ הודעת שגיאה)

הערות:

- התוכניות צריכות להכתב על פי הכללים המקובלים של הנדסת תוכנה
- התוכניות צריכות להכתב באופן שניתן להחליף את האלגוריתמים ואת ה Crypto providers בקלות
- יש לצרף את קובץ הקוד ולתעד אותו באופן שמסביר היטב כיצד השתמשתם בכל אחד מה API ומדוע
- יש להגיש את קובץ הקוד המתועד, את ה JAR המאפשר להריץ את התוכנית כולל הוראות כיצד להריץ את התוכנית וכולל ה Keystore
- יש להגיש פלט ההרצה של התוכנית המאפשר לראות שהתוכנית עובדת כהלכה כולל קובץ הקונפיגורציה שהתוכנית המצפינה יוצרת , הקובץ הגלוי והקובץ המוצפן.
- הניקוד של התרגיל יהיה כדלקמן:
  - נכונות המימוש מבחינה קריפטוגרפית (כולל אופן השימוש ב Java Crypto API) – 35%
  - קוד בנוי באופן שמאפשר לבחור אלגוריתם ולבחור Provider בקלות – 7%
  - שימוש נכון ב Keytool וב Keystore –8%
  - הסבר מפורט של השיקולים שהנחו אתכם במימוש–10%
  - תיעוד של הקוד –15%
  - הנדסת תוכנה - 10%
  - העובדה שהקוד רץ ומיצר תוצאות נכונות (כולל דוגמא לפלט הרצה)- 15%

הנחיות הגשה:

- יש להכין את התרגיל בזוגות !!!
- יש להגיש את התרגיל עד יום א׳ ה 19 לדצמבר 2021
- יש הגיש את התרגיל באמצעות המודל

- יש להגיש קובץ zip ששמו יהיה בפורמט הבא : <ת״ז מגיש 1>_<ת״ז מגיש 2>.
  - לדוגמה, הגשת תרגיל ע״י הסטודנטים בעלי ת״ז 123456789 ו-987654321 תיעשה בקובץ ששמו : 123456789_987654321
- בתוך קובץ ה zip-תהיה תיקיה אחת בשם submission ובה כל הקבצים להגשה כולל קובץ בשם run.txt שבו יהיו הפקודות הנדרשות להרצת קבצי ה JAR. הקובץ יכיל רק את הפקודות. ניתן לשים את התיעוד עליהן בקובץ תיעוד נפרד.
- על הפקודות להיות כתובות כך שהן יריצו את תוכנית ההצפנה ומיד לאחריה את תוכנית הפענוח .הפקודות צריכות לעבוד ללא כל שינוי כאשר הן מורצות מתוך התיקיה submission (כלומר כאשר submission הוא ה-current directory).
- שם קובץ הקלט של ההצפנה יהיה plaintext.txt ושם קובץ הפלט של הפענוח יהיה decrypted.txt, כאשר שני הקבצים האלו ימוקמו בתיקיה submission, והפקודות הנ״ל צריכות להתייחס לשמות הקבצים האלו.

בברכה

ד״ר דוד מובשוביץ