ד"ר בני פנקס

מבוא לקריפטוגרפיה - מועד א'

החוג למדעי המחשב – אוניברסיטת חיפה
סמסטר א' תשס"ה
30.1.2005

הנחיות:

1. בטופס הבחינה שלושה דפים מלבד דף זה. ודאו כי כולם נמצאים בידכם.
2. בבחינה 5 שאלות שמשקלן שווה. **יש לענות על 4 שאלות בלבד.** (לא יבדקו יותר מ-4 שאלות.)
3. הבחינה עם חומר פתוח.
4. **נמקו את כל תשובותיכם.** פתרון ללא הוכחה לא יתקבל.
5. משך הבחינה 2.5 שעות.
6. הנכם רשאים להסתמך על סעיפים קודמים, גם אם לא השבתם עליהם.

בהצלחה!

1. נעיין במערכות הצפנה פומבית הבנויות על העקרונות הבאים:

- המפתח הפומבי מורכב ממספר n באורך 1536 סיביות, וממספר e המקיים $\gcd(e,\varphi(n))=1$.
- המפתח הפרטי הוא מספר d המקיים $e\cdot d=1 \bmod \varphi(n)$.
- ההודעות הן מספרים m המקיימים $0<m<n$ וכן $\gcd(m,n)=1$.
- הצפנה מתבצעת ע"י חישוב $c=m^e \bmod n$.
- פענוח מתבצע ע"י חישוב $m=c^d \bmod n$.

מוצעות שלוש שיטות מימוש שונות:

א. $n=p$, מספר ראשוני.
ב. $n=p\cdot q$, כאשר p ו-q הם מספרים ראשוניים שווים באורכם שניבחרו באקראי.
ג. $n=p\cdot q\cdot r$, כאשר p,q ו-r הם מספרים ראשוניים שווים באורכם שניבחרו באקראי.

ענו על השאלות הבאות:

א. (8%) הסבירו מדוע הפענוח מסתיים בהצלחה בכל אחת מהשיטות.

ב. (8%) השוו את השיטות מבחינת יעילות חישובית.

ג. (9%) השוו את השיטות מבחינת בטיחות.

2. נניח ש-$F(m,k)$ היא שיטת הצפנה סימטרית בה מרחב ההודעות והקריפטוגרמות הוא $\{0,1\}^n$. מוצעת שיטת הצפנה אקראית $G(m,k)$ כלהלן:

בהינתן הודעה $m\in\{0,1\}^n$ בחר באקראי $r\in\{0,1\}^n$ וחשב את $F(r,k)$.
הקריפטוגרמה היא הזוג $G(m,k) = [F(r,k), r\oplus m]$.

א. (10%) הסבירו כיצד יכול מקבל הקריפטוגרמה של G, היודע את k, לפענח את ההודעה m.

ב. (15%) נמקו את הטענה הבאה: אם F עמידה בפני KPA אזי G עמידה בפני CPA.

- KPA – known plaintext attack
  (הניחו כי ההודעות ניבחרות באקראי, ומקבלים את ההודעות ואת ההצפנה שלהן)
- CPA – chosen plaintext attack

<u>רמז:</u> הוכיחו כי אם G אינה עמידה בפני CPA אזי F אינה עמידה בפני KPA. כלומר, הראו כי ניתן לשבור את F ב-KPA אם קיים לרשותנו אלגוריתם A שפועל בצורה הבאה: בוחר m כרצונו, מקבל את $G(m,k)$, מחשב את k ומודיע אותו. (איננו יודעים כיצד A פועל, ביכולתנו רק להפעיל אותו כ-"קופסא שחורה". נניח כי הוא תמיד מוצא את הערך הנכון של k.)

3. יהי p מספר ראשוני איזוגי, ו- r מספר שלם חיובי המקיים $r|(p-1)$. נסמן ב-[rR] את קבוצת האיברים ב-Z^*_p שהם חזקות r-יות מודולו p. כלומר $[rR] = \{a\in Z^*_p \mid \exists b,\ a\equiv b^r \bmod p\}$.

בפתרון השאלות הבאות ניתן להשתמש בעובדה קיום גנרטור (איבר פרימיטיבי) ב-Z^*_p.

א. (10%) הוכיחו שאם $a\in[rR]$ אזי $a^{((p-1)/r)} \equiv 1 \bmod p$.

ב. (10%) הוכיחו שאם $a^{((p-1)/r)} \equiv 1 \bmod p$ אזי $a\in[rR]$.

ג. (5%) אם $a\in[rR]$, כמה שורשי-r יש ל-a ב-Z^*_p ?
כלומר, כמה פתרונות שונים יש ב-Z^*_p למשוואה $a\equiv x^r \bmod p$?

4. יהיו p ו- q מספרים ראשוניים שונים זה מזה ו- $n=pq$.

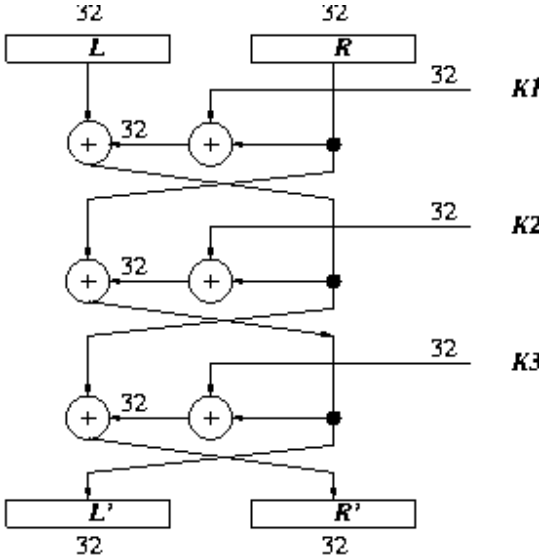
א. (10%) נתונים שני מספרים A ו-B המקיימים $A\equiv B \bmod p$ אבל $A\not\equiv B \bmod q$. הראו איך ניתן לפרק את n ביעילות כאשר נתונים A,B ו- n.

ב. (15%) נתונים מספרים e,d כך ש- $e\cdot d\equiv 1 \bmod \varphi(n)$. תהי $M\in Z^*_n$ הודעה ו- $C=M^e \bmod N$ ההצפנה שלה. מפענח מנסה לפענח את M בצורה הבאה:

- מחשב $M_p = C^d \bmod p$.
- רוצה לחשב $M_q = C^d \bmod q$, אולם טועה בחישוב ומקבל $M'_q \not\equiv M_q \bmod q$.
- מחשב בעזרת משפט השאריות הסיני M' המקיים:
  $M'\equiv M_p \bmod p$, ו- $M'\equiv M'_q \bmod q$.

הראו כיצד ניתן לפרק בקלות את n כאשר נתונים M, M' ו- n.

5. בשאלה זו נראה איך לשבור את מערכת ההצפנה הבאה. זוהי מערכת דמוית DES בת 3 סיבובים, כאשר הפונקציה F מוחלפת ב-⊕.



א. (9%) הראו כי בהינתן זוג קלט-פלט M=(L,R) ו- C=(L',R') של המערכת ישנן 2^{32} אפשרויות בדיוק לשלישיית המפתחות *k*1,*k*2,*k3*.

ב. (8%) נתון כי היריב יודע זוג קלט-פלט אחד של המערכת, M=(L,R) ו- C=(L',R'). הראו כי הוא יכול לחשב ביעילות <u>הצפנה</u> של כל הודעה אחרת מהצורה M*=(L,R*) (כלומר, הודעה בה החצי השמאלי של ההודעה שווה לחצי השמאלי של M).

ג. (8%) נתון כי היריב יודע זוג קלט-פלט אחד של המערכת. הראו כי הוא יכול <u>לפענח</u> ביעילות כל קריפטוגרמה אחרת.