אוניברסיטת חיפה | החוג למדעי המחשב

מבוא לקריפטוגרפיה
(203.3444/203.4444)

סמסטר אביב 2010 – מועד א'
(אחרי תיקונים מהמבחן)

תאריך: 21.6.2011

מרצה: ד"ר אור דונקלמן

1. משך המבחן שעתיים וחצי.
2. במבחן 4 שאלות, ענה/י על כולן.
3. חומר עזר מותר בשימוש: כל חומר עזר מודפס. אין להשתמש בכל חומר עזר אלקטרוני.
4. הקדש/י את 10 הדקות הראשונות לקריאת כל השאלות והבנתן.
5. ענה/י תשובות קצרות וברורות ככל האפשר. נמק/י את תשובתך.
6. באם אינך יודע/ת את התשובה לסעיף, ניתן לרשום "לא יודע/ת", ולקבל כ-20% מציון הסעיף.

בהצלחה!

<u>שאלה 1 (30 נקודות)</u>

אחת הבעיות העיקריות של DES הינה אורך המפתח הקצר (56 ביטים בלבד). כדי להתמודד עם הבעיה, הוצעו בעבר מספר פתרונות, כאשר אחד מהם נקרא DESX.
בצופן DESX, מוגדרים שלושה מפתחות, הראשון $K_{internal}$ באורך 56 ביטים, ושני הנוספים K_{before} ו-K_{after}, באורך של 64 ביטים. ההצפנה ב-DESX מבוצעת באופן הבא:

$$DESX_{K_{before},K_{internal},K_{after}}(P) = DES_{K_{internal}}(P \oplus K_{before}) \oplus K_{after}$$

א. הראה/י כיצד מתבצע הפענוח ב-DESX (בהנתן המפתחות). (3 נק')
ב. הראה/י כי כל התקפה על DESX המוצאת את המפתחות בפחות מ-2^{56} הפעלות DES, יכולה לשמש למציאת מפתח DES בפחות מ-2^{56} הפעלות DES. (5 נק')
ג. הוכח/י כי ב-DESX מתקיים:

$$DESX_{K_{before},K_{internal},K_{after}}(P) = DESX_{\overline{K_{before}},\overline{K_{internal}},\overline{K_{after}}}(P)$$
(5 נק')

ד. האם ל-DESX ישנם מפתחות חלשים עבורם פעולת ההצפנה שקולה לפעולת הפענוח? אם כן, כמה? (5 נק')
ה. הצע/י התקפה המוצאת את שלושת המפתחות בזמן של עד 2^{120} הפעלות DESX. תאר/י את שלבי ההתקפה, וכמה נתונים דרושים כדי למצוא את המפתח באופן יחיד (עד כדי התכונה שהוצגה בסעיף ג'). (7 נק').
ו. כדי להאיץ את ביצועי DESX, הוצע לקבוע את המפתח האמצעי לערך קבוע, כלומר, לקבוע כי $K_{internal} = 0123456789ABCD_x$. תאר/י התקפה המוצאת את K_{before} ו-K_{after}, תוך שימוש בשני זוגות נתונים ידועים $(P_1, C_1), (P_2, C_2)$ בזמן של 2^{65} הפעלות DES. (5 נק')

<u>שאלה 2 (30 נקודות – כל סעיף 5 נק')</u>

שאלה זו דנה באלגוריתם RSA. בכל סעיפי השאלה נניח כי $\gcd(e,(p-1)(q-1))=1$.

א. כפי שהזכרנו בכיתה, לרוב משמש RSA לצורך הצפנת מפתח סימטרי. בחברת ASR, הוחלט להשתמש במפתח RSA המורכב ממכפלה של זוג ראשוניים באורך 768 ביט כל אחד, יחד עם $e=9$, כדי להחליף מפתח באורך 128 ביטים לצורך המשך ההצפנה עם AES (בעל מפתח של 128 ביט). לכן, לצורך שליחת k מפתח ה-AES (באורך 128 ביטים), נשלח הערך $c=k^9 \pmod{n}$.
להפתעת אנשי החברה, כל מפתחות ה-AES שהיו בשימוש במערכת התגלו ע"י התוקפים. הסבר/י כיצד בוצעה ההתקפה.

ב. מהו ערך ה-e המינימלי עבורו מובטח שההתקפה מסעיף א' לא תעבוד עבור ערכי k שאינם 0 או 1?

ג. כדי להתמודד עם ההתקפה, הוחלט בחברה ASR לשלוח את הערך $c=(n-k)^9 \pmod{n}$ כדי להסכים על מפתח ה-AES. עם זאת, מיד עם ביצוע השינוי, נחשפו כל מפתחות ה-AES שהועברו מוצפנים. הסבר/י כיצד בוצעה ההתקפה.

ד. לאחר שבירת המערכת, הוחלט בחברת ASR להשתמש בגרסא משופרת של RSA. בגרסא זו, p נבחר להיות ראשוני גדול מהצורה $p=2^i+1$ עבור $i>1000$, בעוד q הינו מספר ראשוני באורך 768 ביט. המפתח הפומבי בגרסא זו נבחר להיות מהצורה $(n=pq, e=2^{32}+1)$. להפתעתם של אנשי ASR, גם בגרסא זו, כל מפתחות ה-AES שנשלחו מוצפנים התגלו. הסבר/י כיצד בוצעה ההתקפה.
רמז: התבונן/י בייצוג הבינארי של n.

ה. בשלב זה, החליטו אנשי חברת ASR לבחור את זוג הראשונים p,q כראשונים בטוחים באורך 768 ביטים כל אחד. כמו כן, e נבחר להיות $2^{16}+1$. לאחר פרסום מפתח ה-RSA הפומבי $(n=pq,e)$, דלפו 384 הביטים התחתונים של p לרשת האינטרנט. למרות זאת, החליטו אנשי החברה להמשיך להשתמש במפתח הפומבי לצורך הצפנת מפתחות ה-AES. עם זאת, לאחר מספר ימים גילו אנשי החברה ששוב כל מפתחות ה-AES התגלו. הסבר/י כיצד בוצעה ההתקפה.

ו. לאחר סדרת הכשלונות, הוחלט בחברה לפנות לעזרת חברת RSA-is-us. בחברת RSA-is-us, מייצרים מפתחות RSA בטוחים (p ו-q שניהם מספרים ראשונים בטוחים באורך 768 ביטים). מכיוון שחברת RSA-is-us מייצרת עשרות אלפי מפתחות RSA בכל רגע נתון, החליטו אנשי RSA-is-us להכין מראש רשימה בת 1,000,000 מספרים ראשונים בטוחים, ועבור כל משתמש (כמו חברת ASR), לבחור שני מספרים ראשוניים באופן אקראי מהרשימה, ולהשתמש בהם בתור p ו-q. e נבחר להיות מהצורה $2^{16}+1$. לאחר שהוכנס המפתח הפומבי החדש לשימוש בחברת ASR, שוב התגלו כל מפתחות ה-RSA. הסבר/י כיצד בוצעה ההתקפה.

שאלה 3 (30 נקודות)

בשאלה זו נדון בווריאנט לשיטת הזיהוי של פיאט-שמיר.
יהיו p מספר ראשוני גדול (באורך 768 ביטים) עבורו בעיית הלוגריתם הדיסקרטי היא קשה, ויהי $g \epsilon Z_p^*$ יוצר שני קבועים של המערכת הידועים לכל.
ההכנה לפרוטוקול: המוכיח בוחר באקראי $s \epsilon Z_p^*$ ומפרסם את $I \equiv g^s (\mathrm{mod}\, p)$.
הפרוטוקול מורכב מהצעדים הבאים:

1. המוכיח בוחר מספר אקראי $r \epsilon Z_p^*$.
2. המוכיח מחשב את $X \equiv g^r (\mathrm{mod}\, p)$ ושולח את X למוודא.
3. המוודא מבקש את r או את $r+s$ (mod p-1) (אבל לא את שניהם).
4. המוכיח שולח למוודא את המידע המבוקש.
5. המוודא בודק האם $X \equiv g^r (\mathrm{mod}\, p)$ או $IX \equiv g^{r+s} (\mathrm{mod}\, p)$ (בהתאם לבקשתו בשלב 3).

א. הראה/י כי הפרוטוקול הוא שלם (מוכיח שיודע את s יכול להצליח בביצוע הפרוטוקול). (3 נק')
ב. הראה/י כי הפרוטוקול הוא נאות (כלומר, מוכיח שאיננו יודע את s יכשל בהסתברות גבוהה דיה). לאחר t סיבובים של הפרוטוקול, מה הסיכוי שמוכיח שאיננו יודע את s, לא ייתפס? (5 נק')
ג. הוכח כי הפרוטוקול הוא אפס-ידע. (15 נק')
ד. עקב שגיאה במימוש יוצר המספרים האקראיים אצל המוכיח, בעת ריצת הפרוטוקול באיטרציה ה-i (עבור i=1,2,…,t) משמש r=ui (mod p-1), עבור $u \epsilon Z_p^*$ שהוא באמת אקראי. הראה כיצד המוודא יכול למצוא את s במקרה זה. כמה איטרציות של הפרוטוקול צריך המוודא כדי למצוא את s? (7 נק')

שאלה 4 (10 נקודות – כל מושג 2 נק')

נתונים חמישה מושגים בקריפטוגרפיה. לכל מושג, תאר/י בקצרה ובצורה תמציתית את המושג (עד כ-30 מילים למושג).

א. מרחק יחידות.
ב. פונקציית דחיסה קריפטוגרפית (cryptographic compression function).
ג. Message Authentication Code.
ד. התקפת Chosen Plaintext.
ה. סכמת שיתוף סוד.