

פרופ' בני פנקס

מבוא לקריפטוגרפיה 89-656-01

מועד ב'

סמסטר ב' תשע"א

הנחיות:

1. בטופס הבחינה שני דפים מלבד דף זה. ודאו כי כולם נמצאים בידכם.
2. בבחינה 4 שאלות.
3. הבחינה עם חומר פתוח.
4. משך הבחינה שתי שעות וחצי.
5. הנכם רשאים להסתמך על סעיפים קודמים, גם אם לא השבתם עליהם.
6. נמקו את כל תשובותיכם, פרט לפתרונות סעיפי שאלה 1. פתרון לשאלות 2-4 ללא הוכחה לא יתקבל.

בהצלחה

1. (24%) ענו על כל הסעיפים הבאים שלכולם משקל שווה. אין צורך לנמק את התשובות לשאלה זו.

א. (8%) חשבו את $8^{240,000,001} \bmod 35$.

ב. (8%) הסבירו בקצרה מדוע משתמשים ב-IV אקראי בהצפנה ב-CBC MODE. מה קורה אם משתמשים שם ב-IV קבוע?

ג. (8%) לפי פרדוקס היוםולדת (birthday paradox), הסיכוי שלשני ילדים בכיתה בת 40 ילדים יש יום הולדת באותו **החודש**:

- 1) לא רלוונטי, זה לא מקרה של ה-birthday paradox.
- 2) גדול מחצי החל מ-23 תלמידים.
- 3) גדול מחצי החל מ-4 תלמידים.
- 4) שווה לשורש מספר התלמידים.

2. (20%) הוצע לחזק את צופן Vigenere בצורה הבאה: מוצפנות הודעות $M = m_{n-1}, \dots, m_1, m_0$ הכתובות באלף-בית הלטיני (כאשר האותיות a, b, c, \dots, z ייוצגו ע"י המספרים $0, 1, 2, \dots, 25$). המפתח הוא מחרוזת $K = k_{|K|-1} \dots k_1 k_0$ באורך $|K|$. נחלק את ההודעה M לבלוקים באורך $|K|$ אותיות (הבלוק הראשון יהיה בלוק מספר 0, והאחרון בלוק מספר $n/|K|$). האות ה- i בבלוק ה- j תוצפן על ידי כך שנחבר לה (מודולו 26) את הערך $k_j + j$. (בצופן Vigenere המקורי חיברנו לאות זו את הערך k_j). לדוגמא, אם המפתח הוא $K=ab$ וההודעה היא $M=exam$ המוצפנת תהיה $C=eybo$.

- א. (8%) כיצד מתבצע פענוח במערכת הצפנה זו?
- ב. (12%) האם מערכת הצפנה זו היא בטוחה? אם כן, נמקו. אם לא, הציעו התקפה יעילה.

3. (25%) במערכת RSA המפתח הפומבי של אליס הוא (N, e_1) , והמפתח הפומבי של בוב הוא (N, e_2) , כאשר e_1 ו- e_2 זרים זה לזה (המודולוס N זהה עבור שני המשתמשים). אותה הודעה M הוצפנה בנפרד על ידי המפתחות הפומביים של אליס ושל בוב, והתקבלו הודעות מוצפנות C_1 ו- C_2 , בהתאמה. תוקף אשר יודע את שני המפתחות הפומביים מאזין לשתי הודעות מוצפנות אלו.

א. (5%) הראו כיצד התוקף יכול לחשב מספרים שלמים r, s כך שיתקיים $re_1 + se_2 = 1$.

ב. (10%) התוקף מחשב את $(C_2)^s \cdot (C_1)^r \bmod N$, כיצד מידע זה עוזר לו למצוא את M ?

ג. (10%) מכיוון ש- $e_1, e_2 > 0$, אחד מהערכים r ו- s חייב להיות שלילי. נניח שזהו s . כיצד ניתן לחשב את $(C_2)^s$ במקרה זה?

4. (31%) שאלה זו דנה במערכת להסכמה על מפתח לשיחת ועידה. שחקנים A_1, A_2, \dots, A_n, B רוצים להסכים על מפתח משותף שיהיה ידוע להם אך ישמר בסוד מפני כל מאזין. הם משתמשים במערכת הבאה:
- יהא p ראשוני ויהא g איבר מסדר q ב- Z_p^* , כאשר q הוא ראשוני גדול. המספרים p וגם q ידועים לכל השחקנים.
 - השחקן B בוחר באקראי מספר b ב- $\{1, \dots, q\}$ ומחשב את $y = g^b \pmod p$.
 - כל שחקן אחר A_i בוחר באקראי מספר a_i ב- $\{1, \dots, q\}$ ומחשב את $x_i = g^{a_i} \pmod p$.
 - השחקן A_i שולח את x_i ל- B ומקבל בחזרה את $z_i = (x_i)^b \pmod p$.
- א. (11%) הראו כי בהינתן z_i ו- a_i , השחקן A_i יכול לחשב את y .
- ב. (10%) הסבירו מדוע y יכול לשמש כמפתח שיחת הועידה. כלומר, הסבירו מדוע בסוף הפרוטוקול A_1, \dots, A_n, B יכולים לחשב את y , ומדוע (בצורה לא פורמלית) מאזין אינו יכול לחשב את y .
- ג. (10%) הוכיחו את הטענה הקודמת. כלומר, הניחו שישנו אלגוריתם יעיל E , שהקלט שלו מכיל את g ואת הערכים הפומביים שנשלחים בפרוטוקול, והפלט שלו הוא y . הראו שבמקרה זה ישנו אלגוריתם D שיכול לשבור את בעיית דיפי-הלמן החישובית (computational Diffie-Hellman problem). האלגוריתם D מקבל כקלט g, g^a ו- g^b מודולו p ואמור לחשב את g^{ab} . הוא יכול להשתמש באלגוריתם E כקופסא שחורה. ניתן להוכיח רק למיקרה של שני שחקנים, A_1 ו- B . (רמז: האלגוריתם D יכול לשנת את הקלט g שמקבל האלגוריתם E .)