אוניברסיטת בן-גוריון בנגב

המחלקה למדעי המחשב
דר׳ עמוסביימל

קריפטוגרפיה – מועד א׳
סמסטר ב׳ תש״ס

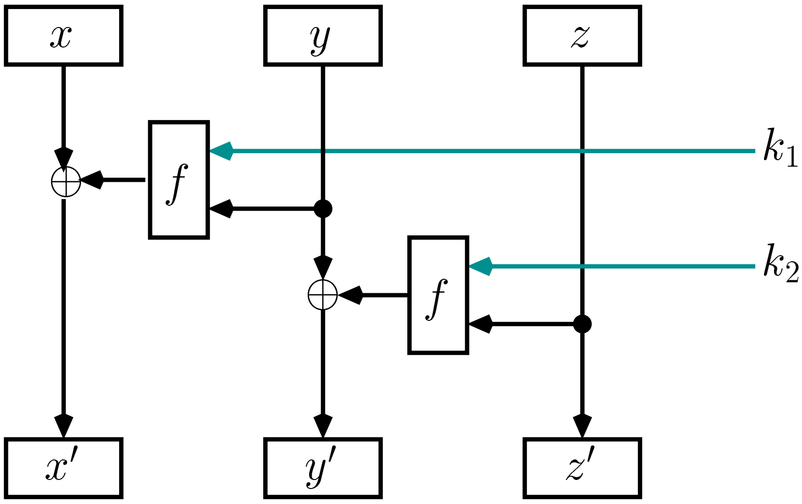
הנחיות:

1. בטופס הבחינה שלושה עמודים מלבד עמוד זה. ודאו כי כולם נמצאים בידכם.
2. בבחינה 4 שאלות שמשקלן אינו שווה. יש לענות על כולן.
3. הבחינה עם חומר פתוח.
4. נמקו את כל תשובותיכם. פתרון ללא הוכחה לא יתקבל.
5. משך הבחינה 3 שעות.
6. מומלץ לא להתקע זמן רב מדי על שום סעיף.
7. הנכם רשאים להסתמך על סעיפים קודמים, גם אם לא השבתם עליהם.

בהצלחה!

שאלה 1 (28 **נקודות**)

עיין ברשת:



הקלטים x, y, z הם מחרוזות בינאריות באורך n, והפעולות דומות לפעולות ב-DES.

סעיף 1 (10 **נקודות**)

נסמן ב-Π את הטרספורמציה המעתיקה את (x, y, z) ל-(x', y', z'). הוכיחו כי Π^4 היא טרספורמצית הזהות.

סעיף 2 (5 **נקודות**)

האם Π היא פרמוטציה? יש לנמק את התשובה.

סעיף 3 (3 **נקודות**)

נסמן ב-Θ את הטרספורמציה $\Theta(x, y, z) = (y, z, x)$. הוכח כי Θ^3 היא טרספורמצית הזהות.

סעיף 4 (10 **נקודות**)

בונים מערכת הצפנה ע"י $\Pi_3 \Theta \Pi_2 \Theta \Pi_1$, כאשר ב-$\Pi_j$ משתמשים במפתחות $k_{1,j}, k_{2,j}$. הראו כיצד לפענח הודעות במערכת זו.

שאלה 2 (28 **נקודות**)

סעיף 1 (14 **נקודות**)
יהי p ראשוני, g יוצר של $\mathcal{Z}_p^*$ ו-r מספר טבעי. נסמן $\alpha = \gcd(r, p-1)$. הוכיחו כי $x^r = 1 \pmod p$ אם ורק אם קיים j, כאשר $1 \le j \le \alpha$, כך ש-$x \equiv g^{\frac{p-1}{\alpha} \cdot j} \bmod p$.

סעיף 2 (14 **נקודות**)
יהי $N = p \cdot q$ עבור p, q ראשוניים. נקודת שבת של מפתח RSA ציבורי (N, e) היא הודעה $M \in \mathcal{Z}_N^*$ כך ש-$RSA(M, (N, e)) = M$. הוכיחו כי מספר נקודות השבת של (N, e) ב-$\mathcal{Z}_N^*$ הוא $\gcd(e-1, p-1) \cdot \gcd(e-1, q-1)$.

שאלה 3 (22 **נקודות**)

בשאלה זו נתאר מערכת חתימה.

- אלגוריתם יצירת המפתחות זהה לאלגוריתם יצירת המפתחות במערכת החתימה של *ElGamal*. כלומר, בוחרים p ראשוני, g יוצר של $\mathcal{Z}_p^*$ ו-$b \in \{1, \ldots, p-2\}$, ומחשבים $B \leftarrow g^b \bmod p$. מפתח החתימה הפרטי הוא (p, g, b) ומפתח הוידוא הציבורי הוא (p, g, B).
- תחום ההודעות הוא $\mathcal{Z}_{p-1}^*$.
- כדי לחתום על מסמך M מוצאים z כך ש-$z \cdot M \equiv b \pmod{p-1}$, והחתימה היא $S \leftarrow g^z \bmod p$.
- אלגוריתם הוידוא מכריז כי חתימה S היא חתימה חוקית על מסמך M אם ורק אם $S^M \equiv B \pmod p$.

תזכורת: חתימה היא חוקית אם אלגוריתם הוידוא מכריז כי חתימה זו חוקית.

סעיף 1 (11 **נקודות**)
הראו כי אלגוריתם הוידוא תקין, כלומר אם החתימה S חושבה ע"י אלגוריתם החתימה אזי החתימה חוקית.

סעיף 2 (11 **נקודות**)
מערכת חתימה זו אינה בטוחה. הראו כיצד זייפן יכול ליצר חתימה חוקית לכל הודעה $M \in \mathcal{Z}_{p-1}^*$.

שאלה 4 (22 **נקודות**)

סעיף 1 (11 **נקודות**)
נסתכל בסכמת חלוקת הסוד של שמיר כאשר $t = 2$, $n = 4$ ותחום הסודות הוא $\mathcal{Z}_5$. נתון כי החלק של מעבד 1 הוא 3 והחלק של מעבד 2 הוא 4. מהו הסוד s? מהו החלק של מעבד 4?

סעיף 2 (11 **נקודות**)
מחלק "רמאי" יכול לחלק חלקים "רעים" בסכמת חלוקת הסוד של שמיר, כלומר חלקים כך שקבוצות שונות בגודל t ישחזרו סודות שונים. בהנתן n חלקים ניתן לבדוק כי החלקים תקינים ע"י ידי שחזור הסוד לכל אחת מ-$\binom{n}{t}$ הקבוצות בגודל t ובדיקה שכל הסודות המשוחזרים זהים. אלגוריתם זה אינו יעיל כאשר t גדול. תארו אלגוריתם יעיל הבודק אם החלקים תקינים.