<u>מיקוד באלגוריתמים – תשפ״ב</u>

במסגרת מדעי המחשב

סמל השאלון: 899381

הנושאים שייכללו בחומר הלימוד לבחינה, לשנה״ל תשפ״ב בלבד, מסומנים ב- v

הנושאים שלא ייכללו בחומר הלימוד לבחינה, לשנה״ל תשפ״ב בלבד, מסומנים ב- X .

פרק	נושא	ייכלל	לא ייכלל
פרק 1	היכרות עם גרפים	v	
פרק 2	ייצוג של גרפים	v	
פרק 3	מסלולים קצרים ביותר ממקור יחיד ושיטת סריקה BFS	v	
פרק 4	מסלולים קצרים ביותר בגרף עם משקלות אי-שליליים- אלגוריתם של דייקסטרה.	v	
פרק 5	סריקה לעומק, רק״חים ו גרף על	v	
פרק 6	מיון טופולוגי		X
פרק 7	עץ פורש מינימלי		X
פרק 8	קידוד ודחיסת נתונים		X
פרק 9	הצפנה עם מפתח סימטרי	יכלל באופן חלקי (ראה מיקוד מדויק)	
פרק 10	מערכת הצפנה עם מפתח אסימטרי	יכלל באופן חלקי (ראה מיקוד מדויק)	
פרק 11	בניית אמון באמצעות מפתח פומבי (PKI) וחתימה דיגיטלית		X

<u>מיקוד חלופת אלגוריתמים בחלק של קריפטוגרפיה-</u> הנושאים שייכללו בחומר הלימוד לבחינה, לשנה"ל תשפ"ב בלבד

1. הצפנה עם מפתח סימטרי
   a. שימוש בפונקציית XOR
   b. פענוח הודעות המיוצגות בביטים ולבצע מעבר מביטים לאותיות באמצעות קוד ASCII
   c. פיתוח צופן OTP
   d. כתיבת אלגוריתם (פסאדו-קוד) עבור פונקציית PRG המבוססת על שיטת ***הריבוע האמצעי*** של ***ג'ון פון נוימן***
   e. אבחנה בין פונקציית PRG חלשה כמו LCG (לינארית בלבד ללא ראנדומליות) ולהדגים כיצד אפשר לשבור אותה.
   f. כתיבת צופן ערבול פשוט באמצעות PRG
2. מערכת הצפנה עם מפתח אסימטרי
   a. ההבדל בין מפתח ציבורי למפתח פרטי.
   b. תהליך יצירת המפתח הפרטי והציבורי ב RSA באמצעות עקרונות מתמטיים: פעולות כפל, חיבור, חיסור מעל שדה מודולרי, הרחבה בינארית, ריבוע עוקב, gcd, פונקצית פיי של אויילר, אוקלידס ואוקלידס המורחב.
   c. כתיבת משוואת הצפנת והפענוח RSA באמצעות המפתחות שיצרנו בסעיפים הקודמים
   d. RSA כ Trapdoor Function - הבנת הקשר בין המפחות (ציבורי ופרטי) לפנקציה חד כיוונית הפיכה. באמצעות המפתח הציבורי קל לחשב אותה, אך ללא המפתח הפרטי, קשה מאוד להפוך בחזרה.