מבחן דוגמה באלגוריתמים

שאלה בגרפים

בשאלה זו שלושה סעיפים, א-ג , שאין קשר בניהם. ענה על כולם.

א. נתון גרף $G = (V,E)$ **מכוון** , המיוצג על ידי מטריצת הסמיכויות שלפניך:

	a	***b***	***c***	***d***	***e***
a	*0*	*0*	*0*	*0*	*1*
b	*0*	*0*	*0*	*1*	*0*
c	*1*	*0*	*0*	*0*	*0*
d	*0*	*0*	*0*	*0*	*1*
e	*0*	*0*	*1*	*0*	*0*

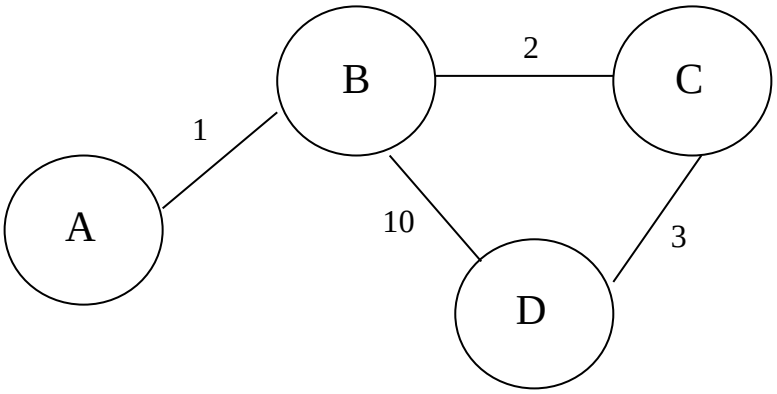
1. שרטט את הגרף G המיוצג על ידי מטריצת הסמיכויות.
2. מהו **המספר המינימלי** של קשתות שיש להוסיף לגרף הנתון כדי שהגרף יכיל רק"ח (Strong Connected Component) אחד בלבד? מהי הקשת או מהן הקשתות שיש להוסיף?

ב. נתון גרף $G = (V,E)$ **לא מכוון** המיוצג על ידי רשימת הסמיכויות הבאה:

a	→ c → b →‖
b	→a → c → d → e →‖
c	→ d → a → b → ‖
d	→ **c** → **b** → **e** →‖
e	→ b → d →‖

1. שרטט את הגרף G המיוצג על ידי רשימת הסמיכויות.
2. התבסס על הייצוג הנתון - רשימת הסמיכויות והפעל אלגוריתם סריקה לעומק (DFS) על הגרף G החל בקדקוד a . כמה קשתות סווגו כ"קשתות אחוריות" ומהן?

ג. נתון גרף קשיר לא מכוון $G=(V,E)$ וכן פונקציית משקל $w:E\to R^+$:



1. מצא את המסלולים הקצרים ביותר מקדקוד A לכל יתר הקדקודים בגרף הנתון ושרטט את עץ המסלולים הקצרים ביותר במשקל מקדקוד A לשאר קדקודי הגרף.
2. עתה נגדיר פונקציית משקל חדשה $c2:E\to R^+$ באופן הזה : $c2(e)=w(e)+a$ כאשר a הוא מספר כלשהו גדול מאפס.
   i. הבא דוגמה ל- a שבעבורו עץ המסלולים הקצרים ביותר מקדקוד A לשאר קדקודי הגרף <u>לא ישתנה</u>. נמק את תשובתך.
   ii. הבא דוגמה ל- a שבעבורו עץ המסלולים הקצרים ביותר מקדקוד A לשאר קדקודי הגרף <u>ישתנה</u>. נמק את תשובתך.

שאלה בקריפטוגרפיה

בשאלה זו שלושה סעיפים, א-ג . ענה על כולם. אין קשר בין סעיף ג' לבין הסעיפים א' – ב'.

סעיף א

הפוך את המחרוזת I Learn Computer Science למחרוזת/רצף של סיביות בינאריות (ביטים).

סעיף ב

נצור פנקס חד פעמי באורך 100 סיביות ונבצע xor עם הייצוג של המחרוזת מהסעיף הקודם, נשתמש באותו מקום בפנקס כדי לפענח את ההודעה.
כעת נשדר שוב ושוב את השדר בשימוש באותו פנקס חד פעמי. האם הצופן בטוח? אם כן, נמק. אם לא, כיצד ניתן לשבור את ההצפנה. נמק.

סעיף ג

תלמיד הציע לבנות מפתח סימטרי באמצעות שימוש ב xor, Alice שולחת מחרוזת רנדומית ל Bob. Bob מגריל מחרוזת רנדומית אחרת באותו האורך ומבצע xor bitwise, שולח את התוצאה ל Alice. Alice מבצעת שוב bitwise xor עם המחרוזת המקורית שהיא שלחה, ומקבלת את המחרוזת הרנדומית ש Bob הגריל. שניהם משתמשים במחרוזת זו כמפתח סימטרי.

1. מה הבעיה בפרוטוקול שהציע התלמיד?
2. כיצד תשנו את הפרוטוקול, כאשר הפעולות הבסיסיות האפשריות הן מהפעולות שבוצעו בפרוטוקול המקורי על מנת לקבל פרוטוקול בטוח ברמת האינפורמציה, בהנחה שהיריב לא מאזין לתקשורת אחת מכל k תקשורות רצופות?