

## אוניברסיטת חיפה - הפקולטה למדעי החברה - החוג למדעי המחשב

### שנתון תואר ראשון – שנה"ל תשפ"ב

תאריך עדכון 26.8.21 (יתכנו שינויים)

#### קורסי חובה

(בקורסים עם מספר קבוצות תרגיל/מעבדה יש לבחור רק אחת).

#### מבוא למדעי המחשב 203.1110

קדם: אין

מושגי יסוד: מבנה סכמטי של מחשב, שפות מחשב, מערכות הפעלה, שפת התכנות C (כולל מצביעים, מבנים, קבצים ורקורסיה). עקרונות בתכנון ותכנות, ניפוי שגיאות. שיטות אלגוריתמיות: בעיות בסיסיות, בעיות הדורשות מערכים, מיון חיפוש ומיזוג. מערכי אינדקסים, שיטות רקורסיביות, יעילות תכניות. קבצים, זיכרון דינמי, רשימות מקושרות, עצים.

סמסטר א':

שם הקורס	סוג	מרצה	שעות	נ"ז	זמנים
מבוא למדעי המחשב	שיעור	פרופ' שולי וינטנר	4	5	ב' 14-16 + ד' 8-10
	תרגיל 1	טרם נקבע	2	0	א' 16-18
	מעבדה 1	טרם נקבע	2	0	ב' 12-14
	תרגיל 2	טרם נקבע	2	0	ד' 14-16
	מעבדה 2	טרם נקבע	2	0	ד' 16-18
תרגיל 3	טרם נקבע	2	2	0	ה' 8-10
מעבדה 3	טרם נקבע	2	2	0	ה' 14-16

#### תכנות מונחה עצמים, 203.1120

קדם: מבוא למדעי המחשב 203.1110

מבוא לפרדיגמה של תכנות מונחה עצמים, הן מבחינה תיאורטית והן מבחינה מעשית. היכרות מעמיקה עם שפת התכנות ++C כדוגמה לפרדיגמה. נושאים: מבוא, מחלקות, הפשטת נתונים והחבאת מידע, הורשה, רב-צורתיות, העמסת יתר, תבניות, קלט-פלט, חריגים, שימוש בתבניות סטנדרטיות.

סמסטר ב':

שם הקורס	סוג	מרצה	שעות	נ"ז	זמנים
תכנות מונחה עצמים	שיעור	פרופ' דן פלדמן	3	4	א' 16-19
	תרגיל	טרם נקבע	2	0	1. ב' 14-16
					2. ד' 8-10

#### ארגון המחשב ושפות סף, 203.1130

קדם: מבוא למדעי המחשב 203.1110

מטרת הקורס היא להקנות לסטודנטים הבנה של ארכיטקטורת מחשבים (הממשק בין החומרה לתוכנה) וארגון המחשב לפי מודל המחשב של פון נוימן. לצורך לימוד עקרונות אלה, הקורס עושה שימוש בארכיטקטורת LC-3 אשר פותחה לצורך זה. בקורס נלמד לתכנת בשפת האסמבלי (סף) של ה-LC-3 כדי להבין כיצד מושגים של שפות תכנות עיליות (כגון C) מתורגמים לאסמבלי, וכמו כן נצלול לתיאור סכמטי של מימוש אפשרי של LC-3 כדי להבין כיצד פקודות אלה מיושמות בחומרה.

סמסטר א':

שם הקורס	סוג	מרצה	שעות	נ"ז	זמנים
ארגון המחשב ושפות סף	שיעור	מר אליאס ג'ידעון	2	3	ג' 8-10
	תרגיל	אור-אל שרה מרום	2	0	1. א' 16-18
					2. ה' 8-10

#### מבוא לחמרה, 203.1210

קדם: אין

אלגברה בוליאנית, פונקציות בוליאניות, שערים לוגיים, מעגלים, טבלאות אמת, נוסחאות, עצי הכרעה. מעגלים צרופיים, מרבב, מפענח, מחברים, שרון, מעגלי זיכרון, טבלת מעברים, בנית יחידות בקרה מורכבות. מבנה יחידת העיבוד המרכזית יחידה ארתימטית / לוגית, זיכרון מיקרו, פקודות מיקרו, שפת סף, זיכרון מטמון, Pipeline.

סמסטר א':

שם הקורס	סוג	מרצה	שעות	נ"ז	זמנים
מבוא לחמרה	שיעור	מר ארז גרליץ	4	5	א' + ד' 14-16
	תרגיל	רוז בדר	2	0	1. ב' 8-10
					2. ג' 18-20

### מערכות הפעלה, 203.2110

**קדמים:** תכנות מונחה עצמים 203.1120, מבני נתונים 203.2310, מבוא לחומרה 203.1210. תפקיד וארגון מערכת ההפעלה, תזמון, ניהול תהליכים ניהול זיכרון, תקשורת בין תהליכים. תסקר מערכת Unix מבחינת הנושאים לעיל. כמו כן, ילמדו הנושאים הקשורים לתזמון סינכרוני ואסינכרוני, מניעה הדדית, קיפאון, פסיקות.

**סמסטר ב':**

שם הקורס	סוג	מרצה	שעות	נ"ז	זמנים
מערכות הפעלה	שיעור	פרופ' רחל קולודני	4	5	א' 12-14 + ד' 08-10
	תרגיל	טרם נקבע	2	0	1. ב' 18-20
					2. ה' 16-18

### מבנה מהדרים, 203.2130

**קדם:** מבני נתונים 203.2310. אוטומט סופי, דקדוקים, ביטויים רגולריים, שפות פורמליות, אוטומט מחסנית, ההיררכיה של חומסקי. בניית אוטומט מחסנית מינימלי. ניתוח תחבירי עבור רכיבים שונים של שפת פסקל, עץ תחביר. בניית טבלת הסמלים ושימוש בפונקציית ערבול. יצירת קוד, כולל פרוצדורות וחוקי קינון. אופטימיזציה: הפצת קבועים הוצאת חישובים מלולאות.

**סמסטר א':**

שם הקורס	סוג	מרצה	שעות	נ"ז	זמנים
מבנה מהדרים	שיעור	פרופ' יוסי בן אשר	4	5	השיעור מתוקשב
	תרגיל	טרם נקבע	2	0	1. א' 8-10
					2. ג' 16-18
					3. ה', 18-20

### מבני נתונים, 203.2310

**קדמים:** מבוא למדעי המחשב 203.1110, מתמטיקה דיסקרטית 203.1850. הקורס יכסה מבני נתונים בסיסיים ומתקדמים תוך שימת דגש על תכנון יעיל מבחינת זמן ומקום, הוכחות נכונות ומימוש בשפת ++C. הגדרות של סיבוכיות זמן ומקום, מערכים ורשימות, עצים, עצים בינאריים, בעיית המילון: עצי חיפוש. ערבול, תור עדיפויות וערמות, קבוצות זרות, מבני נתונים לגרפים ושיטות מיון.

**סמסטר א':**

שם הקורס	סוג	מרצה	שעות	נ"ז	זמנים
מבני נתונים	שיעור	ד"ר גיא אבני	4	5	ב' 14-16 + ה' 12-14
	תרגיל	טרם נקבע	2	0	1. ג' 14-16
					2. ה' 14-16

**סמסטר ב':**

שם הקורס	סוג	מרצה	שעות	נ"ז	זמנים
מבני נתונים	שיעור	פרופ' מורן פלדמן	4	5	ג' 10-12 + ה' 12-14
	תרגיל	טרם נקבע	2	0	1. ב' 12-14
					2. ד', 14-16

### תכנון וניתוח אלגוריתמים, 203.2410

**קדם:** מבני נתונים 203.2310. הקורס יכלול אלגוריתמים דטרמיניסטיים לבעיות קלאסיות תוך שימת דגש על והוכחת נכונות וסיבוכיות. בעיית החציון, דוגמאות שונות של תכנון דינמי, אלגוריתמים לסריקה של גרפים, קשירות, מסלולים קצרים ביותר, עץ פורש מינימלי, זרימה ברשתות ושימושים לזרימה, משפט מנגר. פעולות אלגבריות בסיסיות, טרנספורם פורייה, הכפלת מטריצות, בעיות של מחרוזות.

**סמסטר א':**

שם הקורס	סוג	מרצה	שעות	נ"ז	זמנים
תכנון וניתוח אלגוריתמים	שיעור	פרופ' מורן פלדמן	4	5	ב' 16-18 + ה' 14-16
	תרגיל	טרם נקבע	2	0	1. א', 18-20
					2. ד', 16-18

**סמסטר ב':**

שם הקורס	סוג	מרצה	שעות	נ"ז	זמנים
תכנון וניתוח אלגוריתמים	שיעור	פרופ' אלק וינשטיין	4	5	א' 14-16 + ד' 16-18
	תרגיל	רוז בדר	2	0	1. ד' 12-14
					2. ה' 14-16

## שיטות הסתברותיות, 203.2480

**קדמים:** מבני נתונים 203.2310, חדו"א 203.1840, אלגברה לינארית 203.1810. קורס מבוא בו ילמדו מושגים בסיסיים בתורת ההסתברות ובסטטיסטיקה. יכוסו נושאים כגון: אקסיומות הסתברות, הסתברות מותנה, משתנים מקריים, תוחלת, שונות, מומנטים, התפלגויות בדידות, התפלגויות רציפות, התפלגות משותפת, נראות מקסימלית, משפט הגבול המרכזי, תורת האינפורמציה. הקורס יספק מוטיבציה מתחומים כמו למידה חישובית ויכלול תרגול מעשי, בנוסף לזה התאורטי.

**סמסטר א':**

שם הקורס	סוג	מרצה	שעות	נ"ז	זמנים
שיטות הסתברותיות	שיעור	ד"ר סיימון קורמן	4	5	ד' 8-12
	תרגיל	טרם נקבע	2	0	1. ב' 10-12
					2. ד' 18-20

**סמסטר ב':**

שם הקורס	סוג	מרצה	שעות	נ"ז	זמנים
שיטות הסתברותיות	שיעור	ד"ר אורי רבינוביץ	4	5	א' 10-12 + ג' 10-12
	תרגיל	טרם נקבע	2	0	1. א' 8-10
					2. ג' 14-16

## מבוא ללוגיקה, 203.2850

**קדם:** מתמטיקה דיסקרטית 203.1850. מושגי יסוד בתורת הקבוצות: קבוצות, יחסים, פונקציות, עוצמה, חשבון קרדינלים, משפט קנטור וקנטור-ברנשטיין. תחשיב הפסוקים, צורות נורמליות, הוכחה פורמלית, נאותות ושלמות של תחשיב הפסוקים. תחשיב הפרדיקטים מסדר ראשון (סמנטיקה ותחביר). משפט הדדוקציה, קומפקטיות.

**סמסטר ב':**

שם הקורס	סוג	מרצה	שעות	נ"ז	זמנים
מבוא ללוגיקה	שיעור	ד"ר אורן בן-צבי	2	3	ה' 08-10
	תרגיל	חאתם עדוי	2	0	1. ב' 8-10
					2. ג' 16-18
					3. ד' 18-20

## פרויקט חלק א', 203.3198 (סמס' א') + פרויקט חלק ב', 203.3199 (סמס' ב')

**קדם:** אין, פתוח לרישום לסטודנטים שנה ג'. הפרויקט הינו קורס בו אמור הסטודנט לרכוש מיומנות מקצועית באמצעות עבודה מעשית, כהמשך ללימודים התיאורטיים וכהכנה לעבודתו כבוגר. פרויקטים יוגדרו ויונחו ע"י חברי הסגל ועמיתי הוראה ויתבצעו בזוגות. יקבעו שעות פגישה שבועיות עם המנחה, תאריכי הצגות אמצע, הצגות סופיות והגשת דוחות מסכמים.

חובה להירשם לשני החלקים של הפרויקט (חלק א', 203.3198 ובסמסטר ב' חלק ב' 203.3199).  
3 נ"ז יינתנו אך ורק עם הרישום לשני החלקים.

**הערה:** הציון בפרויקט יעודכן רק אם ישנו רישום לפרויקט חלק א' + פרויקט חלק ב'

## מודלים חישוביים 203.3510

**קדם:** תכנון וניתוח אלגוריתמים 203.2410, **השלמת חובת אנגלית/פטור**, הגדרת בעיות החלטה כבעיית זיהוי שפות, אוטומטים ושפות רגולריות, מכונות טיורינג ואלגוריתמים. התיזה של צ'רץ, מכונה אוניברסלית, בעיות אי-כריעות. סיבוכיות זמן ומקום. מחלקת הבעיות הפולינומיאליות, דטרמיניזם, אי-דטרמיניזם ובעיות שלמות.

**סמסטר א':**

שם הקורס	סוג	מרצה	שעות	נ"ז	זמנים
מודלים חישוביים	שיעור	פרופ' נגה רון צבי	4	5	ב' 8-10 + ד' 16-18
	תרגיל	אילי עבוד	2	0	1. ב', 12-14
					2. ד', 12-14

**סמסטר ב':**

שם הקורס	סוג	מרצה	שעות	נ"ז	זמנים
מודלים חישוביים	שיעור	פרופ' רונן שאלתיאל	4	5	ב' 10-12 + ד' 14-16
	תרגיל	טרם נקבע	2	0	1. א', 14-16
					2. ה', 8-10

## מפגש חוגי חלק א' 203.3777 סמסטר א', חלק ב' 203.3778 סמסטר ב'

**חובה להירשם בזמן בניית מערכת !**

המפגש החוגי נועד לפעילויות השוטפות בחוג. אין להירשם בשעות הללו לקורסים בחוגים האחרים. הקורס מיועד רק לתלמידי החוג. נא לקרוא הנחיות מפורטות בדפי מידע.

שם הקורס	סוג	מרצה	שעות	נ"ז	זמנים
מפגש חוגי		מורי החוג	4	0	ג' 12-14 + ה' 10-12

## קורסי מתמטיקה

### אלגברה ליניארית, 203.1810

קדם: אין

מערכות משוואות ליניאריות: שיטת גאוס. ווקטורים ומטריצות, הופכי של מטריצה. שדות: מספרים מרוכבים, שדות סופיים. מרחבים וקטוריים: תת מרחב, צירוף לינארי, תלות ליניארית. בסיס ומימד. העתקות ליניאריות: גרעין ותמונה, ייצוג, פונקציונאלים לינאריים, המרחב הדואלי, דרגה. דטרמיננטות.

סמסטר א':

שם הקורס	סוג	מרצה	שעות	נ"ז	זמנים
אלגברה ליניארית	שיעור	מר אריאל אמסלם	4	5	ב' 16-18 + ד' 12-14
	תרגיל	יולי זעירא	2	0	1. ג' 16-18
					2. ה' 16-18

סמסטר ב':

הקורס בסמסטר ב' שייך לחוג למתמטיקה 210.1215

ניתן להירשם לקורס זה רק בתקופת השינויים של סמסטר ב'.

מספר המקומות מוגבל. הרישום יבוצע בפועל ע"י הסטודנט עצמו ולא ע"י החוג.

שם הקורס	סוג	מרצה	שעות	נ"ז	זמנים
אלגברה ליניארית	שיעור	פרופ' ולדימיר חניץ	4	5	ב' 16-18 + ד' 14-16
	תרגיל	טרם נקבע	2	0	ב' 18-20

### אלגברה ב', 203.1820

קדם: אלגברה ליניארית 203.1810

ניתן להירשם לקורס זה בסמסטר ב' או בסמסטר קיץ בלבד (פרטים לגבי סמסטר קיץ יפורסמו בהמשך)

ערכים עצמיים ווקטורים עצמיים של מטריצה, מטריצות לכסינות, פולינום אופייני ופולינום מינימאל, משפט פרוק ספקטראלי. רדיוס ספקטרי של מטריצה.

מכפלה פנימית ואורתוגונליות. דמיון אורתוגונלי. מטריצות סימטריות מוגדרות חיובי ואי-שלילית. משפט

SVD ופרוקים אחרים של מטריצות. PCA.

מבוא לתורת החבורות. חבורה סופית, תת-חבורה, משפט לגרנז', משפט פרמה, חבורה סימטרית.

מבוא לשדות סופיים: הרחבת שדה, שורשים של פולינום, אפיון של שדה.

סמסטר ב':

שם הקורס	סוג	מרצה	שעות	נ"ז	זמנים
אלגברה ב'	שיעור	מר אסלאם עכריה	4	5	ב' + ה' 16-18
	תרגיל	טרם נקבע	2	0	1. א' 8-10
					2. ה' 18-20

### חדו"א 1, 203.1830

קדם: אין

המספרים הממשיים, סדרות, פונקציות של משתנה ממשי יחיד, גבולות של פונקציה רציפות של פונקציות, נגזרת של פונקציה, המשפטים היסודיים של החדו"א (רול, לגרנז', פרמה, משפטי לופיטל, משפט טיילור), מבוא לטורי חזקות, חקירת פונקציה, אינטגרל בלתי מסוים, האינטגרל המסוים.

סמסטר א':

שם הקורס	סוג	מרצה	שעות	נ"ז	זמנים
חדו"א 1	שיעור	ד"ר עמי ויסלטר	4	5	א' 12-14 + ג' 10-12
	תרגיל	טרם נקבע	2	0	1. ב' 10-12
					2. ד' 10-12

סמסטר ב':

הקורס בסמסטר ב' שייך לחוג למתמטיקה 210.1115

מתכונת ותכני הקורסים שונים מהקורס הנלמד בחוג בסמסטר א'. המלצת החוג להירשם לקורסים של

החוג בלבד. הרישום והשלמת הקורס הנ"ל באחריות הסטודנט.

ניתן להירשם לקורס זה רק בתקופת השינויים של סמסטר ב'.

מספר המקומות מוגבל. הרישום יבוצע בפועל ע"י הסטודנט עצמו ולא ע"י החוג.

שם הקורס	סוג	מרצה	שעות	נ"ז	זמנים
חדו"א 1	שיעור	פרופ' פרול זפולסקי	4	5	א' 16-18+ד' 14-16
	תרגיל	טרם נקבע	2	0	ד' 12-14

## חדו"א 2, 203.1840

קדם: חדו"א 1 203.1830

### ניתן להירשם לקורס זה בסמסטר ב' או בסמסטר קיץ בלבד (פרטים לגבי סמסטר קיץ יפורסמו בהמשך)

האינטגרל הלא אמיתי. טורי מספרים. מבוא לגאומטריה של מרחבי  $R^n$ . גבולות ורציפות של פונקציות של כמה משתנים. חשבון דיפרנציאלי של פונקציות של כמה משתנים: נגזרות חלקיות וכיווניות, דיפרנציאביליות, כלל השרשרת, נגזרות מסדר גבוה, משפט טיילור, נקודות קיצון מקומיות וקמירות, נקודות קיצון בכפוף לאילוצים. חשבון אינטגרלי של פונקציות של כמה משתנים: הגדרת האינטגרל מעל תיבות, משפט פוביני, תחומי רימן ואינטגרציה מעליהם, שינוי משתנים באינטגרציה, אינטגרליים לא אמיתיים של פונקציות של כמה משתנים, אינטגרל של פונקציית הגאוסיאן.

סמסטר ב':

שם הקורס	סוג	מרצה	שעות	נ"ז	זמנים
חדו"א 2	שיעור	ד"ר עמי ויסלטר	4	5	ב' 8-10 + ד' 12-14
	תרגיל	טרם נקבע	2	0	1. א' 10-12
					2. ד' 16-18

## מתמטיקה דיסקרטית, 203.1850

קדם: אין

מבוא ללוגיקה. אינדוקציה מתמטית וכתובת הוכחות. מבוא לתורת הקבוצות. סכומים סופיים בסיסיים. משוואות הפרשים. מבוא לקומבינטוריקה: שיטת מניה, עקרון החבור והכפל, שובך היונים, הכללה והפרדה מושגים בסיסיים בתורת הגרפים.

סמסטר א':

שם הקורס	סוג	מרצה	שעות	נ"ז	זמנים
מתמטיקה דיסקרטית	שיעור	ד"ר אור מאיר	4	5	א' 8-12
	תרגיל	דפנה קופל	2	0	1. ג', 14-16
					2. ה', 12-14

סמסטר ב':

שם הקורס	סוג	מרצה	שעות	נ"ז	זמנים
מתמטיקה דיסקרטית	שיעור	ד"ר אור מאיר	4	5	ב' 10-14
	תרגיל	דפנה קופל	2	0	1. ג', 14-16
					2. ה', 8-10

## קורסי בחירה

### הנדסת תוכנה, 203.3140

קדם: תכנות מונחה עצמים 203.1120, מבני נתונים 203.2310

הכרת שיטות של הנדסת תוכנה בפיתוח מערכות עתירות תוכנה. הבנה ויישום של כלים לביצוע תהליך פיתוח מלא הכולל ניתוח והגדרת דרישות ותכן, אינטגרציה, בדיקות ותהליכים תומכים. לימוד ושימוש בשפת UML כשפה תקנית לתיאור מבנה ופעולת תוכנה.

סמסטר א':

שם הקורס	סוג	מרצה	שעות	נ"ז	זמנים
הנדסת תוכנה	שיעור	ד"ר מלכי גרוסמן	4	4	ג', 16-20
	תרגיל	ליאל פרידמן	2	0	ה', 8-10

סמסטר ב':

שם הקורס	סוג	מרצה	שעות	נ"ז	זמנים
הנדסת תוכנה	שיעור	ד"ר מלכי גרוסמן	4	4	ג', 16-20
	תרגיל	טרם נקבע	2	0	ג', 18-20

## לימוד ביג דטה בענן, 203.3284

קדמים: תכנון וניתוח אלגוריתמים 203.2410, שיטות הסתברותיות 203.2480

נלמד אלגוריתמי קירוב בעלי הוכחות על איכות תוצאה, זמני ריצה וזיכרון שמיועדים ללימוד מידע אינסופי שזורם לרשת מחשבים ("ענן") כדוגמת ציורים ב"טוויטר" או עדכונים ב"פייסבוק". האלגוריתמים יהיו מבוססים על רעיונות מרכזיים במספר תחומים כולל: אלגוריתמים הסתברותיים וגרסאות דטרמיניסטיות שלהם, אופטימיזציה מבוססת גיאומטריה חישובית, תורת האינפורמציה, עיבוד וניתוח אותות, שיטות דיגיטליות, הכפלה במטריצות סקאצ', סטטיסטי מספיק,  $vc$ -dimension, למידה סטטיסטית וככל שיינתן הזמן.

סמסטר א':

שם הקורס	סוג	מרצה	שעות	נ"ז	זמנים
לימוד ביג דטה בענן	שיעור	פרופ' דן פלדמן	4	4	ב' 8-10 + ד' 10-12

### מבוא לבינה מלאכותית, 203.3610

**קדמים:** חדו"א 2 203.1840, מתמטיקה דיסקרטית 203.1850, מבני נתונים 203.2310, תכנון וניתוח אלגוריתמים 203.2410  
מבוא: סוג הבעיות ושיטות הטיפול. שיטות היוריסטיות ומשחקים. הצגה ושימוש כללי בידע. הבנת שפות טבעיות ראיה הוכחות פורמליות בלוגיקה.  
**סמסטר א':**

שם הקורס	סוג	מרצה	שעות	נ"ז	זמנים
מבוא לבינה מלאכותית	שיעור	מר שי בושניסקי	4	4	ו', 10-14

### גרפיקה ממוחשבת, 203.3710

**קדמים:** תכנות מונחה עצמים 203.1120  
גרפיקה ממוחשבת היא תחום העוסק באחסון, עבוד ותצוגה של אובייקטים גיאומטריים. לגרפיקה יישומים רבים כגון, אנימציה ממוחשבת, משחקי מחשב, מציאות מדומה וכד'. מטרת הקורס היא להכיר את מושגי היסוד והשיטות הבסיסיות בגרפיקה.  
**סמסטר א':**

שם הקורס	סוג	מרצה	שעות	נ"ז	זמנים
גרפיקה ממוחשבת	שיעור	ד"ר רועי פורן	4	4	א', 16-20

### עיבוד תמונה, 203.3730

**קדמים:** תכנון וניתוח אלגוריתמים 203.2410, מתמטיקה דיסקרטית 203.1850, חדו"א 2 203.1840, חדו"א 1 203.1830, אלגברה ליניארית 203.1810, אלגברה ב' 203.1820  
קורס זה עוסק בניתוח והבנת תמונות. נלמד כלים קלאסיים ושימושיים בתחום. נושאים בקורס כוללים: רכישת תמונה, שיפור תמונה, ניתוח תמונה, ייצוגי תמונה (פרמידות), זיהוי שפות, סגמנטציה של תמונה, זיהוי תבניות בתמונה, וכן נושאים נבחרים בראיה ממוחשבת כגון זיהוי תנועה, תמונות תלת-מימד ועוד.  
**סמסטר א':**

שם הקורס	סוג	מרצה	שעות	נ"ז	זמנים
עיבוד תמונה	שיעור	פרופ' חגית הל-אור	4	4	ב'+ד' 14-16
	מעבדה		2	0	1. ב' 18-20
					2. ד' 18-20

### דחיסת תמונה וקול 203.3880

**קדמים:** מתמטיקה דיסקרטית 203.1850, חדו"א 1 203.1830, חדו"א 2 203.1840, אלגברה ליניארית 203.1810, אלגברה ב' 203.1820  
הקורס דן בקשת רחבה של שיטות לדחיסת תמונות, וידאו, דיבור וקול. דחיסת אותות מהסוגים הנזכרים נעשתה חשובה מאד בשנים האחרונות גם ל"צרכן הביתי" של מולטימדיה, בעקבות החיבור הנפוץ לאינטרנט ולאמצעי מולטימדיה ממוחשבים אחרים, כגון DVD, וידאו בטלפון סלולרי ועוד.  
למעשה, כל היישומים בהם מועבר מידע אודיו-וידאו מצריכים דחיסה ברמות שונות ובעקבות צורך זה נוצרה סדרה של תקנים בינלאומיים המותאמים לכל יישום. כ"כ, מיושמות טכניקות אלו ביישומים צבאיים, רפואיים ומסחריים אחרים בהם נדרש עיבוד אות בכלל (כולל דחיסה) ברמה גבוהה.  
תעשיית ההיי-טק בישראל היא מן המובילות בעולם בתחומים אלו, והדרישה בשוק למהנדסים ובוגרי מדעי המחשב המתמצאים בעיבוד אות היא גבוהה מאד.  
בקורס ישולבו לימוד תאורטי ומעשי, תוך שימוש בתכנת MATLAB וסביבות עבודה נוספות.  
**סמסטר א':**

שם הקורס	סוג	מרצה	שעות	נ"ז	זמנים
דחיסת תמונה וקול	שיעור	מר נמרוד פלג	3	3	ה', 16-19

## אלגוריתמי דינג, 203.3925

**קדמים:** תכנות מונחה עצמים 203.1120, שיטות הסתברותיות 203.2480  
אלגוריתמי דינג (מסחר אלגוריתמי) הינו תחום מולטידיסציפלינרי שבו עולם ההשקעות, כלכלה, ומדעי מחשב נפגשים. מסחר אלגוריתמי, מבוסס על שימוש בפלטפורמות מחשוב המשגרות פקודות קניה ומכירה לבורסה, המתקבלים באמצעות אלגוריתמים המריצים אסטרטגיות מסחר/השקעה. מסחר אלגוריתמי הינו תחום חדש יחסית שתוך עשור הפך לטכנולוגיה המניעה את השווקים הפיננסיים בעולם.  
בחלקו הראשון הקורס מקנה את היסודות והכלים להבנת המסחר האלקטרוני בשווקים פיננסיים. בחלקו השני, הקורס מתמקד בהקניית בסיס הידע התאורטי והעקרוני המנחים בתכנון ובניה של אסטרטגיות מסחר ומערכות מסחר אלגוריתמי.

הקורס משלב התנסות מעשית בבניית מערכת מסחר אלגוריתמי על מערכת מקצועית - TradeStation, ומקנה ידע וראיה רחבה של התחום המסחר האלגוריתמי, היכול להוות כרטיס כניסה לתחום ההייטק הפיננסי - Fintech, תחום מרתק הזוכה להתפתחות מואצת בשנים האחרונות הן בעולם וגם בארץ.

### סמסטר א':

שם הקורס	סוג	מרצה	שעות	נ"ז	זמנים
אלגוריתמי דינג	שיעור	מר ארי בן-אפרים	3	3	א', 09-12

## רשתות תקשורת, 203.3210

**קדמים:** שיטות הסתברותיות 203.2480  
קורס מבוא להקניית מושגי יסוד ברשתות תקשורת מחשבים. חשיבות הרשתות הולכת וגדלה כאשר בנוסף על היישומים הקלאסיים של העברת נתונים, הולכים ומתרבים יישומי העברת קול, תמונה ווידאו. נעסוק בהיבטים שונים: פרוטוקולי תקשורת מודל 7 השכבות, רשתות מקומיות, אזוריות ועולמיות, טכנולוגיית האינטרנט, ניהול רשתות, יישומים מתקדמים והתפתחות עתידית.

### סמסטר ב':

שם הקורס	סוג	מרצה	שעות	נ"ז	זמנים
רשתות תקשורת	שיעור	פרופ' אור דונקלמן	4	4	<b>הקורס מתקשב</b> שעת קבלה ביום ה' 12-13
	תרגיל	<b>טרם נקבע</b>	2	0	א' 8-10

## מעבדה בבינה מלאכותית, 203.3630

**קדם:** תכנון וניתוח אלגוריתמים 203.2410, מבוא לבינה מלאכותית 203.3610  
מסגרת המעבדה יועבר מבוא לבינה מלאכותית. הדגש במעבדה יושם על התנסות מעשית האלגוריתמיקה של הבינה המלאכותית. במסגרת המעבדה יתבצע חקר ביצועים של מימושים אלטרנטיביים של האלגוריתמיקה במגוון רחב של נושאים ובכללם: ייצוג ידע, תכנות לוגי, מימושים חליפיים לאלגוריתמי חיפוש, היוריסטיקת חיפוש, פונקציות הערכה, זיכרון אסוציאטיבי, חיפוש מקבילי או מבוזר, פתרון בעיות אופטימיזציה ולמידה חישובית. הקורס מיועד רק לתלמידי החוג.

### סמסטר ב':

שם הקורס	סוג	מרצה	שעות	נ"ז	זמנים
מעבדה בבינה מלאכותית	מעבדה	מר שי בושינסקי	4	4	ו' 10-14

## למידה עמוקה, 203.3834

**קדם:** תכנות מונחה עצמים 203.1120, תכנון וניתוח אלגוריתמים 203.2410, מבוא ללמידה ממוכנת 203.3770

הקורס יורכב מהרצאות בהן נלמד נושאים עיקריים בלמידה עמוקה ותרגול שיעסוק במימוש של רשתות ורכישת ניסיון בספריות ללמידה עמוקה Tensorflow ו-Theano. הקורס יתחיל במושגים ואלגוריתמים בסיסיים בפרט:

- stochastic gradient decent
- backpropagation
- loss function
- regularization וארכיטקטורות רדודות:
- feed-forward neural networks
- logistic regression
- auto-encoders
- convolutional neural networks (CNN) בהמשך נעסוק ברשתות יותר מורכבות:
- VGG, AlexNet, Residual Net, FaceNet, GoogleNet
- RNN, רשתות עמוקות לרצפים של נתונים
- LSTM generative deep networks
- visualization/deconvolution, adversarial networks, variational, auto-encoders
- אם הזמן יאפשר, נדון בלמידה עמוקה ממספר מועט של דוגמאות מתויגות: Transfer learning, One-shot learning, Deep Reinforcement Learning ונלמד על

**סמסטר ב':**

שם הקורס	סוג	מרצה	שעות	נ"ז	זמנים
למידה עמוקה	שיעור	פרופ' ריטה אוסדצי	3	4	ב', 9-12
	תרגיל	טרם נקבע	2	0	ג', 10-12

## מבוא לענן וביג דטה, 203.3840

**קדם:** תכנון וניתוח אלגוריתמים, 203.2410

קורס מבוא יעסוק בחיבור בין שני היבטים מרכזיים של עולם הביג דטה: אחסון ביג דטה ופלטפורמות ביג דטה לניתוח נתונים. במסגרת הקורס סטודנטים יחשפו לסקירה של מערכות ופתרונות העדכניים בעולם של ביג דטה, יילמדו חומר תאורתי ויעשו עבודות מעשיות הכוללות פיתוח קוד. נלמד שיטת Map Reduce לניתוח נתונים ונתמקד על Apache Spark אשר הפך להיות תחום התמחות הכי מבוקש בעולם. כמו כן נלמד על serverless computing ויחשפו לביג דטה. נלמד פתרונות אחסון של ביג דטה, מערכת קבצים מבוססת כגון HDFS, סוגי קבצים כמו Apache Parquet. נלמד על REST API, GraphQL ושימוש שלהם בתור פרוטוקול גישה לענן. נעסוק הרבה ב Cloud based Object Storage ונלמד מושגים רבים מהתחום, כגון replication, Metadata, consistency models, fault tolerance, data partition ונושאים רבים אחרים.

**סמסטר ב':**

שם הקורס	סוג	מרצה	שעות	נ"ז	זמנים
מבוא לענן וביג דטה	שיעור	ד"ר גיל ורניק	2	2	ג', 08-10

## ראייה ממוחשבת, 203.3702

**קדמים:** עיבוד תמונה 203.3730,

בקורס נעסוק בשיטות אלגוריתמיות לניתוח ולמידה מתוך תמונות. נכסה נושאים בסיסיים כמו: גאומטריה של מספר מצלמות, התאמת תמונות, סטריאו, זרימה אופטית, שחזור תלת-מימד, זיהוי אובייקטים, סיווג ואחזור תמונות. נכיר שיטות קלאסיות לפתרון בעיות אלו וכאלה המבוססות על למידה ממוכנת ועמוקה. דגש גדול יהיה על התנסות מעשית, בשימוש בפיתוח וספריות נלוות. רצוי ניסיון מוקדם כלשהו בפיתוח אם כי תיתכן הדרכה בסיסית והפנייה ללמידה עצמית

**סמסטר ב':**

שם הקורס	סוג	מרצה	שעות	נ"ז	זמנים
ראייה ממוחשבת	שיעור	ד"ר סיימון קורמן	4	4	ד' 12-16

## אימות פורמלי, 203.3223

**קדם:** מודלים חישוביים 203.3510

בקורס נלמד נושאים באימות פורמלי: אוטומטים מעל מילים אינסופיות, לוגיקה טמפורלית, משחקים על גרפים, שיטות להתמודדות עם בעית פיצוץ המצבים באימות פורמלי ונושאים נוספים. דרישות: מודלים חישוביים

**סמסטר ב':**

שם הקורס	סוג	מרצה	שעות	נ"ז	זמנים
אימות פורמלי	שיעור	ד"ר גיא אבני	4	3	ב' 12-14 + ד' 10-12



## מעבדה בראייה ממוחשבת, 203.3720

**\*\*מעבדה לא מחליפה פרויקט הנ"ז יחשב כקורסי בחירה במדעי המחשב**

**קדם:** עיבוד תמונה 203.3730

המעבדה תכלול פרויקטים ממגוון נושאים בראייה ממוחשבת, בדגש על הפעלת כלים של למידה עמוקה. כל פרויקט יכלול קריאה של מספר מאמרי רקע, מימוש והרחבה של רעיון מתוך מאמר עדכני שייבחר. ההערכה תתבצע על בסיס מספר פגישות לאורך הסמסטר והצגת הפרויקט במפגש סיום.  
**לא יתקיימו שיעורים קבוצתיים אלא מפגשים אישיים.**

**סמסטר קיץ:** (הרישום לקורסים של סמסטר קיץ יתקיים בתקופת השינויים של סמסטר ב')

שם הקורס	סוג	מרצה	שעות	נ"ז	זמנים
מעבדה בראייה ממוחשבת	שיעור	ד"ר סיימון קורמן	4	3	מפגשים אישיים

## מבני נתונים מתקדמים, 203.8006

**קדם:** תכנון וניתוח אלגוריתמים 203.2410

מודלים של מבני נתונים, ניתוח תחרותי, וניתוח לשיעורין. עצי חיפוש וקודם/עוקב, חיפושי טווח, מבני נתונים למספרים שלמים, מבני נתונים למחרוזות, מבני נתונים המאזנים את עצמם, ערבול מושלם, גרפים דינמיים.

**סמסטר קיץ:** (הרישום לקורסים של סמסטר קיץ יתקיים בתקופת השינויים של סמסטר ב')

שם הקורס	סוג	מרצה	שעות	נ"ז	זמנים
מבני נתונים מתקדמים	שיעור	פרופ' אורן וימן	4	3	טרם נקבע

## סמינרים לתואר ראשון

### ניטור במערכות מבוזרות - סמינר, 203.3156

**קדם:** תכנון וניתוח אלגוריתמים 203.2410, חדו"א 2 203.1840, אלגברה ב' 203.1820, **השלמת חובת אנגלית/פטור**

הסמינר יתמקד בניטור וזיהוי תופעות גלובליות במערכות מבוזרות דינמיות. המטרה היא לזהות במהירות ובמינימום תקשורת "טרנדים" גלובליים או "שינויי פאזה" במערכות כאילו. הנושאים המרכזיים יהיו sketches, slack distribution, וניטור בעזרת שיטות גיאומטריות. הסמינר יכסה שיטות ושימושים שונים, כגון ניטור ברשתות חישניים וזיהוי של התקפות "DDOS". מרבית הטכניקות שילמדו מבוססות על אלגוריתמים וכלים הסתברותיים וגיאומטריים.

**סמסטר א':**

שם הקורס	סוג	מרצה	שעות	נ"ז	זמנים
סמינר בניטור מערכות מבוזרות	סמינר	פרופ' דניאל קרן	2	2	א', 12-14

### סמינר בתורת הרשתות, 203.3214 – חדש!

**קדם:** תכנון וניתוח אלגוריתמים 203.2410, מטרת הסמינר היא לבחון ולהכיר את תורת הרשתות מהממד המתמטי, אלגוריתמי שלה. נמדל רשת כגרף ונבחן את תכונותיו עבור רשתות מסוימות. מרכזיות של צומת ברשת, הגדרות ואלגוריתמים למציאת צומת מרכזי. פרדוקס החברויות ושימושו בבעיית המרכזיות. מודלים דינמיים להתפשטות מידע ברשת ואלגוריתמים. הצבעות רוב מקומי ורשתי (local-global). טופולוגיה של רשתות חברתיות. דגימה ב-ויצירה של-רשתות חברתיות.

#### סמסטר א':

שם הקורס	סוג	מרצה	שעות	נ"ז	זמנים
סמינר בתורת הרשתות	סמינר	ד"ר אורן בן צבי	2	2	ה', 8-10

### אופטימיזציה קומבינטורית מופשטת - סמינר, 203.3443

**קדם:** תכנון וניתוח אלגוריתמים 203.2410, שיטות הסתברותיות 203.2480, **השלמת חובת אנגלית/פטור** אופטימיזציה קומבינטורית עוסקת בפתרון בעיות אופטימיזציה בדידות (כלומר, בעיות שיש להן מספר סופי של פתרונות אפשריים). ניתן לחקור בעיות מוחשיות מסוג זה (כדוגמת הבעיות הנלמדות בקורס "תכנון וניתוח אלגוריתמים"), או בעיות מופשטות המספקות מסגרת כללית המאפשרת למצוא פתרון אחיד למשפחה רחבה של בעיות מוחשיות. בסמינר זה נעסוק בבעיות מהסוג האחרון, וביניהן בעיות עם פונקציית מטרה תת-מודולרית ואו אילוצי מטראידי. מרבית העיסוק יהיה במחקר התיאורטי של בעיות אלה, אך נעסוק מעט גם ביישומים שלהן (בעיקר בתחום למידת המכונה).

דרישות הקורס: כל משתתף או זוג, יעביר הרצאה במהלך הסמסטר.

#### סמסטר א':

שם הקורס	סוג	מרצה	שעות	נ"ז	זמנים
אופטימיזציה קומבינטורית מופשטת - סמינר	סמינר	פרופ' מורן פלדמן	2	2	ג', 10-12

### סמינר באלגוריתמים מקוונים, 203.3421

**קדם:** תכנון וניתוח אלגוריתמים 203.2410, שיטות הסתברותיות 203.2480, **השלמת חובת אנגלית/פטור** סמינר זה יעסוק באלגוריתמים תיאורטיים לקבלת החלטות בסביבות של חוסר וודאות. במסגרת זאת נעסוק באלגוריתמים מקוונים (online algorithms) ואלגוריתמים לאופטימיזציה סטוכסטית. ניגע מעט גם בנושא של אלגוריתמי הזרמה (streaming algorithms) שקרוב מבחינה טכנית לשאר נושאי הסמינר, למרות שהמוטיבציה לו היינה בנתוני עתק (Big Data) ולא בחוסר וודאות. כל סטודנט ידרש לקרוא מאמר מתוך רשימה שתינתן בתחילת הסמסטר, ולהציג אותו לשאר הקבוצה. תהיה גם חובת נוכחות ב-80% ממפגשי הסמינר.

**סמסטר ב':**

שם הקורס	סוג	מרצה	שעות	נ"ז	זמנים
סמינר באלגוריתמים מקוונים	סמינר	פרופ' מורן פלדמן	2	2	א', 10-12

### סמינר בתורת המשחקים, 203.3675

**קדם:** מודלים חישוביים 203.3510, **השלמת חובת אנגלית/פטור** הסמינר יסקור נושאים בתורת המשחקים ובעיקר משחקים שרלוונטיים למדעי המחשב: משחקי סכום אפס ומשפט ה-minmax, משחקים כלליים ושיווי משקל נאש, נושאים בגבול כלכלה וחישוב: מכרזים, משחקי רשתות זרימה, ועוד.

**סמסטר ב':**

שם הקורס	סוג	מרצה	שעות	נ"ז	זמנים
סמינר בתורת המשחקים	סמינר	ד"ר גיא אבני	2	2	ב', 10-12

### עיבוד תמונה מתקדם, 203.3775

**קדם:** עיבוד תמונה 203.3730 (בציון 85 ומעלה) **השלמת חובת אנגלית/פטור** סמינר בנושא מתקדם בעיבוד תמונה וראייה ממוחשבת. נושאים לדוגמה: זיהוי אובייקטים, תנועה, תלת מימד, למידה ממוכנת בראייה ממוחשבת ועוד. לסמינר זה יתקבלו אך ורק סטודנטים אשר סיימו את הקורס: "עיבוד תמונה" בציון 85 ומעלה. לסטודנטים אשר לא יעמדו בדרישה הרישום לסמינר יבוטל בתקופת השינויים של סמסטר ב'. סטודנט שנרשם בסמסטר א' תשי"פ לקורס עיבוד תמונה יהיה תקף רק למועדי בחינות א + ב.

**הקבלה לסמינר אינה אוטומטית, יש לשלוח מייל בקשה לרישום לפרופ' חגית הל אור**

**עד לתאריך 28.9.21 [hagit@cs.haifa.ac.il](mailto:hagit@cs.haifa.ac.il)**

**סמסטר ב':**

שם הקורס	סוג	מרצה	שעות	נ"ז	זמנים
סמינר בעיבוד תמונה מתקדם	סמינר	פרופ' חגית הל-אור	2	2	ב', 16-18

### שיכון גרפים במישור, 203.3595

- קדם:** תכנון וניתוח אלגוריתמים 203.2410, **השלמת חובת אנגלית/פטור**
1. מבוא: גרפים מישוריים, מכשולים למישוריות, משפט קוראטובסקי, אלגוריתמים נאיביים.
  2. חיפוש בעומק ואלגוריתם של הופקרופט וטרגין.
  3. מספור-st ואלגוריתמים מבוססים עליו.
  4. עצי-PQ ושימושיהם.
  5. עצי-טרמו ושימושיהם.
  6. ניתוח השוואתי של אלגוריתמי שיכון.

**סמסטר ב':**

שם הקורס	סוג	מרצה	שעות	נ"ז	זמנים
שיכון גרפים במישור	סמינר	פרופ' אלק וינשטיין	2	2	ד', 18-20

### נושאים מתקדמים בעיבוד תמונה, 203.3755 (סמינר מתואר שני פתוח גם לתואר ראשון)

**קדם:** עיבוד תמונה 203.3730, **השלמת חובת אנגלית/פטור**

סמינר בנושא מתקדם בעיבוד תמונה וראייה ממוחשבת. נושא הקורס יבחר לקשור בין ראייה ממוחשבת ולמידה ממוכנת.

לסמינר זה יתקבלו אך ורק סטודנטים אשר סיימו את הקורס: "עיבוד תמונה" בציון 85 ומעלה. סטודנטים אשר לא עמדו בדרישה הרישום לסמינר יבוטל. הקבלה לקורס זה אינה אוטומטית, יש לשלוח מייל בקשה לרישום לפרופ' חגית הל אור [hagit@cs.haifa.ac.il](mailto:hagit@cs.haifa.ac.il) עד לתאריך 11.9.21.

**סמסטר א':**

שם הקורס	סוג	מרצה	שעות	נ"ז	זמנים
נושאים מתקדמים בעיבוד תמונה	סמינר	פרופ' חגית הל-אור	2	2	ב' 16-18

### סמינר בחישוב בטוח רב משתתפים, 203.3335 (סמינר מתואר שני פתוח גם לתואר ראשון)

**קדם:** תכנון וניתוח אלגוריתמים 203.2410, מודלים חישוביים 203.3510, **השלמת חובת אנגלית/פטור**

חברות מסחריות כגון, אמזון, גוגל, ופייסבוק מחזיקות מידע מסחרי סודי אותו הן מסתירות מפני מתחריהן. האם הן יכולות לבצע כריית נתונים על אוסף הנתונים הגדול של כלל המידע שלהן, אך מבלי לחשוף זו לזו את המידע הסודי? התשובה היא כן: הטכנולוגיה של חישוב בטוח רב משתתפים -- נושא סמינר זה – מאפשרת לשניים או יותר משתתפים לחשב יחדיו פונקציה שהקלט עבורה הוא סך כל הקלטים הפרטיים שלהם, אך מבלי לחשוף זה לזה שום מידע על הקלטים הללו (מעבר למה שניתן להסיק מתוצאת החישוב). תלמידי הסמינר יתוודעו לפרוטוקולים, הגדרות, מימושים וניתוחים שמהווים את הבסיס לחישוב בטוח רב משתתפים.

**סמסטר ב':**

שם הקורס	סוג	מרצה	שעות	נ"ז	זמנים
סמינר בחישוב בטוח רב משתתפים	סמינר	ד"ר עדי עקביה	2	2	ג', 16-18

### סמינר בנושא סיבוכיות עדינה, 203.3411

**קדם:** מודלים חישוביים 203.3510

סמינר זה עוסק בבעיות שמסורתית במדעי המחשב נחשבו ל"קלות", כלומר בעלות אלגוריתמים פולינומיאליים. האלגוריתמים המהירים ביותר הידועים לבעיות קלות רבות הם בעלי זמן ריצה גבוה ולרוב לא פרקטיים לשימוש בפועל. שיפור זמני הריצה הוא בעיה פתוחה ארוכת שנים, עם התקדמות מועטה בלבד. לפיכך, מתקבל על הדעת כי האלגוריתמים הללו הם מיטביים. עם זאת, פיתוח חסמים תחתונים נראה כמעט בלתי אפשרי בטכניקות הקיימות. הסמינר עוסק בתיאוריה חדשה שפותחה לאחרונה ובה מוכיחים קושי של בעיות בהסתמך על מספר השערות מתקבלות על הדעת. בסמינר נראה רדוקציות מעניינות (בין בעיות לכאורה שונות מאוד) שמראות שהסיבה לכך שקשה היה לשפר את האלגוריתמים הידועים היא זהה (למרות שזמני הריצה שלהם יכולים להיות שונים מאוד).

**סמסטר קיץ: (הרישום לקורסים של סמסטר קיץ יתקיים בתקופת השינויים של סמסטר ב')**

שם הקורס	סוג	מרצה	שעות	נ"ז	זמנים
סמינר בנושא סיבוכיות עדינה	סמינר	פרופ' אורן וימן	2	2	טרם נקבע

### סמינר בנושאים מתקדמים בראייה ממוחשבת, 203.3765

**קדם:** עיבוד תמונה 203.3730

סילבוס מתקדם בראייה ממוחשבת, שבו נסקור מאמרים עדכניים במגוון נושאים, עם דגש על שימוש בכלים של למידה עמוקה לפתרון בעיות של התאמה בין תמונות, שחזור תלת-ממד וגיאומטריה של מצלמות.

**סמסטר קיץ: (הרישום לקורסים של סמסטר קיץ יתקיים בתקופת השינויים של סמסטר ב')**

שם הקורס	סוג	מרצה	שעות	נ"ז	זמנים
סמינר בנושאים מתקדמים בראייה ממוחשבת	סמינר	ד"ר סיימון קורמן	2	2	טרם נקבע

## קורסי בחירה מתואר שני (פתוחים לסטודנטים בתואר ראשון)

### אבטחת מחשבים ורשתות, 203.3448

קדם: מע' הפעלה 203.2110

עקרונות בסיס באבטחת מערכות מחשב. סוגי איומים על מערכות מחשב: וירוסים, תולעים וקוד עיון, שיטות התמודדות עם איומים, מבוא לקריפטוגרפיה, תשתית מפתחות פומביים, פרוטוקולי זיהוי משתמש, איומים על תקשורת מחשבים, חומות אש, פרוטוקולי תקשורת מאובטחים, יצירת VPN-ים מאובטחים.

סמסטר א':

שם הקורס	סוג	מרצה	שעות	נ"ז	זמנים
אבטחת מחשבים ורשתות	שיעור + תרגול	פרופ' אור דונקלמן	4	4	א' 14-16+ה' 12-14

### סיבוכיות תקשורת, 203.3574

קדם: שיטות הסתברותיות 203.2480, מודלים חישוביים 203.3510

סיבוכיות תקשורת היא תחום תיאורטי העוסק בשאלה הבאה: נניח שיש לנו שני מחשבים או יותר, שלכל אחד מהם יש מידע שאין לאחרים. הם רוצים לבצע חישוב מסוים ביחד. כמה ביטים הם יצטרכו לשדר אחד לשני כדי לבצע את החישוב? בקורס נראה חסמים עליונים ותחתונים על כמות התקשורת הנדרשת, ויישומים של החסמים האלה לניתוח הסיבוכיות של אלגוריתמים. אנו נוכיח את החסמים באופן מתמטי, בעזרת שיטות מקומבינטוריקה, הסתברות ואלגברה.

סמסטר א':

שם הקורס	סוג	מרצה	שעות	נ"ז	זמנים
סיבוכיות תקשורת	שיעור	ד"ר אור מאיר	3	3	א', 13-16

### עיבוד שפות טבעיות, 203.3670

קדם: מבוא ללמידה ממוכנת 203.3770

קורס זה מקנה הכרות ראשונית אך מעמיקה עם גישות מודרניות לעיבוד ממוחשב של שפות טבעיות. הקורס מציג את האלגוריתמים העיקריים המשמשים לעיבוד שפות, כמו גם את התכונות החשובות של שפות טבעיות. הקורס מתמקד בגישות סטטיסטיות אמפיריות: שימוש בקורפוסים של טקסט, מודלים הסתברותיים ואלגוריתמים יציבים וסקלביליים ליישומים אמתיים. בין הנושאים שייסקרו: מודל שפה, מודל מרקוב חבוי, תיוג חלקי דיבר, הפגת עמימות ברמת המילה, אחזור מידע, סיווג טקסטים, ניתוח תחבירי סטוכסטי, ותרגום אוטומטי סטטיסטי.

סמסטר ב':

שם הקורס	סוג	מרצה	שעות	נ"ז	זמנים
עיבוד שפות טבעיות	שיעור	פרופ' שולי וינטנר	3	3	מתוקשב

### מעבדה בגרפיקה ממוחשבת, 203.3704

קדם: אין

גרפיקה ממוחשבת היא תחום נרחב ביותר המכיל בתוכו מגוון של בעיות ואפליקציות שונות. במסגרת המעבדה הסטודנטים יעבדו על פרויקט בתחום גרעיני בגרפיקה הממוחשבת, אנימציה, סימולציה פיזיקלית, ייצור חישובי או משחק מחשב.

לצורך בחירת נושא, יש לתאם פגישה עם המרצה. מבחר נושאים יוצעו בתחילת הסמסטר. שימו לב: לפחות 50% מהפרויקט חייב להיות ממומש לפני סוף הסמסטר. לא ניתן להתחיל את הפרויקט לאחר סוף סמסטר.

\*לא יתקיימו שיעורים קבוצתיים אלא מפגשים אישיים. לתיאום מפגש נא לפנות במייל לד"ר רועי פורן

[roiporanne@cs.haifa.ac.il](mailto:roiporanne@cs.haifa.ac.il)

סמסטר א' או סמסטר ב':

שם הקורס	סוג	מרצה	שעות	נ"ז	זמנים
מעבדה בגרפיקה ממוחשבת	מעבדה – מחליפה פרויקט	ד"ר רועי פורן	3	3	מפגשים אישיים

### מבוא ללמידה ממוכנת, 203.3770

**קדמים:** שיטות הסתברותיות 203.2480, חדו"א 2 203.1840, אלגברה ליניארית 203.1810, אלגברה ב' 203.1820

המטרה של למידה ממוכנת היא לבנות מערכות המסוגלות ללמוד לפתור בעיות כאשר נתונה קבוצה של דוגמאות מייצגות ואיזשהו מידע מוקדם על הבעיות הללו. האפליקציות של למידה ממוכנת כוללות סיווג תמונות, זיהוי דיבור, זיהוי כתב יד, information retrieval, וכיוצא בזה. המטרה של הקורס היא להכיר עקרונות של למידה ממוכנת, לרבות אספקטים תיאורטיים כגון תכונות הכללה (איך המודל יעבוד על דוגמאות חדשות) ואספקטים מעשיים כגון מודלים סטטיים ודינאמיים חדשניים לסיווג, רגרסיה והערכת פילוגים. בקורס נראה אפליקציות לבעיות אמיתיות על מנת להדגים שימושים של למידה ממוכנת. הנושאים כוללים: שיטות באסיאניות, פרמטריות ואי-פרמטריות, רגרסיה ליניארית, בחירת מודל, תאמה יתרה, חסמים על שגיאות, שיטות רגולריזציה, דיסקרימינציה ליניארית, עצי החלטות, רשתות עצביות רב שכבתיות ואלגוריתמי אופטימיזציה, אלגוריתמי קבוץ PAC, SVM, (k-means), הפחתת מימדיות מידע PCA, בחירת מאפיינים, Boosting.

**סמסטר א':**

שם הקורס	סוג	מרצה	שעות	נ"ז	זמנים
מבוא ללמידה ממוכנת	שיעור מעבדה	פרופ' ריטה אוסדצי	3	3	ג' 09-12
		<b>טרם נקבע</b>	2	0	ד' 18-20

**סמסטר ב':**

שם הקורס	סוג	מרצה	שעות	נ"ז	זמנים
מבוא ללמידה ממוכנת	שיעור מעבדה	ד"ר דן רוזנבאום	3	3	ה' 14-17
		<b>טרם נקבע</b>	2	0	ב' 8-10

### מעבדה בחישוב בטוח בענן 203.3850

**קדם:** תכנון וניתוח אלגוריתמים 203.2410

אחסון מידע וביצוע חישוב עליו הופכים בשנים האחרונות למוצר צריכה, עם מגמה מתגברת של ארגונים ויחידים לביצוע מיקור חוץ (אאוטסורסינג) של פעולות החישוב והאחסון אל גורם שלישי המכונה לרוב "הענן". כאשר הדוא"ל שלנו, המסמכים הרפואיים, המידע הפיננסי ועוד עוברים לאחסון בענן, חיוני להבטיח את פרטיות המידע בנוסף לזמינות המידע ונכונות החישוב עליו. בנוסף, חובה לספק כל זאת ביעילות מרבית לאור השכיחות הגבוהה של משימות מרובות מידע ("ביג דאטא"). צרכי ההצפנה שלנו משתנים בהתאם עם דרישה למערכות אשר מבטיחות בו-זמנית יעילות גבוהה, בטיחות גבוהה, ופונקציונליות גבוהה. תורת ההצפנה מציעה מספר גישות לביצוע חישוב פרטי בענן ובמרכזן: חישוב בטוח רב משתתפים (Secure Multi-Party Computation), וחישוב על מידע מוצפן בעזרת Fully homomorphic encryption ו-functional encryption. תלמידי המעבדה ייחשפו למגוון שיטות אלו תוך דיון בכיתה על הספרות המקצועית הרלוונטית ועבודה מעשית בבית בפרויקט פיתוח פתרונות חישוב בטוח.

\*לא יתקיימו שיעורים קבוצתיים אלא מפגשים אישיים. לתיאום מפגש נא לפנות במייל לד"ר עדי עקביה

**סמסטר א':**

שם הקורס	סוג	מרצה	שעות	נ"ז	זמנים
מעבדה בחישוב בטוח בענן	מעבדה (מחליפה פרויקט)	ד"ר עדי עקביה	3	3	מפגשים אישיים

### חישוב בטוח רב משתתפים, 203.3861

**קדם:** תכנות מונחה עצמים, 203.1120, שיטות הסתברותיות 203.2480, מבני נתונים 203.2310

חישוב בטוח רב משתתפים (MPC) הוא כלי מרכזי בתורת ההצפנה המודרנית. MPC מאפשר לשניים או יותר משתתפים, כל אחד עם קלט פרטי משלו, לחשב פונקציה של כלל הקלטים תוך שמירה על פרטיות הקלטים. לחישוב בטוח יש שימושים בתחומים מגוונים, כגון: הצבעה אלקטרונית, מכרזים אלקטרוניים, כסף דיגיטלי, טרנסאקציות אנונימיות, גישה וחיפוש פרטי במאגרי מידע, מיקור חוץ פרטי של חישוב על מידע רגיש. הדרישות מחישוב בטוח כוללות בין השאר: נכונות, פרטיות, ויעילות. בקורס ילמדו טכניקות מפתח של MPC, וביניהן:

Yao, GMW, BGW, OT, OTE, FHE, Secret Sharing, FSS, ZK proofs, PIR, ORAM, IPS compiler, "MPC in the head", PSI constructions, ABY approach, SPDZ, and TinyO.

**סמסטר א':**

שם הקורס	סוג	מרצה	שעות	נ"ז	זמנים
חישוב בטוח רב משתתפים	שיעור	ד"ר עדי עקביה	3	3	ג', 14-17

### מעבדה ברובטיקה מתקדמת, 203.3277

**קדם:** מודלים חישוביים 203.3510, תכנון וניתוח אלגוריתמים 203.2410, חדו"א 203.1840, אלגברה ב' 203.1820

נצא מהמסך של המחשב כדי לתכנת עצמים בעולם האמיתי כמו משקפיים, רובטים, "קוראי מחשבות" (EEG). לאחר מכן נלמד איך ללמוד ולעבד את המידע העצום בזמן אמת בעזרת אלגוריתמים מקבליים ו-Streaming שרצים על ענן מחשב.  
המעבדה תכלול סקירה של המודל החישובי החדש: חומרה, תוכנה, ואלגוריתמים.

מס' המקומות למעבדה זו הנו מוגבל. הקבלה למעבדה כרוכה בעמידה בתנאים הבאים (עמידה בתנאים 1-2 אינה מבטיחה קבלה למעבדה):

1. ציון של 75 לפחות בקורסי הקדם.
2. ממוצע ציונים בתו"ל של 85 לפחות
3. ראיון אישי עם פרופ' דן פלדמן

סטודנטים המעוניינים להירשם למעבדה מתבקשים לשלוח קורות חיים ותדפיס ציונים עדכני לאמיר בר און עד לתאריך 28.9.21, [AmBarOn@univ.haifa.ac.il](mailto:AmBarOn@univ.haifa.ac.il), יש לציין בנושא המייל: רובטיקה מתקדמת.

**סמסטר ב':**

שם הקורס	סוג	מרצה	שעות	נ"ז	זמנים
רובטיקה מתקדמת	מעבדה מחליפה פרויקט	פרופ' דן פלדמן	3	3	מפגשים אישיים

### מבוא לקריפטוגרפיה, 203.3444

**קדם:** מודלים חישוביים 203.3510

קריפטוגרפיה קלאסית, קריפטוגרפיה עם מפתח פרטי (הצפנה סימטרית), בטיחות מושלמת וחישובית, קריפטואנליזה, אימות הודעות, מבוא לתורת המספרים, קריפטוגרפיה עם מפתח פומבי (הצפנה אסימטרית), חתימות דיגיטליות ופונקציות תמצות קריפטוגרפיות, הוכחות באפס ידע, סכמות שיתוף סוד.

**סמסטר ב':**

שם הקורס	סוג	מרצה	שעות	נ"ז	זמנים
מבוא לקריפטוגרפיה	שיעור+תרגול	פרופ' אור דונקלמן	4	4	א'ה' 14-16

### נושאים בתיאוריה של מדעי המחשב, 203.3534

**קדם:** שיטות הסתברותיות 203.2480, תכנון וניתוח אלגוריתמים 203.2410, אלגברה ב' 203.1820

הקורס יעסוק בהקניית כלים מתמטיים הנדרשים לעוסקים בתיאוריה של מדעי המחשב עם דגש על השימושים.

**סמסטר א':**

שם הקורס	סוג	מרצה	שעות	נ"ז	זמנים
נושאים בתיאוריה של מדעי המחשב	שיעור	ד"ר אורי רבינוביץ	3	3	ה', 16-19

### מעבדה בחקר חישוב של התנהגות אנושית, 203.3734

**קדמים:** עיבוד תמונה 203.3730, תכנות מונחה עצמים 203.1120

קורס מעבדה בו סטודנטים יבצעו פרויקט מחקרי בתחום חקר חישובי של התנהגות חישובית. הפרויקט יכול לקחת מערכת ושימוש בטכנולוגיות והרצת פיילוט ניסויי עם ניתוח תוצאות. חלק מהפרויקטים יהיו בשיתוף עם חוקרים אחרים באוניברסיטה (פסיכולוגיה, פיזיותרפיה, חינוך ועוד) ויתכן ויתבצעו בשטח המעבדה שלהם. דוגמאות לפרויקטים: מעקב אחר תנועות פנים, ידיים, ניתוח תנועות גופניות, מעקב אחר תנועות עיניים בעת ביצוע משימה ועוד.

לקורס זה יתקבלו רק סטודנטים אשר סיימו את הקורס: "עיבוד תמונה בציון 85 ומעלה. סטודנט שנרשם בסמסטר א' תשפ"א לקורס עיבוד תמונה יהיה תקף רק למועדי בחינות א+ ב, בנוסף במידה ולא עמד בדרישות הקדם, הרישום לקורס זה יימחק ממערכת הלימודים שלו בתקופת השינויים של סמסטר ב'.

הקבלה לקורס זה אינה אוטומטית, יש לשלוח מייל בקשה לרישום לפרופ' הגית הל אור [hagit@cs.haifa.ac.il](mailto:hagit@cs.haifa.ac.il) עד לתאריך 28.9.21.

**סמסטר ב':**

שם הקורס	סוג	מרצה	שעות	נ"ז	זמנים
מעבדה בחקר חישוב של התנהגות אנושית	מעבדה - מחליפה פרויקט	פרופ' הגית הל-אור	3	3	ד', 16-19

### עיבוד גיאומטרי, 203.3747

קדם: גרפיקה ממוחשבת 203.3710

בקורס נלמד מספר נושאים מתקדמים העיבוד גיאומטרי: סריקה ושחזור משטחים, גיאומטריה דיפרנציאלית דיסקרטית, אנליזה של משטחים, פרמטריזציה ודפורמציה של משטחים, אופטימיזציה ואלמנטים סופיים בהקשר של גיאומטריה. הקורס דורש שליטה טובה ב-C++.

סמסטר ב':

שם הקורס	סוג	מרצה	שעות	נ"ז	זמנים
עיבוד גיאומטרי	שיעור	ד"ר רועי פורן	3	3	ב' 16-19

### מעבדה בלמידת מכונה משמרת פרטיות, 203.3762

קדם: תכנות מונחה עצמים 203.1120, מבני נתונים 203.2310

למידת מכונה (machine learning) הפכה לגורם רב השפעה במבנה הכלכלי והחברתי, עם מגוון השפעות חיוביות ושליטיות על אנשים, טכנולוגיה וחברה. ההצלחה של למידת המכונה כרוכה בגישה לדאטה נרחב ואיסוף נתוני עתק על אנשים פרטיים, ארגונים ועוד, המשמש לאימון המערכות הלומדות ולחיזוי בעזרתן. הגישה הרחבה של חברות וארגונים לדאטה נרחב על פרטים בחברה עשויה להוביל למגוון איומים, על פרטיות, על בטחון (אישי, כלכלי, תעסוקתי, ביטחוני), על יציבות פוליטית, ועוד.

לא יתקיימו שיעורים קבוצתיים אלא מפגשים אישיים. לתיאום מפגש נא לפנות במייל לד"ר עדי עקביה

סמסטר ב':

שם הקורס	סוג	מרצה	שעות	נ"ז	זמנים
מעבדה בלמידת מכונה משמרת פרטיות	מעבדה - מחליפה פרויקט	ד"ר עדי עקביה	3	3	מפגשים אישיים

### אקראיות בחישוב, 203.3426

קדם: שיטות הסתברותיות 203.2480, תכנון וניתוח אלגוריתמים 203.2410

אלגוריתמים הסתברותיים הם אלגוריתמים שמטילים מטבעות אקראיים תוך כדי פעולתם. אלגוריתמים כאלה הם במקרים רבים, יעילים ופשוטים יותר מאלגוריתמים דטרמיניסטיים סטנדרטיים. האם אפשר ליהנות מהפשטות והיעילות של אלגוריתמים הסתברותיים ללא הטלת מטבעות? כדי לנסות באופן חיובי על השאלה הזו, פותחה תורה מתמטית של פסאודו-אקראיות. הרעיון הוא לנסות ליצור מטבעות "פסאודו-אקראיים" ש"נראים" אקראיים לאלגוריתמים, למרות שאינם אקראיים כלל. התורה הזו (שחלקים נרחבים ממנה פותח ע"י מדענים ישראלים עטורי פרסים כמו שפי גולדווסר, עודד גולדרייך ואבי ויגדרזון) מעבירה את הדגש מתכונות מתמטיות של הטלות מטבע לכח החישובי של האלגוריתם שמשמש במטבעות. בקורס נסקור אלגוריתמים הסתברותיים יסודיים וכלים בסיסיים מהתורה המתמטית של פסאודו-אקראיות, בין השאר נכסה את הנושאים הבאים:

- הכח של אקראיות במגוון של סיטואציות חישוביות (זמן, מקום, תקשורת, אלגוריתמים מבוזרים).
  - $k$ -wise independent hash functions ושימושיהם.
  - $\epsilon$  bias ואנליזה ספקטרלית של התפלגויות.
  - אנליזה ספקטרלית של גרפים, ו-expander graphs.
  - האלגוריתם של ריינגולד למסלול קצר ביותר עם מעט זיכרון.
  - extractor graph ושימושיהם.
  - המחלקה BPP והניסיונות להוכיח ש  $BPP=P$ .
- אנו ממליצים לקחת את הקורס אחרי (או במקביל) לקורס מודלים חישוביים (אבל זה אינו נדרש).

סמסטר א':

שם הקורס	סוג	מרצה	שעות	נ"ז	זמנים
אקראיות בחישוב	שיעור	פרופ' רונן שאלתיאל	3	3	ד' 13-16

### פונקציות בוליאניות ועצי הכרעה, 203.3594

קדם: תכנון וניתוח אלגוריתמים

פונקציות בוליאניות, קומבינטוריקה של הקוביה, עצי הכרעה בוליאניים דטרמיניסטיים ואקראיים, מודלים קשורים אחרים, עצי השוואה ובעיות מיון.

סמסטר א':

שם הקורס	סוג	מרצה	שעות	נ"ז	זמנים
פונקציות בוליאניות ועצי הכרעה	שיעור	פרופ' אילן נוימן	3	3	א' 16-19



### מעבדה בלמידה ממוכנת, 203.3771

**קדם:** אלגברה ליניארית 203.1810, חדו"א 203.1840, שיטות הסתברותיות 203.2480. למידה ממוכנת משפיעה על תחומי מחקר רבים, כגון ראייה, שפה, ביולוגיה, מסחר, פיננסים, ורפואה. במעבדה נחקר שיטות מודרניות בלמידה ממוכנת, וניישם אותן בתחומי מחקר שונים. מפגש ראשון יתקיים ביום ה' ה-14.10.21 בשעה 10:00.  
\*לא יתקיימו שיעורים קבוצתיים אלא מפגשים אישיים.

**סמסטר א':**

שם הקורס	סוג	מרצה	שעות	נ"ז	זמנים
מעבדה בלמידה ממוכנת	מעבדה מחליפה פרויקט	פרופ' ריטה אוסדצי	3	3	מפגשים אישיים 14.10.21 בשעה 10

### אופטימיזציות מתקדמות של מהדרים, 203.3137

**קדם:** מבנה מהדרים, 203.2130. בעשור השנים האחרונות חלה התקדמות משמעותית ביכולתם של מהדרים לייצר קוד המתאם לחומרה. יכולת זו מושגת ע"י שורה של אנליזות וטרנספורמציות שמבצע המהדר על קוד המכונה שהוא יוצר. בקורס נלמד חלק ממרכיבים אלו: מבנה המעבד אופטימיזציות מקור הקצאת אוגרים תיזמון גלובלי תזמון בלוקים תזמון של לולאות ואופטימיזציות מודרכות קדם ריצה.

**סמסטר ב':**

שם הקורס	סוג	מרצה	שעות	נ"ז	זמנים
אופטימיזציות מתקדמות של מהדרים	שיעור	פרופ' יוסי בן אשר	3	3	ג' 17-20

### מעבדה בתכנון רכיבי חומרה למערכות משובצות, 203.3260

**קדם:** מבוא למדעי המחשב 203.1110, מבוא לחומרה 203.1210. ישראל נמצאת במקום השני בעולם מבחינת כמות הציפים המתוכננים בה. תכנון רכיבי חומרה נעשה לחלוטין ע"י תכנות בשפת חומרה (Verilog). במסגרת המעבדה נלמד לתכנת ב-Verilog ולהפעיל סינתזה של תוכנית ב-Verilog לרכיב FPGA ואולי גם לסינתזת ASIC. הפרויקט יהיה מימוש של אלגוריתם מסויים ב-Verilog. כמו כן, תהיה השוואה להמרה אוטומטית של תוכנה לחומרה.

\*לא יתקיימו שיעורים קבוצתיים אלא מפגשים אישיים. לתיאום מפגש נא לפנות במייל לפרופ' יוסי בן אשר

**סמסטר ב':**

שם הקורס	סוג	מרצה	שעות	נ"ז	זמנים
מעבדה בתכנון רכיבי חומרה למערכות משובצות	מעבדה - מחליפה פרויקט	פרופ' יוסי בן אשר	3	3	מפגשים אישיים

### תורת האינפורמציה במדעי המחשב, 203.3370

**קדם:** תכנון וניתוח אלגוריתמים 203.2410, שיטות הסתברותיות 203.2480. תורת האינפורמציה עוסקת בכימות של מידע ובאפשרות דחיסתו. עקרונות מתחום תורת האינפורמציה עומדים בבסיס רבות ממערכות התקשורת ועיבוד הנתונים בהן אנו משתמשים בחיי היום יום, והיא מהווה תחום מחקר פעיל עם שימושים רבים במדעי המחשב ובהנדסה. בקורס נציג מושגים וכלים בסיסיים בתורת האינפורמציה, תוך שימת דגש על שיטות אלגוריתמיות לדחיסת נתונים. כמו כן נדגים שימושים של תורת האינפורמציה בתחומים שונים במדעי המחשב כגון למידה חישובית, קריפטוגרפיה, מבני נתונים וחישוב מבוזר.

**סמסטר ב':**

שם הקורס	סוג	מרצה	שעות	נ"ז	זמנים
תורת האינפורמציה במדעי המחשב	שיעור	פרופ' נגה רון צבי	3	3	ד' 16-19

### אלגוריתמים הסתברותיים, 203.3424

**קדם:** תכנון וניתוח אלגוריתמים, 203.2410  
 אלגוריתמים הסתברותיים משתמשים בהטלות מטבע אקראיות לצורך פתרון בעיות חישוב. אלגוריתמים אלה הנם במקרה פשוטים ויעילים יותר מאשר אלגוריתמים "רגילים". הקורס יציג אלגוריתמים ופרוטוקולים הסתברותיים החוסכים במגוון משאבי חישוב כגון: זמן ריצה, זיכרון, תקשורת ומקביליות עבור בעיות חישוב שונות.

#### סמסטר ב':

שם הקורס	סוג	מרצה	שעות	נ"ז	זמנים
אלגוריתמים הסתברותיים	שיעור	פרופ' אילן נוימן	3	3	ה' 16-19

### יסודות הקריפטוגרפיה, 203.3447

**קדם:** שיטות הסתברותיות 203.2480, מודלים חישוביים, 203.3510  
 האם אפשר לתכנן שיטות הצפנה עם הוכחה מתמטית לבטיחות? (בדומה לצורה שבה אנו מוכיחים נכונות של אלגוריתמים). התחום של יסודות הקריפטוגרפיה שואף לבנות שיטת להצפנה, חתימות דיגיטליות, הוכחות באפס ידיעה, ופרוטוקולים קריפטוגרפיים נוספים, יחד עם הוכחה מתמטית לבטיחות. מכיון (או הנחות דומות). NP שונה מ-P, עלינו להתבסס על ההנחה ש NP שונה מ-P שאיננו יודעים להוכיח ש- בארבעים השנה האחרונות רעיונות אלה (שחלקים נרחבים מהם פותחו ע"י מדענים ישראלים עטורי פרסים כמו שפי גולדווסר, עודד גולדרייך, אבי ויגדרזון ומוני נאור) עשו מהפכה בקריפטוגרפיה (ובתחומים אחרים במדעי המחשב). מסתבר, שצעד משמעותי, ולא טריויאלי הוא להגדיר בצורה מתמטית מדויקת מהי בטיחות קריפטוגרפית. במקרים רבים מציאת ההגדרה הנכונה היא חלק משמעותי בפתרון. בקורס נסקור רעיונות בסיסיים ביסודות הקריפטוגרפיה. בין השאר נכסה את הנושאים הבאים:

-One way functions -Hard-core bits -Pseudorandom generators -Bit commitment schemes -Coin tossing over the phone -Zero knowledge proofs -Signature schemes -Encryption schemes -Secure function evaluation

אנו נשים דגש על הגדרות בטיחות פורמליות, והוכחות מתמטיות מדויקות. (זהו אספקט ששונה מהקורס "מבוא לקריפטוגרפיה" שסוקר נושאים רבים יותר, ואנו ממליצים לסטודנטים שמתעניינים בקריפטוגרפיה על שני הקורסים).

#### סמסטר ב'

שם הקורס	סוג	מרצה	שעות	נ"ז	זמנים
יסודות הקריפטוגרפיה	שיעור	פרופ' רונן שאלתיאל	3	3	ג' 14-17

### למידת נתונים במערכות זמן אמת, 203.3274

**קדם:** תכנון וניתוח אלגוריתמים 203.2410, תכנות מונחה עצמים 203.1120, אלגברה ב' 203.1820, חדו"א 203.1840  
 כל קבוצת סטודנטים תקבל פרויקט שיעסוק בתכנון ומימוש מערכת שלומדת נתונים בזמן אמת. אפשר לבחור אחת משתי האפשרויות: מערכות רובוטיות - כולל רחפנים, מכוניות, מערכות EEG ("קריאת מחשבות"), משקפי מציאות מדומה, זרוע רובוטית וכו'. מחשוב ענן - תכנון ומימוש אלגוריתמים למידה וניתוח טרה בייטים של מידע ממקורות טוויטר, מאגרי תמונה או קול על מאות מחשבים בענן (בד"כ של אמזון).  
 מס' המקומות למעבדה זו הנו מוגבל. הקבלה למעבדה כרוכה בעמידה בתנאים הבאים:

1. ציון של 75 לפחות בקורסי הקדם.
  2. ממוצע ציונים בתו"ל של 85 לפחות
  3. ראיון אישי עם ד"ר דן פלדמן
- עמידה בתנאים 1-2, אינה מבטיחה קבלה למעבדה.

סטודנטים המעוניינים להירשם למעבדה מתבקשים לשלוח קורות חיים ותדפיס ציונים עדכני לאמיר בר און עד לתאריך 28.9.21, [AmBarOn@univ.haifa.ac.il](mailto:AmBarOn@univ.haifa.ac.il), יש לציין בנושא המייל: למידת נתונים במערכות זמן אמת.

#### סמסטר קיץ:

שם הקורס	סוג	מרצה	שעות	נ"ז	זמנים
למידת נתונים במערכות זמן אמת	מעבדה (מחליפה פרויקט)	פרופ' דן פלדמן	3	3	אין