

סילבוס קורס

קריפטוגרפיה

7090003

פרטי הקורס

קמפוס: אשדוד

מחלקה: מדעי המחשב

תחום:

שנת לימוד: ב'

סמסטר: א

נקודות זכות: 3

נקודות ECTS: 4.5

מרצה/ים: ד"ר ירמיהו מילר

jeremmi@sce.ac.il

שנה אקדמית: תשפ"ו

סוג הקורס: חובה

רמת הקורס: תואר ראשון

צורת העברה: פנים אל פנים.

דרישות קדם:

דרישות במקביל: מבוא להסתברות למדמ"ח

שפת הוראה: עברית

סביבת עבודה:

מתרגל/ים:

מטרה

הקניית העקרונות והמושגים הבסיסיים של קריפטוגרפיה מודרנית ויישומם באפליקציות מעשיות במדעי המחשב.

תפוקות למידה

- עם סיום מוצלח של הקורס, הסטודנטים יהיו מסוגלים:
1. להשתמש באלגוריתם של אוקליד כדי למצוא את המחלק הגדול ביותר של שני איברים בחוג, ולמצוא את השארית של מספר שלם בחלוקה במשפר שלם אחר.
2. להבחין האם קריפטו-מערכת ניתנת לפענוח באמצעות המשפטים היסודיים של תורת המספרים, תכונות של מספרים ראשוניים, משפטי פרמה ופונקצית אוילר.
3. לפתור מערכת של משוואות מודולריות מעל חוגים באמצעות המשפט השאריות הסינית.
4. לייצג האלפיבית הלטינית באמצעות החוג Z_{26} לבצע חיבור וכפל של איברים בחוג Z_{26} ולבצע כפל מטריצות ולהפוך מטריצה בחוג Z_{26} והכללה ל- m אותיות.
5. להצפין טקסט גלוי ולפענח טקסט מוצפן לפי הצפנים הבסיסיים, כולל צופן הזהה (צופן קיסר), צופן החלפה, צופן של תמורה, צופן היל וצופן ויז'נר.
6. להשתמש בקריפטו-אנליזה לפענח טקסט מוצפן ולבנות אלגוריתמים לשיתוף סודות והסתרת מידע.
7. להוכיח האם לקריפטו-מערכת יש סודיות מושלמת על ידי תורת שנון ולהשתמש בשיטות שונות לאבטחת העברת ועיבוד המידע.
8. להצפין ולפענח מספרים בינאריים באמצעות צופן פייסטל, צופן DES וצופן IDEA.
9. להצפין ולפענח מספרים שלמים באמצעות צופן RSA וצופן אל-גמאל.
10. לזהות שלמות המידע.

תוכן הקורס

שבוע	נושא	מקורות רלוונטים
1	תורת המספרים: אריתמטיקה מודולרית. משפט החילוק של אוקליד, האלגוריתם של אוקליד והאלגוריתם המוכלל של אוקליד. המשפטים של פרמה. משפט הפירוק לראשוניים.	[1] פסקאה 1.1 [2] פסקאה 2.1 [3] פסקאות 1.5 - 1.6
2	ההגדרה הפורמלית של חוג מתמטי. קבוצת השארית מודולו p . חוגים של אלפבתיות. החוג Z_{26} של האלפיבית הלטינית וחוגים של אלפבתיות כלליות Z_m . הפיכת מטריצה בחוגים.	[1] פסקאה 1.1 [2] פסקאה 2.1 [3] פסקאות 1.5 - 1.6
3	הגדרות פורמליות של פונקציית הצפנה, ופונקציית פענוח, טקסט גלוי וטקסט מוצפן. צפנים הבסיסיים: הצפנים הבסיסיים: צופן ההזהה, צופן ההחלפה, צופן האפיני, צופן התמורה, צופן ויז'נר. התנאים ההכרחיים של צופן הניתן לפענוח.	[1] פסקאות 1.1 - 1.2 [2] פסקאות 2.1 - 2.2
4	קריפטו - אנליזה: סוגים של התקפת סייבר. פונקציית ההסתברות של האותיות של האלפיבית הלטינית. המדד צירוף המקרים. קריפטו-אנליזה של הצופן האפיני, צופן ההחלפה וצופן של היל.	[1] פסקאות 1.1 - 1.2 [2] פסקאות 2.1 - 2.2
5	צופן RSA: הפרוטוקול דיפי-הלמן לקביעת מפתח משותף. ההגדרה הפורמלית של צופן RSA וההוכחה שהוא ניתן לפענוח. המשפט השאריות הסיני ושימוש בפענוח של צופן RSA. שימוש בשארית ריבועית מודולו ראשוני p בפענוח של צופן RSA.	[1] פסקאות 5.1 - 5.3 [2] פסקאות 6.1 - 6.3
6	הבעיית הפירוק של מספרים וצופן רבין: מבחנים ראשוניות. שימוש בקריטריון אוילר. האלגוריתם מילר-רבין לבדיקת ראשוניות. שיטת החישוב של שורש מודולו p . אלגוריתמים לפירוק של מספרים שלמים. צופן רבין.	[1] פסקאות 5.4 - 5.8 [2] פסקאות 6.4 - 6.8
7	צופן אל-גמאל וקריפטוגרפיה של מפתח פומבי: ההגדרה הפורמלית של הצופן אל-גמאל וההוכחה שהוא ניתן לפענוח. בעיית הפירוק לגורמים ובעיית הלוגריתם הדיסקרטי. חישוב משותף של הפרמטרים הפומביים. שימוש בערך המשותף. פרוטוקול דיפי-הלמן מעל חבורה כללית. בטיחות השיטה ובעיות דיפי-הלמן.	[1] פסקאות 6.1 - 6.7 [2] פסקאות 7.1 - 7.2

8	תורת שגון של סודיות: חזרה של תורת הסתברות בסיסית. ההצפנה של האפמן ושיטת עץ ההצפנה. ההגדרות הפורמליות של אנטרופיה וסודיות מושלמת. קוד מורס.	[1] פסקאות 2.1 - 2.5 [2] פסקאות 3.1 - 3.4
9	צפני בלוק וצפני זרם? הגדרה פורמלית של תמורה מתמטית וחישובים עם תמורות. רשתות החלפה-תמורה. צופן פייסטל. תקן הצפנת הנתונים - DES (data encryption standard). תרגילים פשוטים של הצפנה ופענוח ע"י DES. תקן ההצפנה המתקדם - AES (advanced encryption standard). תרגילים פשוטים של הצפנה ופענוח ע"י AES.	[1] פסקאות 3.2, 3.5-3.6 [2] פסקאות 4.1 - 4.6
10	פונקציות תמצות קריפטוגרפיות: פונקציות תמצות ואמינות המידע. בטיחות של פונקציות תמצות. מודל האורקל האקראי. אלגוריתמים במודל האורקל האקראי. השוואה בין קריטריוני בטיחות.	[1] פסקאות 4.1 - 4.2 [2] פסקאות 5.1 - 5.2
11	פונקציות תמצות קריפטוגרפיות (המשך): פונקציות תמצות איטרטיביות. הבניית מרקל-דמגרד (Merkle-Damgard). בניית ספוג ופונקציית התמצות SHA-3. קודמים לאורתנטיקציה של הודעות: MAC, מקונן ו-HMAC.	[1] פסקאות 4.3 - 4.5 [2] פסקאות 5.3 - 5.5
12	שיטות חתימה: דרישות בטיחות משיטות חתימה. שיטת החתימה של אל-גמאל. וריאנטים של שיטת החתימה של אל-גמאל. שיטת החתימה של שנור. אלגוריתם החתימה הדיגיטלי. סרטיפיקטים.	[1] פסקאות 7.2 - 7.4 [2] פסקאות 8.2 - 8.5
13	סכמות? לשיתוף סודות: סכמת הסף של שמיר. סכמת סף (t,t) פשוטה. מבני גישה ושיתוף סודות כללי. בניית המעגל המונוטוני. סכימות שיתוף סודות ניתנות לאימות.	[1] פסקאות 7.5 - 7.7 [2] פסקאות 9.1 - 9.4

מקורות ספרות נדרשים ומומלצים

ספר הקורס:
מקורות נוספים:

1. D.R. Stinson, Cryptography: Theory and Practice , 4th ed. Chapman Hall/CRC, 2018
2. C. Paar, J. Pelzl, "Understanding Cryptography: A Textbook for Students and Practitioners" (available online for SCE students), Springer, 2010
3. Joseph J. Rotman "A first course in abstract algebra 2nd ed., Upper Saddle River, N.J., Prentice Hall PTR, 2000
4. Charlie ????,Radia???Kaufman,???Mike???Speciner, Network security: private communication in a public world 2nd ed., Upper Saddle River, N.J., Prentice Hall PTR, 2002
5. Baimel A., Dolev Sh., "Anonymous message delivery", Proceeding of FUN 2001
6. Aumasson J-P, "Serious Cryptography. A practical introduction to modern encryption", No Starch Press, 2018
7. Bashir I. "Mastering Blockchain", Packt Publishing Ltd., 2017
8. Smart card & Security basics", CardLogix, 2019"

פעילויות למידה מתוכננות ושיטות הוראה

שעות הרצאה שבועיות: 3
שעות הרצאה שבועיות: 3. אין תרגול בקורס זז.
ההוראה תתקיים בצורה פונטאלית.

שיטות הערכה וקריטריונים

הערות	אחוז	קריטריון
ציון 56 ומעלה במבחן הינו תנאי לשקלול הבוחן ועבודות הגשה בציון הסופי. אחרת ציון המבחן הינו הציון הסופי בקורס.	75	בחינה סופית:
במהלך הסמסטר ינתנו כ-3 עבודות בית.	25	תרגילים: