המכללה האקדמית להנדסה סמי שמעון

סילבוס קורס
מבוא לקריפטוגרפיה למדמ"ח

פרטי הקורס

קמפוס:	באר שבע	שנה אקדמית:	תשפ"ו
מחלקה	מדעי המחשב	סוג הקורס:	בחירה
תחום:	רמת הקורס:		תואר ראשון
שנת לימוד:	ב'	צורת העברה:	פנים אל פנים
סמסטר:	א'	דרישה קדם:	אלגברה ליניארית 1 אלגברה 2 מבוא להסתברות למדמ"ח
נקודות זכות:	3	שפת מקביל:	
נקודות ECTS:	4.5	שפת הוראה:	עברית
		סביבת הוראה:	פרונטאלי.
מרצה/ים:	ד'ר ירמיהו מילר jeremmi@sce.ac.il		

מטרה

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

תפוקות למידה

עם סיום מוצלח של הקורס, הסטודנט יהיה מסוגל:

1. להשתמש באלגוריתם של אוקליד כדי למצוא את המחלק המשותף הגדול ביותר של שני איברים בחוג, ולמצוא את השאריתשל מספר שלם בחלוקה במספר שלם אחר.
2. להבחין האם קריפטו-מערכת ניתן לפענח 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 $Z26$, לבצע חיבור וכפל של איברים בחוג $Z26$, ולבצע כפל מטריצות ולהפורמטריצה בחוג $Z26$, ולהכליל את היצוג הזה לאלפיביתיות בעלות m אותיות.
5. להצפין טקסט גלוי ולפענח טקסט מוצפן לפי הצפנים הבסיסיים, כולל צופן הזזה (צופן קיסר), צופן החלפה, צופן של תמורה,צופן היל וצופן ויז'נר. לפתור בעיות של אותנטיקציה וזיהוי.
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 ועיבודהמידע.
8. להצפין ולפענח מספרים בינארים 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
1	תורת המספרים: אריתמטיקה מודולרית. משפט החילוק של אוקלידס, האלגוריתם של אוקלידס והאלגוריתם המוכלל של אוקלידס. המשפטים של פרמה. משפט הפירוק לראשוניים.	[1] פסקאה 1.1 [2] פסקאה 2.1. [3] פסקאות 1.5-1.6.
2	חוגים מתמטיים של אלפבתיות: ההגדרה הפורמלית של חוג מתמטי. קבוצת השארית מודולו p. חוגים של אלפבתיות. החוג $\mathbb{Z}_{26}$ של האלפבית הלטינית וחוגים של אלפבתיות כלליות $\mathbb{Z}_m$. הפיכת מטריצה בחוגים.	[1] פסקאה 1.1 [2] פסקאות 2.1-2.2. [3] פסקאות 1.5-1.6.
3	צפני הבסיסיים: הגדרות פורמליות של פונקצית הצפנה, ופונקצית פענוח, טקסט גלוי וטקסט מוצפן. הצפנים הבסיסיים: צופן ההזזה, צופן ההחלפה, צופן האפיני, צופן התמורה, צופן ויז'נר. התנאים ההחרכיים של צופן הניתן לפענוח.	[1] פסקאה 1.1-1.2 [2] פרק 2 פסקאות 2.1-2.2 .
4	קריפטו - אנליזה: סוגים של התקפת סייבר. פונקצית ההסתברות של האותיות של האלפבית הלטינית. המדד צירוף המקרים. קריפטו-אנליזה של הצופן האפיני, צופן ההחלפה וצופן של היל.	[1] פסקאה 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 שֶנוֹן 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 - data encryption standard (DES). תרגילים פשוטים של הצפנה ופענוח ע"י DES. תקן ההצפנה המתקדם - Advanced encryption standard (AES). תרגילים פשוטים של הצפנה ופענוח ע"י AES.	[1] פסקאות 3.2 ו- 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 הדיגיטלית. 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 .
14	חזרה לפני המבחן.	

ספרי הקורס:

[1] D.R. Stinson, Cryptography: Theory and Practice, 4th ed. Chapman & Hall/CRC, 2018

מקורות נוספים:

[2] טסה תמיר, מבוא לקריפטוגרפיה ,מדריך למידה בהוצאת האוניברסיטה הפתוחה, פברואר 20
[3] Josehph J, Rotman A first course in abstract algebra 2nd ed., Upper Saddle River, N.J., Prentice Hall PTR, .2000
[4] Charlie Perlman Radia Kaufman, Mike Speciner, Network security: private communication in a public world 2nd ed., Upper Saddle River, N.J., Prentice Hall PTR, .2002
[5] C. Paar, J. Pelzl, “Understanding Cryptography: A Textbook for Students and Practitioners” (available online for SCE students), Springer, .2010
[6] Baimel A., Dolev Sh., “Anonymous message delivery”, Proceeding of FUN 2001
[7] Aumasson J-P, “Serious Cryptography. A practical introduction to modern encryption”, No Starch Press, 2018
[8] Bashir I. “Mastering Blockchain”, Packt Publishing Ltd., 2017
[9] “Smart card & Security basics”, CardLogix, 2019

פעילויות למידה מתוכננות ושיטות הוראה

עות הרצאה שבועיות: 3. אין תרגול בקורס זו.
ההוראה תתקיים בצורה פרונטאלית.

שיטות הערכה וקריטריונים

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

הנחיות

יתכנו שינויים בנושאי השיעורים וההתקדמות עקב המלחמה.