

סילבוס קורס

קריפטוגרפיה 7090003



שנה אקדמית: תשפו

סוג הקורס: בחירה

רמת הקורס: תואר ראשון

צורת העברה: פנים אל פנים.

. 370004 דרישות קדם: אלגברה לינארית 1 למדמ"ח

מבוא להסתברות למדמ"ח 7000007

בציון 0

דרישות במקביל:

שפת הוראה: עברית

סביבת עבודה:

מתרגל/ים:

קמפוס: באר שבע מחלקה: מדעי המחשב

10100

תחום:

שנת לימוד: ב'

סמסטר: א

נקודות זכות: 3

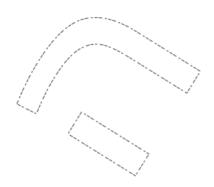
4.5 :ECTS נקודות

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, הסטודנטים יהיו מסוגלים:

- 1. להשתמש באלגות מל אוקליד כדי למצוא את המחלק המשותף הגדול ביותר של שני איברים בחוג, ולמצוא את השארית של מספר שלם בחלוקה במספר שלם אחר.
- להבחין האם קריפטוּ-מערכת ניתן לפענח באמצעות המשפטים היסודיים של תורת המספרים, תכונות של מספרים \ / ראשוניים, משפטי פרמה ופונקצית אוילר.
 - . ∕לפתור מערכת של משוואות מודולריות מעל חוגים באמצעות המשפט השאריות הסינית.
 - 4. לֿײַצג הُאֹלֿפִיבית ָהּלֹטינית באמצעות החוג Z26, לבצע חיבור וכפל של איברים בחוג Z26, ולבצע כפל מטריצות ולהפור במטריצה בחוג Z26, ולהכליל את היצוג הזה לאלפיביתיות בעלות m אותיות.
- להצפין טקסט גלוי ולפענח טקסט מוצפן לפי הצפנים הבסיסיים, כולל צופן הזזה (צופן קיסר), צופן החלפה, צופן של .5 תמורה, צופן היל וצופן ויז'נר. לפתור בעיות של אותנטיקציה וזיהוי.
 - 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.
 - 3. 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

מקורות רלוונטים		נושא	שבוע
[1] פסקאה 1.1 [2] פסקאה 2.1. [3] פסקאות 1.5-1.6	החילוק של אוקליד, האלגוריתם של אוקליד . המשפטים של פרמה. משפט הפירוק	תורת המספרים: אריתמטיקה מודולרית. משפט ו והאלגוריתם המוכלל של אוקליז לראשוניים.	1
[1] פסקאה 1.1 [2] פסקאה 2.1-2.2. [3] פסקאות 1.5-1.6	נמטי. קבוצת השארית מודולו p. חוֻגי ם של. פבית הלטינית וחוגים של אלפבתיות	חוגים מתמטיים של אלפבתיות: ההגדרה הפורמלית של חוג מת אלפבתיות. החוג Z26 של האל כלליות Zm הפיכת מטריצה בח	2
[1] פסקאה 1.1-1.2 [2] פסקאה 2.1-2.2.	הצפנה, ופונקצית פענוח, טקסט גלוי ם: צופן ההזזה, צופן ההחלפה, צופן נר. התנאים ההחרכיים של צופן הניתן	וטקסט מוצפן. הצפנים הבסיסיי	3
[1] פסקאה 1.1-1.2 [2] פסקאה 2.1-2.2	נית ההסתברות של האותיות ש <i>ׁל האׁלּ</i> פבית . קריפטו-אנליזה של הצופן האפיני, צופן	קריפטו-אנליזה: סוגים של התקפת סייבר. פונקצ הלטינית. המדד צירוף המקרים. ההחלפה וצופן של היל.	4
[1] פסקאה 5.1-5.3 [2] פסקאה 6.1-6.3	מפתח משותף. ההגדרה הפורמלית של לפענוח. המשפט השאריות הסיני ושימוש בשארית ריבועית מודולו ראשוני p בפענוח	צופן RSA וההוכחה שהוא ניתן	5
[1] פַּסַקאה 5.4-5.8 [2] פֿסקאה 6.4-6.8	יטריון אוילר. האלגוריתם מילר-רבין ווב של שורש מודולו-p.	הבעיית הפירוק של מספירם וצו מבחנים ראשוניות. שימוש בקרי לבדיקת ראשוניות. שיטת החיש אלגוריתמים לפירוק של מספריו	6
[1] פסקאות 1.6.1-6.7 [2] פסקאות 2.7-1.7.	אל-גמאל וההוכחה שהוא ניתן לפענוח. הלוגריתם הדיסקרטי. חישוב משותף של בערך המשותף. פרוטוקול דיפי-הלמן מעל	בעיית הפירוק לגורמים ובעיית ו	7

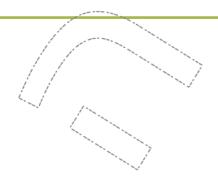


	תורת שֶנוֹן של סודיות: חזרה של תורת הסתברות בסיסית. ההצפנה האפמן ושיטת עץ ההצפנה. ההגדרות הפורמליות של אנטרופיה וסוז מושלמת. קוָדַ מוּרַסָ.	8
,	צפני בלוק וצפני זרם: הגדרה פובמלית של תמורה מתמטית וחישובים עם תמורות. רשתו החלפה-תמורה. צופן פייסטל. תקן הצפנת הנתונים (data encryption standard DES). תרגילינ פשוטים של הצפנה ופענוח על ידי DES. תקן ההצפנה המתקדם (advanced encryption standard AES) . תרגילים פשוטים של ופענוח על ידי AES.	9
[1] פסקאות 4.1-4.2. ל [2] פסקאות 5.1-5.2	פונקציות תמצות קריפטוגרפיות: פונקציות תמצות ואמינות המידע. בטיחות של פונקציות תמצות. מוד האורקל האקראי. אלגוריתמים במודל האורקל האקראי. השוואה בין קריטריוני בטיחות.	10
[1] פסקאות 4.3-4.5. [2] פסקאות 5.3-5.5	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.	11
[1] פסקאות 7.2-7.4. אנטים [2] פסקאות 8.2-8.5. תם	שיטות חתימה: דרישות בטיחות משיטות חתימה. שיטת החתימה של אל-גמאל. וריי של שיטת החתימה של אל-גמאל. שיטת החתימה של שנור. אלגורי החתימה הדיגיטלית. סרטיפיקטים.	12
טודות [1] פסקאות 7.5-7.7. [2] פסקאות 9.1-9.4	סכמת הסף של שמיר. סכמת סף (t ,t) פשוטה. מבני גישה ושיתוף כ כללי. בניית המעגל המונוטוני. סכימות שיתוף סודות ניתנות לאימות.	13

מקורות ספרות נדרשים ומומלצים

ספר 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 האוַנִיברסיטה הפתוחה פברואר 2020
- 3. Josehph J, Rotman A first course in abstract algebra .2nd ed., Upper Saddle River, N.J., Prentice Hall PTR, 2000
- Baimel A., Dolev Sh., "Anonymous message delivery", Proceeding of FUN, 2001
 Aumasson J-P, "Serious Cryptography. A practical introduction to modern encryption, No" Starch Press, 2018
- 6. Bashir I. "Mastering Blockchain", Packt Publishing Ltd., 2017
- 7. "Smart card & Security basics", CardLogix, 2019
 8. 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
- 9. C. Paar, J. Pelzl, "Understanding Cryptography: A Textbook for Students and Practitioners" (available online for SCE students), Springer, 2010





פעילויות למידה מתוכננות ושיטות הוראה

שעות הרצאה שבועיות:-3 ההוראה תתקיים בצורה פרונטאלית.

שיטות הערכה וקריטריונים

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

הנחיות

יתכנו שינויים בנושאי השיעורים וההתקדמות עקב המלחמה.

