

# סילבוס קורס

קריפטוגרפיה 7090003



שנה אקדמית: תשפו

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:

קמׄפוּס; אשדַודּ־

מחלקה: מדעי המחשב

תחום:

שנת לימוד: ב' סמסטר: א

נקודות זכות: 3

4.5 :ECTS נקודות

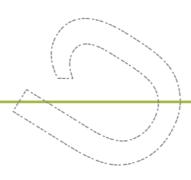
מרצה/ים: ד"ר ירמיהו מילר

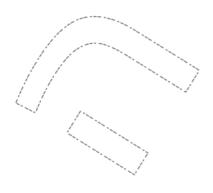
jeremmi@sce.ac.il



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 תם של אוקליד כדי למצוא את המחלק הגדול ביותר של שני איברים בחוג, ולמצוא את השארית של מספר שלם בחלוקה במשפר שלם אחר.
  - להְבחין האם קריפטוּ-מערכת ניתנת לפענוח באמצעות המשפטים היסודיים של תורת המספרים, תכונות של ג'ל להְבחין האם קריפטוּ-מערכת ניתנת לפענוח באמצעות המשפטים היסודיים של תורת המספרים, תכונות של ג'ל מספרים ראשוניים, משפטי פרמה ופונקצית אוילר.
    - 3. /לפתוך מערכת של משוואות מודולריות מעל חוגים באמצעות המשפט השאריות הסינית.
  - לייצג האלפיבית הלטינית באמצעות החוג ,Z26 לבצע חיבור וכפל של איברים בחוג ,Z26 ולבצע כפל מטריצות לייצג האלפיבית בחוג ,Z26 והכללה ל- 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.
  - 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.
    - . IDEA וצופן DES להצפין ולפענח מספרים בינארים באמצעות צופן פייסטל, צופן 8.
      - 9. להצפין ולפענח מספרים שלמים באמצעות צופן RSA וצופן אל-גמאל.
        - 10. לזהות שלמות המידע.

#### תוכן הקורס

מקורות רלוונטים	שא מקורות רלוונטים		
[1] פסקאה 1.1 [2] פסקאה 2.1 [3] פסקאות 1.5 - 1.6	האלגוריתם של אוקליד והאלגוריתם המוכלל של אוקליד. המשפטים של [2		
[1] פסקאה 1.1 [2] פסקאה 2.1 _[3] פסקאות 1.5 - 1.6	ההגדרה הפורמלית של חוג מתמטי. קבוצת השארית מודולו p. חוגים של אלפבתיות. החוג Z26 של האלפבית הלטינית וחוגים של אלפבתיות כלליות Zm. הפיכת מטריצה בחוגים.	2	
[1] פסקאות 1.1 - 1.2 [2] פסקאות 2.1 - 2.2	הגדרות פורמליות של פונקצית הצפנה, ופונקצית פענוח, טקסט גלוי וטקסט מוצפן. צפנים הבסיסיים: הצפנים הבסיסיים: צופן ההזזה, צופן ההחלפה, צופן האפיני, צופן התמורה, צופן ויז'נר. התנאים ההחרכיים של צופן הניתן לפענוח.	3	
[1] פסקאות 1.1 - 1.2 [2] פסקאות 2.1 - 2.2	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.	4	
[1] פסקאות 5.3 - 5.1 [2] פסקאות 6.3 - 6.3	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.	5	
5.4 - 5.8 פסקאות [1] [2] פסקאות 6.4 - 6.8	הבעיית הפירוק של מספירם 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.	6	
6.1 - 6.7 פסקאות 6.7 - 7.1 [2] פסקאות 7.2 - 7.1	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.	7	



[1] פסקאות 2.5 - 2.1 [2] פסקאות 3.4 - 3.1	תורת שֶנוֹן של סודיות: חזרה של תורת הסתברות בסיסית. ההצפנה של האפמן ושיטת עץ ההצפנה. ההגדבות הפורמליות של אנטרופיה וסודיות מושלמת. קוד מורס.	
[1] פסקאות 3.2, 3.5-3.6 [2] פסקאות 4.6 - 4.1	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 - ופענות ע"י advanced encryption standard (AES).	9
1] פסקאות 4.2 - 4.1 [2] פסקאות 5.2 - 5.1	פונקצׄיוּתּ תּמצוֹת קריפטוגרפיות: פונקציות תמצות ואמינות המידע. בטיחות של פונקציות תמצות. מודל האורקל האקראי. אלגוריתמים במודל האורקל האקראי. השוואה בין קריטריוני בטיחות.	10
1.3 פסקאות 4.5 - 4.3 [2] פסקאות 5.5 - 5.3	פונקציות תמצות קריפטוגרפיות (המשרְ): 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 7.4 - 7.2 [2] פסקאות 8.2 - 8.2	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.	12
[1] פסקאות 7.5 - 7.5 [2] פסקאות 9.4 - 9.1	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.	13

# מקורות ספרות נדרשים ומומלצים

ספר הקורס:

- 1. D.R. Stinson, Cryptography: Theory and Practice, 4th ed. Chapman Hall/CRC, 2018 מקורות נוספים:
- 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 ????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. Baimel A., Dolev Sh., "Anonymous message delivery", Proceeding of FUN
- 6. Aumasson J-P, "Serious Cryptography. A practical introduction to modern encryption", No Starch Press, 2018
- Bashir I. "Mastering Blockchain", Packt Publishing Ltd., 2017
   Smart card & Security basics", CardLogix, 2019"



## פעילויות למידה מתוכננות ושיטות הוראה

שעות הרצאה שבועיות:-3 שעות הרצאה שבועיות: 3 אין תרגול בקורס זו. ההוראה תתקיים בצורה פתונטאלית.

### 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 כ3 עבודות בית.	25	:תרגילים

