

סילבוס קורס

מבוא לקריפטוגרפיה למדמ"ח

פרטי הקורס

קמפוס: אשדוד 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:

עברית שפת הוראה: עברית 4.5 :ECTS נקודות

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 ולהפוךמטריצה 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.
- 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
 - 9. להצפין ולפענח מספרים שלמים באמצעות צופן RSA וצופן אל-גמאל.
 - 10. לזהות שלמות המידע.



תוכן הקורס

מבוכות	WHILE WAR AND A STATE OF THE PARTY OF THE PA	шаш
מקורות	ע נושא	
[1] פסקאה 1.1 [2] פסקאה 2.1. [3] פסקאות 1.5-1.6.	תורת המספרים: אריתמטיקה מודולרית. משפט החילוק של אוקליד, האלגוריתם של אוקליד והאלגוריתם המוכלל של אוקליד. המשפטים של פרמה. משפט הפירוק לראשוניים. 	1
[1] פסקאה 1.1 [2] פסקאות 2.1-2.2. [3] פסקאות 1.5-1.6	חוגים מתמטיים של אלפבתיות: ההגדרה הפורמלית של חוג מתמטי. קבוצת השארית מודולו p . חוגים של אלפבתיות. החוג מחוגים של חוג מתמטי. קבוצת השארית מודולו \mathbb{Z}_m . הפיכת מטריצה בחוגים.	2
[1] פסקאה 1.1-1.2 [2] פרק 2 פסקאות 2.1-2.2	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.	3
1.1-1.2 פסקאה 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 5.1-5.3, [2] פסקאות 6.1-6.3.	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
[1] פסקאות 5.4- 5.8. [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
[1] פסקאות 6.1-6.7. [2] פסקאות 7.1-7.2 .	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 2.1-2.5 . [2] פסקאות 3.1-3.4 .	תורת שֶנוֹן של סודיות: חזרה של תורת הסתברות בסיסית. ההצפנה של האפמן ושיטת עץ ההצפנה. ההגדרות הפורמליות של אנטרופיה וסודיות מושלמת. קוד מורס.	8
[1] פסקאות 3.2 ו- 3.5-3.6. [2] פסקאות 4.1 - 4.6.	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 - Advanced encryption standard (AES). תרגילים פשוטים של הצפנה ופענוח ע"י AES.	9
(1] פסקאות 4.1-4.2. [2] פסקאות 5.1-5.2.	פונקציות תמצות קריפטוגרפיות: פונקציות תמצות ואמינות המידע. בטיחות של פונקציות תמצות. מודל 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. [2] פסקאות 8.2-8.5.	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 7.5-7.7. [2] פסקאות 9.1-9.4	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. חזרה לפני המבחן.	13 14
	ווו וו לפני וומבוון.	1-1



:ספרי הקורס

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

מקורות נוספים:

- [2] טסה תמיר, מבוא לקריפטוגרפיה ,מדריך למידה בהוצאת האוניברסיטה הפתוחה, פברואר 20
- Josehph J, Rotman A first course in abstract algebra 2nd ed., Upper Saddle River, [3] N.J., Prentice Hall PTR, .2000
- Charlie Perlman Radia Kaufman, Mike Speciner, Network security: private [4] communication in a public world 2nd ed., Upper Saddle River, N.J., Prentice Hall PTR, .2002
- C. Paar, J. Pelzl, "Understanding Cryptography: A Textbook for Students and [5] Practitioners" (available online for SCE students), Springer, .2010
 - Baimel A., Dolev Sh., "Anonymous message delivery", Proceeding of FUN 2001 [6]
- Aumasson J-P, "Serious Cryptography. A practical introduction to modern encryption", [7]

 No Starch Press, 2018
 - Bashir I. "Mastering Blockchain", Packt Publishing Ltd., 2017 [8]
 - "Smart card & Security basics", CardLogix, 2019 [9]

פעילויות למידה מתוכננות ושיטות הוראה

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

שיטות הערכה וקריטריונים

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

הנחיות

יתכנו שינויים בנושאי השיעורים וההתקדמות עקב המלחמה.