

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
נקודות זכות:	3	מבוא להסתברות למדמ"ח	
נקודות ECTS:	4.5	שפת מקביל:	שפת מקביל:
		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:

- להשתמש באלגוריתם של אוקליד כדי למצוא את המחלק המשותף הגדול ביותר של שני איברים בחוג, ולמצוא את השארית של מספר שלם בחלוקה במספר שלם אחר.
- להבחין האם קריפטו-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.
- לייצג האלפיבית הלטינית באמצעות החוג Z26, לבצע חיבור וכפל של איברים בחוג Z26, ולבצע כפל מטריצות ולהפוך מטריצה בחוג Z26, ולהכליל את היצוג הזה לאלפיביתיות בעלות מ אותיות.
- להצפין טקסט גלוי ולפענח טקסט מוצפן לפי הצפנים הבסיסיים, כולל צופן הזה (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.
- להוכיח האם לקריפטו-מערכת יש סודיות מושלמת על ידי תורת שנון ולהשתמש בשיטות שונות לאבטחת העברת ועיבוד המידע.
- להצפין ולפענח מספרים בינארים באמצעות צופן פייסטל, צופן DES וצופן IDEA.
- להצפין ולפענח מספרים שלמים באמצעות צופן RSA וצופן אל-גמאל.
- לזהות שלמות המידע.

תוכן הקורס

שבוע נושא	מקורות
1 תורת המספרים:	[1] פסקאה 1.1 [2] פסקאה 2.1 [3] פסקאות 1.5-1.6
2 חוגים מתמטיים של אלפבתיות:	[1] פסקאה 1.1 [2] פסקאות 2.1-2.2 [3] פסקאות 1.5-1.6
3 צפני הבסיסיים:	[1] פסקאה 1.1-1.2 [2] פרק 2 פסקאות 2.1-2.2
4 קריפטו - אנליזה:	[1] פסקאה 1.1-1.2 [2] פסקאות 2.1-2.2
5 צופן RSA:	[1] פסקאות 5.1-5.3 [2] פסקאות 6.1-6.3
6 הבעיית הפירוק של מספרים וצופן רבין:	[1] פסקאות 5.8-5.4 [2] פסקאות 6.8-6.4
7 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 שונן של סודיות:	[1] פסקאות 2.1-2.5 [2] פסקאות 3.1-3.4
9 צפני בלוק וצפני זרם:	[1] פסקאות 3.2 [2] פסקאות 3.5-3.6 [3] פסקאות 4.1-4.6
10 פונקציות תמצות קריפטוגרפיות:	[1] פסקאות 4.1-4.2 [2] פסקאות 5.1-5.2
11 פונקציות תמצות קריפטוגרפיות (המשך):	[1] פסקאות 4.3-4.5 [2] פסקאות 5.3-5.5
12 שיטות חתימה:	[1] פסקאות 7.2-7.4 [2] פסקאות 8.2-8.5
13 סכמות לשיתוף סודות:	[1] פסקאות 7.5-7.7 [2] פסקאות 9.1-9.4
14 חזרה לפני המבחן.	

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
- Joseph 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

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.