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. ידע בסיסי בהצפנה ופענוח.
2. לפתור בעיות של אותנטיקציה וזיהוי.
3. לזהות שלמות המידע.
4. ללמוד כלים הקשורים לשיתוף סודות, הסתרת מידע.
5. ללמוד נושאים הקשורים לאבטחת העברת ועיבוד המידע.

תוכן הקורס

שבוע	נושא	מקורות
1	**קריפטוגרפיה קלאסית**: קריפטו-מערכות וצפנים פשוטים. צופן ההזזה, צופן ההחלפה, צופן האפיני, צופן התמורה, צופן ויז'נר. קריפטו-אנליזה: אנליזה של הצופן האפיני, צופן ההחלפה וצופן של היל.	[1] פרק 2 פסקאות $2.1 - 2.2$.
2	**תורת שֶנוֹן של סודיות**: חזרה של תורת הסתברות בסיסית. בטיחות חישובית, בטיחות יחסית, בטיחות בלתי-מותנית. סודיות מושלמת. בטיחות סמנטית. אי-יכולת הבדלה בין הצפנות. התופן החד-פעמי.	[1] פרק 3 פסקאות $3.1 - 3.4$.
3	**צפני בלוק וצפני זרם**: רשתות החלפה-תמורה. תקן הצפנת הנתונים - data encryption standard (DES). תיאור DES וניתוח DES. תקן ההצפנה המתקדם - Advanced encryption standard (AES). תיאור AES וניתוח AES.	[1] פרק 4, פסקאות $4.1 - 4.6$.
4	**צפני בלוק וצפני זרם (המשך)**: התקפת אורקל ריפוד על אופן ההפעלה. אופן הפעלה של צופן בלוקים - block cypher mode (CBC). צופני זרם ושימושים. אוגרי הזזה לינאריים. הצפנה סימטרית והצפנה אי-סימרטית.	[1] פרק 4, פסקאות $4.7 - 4.8$.
5	**פונקציות תמצות קריפטוגרפיות**: פונקציות תמצות ואמינות המידע. בטיחות של פונקציות תמצות. מודל האורקל האקראי. אלגוריתמים במודל האורקל האקראי. השוואה בין קריטריוני בטיחות.	[1] פרק 5, פסקאות $5.1 - 5.2$.
6	**פונקציות תמצות קריפטוגרפיות (המשך)**: פונקציות תמצות איטרטיביות. הבנייה של מרקל-דמגרד (Merkle-Damgard). בניית ספוג ופונקציית התמצות SHA-3. קודמים לאורתנטיקציה של הודעות: MAC, מקונן, ו- HMAC.	[1] פרק 5, פסקאות $5.3 - 5.5$.
7	**פירוק מספרים**: קריפטוגרפיה של מפתח פומבי. תורת המספרים: משפט המספרים הראשוניים. קבוצת השארית מודולו p. שארית ריבועית מודולו p. אלגוריתם אוקלידי, משפט השארית הסיני. מבחנים ראשוניות. צופן רבין.	[1] פרק 6, פסקאות $6.1 - 6.2$.
8	**צופן RSA** : צופן RSA. מבחנים ראשוניות. האלגוריתם מילר-רבין לבדיקת ראשוניות. המושג של עד אמת ועד שקר. נקודות תורפה של צופן RSA. צופן רבין. בעיית הפירוק לגורמים.	[1] פרק 6, פסקאות $6.3 - 6.5$.
9	**קריפטוגרפיה של מפתח פומבי**: בעיית הלוגריתם הדיסקרטי. שיטות המפתח הפומבי. בעיית הלוגריתם הדיסקרטי. צופן אל-גמאל. הפרוטוקול דיפי-הלמן לקביעת מפתח משותף. חישוב משותף של הפרמטרים הפומביים. שימוש בערך המשותף.	[1] פרק 7, פסקאות $7.1 - 7.2$.
10	**קריפטוגרפיה של מפתח פומבי (המשך)**: פרוטוקול דיפי-הלמן מעל חבורה כללית. בעיית ההכרעה של דיפי-הלמן. שימוש בשארית ריבועית מודולו ראשוני p. שימוש בקריטריון אוילר. בטיחות השיטה ובעיות דיפי-הלמן.	[1] פרק 7, פסקאות $7.1 - 7.2$.
11	**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] פרק 8, פסקאות $8.2 - 8.5$.
12	**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] פרק 9, פסקאות $9.1 - 9.4$.
13	**חזרה לפני המבחן.**	

ספרי הקורס:

[1] טסה תמיר, מבו אל קריפטוגרפיה ,מדריך למידה בהוצאת האוניברסיטה הפתוחה, פברואר 20

מקורות נוספים:

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

[3] 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.

[4] C. Paar, J. Pelzl, "Understanding Cryptography: A Textbook for Students and Practitioners" (available online for SCE students), Springer, 2010.

[5] Baimel A., Dolev Sh., "Anonymous message delivery", Proceeding of FUN 2001

[6] Aumasson J-P, "Serious Cryptography. A practical introduction to modern encryption", No Starch Press, 2018

[7] Bashir I. "Mastering Blockchain", Packt Publishing Ltd., 2017

[8] "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.