המכללה
הטכנולוגית
באר שבע
בשיתוף WORLD ORT
קדימה מדע

המכללה הטכנולוגית באר שבע

מגמת לימוד: הנדסת תוכנה

סילבוס במקצוע קריפטוכרפיה

שיוך לבחינה ממלכתית מ.ה.ט – אין

פרטי מקצוע

קמפוס: באר שבע

התמחות: סייבר מגמות משנה:

שנת הלימוד: ב סמסטר: ב שנה קלנדרית: תשע"ט

מרצה: אלונה קוציי דוא"ל: alonhkoz@ac.sce.ac.il

רמת מקצוע: סטודנט לתואר הנדסאי

מתכונת הלימוד: שעור

דרישות קדם מקצועיות: אין

לימוד במקביל ל:

שפת הלימוד: עברית

מיקום לימוד: המכללה הטכנולוגית באר שבע

תאריך עדכון אחרון: 02/10/2018

מטרה מקצוע:

מטרת הקורס היא להבין כיצד ניתן ליישם טכניקות מתקדמות של תחום הקריפטוגרפיה. נלמד אלגוריתמי הצפנה שונים, יישומם, שימושם והתקפות עליהם.

תוצאות/הישגים בלימוד המקצוע:

ילמדו אפקטים יחודיים בקריפטוכרפיה.

ידעו לנהל אימות חתימה ושמירת מצב.

ידעו להבדיל בין התקפות שונות.

נושאי הלימוד:

שבוע/ות	נושא	מקראה/מקורות
1-2	אפקטים יחודיים באבטחת מידע	1
3-4	DES	1
5-6	AES	2
7-8	SHA	2
9-10	RSA	1
11-12	ElGamal	2
13-14	Diffie-Hellman	2

- יתכנו שינוים/תוספות בדגשים ובשבועות בהתאם להתקדמות הכיתה בפועל

מבנה הוראת המקצוע: מצגות

פעילות הלימוד:

- שעורים פרונטליים
- תרגול בכיתה
- הגשת מטלות בית

ציוד, חומרים ואמצעי עזר (לבוש, נעליים, סינור, שביס) - אין

הערות כלליות:

- יש להדגיש שחומר הלימוד כולל את כל המקורות/ההפניות/ההשלמות ולא רק החומר בכיתה.
- בעבודות התקדמות יש להדגיש הגשות בזמן ולהציג שלבי התקדמות (בזמנים מוגדרים).
- יש להדגיש מטלות הגשה הקובעות זכאות לבחינה/ציון מקצוע.
- סטודנט שנקטע רצף ההגשות – ממשיך/מאבד זכותו להשתתף בשעורי המקצוע.
  מתכונת ההגשה אישית
- יש להדגיש חסימה במקרה של כשלון

ספרים ומקורות ביבליוגרפיים:

מחבר	כותר	שנת הוצאה/מהדורה	הוצאה לאור
1. Paar	Understanding Cryptography	2012	Prentice Hall
2. W. Stallings	Network Security	2006	Prentice Hall

המכללה
הטכנולוגית
באר שבע
בשיתוף WORLD ORT
קדימה מדע

מקורות אינטרנט : אין

חובות מקצוע והרכב הציון:

הרכב הציון :

פרוייקט : 60% - חובת הגשה

בוחן : אין

הגשת תרגילים : 40% - חובת הגשה

התניות : שקלול הגשת התרגילים והבוחן בתנאי ציון עובר(מינימום 55) בבחינת סמסטר.

חובת נוכחות 80% מינימום

הצגת אישורי ש.מ.פ./אשפוז/מחלה ממושכת למנהל הסטודנטים בזמן.