תאריך עדכון: 25.8.2018

שם ומספר הקורס:

סמינריון נושאים בקריפטוגרפיה יישומית

Seminar: topics in applied cryptography

89-4371-01

סוג הקורס: סמינר

שנת לימודים: תשע"ט **סמסטר**: ב' **היקף שעות**: 2 ש"ש

אתר הקורס באינטרנט:

א. מטרות הקורס (מטרות על / מטרות ספציפיות):

קריפטוגרפיה הינה כלי המשמש לאבטחת מידע במערכות ממוחשבות. מערכות מבוססות קריפטוגרפיה נמצאות בשימוש יומיומי בידי מיליארדי בני אדם, הן להגנה על מידע אשר מאוחסן בצורה סטטית והן להגנה על מידע במהלך הרצת פרוטוקולי תקשורת בין שני שחקנים או יותר.
במסגרת הסמינר נעסוק ביישומים מעשיים של כלים קריפטוגרפיים לצורך פתרון בעיות בעולם האמיתי.
המטרה המרכזית של הסמינר הינה להבין אלה אתגרים מעמיד עולם הסייבר כעת בפני הקריפטוגרפיה, ומהם הפתרונות המוצעים להם.

ב. תוכן הקורס:

מהלך השיעורים: השיעורים יועברו על ידי הסטודנטים, פרט לשיעורים הראשונים שיועברו על ידי המרצה וישמשו מבוא לנושאים אשר יילמדו במהלך הסמסטר.

תכנית הוראה לכל השיעורים:
השיעורים הראשונים ינתנו על ידי המרצה ויכללו חזרה כללית על הנושאים הבאים:

- הגדרות של סכמת הצפנה
- הצפנה סימטרית – הגדרה ומימוש בעולם האמיתי (AES)
- הצפנה א-סימטרית – הגדרות ויישומים
- אותנטקיציה
- פונקציות HASH – הגדרה ושימושים
- פרוטוקולים קריפוגרפיים- דוגמאות ויישומים.

בהמשך הסמינר יילמדו מאמרים מתקדמים אשר התפרסמו לאחרונה בכנסים המובילים בנושאי אבטחת מידע ואשר מתמקדים בשימוש בקריפטוגרפיה לצורך פתרון בעיות אבטחת מידע או בהתאמת מערכות קריפטוגרפיות קיימות לצרכים מעשיים.

ג. חובות הקורס:

דרישות קדם: מבוא לקריפטוגרפיה/ תכנות בטוח ואבטחת תקשוב או בתיאום עם המרצה.

חובות / דרישות / מטלות: העברת הרצאה בנושא מסוים (ראוי להדגיש כי מאמרים אקדמיים אינם בהכרח שלמים, ולעיתים נדרשת גם קריאה של חומר רקע נוסף כדי להגיע להבנה מלאה של הנושא).

מרכיבי הציון הסופי: 90% - ציון להרצאה, 10% - נוכחות בהרצאות.

הציון להרצאה יינתן על סמך ההצגה של כל סטודנט אשר צריכה לכלול את הנקודות הבאות:

- הצגת הרקע לנושא בו עוסקת ההרצאה.
- הצגת הבעיה אשר המאמר מנסה לפתור ברמה האינטואיטיבית, והסבר של מה נעשה עד כה בנושא (מאמרים קודמים וכדומה).
- תיאור פורמלי של הבעיה באמצעות ההגדרות המתמטיות בהן משתמש המאמר.
- תיאור הפתרון המוצע במאמר תוך הסבר על ההבדל בין הפתרון לפתרונות אחרים שהוצעו בעבודות קודמות. הוכחות ניתן לתאר באופן כללי בלבד מבלי להיכנס לכל הפרטים.

ד. ביבליוגרפיה: (חובה/רשות): מאמרים עדכניים בתחום (הפירוט יינתן בתחילת הסמסטר).