אוניברסיטת בן-גוריון בנגב
הפקולטה למדעי הטבע - המחלקה למדעי המחשב
סמסטר ב' תשע"ז

סילבוס קורס

שם הקורס בעברית: קריפטוגרפיה 2

שם קורס באנגלית: Cryptography 2

מס' קורס: 202-2-4891

סוג קורס: קורס חובה למסלול לאבטחת המרחב המקוון וקורס בחירה לתואר שני ושלישי

נק"ז: 2 נק"ז

מרצה הקורס: פרופ' עמוס ביימל

דרישות קדם: קריפטוגרפיה 202-2-5871 או קריפטוגרפיה שימושית 202-2-5821

סילבוס בעברית

מטרת הקורס היא לתת לסטודנטים ידע בסיסי על הבסיס המדעי של בניית מערכות קריפטוגרפיות. נושאי הקורס יכללו:

1. פונקציות חד כיווניות וגנרטורים פסאודו-אקראיים.
2. מערכות הצפנה: הגדרות פורמאליות ובניות.
3. הוכחות באפס מידע.
4. נושאים מתקדמים בקריפטוגרפיה כגון חישוב בטוח

סילבוס באנגלית

The goal of this course is to provide the scientific basis on the construct ion of cryptographic systems. The topics covered in this course iare:
1. One-way functions and pseudorandom generators.
2. Encryption systems: definitions and constructions.
3. Interactive proofs and zero knowledge.
4. Advanced topics in cryptograph, e.g., secure multiparty computation.

מטרת ונושא הקורס

הקורס מיועד לסטודנטים שלמדו כבר קורס בסיסי בקריפטוגרפיה. מטרתו היא לתת לסטודנטים את הרקע המדעי של תכנון מערכות קריפטוגרפיות, החל בהגדרות הפורמאליות של בטיחות, הנחות מינימאליות בקריפטוגרפיה, בניית מערכות על סמך ההנחות והוכחת הנכונות שלהם. הקורס יכין את הסטודנטים למחקר בקריפטוגרפיה.

נושאי ההרצאות

1. **פונקציות חד כיווניות – הגדרות ותכונות**
2. **בניית גנרטורים פסאודו-אקראיים ומערכות הצפנה מפרמוטציות חד כיווניות.**
3. **מערכות הצפנה: הגדרות פורמאליות ובניות.**
4. **הוכחות באפס מידע.**
5. **נושאים מתקדמים בקריפטוגרפיה כגון חישוב בטוח**

<u>דרישות הקורס</u>

השתתפות חובה
תרגילי בית

<u>מרכיבי ציון הקורס</u>

- **מבחן 50%**
- **תרגילי בית 50%**

<u>ספרות הקורס</u>

- **Jonathan Katz and Yehuda Lindell. Introduction to Modern Cryptography. Chapman & Hall/Crc Cryptography and Network Security Series, Second Edition, 2014.**

- **Oded Goldreich. Foundations of Cryptography - Volume 1 (Basic Tools). Cambridge University Press, 2001.**