



# יום עיון בקריפטולוגיה

הפקולטה למדעי המחשב, הטכניון, חיפה

יום ג', 7 ביולי, 2009

## תוכנית יום העיון:

התכנסות, כיבוד קל	12.30
פרופ' מוני נאור, מכון ויצמן למדע Public-Key Cryptosystems Resilient to Key Leakage	13.00
פרופ' אמיר הרצברג, אוניברסיטת בר-אילן Degradation Attacks on Secure Channels	13.50
הפסקה	14.40
פרופ' טל מור, הטכניון Quantum Key Distribution (QKD) with classical Alice	15.10
דר' בני פנקס, אוניברסיטת חיפה Implementing Secure Multi-Party Computation	16.00
הפסקה	16.50
ניב כרמלי, הטכניון Bug Attacks	17.00
סיום	17.50

ההרצאות תתקיימנה בעברית  
 יום העיון יתקיים בטכניון בחיפה, בנין טאוב, אולם 337  
 ההשתתפות ביום העיון חופשית, אנא הרשמו מראש באתר  
 תתאפשר כניסה עם רכב לטכניון  
 לפרטים נוספים ובירורים: yanivca@cs.technion.ac.il

www.cs.technion.ac.il/~yanivca/cryptoday