



# יום עיון בקריפטולוגיה

הפקולטה למדעי המחשב, הטכניון, חיפה  
יום ד', 9 ביוני, 2010

## תוכנית יום העיון:

	09.00	התכנסות, כיבוד קל
	09.30	דר' אור דונקלמן, מכון ויצמן למדע The Not So Happy Ending of the AES' Security Fairytale
	10.25	דר' כרמית חזאי, מכון ויצמן למדע והמרכז הבינתחומי On Compression of Data Encrypted with Block Ciphers
	11.15	הפסקה והצגת פוסטרים
	11.50	דר' אלון רוזן, המרכז הבינתחומי Cryptographic Elections – Challenges and Opportunities
	12.40	הפסקה
	13.40	דר' דן צפריה, הטכניון Portably Preventing File Race Attacks with User-Mode Path Resolution
	14.30	פרופ' רן קנטי, אוניברסיטת תל-אביב Program Obfuscation: A Cryptographic Viewpoint
	15.20	פרופ' אבישי וול, אוניברסיטת תל-אביב RFID-Based Electronic Voting: What Could Possibly Go Wrong?
	16.10	סיום

ההרצאות תחיימנה בעברית. תחאפשר כניסה עם רכב לטכניון  
יום העיון יתקיים בטכניון בחיפה, בניין טאוב, אודיטוריום 1  
ההשתתפות ביום העיון חופשית, אנא הרשמו מראש באתר  
סטודנטים מוזמנים להציג תוצאות מחקריות בפוסטרים. פרס כספי יוענק לפוסטר הטוב ביותר  
פרטים נוספים באתר  
יום העיון נערך בחסות מפא"ת

[www.cs.technion.ac.il/~yanivca/cryptoday](http://www.cs.technion.ac.il/~yanivca/cryptoday)