

הנושא: חדשות

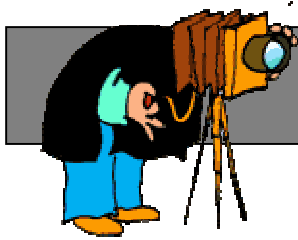
מערכת על"ה/חמוטל דוד ובתיה עמית. הוכן ע"י:

תקציר:
חדשות המתמטיקה: בחלקו הראשון של המדור כתבה העוסקת במספרי RSA, להן תפקיד חשוב בתורת ההצפנה בעקבות גילוי הפירוק של המספר RSA-640 בן 193 הספרות למכפלה של שני ראשוניים בעזרת מחשב. בחלקו השני של המדור דיווח על הזכייה של פרופסור ישראל רוברט אומן ממכון איינשטיין למתמטיקה ומהמרכז לחקר הרציונליות באוניברסיטה העברית בירושלים בפרס נובל לכלכלה לשנת 2005. פרופ' אומן זכה בפרס יחד עם עמיתו פרופ' תומס ס' שלינג מאוניברסיטת מרילנד בארה"ב על תרומתם להבנה של תהליכי סכסוך ושיתוף פעולה באמצעות תורת המשחקים.

מילות מפתח:
כתב העת על"ה, על"ה 35, חדשות, מספרי RSA, תורת המספרים, תורת הצפינה, מספרים ראשוניים, מספרים פריקים, פרס נובל, פרופ' ישראל אומן, כללי.

החומר פורסם במסגרת: על"ה 35, תשס"ו 2005, עמודים 4-5.

החומר מכיל בנוסף לעמוד הפתיחה: 2 עמודים.



חדשות

מספרי RSA

RSA-576 שהוא בן 174 ספרות ולפני כן את הפירוק למספר RSA-200 בן 200 ספרות. הקבוצה השתמשה באלגוריתם מיוחד, אשר מחשב משוכלל הפעיל במשך שלושה חודשים. הפירוק שהתקבל עבור RSA-640 הוא:

1,634,733,645,809,253,848,443,133,883,865,
090,859,841,783,670,033,092,312,181,110,852,
389,333,100,104,508,151,212,118,167,511,579
X

190,087,128,164,822,113,126,851,573,935,
413,975,471,896,789,968,515,493,666,638,539,
088,027,103,802,104,498,957,191,261,465,571

בדיקת הנכונות של הפירוק היא כמובן משימה פשוטה מאד. כופלים וזהו.

יצוין כי המספר המופיע בשם של מספר RSA מציין את מספר הספרות הנחוץ לכתבתו בבסיס בינארי או בבסיס עשר. לעובדה זו סיבה היסטורית. מספר RSA הגדול ביותר, אשר בשמו מופיע מספר ספרותיו בכתב עשרוני, הוא RSA-200. כל מספרי RSA שניצב עדיין פרס למציאת פירוקם מכילים בשם המספר את מספר הספרות הנחוץ לכתבתם בבסיס בינארי.

כאמור, מספרי RSA נוספים מחכים לפירוק ופרס כספי נאה מובטח לחוקר העקשן והעקבי שימצא את הפירוק. בטבלה הבאה מפורטים סימניהם, מספר הספרות הנחוץ לכתבתם בבסיס עשר וגודל הפרס.

פרס כספי	מספר ספרות	שם המספר
30,000\$	212	RSA-704
50,000\$	232	RSA-768
75,000\$	270	RSA-896
100,000\$	309	RSA-1024
150,000\$	463	RSA-1536
200,000\$	617	RSA-2048

קבוצת חוקרים מהסוכנות הפדראלית הגרמנית לאבטחת מידע טכנולוגי הודיעה בנובמבר 2005, כי מצאה בעזרת מחשב את הפירוק לגורמים של מספר בן 193 ספרות, המוכר בכינוי: RSA-640 וכמספרי RSA נוספים הוכרו פרס כספי נאה למוצא את פירוקם. המספר הוא:

3,107,418,240,490,043,721,350,750,035,888,
567,930,037,346,022,842,727,545,720,161,948,
823,206,440,518,081,504,556,346,829,671,723,
286,782,437,916,272,838,033,415,471,073,108,
501,919,548,529,007,337,724,822,783,525,742,
386,454,014,691,736,602,477,652,346,609

מספרי RSA הם מספרים "כמעט ראשוניים" כלומר מספרים הניתנים להצגה כמכפלה של שני מספרים ראשוניים בלבד. בשל כך פירוקם לגורמים ראשוניים קשה עד מאד. שמם ניתן להם, בשנת 1977, בהיותם אבן הפינה לאלגוריתם הראשון בתורת ההצפנה המודרנית שנודע בשם אלגוריתם RSA – האותיות הראשונות של שמותיהם של שלושת מפתחיו: רון ריבסט (R), עדי שמיר (S) ולן אדלמן (A). באלגוריתם זה המצפין משתמש במספר פריק גדול, המהווה מכפלה של שני מספרים ראשוניים השמורים עימו, ומעביר מסר מוצפן וקשה מאד לפיצוח (ויש אומרים, בלתי ניתן לפיצוח בזמן חיים סביר). כדי לפצח את הצופן יש למצוא שיטה לפרק את המספר הגדול לגורמים ראשוניים. חוקרים העוסקים בתורת ההצפנה מחפשים הן אלגוריתמים להצפנה והן אלגוריתמים לפענוח צפנים. עדיין לא נמצא אלגוריתם לפירוק מספרי RSA לגורמים, אך גם לא הוכח כי אלגוריתם כזה אינו קיים. ידוע רק שהמלאכה קשה עד מאד אפילו למחשבי על.

קבוצת החוקרים, שמצאה את הפירוק של המספר הנזכר, מצאה במאי 2005 את הפירוק של המספר

להרחבת הידע ניתן לעיין למשל:

[Edward B. Burger and Michael Starbird \(2005\). The heart of Mathematics – An invitation to effective thinking Key College Publishing, California. pp. 95-109](#)
<http://mathworld.wolfram.com/news/2005-11-08/rsa-640>
<http://en.wikipedia.org/wiki/RSA>
<http://www.rsasecurity.com/rsalabs/node.asp?id=2093>

נובל ! 2005 !

האקדמיה המלכותית השבדית למדעים הודיעה על ההחלטה להעניק את פרס נובל לכלכלה לשנת 2005 לפרופ' ישראל רוברט אומן ממכון איינשטיין למתמטיקה ומהמרכז לחקר הרציונליות באוניברסיטה העברית בירושלים ולעמיתו פרופ' תומס ס' שלינג מאוניברסיטת מרילנד בארה"ב. בנימוקיה קבעה ועדת הפרס כי הם העמיקו את הבנתנו בסכסוך ובשיתוף פעולה באמצעות ניתוח של תורת המשחקים.

שניהם השתמשו ברעיונות בסיסיים שנבנו על-ידי קודמיהם ובנו מודלים מורכבים יותר המשפיעים על מצבים מחיי היום יום. עבודתם השפיעה ישירות על הבנת הדינאמיקה במרוץ החימוש הגרעיני ובהבנה הנוכחית של מצבי קונפליקט ושיתוף פעולה בכלכלה ובמדעי החברה.

פרופ' אומן נולד בשנת 1930 בפרנקפורט, גרמניה. בשנת 1955 קיבל תואר דוקטור מהמכון הטכנולוגי של מסצ'וסטס MIT. פרופ' אומן הוא חבר הסגל האקדמי באוניברסיטה העברית משנת 1956, כתב כמאה מאמרים מדעיים ושישה ספרים ; חתן פרס ישראל

לחקר הכלכלה לשנת תשנ"ד וחתן פרס אמ"ת לשנת 2002. פרופ' אומן הוא מתמטיקאי בעל שם בין-לאומי ונודע כחוקר בתחום תורת המשחקים. בהודעתה על הענקת הפרס ציינה האקדמיה המלכותית השבדית, "רוברט אומן היה הראשון לפתח ניתוח רשמי פֶּשֶל של מה שקרוי האין סופיות של משחקים חוזרים. הניתוח שלו זיהה בדיוק אלו תוצאות עשויות להתחזק במערכות יחסים ארוכות טווח".

פרסי נובל כבר הוענקו בעבר לישראלים הבאים: ש"י עגנון, חתן פרס נובל לספרות לשנת 1966, מנחם בגין, חתן הפרס לשלום לשנת 1978 (יחד עם נשיא מצרים אנואר סאדאת). יצחק רבין ושמעון פרס חתני פרס נובל לשלום לשנת 1994 (יחד עם יאסר ערפאת). דניאל כהנמן (חי בארה"ב), חתן פרס נובל לכלכלה לשנת 2002. אהרון צ'יחנובר ואברהם הרשקו חתני פרס נובל לכימיה לשנת 2004. דוד גרוס (חי בארה"ב), חתן פרס נובל לפיסיקה לשנת 2004.

תורת המשחקים היא תחום ידע מתמטי המספק מודלים להבנת מצבים של קונפליקט, ומיושמת לצבאיות ולתהליכים במדעי המדינה ובמדעי החברה.

הבסיס לתחום הונח ב-1940 ע"י ג. ון-ניומן וא. מורגנשטיין. מאוחר יותר, התפתח התחום באופן ניכר ע"י חתן פרס נובל המתמטיקאי ג'ון נאש ואחרים. ב-1950 וב-1960 בהיות המלחמה הקרה בעיצומה ובשל התפתחות עולמית בקפיטליזם, התעורר צורך עז בלימוד קפדני של שיטות התנהגות במצבים שבהם קונפליקט מגביר לחצים.

לקריאה נוספת:

[/http://nobelprize.org](http://nobelprize.org)

<http://www.huji.ac.il/huji/nobel/israel.htm>

ליקוט ועריכה: חמוטל דוד ובתיה עמית