הסיוט של חברות הסלולר

פרופ׳ ביהם (מימין) והדוקטורנט ברקן, השבוע בטכניון. ״כל העניין הוא משחק ילדים״
תצלום: טל כהן

פרופ' אלי ביהם מהטכניון, שפיצח עם שני תלמידיו הצעירים את צופן רשת הטלפונים הסלולריים הנפוצה בעולם "ג'י־אס־אם", הוא דמות נערצת בטכניון ● כשהתלמיד ברקן גילה את הפירצה, ביהם לא האמין: "זה היה טיפשי מדי מצד המתכננים לעשות כזו טעות" ● ביהם, שסולק מבית־הספר בגיל 16, כבר סייע בעבר לפצח צופן בנקאי מאובטח ● "בעתיד נפצח עוד צפנים, בעיקר כאלה שבעליהם טוענים ביהירות שהם בלתי פציחים"

דודי גולדמן

תגיד, אתה יכול לשים אצבע בין שני עמודים עוקבים בספר?", שואל אותי פרופ' אלי ביהם מהטכניון, האיש שפיצח, יחד עם שניים מתלמידיו, את צופן רשת הטלפונים הסלולריים הפופולרית בעולם, "ג'י־אס־אם".

אני לא מבין את השאלה ומנסה להרוויח קצת זמן. מה פירוש מספרים עוקבים, אני שואל. "נגיד 79 ו־80 הם שני מספרים עוקבים, הוא עונה עם ניצוץ זדוני בעיניים. "כל העניין פשוט מאוד: לוקחים דף, ובאמצעות סכין יפאני חותכים אותו לשניים, וכך אני שם אצבע בין שני עמודים עוקבים. זה מה שהיה צריך להוכיח". הוא צוהל כמו ילד שהצליח לבצע טריק חדש.

לפרופ' אלי ביהם, 41, יש סיבות טובות לצהלה. למשל, פיצוח צופן רשת הטלפונים הסלולריים המאובטחת ביותר, GSM. יותר מ־850 מיליון בני־אדם ברחבי העולם משתמשים בטכנולוגיית התקשורת הסלולרית הזו, כ־71 אחוז מכלל משתמשי הסלולרי בעולם. שימוש זדוני בטכנולוגיה הזו יכול ליצור אנדרלמוסיה: אפשר יהיה לצותת למאות מיליוני הטלפונים הסלולריים. אין סיוט גדול מזה עבור חברות הסלולר. למעשה, הדרך היחידה שלהן להתמודד עם חשיפת הקוד היא להחליף את כל המכשירים הסלולריים.

פרופ' אלי ביהם מגחך כשאומרים לו שכל העולם מדבר על הצופן החדש. על השאלה איפה מאוחסן המידע על פיצוח השיטה, הוא עונה בחיוך: "במקום בטוח. פירסמנו את זה בכנס מקצועי בסנטה ברברה, וכל אחד שמכבד את עצמו בתחום קרא את המאמר".

— עבור אנשים מסויימים הצופן הזה יכול להיות שווה הון־עתק. כשהצופן בידיך, אתה עשוי להיות אדם מבוקש למדי עבור עבריינים ו/או שירותי ביון.

פרופ' ביהם מגחך. "אני לא חושש, וכדאי לה־בהיר, מדובר באלפי נוסחאות מתמטיות".

— למה לא מברתם את השיטה לשוק הפרטי?

"בוא ננתח מה זה השוק הפרטי בתחום הזה: פושעים ואנשים בעלי כוונות לא טהורות, כאלה שרוצים לרגל אחר שיחות לא להם. ברור שיכולנו למכור להם בהרבה כסף, אבל לא, תודה. אין סיכוי. זה גם לא עלה על דעתנו".

"ברור שיכולנו למכור את השיטה לשוק הפרטי בהרבה כסף, אבל לא תודה", אומר פרופ' ביהם. "מה זה השוק הפרטי בתחום הזה? פושעים ואנשים שרוצים לרגל אחר שיחות לא להם"

"יום אחד", משחזר ברקן, "באתי לפרופ' ביהם ואמרתי לו, 'תגיד, יכול להיות שצופן הסלולר הזה כולל בתוכו כשל אבטחה לוגי כזה'. הוא ענה לי: 'אין סיכוי, אבל תבדוק שוב'"

אלעד ברקן: "מגיל צעיר זה נראה לי פלא, האפשרות להסתיר מידע שכולם יכולים לשמוע אותו. כילד הייתי חולה על קסמים, ופיצוח צפנים בשבילי זה קסם. בכלל, במקרים רבים מתמטיקה היא שעשוע"

טעות טיפשית מדי

פרופ' אלי ביהם הוא דמות נערצת במיוחד בטכניון. מאות סטודנטים שוחרים אל שיעורי המתמטיקה וההצפנה שלו. אבל הקורסים המתקדמים מאוד, כמו סמינריונים באוניברסיטה, אלה המתאימים למרכשרים ביותר בתחום הזה של פיצוח והצפנה, כוללים לעתים לא יותר מארבעה תלמידים. זה לא מפריע לביהם להקדיש לקורסים האלה זמן רב, ולהשתובב עם תלמידיו. מאחד הקורסים הללו יצאה הבשורה על פיצוח הצופן הסלולרי.

הדוקטורנט אלעד ברקן והחוקר נתן קלר, כיום חייל בצה"ל, הם שני התלמידים השותפים לפיצוח. שניהם בוגרי מסלול המצויינות של הטכניון. "יום אחד", משחזר ברקן, בן 28, "שאלתי את אלי אם יית־כן שצופן ה־GSM כולל בתוכו פונקציה מסויימת, שבמקום לפעול אחרי השיחה בטלפון, היא מופיעה לפני השיחה, ולכן יש כאן כשל אבטחה לוגי.

"אלי ירה לעברי: 'לא. אין סיכוי כזה. זה יהיה טיפשי מצידם לעשות כזו טעות. אבל היי, תבדוק שוב'. בדקתי שוב, וחזרתי אליו. הוא אמר לי, 'תבדוק שוב, ותחזור כשתהיה בטוח'. וכך היה".

החוקרים הישראלים, מתברר, גילו חולשה יסודית במערכת ההצפנה של הטכנולוגיה, שלא היתה ידועה קודם. פיתוח הצופן התבסס על ניצול החולשה הזו. "הצופן הזה היה סוד כמוס עד שברקן מצא את התקלה החמורה במערכת האבטחה", אומר פרופ' ביהם. "הוא מצא שהרשת עובדת בסדר לא נכון — קודם היא 'מנפחת' את המידע העובר בה, כדי לתקן רעשים, ורק אחר־כך מצפינה אותו. הם עשו טעות, אני לא יודע להסביר אותה. זה איפשר לנו לפתח שיטת פריצה, שעובדת בחלקיק שנייה על נתונים שאנחנו שומעים בשידור אלחוטי, בלי צורך בשום דבר אחר".

קסמים וניצוח צפנים

המחקר של פרופ' ביהם ותלמידיו נשלח לארגון ה־GSM העולמי לצורך תיקון הבעיה, והשיטה נרשמה כפטנט שיוכל בעתיד לשמש את רשויות החוק. החוקרים מבהירים, כי לא יפרסמו את תוצאות המחקר ברבים ויחשפו אותו רק בפני רשויות החוק, וגם זה עבור תשלום.

הדוקטורנט ברקן אומר שהפיצוח לא היה מקרי. כתיכוניסט הוא זכה במקום השני בתחרות ארצית לפיזיקה של כל בתי־הספר התיכוניים. לאחר שיחרורו מהצבא התקבל לתוכנית המצויינות של הטכניון במסלול ישיר לדוקטורט. "האווירה בשיעורים של פרופ' אלי ביהם היא מדהימה", הוא אומר. "אנחנו, כמה סטודנטים ביחד, יושבים על פיצוח צפנים. זה ממש כיף, כמו משחק ילדים מרתק".

— ממתי אתה מתעניין בהצפנה?

ברקן: "מאז ומעולם. מגיל צעיר זה נראה לי פלא, האפשרות להסתיר מידע, למרות שכולם יכולים לשמוע אותו — אבל לא להבין. בצד השני יש מישהו ששומע ומבין. זה ממש קסם בשבילי, עניין הקריפטולוגיה (תורת פיצוח הצפנים) המודרנית. כילד הייתי חולה על קסמים. עד היום. אנחנו יושבים במשרד של אלי בטכניון, והוא תמיד מתקיל אותנו בכל מיני שאלות שעשוע, שנשמעות כמו בדיחה, אבל בעצם הן סוג של חשיבה מדעית פורצת־דרך. החיים שלנו, של אלי והסטודנטים, הם ממש משחק. בכלל, במקרים רבים מתמטיקה היא שעשוע".

השותף השלישי לפיצוח, נתן קלר, עלה לישראל מרוסיה כילד בן 8 ומיד נרשם לחוגי נוער שוחר מדע בטכניון. הוא נער דתי־חרדי, חובש כיפה שחורה ומגדיר את עצמו כ"חרד"לי" (חרדי־דתי־לאומי). הוא משרת כעת בצבא במסגרת ישיבות ההסדר.

"זה, כנראה, לא הצופן האחרון שהם יפצחו", אומר פרופ' ביהם על תלמידיו. "יש לי הרגשה שהעתיד צופן לנו פיצוח צפנים נוספים, בעיקר כאלה שבעליהם טוענים ביהירות שהם בלתי פציחים".

הפטנט של רופרט מרדוק

ימיה של ההצפנה עתיקים כמעט כימיה של ההיסטוריה הצבאית. שיטת הצפנה פשוטה, שכמעט כל ילד מכיר, היא כתיבה באמצעות בצל חי על דף נייר. רק מי שמכיר את שיטת ההצפנה יודע, שיש להביט על הנייר הריק מעל אש כדי לראות את הכתוב. אם לא – הדף ייראה נקי.

שיטות ההצפנה שוכללו באירופה בתקופה שבין שתי מלחמות העולם. במלחמת העולם השנייה הפעילו הגרמנים מכונת הצפנה, "אניגמה", שנחשבה למשוכללת ביותר ולבלתי ניתנת לפיצוח. בדרך עקלקלה הגיעה המכונה הגרמנית למתמטיקאי האקצנטרי והגאון, אלן טיורינג, שבעזרת צוות של מתמטיקאים באנגליה, הצליח לפצח את סודותיה, מה שעזר לבעלות־הברית להגיע להכרעה בצפון אפריקה נגד כוחות גרמניה בפיקודו של רומל.

מאז, הקריפטולוגיה היא חלק מלימודי המתמטיקה השימושית, ומתמחים בתחום, כמו פרופ' עדי שמיר, מרוויחים כסף רב ממכירת אלגוריתמים (נוסחאות) להצפנה. וכיצד מוכרים אלגוריתם הצפנה חדש? דרך קיעקוע הקיים. אחרת, אף תאגיד־על, סלולרי או אחר, לא יקנה במיליונים רבים של דולרים אלגוריתם הצפנה חדש.

איל התקשורת רופרט מרדוק עשה מההצפנה הון. החברה שלו, NDS, מפתחת ומייצרת ממירים וקופסאות חכמות, שהם למעשה מפענחים. הטכניקה הזו מאפשרת לגבות כסף תמורת צפייה בשידורי טלוויזיה מקודדים. כך פועלת הטלוויזיה הדיגיטלית, בכבלים ובלוויין.

אין לימודים, יש מדע

אלי ביהם, גרוש ואב לשתי בנות, גדל במשפחה ממוצא צ'כי ביישוב חופית, מול בית־ינאי. ילד אמצעי בין אח גדול, כיום פרופסור לפיזיקה באוניברסיטה העברית בירושלים, לבין אחות קטנה. הוא מעיד על עצמו, שכילד לא מצא שקט והשתעמם בשיעורים, עד תחילת כיתה י"א. "חודש לאחר תחילת הלימודים", הוא משחזר, "אמר לי סגן מנהל התיכון האזורי, שכנראה עליתי על העצבים שלו, שלא אחזור לבית־הספר בלי ההורים. אוקיי, אמרתי, ולא חזרתי".

הנער חסר־המנוח חדל להגיע לבית־הספר, אבל בילה שעות בחוגי נוער שוחר מדע של אריקה לנדאו בתל־אביב. "זה היה כיף, אצלה אף פעם לא שיעמם. בזכותה הלכתי עוד כנער לאוניברסיטת תל־אביב להרצאות ולשיעורים שעניינו אותי. לימים, חלק מהקורסים האלה נחשבו לי בניקוד לתואר ראשון".

עוד לפני שהיתה לו תעודת בגרות, סיים ביהם תואר ראשון במתמטיקה ובמדעי המחשב, התגייס לצה"ל ושירת ביחידת מחשבים מסווגת בחיל האוויר. לאחר שיחרורו למד מתמטיקה במסלול הישיר לדוקטורט במכון ויצמן למדע, אצל פרופ' עדי שמיר, הקריפטולוג הישראלי הידוע ביותר, שאף זכה בפרס טיורינג (ע"ש אלן טיורינג), אבי המחשב המודרני, פרס הנחשב ל"נובל של המתמטיקה השימושית".

בשנת 91' פיצחו יחד התלמיד ביהם והמורה שמיר את הציפן DES. ששימש כצופן מאובטח מאוד בבנקאות, כולל בכל מכשירי הכספומטים. הפיצוח חולל רעש עצום במערכת הבנקאית. לימים, פרופ' שמיר מצא דרך לפצח את הכרטיס החכם של טלוויזיות דיגיטליות, ומכר שיטת קידוד בלתי ניתנת לפיצוח (בינתיים) לרופרט מרדוק.

פרופ' ביהם מספר שפיצוח השיטה הסלולרית ארך כשנה. "מאז שאלעד גילה שם תקלה מבנית ועד שפיצחנו את הכל עברה בערך שנה, אבל אנחנו ממשיכים לפצח דברים אחרים".

— קודים סלולריים אחרים?

"לא חושב. הקוד שפיצחנו נחשב בין המוגנים והטובים בעולם הסלולרי, ואני אומר לך, שהוא עדיין בהחלט טוב. השיטות האחרות, ולא הייתי רוצה לפרט וליצור בהלה, אינן טובות יותר. להיפך. כך שאין כאן אתגר גדול לפצח אותן". ■