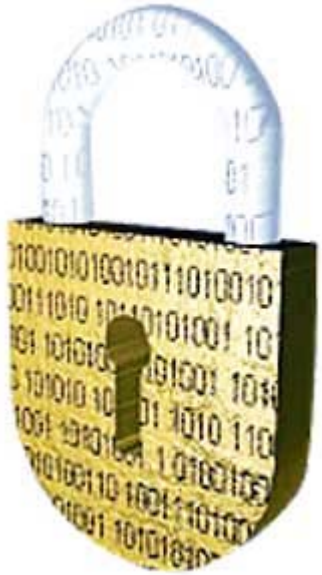
המספרים הראשוניים יזוהו, הצופן יישבר

מאת אוריאל בריזון

אלגוריתם המאפשר לקבוע בוודאות אם מספר הוא ראשוני עשוי לרוקן מתוכן את אחת משיטות ההצפנה המובילות בעולם, שרווחת מאוד באינטרנט



שלושה מדעני מחשב הודים טוענים שפיתחו שיטה חדשה, המאפשרת לקבוע אם מספר הוא ראשוני או לא. ייחודה של השיטה הוא שאפשר לבדוק באמצעותה גם מספרים גדולים מאוד, ואם היא אכן פועלת, כפי שסבורים מתמטיקאים מובילים שבדקו אותה, היא תוכל לשמש אמצעי יעיל לשבירת צפנים דיגיטליים.

שלושת המדענים - מנינדרה אגרואל, ניראג׳ קאיאל וניטין סקסנה מהמכון ההודי לטכנולוגיה בעיר קנפור - מצאו לטענתם אלגוריתם המאפשר לקבוע, במהירות ובוודאות מוחלטת, אם מספר מסוים הוא ראשוני. למספרים ראשוניים חשיבות עצומה בכל הקשור להצפנת מסרים דיגיטליים, ורוב מנגנוני ההצפנה המשמשים שירותים חשאיים, ארגונים גדולים וגופים אחרים הנזקקים לסודיות, מבוססים עליהם. כדי לפצח את ההצפנה יש למצוא מספרים ראשוניים גדולים. השיטות הקיימות כיום לקביעת ראשוניותם של מספרים הן אטיות מדי או שאינן ודאיות. בשיטות הללו המחשבים החזקים ביותר נדרשים לעבוד במשך חודשים ואף שנים כדי לבדוק ראשוניות, מה שהופך את כל העניין ללא כדאי. מצד אחר, מחיר קיצור הזמן הוא תוצאות שאינן חד-משמעיות - פתרון בעייתי לא פחות.

מספרים ראשוניים הם מספרים שאינם מתחלקים ללא שארית בשום מספר, פרט לעצמם ולאחד. המספרים הראשוניים הקטנים (1, 2, 3, 5, 7, 11, 13, 17, 19, 23, ...) הם ראשיתה של רשימה מורכבת ביותר. חקר פיזורם של המספרים הראשוניים על ציר המספרים העסיק מתמטיקאים ביוון העתיקה, והוא ממשיך להעסיק מתמטיקאים גם כיום. כדי לקבוע אם מספר הוא ראשוני יש לוודא כי אין לו גורמים פרט לאחד ולעצמו. פעולה זו פשוטה במספרים קטנים, אך ככל שהמספר הנבדק גדול יותר הופכת המשימה לקשה ביותר, עד כדי כך שגם מחשבי-על לא יכולים לבצע אותה. לדוגמה: הדפדפן הפופולרי "אקספלורר" של מיקרוסופט מגיע כיום כשהוא מצויד ביכולת הצפנה של 128 ביט. פריצת הצפנה זו מחייבת לבדוק את ראשוניותם של מספרים בסדר גודל של 39 ספרות. גם למחשב חזק ביותר יידרש זמן רב כדי לבדוק אם מספר כזה מתחלק במספר אחר ללא שארית.

חשיבותם ותפוצתם של צפנים עלתה מאוד עם התפתחותה של רשת האינטרנט. נוחות השימוש ברשת והנגישות שהיא מאפשרת היו תמריץ חזק לארגונים וגורמים רבים להשתמש בה כדי לשנע מידע - גם מידע רגיש ומסווג. סוגים שונים של שיטות הצפנה, ששימשו עד כה בעיקר צבאות ושירותים חשאיים, נהפכו למצרך נדרש ביותר, וקהילת מדעני המחשב ומהנדסי המחשב נדרשת לתת מענה לצורך המורכב בהעברת מידע רגיש ברשת מידע ציבורית ופתוחה כמו האינטרנט. המאמץ מוליד שיטות חדשניות והתפתחות רבה.

נניח שאני מעוניין לשלוח באינטרנט מסר מוצפן לאחי בניו יורק. שיטות הצפנה קלאסיות רבות מאפשרות לי לערבל את המסר (שנכתב בעברית) כך שאם ייפול לידיים הלא נכונות לא יהיה ניתן להבינו - הוא ידמה לרצף בלתי קריא של אותיות וסימנים. בעת הערבול, או ההצפנה, אעשה שימוש בסיסמה. כדי לפענח את המסר יהיה צורך להעביר אותו שוב דרך מנגנון ההצפנה, תוך ביצוע הפעולה ההפוכה, פענוח, ולהשתמש בסיסמת ההצפנה. אלא שכאן ישנה בעיה רצינית. אחי, נמען המסר, אינו סוכן חשאי ולכן לא טרח לתאם אתי סיסמה מוסכמת להעברת מסרים סודיים מבעוד מועד. אני יכול לשלוח לו את הסיסמה שבה השתמשתי, אך ברגע שהדבר נעשה באפיק תקשורת יכול גורם זר לצותת למסר הבלתי מוצפן ובכך להשיג את הסיסמה ולהפוך את כל מאמצינו לחסרי תכלית. יוצא, בעצם, שכדי לשלוח מסר מוצפן יש להעביר ראשית מידע חיוני במסר מוצפן.

הבעיה הזאת נפתרה לפני זמן רב, ובאמצעות הפתרון אפשר להדגים את חשיבותם של מספרים ראשוניים למדע ההצפנה. בשנת 1977 פיתחו שלושה מדענים - עדי שמיר, פרופסור למדעי המחשב ממכון ויצמן, רונלד ריבסט וליאונרד אדלמן - שיטה להצפנת מסרים ללא תיאום מראש. השיטה מתבססת על רעיון המכונה "מפתח ציבורי - מפתח פרטי". לפי שיטה זו בונים מנגנון הצפנה שיש לו שתי סיסמאות - אחת להצפנה בלבד ואחת לפענוח בלבד; מסר שהוצפן על ידי הסיסמה הראשונה יוכל להתפענח רק באמצעות הסיסמה השנייה. את הסיסמה הראשונה ניתן לשלוח באופן גלוי לכל אדם שממנו נרצה לקבל מסרים סודיים. אותו אדם ישתמש בה כדי להצפין את המסר ולשולחו בחזרה אלינו. אין סכנה בגילוי הסיסמה הראשונה (המפתח הציבורי) היות שהיא

מצפינה בלבד ואינה מפענחת דבר. רק הסיסמה השנייה (המפתח הפרטי), שעליה נשמור בסודיות, תאפשר לנו לפענח מסרים שהוצפנו על ידי בת זוגה הציבורית.

ניתן להמחיש את הרעיון כך: כדי לקבל מכתב סודי מאדם מסוים אשלח לו ראשית מנעול קפיצי, מהסוג שננעל בלחיצה. את המפתח אשאיר אצלי. אותו אדם יקבל את המנעול כשהוא פתוח וישתמש בו כדי לנעול את המכתב הסודי שהוא רוצה לשלוח לי. הוא יניח את המכתב בתיבה וינעל אותה עם המנעול, על ידי לחיצה. מרגע הנעילה אין איש מלבדי (גם לא "נועל" המכתב) יכול להגיע אל המכתב, היות שרק בידי המפתח. אם ארצה כעת לשלוח מכתב סודי בחזרה, אבקש מאותו אדם שישלח לי מנעול וישאיר את המפתח אצלו, באותו אופן. התחכום נובע מהפרדת המנעול מהמפתח - סיסמת ההצפנה מסיסמת הפענוח. כך ניתן להעביר מסרים סודיים ללא תיאום של סיסמאות.

השיטה מיושמת בפועל באינטרנט, ובהצלחה רבה. מסרים מוצפנים בעזרת המפתח הציבורי ומפוענחים בעזרת המפתח הפרטי. שני סוגי המפתחות מורכבים ממספרים ראשוניים. זה פועל בערך כך: תוכנות ההצפנה והפענוח מחולקות בחינם, כחלק מדפדפנים, בתוכנות דואר אלקטרוני או בתוכנות עזר אחרות. התוכנות הללו מייצרות מפתחות ציבוריים ופרטיים עבור המשתמש. המפתח הציבורי, המצפין בלבד, הוא מספר גדול מאוד המתקבל על ידי כפל של שני מספרים ראשוניים (המספרים עצמם אינם ידועים, רק מכפלתם). המפתח הפרטי, המאפשר פענוח, מורכב משני המספרים הראשוניים עצמם. את שני המספרים הללו נשמור במחשב שלנו בסודיות. את המפתח הציבורי ניתן לשלוח ללא חשש לחברים או לקוחות. מי שמקבל מאתנו את המפתח הציבורי משתמש בו כדי להצפין מסרים שהוא שולח אלינו. רק אנחנו נוכל לפענח את המסרים הללו היות שרק אנחנו מחזיקים בשני מספרים ראשוניים שנכפלו ויצרו את מפתח ההצפנה הציבורי. מי שאינו מחזיק בהם וינסה לפצח את המסר יהיה חייב למצוא את אותם כופלים ראשוניים בעצמו, ולשם כך יהיה עליו לסרוק מספרים גדולים מאוד ולבדוק אם הם ראשוניים. וכדי לסרוק מספרים ראשוניים גדולים ביעילות ובאמינות נדרשת שיטה כמו זו שפותחה כעת על ידי המדענים מהודו.

החוקרים ההודים טרם פירסמו את ממצאיהם בכתב עת מדעי מקובל. הפרטים נשלחו לכמה מדענים בעולם לבדיקה, והתגובות מתקבלות בימים אלה. אחד החוקרים הבולטים בתחום המספרים הראשוניים הוא פרופ' שפי גולדווסר ממכון ויצמן, שאמר ל"ניו יורק טיימס" כי "זוהי התוצאה המחקרית הטובה ביותר בעשור האחרון". לשיטה, כך מודים החוקרים בעצמם, יש מגבלה מסוימת: היא אטית יותר משיטות אחרות שפותחו בעבר. אך במחיר של זמן עיבוד נוסף לא רב, מבטיחים החוקרים אמינות מוחלטת. בזמן הקרוב יתברר אם זהו אכן פיתוח המערער את היכולת להצפין מידע דיגיטלי.