איך לשמור סוד

צילום: אימג' בנק ישראל Gary S. and Vivian Chapman

ב-30 השנים האחרונות, מאז הופקעה הקריפטולוגיה מבעלותם הכמעט בלעדית של צבאות וסוכנויות ביון, היא הפכה ממדע רדום לאחד מתחומי המדע התוססים ביותר. מידע הוא כוח - את זה ידע גם יוליוס קיסר, שניסה להגן על הודעותיו הצבאיות באמצעות החלפה פשוטה של אותיות, ואת זה יודע היום כל ילד שגולש באינטרנט. הצרכים החדשים שנוצרו בעקבות מהפכת התקשורת דוחפים את תורת ההצפנות לחזית המחקר המתמטי היישומי

תמיר טסה

קריפטולוגיה — תורת הצפנים בתרגום מילולי, או מדע אבטחת המידע במובן המודרני של המלה — מבוססת על המשוואה עתיקת היומין מידע=כוח. הדרך הטבעית והפשוטה להגן על מידע היא באמצעים פיזיים. למשל, נעילתו בכספת, העברתו אל היעד באמצעות בלדר אמין, או השמדת המדיום שנשא את המידע (נייר, קלטת, שליח) לאחר שינונו. שיטות אלו אינן משנות את המידע עצמו, אלא רק מציבות גדרות סביבו.

הקריפטולוגיה נוצרה עם השיטות הראשונות ששילבו את גדר ההגנה בתוך המידע עצמו. בשיטות אלו, ההגנה על מידע x מושגת על ידי שילובו עם ערך סודי כלשהו k ושינויו על ידי כך לפיסת מידע אחר, y, כך שמי שנחשף ל-y יתקשה מאוד לשחזר ממנו את x אלא אם הוא יודע את ערכו של k. שיטה כזו נקראת שיטת הצפנה, המידע המקורי x נקרא המידע הגלוי*, y הוא המידע המוצפן ואילו k נקרא המפתח. הפעולה של הפיכת המידע הגלוי למוצפן נקראת

הצפנה, והפעולה ההפוכה, של שחזור הגלוי מהמוצפן באמצעות המפתח, נקראת פענוח. כל נסיון למצוא את x מתוך y ללא ידיעת המפתח נקרא התקפה; התקפה מוצלחת נקראת שבירה.

אותיות מתחלפות

קל להדגים עיקרון זה באמצעות תיאור אחת משיטות ההצפנה המתועדות העתיקות ביותר. בשיטה זו, שבאמצעותה הגן יוליוס קיסר על הודעותיו, מוחלפת כל אות בזו שמופיעה שלושה מקומות אחריה באלפבית הלטיני. כלומר, A מוחלפת ב-D, B מוחלפת ב-E וכך הלאה, עד לסגירה מעגלית לפיה X, Y ו-Z מוחלפות ב-A, B ו-C בהתאמה. המלה CEASER, למשל, תוצפן באופן זה ל-FHDVHU. שיטה זו, הקרויה שיטת ההזזה, יכולה לעבוד עם כל ערך הזזה שהוא בין 1 ל-25 (שכן באלפבית הלטיני יש 26 אותיות). ערך זה, שנבחר כ-3 במקרה של יוליוס קיסר, נקרא המפתח של השיטה.

שיטה זו, כמובן, אינה מרשימה בתחכומה. מי שרוצה לשוברה, ויודע ששיטת ההצפנה היתה שיטת ההזזה, צריך לנסות לכל היותר 25 ערכי מפתח עד שיגיע לפיענוח הנכון. לכן, תנאי הכרחי לבטיחותה של שיטה הוא מספר רב של מפתחות, כזה שלא יאפשר בדיקה של כולם בזמן סביר. תנאי זה מושג על ידי שיטת התמורה המשכללת את שיטת ההזזה. במקום להזיז את האותיות, נסדר אותן מחדש.

לשם כך, נבנה טבלה בת 26 עמודות ושתי שורות. בשורה הראשונה נרשום את כל אותיות האלפבית כסדרן ובשורה השנייה נרשום תמורה שלהן — כלומר, סידור אחר של כל 26 האותיות. כעת, על מנת להצפין נחליף כל אות בהודעה באות המופיעה מתחתיה בטבלה. בפיענוח, נחליף כל אות בהודעה המוצפנת באות המופיעה מעליה בטבלה. המפתח, במקרה זה, הוא הטבלה המתארת תמורה של 26 האותיות. מספר התמורות הללו הוא !26 (26 עצרת), כלומר 1X2X...X26=403291461126605635584000000. מספר זה אינו מאפשר בדיקה של כל האפשרויות, אפילו לא במחשב.

אולם התנאי ההכרחי של ריבוי מפתחות מסתבר כלא מספיק. מכיוון שבשפה טבעית מתפלגות האותיות באופן לא אחיד, ניתוח פשוט של התפלגות האותיות ותבניותיהן בטקסט המוצפן (בהנחה שאנו יודעים מהי השפה שבה נכתב הטקסט הגלוי) יכול לחשוף בזמן קצר את המפתח, לעתים אף ללא סיוע מחשב.

בשלבים הבאים שוכלל עקרון ההחלפה הפשוטה שתואר לעיל. בשיטה שהגה הדיפלומט הצרפתי ויז'נר, בן המאה ה-16, אומץ עיקרון של החלפה מורכבת, לפיו האופן בו מוחלפת כל אות מושפע גם ממיקומה בטקסט. כלומר, אם בשיטת התמורה הוחלפה האות A תמיד ב-R, למשל, הרי שבשיטת ויז'נר היא תוחלף כל פעם באות אחרת, בהתאם למיקומה בטקסט. דבר זה מקשה מאוד על שבירת השיטה. אך לא לעולם חוסן: קסיסקי הפרוסי פירסם התקפה אחת על שיטות מסוג זה ב-1863. פרידמן האמריקאי פירסם שיטת תקיפה אחרת ב-1920 וטבע את המושג קריפטאנליזה לציון התיאוריה של בטיחותן של שיטות קריפטוגרפיות ודרכים לשבירתן.

בשיטה אחרת, הקרויה על שמו של היל, שפירסם אותה ב-1929, אופן החלפת האותיות מושפע גם ממיקומן וגם מערכן של האותיות הסמוכות. שיטות אחרות שילבו החלפה של אותיות עם שינוי הסדר שלהן. שיטות אלו הגיעו לשכלולן במכונות חוגה להצפנה, עליהן נמנית מכונת ההצפנה הגרמנית "אניגמה". אף אחת מהשיטות הללו לא האריכה ימים, כיוון שכולן הותקפו בהצלחה בכלים מתימטיים וחישוביים.

קל להבין, אם כן, מדוע הצפנה היא עניין המחייב דיון מדעי רציני. כל הצעה לשיטת הצפנה חייבת להיות מלווה בניתוח מעמיק של השיטה ובנסיונות לתקוף אותה. תקופת המבחן של השיטה צריכה להיות ארוכה ככל האפשר, כדי להותיר זמן להבשלת רעיונות לתקיפתה. לפיכך, נוצר הצורך בקיומה של שיטה סטנדרטית להצפנה, שתעמוד במבחן לאורך זמן. בהבנה זו טמון אחד העקרונות הבסיסיים של הקריפטולוגיה: אופן הפעולה של השיטה חייב להיות מידע גלוי, שאינו צריך (ואף אינו יכול) להישמר בסוד. רק המפתח נשמר בסוד, והוא לבדו מהווה את גדר ההגנה על המידע.

DES, IBM והאח הגדול

ב-15 במאי 1973 פירסם מכון התקנים האמריקאי הודעה המזמינה הגשת הצעות לאלגוריתם הצפנה שיאומץ כסטנדרט. האלגוריתם נדרש להיות קל למימוש, לא מוגבל על ידי פטנטים, ובטוח (כלומר: חסין כנגד כל שיטות ההתקפות המוכרות, בהינתן כוח החישוב באותה תקופה). מכיוון שכוח החישוב של מחשבים מכפיל את עצמו כל 18 חודשים בקירוב (כלל הידוע ככלל מור) מן ההכרח לדרוש את עמידותו של האלגוריתם הנידון לאורך שנים אחדות לפחות.

שנתיים ויומיים מאוחר יותר פירסמה IBM את פרטי האלגוריתם שפיתחה — DEA (Data Encryption Algorithm). לבסוף, בינואר 1977, אומץ האלגוריתם כתקן הידוע עד היום בשם DES (החלפת ה-A ב-S מציינת את קבלתו כסטנדרט). אלגוריתם זה הפך לאלגוריתם ההצפנה הסימטרי הנפוץ ביותר — מאז ועד היום. הוא משמש להצפנת תקשורת, להצפנת קבצים, לצורכי זיהוי (אותנטיקציה), לאימות קודים אישיים ועוד.

האלגוריתם הוא בינארי, כלומר, המידע הגלוי וגם המוצפן מיוצג בביטים 0 ו-1. לפיכך, על מנת להשתמש באלגוריתם יש לתרגם תחילה את המידע (טקסט, תוכנית מחשב, תמונה וכו') לרצף של ביטים. לאחר מכן יש לפרק את המידע לבלוקים של 64 ביטים, כיוון שזה אורך הקלט שמסוגל האלגוריתם לקבל. המפתח בשיטת DES מיוצג על ידי 56 ביטים, והפלט המוצפן הוא בן 64 ביטים.

אופן הפעולה של DES סבוך למדי. הקלט עובר 16 שלבי הצפנה הקרויים סיבובים. בכל סיבוב "מעורבב" הקלט עם 48 ביטים מתוך המפתח (כל סיבוב בוחר 48 ביטים מסוימים מתוך 56 ביטי המפתח) והפלט של כל סיבוב משמש כקלט לסיבוב הבא. במסגרת המסע המייגע עוברים הביטים בכל סיבוב דרך 8 קופסאות וירטואליות הקרויות S-boxes. כל קופסה כזו מסוגלת לקבל 6 ביטים ולהוציא 4. כל קופסה מתוארת על ידי טבלה הקובעת מהו הפלט המתאים לכל אחד מ-64 הצירופים האפשריים של 6 ביטים. אופן פעולה כזה, שאינו ניתן לתיאור בנוסחה פשוטה, הופך את DES לקשה יותר לשבירה.

גם היום, 27 שנים לאחר פרסום השיטה, הדרך היחידה לשבור ›

* **הערה:** "המידע הגלוי" הוא המידע שאנו מנסים לגלות.

את DES היא על ידי מעבר על כל 2^{56} המפתחות האפשריים בחיפוש אחר המפתח שייתן פיענוח נכון. מכיוון שמספר זה של מפתחות אינו גדול במיוחד, נהוג להשתמש בגרסאות מחוזקות של DES, המשתמשות במפתח כפול או משולש.

כאמור, ה-S-boxes הן החוליה החזקה של האלגוריתם ולכן הקדישו האנליסטים תשומת לב רבה לתוכנן של הטבלאות הללו ולקריטריונים שהנחו את מדעני IBM בבחירת המספרים המופיעים בהן. אם אכן מסתתר עיקרון כלשהו מאחורי בחירה זו, הוא עשוי לאפשר למי שמכיר אותו לשבור הודעות המוצפנות ב-DES בהצלחה (כזה סוג של מידע נקרא "דלת סתרים", שכן הוא מבטל את הצורך במפתח עבור דלת הפיענוח הראשית).

המרחק מכאן ועד להפצעת שמועות בדבר קיום "דלת סתרים" שכזו היה קטן. כיוון ששיטת DES, בהיותה סטנדרט מקובל, מאבטחת כמויות אדירות של מידע, קיומה של "דלת סתרים" עלול להעניק למי שמכיר אותה כוח אדיר. החשוד המיידי היה ה-NSA — הסוכנות לביטחון לאומי. הטענה היתה שה-NSA "עזר" ל-IBM בתכנון ה-S-boxes ושמר לעצמו את המידע הסודי שיכול לשמש כמפתח מאסטר לפיענוח הודעות המוצפנות ב-DES. טענה כזו משתלבת יפה בתדמיתו של ה-NSA כ"אח הגדול" העוקב אחרי כולם. כל טענות IBM שהטבלאות הן תוצאת מחקר פנימי בן 17 שנות אדם לא עזרו להרגעת הרוחות: ועדה מיוחדת של הסנאט מונתה ב-1978 לחקור את הנושא וקיבלה לשם כך סיווג סודי ביותר. הוועדה ניקתה את ה-NSA מהחשדות, אך לא פירסמה את פרטי חקירתה. הדיון הציבורי במעורבות גורמי הביון בתכנון שיטות הצפנה ובשאלה האם מצויים בידיהם כלים וידע העולים על אלה המוכרים באקדמיה ובתעשייה נמשך למעשה עד היום.

כיוונים חדשים בקריפטוגרפיה

כל שיטות ההצפנה שתוארו לעיל הן שיטות סימטריות, כלומר: המפתח ששימש בעת ההצפנה משמש גם בעת הפיענוח (אם כי בדרך שונה). סימטריה זו מציבה קושי מסוים ביישום השיטה. הצדדים המבקשים לתקשר באופן מאובטח צריכים לתאם ביניהם את שיטת ההצפנה והמפתח שבו ישתמשו. את השיטה אפשר לתאם בגלוי, אך כיצד יתאמו את המפתח? לשם כך עליהם להיפגש ולהחליט על מפתח בארבע עיניים.

אילוץ זה לא היה בעיה חמורה לפני מהפכת המיחשוב. השימוש בצפנים היה בדרך כלל נחלתם של צבאות, סוכנויות ביון ומשרדים ממשלתיים. למערכות התקשורת של גופים כאלה יש לרוב מבנה ממורכז, והשחקנים המשתתפים במשחק ידועים וקבועים. נתונים אלה מאפשרים שגרה של תיאום המפתחות. אך עם מהפכת המיחשוב והתקשורת נוצרו כללי משחק חדשים. כיצד יכול סניף בנק בישראל לבצע העברה בנקאית מאובטחת לחברה בסין, אם שני גורמים אלה מעולם לא נפגשו ואף אינם יכולים להיפגש כדי לתאם מפתח ביניהם?

המענה הראשון לבעיה בא בשנת 1976, כשוויטפילד דיפי (Diffie) ומרטין הלמן (Hellman) פרסמו מאמר בשם "כיוונים חדשים בקריפטוגרפיה". מאמר זה, ממש כפי שמעיד שמו, היווה פריצת דרך בקריפטוגרפיה וניתן לראותו כמבשר של הקריפטוגרפיה המודרנית. דיפי והלמן הציעו שיטה המאפשרת לשני גורמים זרים לתאם ביניהם מפתח משותף מבלי להיפגש, על ידי החלפת מספר הודעות פשוטות באמצעות ערוץ תקשורת לא מאובטח, כך שגם אם מישהו יצותת לערוץ ויקלוט את כל ההודעות, הוא לא יוכל להסיק מן ההודעות מהו המפתח המשותף עליו הסכימו שני הצדדים. על מנת להסביר את הקסם, איננו יכולים להתחמק מקצת מתימטיקה.

בעיה מתימטית קשה במיוחד

נניח ש-p ו-a הם מספרים טבעיים (שלמים וחיוביים). אם נחלק את a ב-p נקבל מנה q ושארית r. למשל, בחלוקת a=47 ב-p=11 נקבל מנה q=4 ושארית r=3. לשארית יש חשיבות רבה ועל כן היא זוכה לסימון מיוחד, $r = a \bmod p$. שארית זו יכולה לקבל כל ערך בין 0 (השמור למספרים a שהם כפולה שלמה של p) ועד p-1 (המתאים למספרים שחסרים 1 לכפולה שלמה של p). נניח ש- p הוא מספר ראשוני ונבחן את קבוצת המספרים הטבעיים {1,2,...p-1}. קבוצה זו מכילה את כל ערכי השארית שיכולים להתקבל אם מחלקים מספר טבעי a ב-p , בתנאי ש-a אינו כפולה שלמה של p (לכאלה מספרים יש שארית 0, שאותה לא כללנו בקבוצה).

אוסף זה של מספרים הוא חשוב ועל כן זכה לסימון מיוחד — Z_p^*. למשל, Z_7^* מורכב משמשת המספרים {1,2,3,4,5,6}. נבחר כעת איבר מסוים, g, מקבוצה זו. אנו יכולים לחשב עבורו את החזקה השנייה g^2 ואז להוציא מהתוצאה שארית בחלוקה ב-p. התוצאה תהיה שוב מספר ב-Z_p^*. תוצאה זו ניתן שוב להכפיל ב-g ולחשב שארית בחלוקה ב-p. על תהליך זה, הנקרא חישוב חזקה מודולרית, ניתן לחזור שוב ושוב. המספרים שנקבל בתהליך יהיו $g^2 \bmod p$, $g^3 \bmod p$, $g^4 \bmod p$ וכן הלאה. במסגרת מודגם חישוב זה על שני מספרים. ‹

חישוב חזקה מודולרית עבור p=7 ו- g=2

$2^1 \bmod 7 = 2$
$2^2 \bmod 7 = (2 \cdot 2) \bmod 7 = 4$
$2^3 \bmod 7 = (4 \cdot 2) \bmod 7 = 1$
$2^4 \bmod 7 = (1 \cdot 2) \bmod 7 = 2$

חישוב חזקה מודולרית עבור p=7 ו- g=3

$3^1 \bmod 7 = 3$
$3^2 \bmod 7 = (3 \cdot 3) \bmod 7 = 2$
$3^3 \bmod 7 = (2 \cdot 3) \bmod 7 = 6$
$3^4 \bmod 7 = (6 \cdot 3) \bmod 7 = 4$
$3^5 \bmod 7 = (4 \cdot 3) \bmod 7 = 5$
$3^6 \bmod 7 = (5 \cdot 3) \bmod 7 = 1$
$3^7 \bmod 7 = (1 \cdot 3) \bmod 7 = 3$

כיצד יכול בנק בישראל לבצע העברה בנקאית מאובטחת לחברה בסין, אם שני גורמים אלה אינם יכולים להיפגש כדי לתאם מפתח ביניהם? המענה הראשון לבעיה בא בשנת 1976, כשדיפי והלמן (בתמונה עם עמיתם מרקל, משמאל) פירסמו את המאמר שנחשב למבשר הקריפטוגרפיה המודרנית

בשני המקרים, החישוב חוזר בשלב מסוים לנקודת ההתחלה (במקרה של g=2 לאחר שלושה חישובים ובמקרה של g=3 לאחר שישה חישובים). כמו כן, כל התוצאות המתקבלות עד שלב זה שונות זו מזו. נשים לב שבמקרה השני, מכיוון שעברנו שישה שלבים עד לחזרה, קיבלנו כתוצאות ביניים את כל ששת המספרים בקבוצה Z_7^*.

מסתבר שאין זה מקרה. אם p הוא מספר ראשוני כלשהו, תמיד נוכל למצוא ב-Z_p^* (דהיינו, בקרב המספרים בין 1 ל-p-1) מספר g כך שחישוב החזקות המודולריות שלו יתחיל לחזור על עצמו רק לאחר p-1 חישובים, ואגב כך, ייצור את כל המספרים ב-Z_p^*. מספר כזה נקרא מספר יוצר (ויש רבים כאלה). למשל, עבור הראשוני p=8304707, מהווה g=17 מספר יוצר. כלומר, לכל מספר a בין 1 ל-8304706 קיימת חזקה k מתאימה, אף היא בטווח שבין 1 ל-8304706, כך ש-a שווה ל-$17^k \bmod p$. למשל, המספר a=975890 מתקבל על ידי העלאת 17 בחזקת k=1234567, וחישוב שארית בחלוקה ב-p.

כעת אנו מגיעים לנקודה המהותית ביותר. בהינתן ערך החזקה k קל לבצע תהליך של העלאה בחזקה מודולרית ולהגיע לתוצאה a. לעומת זאת, אם נתבקש לעשות את התהליך ההפוך, כלומר לשחזר מתוך a את ערך החזקה k המתאים לו — הבעיה תהיה קשה בהרבה. על פניו, לא יהיה מנוס מביצוע תהליך העלאה בחזקה סדרתי (כלומר, חישוב כל החזקות של 17 מודולו p) עד שנקבל תוצאה השווה ל-a. כיוון שהחזקה k יכולה להיות גדולה מאוד (כל מספר בין 1 ל-p-1 הוא "בחזקת חשוד"), החיפוש עלול להיות מייגע ביותר. למעשה, אם המספר p גדול מספיק (בעל מאות ספרות עשרוניות), אין אפשרות לבצע חיפוש כזה גם באמצעות החזק במחשבי העל של ימינו.

בעיה זו נקראת בעיית הלוגריתם הדיסקרטי ("לוגריתם" משום שהנעלם k הוא החזקה המתאימה למספר הנתון, ו"דיסקרטי" משום שיש מספר סופי של אפשרויות לערכו של k). בעיה זו נחשבת לקשה כאשר המספר p גדול מאוד (ומקיים תכונות נוספות שלא נתאר כאן). כיום ידועות שיטות לקיצור דרך בפתרונה, המצליחות לפתור את הבעיה בזמן קצר בהרבה מתהליך החיפוש השיטתי שתואר לעיל. אך זמן זה עדיין בלתי מעשי כאשר המספר p שעומד בבסיס הבעיה הוא בגודל של מאות ספרות עשרוניות. שיטת דיפי-הלמן מבוססת על בעיה זו.

אליס ובוב מחליפים מפתחות

בספרות הקריפטולוגית מופיעים תמיד אותם גיבורים: אליס ובוב הם השחקנים הראשיים, המבקשים לתקשר ביניהם באופן מאובטח. איב (לציון המלה Eavesdropper) או אוסקר (לציון המלה Opponent) משחקים בתור היריב המנסה לצותת לשיחתם. נאמץ מוסכמה זו כדי לתאר את פרוטוקול דיפי הלמן.

נניח שאליס, החיה בסידני, פגשה בצ'ט את בוב, שמעולם לא עזב את אומהה, נברסקה. לאחר שיחות רבות בצ'ט, שבמהלכן שיקרו אליס ובוב זה לזה ללא שום בושה, הם מחליטים שהבשיל הזמן להחלפת כתובות ומספרי טלפון. כיוון ששניהם מודעים לסכנות הטמונות בהסגרת מידע רגיש ברשת כה פרוצה, הם מחליטים לעבור לערוץ מאובטח. אליס, שקראה והפנימה את המאמר של דיפי והלמן, מציעה להשתמש בשיטתם. לצורך כך:

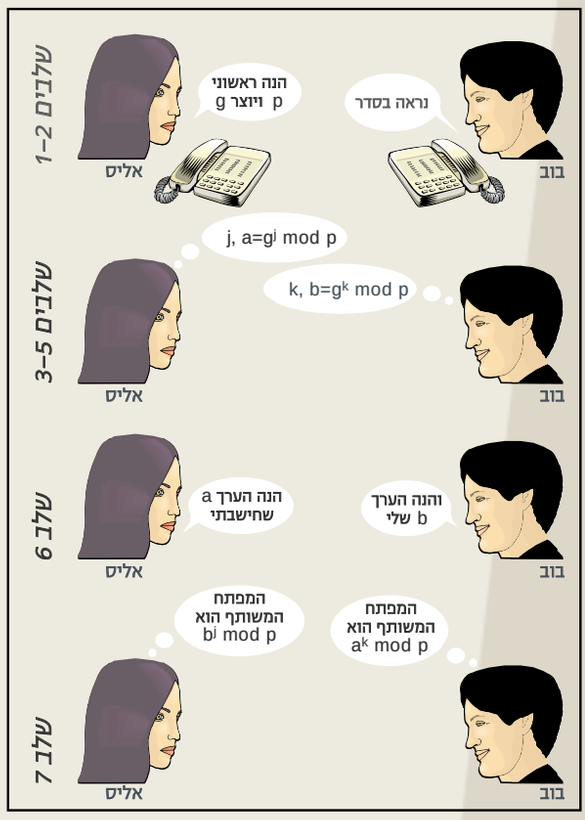
1. אליס מגרילה מספר ראשוני ענק p, ומוצאת מספר יוצר מתאים g (היריעה קצרה מלתאר כיצד מבצעים שתי משימות לא טריוויאליות שכאלו).
2. אליס שולחת את המספרים הללו לבוב, שבודק אותם ומוצא שהם אכן ראשוני ראוי ויוצר מתאים.
3. כעת, אליס מגרילה מספר אקראי j בין 1 ל-p-1. גם בוב עושה דבר דומה ומגריל מספר אקראי אחר k באותו הטווח.
4. אליס מחשבת את השארית שמשאיר המספר g^j בחלוקה ב-p על-ידי תהליך ההעלאה בחזקה המודולרית. התוצאה היא מספר בין 1 ל-p-1, שנסמנו $a=g^j \bmod p$.
5. גם בוב עושה דבר דומה ומחשב $b=g^k \bmod p$.
6. אליס שולחת לבוב את המספר a ואילו בוב שולח לאליס את b.
7. לבסוף, אליס מחשבת את המספר $b^j \bmod p$ ואילו בוב מחשב את המספר $a^k \bmod p$.

לא קשה לראות ששני המספרים הסופיים שמחשבים אליס ובוב שווים. המספר שאליס מחשבת יוצא, על סמך חוקי חזקות בסיסיים הזכורים מהתיכון, $b^j=(g^k)^j=g^{jk}$ (הסימון mod p הושמט לצורך הבהירות). המספר שבוב מחשב הוא $a^k=(g^j)^k=g^{jk}$. אכן — אותו מספר! כעת יכולים אליס ובוב לייצג מספר זה כרצף של ביטים, ואז להשתמש ב-56 ביטים כלשהם מתוך המספר כמפתח DES משותף. כאן מסתיים פרוטוקול דיפי-הלמן; מכאן

והלאה ימשיכו אליס ובוב לתקשר ביניהם באופן מאובטח על ידי שימוש בשיטת DES עם המפתח המשותף שזה עתה חישבו.

לפיכך, שיטת דיפי הלמן אינה מציעה חלופה לשיטות הסימטריות. כל מה שמציעה השיטה היא דרך פשוטה ומהירה לתיאום מפתח המיועד לשימוש בשיטה סימטרית. אך האם דרך זו בטוחה? נניח שאיב צותתה להודעות שאליס ובוב העבירו ביניהם. האם היא תוכל לחשב את המספר $g^{jk} \bmod p$, שהוא המספר המשותף אליו הגיעו השניים וממנו נגזר מפתח ה-DES המשותף? המספרים שאיב מכירה הם p, g, a ו-b. כדי לחשב את $g^{jk} \bmod p$ נראה שאין מנוס מחישוב j (ואז תחשב איב את $b^j \bmod p$ כדי להגיע למחוז חפצה) או k. אך j ו-k הם ערכי הלוגריתם הדיסקרטי של a ו-b, ולכן קשה מאוד (ולמעשה בלתי אפשרי) למצוא אותם בזמן סביר. לכן אליס ובוב יכולים לתקשר בבטחה מבלי לחשוש מאיב.

מה עשוי לערער את בטיחותה של שיטה זו? אפשרות אחת היא מהפכה דרמטית במבנה המחשבים, שתנתץ את קצב ההאצה הידוע על פי חוק מור. אפשרות אחרת היא פריצת דרך בחקר הבעיה של הלוגריתם הדיסקרטי. אם תתגלה שיטה לפתרון הבעיה, המהירה בהרבה מהשיטה היעילה ביותר הידועה היום, בטיחות שיטת דיפי-הלמן תיחלש. אפשרות שלישית היא שתפותח שיטה חליפית לביצוע החישוב שאיב אמורה לבצע, שיטה שלא תזדקק לפתרון בעיית הלוגריתם הדיסקרטי. בכל אחד מהמקרים הללו, סביר שהגדלת המספר p באופן משמעותי תהווה פתרון יעיל.



את RSA, שיטת ההצפנה האסימטרית המקובלת ביותר בשימוש, המציאו רונלד ריווסט, עדי שמיר ולאונרד אדלמן ב-1977. בטיחות השיטה מסתמכת על הקושי בפירוק מספר לגורמיו הראשוניים כאשר אלה גדולים מאוד (מימין: ה-A ה-R וה-S: אדלמן, ריווסט ושמיר)

מפתח פרטי ומפתח פומבי

שיטת דיפי-הלמן סימנה את התחלת עידן המפתח הפומבי. כפי שכבר צוין, כל שיטות ההצפנה עד שלב זה היו סימטריות: אותו המפתח שימש גם בהצפנה וגם בפיענוח. מפתח כזה מכונה מפתח פרטי, כיוון שערכו חייב להיקבע בדיסקרטיות ושני הצדדים חייבים להגן עליו מפני חשיפה. בעקבות דיפי והלמן החלו לצוץ שיטות הצפנה המכונות שיטות אסימטריות או שיטות של מפתח פומבי. בשיטות אלו מחזיק כל גורם — הבה נקרא לו בוב — שני מפתחות (שלצורך העניין הם שני מספרים גדולים מאוד). אחד מהם מכונה פומבי, ואותו מפרסם בוב במאגר מידע מתאים, והאחר נקרא פרטי, ועליו שומר בוב מכל משמר.

אם אליס מעוניינת לשלוח הודעה מוצפנת לבוב, היא מצפינה אותה באמצעות המפתח הפומבי הרלוונטי, כפי שהופיע במאגר המידע שבו פורסם. את ההודעה המוצפנת היא שולחת לבוב, בביטחון מוחלט שאיש לא יוכל לפענחה, שכן הדרך היחידה לפענח אותה היא ע"י שימוש במפתח הפרטי, הידוע רק לבוב עצמו.

הדרך המקובלת לתאר את ההבדל המהותי בין הגישה הסימטרית לזו האסימטרית היא לדמות את ההצפנה הסימטרית לשימוש במנעול הננעל ונפתח על ידי שימוש באותו מפתח, ואת ההצפנה האסימטרית למנעול הננעל בלחיצה, אך נפתח רק על ידי שימוש במפתח המתאים.

בכל השיטות המבוססות על עיקרון זה ניתן לחשוב על המפתחות הפומבי והפרטי כמספרים גדולים מאוד שקיים ביניהם קשר מתימטי מסוים. בהינתן המפתח הפרטי, קל ופשוט לחשב את המפתח הפומבי המתאים לו. אך בהינתן המפתח הפומבי, יש לפתור בעיה מתמטית קשה ביותר כדי למצוא את המפתח הפרטי.

עיקרון זה מודגם יפה בשיטת דיפי-הלמן, למרות שאין היא שיטה להצפנה, אלא רק שיטה לתיאום מפתחות: הערכים

המשך בעמ' 38, עמודת הצפנה אסימטרית

הפומביים שנחשפים לעין כל הם $g^j \bmod p$ ו-$g^k \bmod p$. הערכים הפרטיים שלפחות אחד מהם נחוץ לצורך שבירת השיטה הם החזקות j ו-k. בהינתן j, קל מאוד לחשב את הערך $g^j \bmod p$. אבל בהינתן הערך האחרון, קשה מאוד לשחזר את j מכיוון שהדבר כרוך בפתרון בעיית הלוגריתם הדיסקרטי.

שיטת RSA

שיטת ההצפנה האסימטרית המקובלת ביותר בשימוש עד היום היא זו שהמציאו רונלד ריווסט, עדי שמיר ולאונרד אדלמן ב-1977, המכונה על פי ראשי התיבות של שמותיהם, שיטת RSA. בשיטה זו בוחר בוב בשני מספרים ראשוניים גדולים במיוחד, p ו-q, מכפיל אותם ומקבל את המכפלה n=pq. לאחר מכן הוא מוצא שני מספרים a ו-b, המקיימים קשר מסוים — הקשר הדרוש הוא שהמספר ab-1 יהיה כפולה שלמה של המספר (p-1)(q-1). את המספרים n ו-b מפרסם בוב כמפתח הפומבי שלו. את המספר a, לעומת זאת, הוא שומר חסוי וביחד עם n הוא מהווה את המפתח הפרטי שלו. אם אליס תחפוץ בשליחת מסר סודי לבוב, היא תוכל לעשות זאת בתנאי שהמסר יהיה מספר אחד בלבד בטווח שבין 1 ל-n (מספר אחד בוודאי לא יוכל להעביר את המסר המורכב שלה, אך הוא יספיק על מנת להעביר לבוב את מפתח ה-DES שבאמצעותו היא תצפין את המסר שלה מיד לאחר מכן).

נניח שההודעה המיועדת לשליחה היא המספר x. אליס תחשב את המספר $x^b \bmod n$ ותשלח אותו לבוב. מספר זה, שנסמנו ב-y, הוא ההודעה המוצפנת. בוב יפענח את y על ידי החישוב $y^a \bmod n$. אופן הבחירה של n, a ו-b מבטיח שתוצאת החישוב האחרון תהיה x, שזו ההודעה שאליס חפצה להעביר לבוב.

למרות הדמיון לשיטת דיפי-הלמן, שהרי גם כאן מבצעים חישובי חזקה מודולריים, יש הבדל רב בין שתי השיטות. תוקף שיבקש לשבור את השיטה ולהסיק את ערכו של המפתח הפרטי מזה הפומבי, ייאלץ למצוא את שני גורמיו הראשוניים של n (או למצוא דרך חליפית ובלתי מוכרת לשבירת השיטה). בעיית פירוק מספר לגורמיו הראשוניים, כאשר אלה גדולים מאוד, נחשבת לבעיה קשה ביותר. על קושי זה מסתמכת בטיחות השיטה.

עידן הזוהר של הקריפטולוגיה

שלוש השיטות שתוארו לעיל מסמנות את תחילת העידן המודרני בקריפטולוגיה. הקריפטולוגיה הפכה לדיסציפלינה מדעית מוכרת, ומשנות ה-70 המאוחרות קיבל המחקר בה תנופה עצומה. פותחו אלטרנטיבות רבות ל-DES והוצעו שיטות הצפנה אסימטריות מגוונות. במקביל פותחו שיטות תקיפה חדשות, שחייבו את חיזוקן וביצורן של שיטות ההצפנה.

ניתן לדמות את הקריפטולוגיה ליצור חי בעל שתי רגליים, המתקדם באמצעות צעידה קדימה בשתיהן, זו לצד זו: הקריפטוגרפיה — שעניינה יצירת שיטות אבטחת מידע, והקריפטאנליזה — הבוחנת שיטות אלו ומנסה לתקוף אותן. תיארנו חלק מהצעדים המשמעותיים שעשתה הקריפטוגרפיה. נזכיר רק שני צעדים מרשימים שנעשו בקריפטאנליזה ב-20 השנים האחרונות: קריפטאנליזה דיפרנציאלית וקריפטאנליזה ליניארית, שפותחו בתחילת שנות ה-90, היעילות כנגד כמה שיטות סימטריות (ש-DES

עוד על סטגנוגרפיה במדור אתגרים, עמ' 74

אינה אחת מהן); ושיטות ניפוי (sieving), שניצניהן בשנות ה-80, המיועדות לפרק מספר לגורמיו ועל כן מכוונות בעיקר כנגד RSA.

אחד ממאפייניה הראויים לציון של הקריפטולוגיה הוא המרחק הקטן מהתיאוריה ליישום התעשייתי. למשל, בכנסים העוסקים בנושא החם של קריפטולוגיה המבוססת על עקומות אליפטיות, ניתן למצוא מתמטיקאים העוסקים באחד התחומים המופשטים והקשים ביותר במתימטיקה (גיאומטריה אלגברית) לצד מהנדסי חומרה המממשים את התיאוריה של עקומות אליפטיות על הסיליקון של כרטיסים חכמים.

עיסוקה של הקריפטולוגיה איננו רק הצפנות. עם מהפכת התקשורת (אינטרנט, טלפוניה סלולרית, טלוויזיה דיגיטלית) נוצרו צרכים חדשים והוצעו פתרונות מתאימים. נזכיר רק כמה דוגמאות:

- זמינותן של רשתות תקשורת מסוגים שונים מזמינה ביצוע עסקאות באופן אלקטרוני. שני הצדדים בעסקה כזו צריכים לזהות בוודאות זה את זה ועליהם גם להיות מחויבים לתוכנן של ההודעות שהם שולחים. החתימה הדיגיטלית היא המכשיר המשיג שתי מטרות אלו. סטנדרט החתימה הדיגיטלית הנפוץ ביותר הוא DSS, המבוסס אף הוא על בעיית הלוגריתם הדיסקרטי.
- בעולם וירטואלי כל אחד יכול להתחזות למישהו אחר. כיצד יכול בנק לאפשר ללקוחותיו גישה לחשבונם דרך האינטרנט, או כיצד יכולה חברה לאפשר לעובדיה הפזורים ברחבי הארץ גישה למאגר נתונים מרכזי, מבלי להתיר גישה דומה למתחזים? הפתרון הפשוט והנפוץ הוא שימוש בסיסמה. אך סיסמה קבועה איננה בטוחה לגמרי כאמצעי זיהוי. לפיכך פותחו טכניקות זיהוי חזקות יותר, המשלבות מידע שיש לגורם המזדהה (כמו סיסמאות קבועות או משתנות), התקן פיזי (למשל כרטיס חכם עם מפתח פרטי) או תכונות ביומטריות אופייניות (טביעות אצבע, מאפייני קול או מאפייני העין).
- ברשתות טלוויזיה דיגיטלית בתשלום אמור כל לקוח לקבל גישה רק לערוצים ולתוכניות שעליהם שילם. על מנת להבטיח זאת, פותחו בשנים האחרונות פרוטוקולים לאבטחת מידע במערכות שידור.
- עם המעבר לפורמט הדיגיטלי הפכה הפיראטיות לאטרקטיבית יותר מתמיד, שכן בהעתקת תקליטורים שומר העותק על איכות המקור, ולכן ניתן גם להעתיק ממנו. נוצר הצורך באמצעי לחימה בפיראטיות, אקטיביים — שימנעו העתקה, ופסיביים — שיאפשרו לאתר את מקור הדליפה בדיעבד. מטרה זו מושגת על ידי השתלת סימנים בלתי מורגשים בתוך המידע עצמו. התחום הקריפטולוגי העוסק בהטמנת אינפורמציה נסתרת נקרא סטגנוגרפיה והוא קיבל דחיפה ניכרת בשנים האחרונות, בשל הצורך הגובר בהגנה על זכויות יוצרים.

בתוך פחות מ-30 שנה, מאז הופקעה הקריפטולוגיה מבעלותם הכמעט בלעדית של צבאות וסוכנויות ביון, היא הפכה ממדע רדום לאחד מתחומי המדע התוססים ביותר, המקיים יחסי גומלין הדוקים עם מהפכות המיחשוב והתקשורת ומשגשג על קו התפר שבין המתימטיקה למדעי המחשב. ❇

ד"ר תמיר טסה, ביה"ס למדעי המתימטיקה,
אוניברסיטת תל אביב tamir_tassa@yahoo.com