

סוד מוחלט בהחלט

הגנה על מסמכים בעידן האינטרנט והמחשבים הניידים: שיטות הצפנה, חתימה אלקטרונית וכרטיסים חכמים > חיים סולדנו, נפתלי זיגרט

בעבר היה מקובל לשמור על מסמכים מסווגים בכספות, אבל כיום כמעט כל המידע נמצא במחשבים, חלקם מחשבים ניידים אותם קל מאוד לגנוב או לאבד. חלק משמעותי מהמידע עובר בדואר אלקטרוני, אותו האקרים מסוגלים לייטר.

לפני מאות שנים חיפשו אנשים שיטות להעביר הודעות, מבלי שהשליח יצליח לקרוא את הכתוב. איש אינו יודע מתי באמת התפתחו שיטות ההצפנה הראשונות, אבל אחת מהוותיקות והמפורסמות שבהן קרויה על שם ממציאה – יוליוס קיסר.

צופן קיסר פשוט מאוד: החלפת אותיות לפי הסדר הרץ של הא"ב. למשל: נחליף את האות א' באות ב', את האות ב' באות ג' וכן הלאה, עד שהאות ת' תוחלף באות א', וכך המילה "אבא" תהפוך להיות "בגב", וכמו "סודי" תהפוך ל"עזהך".

פענוח צופן מסוג זה הפך לטריוויאלי לפני שנים רבות, ובהדרגה התפתחו שיטות הצפנה מורכבות יותר, כגון החלפה אקראית בין אותיות בעזרת טבלת החלפה. השולח חייב להעביר לנמען את טבלת המפתח לפענוח המסמך המוצפן – כלומר את סדר החלפת האותיות שיאפשר את קריאת המילים. ברור שאי-אפשר להעביר את טבלת הפענוח בעזרת אותו שליח שמעביר את המכתב, אלא יש להעביר אותה מראש או בידי שליח אחר.

בימי הביניים נוצרו שיטות רבות ומגוונות של צפנים המבוססים על החלפת אותיות, אבל לכל השיטות הללו היתה חולשה עקרונית אחת: בכל שפה ניתן לחשב את תדירות חזרת האותיות. אותיות מסוימות חוזרות על עצמן בתדירות גבוהה מאוד, כגון י', א' או ו'.

חיים סולדנו ונפתלי זיגרט CISSP, חברת דיס ביקורת ואבטחת מידע

בעברית. האות י' מופיעה בעברית בתדירות של 12%, ולכן אם נחליף את אותה באות ע', שהיא נדירה באופן יחסי, הדבר יקל על המפצח. הוא יוכל לנסות ולשחק עם החלפת אותיות לפי סבירות חזרתן, ולבסוף לקרוא את המכתב המוצפן.

מתחילת המאה ה-20 פותחו שיטות מיכניות לשיפור ההצפנה, לעיתים בשיטות המנצלות את מבנה מכונת הכתיבה מבוססת גלילים, עליהם הוטבעו אותיות, אך לטובת ההצפנה שינו את סדר האותיות.

במלחמת העולם השנייה התפרסמה הגרסה המתוחכמת ביותר של מערכת ההצפנה מכנית זו, ה"אניגמה" הגרמנית. במכונה זו ניתן היה לשנות את סדר האותיות מדי יום, ומעת לעת הופצה חוברת המרה של סדר האותיות. ואולם, הבריטים פיצחו את הצופן כבר בתחילת המלחמה, והתגברו לאורכה גם על נסיונות גרמניים לשכלל אותה.

עידן המיחשוב העלה מאוד את הצורך בהצפנה. הקלות הרבה של פענוח צפנים מבוססי החלפת אותיות, הביאה לפיתוח צפנים מתוחכמים בהרבה, המבוססים על עקרונות מתימטיים שונים כגון תורת הסייבוכיות, תורת המספרים וסטטיסטיקה. ההצפנה החלה להתבסס על שיטת הקידוד של המידע במחשבים, כגון על בסיס קודי ה-ASCII או ה-Ebcedic, בעזרתם מיוצג המידע במחשבים.

שיטות הצפנה אלו היו הרבה יותר מסורכיות לפענוח בידי גורם לא מורשה, אבל גם דרשו הרבה יותר עוצמת מיחשוב לשם ביצוע החישובים הרבים שנדרשו הן להצפנה והן לפענוח. לכן, בשנות ה-50 וה-60 שימשו הצפנות אלו בעיקר גורמים צבאיים, אשר השקיעו ממון רב בפיתוח טכנולוגי בשנות המלחמה הקרה.

רק באמצע שנות ה-70, נוצר סטנדרט ראשון של הצפנה בשם DES (Data Encryption Standard) בידי מדעני IBM בשיתוף

גוף המודיעין האמריקני NSA. תקן זה אושר בהדרגה גם לשימוש גורמים מסחריים אזוריים, והפך נפוץ בעולם כולו. עם השיפור בעוצמת המיחשוב, נוצרו גרסאות משופרות לצופן זה, כגון 3des ו-AES.

תקן זה, בדיוק כמו שיטות ההצפנה העתיקות, מכונה צופן "סימטרי", שכן שני הצדדים – השולח והמקבל – נדרשים להשתמש באותו מפתח. כלומר, גם בצפנים הממוחשבים המודרניים, נותרה הבעיה בת אלפי השנים – עלינו להעביר את המפתח מראש או בנפרד לנמען ההודעה.

בשנת 1976 מצאו שני מדענים אמריקנים, ויטפילד דיפי ומרטין הלמן, את הפתרון לבעיה. הם המציאו שיטה המשתמשת בשני מפתחות שונים, המשלימים זה את זה. צופן אחד, המכונה "צופן פומבי", ניתן להפצה לכל גורם שאמור לשלוח אלינו מידע, ובעזרתו ניתן להצפין את המידע או הקובץ ולשולחו בדואר אלקטרוני. פתיחת הדואר המוצפן יכולה להתבצע רק באמצעות צופן שני, המכונה "צופן פרטי".

טכנולוגיה זו מכונה "הצפנה א-סימטרית", והמשך פיתוחה בידי מדענים שונים, כגון עדי שמיר הישראלי, הביא לעולם שיטות כגון החתימה הדיגיטלית (או חתימה אלקטרונית). חתימה זו מאפשרת ליצור סימון חד-ערכי על מקורות של מסמך ממוחשב.

בנוסף, סימון זה מעיד שנוסח המסמך לא שונה ע"י גורם זדוני כלשהו בדרך, או שטרם שחו השתבש בשל תקלה, וזאת ע"י אלגוריתם מתימטי המאפשר לאדם להשתמש בצופן הפרטי שלו (שלעולם אין לחשוש בפני זר כלשהו) על מנת לחתום את המסמך. הנמען, המשתמש במפתח הפומבי, יכול לוודא בקלות את מקורות המסמך שקיבל.

חתימה דיגיטלית על מסמך ממוחשב, או הטבעת חתימה זו על ביצוע פעולה מסוימת במחשב, מקובלת כיום כאמצעי היעיל ביותר ל"מניעת התכחשות". החתימה על המסמך

או ה
הביצ
מאור
הכנס
האלק
עדיפו
ה
ולסיי
שנות
לאמת
המוט
או כר
המפת
את ע
באופן
הזיהוי
לר
טוקן
בעבוד
שהונפ

שהקליד סיסמא לפני עליית המחשב יוכל לקרוא את המידע השמור בו. מובן שניתן לקבוע שההצפנה תיפתח רק לאחר הכנסת כרטיס חכם או טוקן למחשב. שימוש בתו־כנות הצפנה אלו יבטיח שאם המחשב אבד או נגנב, שנתנו לא תנדוד מחשש שסודותינו ייחשפו בפני הגנב או מי שירכוש ממנו את המחשב.

עם זאת, יישום ההצפנה איננו כה פשוט. השוק רווי במוצרים ושיטות, שחלקם הגדול נתפרו למטרות ספציפיות, ולכן לא כולם יעילים או מתאימים לצרכים של כל ארגון. שימוש לא מושכל בהצפנה אף עלול להאט את פעולת המחשבים, ובמקרים קיצוניים מסוימים עלול גם לגרום מצב שבו נצפין מידע ולא נוכל לפענח אותו בעצמנו. לכן, מומלץ להיעזר במומחה על מנת ליישם את ההצפנה ושמירת המידע הארגוני באופן מדורג ומו־שכל, על מנת שנהנה מסגולותיה הרבים של ההצפנה, אך לא ניפגע מכמה מחסרונותיה. ●

מעין רכיב (צ'יפ) שבאמצעותו ניתן לבצע רכישות באשראי ברוב מדינות אירופה. ממשלת ישראל מנסה מזה שנים לחלק לכולנו כרטיס חכם, המכונה "תעודת הזהות החכמה", אך המכרז להכנת התעכב למעלה מעשור, ורק לאחרונה נראה שבית המשפט אישר סופית את הזוכה במכרז. על פי התוכנית, יחולקו לכל תושבי ישראל כרטיסים חכמים כתעודות זהות, אשר ישאו בתוכן הן צופן פרטי שלנו, וככל הנראה גם סימנים אישיים שלנו כגון טביעות אצבע ותווי פנים משלימים לזיהוי ביומטרי.

ומה לגבי המחשבים הניידים הנוטים להיגנב? אותן שיטות הצפנה המיועדות למשלוח מידע בדואר אלקטרוני, קיימות גם להצפנת מידע על גבי דיסקים קשי"ח, תקליטורים ואפילו על דיסק ה־USB הקטנטן.

קיימים בשוק מוצרים רבים המאפשרים להצפין את המידע במחשב, כך שרק מי

או הפעולה משולבים עם מועד מדויק של הביצוע, ומבצע הפעולה לא יוכל לטעון מאוחר יותר שמישהו אחר ביצע אותה. הכנסת חוקקה בשנת 2001 את חוק החתימה האלקטרונית, המקבל חתימה זו כשווה ואף עדיפה על פני חתימה ידנית על מסמכים.

הרכיב הבא, שנועד להשלים את התמונה ולסייע במניעת ההתכחשות, הגיע בסוף שנות ה־80 בדמות טכנולוגיה המאפשרת לאמת את זהותנו ע"י שימוש במפתח פרטי המוטבע על גבי רכיב אלקטרוני, כגון טוקן או כרטיס חכם. ברכיב זה ניתן לשמור את המפתח הפרטי שלנו, אשר יאפשר לנו לזהות את עצמנו באופן חד־ערכי, ולהזין למחשב באופן חסוי את המפתח הפרטי לשם אימות הזיהוי או ביצוע חתימה אלקטרונית.

לרבים מאיתנו כבר יש כרטיס חכם או טוקן כזה, אם לצורך גישה מרחוק למחשב בעבודה, או לדוגמא כרטיסי ישראל כרטיס שהונפקו בשנתיים האחרונות, עליהם יש

קיימים בשוק מוצרים רבים המאפשרים להצפין את המידע במחשב, כך שרק מי שהקליד סיסמא לפני עליית המחשב יוכל לקרוא את המידע השמור בו. מובן שניתן לקבוע שההצפנה תיפתח רק לאחר הכנסת כרטיס חכם או טוקן למחשב. שימוש בתוכנות הצפנה אלו יבטיח שאם המחשב אבד או נגנב, שנתנו לא תנדוד מחשש שסודותינו ייחשפו בפני הגנב או מי שירכוש ממנו את המחשב

