מדינת ישראל
משרד האוצר - אגף החשב הכללי
WWW.ITPOLICY.GOV.IL

שם המסמך: העברה בטוחה של מידע ברשת האינטרנט
תאריך כתיבה: 22/8/97 תאריך עדכון: 19/3/2002
גירסא: 1.0
כותב המסמך: איציק ירחי

העברה בטוחה של מידע ברשת האינטרנט

במצבה הנוכחי של רשת האינטרנט, התרחיש הבא יכול לקרות לכל אחד ואחד מאיתנו. אתם מקבלים דואר אלקטרוני מחבר טוב שלכם. החבר מספר שקיבל "מידע פנימי" לפיו שער מניותיה של חברת "נפט - חיפושים בע"מ" עומד לזנק כלפי מעלה. באופן טבעי, אתם ממהרים להוציא בחשאי הוראת רכישה של מניות החברה ליועץ ההשקעות שלכם, ולאחר שבוע מתברר לכם כי נפלתם קורבן לתרמית. ושבעצם, אותו חבר כלל לא שלח לכם דואר אלקטרוני.

רשת האינטרנט הופכת להיות ערוץ תקשורת עיקרי וחשוב. מהפיכת המידע נמצאת רק בחיתוליה, והבום הגדול עוד לפנינו. כלים כמו דואר אלקטרוני, קניה דרך הרשת, וכניסה לאתרים של חברות או גופי ממשלה הופכים לנחלתו היומיומית של כלל הציבור, וכבר מזמן אינם חזון נפרץ. כל אלה לא ימשיכו להתקיים ללא יכולת להעברת מידע בטוחה ברשת.

מבוא - מהי העברה בטוחה

כל התורה כולה נשענת על בסיסן של שלוש טכניקות. הראשונה - כיצד מצפינים ומפענחים דפי מידע או הודעות של דואר אלקטרוני. השנייה - כיצד חותמים דיגיטלית או בודקים אותנטיות של חתימה דיגיטלית על מסמכים. והשלישית - טיפול בתעודות זיהוי דיגיטליות - מתי מאמינים להן ומתי לא. תעודת זיהוי דיגיטלית, בה כתובים פרטיו אישיים של האדם או הגוף מולו מנהלים את התקשורת, היא אמנם ראשיתה של כל העברת מידע בטוחה, אבל אנו נטפל בטכניקות אלה על פי סדר זה.

תרמית מסוג אחר, אבל אפשרית באותה מידה היא נפילה לרשתם של מתחזים. אתם מחפשים את המילים **"buy & bicycle"** במנועי החיפוש ברשת כי אתם רוצים לקנות אופניים. באתר מתאים בארה"ב אתם מתפתים לקנות אופני הרים במחיר מציאה. האתר שאליו הגעתם אכן מצפין את כל דפי המידע וטפסי הרכישה ביניכם, ולכן אתם מתרצים ורוכשים את האופניים באמצעות מספר כרטיס האשראי שלכם. לאחר כמה ימים מתקשרים אליכם מחברת האשראי, ומתברר כי השתמשו בכרטיס האשראי שלכם לרכישות מוצרים רבים בארה"ב. לו הייתם שמים לב טוב יותר לתעודת הזהות של אותה חנות ברשת, הייתם רואים כי היא אינה חתומה ע"י אף גורם מוכר.

עתידה של רשת האינטרנט כערוץ תקשורת אמיתי, היה נידון לכליה ללא היכולת להעברת מידע באופן בטוח ברשת. הגעה למצבים מביכים כפי שתוארו כאן, פשוט אינה מתקבלת על הדעת. מסתבר, שכלי תוכנה להעברה בטוחה אכן קיימים, אך טרם נמצאת להם דרישה אצל ההמונים. אחת הסיבות היא, שרובם עדיין אינם ידידותיים מספיק. ברם, אין ספק כי יכולת ההעברה הבטוחה היא השלב העיקרי או אולי האחרון בדרכה של רשת האינטרנט לעבור את גיל ההתבגרות ולהפוך למדיום העברת מידע אמיתי בין גופים ואנשים.

מטרתו של מאמר זה היא להציג את ההיבטים המעשיים הכרוכים בהעברה בטוחה של מידע ברשת האינטרנט. כמו שכל אחד יודע כיצד להשתמש בתוכנת הדואר שלו לתיוקה של הודעת דואר בתיקיה נפרדת, כך יתן המאמר כלים לניתוח רמת האבטחה של הודעת הדואר: האם

מובטח לנו ששולח המכתב הוא השולח האמיתי? והאם הייתה סכנה שההודעה היתה חשופה לעיניים זרות? וכשם שכל אחד יודע להשתמש במנועי החיפוש ברשת, המאמר יסביר כיצד ניתן לבחון את מהימנותם של אתרים באינטרנט, האם ניתן לקנות בהם ועד כמה בטוח למסור להם את מספר כרטיס האשראי שלכם.

כסף דיגיטלי או העברת כספים ברשת אף הן יכולות אותן היינו רוצים לרכוש. יש לדעת כי שיטות התשלום ברשת נסמכות על יכולת העברה בטוחה. שיטות שונות בנויות ממרכיבים שונים של הצפנה, של חתימה ושל תעודות זיהוי.

המאמר בנוי בהדרגתיות, כך שהבנת סעיפים חדשים מתבססת על הכתוב בסעיפים הקודמים. קראו את המאמר לאט ובעיון. בכל מקרה, לא יופיעו פרטים טכניים של ממש, כך שרמת המאמר מותאמת לכל מי שעכברו בידו, ודפדפנו מול עיניו. בסעיפים המתקדמים ניתן את דעתנו גם על סוג התשתיות שעל הממשלה להקים לטובת המשתמשים הרגילים. בסוף המאמר יופיעו סעיפי המלצות לפעולה. בנספחים של המאמר יופיע חומר נוסף בנושא.

הצפנה - הפתרון האולטימטיבי

כאשר אנו מדברים על מידע העובר באינטרנט אנו מדברים על הודעות. ההודעה צריכה להגיע שלמה מנקודת ההתחלה לנקודת הסיום. בדרך, עוברת ההודעה שלנו דרך כמה צמתי ביניים. באופן מעשי בהחלט, כל צומת כזו יכול לצותת לכל ההודעות העוברות דרכו. במקרים חמורים, ניתן בהחלט לשנות את תוכן ההודעה או לייצר הודעה מתחזה משל עצמה. שיטה זו של העברת מידע, בה כל המידע חשוף לעין כל וכל הודעה עשויה ליפול קורבן לטעויות תקשורת או לחסדיה של יד זדונית, היא מקור כל הבעיה.

כדי להבטיח כי הודעה תעבור באופן בטוח מנקודת ההתחלה לנקודת הסיום מספיק להצפין אותה. בזה בעצם ייעלמו כל הספקות. הצפנה כזו, מבטיחה כי ההודעה לא תתפענח כיאות אם היא שונתה בדרך, וכן שאף אחד פרט לנמען לא יוכל לקרוא אותה.
טכניקת ההצפנה בה משתמשים היא הצפנה סימטרית. כלומר, השולח והנמען חולקים ביניהם איזשהו מפתח סימטרי, מעין סיסמא משותפת, בעזרתה השולח מצפין את ההודעה, והנמען מפענח אותה. ההצפנה הסימטרית מהירה ויעילה מאוד, ולכן תפסה את מקומה כשיטת ההצפנה היחידה להודעות באינטרנט.

כל שיש לעשות, הוא להחליט על מפתח סימטרי המשותף לשולח ולנמען. אותו המפתח משמש גם להצפנה וגם לפענוח. למשל, אליס שולחת לבוב הודעה: אליס מצפינה את ההודעה עם המפתח הסימטרי, שרק בוב מכיר. אליס שולחת את ההודעה המוצפנת, כמו ששולחים דואר אלקטרוני רגיל. אף אחד בדרך לא יוכל לפענח את ההודעה, מלבד בוב. דוגמא נוספת, הדפדפן והשרת מחליטים על מפתח סימטרי זמני שרק שניהם יודעים. כל פיסת מידע, העוברת בין השרת לדפדפן או להיפך פשוט מוצפנת או מפוענחת ע"י המפתח הסימטרי. מכיוון שרק שניהם יודעים מהו המפתח, אף אחד לא יוכל לקרוא את התקשורת ביניהם. בכך נפתרו 99% מהצרות.

ההצפנות באינטרנט רובן ככולן אמנם מתבצעות בהצפנות סימטריות. יתרון השימוש במפתח הסימטרי נובע מכך שקיימים פרוטוקולים יעילים שונים, המאפשרים הצפנה ופענוח מהירים מאוד. למשל: **DES**, **Triple-DES**, **IDEA**, **RC4**, **RC2** ועוד (ראה קישורים בנספח ה'). למשל, ניתן למימוש ע"י רכיבי חומרה. במילים אחרות, שני הצדדים צריכים להחליט עוד לפני ההתקשרות, מהי שיטת ההצפנה ומהו המפתח הסימטרי שבו ישתמשו. לא חשוב באיזו שיטה בוחרים, רק חשוב ששני הצדדים ישתמשו באותה השיטה כמובן, ושיחליטו על כך לפני תחילת ההעברה הבטוחה ביניהם.

הקוראים העירניים, שמו לב לבעיה קשה שהתעוררה. את המפתח הסימטרי לא ניתן להעביר סתם כך בין הצדדים. צריך להעביר אותו מוצפן, אבל עדיין אין לנו יכולת להצפין כי טרם העברנו שום מפתח הצפנה ...

כיצד להעביר את המפתח הסימטרי מאליס לבוב

בדוגמא הקודמת ראינו, שכדי להצפין אליס ובוב צריכים להשתמש באותו מפתח סימטרי, על מנת שיוכלו להחליף הודעות מוצפנות ביניהם. כיצד אם כן, ניתן להחליף מפתחות סימטריים מבלי שהעברת מידע כזו תהיה גלויה, מבלי שצומת ביניים באינטרנט תוכל לחשוף את המפתח? התשובה היא ... כמובן, ע"י הצפנה... אבל, הצפנה מסוג אחר. הפעם נצטרך להשתמש בשיטת המפתח הפומבי. שיטה זו אמנם איטית מאוד ומסורבלת, אך אם נצפין בעזרתה רק בתחילת ההתקשרות את המפתח הסימטרי בלבד, אזי פתרנו את כל בעיותינו.

לצורך הצפנה ופענוח בשיטת המפתח הפומבי בוחרים זוג מפתחות, שיש ביניהם קשר מתימטי מסוים. מפתח אחד נשמר בסוד ונקרא מפתח-פרטי, ואת השני מפרסמים ברבים ולכן הוא מכונה מפתח-פומבי. בעזרת חוקים מתמטיים,ניתן לוודא שהצפנה שנעשית בעזרת המפתח הפרטי, יכול רק המפתח הפומבי לפענח, ולהיפך. הצפנה שנעשית ע"י המפתח הפומבי, יכול לפענח רק המפתח הפרטי. יתרונה העצום של שיטת המפתח-הפומבי הזו הוא שהיא פותרת את בעית העברת המפתח. מכיוון שממילא המפתח הפומבי גלוי וניתן להשתמש בו להצפנה. אבל, רק מי שברשותו המפתח הפרטי, בן הזוג התואם שלו יוכל לפענח את ההודעה. נדגים זאת שוב עם אליס ובוב.

אליס רוצה לדבר עם בוב באופן מוצפן. בוב בוחר מפתח סימטרי, והוא צריך להעביר אותו לאליס. לשם כך, בוב משתמש במפתח הפומבי של אליס. בוב מצפין עם המפתח הפומבי של אליס, את המפתח הסימטרי, בו הוא מעוניין להשתמש לתקשורת ביניהם. מכיוון, שאליס שמרה את המפתח הפרטי, בן זוגו של המפתח הפומבי, בסוד מוחלט. ורק היא יודעת מהו, רק היא תוכל לפענח את ההודעה המוצפנת של בוב, ולקבל את המפתח הסימטרי. כעת, כמו בדוגמא הקודמת, אליס ובוב מחליטים על שיטת הצפנה והם יכולים לתקשר ביניהם.

ישנן כמה שיטות ליישום מפתח-פומבי, כאשר הנפוצה והפופולרית מכולן היא **RSA**. **RSA** הייתה פטנט רשום של חברת **RSA Data Security, Inc** (**www.rsa.com**). בתאריך 6 ספטמבר 2000 (זמן מועט לפני תום תוקף הפטנט) שחררה חברת **RSA** את האלגוריתם לכלל הציבור, והשימוש בו כעת הוא חופשי.

הצפנה במפתח פומבי

האיש (האדום) משמאל היא אליס. בוב (בכחול) מימין, מעביר לאליס הודעה מוצפנת (קלף נעול במנעול כסף), ומפתח סימטרי (מפתח זהב) מוצפן במפתח הפומבי (סגור בקופסת עץ). רק המפתח-הפרטי של אליס יפתח את קופסת העץ, ורק היא תוכל לפענח את ההודעה.

הערה: כל אחד יכול לנעול את קופסת העץ (מפתח פומבי), אבל רק אליס יכולה לפתוח (מפתח פרטי).

חבילת PGP

PGP (**Pretty Good Privacy**) היא חבילת התוכנה הותיקה ביותר (1991) שמספקת שירותי הצפנה. עבור רבים ממשתמשיה, **PGP** היתה במשך שנים כלי ההצפנה האמין היחידי. בשנת 2002, נסגרה חברת **PGP** ומרבית מוצריה נמכרו לחברת **McAfee**, שם הם הוטמעו במוצרי החברה השונים. תוכנות ההצפנה של **McAfee** מאפשרות להצפין קבצים טקסטואליים או

בינאריים ע"י מגוון של שיטות ובעיקר: **RSA** למפתח פומבי, ו- **IDEA** להצפנה סימטרית. כיום קיימות גרסאות לרוב מערכות ההפעלה: **Unix, Windows, Mac, Vms**.

התוכנה מאפשרת למשתמש להצפין ולפענח קבצים במחשב שלו. באופן זה, הוא מגן על פרטיותו מפני חדירה למערכת שלו. בנוסף לכך, **PGP** יודעת לעבוד במשולב עם כמה תוכנות דואר: **Eudora, Microsoft Exchange**, **MicroSoft OutLook**. **PGP** מאפשרת להצפין ולפענח הודעות מתוך תוכנת הדואר. בנוסף, **PGP** מאפשרת כעת הצפנה של מידע העובר באפליקציות מסרים מיידים (כדוגמת **ICQ**). חסרון ראשון של **PGP** הוא, שגם השולח וגם הנמען צריכים שניהם להשתמש ב **PGP**. חסרון שני נובע מהעובדה שהמשתמש אחראי להפעיל באופן אישי את ההצפנה והפענוח. פעולות רוטיניות אלה אינן נעשות אוטומטית והמשתמש צריך לבצע אותן בעצמו.

כדי להעביר הודעה באופן בטוח, יש לדעת קודם כל את המפתח הפומבי של הנמען. **PGP** תבחר עבורך מפתח סימטרי להצפנת ההודעה ובעזרת המפתח הפומבי שנתת לה, היא תצפין את המפתח הסימטרי עצמו, כדי שהנמען ורק הנמען יוכל לפענח את ההודעה. ישנן שתי דרכים להשיג את המפתח של הנמען: הראשונה, לבקש מהנמען לשלוח לך את המפתח הפומבי שלו. השנייה, להיעזר בשרתי-מידע מיוחדים, שמחזיקים מאגר של מפתחות פומביים לפי פרטי המשתמשים. באינטרנט ישנה רשת ענפה של מאגרים פומביים כאלה, המעדכנים זה את זה. **PGP** תומכת גם בחתימה דיגיטלית על מסמכים.

למידע נוסף: **http://www.pgp.com/products/mail-file-encryption/default.asp**

חתימה על מסמכים

עד עתה דיברנו רק על הצורך להעביר מידע מוצפן כדי להבטיח אותנו מפני ציטוט וחשיפה. בחיי היומיום אנו זקוקים גם ליכולת חתימה. אנחנו רוצים לשלוח ולקבל הודעות, תוך קבלת בטחונות על מקור ההודעה. במילים אחרות, נרצה לחתום על מסמכים שלנו ולוודא את חתימתם של אחרים על המסמך. למשל, נרצה לקבל תלושי משכורת דיגיטליים חתומים ע"י המעביד. תלושים כאלה יהיו קבילים בפני רשויות המס, בנקים או כל גוף אחר. או למשל, הוצאת חשבונית-מס ללקוח, אף היא זקוקה לחתימה דיגיטלית של המוציא. החתימה הדיגיטלית המצורפת למסמך, היא שמוכיחה את מהימנותו. היום, באופן נאיבי, אנו מחשיבים מסמכים מודפסים על נייר, כמסמכים לא מזויפים. בעתיד, נדרוש לקבל עותק דיגיטלי חתום של אותם המסמכים.

שלב ראשון בתהליך חתימה על מסמך הוא חישוב טביעת האצבע שלו. טביעת האצבע היא קצרה מאוד יחסית למסמך עצמו, לרוב היא קצרה מ 20 אותיות של מחשב. ושוב ישנן שיטות רבות לחישוב טביעת האצבע. השיטות הנפוצות הן: **RIPEMD-160**, **Tiger** , **SHA, MD4, MD5** (ראה קישורים בנספח ה'). הטענה היא שלא ניתן לזייף אותן. כלומר, לא ניתן לבנות שני מסמכים שונים, בעלי טביעת אצבע זהה. כלומר, לא ניתן לשנות מסמך, מבלי לשנות את טביעת האצבע שלו, וכמו שלא קיימים שני אנשים בעלי טביעת אצבע זהה, כך לא קיימים שני מסמכים בעלי טביעת אצבע זהה.

בעזרת **RSA** חתימה דיגיטלית היא פשוטה מאוד וזו הסיבה ש **RSA** כל כך פופולרית. את טביעת האצבע של המסמך מצפינים ע"י המפתח הפרטי של הגוף או האדם החותם. את התוצאה מצרפים כחתימה דיגיטלית למסמך שרוצים לחתום עליו. מי שמקבל לידיו את המסמך והחתימה, יכול לוודא בקלות את האותנטיות של המסמך. תחילה הוא מחשב את טביעת האצבע של המסמך המקורי, אח"כ הוא מפענח את החתימה הדיגיטלית תוך שימוש במפתח הפומבי. אם פענוח החתימה הדיגיטלית, וטביעת האצבע של המסמך זהות, אזי אותו אדם אכן חתם על המסמך המקורי. חוסר התאמה מצביע על זיוף המסמך המקורי, או על שינויים במסמך הנובעים מתקלות תקשורת.

נדגים שוב את תהליך החתימה על מסמכים, כאשר הפעם אליס חייבת $1000 לבוב. כדי לשלם לבוב באמצעות רשת האינטרנט, אליס כותבת במעבד התמלילים שלה ייפוי כח לבוב, למשוך $1000 מחשבון העו"ש שלה בבנק. כדי לתת תוקף משפטי לקובץ המחשב, היא מחשבת את טביעת האצבע של הקובץ. מצפינה את טביעת האצבע ע"י המפתח הפרטי שלה. ושולחת לבוב שני קבצים: את ייפוי הכוח, ואת טביעת האצבע המוצפנת. בוב שולח את שני הקבצים לבנק. הבנק מחשב את טביעת האצבע של ייפוי הכוח, מפענח את טביעת האצבע שנמצאת בקובץ השני ע"י

המפתח הפומבי של אליס, ומקבל התאמה. הבנק מעביר 1000$ מחשבונה של אליס לחשבונו של בוב.

רוב התוכנות המצפינות דואר אלקטרוני, מצרפות אוטומטית גם חתימה דיגיטלית לכל הודעה.

חתימה על חוזים משפטיים

חלק מהקוראים אולי שמו ליבם לבעיה קשה. מה קורה אם אליס גילתה כי מישהו חדר למחשב האישי שלה, וגנב ממנו את המפתח הפרטי שלה. אותו פורץ אלמוני יכול מעתה והלאה לחתום בשמה של אליס ולהתחייב כספית לאנשים רבים. אליס מבחינתה תיאלץ לבחור זוג מפתחות פרטי ופומבי חדשים ולהשתמש מעתה והלאה רק איתם. אבל, כל התחייבויותיה הקודמות של אליס יאבדו כל תוקף, מחשש לזיוף.

במקרים חמורים יותר, ישנה סכנה כי אליס תיזום בעצמה הודעת שווא כזאת, לאחר חתימה על חוזה חשוב. במקרה זה היא תוכל לטעון שמישהו אחר, אותו פורץ אלמוני, חתם על החוזה בשמה ולכן היא אינה מחוייבת לו עוד.

כדי לפתור בעיה זו, יש להשתמש בשירותם של נוטריונים דיגיטליים. הנוטריון הדיגיטלי מוסיף את חתימתו המוכרת והידועה לכולם לחוזה, בנוסף לחתימתם של הצדדים החותמים, ולתאריך שמוטבע בגוף החוזה. מכיוון שהנוטריון הוא גוף אמין ומקובל על כל הצדדים ומכיוון שיש לו כלים לוודא במידה הדרושה את זהותם של הצדדים וכי המפתחות הפרטיים שלהם הם אכן שלהם, החוזה יקבל משנה תוקף ואף צד לא יוכל להתכחש לו.

נוטריון דיגיטלי: **http://www.surety.com/**

הפצתם של מפתחות-פומביים: רשות זיהוי ותעודות זיהוי

שיטות ההצפנה והפענוח נחשבות לעמידות בפני פריצה. ולכן פורץ שירצה לזייף מסמכים או לחדור למידע מוצפן, ינסה להפיץ מפתח פומבי מזויף. הפורץ ינסה לנצל את העובדה שהשגתו של המפתח הפומבי תיעשה בתקשורת גלויה על גבי האינטרנט. מכיוון שכך, הוא ינסה להעביר לנו מפתח פומבי מזויף במקום המפתח האמיתי. אם הפורץ אכן יצליח לשלוח לנו מפתח פומבי מזויף, במקום זה של הנמען, אזי הוא יוכל לפענח כל מסמך מוצפן שנשלח לנמען. ואפילו להפיץ מסמכים כוזבים החתומים כביכול בשם הנמען.

כדי לפתור בעיה זו משתמשים בתעודת זיהוי (**Certificate**). תעודת זיהוי היא מסמך (קובץ), הכולל בתוכו את פרטיו האישיים של בעל התעודה בצירוף המפתח הפומבי שלו ובתוספת של חתימה דיגיטלית, המאשרת את נכונות המידע שבו. כלומר, צריך להשתמש בשירותיו של גוף אמין, ידוע לכל, המקובל על כולם, ושהמפתח הפומבי שלו ידוע בציבור בזכות עצמו, כדי שיחתום על תעודת הזיהוי ויערוב למהימנותם ע"י שמו הטוב. גוף כזה נקרא: רשות זיהוי (**A - Certificate Authority**).

נדגים זאת שוב. בוב, שזו הפעם הראשונה שבה הוא מדבר עם אליס, רוצה להצפין לה הודעה בדואר אלקטרוני. לשם כך, הוא בוחר מפתח סימטרי, מצפין את ההודעה, ומצפין את המפתח הסימטרי שבחר בעזרת המפתח הפומבי של אליס. לבוב יש את תעודת הזיהוי של אליס, ועל כן הוא יכול להיות בטוח שרק אליס תקרא את ההודעה. תעודת הזיהוי מקשרת בין שמה של אליס ובין המפתח הפומבי שלה. על התעודה חתומה רשות זיהוי, שאיתה בוב יכול לבדוק בכל רגע את אמיתות התעודה.

חברת **VeriSign** (**www.verisign.com**) לדוגמא, מגדירה את עצמה כרשות זיהוי כזו. והיא מנפיקה תעודות זיהוי ללקוחותיה. כלומר, היא חותמת על מסמך, המכיל מפתח פומבי , יחד עם שמו של הבעלים, תאריך הוצאה ותאריך תפוגת האישור. אנחנו יכולים לוודא את חתימתה של חברת **VeriSign** על התעודה, ובכך לקבל בטחונות על מהימנותו של המפתח הפומבי שבידינו. למשל, שני הדפדפנים **Netscape Navigator** וגם **Internet Explorer** מופצים כאשר המפתח הפומבי של **VeriSign** טבוע בתוכם.

חברות נוספות המשמשות כרשות זיהוי הינן **Thawte** - http://www.thawte.com
ו-**Entrust** http://www.entrust.com.

ומה לגבי רשויות זיהוי אחרות, או חדשות? מי יערוב לנו למהימנות המפתח הפומבי שלהן? ובכן, אחת האפשרויות היא ש **VeriSign** או רשות זיהוי ברמה עליונה, תחתום על תעודות זיהוי עבור יתר רשויות הזיהוי וכך נקבל מעין רשת של בטחונות (**Web of Trust**), בה רשויות זיהוי שונות ערבות אחת לשניה. אם מפתח פרטי של רשות זיהוי נפרץ, תאבד אותה רשות זיהוי הרבה מאוד מאמינותה. ולכן, תנאי יסוד לאמינותה של רשות זיהוי הוא ההבטחה שלה להשתמש באמצעי חומרה מיוחדים לשמירת המפתח הפרטי. כאלה, המונעים אפילו מעובדי הרשות עצמה (שוחד) לקרוא אותו.

דף הבית: http://digitalid.verisign.com
מסמך ה **CPS** (**Certification Practice Statement**) מתאר את "הכרזת המחויבויות" של **Verisign**, תהליכי אישור ורישום, ומהות המושג "תעודת זיהוי":
https://www.verisign.com/repository/CPS

שימוש בתעודות זיהוי להצפנה

האיש (האדום) משמאל היא אליס. בוב (בכחול) מימין, מבקש מאליס תעודת זיהוי, כדי לשלוח לה הודעה מוצפנת. אליס מעבירה לו את התעודה המכילה את שמה (ציור הפנים), ואת המפתח הפומבי (קופסת עץ).

תקן X.509

תקן זה מגדיר אילו פרטים יש לכלול בתעודת זיהוי (**Certificate**) דיגיטלית, וכן את מבנה התעודה. זהו התקן הנפוץ ביותר ליישום תעודות זיהוי כאלה. גרסה **3** היא האחרונה והיא מכילה תיקונים לגרסאות הקודמות. תעודת זיהוי של **X.509** כוללת את הפרטים הבאים: גרסת התעודה, מספר סידורי, שיטת החתימה הדיגיטלית, שמה של הרשות המנפיקה, תאריך תפוגה, שמו של בעל התעודה, המפתח הפומבי של בעל התעודה, שם חד-חד-ערכי של הרשות, שם חד-חד-ערכי של בעל התעודה, אפשרות לתוספות והחתימה עצמה.
מידע נוסף ניתן למצוא ב- http://www.entrust.com/resources/pdf/509_overview.pdf

בנוסף, קיימים כיום בשוק כלים המאפשרים ליצור מפתחות ותעודות חתומות עצמאית. דוגמה לכלי כזה הינו ה-**Keytool** של חברת **Sun**
(http://java.sun.com/products/jdk/1.2/docs/tooldocs/win32/keytool.html)

פרוטוקולים אלה משתמשים ב **X.509** לתעודות זיהוי: **PEM, PKCS, S-HTTP, SSL, S/MIME**.
S/MIME - פרוטוקול להצפנה ופענוח של דואר אלקטרוני
SSL - פרוטוקול לתקשורת אינטראקטיבית מוצפנת, **S-HTTP** - פרוטוקול **HTTP** מאובטח

PKCS - אוסף פרוטוקולים כלליים של חברת **RSA**, **PEM** - חבילת תוכנה להצפנת דואר אלקטרוני).

ניהול תעודות זיהוי - באחריות רשות הזיהוי

אמינותן של תעודות הזיהוי היא בעלת חשיבות עצומה להעברה בטוחה באינטרנט. זוהי למעשה הערבות היחידה למהימנותו של העומד בצד השני. רשות הזיהוי שמנפיקה את התעודה חייבת להיות אמינה וחייבת לקיים נהלים ברורים לאופן הזיהוי של בעל התעודה. למשל רשות זיהוי שהיתה ממוקמת במשרד הפנים, היתה זוכה לאמינות רחבה. תעודה כזו תתקבל ללא עוררין ברשת כאמצעי לזיהוי שמם האמיתי של אזרחי ישראל, כאשר הם מבצעים התקשרויות ברשת האינטרנט. לעומת זאת, אם חברת היי-טק צעירה ואנונימית היתה נוטלת על עצמה לנפק תעודות כאלה, ספק אם מישהו היה מכבד תעודות זיהוי שלה.

רשות זיהוי חייבת גם לנהל ולהפיץ בציבור רשימת תעודות זיהוי גנובות או מזויפות (**CRL** - **Cetificate Revokation List**). אלה הן תעודות, שהמפתח הפרטי של בעליהם נפרץ ויש חשש שישתמשו בו כדי לזייף מסמכים. רשימה כזו היא קשה מאוד לניהול, מאחר שיש בעיה לבדוק את זהותו של מוסר ההודעה על הזיוף. כיצד באמת ניתן להבטיח את זהותו של המודיע על הזיוף?

מסיבה זו, ומסיבות ניהול אחרות, הקמת רשות זיהוי מהווה משימה לא פשוטה. במיוחד אסור לרשות זיהוי לפשוט את הרגל או להתפשר באמצעי הבטיחות הנהוגים בה. לכן הקמתה של רשות זיהוי כזו מתוך מוסד שלטוני ישראלי, עשויה להוות את הבסיס הרחב והאמין שממנו ניתן להתחיל את היכולת להפקת תעודות זיהוי. רשות זיהוי זו יכולה לשמש כרשות על, שתסמיך רשויות זיהוי פרטיות ומסחריות.

מסמך **RFC** בנושא: **http://www.freesoft.org/CIE/RFC/1422/**

שכבת SSL

SSL (**Secure Socket Layer**) הוא פיתוח של חברת **Netscape**, ומאפשר העברה בטוחה אינטראקטיבית בין שרת ללקוח באינטרנט. **SSL** מיועד לשימוש להעברה בטוחה של כל סוגי המידע. באופן זה ניתן לאבטח כל תקשורת שהיא בין שתי כתובות באינטרנט. הפרוטוקול מתאים להצפנת תקשורת **HTTP** - דפי מידע, דרך **FTP** המשמש להעברת קבצים, **Telnet** להתקשרות למחשבים מרוחקים וכל פרוטוקול אינטראקטיבי אחר. כלומר, כותב התוכנה יכול להעביר כל מידע שהוא, כאשר הוא משתמש ב **SSL** כבשכבת העברה, מעל לשכבת ה **TCP/IP**.

תוכנות הדפדפן של **Netscape** מאז גרסה **1.0** יודעות להשתמש בהעברה בטוחה עם **SSL**. **Netscape** מנסה לקדם את **SSL** כתקן פתוח באינטרנט וכל אחד יכול לרכוש חבילת תוכנה ליישום **SSL** בתוכנות שלו. כמו כן **Netscape** היא ספקית של שרתי-מידע המשתמשים ב **SSL** להצפנה, וע"י כך מאפשרים לארגון לקיים העברת מידע בטוחה באינטרנט. על בסיס **SSL** פיתחה **Netscape** את **HTTPS** שהוא פרוטוקול לשליחת דפי מידע מוצפנים. מלבד זאת הכריזה **Netscape** על אוסף של פרוטוקולים מוצפנים כגון: **SSMTP** - להעברת דואר אלקטרוני, **SPOP3** - למשיכת הודעות דואר אלקטרוני, **SNEWS** - קבוצות דיון מאובטחות ועוד.

SSL כאמור, הוא פרוטוקול אינטראקטיבי, המיועד אך ורק להצפנה ופענוח. בתהליך ההצפנה שולח שרת המידע תעודת זיהוי (**X.509**). בתעודת הזיהוי מופיע מפתח-פומבי (**RSA**). הלקוח מוודא שהשרת אכן יודע לפענח הודעות, המוצפנות במפתח הפומבי כתנאי להמשך הקשר. גם כאן המשתמש קובע את מדיניות השימוש בתעודות הזיהוי. במידה שרשות הזיהוי החתומה על התעודה אינה אמינה בעיניו, יכול המשתמש לסרב ליצירת הקשר המוצפן. **SSL** מאפשר גם זיהוי דו-כיווני של המשתמש בפני השרת, כך שגם השרת יכול לסרב ליצירת קשר ביניהם. הדפדפנים הקיימים היום בשוק אינם תומכים בבדיקה אוטומטית של התעודה מול מאגר של תעודות מזויפות (**CRL**), אך הוא מאפשר למשתמש לדרוש בדיקה כזו.

דף המידע: **http://developer.netscape.com/tech/security/ssl/howitworks.html**
וגם: **http://www.faqs.org/faqs/computer-security/ssl-talk-faq/**

החל מגרסת **Internet Explorer 3.0** של **Microsoft**, משולבת תמיכה מלאה ב **SSL**.

פרוטוקול S/MIME

S/MIME הוא תקן, המוסכם על כולם להצפנה ולחתימה על הודעות דואר אלקטרוני. חברת **RSA** היא היוזמת. בין החברות התומכות ב **S/MIME** ניתן לכלול את **Netscape**, **Microsoft**, **VeriSign** ועוד. דפדפני הדור הרביעי של **Netscape** ו **MicroSoft** תומכים בפרוטוקול זה לשליחת דואר אלקטרוני מוצפן.

הפרוטוקול משתמש בשיטת **MIME** כדי לצרף חלקים מוצפנים לתוך הודעת דואר אלקטרוני. למשל, ניתן לצרף (**attachment**) להודעת הדואר, תמונה מוצפנת. מקבל ההודעה יוכל לזהות את שיטת ההצפנה וגם את העובדה שהמידע המוצפן הוא תמונה. בלחיצת עכבר אחת הוא יוכל לאשר לתוכנת הדואר שלו להשתמש במפתח-הפרטי שלו כדי לפענח את ההודעה, ולהציג אוטומטית את התמונה. בניגוד ל **PGP**, התוכנה מסוגלת לבצע אוטומטית הצפנה, פענוח והצגה של הודעות.

S/MIME אינו קובע מראש את שיטת ההצפנה או החתימה. להיפך, כל הודעה יכולה להיות מוצפנת או חתומה בכל שיטה שהיא. התנאי לפענוח הוא, שתוכנת ה **S/MIME** של הנמען אכן מכירה את אותה שיטת הצפנה. לכן, בספר הכתובות של תוכנת **S/MIME** שומרים מלבד את כתובת הנמען ושמו גם את המפתח הפומבי, תעודת זיהוי וכמובן מידע לגבי שיטת ההצפנה בה יש להשתמש במכתבים שיישלחו אל הנמען.

פרוטוקול **S/MIME** אינו קובע מראש את מדיניות קבלת תעודות הזיהוי. כל יישום וכל משתמש יכול לאמץ מדיניות משלו. כמשתמשים, אנחנו צריכים להחליט על מדיניות זיהוי מחמירה יותר או מחמירה פחות. כלומר, עלינו לקבוע מפורשות עבור כל תעודת זיהוי המוצגת לנו, האם אנו מכבדים את חתימה רשות הזיהוי עליה או לא.

שאלות ותשובות : **http://www.rsasecurity.com/standards/smime/faq.html**

מגבלות יצוא של טכנולוגית הצפנות מארה"ב

ממשלת ארה"ב רואה בטכנולוגיית הצפנה טכנולוגיה צבאית. לשכת היצוא (**BXA**, **http://www.bxa.doc.gov**) במשרד המסחר האמריקאי מפרסמת תקנות מפעם לפעם, על היתרים לשימוש במוצרים מוצפנים בארה"ב, ועל היתרים ליצוא של מוצרים כאלה. ההקלות המתפרסמות מדי פעם הן חלק ממדיניות הממשל, הרואה בקיום תשתית למסחר האלקטרוני נכס אמריקאי לאומי.

תמצית : **http://csrc.nist.gov/keyrecovery/policy.txt**

בשנת 2000 ביטל הממשל האמריקאי את מרבית המגבלות על יצוא טכנולוגיות ההצפנה, וכיום יכולות חברות אמריקאיות לייצא מוצרי תוכנה לשיווק המוני, המכילים גם טכנולוגיות הצפנה. יצוא זה מורשה לרוב מדינות העולם פרט, כמובן, למדינות "אסורות לייצוא" כגון אירן, עירק, לוב וכד'.

לשכת היצוא אינה מגבילה את אורך המפתח במוצרים המיועדים לזיהוי. אבל חברה, המעוניינת למכור מוצרים כאלה, צריכה להוכיח שהם אינם ניתנים להסבה למוצרי הצפנה ובכך עלולים לעקוף את מגבלות היצוא.

למידע נוסף : **http://www.bxa.doc.gov/Encryption**

האם ההצפנה עצמה עמידה בפני פריצה

בעצם, זוהי שאלת המפתח תרתי-משמע. לא דנו עדיין בחוזקן של שיטות ההצפנה, אבל זוהי סוגיית הבסיס. ככלל, חוזק ההצפנה תלוי באורך המפתח. מפתח ארוך יותר, יעניק הגנה חזקה יותר מפני פריצות. מפתח קצר מדי, יחשוף את ההודעה לנסיונות פריצה.

כדי לשבור בכוח (**brute force**) הודעה מוצפנת, יש צורך לנסות את כל האפשרויות למפתח הסימטרי בזה אחר זה. למשל, לשבירת מפתח באורך של 40 ביטים, נזדקק ל 2^{40} נסיונות שונים. נניח שעומדים לרשותינו, 1000 מחשבים, המסוגלים ל 1,000,000 פעולות שונות של פענוח בשניה. נזדקק בסך הכל ל 1100 שניות שהן 18 דקות. יש לשים לב שאחרי 9 דקות יש סיכוי של יותר מ 50% שכבר מצאנו את המפתח. הגדלת המפתח ל 56 ביטים, עם הגדלת כמות המחשבים ל 1,000,000 , נזדקק ל: 10 שעות לסיכוי של 50% ולכל היותר ל- 20 שעות חישוב לפיצוח. אבל, עדיין נזדקק ל 1,000,000 מחשבים...

חברת **Netscape** העמידה למבחן הודעות מוצפנות ב **SSL** של **Navigator 1.1** תוך שימוש בשיטת **RC2** ומפתח באורך של 40 ביטים. ההודעה המוצפנת הראשונה נשלחה ב 14/7/95 ופוצחה ב 15/8/95 ע"י שני צוותים נפרדים. הודעה שניה שהועמדה למבחן ב 19/8/95 נפרצה תוך 32 שעות (!!) ע"י הפעלת אלגוריתם מתוחכם שפיזר את העבודה ע"פ רשת של מחשבים באינטרנט. ב 17/9/95 הצליחו שני מדענים, לחשוף את מנגנון בחירת המפתח הסימטרי האקראי של **Navigator 1.1**. וכתוצאה מכך, הם כתבו תוכנה שרצה על מחשב יחיד, ומסוגלת לשבור הודעה מוצפנת של **SSL** באורך 40 ביטים בתוך שעות ספורות (!!).

דף מידע: **http://pauillac.inria.fr/~doligez/ssl/**

במרץ 1994 הצליחו מתמטיקאים לשבור את אתגר **RSA-129**. הם הצליחו לפרק לגורמים מספר בעל 129 ספרות, שהן 428 ספרות בינאריות. המאמץ נמשך 8 חודשים, וכלל 600 אנשים, ו 1600 מחשבים באינטרנט. המדענים השתמשו בטכניקה תיאורטית שפורסמה 5 שנים קודם לכן. כבר בסיום הפיצוח, פורסמה תיאוריה מתימטית חדשה, המצליחה לקצר את זמן הפיצוח פי 10. מסקנתם של המדענים: "מפתחות **RSA** באורך של 512 ביטים אינם בטוחים יותר, משום שהם ניתנים לשבירה ע"י אירגונים שיהיו מוכנים לשלם כמיליון דולר, ושברשותם מספיק זמן".

דף מידע: **http://www.math.okstate.edu/~wrightd/numthry/rsa129.html**

עיסוק באמצעי הצפנה, התשל"ה-1974

בישראל, הוראות צו הפיקוח על מוצרים ושירותים (עיסוק באמצעי הצפנה), התשל"ה-1974 אוסר על שימוש במערכות הצפנה ללא היתר מפורש מגורמי הבטחון:

"לא יעסוק אדם באמצעי הצפנה אלא על פי רשיון מאת המנהל ובהתאם לתנאי הרשיון".

"עיסוק בפיתוח, בייצור, בהחזקה, בשימוש, ביבוא, בהובלה, בהעברה ממקום למקום או מיד ליד, בהפצה, במכירה או ברכישה של אמצעי הצפנה, של שיטת הצפנה, של מפתח הצפנה, או של רשימה המתייחסת להצפנה, או טיפול בהם בכל דרך אחרת."

נוסח הצו: http://www.law.co.il/computer-law/encryption_order.htm

הוראות צו זה עדיין לא תוקנו, כך שבפועל עדיין קיים איסור לשימוש נרחב באמצעי העברה בטוחה, ללא אישור פרטני. צו גורף זה, מונע שימוש בהצפנה, אך הוא אינו אוסר במישרין שימוש בחתימה דיגיטלית עבור מסמכים לא מוצפנים.

מדינת ישראל מודעת ליתרונותיו הגדולים ולחשיבותו של המסחר האלקטרוני. וכמו כן, ברור לכל שללא תשתית מתאימה של אמצעי זיהוי חזקים, ואמצעי הצפנה מתאימים לא יתקיים מסחר אלקטרוני, ולא ניתן יהיה לנצל את האינטרנט כתשתית לתקשורת מחשבים. לדוגמא, הממשל האמריקני הנוכחי מוביל מדיניות ברורה של שימוש חופשי באמצעי זיהוי, תוך הגבלה של חוזק ההצפנה בה משתמשים (ראה נספח ב').

אורך המפתח שיש לבחור

בעבר, מכיוון שלא היה אישור ייצוא מארה"ב של מפתחות גדולים מ-56 ביטים, אנו כאזרחי ישראל היינו ניצבים בפני בעיה, ומבחינת החוק היבש אין לעסוק כלל בהצפנת. הצפנה כזו, של 56 ביטים, אינה חסינה במיוחד. ארגונים גדולים (ממשלות) בעלי מוטיבציה, ממון, וזמן יכלו אז לפצח הודעות שלנו.
אך כיום, מכיוון שאין הגבלה על אורך המפתח, מקובל היום לחשוב על 768 ביטים כאורך מומלץ למפתח-פומבי של **RSA** לאנשים פרטיים, ו 1024 ביטים למוסדות. רשויות זיהוי צריכות להשתמש במפתחות של 2048 ביטים לפחות. חברת **RSA** מפרסמת מפעם לפעם, אורכים מומלצים למפתחות פומביים. ההמלצה נובעת מגילויים ופריצות דרך במחקרים מתמטיים, ומההתפתחות הטכנולוגית התמידית של המחשבים.

הודעות של מעבדות **RSA** : **http://www.rsasecurity.com/rsalabs/technotes**

כיצד צריכים ארגונים להיערך להעברה בטוחה

כבר כיום מציע שוק התוכנה אפשרויות זמינות של חבילות המאפשרות הצפנה. פרוטוקול **SSL** הוא נפוץ ביותר, וישים מיידית לשימוש. **SSL** מיועד כאמור לשמש כמדיום להעברה בטוחה של דפי מידע (**HTTP**). ניתן לשלב בפרוטוקול אפשרות לזיהוי מוחלט של המשתמשים, ולא רק של השרת. כל הדפדפנים המוכרים הקיימים כיום בשוק תומכים בפרוטוקול תמיכה מלאה. וקיימת אפשרות לרכוש שרתי מידע מתאימים של רוב חברות התוכנה.

לגבי דואר אלקטרוני, כדאי לבחור ב **S/MIME**. גם הוא זוכה לתמיכה נרחבת של כל החברות המובילות, ומאפשר : הצפנה, פענוח וחתימה של מסמכים מכל סוג שהוא. **S/MIME** כמו יתר שיטות ההעברה הבטוחה לדואר אלקטרוני, אינו מחייב התקנת שרתי-דואר מיוחדים או תשתית נפרדת. הדפדפנים מהדור הרביעי של **Netscape** ושל **Microsoft** כבר תומכים בפרוטוקול.

על האירגון לדאוג להמצאותן של תעודות זיהוי בידי עובדיו. למשל, הוא יכול ליצור התקשרות עם רשות זיהוי מתאימה, ולהנפיק דרכה תעודות זיהוי לעובדים. ולחילופין, הוא עשוי להחליט על החזקת רשות זיהוי עצמאית משלו בתוך הארגון עצמו, ולהנפיק עצמאית תעודות זיהוי לעובדים. במקרה השני, הדבר דורש אמצעי אבטחה וחומרה מיוחדים. התקן לתעודות זיהוי הוא כאמור **X.509**, הנתמך ע"י כל תוכנות ההצפנה בשוק כיום.

פעולה אחרונה אך לא פחות חשובה היא כמובן ימי הדרכה ועיון לעובדים. העובד צריך להבין מושגים כמו : הצפנה, פענוח, מפתח פרטי, מפתח פומבי, תעודת זיהוי, ורשות זיהוי. ניתן להצמיד יום הדרכה כזה, להדרכה שיש להעביר בארגון לגבי שימוש בדפדפן אינטרנט מהדור הרביעי. לעובדים שזקוקים לכך, יש להעביר יום עיון נפרד לגבי יכולות להעביר כספים באמצעות האינטרנט.

מה צריך לדעת משתמש הקצה כדי להשתמש בהעברה בטוחה

משתמש הקצה שולט על תוכנות ההעברה הבטוחה, דרך תעודות זיהוי דיגיטליות ודרך המפתח הפרטי שלו. באופן כללי ניתן לפרק את פעולות המשתמש העיקריות למספר פעולות מצומצם.

התחברות לאתר דרך הדפדפן : כאשר הוא מתחבר לאתר באינטרנט המשתמש בהצפנה (**SSL**) כדי להעביר דפי מידע, הדפדפן יבקש מהמשתמש אישור מיוחד כדי לקבל את תעודת הזיהוי של האתר. באחריותו של המשתמש לבדוק מי חתום על התעודה, ולנהוג בהתאם. הנחיות לקבלה או אי-קבלתן של תעודות זיהוי צריכות להיות מופצות בארגון, ע"י אנשים שיתעדכנו דרך קבע במתחדש בתחום.

טיפול בדואר אלקטרוני : המשתמש צריך לנהל פנקס כתובות הכולל בתוכו תעודות זיהוי של הנמענים. במידה ואין לו את תעודת הזיהוי של הנמען, הוא לא יוכל להצפין את ההודעה, אלא רק לחתום עליה. באחריותו של המשתמש, ובניהולה של תוכנת הדואר הוא לעדכן את פנקס הכתובות. אם ההודעות שהגיעו בדואר האלקטרוני סודיות, על המשתמש לנהוג בהן ככאלה.

שמירה על המפתח הפרטי : תנאי מקדים לכל תקשורת מהסוג שתואר הוא שיש למשתמש תעודת זיהוי משלו, ושהוא מחזיק מפתח פרטי באופן שמור. כלומר, על המשתמש לקבוע מדיניות

לשמירת המפתח הפרטי במחשב האישי שלו. שמירת המפתח הפרטי בסוד היא נקודת המוצא, והמשימה הקשה ביותר המוטלת על המשתמש באופן אישי. אין ספק, כי בעתיד המפתח הפרטי ישמר בנפרד מהמחשב על גבי כרטיס חכם, ואז יעלמו כל בעיותינו.

סיכום

עתידה ומהירות התפתחותה של האינטרנט, תלוי ביכולתה לתת למשתמשיה כלי העברה בטוחה: הצפנה, חתימה ותעודות זיהוי.

התפתחות האינטרנט בארץ, והתגברות השימוש במסחר אלקטרוני תלוי בתשתית לתעודות זיהוי דיגיטליות, ולהתפתחות חקיקה בהקשר של הצפנות לצרכי מסחר.

משתמשי האינטרנט צריכים לדעת כיצד להשתמש בכלים להעברה בטוחה הפופולריים, קרי להפעיל נכון את דפדפני הדור הרביעי.

נספח א' - ניתוח שיטת RSA

RSA היא פטנט רשום בארה"ב משנת **1983**, הרשום על שמם של: **Rivest - Shamir - Adelman**.
הרעיון מאחורי ההצפנה הוא שקשה מאוד לפרק לגורמים מספרים גדולים, וכן משפט מתורת המספרים המוכיח כי כמות המספרים הראשוניים היא גדולה מאוד. לכן, יהיה לי קל מאוד למצוא שני מספרים ראשוניים בגודל 200 ספרות (כי יש הרבה), ואם אכפול אותם זה בזה, אקבל מספר בן 400 ספרות, שיהיה קשה מאוד לפרק אותו חזרה למספרים שבחרתי.

לדוגמא: נבחר מספרים ראשוניים בני שתי ספרות: **47** ו **71**. נקבל מכפלה שהיא: **3337**.
כדי לפרק מספר בין **4** ספרות לגורמים צריך לבדוק אם הוא מתחלק בכל המספרים הראשוניים הדו-ספרתיים. אם היינו בוחרים מספרים בני 200 ספרות, היה צורך לבדוק את כל המספרים הראשוניים בני 200 ספרות.

כעת נחשב **(1 - 71)(1 - 47) = 3220**. ונבחר זוג מספרים ראשוניים חדשים: **1019, 79**.
נשים לב ש: **1019** כפול **79 = 1** לפי מודולו **3220**.
המפתח הפומבי: **(3337, 79)** והמפתח הפרטי: **(3337, 1019)**.

כעת אנו יכולים להצפין מספרים הקטנים מ **3337**. אם יש לנו הודעה ארוכה, נפרק אותה לסדרה של מספרים הקטנים מ **3337**.
כדי להצפין את המספר **688** בעזרת המפתח הפומבי יש לחשב **688** בחזקת **79** (מודולו **3337**)=**1570**.
כדי לפענח בעזרת המפתח הפרטי, יש לחשב **1570** בחזקת **1019** (מודולו **3337**)=**688**.

הטענה היא שלא ניתן לנחש את המספר **1019**, אלא ע"י פירוק לגורמים של **3337**, ושימוש ב **79**.
טענה זו אגב, היא חסרת הוכחה מתימטית ! כבר למעלה מ 20 שנה. אבל, כפי שראינו מיטב המתמטיקאים מנסים זה זמן רב להפריך או לאשש אותה ללא הצלחה. במידה שיוכח כי קיימת דרך מהירה אחרת מלבד פירוק לגורמים, ישנה סכנה לפריצת **RSA**.

ראוי לב לעובדה המפתיעה שככל שעצמת המחשבים גדולה יותר, כך עוצמתה של **RSA** מתחזקת.
אמנם לצידו של הפורץ יעמדו משאבי חישוב חזקים, אבל אז נוכל גם אנו להגדיל את אורך המפתח. וזאת משום, שהמחשבים האישיים יוכלו לבצע חישובי העלאה בחזקה מהר יותר, ולכן נגדיל את אורך המפתח. כמו כן, נוכל להבין מדוע הצפנה ב **RSA** היא איטית. וזאת, משום שמשתמשים בהעלאת מספרים בחזקות גבוהות, פעולה הגוזלת זמן חישוב רב.

נספח ב' - הממשל האמריקאי והצפנות

גופים אלה עוסקים בענייני הצפנות בארה"ב.

NSA - Natiaonal Security Agency היא סוכנות מודיעין אמריקאית שעצם קיומה נשמר בסוד שנים רבות. הסוכנות הוקמה ב **1952** ומטרתה היתה לפצח תשדורות רוסיות מוצפנות, וכן לבסס

יתרון אסטרטגי ביכולות הצפנה לגורמי מודיעין אמריקאיים. זהו הגוף שבו עובדים מספר המתמטיקאים הגדול בעולם, יותר מ 6000. מניחים ש **NSA** מקדימה את המחקר האקדמי הגלוי בשנים מספר, ככול שהדבר נוגע להצפנות. כמו כן, זו היא הנחה מקובלת והגיונית היא שלסוכנות מחשבים חזקים ויקרים המיועדים לשבירת הצפנות. הנחה הגיונית נוספת היא ש **NSA** ממקדת תשומת לב רבה יותר ויותר למידע שזורם באינטרנט.

דף הבית: **http://www.nsa.gov**

NIST - National Institute of Standards and Technology היא למעשה אגף במשרד המסחר האמריקאי. ב 1977 הכריזה **NIST** על **DES** כשיטת ההצפנה הרשמית בממשל האמריקאי, ומדי 5 שנים, **NIST** מחדשת את ההגדרה על פי הפיתוחים בתחום. ב 1987 הטיל הקונגרס על **NIST** רשמית את האחריות לפיתוח תקנים להעברה בטוחה עבור שלוש רמות: "מידע רגיש אך לא מסווג" - בין גופי ממשל, "מידע עסקי" - בתוך גבולות ארה"ב, ו "מידע למטרות יצוא" - מסחר אלקטרוני עולמי. **NIST** פנתה ל **NSA** לשם פיתוח האלגוריתמים.

מחלקת אבטחת מידע: **http://csrc.nist.gov/**

BXA - Bureau of Export Administration שייכת אף היא למשרד המסחר ועוסקת בקביעת ההיתרים ליצוא בכלל, וליצוא של מערכות מוצפנות. **BXA** מקבלת הנחיות מ **NIST**, התואמות את מדיניותה של **NSA**. אורך המפתח הסימטרי הוא הקריטריון העיקרי לקביעת היתר היצוא של מוצרי הצפנה.

פירסומים: **http://www.bxa.doc.gov**

ממשל קלינטון-גור, פתח ביוזמה לקידום הפיתוח של סביבת מסחר אלקטרוני אמינה. לשם כך, ברור כי אמצעי הצפנה, ובמיוחד טכנולוגיות של זיהוי וחתימה הם צורך הכרחי ליצירת סביבה כזו. רק תשתית אמינה של העברה בטוחה יכולה לגרום ללקוחות כמו גם למוכרים להשתמש ברשת למסחר אלקטרוני. תשתית זו, מאידך גיסא, אסור לה לפגוע ביכולתן של סוכנויות הביטחון האמריקאיות, לבצע את פעולתם.

ריכוז מידע על מדיניות הממשל: **http://www.epic.org/crypto/**
התנגדות למדיניות הממשל: **http://www.cdt.org/crypto/, http://www.crypto.com**

נספח ג' - העברה בטוחה בשכבת ה IP

עד עתה, דיברנו על תוכנות ופתרונות המחייבים התקנת תוכנה חדשה. יש הטוענים שניתן להימנע מכך, אם ההעברה הבטוחה תתבצע בשכבת ה **IP**. כלומר, אם נחזור לתיאור הסכימטי שבו כל הודעה מועברת באינטרנט מיד ליד דרך צמתים, אזי עלינו לדאוג להצפנה ברמת הצמתים. כלומר, כל הודעה שתצא מהצומת הראשונה, תהיה הודעה מוצפנת. תפקיד הצומת האחרונה בשרשרת, הוא לפענח כל הודעה שמגיעה מהרשת. יש לשים לב, כי חלק מההודעות שתעביר הצומת הראשונה, לא יהיו מוצפנות. זה יקרה, אם הצומת האחרונה היא צומת שלא יודעת לפענח.

היתרונות ברורים: אין צורך בהחלפה או התקנת תוכנה חדשה במחשבים האישיים של המשתמשים, ואין צורך ללמד את המשתמשים מיומנויות של העברה בטוחה. החסרון הוא שהנמען והשולח תלויים זה בזה. כלומר, המשתמש הסופי עלול לטעות ולהעביר מידע רגיש לא מוצפן באינטרנט, אם לנמען אין מערכת מפענחת.

קיימות כמה הצעות ליישום מערכת כזו. **IPSEC** - פרוטוקול להצפנה ולבדיקת מקור הודעה. **S/WAN** - יוזמה של **RSA** לקביעת תקן לקופסאות הצפנה ופענוח כאלה אשר יחצצו בין הארגון ובין האינטרנט.
הצעות אלו הביאו לפיתוחן של מערכות ה-**VPN**, שלא ידונו במסמך זה.

ברור, כי פתרון מסוג זה לא עונה על יתר הדרישות כמו למשל: חתימה דיגיטלית. והוא אינו מהווה פתרון אמיתי עבור שירותי מידע מסויימים, למשל דואר אלקטרוני. לכן, פתרון זה יתקיים כתוספת או כבסיס לפתרונות שהצגנו קודם.

דף מידע: **http://www.cisco.com/warp/public/105/IPSECpart11.html**

נספח ד' - כסף דיגיטאלי באינטרנט

העברה בטוחה מהווה תנאי הכרחי, להפיכת האינטרנט לתשתית מסחר אלקטרוני. טכניקות של חתימה דיגיטלית, והצפנת התקשורת העסקית הן הבסיס עליו נבנים פרוטוקולים שונים. בנספח זה, נתאר בקצרה דרכים להעביר כספים, ונתאר בקצרה את מהות ההצפנה בכל אחת מהן.

פרוטוקול **SET** - הוא הסטנדרט לתשלום באמצעות כרטיסי האשראי. בעל כרטיס האשראי, צריך להצטייד בתעודת זיהוי מיוחדת, שבעזרתה הוא יכול להתחייב לתשלום. בעל חנות ברשת, מזהה את לקוחותיו דרך תעודת זיהוי זו, שלא חייבת להכיל פרטים אישיים של בעל הכרטיס. בתהליך התשלום עצמו, מזדהים הדדית בעל החנות ובעל הכרטיס זה בפני זה. חברת כרטיסי האשראי, מעניקה גיבוי אינטראקטיבי, ומאפשרת לוודא אותנטיות של תעודות זיהוי, וכן מאשרת את ביצוע העסקה לפי גובה הסכום. הפרוטוקול נחשב לאמין ובטוח במיוחד, בגלל הצלבות המידע, והשימוש המאסיבי בתעודות הזיהוי ובהצפנת כל התקשורת הקשורה בעסקה. הפרוטוקול מאפשר ביצוע תשלומים בינוניים (החל מ $20), ותשלומים גדולים מאוד ($10,000 ויותר).

מידע נוסף: **http://www.visa.com/**
וגם: **http://www.mastercard.com/**

כרטיס חכם **Mondex** - זהו התקן חומרה קומפקטי, המיועד להשתלב פיזית על כרטיס האשראי שלנו. בכרטיס צרובה תעודת זיהוי של הבעלים, וכן יש בו רכיבים אלקטרוניים בעלי יכולות הצפנה. הכרטיס מבצע סימולציה של מטבעות דיגיטליים, אותם טוענים לתוכו דרך מכשיר **Mondex** מיוחד בבנק. בכל העברת מטבע בין שני כרטיסים, מחליפים הכרטיסים את תעודות הזיהוי, ומוודאים שיש התאמה בין המפתח הפומבי, למפתח הפרטי של הכרטיס השני. בגלל היישום בחומרה של הכרטיס, ובגלל חוסר הצורך באישור אינטראקטיבי, מאפשר הכרטיס ביצוע של תשלומים קטנים (פחות מ $1) , ובינוניים (עד $100).

מידע נוסף: **http://www.mondex.com/**

כסף אלקטרוני **DigiCash** - מבצע סימולציה של שטרות כסף, אותם מנפיק הבנק ללקוח, ע"פ בקשתו. השטר עצמו הוא הלכה למעשה קובץ מחשב, אותו ניתן להעביר מצד לצד באופן דיגיטאלי. על כל שטר כזה, מופיעה חתימה דיגיטלית של הבנק המאשרת את ערכו, ומעניקה ערבות מתאימה. יש לשים לב, כי הבעלים של השטר יכול לשכפל אותו מספר פעמים, או להעביר אותו כתשלום לאנשים שונים. לכן מי שמקבל שטר כזה, חייב מיידית לפדות את תמורתו הכספית מהבנק. מלבד הבנק, כל הצדדים נשארים אנונימיים לחלוטין. גם כאן מדובר בסכומים בסדר גודל בינוני (עד $100).

מידע נוסף: **http://www.digicash.com/**

מאמר של הועדה בנושא: **http://www.itpolicy.gov.il/topics_ecom/money.htm**

נספח ו' - קישורים והפניות

- מבוא טוב לנושא ההעברה הבטוחה:
  http://www.cs.hut.fi/ssh/crypto/
  הפניות: http://www.cosc.georgetown.edu/~denning/crypto

- שאלות ותשובות:
  /http://www.rsasecurity.com/rsalabs/faq

http://www.cis.ohio-state.edu/hypertext/faq/usenet/cryptography-faq/top.html

- ה **CyberPunks** הם קבוצה ברוטלית, המנסה להפיץ טכנולוגית הצפנות :
http://www.csua.berkeley.edu/cypherpunks/Home.html

- ספר התנ"ך של הקריפטוגרפיה :
"Applied Criptography" / Bruce Schinner, John Wiley & Sons. Second Edition
http://www.counterpane.com/

- מסמכי **RFC** העוסקים בהעברה בטוחה :
http://www.cis.ohio-state.edu/cgi-bin/rfc/rfcNNNN.html