



4 שכבות של אבטחה

- גורם אנושי (הנדסה חברתית, ריגול וכו')
- גורם פיזי
- תוכנה
- תקשורת

סרטון מוטיבציה

User Authentication

- Authentication Using Passwords
 - Complex Password, One time Password, Challenge and Response
- Authentication Using a Physical Object
 - Smart Card, ID Card

Accidental Data Loss

1. Acts of God: fires, floods, earthquakes, wars, riots, or rats gnawing tapes or floppy disks.
2. Hardware or software errors: CPU malfunctions, unreadable disks or tapes, telecommunication errors, program bugs.
3. Human errors: incorrect data entry, wrong tape or disk mounted, wrong program run, lost disk or tape, or some other mistake.


התקפות סייבר דומות לתקיפות פיזיות, אבל גם מאוד שונות:

- **חזרות** – ניתן לנסות בצע התקפת סייבר מיליוני פעמים בשנייה אחת.
- **מרחב היעדים** – גדול בהרבה מאשר מקומות פיזיים.
- **פריצה מרחוק** – לא צריך אפילו לצאת מהבית כדי לבצע התקפת סייבר.
- **הפצה נרחבת** – ניתן להפיץ בקלות רבה (וירוסים וכד').

התקפות סייבר יכולות להתבצע על כל רמה במערכת:

- **התקפה על חומרה** – השתלת צ'יפים, פעימה אלקטרומגנטית.
- **התקפה על תוכנה** – וירוס, תולעת, סוס טרויאני.
- **התקפה על מסד הנתונים** – הזרקת SQL.
- **התקפה על התקשורת** – רחרוח הנתונים, מתקפת מניעת שירות.
- **הגורם האנושי** – החוליה החלשה בשרשרת.

סוגי ההתקפות הללו נקראים **שטח מתקפה (attack surfaces)** – כשאנו באים להגן על מערכת מחשוב צריך תמיד לקחת הכול בחשבון, החל מהחומרה, המשך בתוכנה וכלה בגורם האנושי.



- Confidentiality (סודיות).
- Integrity (שלמות).
- Availability (זמינות).

המטרה	האיום
סודיות המידע	חשיפת מידע
שלמות המידע	שינוי המידע
זמינות המערכת	מניעת שירות

תורת ההצפנה - crypto

כפי שראינו, חלק מההגנה על מידע היא הסודיות שלו. את הסודיות נוכל לספק באמצעות **הצפנה**.
ההצפנה מתבצעת באמצעות מפתח (key) שמשמש כמו מפתח של דלת, שרק בעל המפתח יכול לפתוח (או לנעול) אותה, כך גם מפתח זה מאפשר רק למי שמחזיק אותו בידו לפענח את התוכן שהוצפן.

סוגי הצפנות
נראה עכשיו מספר דוגמאות להצפנות פופולאריות:

- צופן קיסר** בצופן זה עשה שימוש יוליוס קיסר כדי להסתיר את תוכנו של הודעות צבאיות שהוא העביר למפקדיו. צופן זה הוא אחד הצפנים הפשוטים והידועים בעולם ההצפנה. זהו סוג של צופן החלפה שבו כל אות בטקסט מוחלפת על ידי אות הנמצאת בהיסט קבוע של 3. למשל האות A תוחלף באות D, האות B תוחלף ב-E וכן הלאה:



- צופן החלפה בסיסי** צופן זה הוא שדרוג מסוים לצופן קיסר. במקום הזחה קבועה של 3 כאן נוכל לבחור הזחה של $25 \leq n \leq 26$ (בשפה האנגלית 26 אותיות).
לפני העברת ההודעות המוצפנות בין שני צדדים, הם מחליטים בניהם מה המפתח, כלומר מהי ההזחה, וכך כל אחד יכול להצפין ולפענח הודעות.

HELLO

הצפנה

מפתח
צופן החלפה
n=15

WTAAD

פיתוח

מפתח
צופן החלפה
n=15


HELLO

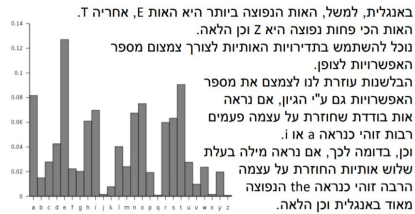
הצפנה

בצופן ההחלפה הבסיסי יש לנו בסה"כ 26 מפתחות, בדיוק כמספר הקומבינציות שאנו יכולים לבצע.

צופן החלפה

צופן זה גם מחליף אותיות אחת בשנייה, אך כאן נבחר תערובת מקרית של אותיות ולא דווקא לפי הסדר. לדוגמא: את A נחליף עם G, את B עם Z, את C עם E וכן הלאה.
שני הצדדים יקבלו טבלת פענוח לאותיות והיא תהיה המפתח. נשים לב כי בצופן זה ישנן 26! מפתחות שונים. זהו מספר עצום של קומבינציות. מעל 2^{88} .
האם זה אומר כי צופן זה אינו פריץ? לא!
אמנם, ניסיון פענוח מתמטי לצופן זה ייקח גם למעבד החזק ביותר מספר שנים טובות, אבל נוכל להשתמש בבלשנות לצורך הפענוח.





מכך אנו למדים דבר מאוד חשוב:
מרחב מפתחות גדול, לא דווקא גורם לצופן להיות יותר חזק.

סוגי התקפות על צפנים מתחלקים למספר סוגים,
ככל שהתוקף יודע יותר על סוג הצופן או על התוכן המוצפן (Known plaintext), כך זה מקל עליו בפריצה. התוקף יכול לנסות לשלוח תוכן משלו (Chosen plaintext/ciphertext) לשרת, לדוגמה, והשרת מצפין או מפענח אותו, וכך הוא יכול לגלות את סוג ההצפנה ולהתקרב אל פיצוח המפתח.

קלוד שאנון



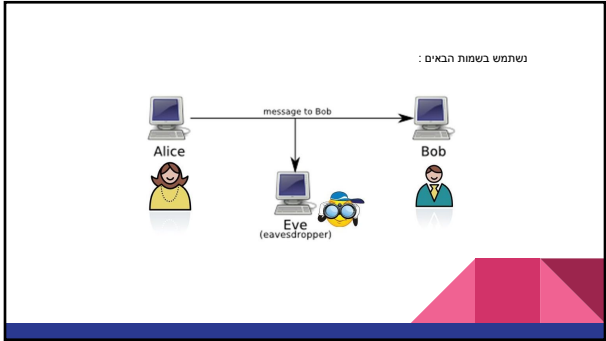
שאנון נחשב לאבי תורת המידע ובעל תרומה נכבדה למדע הקריפטוגרפיה והאלקטרוניקה.

אין אלגוריתם שיכול להחליט עד כמה ההצפנה שלנו חזקה או עד כמה היא פריצה, אך יש לנו את שני המאפיינים שפיתח שאנון על מנת לעזור לנו להעריך עד כמה ההצפנה שלנו טובה:

- **בלבול (confusion)** – מגדיר את מידת הקשר בין הטקסט המקורי לטקסט המוצפן. ככל שיש פחות קשר בין הטקסטים, כלומר, שהבלבול גדול יותר – כך הצופן חזק יותר.
- **פיזור (diffusion)** – מגדיר את מידת פיזור התווים בטקסט. לדוגמה, בצופן ההחלפה, שינוי אות אחת בטקסט המקורי מוביל לשינוי אות אחת בלבד בטקסט המוצפן – כאן הפיזור נמוך. ככל שיש פיזור גדול יותר בין הטקסטים – כך הצופן חזק יותר.

סרטון הדגמת הצפנות ומפתחות

<https://www.youtube.com/watch?v=6-ijHa-olPk&feature=youtu.be>



צופן סימטרי
אלגוריתם הצפנה שבו משתמשים במפתח הצפנה יחיד הן להצפנה של הטקסט הקריא והן
לפענוח של הטקסט המוצפן

חסרונותיהם של הצפנים הסימטריים:
הבעיה העיקרית בצפנים סימטריים היא שכדי ששני צדדים יוכלו לתקשר על
שניהם להיות בעלים של **המפתח**, הן כדי להצפין את הטקסט לפני שליחתו
לצד השני והן כדי לפענחו לאחר שהגיע מהצד השני.
כל העניין הזה פשוט וקל כשצד אחד יכול להעביר לצד השני את המפתח,
אבל מה קורה שאני רוצה לתקשר עם גורם בצד השני של כדור הארץ בלי
שיצוטטו לשיחה?
עוד בעיה בצפני הסימטריים הינה **מחסור בהכחשה**. במידה ומגיעה אליי
הודעה מוצפנת, אינני יכול להוכיח מי יצר אותה מכיוון שלשני הצדדים יש את
המפתח ושניהם יכולים להצפין אותה.

צופן א-סימטרי
מפתח ההצפנה != ממפתח הפענוח
מפתח ציבורי (Public key) שהוא מפתח הצפנה
ומפתח פרטי (Private key) - פענוח
ההתאמה היא חד-חד-ערכית (לכל מפתח ציבורי קיים אך ורק מפתח פרטי יחיד המתאים לו, ולהפך). כדי להצפין
מסר בשיטה זו על המצפין להשיג לידו עותק אותנטי של המפתח הציבורי של המקבל, שכנעתו הוא מצפין
ושולח לו את המסר. רק המקבל מסוגל לשחרר את הטקסט המוצפן בעזרת המפתח הפרטי המתאים שברשותו.
ביטחון שיטת המפתח הציבורי נשען על הקושי שבחישוב המפתח הפרטי מתוך המפתח הציבורי. מסיבה זו
מכונה שיטה זו "א-סימטרית", בניגוד לשיטת הצפנה סימטרית, שבה מפתח הפענוח זהה למפתח ההצפנה

הנשמר בסוד אצל הש

הנשמר בסוד אצל השרת.

1

את בש

מס: 3+7, 2+8, 1+9 = 10
20+80, 10+90 = 100
200+800, 100+900 = 1000

א	ט
ב	ח
ג	ז
ד	ו
ה	פ
ו	צ
ז	כ
ח	ל
ט	מ
י	נ
כ	ס
ל	ק
מ	ר
נ	ש
ס	ת
ק	י
ר	א
ש	ב
ת	ג
י	ד

א	י
ב	כ
ג	ל
ד	מ
ה	נ
ו	ס
ז	ק
ח	ר
ט	ש
י	ת
כ	י
ל	א
מ	ב
נ	ג
ס	ד
ק	ה
ר	ו
ש	ז
ת	ח
י	ט
א	י

א	ט
ב	ח
ג	ז
ד	ו
ה	פ
ו	צ
ז	כ
ח	ל
ט	מ
י	נ
כ	ס
ל	ק
מ	ר
נ	ש
ס	ת
ק	י
ר	א
ש	ב
ת	ג
י	ד

אנטרפיה - מדד לעדול האפקטיבי של מרחב הסתברות.
פיתח קלאוד שאנון

לדוגמה, הטלת מטבע מחזירה אחת מבין שתי אפשרויות, והטלת קובייה מחזירה אחת מבין שש אפשרויות. ברור שאת התוצאה של הטלת הקוביה קשה יותר לחזות מאשר את זו של המטבע. חיבור התוצאות של שתי קוביות מחזיר אחת מבין 11 אפשרויות, שבהן 7 היא השכיחה ביותר, ואילו 2 או 12 נדירות ביחס. כאן לא די למטר שגדל מרחב ההסתברות הוא 11 - ההסתברויות אינן אחידות, ולכן לא ניתן במבט ראשון לקבוע האם תוצאת החיבור קשה יותר לזיזוי מאשר, נאמר, בחירה של ספרה אקראית בין 1 ל-9 (בהתפלגות אחידה בדידה). המטרך להשוות באופן מדויק בין מרחבי ההתפלגות שונים קיים בכל תחומי המדע, ומדידת האנטרופיה באופן שיוצג לוחן שכיחה בפזיקה, בתורת האינפורמציה בביוכימיה (שם היא נקראת מדד שאנון-ויבר) ובתחומים נוספים.

שלמות - Integrity

אז הצלחנו להעביר את ההודעה בסודיות, מה עם השלימות?

Mac

קוד אימות מסרים - Message Authentication Code או בקיצור MAC, הוא שם כולל לקבוצה של פונקציות עם מפתח סודי המשמשות לאימות ולהבטחת שלמות הטקסט הנשלח. פונקציית ה-MAC מקבלת מפתח סודי ואת ההודעה ומפיקה "תג" אותו היא מצמידה להודעה המקורית אשר נשלחת לצד השני. כשהצד המקבל מקבל את ההודעה הוא מפריד ממנה את ה"תג" ומפעיל עליה אף הוא את פונקציית ה-MAC עם אותו המפתח ומקבל אף הוא תג. לאחר מכן הוא משווה בין התג שהשולח שלח עם ההודעה לבין תג זה, וכך הוא יכול לדעת אם ההודעה השתנתה בדרך או לא.

השוחזר:

מכניס את ההודעה ביחד עם המפתח לפונק' MAC ומקבל "תג".
את ההודעה והתג הוא מצמיד ושולח למקבל.



המקבל:

מפעיל אף הוא את פונק' ה-MAC על ההודעה וממפתח ומקבל תג.
לאחר מכן הוא בודק האם אכן שני התגים שווים.



פונקציית גיבוב (hash) חד כיוונית

פונקציית גיבוב חד כיוונית היא פונקציה הממירה קלט באורך כלשהוא לפלט באורך קבוע וידוע מראש.

- פונקציה זו מתוכננת כך שכל שינוי בקלט יגרום לשינוי משמעותי בפלט.
- לא ניתן לחזור להודעה המקורית לאחר הגיבוב.
- אין שתי הודעות עם אותו הגיבוב.

פונקציות גיבוב חג כיווניות ידועות:

- MD5 – המספקת פלט באורך 128 ביט.
- SHA-1 – המספקת פלט באורך 160 ביט.
- SHA-256 – המספקת פלט באורך 256 ביט.

ככל שאורך פלט פונקציית הגיבוב גדול יותר כך הגיבוב נחשב בטוח יותר.

מה ההבדל בין MAC ל-hash? MAC משתמש במפתח בניגוד ל-hash ומכיוון שכך מספק גם "אי הכחשה". כן, ב-hash לא ניתן לחזור חזרה להודעה המקורית, בניגוד ל-MAC.

חתימה דיגיטלית

חתימה דיגיטלית משמשת לאימות זהות מקור מסמך דיגיטלי וכן מהווה אמצעי להבטחת שלמות המסמך ומניעת התכחשות.

כזכור, בהצפנה א-סימטרית יש זוג מפתחות, פומבי ופרטי, שאת מה שהוצפן בפומבי ניתן לפענח רק עם הפרטי ואת מה שהוצפן בפרטי ניתן לפענח רק עם הפומבי.

איך זה מתבצע? השולח מצפין עם המפתח הפרטי שלו את ההודעה (או, ברוב המקרים, את hash) ושולח לנו אותה, כשאני מצליח לפענח את ההודעה עם המפתח הפומבי שלי אני יכול להיות סמוך ובטוח כי מקור ההודעה הוא אכן מהשולח האמיתי, כיוון שקיימת התאמה חד חד ערכית בין המפתח הפרטי למפתח הפומבי, בטוח כי המסמך נחתם אך ורק על ידי מי שמחזיק במפתח הפרטי המתאים.

מכיוון שאלגוריתם הצפנה א-סימטרית דורש עיבוד רב, לרוב נעדיף לחתום על hash שהוא קטן בהרבה, בדר"כ, מן ההודעה המקורית.

חתימה דיגיטלית היא דוגמא לשימוש בא-סימטריות לצורך שלמות. כאן, המפתח הפרטי משמש לחתימה ואילו המפתח הפומבי משמש לאימות החתימה.

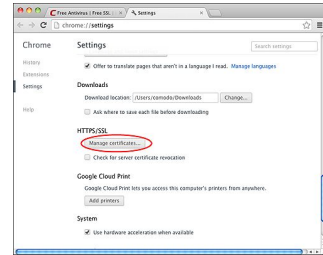
אילו שירותים משתמשים היום בחתימה דיגיטלית



סרטיפיקט



הסרטיפיקט משמש כתעודת זהות דיגיטלית. מסמך זה מכיל פרטים מזוהים אודות בעל הסרטיפיקט, מפתח פומבי של הבעלים, תאריך תפוגה ועוד. הסרטיפיקט חתום ע"י גורם שאנו סומכים עליו שאימת את זהות הבעלים. **איך זה למעשה עובד?** יש מספר לא גדול של ארגונים בינלאומיים הנקראים Certificates Authorities, אלו למעשה ארגונים מוכרים הידועים כאמינים. כשבעל אתר מעוניין בסרטיפיקט כדי שלקוחותיו יוכלו לאמת את זהותו, הוא פונה לאחד מהארגונים האלו עם זוג מפתחות פרטי וציבורי. הארגון מוודא פזיזת את זהותו ולאחר מכן מביאים לו סרטיפיקט חתום לתקופה קצובה. כל דפדפן כיום יודע מי הם הארגונים הללו, וכשאינו נכנס לאתר מסוים מהדפדפן הוא יודע לזהות האם יש או אין סרטיפיקט לאתר וכן להתריע באם הסרטיפיקט שגוי, פג תוקף וכד'. וכך אני יכול לאמת את זהות הבעלים.



תרגול