הצפנה והסתרת מידע

CYBER SCHOOL

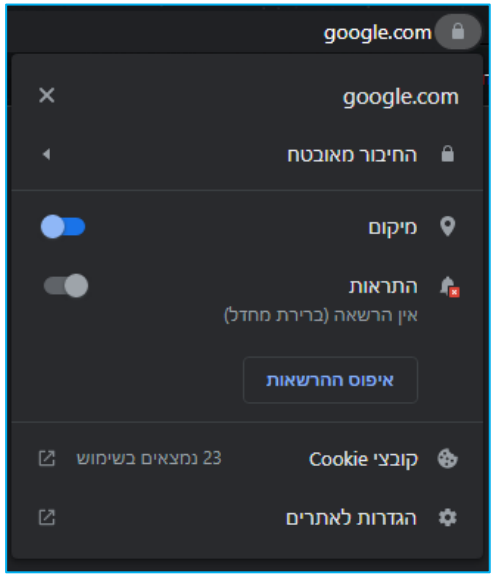
מבוא להצפנה

- שלמות המידע
- סודיות המידע
- סוגי הצפנות ותרגול

חשיבות ההצפנה

הצפנה יעילה היא מאבני הבניין של רשת האינטרנט. ללא הצפנה איכותית שניתן לסמוך עליה, כמעט ולא היינו יכולים להשתמש ברשת!

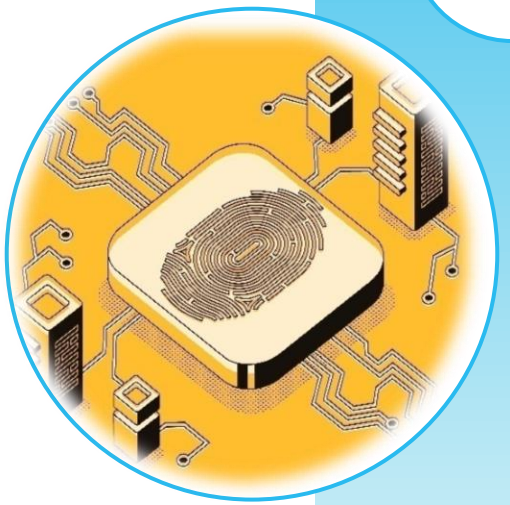
ההודעות והשיחות מוצפנות מקצה-לקצה. לאף אחד מחוץ לצ'אט זה, גם לא ל-WhatsApp, אין אפשרות לקרוא אותן או להאזין להן. יש להקיש לקבלת פרטים נוספים.



הצפנה- הגדרות בסיסיות

שלימות המידע

כוונת המושג שלמות הוא - שהמידע ששלחתי הוא בדיוק אותו המידע שהגיע ליעד. מדוע זה כל כך חשוב?! אז בואו נאמר ששלחתי מתכון סודי לעוגה, אם מישהו שינה לי את תוכן הקובץ, העוגה כבר לא תצא אותו דבר נכון?



אז איך נשמור על המידע שלנו שלם?

כדי לשמור על שלימות המידע אנו משתמשים באלגוריתם מסוג HASH.

מה זה אומר? אלגוריתם הממיר בצורה חד כיוונית את התוכן לקוד מסוים.

<u>דוגמה:</u>

אם אזין את המילה "שלום",

כתובת הHASH הייחודית המוגדרת למילה היא:

037f8f18b89a943fc03d827d465ab493

טרמינולוגיה והבנות בסיסיות

דוגמה לחידוד ההבנה!

בואו נאמר שאנו צריכים לשלוח חבילת ממתקים לחבר שלנו לכבוד החג ומאוד חשוב לנו שהוא יקבל את כל החבילה בשלמותה ושאף אחד לא יוציא שום דבר.

בשביל להצליח אנו יכולים לעשות רשימה של כל הממתקים שנמצאים בתוך החבילה ולשלוח את החבילה עם הרשימה, בשביל שהחבר יוכל לבדוק אם מה שהוא קיבל תואם לרשימה ששלחנו, ולדעת שכל הממתקים עברו בבטחה!

תרגול קצר

המרת HASH

המשימה

נתנסה בהמרת טקסט באמצעות מחשבון HASH מסוג MD5

https://www.md5hashgenerator.com/

השלבים

- היכנסו לאתר הממיר טקסט ל-HASH והמירו את שמכם
- תשוו בין חברי וחברות הכיתה את המחרוזות...
- האם יתכן שיצאו מחרוזות זהות? אם כן, איך?

כלים

דפדפן

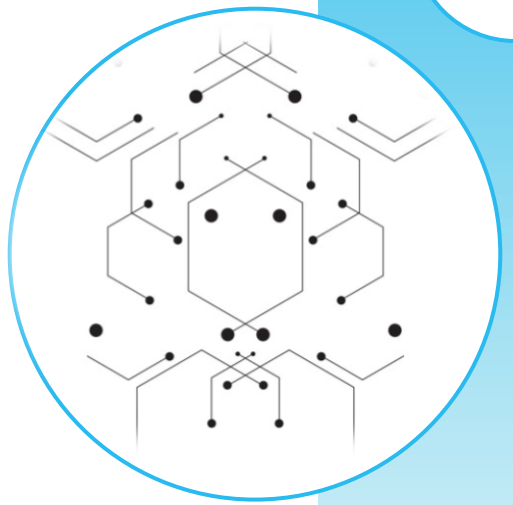
קבצים קשורים

הצפנה – סודיות המידע

הצפנת המידע דואגת שלאף אחד לא תהיה גישה למידע שלי, ע"י כך שאצפין אותו בעזרת אלגוריתם דו צדדי: שלא כמו HASH ניתן לתרגם אותו ע"י מפתח ההצפנה. לאלגוריתם אנחנו קוראים מפתח ההצפנה, משום שבעזרתו נצפין ונפענח את המידע, כמו שמפתח נועל ופותח דלת או ארון.

טרמינולוגיה והבנות בסיסיות

סוגי הצפנות – שחלוף (א"ת ב"ש)



הצפנה על פי צופן שחלוף, כל אות מוחלפת במסר המקורי באות אחרת – כך מתקבל המסר המוצפן. מכאן השם צופן שחלוף. סדר האותיות אינו משתנה בתהליך ההצפנה. אחת משיטות השחלוף הפשוטות נקראת אתב"ש.

טרמינולוגיה והבנות בסיסיות

סוגי הצפנות – צופן הזזה (יוליוס קיסר)

צופני הזזה הם סוג של צפני שחלוף. הם נקראים גם בשם צפני יוליוס קיסר, כיוון שהוא היה הראשון שהשתמש בהם, להעברת מסרים כבר לפני 2500 שנים. מפתח הצופן הוא מספר, הידוע רק לשולח המסר ולנמען. מספר זה מצביע על גודל ההזזה.
דוגמה : א' במפתח הזזה של +1 הופך ל-ב'.

תרגול קצר

פענוח של צופן הזזה

המשימה

פענחו את הצפנים הבאים:

1. " **רכמקצ** " לפי מפתח א"ת ב"ש
2. " **געיפ עסיעם** " לפי צופן שיחלוף מפתח +4.

השלבים

- השתמשו במפתחות ההצפנה לפי סוג ההצפנה.
- העתיקו את הצופן לעורך טקסט.
- וכתבו את הפתרון מתחת לכל אות.

כלים

עורך טקסט

קבצים קשורים

- מפתחות ההצפנה (בשקופית הבאה)

מפתחות הצפנה

חשוב לשים לב : בהצפנה נבחר אותיות מהשורה העליונה ונחליף אותן בשורה התחתונה .

בפענוח : נבחר אותיות מהשורה התחתונה ונחליף אותם באותיות מהשורה העליונה.

- **מפתח הצפנה א"ת ב"ש:**

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

- **מפתח הצפנה שיחלוף 4+:**

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

הצפנה בהיסטוריה

בעיר ספרטה, הנמצאת ביוון העתיקה, השתמשו כבר במאה ה 5 לפני הספירה, בפס צר של פפירוס, או קלף עור המגולגל על מוט בקוטר מסוים. זוהי שיטת ההצפנה העתיקה ביותר המתועדת בהיסטוריה. מלכים ומפקדי צבא היו משתמשים בשיטה זו כדי להעביר מידע חשוב אל ומשדה הקרב.

מאוחר יותר בהיסטוריה התפתחו שיטות הצפנה מורכבות וחזקות יותר, כדוגמת ה**אניגמה** במלחמת העולם השנייה (הצפנה אשר פיצוחה הוביל להמצאת המחשב על ידי אלן טיורינג).

CYBER SCHOOL

הסתרת מידע – סטנוגרפיה

מבוא להסתרת מידע

- מהי "סטגנוגרפיה"?
- הטכניקות השונות
- נחביא תמונה בתוך קובץ טקסט

מהי סטנוגרפיה?

"סטנוגרפיה" נקראת גם – "אמנות הכתיבה המכוסה".
הסיבה לכך היא מפני ש-"סטנו" פירושו כיסוי ו-"גרפיה" היא כתיבה.

והכוונה היא להעברת מידע בצורה סודית.
בקריפטוגרפיה (הצפנה) אנו מצפינים את המידע
אך לא מסתירים אותו.

סטנוגרפיה

מטרות השימוש בסטנוגרפיה:

- ארגוני טרור ברחבי העולם
- ארגוני ביון חשאיים של מדינות שונות
- האקרים בפשעי סייבר שונים

CYBER SCHOOL

טכניקות הסתרה

טכניקות שונות

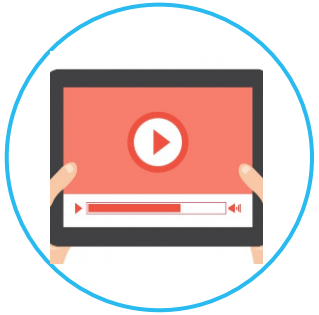
באופן כללי יש שני סוגים של סטנוגרפיה: פיזית ודיגיטלית.

הסתרה פיזית - מי שמחביא תשובות במבחן בבית הספר יודע במה מדובר!

הסתרה דיגיטלית - ניתן להסתיר תוכן בקבצים ולשולחם בעזרת האינטרנט.

טכניקות הסתרה דיגיטליות

ניתן להסתיר מידע בתוך תמונה



ניתן להסתיר מידע בקבצים בפורמטים שונים כגון אודיו וידאו ועוד..

בדרכים יותר מתקדמות נשתמש באלגוריתמים מאוד מתוחכמים שפותחו לצורך זה.

CYBER SCHOOL

תרגיל

התנסות בהסתרת מידע

המשימה

הסתרת קובץ טקסט בתוך תמונה.

השלבים

- ניצור קובץ טקסט.
- נוריד תמונה של jpg.
- נשתמש בCMD על מנת להריץ את הפקודה.

כלים

עורך טקסט

CMD

קבצים קשורים

- קובץ מעבדה 1

שאלות?