**מערך שיעור קצר**

**המשימה:** כתיבת פעילות קצרה תחת הנושא רשתות ואינטרנט (נושא ספציפי לבחירתך) בטופס זה. אורך הפעילות צריך להיות בין 10-20 דקות (לפי הצורך שלך) מותר שיהיה דרוש ידע מקדים מהחניכים רק נדרש לציין זאת.

הקפד למלא את כל החלקים.

**שים לב -** המטרה לכתוב פעילות ולא שיעור. העבר את התוכן הרצוי בעזרת משחקים/ הדמיות/ כל דרך יצירתית.

**בהצלחה!**

* **פרטי מחבר המערך:**
* שם: ניר חמו
* מייל: nir.chamo@gmail.com
* טלפון: 0545706728
* מיועד לטווח לגילאים: 15-18

* **תיאור השיעור**

בשיעור נלמד על הצפנה סימטרית, ובפרט את זו של diffie hellman, אותה גם ניישם. נצפה בסרטון תאורטי אשר מסביר את הנושא, נתנסה בעצמנו באמצעות צבעי מים / גואש ולאחר מכן החניכים יתחלקו לזוגות וישלחו אחד לשני תמונות מוצפנות.

* **מה התלמידים יפיקו מהשיעור? (מטרות)**
* החניכים ילמדו מה זו הצפנה סימטרית
* החניכים יתנסו בכך באופן קונספטואלי
* החניכים יבצעו זאת באמצעות מחשב כאשר הם מבינים את התהליך
* **דרישות קדם מהתלמידים:**
* הבנה כללית במחשבים, אין ידע ספציפי שיש בו צורך, בעיקר אינטואיציה
* ידע מספק באנגלית כדי לראות סרטון לימודי
* **לוגיסטיקה נדרשת:**
* רשת של מחשבים מחוברת
* צבעי מים / גועש
* מקרן ורמקולים
* Discord או כל אפליקציית צ'אט אחרת בה יוכלו להיות כל חברי הכיתה באותה הקבוצה
* **מהלך השיעור:**

💡 – נושא לדיון עם הילדים

⭐ - פעילות

🎥 - צפייה בסרטון

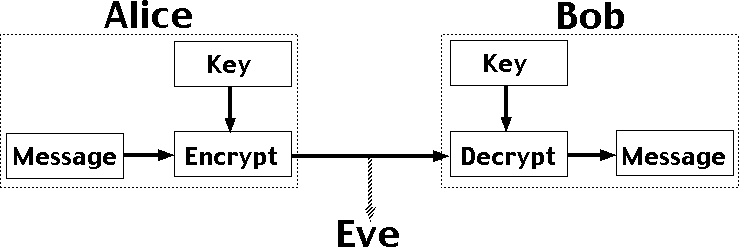
⭐ נתחיל את השיעור בפעילות (5 דק') –

* + החניכים יתחלקו לקבוצות של 3, שני ייצרני צבעים ומנחש אחד.
  + תחילה, יבחרו השלושה צבע אחד עליו כולם מסכימים אשר יהיה הצבע הציבורי. לאחר מכן, כל אחד מהצבעים יבחר צבע פרטי, אשר רק הוא יידע מה הוא.
  + כעת, כל ילד יערבב את הצבע המוסכם על כולם יחד עם הצבע הפרטי שלו, ויעביר את התערובת לילד השני, כך שהמנחש יכול לראות את התערובות שהשניים העבירו ביניהם.
  + כעת, כל אחד מהילדים יערבב את הצבע החדש אותו קיבל עם צבע הפרטי שלו. משמע, לכל אחד מהילדים יש את אותו הצבע. צבע זה יהיה הצבע הסודי.
  + המנחש ינסה לנחש, לפי הצבע הציבורי והתערובת שעברה בין הצבעים, מה הצבעים הסודיים של הצבעים.

🎥 - כעת נצפה [בסרטון](https://www.youtube.com/watch?v=YEBfamv-_do) אשר מסביר על הצפנה עד ל- 04:23.

כעת, משהילדים הבינו כי התנסו בהצפנה סימטרית, הגיע הזמן לנסות זאת במחשבים.

\* חשוב לוודא שכולם הבינו את הסרטון, במידת הצורך אפשר גם להוסיף דפי הסביר שיהיו לילדים לחלק עם המעבר למחשבים ובכללי שיהיה להם מהפעילות \*



⭐ - Meme Generator – מול המחשבים (5 – 10 דקות)

נבקש מכולם להיכנס לקישור :

[nirch99/meme-hash: Educational DH encryption tutorial for Tech Lift (github.com)](https://github.com/nirch99/meme-hash)

בקישור ישנו קובץ README אשר מסביר את ההוראות. לדעתי זו התנסות מעולה לאלו מהם שעדיין לא ראו איך נראה פרויקט ומה זה git.

מצרף כאן הסבר בעברית עבור המנחה כך שיוכל להסביר לילדים:

מדובר בעמוד אינטרנטי אשר מהווה גנרטור ליצור והצפנה של ממים. הגנרטור משתמש בשיטת דיפי-הלמן ליצירת המפתחות הסודיים, כאשר החניכים צריכים לשתף ביניהם את הערך public key ולשמור בסוד את private key ואת secret. לאחר מכן, החניכים יכולים לייצר ממים על בסיס טמפלייט של “Doge” ולשלוח אותם מוצפנים האחד לשני, כך שכל צמד של חניכים יוכל להצפין ולפענח ממים ביניהם מבלי ששאר חברי הכיתה יוכלו לפענח אותם.

קישור לעמוד - [Meme Hash - Tech Lift (nirch99.github.io)](https://nirch99.github.io/meme-hash/)

הפעילות מחולקת ל-3 שלבים:

חלק 0 – הכנה לפעילות

תחילה, יש לחלק את החניכים לזוגות, ולפתוח לכולם חדר משותף ב-Discord / כל פלטפורמה אחרת. נבקש מהם לנהל את כל השיח ביניהם רק שם.

חלק I – מפתחות ויצירת "סוד"

לכל חניך ניתן מראש מפתח פרטי ומפתח ציבורי. אלו חושבו מראש כדי לחסוך סיבוך וטעויות אפשריות. על כל חניך לשלוח בקבוצה את המפתח הציבורי שלו בלבד. כעת, כל אחד יעתיק את המפתח שבן הזוג שלו ויזין אותו בשדה Your partner's public key.  
כעת, כל חניך ילחץ על הכפתור Generate secret ויתקבל ה-"סוד". ה-"סוד" אמור להיות זהה אצל שניהם, אולם אסור להם לשלוח אותו.

חלק II – יצירת ממים והצפנתם

כעת כל חניך יצור מם כרצונו, ויצפין אותו באמצעות ה-"סוד" שלו, אשר אותו הוא יזין בחלון קופץ כאשר ילחץ על הכפתור encrypt. שדה הטקסט התחתון יכיל את הניתוב למם באופן מקודד.

על כל חניך להעתיק את הניתוב המקודד ולשלוח בקבוצה עם שאר החניכים.  
  
הכפתור preview מאפשר תצוגה מקדימה של המם, אולם לא חייב ללחוץ עליו כדי לייצר את המם.

חלק III – פענוח המם

כל חניך יכניס את הנתיב המקודד אותו קיבל מחברו, ובחלון הקופץ יזין את ה"סוד". כעת, המם של בן הזוג שלו יופיע מצד ימין.  
ניתן להציע לחניכים לקחת נתיבים מקודדים שחניכים אחרים שלחו ולפענח אותם באמצעות ה-"סוד" שלהם, כך שיוכלו לראות בעצמם כי הדבר לא יעבוד.

וזהו, נקווה שכולם נהנו ולמדו!

**בהצלחה!**