24 יולי 2021

אבטחת מידע 10313

<u>תרגיל 1</u>

יש להגיש לכל היאוחר עד: 7 באוגוסט 2021 בשעה 23:00

הגשה ביחידים (**<u>לא</u>** זוגות)

מרצה: ד"ר עמית קליינמן

בודק: ערד פלד

1. במילים שלכם, השתמשו בכל המושגים הבאים להרכבת פסקה המסבירה את הקשרים ביניהם.

א. **פגיעות** (Vulnerability)

ב. **ניצול** (Exploit)

ג. **בדיקות חדירות** (Penetration Testing)

.2

א. בעזרת מילת הקוד **SECURITY** <u>פענחו</u> את המסר **UEPN KWNAJ TUBL**, שהוצפן בשיטת ויז'נאר <u>AutoKey</u>.
(תשובה סופית ללא דרך לא תתקבל!)

ב. מסר ארוך יותר, באורך 200 תווים, הוצפן באותה מילת מפתח.
כאשר המסר שודר לצד המפענח, חל שיבוש באות ה-31 במסר המוצפן והיא התחלפה לאות אחרת. כאשר המפענח, אשר אינו מודע לשיבוש, ינסה לפענח את ההודעה, אילו אותיות יתפענחו נכון ואילו לא?

ג. הניחו כי אתם צריכים להצפין מחדש את ההודעה המוצפנת המופיעה בסעיף א. **באותה שיטה עם אותו מפתח.** האם ניתן לבצע את שתי פעולות ההצפנה באמצעות פעולת הצפנה אחת (באותה השיטה) של ההודעה הגלויה? הסבירו את תשובתכם. אם תשובתכם חיובית - מה יהיה המפתח לפעולה זאת? אחרת הסבירו מדוע.

.3

הצפינו הודעה בת 12 אותיות באמצעות **Vigenère** באופן הבא:

I. ההודעה שעליכם להצפין הינה שמכם הפרטי משורשר לשם משפחתכם (הכל באנגלית וללא רווחים).
II. אם ההודעה ארוכה מ 12 אותיות, השמיטו את האותיות האחרונות. אם ההודעה קצרה מ 12 אותיות, הוסיפו אותיות מהאלפבית האנגלי שטרם הופיעו בהודעה ע"פ סדר הופעתם באלפבית.

לדוגמא אם השם הוא John Snow ההודעה שעליך להצפין הינה: JOHNSNOWABCE

III. השתמשו במפתח: **CYBER**

ציינו את ה Plaintext, Ciphertext והסבירו את תהליך ההצפנה.

4. הסבירו את המושג **מתקפת כוח גס** (Brute Force Attack) – האם מעשי להשתמש בה? אם לא מדוע? אם כן מדוע? באילו נסיבות? .