**שיעורי בית - סייבר**

**ש.ב 1**

1. הוירוסים הראשונים נכתבו למטרות POC ועל מנת לספק את האתגר והסקרנות של המפתחים
2. בשנת 2003 פותח וירוס בשם Fizzer למטרות רווח
3. שחקנים נוספים נכנסו לתחום המו"פ של וירוסים - למשל גופי ביון, חברות אבטחת מידע (מהצד המגן). דוגמאות בולטות הן מתקפות סייבר שמבוצעות על ידי מדינות כלפי מדינות אחרות.  
   ממש ביומיים האחרונים דווח על השבתה נרחבת בתחנות דלק רבות באיראן, והשתלטות על שלטי חוצות ושתילת מסרים המעודדים התקוממות.  
   בנוסף, דווח בתקשורת הזרה כי וירוס שכונה Stuxnet פגע פגיעה אנושה בתוכנית הגרעין של איראן לפני כעשור.

**ש.ב 3**

שרלוק הולמס ותעלומת הדמויות המרקדות:

**קריפטוגרפיה** - קריפטוגרפיה היא המלאכה של העברת מידע בין צד א' לצד ב' כך שרק שני הצדדים מסוגלים להבין את המידע המשודר ולשדר בעצמם. בדרך כלל נעשה באמצעות "ערבול" המידע באופן הידוע רק לצדדים המשוחחים. שפת "הדמויות המרקדות" הינה דוגמא לקריפטוגרפיה שנעשה בה שימוש על מנת להסתיר את תכני השיחות בין אנשי פשיעה בשיקגו בעבר וכמו"כ בין הדמויות אייב ואלסי.

**קריפטואנליסיס** - מלאכת גילוי או פענוח הצפנה או מסרים שמועברים בשיטות קריפטוגרפיות. בסרטון מודגם כיצד שרלוק הולמס מצליח להבין באמצעות שכיחותן של מילים ואותיות בשפה האנגלית, כיצד נראית חוקיות ההצפנה ולשבור אותה.

**התחזות** - גרימה לאחד הצדדים בשיחה קריפטוגרפית להאמין כי הוא מדבר עם הצד השני, באמצעות שימוש בשפה הקריפטוגרפית הסודית. שרלוק משתמש בשיטה זו על מנת להערים על אייב ולגרום לו להגיע אליו ולבסוך להילכד.

**ש.ב 4**

בסרטון מתארים החוקרים חולשות בקונסולת המשחק PlayStation3. לקראת סוף הסרטון מתוארת חולשה בעייתית במיוחד שבעצם חושפת את הקונסולה באופן מוחלט לפגיעויות.

הקונסולה עושה שימוש באלגוריתם הצפנה א-סימטרית על מנת להצפין מידע, ובתעודות חתומות דיגיטלית על מנת להוכיח את אמינות המידע.

האלגוריתם שבו נעשה שימוש הינו אלגוריתם ידוע ונפוץ, שלא ידועה כיום דרך יעילה לפרוץ אותו בזמן סביר.

עם זאת, מדובר באלגוריתם שעושה שימוש בנוסחאות מתמטיות שחלקן נסמך על כך שיוגרל בכל שימוש מספר גבוה מספיק ורנדומלי מספיק כדי להבטיח את יעילותו, ואילו מפתחי הקונסולה טעו בכך שהשתמשו במספר קבוע שבסופו של דבר נוחש.

ניחוש המספר איפשר לחוקרים לפצח את מפתחות ההצפנה וכך נותרה המערכת פגיעה לזיופים ושינויים.

החולשה לא תוקנה מכיוון שמדובר בשינויים חומרתיים או בשנמוך משמעותי של המכשיר, וכך נוצר נזק בלתי הפיך למוצר.

**ש.ב 6**

רשת AirGap היא רשת סגורה המבודדת משאר האינטרנט, לוגית ופיזית. מטרת רשת מהסוג הזה הינה הגנה ברמה גבוהה יותר מפני איומים חיצוניים, בדרך כלל בעקבות רגישות המידע המוחזק ברשת.

דרכים לחדור אל הרשת:

1. רמקולים: החדרת תוכנה באמצעים פיזיים (flash drive או דיסק) שגורמת לרמקולים להשמיע צלילים בתדר שקשה לשמוע, שאותם ניתן לתרגם לאותות דיגיטליים באמצעות, למשל, מכשיר סלולרי שנמצא בסביבה.
2. קרינה אלקטרומגנטית: רכיבים במחשב פולטים קא"מ, וניתן באמצעות וירוס לבצע מניפולציות תוכנה כך שתיפלט קרינה שאפשר לתרגם למידע דיגיטלי.
3. מאווררים: ניתן לגרום אפילו למאוורר של מחשב לנוע באופן מסוים ולהשמיע קולות בצורה שמאפשרת "לקודד" ולקלוט מידע דיגיטלי.