13 אוגוסט 2021

אבטחת מידע 10313

**<u>תרגיל 2</u>**

**יש להגיש לכל היאוחר עד: 20 באוגוסט 2021 בשעה 17:00**

מרצה: ד"ר עמית קליינמן

בודק: ערד פלד

1. מודיעין חיל הים (מד"ן) קלט הודעות מכלי שייט עוין של ארגון טרור. ידוע כי:

- ההודעות הוצפנו ע"י מכונת אניגמה שארגון הטרור רכש באתר AliExpress.
- ארגון הטרור רכש 2 מכונות אניגמה ומד"ן הסיק ששתיהן יוצרו בגרסה האזרחית (לא הצבאית), ע"פ המספרים הסדוריים של המכונות שנרכשו.
- מד"ן גילה גם כי ארגון הטרור רכש 2 סדרות זהות של 5 דיסקים בכל אחת, כאשר בכל דיסק 26 אותיות המסודרות בסדר אקראי שונה.
- לכל מכונה יש 3 חריצים כאשר יש להכניס אליהם 3 דיסקים.
- הצד השולח והצד המקבל מסכמים ביניהם על שלושת הדיסקים שיוכנסו ובאיזה סדר.

במד"ן קיים כיום לחץ עבודה עצום בין השאר לאור אירועי תקיפת הספינות במפרץ הפרסי. לפיכך הוחלט על שכירת סטודנטים חכמים ממחלקת מדמ"ח במכללת אפקה לשם סיוע בפענוח התשדורות החשובות שנקלטו מכלי השייט העוין הנ"ל.

1.1. בסיכום המקצועי שאתם מכינים למד"ן עליכם להצביע על 3 חולשות של מכונת האניגמה (במכונה עצמה ו/או בתשדורת שלה) שסייעו בשבירת תשדורות אניגמה בזמן מלחמת העולם ה-2. אנא הסבירו כל אחת מחולשות אלו.

1.2. מד"ן גילה שארגון הטרור משדר מכלי השייט העויין הודעות המכילות בתחילתן את מפתח ה-session בדיוק כפי שהגרמנים שידרו בזמן מלחמת העולם ה-2. לפיכך מחלקת הרכש של מד"ן רכשה מכונת אניגמה זהה, ביצעה חישובי אורכי שרשראות עבור כל אחד מהמפתחות האפשריים ושמרה את כל רשומות הערכים במסד נתונים. מבנה הרשומה הינו:
{מפתח, [סדרת אורכי שרשראות]}.
טבלה 1 כוללת 4 רשומות מתוך מסד נתונים זה.
מה מספר הרשומות הכולל במסד הנתונים הזה? הסבר/י את תשובתך!

**<u>טבלה #1</u>**

| # | Chain lengths<br>Mater-key | I | II | III |
|---|---|---|---|---|
| **1** | A B E | {2, 6, 10, 2, 3, 3} | {9, 10, 7} | {10, 11, 5} |
| **2** | C A T | {4, 9, 8, 2, 3} | {5, 2, 5, 6, 8} | {10, 11, 5} |
| **3** | D I R | {4, 9, 8, 2, 3} | {9, 10, 7} | {8, 6, 12} |
| **4** | S A T | {2, 6, 10, 2, 3, 3} | {5, 2, 5, 6, 8} | {8, 6, 12} |

1.3. טבלה 2 כוללת את ששת התוים הראשונים של כל אחת מ-30 ההודעות שנשלחו מכלי השייט העויין ונקלטו ע"י חוליית מד"ן על ספינת חיל הים.
מהו המפתח הראשי (Master Key) של מכונת האניגמה בזמן התשדורות הנ"ל? עליך להראות בדו"ח שלך את חישובך ולהסביר בפרוט כך שקציני מד"ן יבינו כהלכה את התשובה.

**טבלה #2**

| 6 | 5 | 4 | 3 | 2 | 1 | Letter number / Message number |
|---|---|---|---|---|---|---|
| M | P | T | V | A | B | **1** |
| K | L | F | B | Z | E | **2** |
| J | B | Q | M | K | D | **3** |
| D | F | V | P | G | X | **4** |
| K | O | J | B | H | N | **5** |
| C | H | V | X | I | X | **6** |
| J | N | R | M | L | O | **7** |
| P | X | A | Y | Y | C | **8** |
| G | Z | B | A | X | F | **9** |
| H | T | D | C | Q | Y | **10** |
| V | C | C | E | M | A | **11** |
| F | G | E | G | N | G | **12** |
| Q | J | G | D | R | Z | **13** |
| Y | A | K | F | V | M | **14** |
| L | V | I | S | O | H | **15** |
| A | Q | L | H | W | K | **16** |
| B | K | H | T | P | I | **17** |
| E | D | N | I | B | P | **18** |
| I | W | O | K | S | Q | **19** |
| O | U | P | L | C | J | **20** |
| R | E | M | J | T | L | **21** |
| U | I | S | N | D | R | **22** |
| X | F | W | Q | G | V | **23** |
| N | R | U | R | E | W | **24** |
| W | S | X | O | J | S | **25** |
| T | M | Z | U | F | T | **26** |
| C | Y | Y | X | U | U | **27** |
| P | L | G | Y | Z | Z | **28** |
| Z | K | C | W | P | A | **29** |
| S | G | D | Z | N | Y | **30** |

2. המחלק המשותף הגדול ביותר ((Greatest Common Divisor (GCD)
מצא/י את GCD לזוגות הבאים. בבקשה הצג/י את חישובך:
   I. GCD(195,13)
   II. GCD(250,17)
   III. GCD(2021,60)
   IV. GCD(333, 259)
   V. GCD(908, 907)

3. אלגוריתם אוקלידס המורחב (Extended Euclidean Algorithm)
מצא/י X ו-Y המקיימים את המשוואות הבאות. בבקשה הצג/י את חישובייך
   I. $x \cdot 2020 + y \cdot 151 = GCD(2020,151)$
   II. $x \cdot 2020 + y \cdot 275 = GCD(2020,275)$