



המוזיאון הלאומי למדע, טכנולוגיה וחלל  
מרכז דניאל ומטילדה רקנאטי (ע.ר.)  
חיפה



"קשר חם" – המרכז לקידום  
שיפור וריענון החינוך המתמטי  
הטכניון, חיפה

# הצפנה

חלק ב' – הצפנה אסימטרית

כתיבה: תמר ריינר  
בסיוע: יעל אדרי

ייעוץ מדעי: פרופ' נצה מובשוביץ הדר - הטכניון,  
פרופ' מוני נאור - מכון ויצמן למדע

## תודות

שתי החברות העוסקות בהצפנה מוצעות לחוגי מחוננים, למורים ולמדריכים בחוגי מדע. החוברת הראשונה "הצפנה סימטרית", מתאימה לחט"ב. החוברת השניה "הצפנה אסימטרית", לחטיבה העליונה. במקורו נכתב החומר עבור פרוייקט האולימפידיע של מדע-טק בשנת 2003. פרוייקט שמטרתו עידוד המצוינות בקרב תלמידי חט"ב.

כשהציעה לי פרופסור נצה מובשוביץ-הדר לכתוב חומר לימוד בנושא ההצפנה, עבור משתתפי האולימפידיע, נראתה לי המשימה קשה ומורכבת. שכן, הנושא הוא חדשני ולמיטב ידיעתי לא עובד עדיין ללימוד לא אוניברסיטאי. לאחר לבטים החלטתי להיכנס להרפתקה, שתוצאתה היא חוברות הלימוד המונחות לפניכם. אחרי תחקיר ראשוני נפגשנו עם פרופסור מוני נאור שהוא מומחה בעל מוניטין בינלאומי בתחום - וקבלנו ממנו את ברכת הדרך. בהמשך הצטרפה למאמץ יעל אדרי, מרכזת האולימפידיע במוזיאון הלאומי למדע בחיפה. אני אסירת תודה לכולם על תרומתם.

לפרופסור נאור שנאות לתרום מזמנו ולעצותיו החשובות שסייעו לי למצוא את דרכי בשפע החומר, הסבוך לעיתים. לפרופסור נצה מובשוביץ-הדר, שאלמלא היא לא היה החומר נכתב. היא שהעלתה את הרעיון להקדיש את האולימפידיע לנושא ההצפנה ותרמה לאורך כל הדרך את רעיונותיה היצירתיים, את ניסיונה בהוראת המתמטיקה ואת קפדנותה הבלתי מתפשרת לאיכות החומר הכתוב.

לצוות המוזיאון שעצותיו תרמו לשיפור החומר: לפרופסור יורם זבירין, מנהל המוזיאון, שלמרות עיסוקיו הרבים, טרח לקרוא בקפדנות את החומר והעיר את הערותיו.

ליעל אדרי, רכזת פרוייקט האולימפידיע, שעברה בקפדנות על הטיוטות, חשפה נקודות תרפה והציעה שיפורים משמעותיים. תכננה ובצעה את כל השרטוטים מאירי העיניים, הדיאלוג הענייני בינינו השביח את המוצר הסופי.

לדליה כץ, מנהלנית המוזיאון, על נכונותה לסייע תמיד. למיכל טל, שטרח ללא ליאות על הדפסת המהדורה הראשונה של החומר ועל עיצובו הנאה, ולטלי זמירין המעצבת הגראפית, על עיצוב הכריכה. תודה לעוד רבים בצוות המוזיאון, שתקצר היריעה מלנקוב בשמם, על שיתוף הפעולה ועל מאור הפנים ול"קשר חם" – המרכז לקידום שיפור ורענון החינוך המתמטי בישראל שבסיועו התאפשרה הוצאת המהדורה הנוכחית המתוקנת.

לכולם תודתי והשגיאות, אם עדין ישנן, - - עלי.

ואתם הקוראות והקוראים דעו, נושא ההצפנה הוא מרתק ורב פנים, צאו לדרך ותיווכחו בכך.

תמר ריינר,

ינואר 2008

## תוכן העניינים

|          |                                                             |               |
|----------|-------------------------------------------------------------|---------------|
| <b>1</b> | <b>סיפור קצר (במקום הקדמה) .....</b>                        | <b>עמ' 6</b>  |
| <b>2</b> | <b>מבוא .....</b>                                           | <b>עמ' 7</b>  |
| 2.1      | איזה שיטת הצפנה אנחנו מחפשים?                               | עמ' 7         |
| 2.2      | איזה הצפנות כבר הכרנו?                                      | עמ' 8         |
| 2.3      | איזה מערכת הצפנה אנחנו רוצים לבנות?                         | עמ' 8         |
| 2.4      | המגלים והמפתחים של ההצפנה האסימטרית                         | עמ' 9         |
| 2.5      | פתרונות                                                     | עמ' 10        |
| <b>3</b> | <b>סיבוכיות חישובית - מושגי יסוד .....</b>                  | <b>עמ' 11</b> |
| 3.1      | מה אפשר ללמוד על סיבוכיות מהמשחק "בול קליעה" (Master Mind)? | עמ' 11        |
| 3.2      | מהי סיבוכיות חישובית?                                       | עמ' 14        |
| 3.3      | הגדרת המושג סיבוכיות חישובית                                | עמ' 15        |
| 3.4      | הסיבוכיות של פעולות חשבון שונות                             | עמ' 16        |
| 3.5      | סיכום ביניים                                                | עמ' 20        |
| 3.6      | יעילות של אלגוריתמים                                        | עמ' 21        |
| 3.6.1    | איך אפשר לייעל חיפוש במילון?                                | עמ' 22        |
| 3.6.2    | אלגוריתם לחיפוש קווי                                        | עמ' 23        |
| 3.6.3    | אלגוריתם לחיפוש בינרי                                       | עמ' 23        |
| 3.7      | דיון וסיכום                                                 | עמ' 27        |
| 3.8      | סיבוכיות של צופנים סימטריים                                 | עמ' 27        |
| 3.8.1    | הסיבוכיות של פיצוח צופן קיסר                                | עמ' 27        |
| 3.8.2    | הסיבוכיות של צופן הזזה מונואלפבתי                           | עמ' 28        |
| 3.8.3    | הסיבוכיות של צופן שחלוק מונואלפבתי                          | עמ' 29        |
| 3.8.4    | הסיבוכיות של פיצוח הצפנה באלגוריתם DES                      | עמ' 32        |
| 3.8.5    | השוואת הסיבוכיות החישובית של פונקציות שונות                 | עמ' 33        |
| 3.8.6    | סיכום ביניים                                                | עמ' 34        |
| 3.8.7    | הסיבוכיות של One Time Pad                                   | עמ' 36        |
| 3.8.8    | הסיבוכיות של צופן כפל מודולרי                               | עמ' 36        |
| 3.8.9    | הערה: פונקציה חד כיוונית עם דלת סתרים                       | עמ' 37        |
| 3.9      | סיכום                                                       | עמ' 38        |
| 3.10     | פתרונות                                                     | עמ' 39        |
| <b>4</b> | <b>איך מחליפים מידע סודי בערוצים גלויים/פתוחים? .....</b>   | <b>עמ' 44</b> |
| 4.1      | הקדמה                                                       | עמ' 44        |
| 4.2      | ההברקה של מרקל: העברת מפתח סודי בערוצים פתוחים              | עמ' 44        |
| 4.2.1    | המגבלות של המצאת מרקל                                       | עמ' 49        |
| 4.3      | סיכום ביניים                                                | עמ' 49        |

|               |                                                                    |          |
|---------------|--------------------------------------------------------------------|----------|
| <b>עמ' 50</b> | <b>קצת מתמטיקה</b>                                                 | <b>5</b> |
| עמ' 50        | הקדמה                                                              | 5.1      |
| עמ' 51        | תכונת הזהות של פעולות מתמטיות                                      | 5.2      |
| עמ' 52        | מספרים הפכיים ופעולות הפוכות                                       | 5.3      |
| עמ' 53        | 5.3.1 הפכיים של הצפנה                                              |          |
| עמ' 54        | חשבון מודולרי, או, העיקר מה שנשאר                                  | 5.4      |
| עמ' 56        | חשבון מודולרי כחשבון מעגלי                                         | 5.5      |
| עמ' 58        | כפל מודולרי                                                        | 5.6      |
| עמ' 58        | 5.6.1 הפכיים כפליים מודולריים                                      |          |
| עמ' 63        | 5.6.2 השימוש בהפכיים מודולריים להצפנה                              |          |
| עמ' 63        | 5.6.3 איזה מספר מתאים לשמש כמפתח הצפנה?                            |          |
| עמ' 65        | מספרים ראשוניים ומספרים זרים                                       | 5.7      |
| עמ' 68        | מציאת ההפכי הכפלי                                                  | 5.8      |
| עמ' 68        | 5.8.1 הקדמה                                                        |          |
| עמ' 68        | 5.8.2 האלגוריתם של אוקלידס                                         |          |
| עמ' 71        | 5.8.3 השימוש באלגוריתם של אוקלידס למציאת ההפכי הכפלי               |          |
| עמ' 74        | זהויות מעריכיות                                                    | 5.9      |
| עמ' 74        | 5.9.1 מהי זהות מתמטית?                                             |          |
| עמ' 74        | 5.9.2 קיצורי דרך בעזרת חשבון מודולרי                               |          |
| עמ' 76        | תרומתם של פרמה ואילר                                               | 5.10     |
| עמ' 76        | 5.10.1 המשפט הקטן של פרמה                                          |          |
| עמ' 77        | 5.10.2 משפט אוילר                                                  |          |
| עמ' 78        | 5.10.3 דוגמה מספרית למשפט אוילר                                    |          |
| עמ' 79        | 5.11 פתרונות                                                       |          |
| <b>עמ' 86</b> | <b>הצפנה אסימטרית</b>                                              | <b>6</b> |
| עמ' 86        | 6.1 מפתחות נפרדים להצפנה ולפענוח                                   |          |
| עמ' 86        | 6.2 שימוש בפונקציית RSA להצפנה ופענוח באמצעות זוג מפתחות אסימטריים |          |
| עמ' 86        | 6.2.1 הקדמה                                                        |          |
| עמ' 87        | 6.2.2 משל להמחשת ההצפנה באלגוריתם של RSA                           |          |
| עמ' 89        | 6.2.3 אוילר ופרמה על המסילה המעגלית                                |          |
| עמ' 90        | 6.2.4 פיצול המסע ובניית המפתחות                                    |          |
| עמ' 90        | 6.2.5 דוגמה מספרית                                                 |          |
| עמ' 92        | 6.2.6 תאור האלגוריתם RSA                                           |          |
| עמ' 93        | 6.2.7 הצפנת אותיות באלגוריתם RSA                                   |          |
| עמ' 95        | 6.2.8 משל המסילה והאלגוריתם של RSA                                 |          |
| עמ' 096       | 6.3 פתרונות                                                        |          |
| <b>עמ' 96</b> | <b>הגורמים שמשפיעים על מידת הבטיחות של RSA</b>                     | <b>7</b> |
| עמ' 96        | 7.1 מהם הצעדים הדרושים לפיצוח שיטת ההצפנה RSA                      |          |
| עמ' 98        | 7.2 משימות המצפינים והמפצחים בשיטת RSA                             |          |
| עמ' 98        | 7.2.1 מהי משימתם הראשונה של המצפינים בשיטת RSA?                    |          |
| עמ' 98        | 7.2.2 מהי משימתם של אלה שמנסים לפצח הצפנת RSA?                     |          |
| עמ' 99        | 7.3 הסיבוכיות של פירוק לגורמים                                     |          |

|         |                                                                              |          |
|---------|------------------------------------------------------------------------------|----------|
| עמ' 100 | ..... על מספרים ראשוניים ועל הסיבוכיות של בדיקת ראשוניות                     | 7.4      |
| עמ' 100 | ..... 7.4.1 היכרות נוספת עם המספרים הראשוניים                                |          |
| עמ' 104 | ..... 7.4.2 בדיקת ראשוניות של מספר                                           |          |
| עמ' 105 | ..... 7.4.3 תרומתו של פרמה לבדיקת ראשוניות                                   |          |
| עמ' 107 | ..... 7.4.4 אלגוריתמים הסתברותיים לבדיקת ראשוניות                            |          |
| עמ' 109 | ..... 7.4.5 השוואת הסיבוכיות של פירוק לגורמים עם הסיבוכיות של בדיקת ראשוניות |          |
| עמ' 110 | ..... 7.5 מידת הבטיחות של הצפנת RSA                                          | 7.5      |
| עמ' 110 | ..... 7.5.1 בטיחות בלתי מותנית                                               |          |
| עמ' 110 | ..... 7.5.2 בטיחות חישובית                                                   |          |
| עמ' 111 | ..... 7.5.3 בטיחות סמנטית                                                    |          |
| עמ' 111 | ..... 7.5.4 העדר אפשרות להבחין בין מסרים                                     |          |
| עמ' 111 | ..... 7.5.5 סיכום ביניים                                                     |          |
| עמ' 112 | ..... 7.5.6 הבטיחות של הצפנת RSA                                             |          |
| עמ' 113 | ..... 7.5.7 הצפנה הסתברותית                                                  |          |
| עמ' 114 | ..... 7.5.8 פתרון מוצלח                                                      |          |
| עמ' 115 | ..... 7.6 פתרונות                                                            |          |
| עמ' 117 | ..... <b>הערות סיכום</b>                                                     | <b>8</b> |
| עמ' 117 | ..... 8.1 יתרונות ההצפנה במפתח פומבי על פני ההצפנה במפתח סודי                |          |
| עמ' 117 | ..... 8.2 מגבלות ההצפנה במפתח פומבי לעומת ההצפנה במפתח סודי                  |          |
| עמ' 118 | ..... <b>נספח א': הוכחה לנוסחת פתרונות המשוואה הריבועית</b>                  |          |
| עמ' 119 | ..... <b>נספח ב': הוכחת האלגוריתם של אוקלידס</b>                             |          |
| עמ' 120 | ..... <b>ביבליוגרפיה</b>                                                     |          |

## 1 סיפור קצר (במקום הקדמה)

תארו לכם מדינה, שכל פקידי הדואר בה מושחתים. הם פותחים כל חבילה, גונבים את תכולתה ושולחים אותה ריקה ליעדה. באותה מדינה דמיונית, מבקשת "פלונית" לשלוח לידידה "פלמוני" טבעת זהב. אין לה כל דרך אחרת לשלוח את הטבעת, אלא רק על ידי הדואר ופקידיו המושחתים. מה יכולים "פלונית" ו"פלמוני" לעשות כדי שהטבעת תגיע בשלום ליעדה?

הנה הפתרון שמצאו. "פלונית" אורזת את הטבעת היקרה בתיבה ונועלת אותה במנעול. את המפתח היא שומרת אצלה ושולחת את התיבה הנעולה ל"פלמוני". לפקידי הדואר אין מפתח לפתיחת התיבה, לכן אין הם יכולים לגנוב את תכולתה. הם נאלצים להעביר אותה, נעולה כשהייתה, ל"פלמוני". כשהתיבה מגיעה אליו, גם הוא אינו יכול לפתוח אותה, כי גם לו אין מפתח. במקום זה הוא נועל את התיבה במנעול נוסף, במקביל לקודם ושומר את המפתח אצלו. את התיבה הנעולה בשני מנעולים, הוא שולח בחזרה ל"פלונית".



פעם נוספת נחלצת התיבה מהפקידים הגנבים ומגיעה ל"פלונית" בשלום. היא מקבלת את התיבה, פותחת את המנעול שלה, מסירה אותו ושולחת ל"פלמוני" את הטבעת, הנעולה כעת רק במנעול שלו. התיבה עם הטבעת היקרה מגיעה בפעם השלישית לסניף הדואר וגם הפעם נחלצת ללא פגע. וכך בסופו של מסע ארוך, היא מגיעה ל"פלמוני", שפותח את המנעול בקלות עם המפתח שלו ושם את הטבעת על אצבעו, על אפם וחמתם של כל גנבי הדואר.

מה מוסר ההשכל? גם בערוצים פתוחים ולא מאובטחים, אפשר להתחכם ולהעביר מסרים חסויים, אם מצליחים "לנעול" אותם כראוי. הצפנת המסר היא ה"נעילה" שלו. המצפין "נועל" את המסר ב"מנעול", המפענח מקבל את המסר, "פותח" את הנעילה, ב"מפתח" המתאים ל"מנעול", כלומר לצופן. בחוברת זו נכיר "נעילות" ו"פתיחות" חדשות. במערכות שהכרנו בחוברת הקודמת, "נעילת" התיבה על ידי אילנית ו"פתיחתה" על ידי בני בוצעו במפתחות על ידי כך שלרשותם היו מראש מפתחות זהים. בסיפור הקצר ראינו שיתכן עוד פתרון להעברת מידע חסוי בערוצים פתוחים. בהמשך נכיר פתרונות נוספים.

## 2 מבוא

### 2.1 איזה שיטת הצפנה אנחנו מחפשים?

אנחנו כבר יודעים כי כל מערכת הצפנה מתאפיינת על ידי מפתח, שנשמך אותו ב-  $K$ , על ידי אלגוריתם הצפנה שנשמך אותו ב-  $E_k$  (הצפנה = Encryption) ואלגוריתם הפענוח שנשמך אותו ב-  $D_k$  (פענוח = Decryption), שהוא ההפכי של  $E_k$ . בפרק הקודם נוכחנו כי במערכת סימטרית, אם יודעים את אלגוריתם ההצפנה  $E_k$ , אזי מציאת אלגוריתם הפענוח  $D_k$  מהירה, כיוון שמציאת ההפכי של  $E_k$  היא פשוטה. הזכרנו כבר קודם, כי הנחת העבודה של המצפינים היא, שהאויב יודע מהו אלגוריתם ההצפנה, אך אינו יודע מהו מפתח ההצפנה. לכן במערכות הסימטריות, כל בטחון ההצפנה מותנה בשמירה על סודיות המפתח. במילים אחרות, מתכונת הסימטריות של המערכת נובע גם הצורך לשמור על סודיות המפתח ולהקפיד שלא יתפרסם אלא יישאר פרטי של השולח (המצפין) והנמען (המפענח) בלבד. האם ניתן לבנות מערכת הצפנה שתהיה משוחררת מן המגבלות הנובעות מן הסימטריה?

### 2.2 תזכורת: איזה הצפנות כבר הכרנו?

החוברת הראשונה, שעסקה בהצפנה, הוקדשה כולה לחקר הצפנות סימטריות. למשל, הכרנו את צופן ההזזה, שהוא דוגמה פשוטה לצופן סימטרי. בצופן זה, אם לשם הצפנה הזזנו כל אות במסר המקורי, שלושה מקומות קדימה (פעולה מתמטית של חיבור), אזי לשם פענוח היה עלינו לבצע את הפעולה ההפוכה ולהזיז כל אות שלושה מקומות לאחור (פעולת חיסור). באופן כללי נכון לומר, שצופנים סימטריים מתאפיינים בכך שפענוחם מושג על ידי פעולה הפוכה לפעולת ההצפנה. לעומת זה, בסעיף 4.3, בחוברת הראשונה, כשיצרנו צופני תמורות על ידי כפל מודולרי, בצענו גם את הפענוח על ידי כפל - כפלנו את המסר המוצפן בהפכי הכפלי המודולרי של מפתח ההצפנה. זוהי דוגמה לצופן אסימטרי. כשעבדנו אתו, נוכחנו, שפעולת הפענוח בו יותר מסובכת, כיוון שמציאת מפתח הפענוח, שהוא ההפכי הכפלי המודולרי של מפתח ההצפנה, אינה מיידית. עד עתה בדקנו פענוח בעזרת הפכי מודולרי במקרים פשוטים והצלחנו בכך, בסופו של דבר. אבל בהמשך ניווכח כי במערכת אסימטרית, אפשר ליצור הצפנות כאלה, שגם מי שיודע את כלל ההצפנה של המסר לא בהכרח יידע את כלל הפענוח שלו. כדי לרענן את הזיכרון, נבחן דוגמה נוספת של הצפנה אסימטרית.



#### שאלה מספר 1

- א. הצפינו את המסר "NO KEY", באלגוריתם השחלוף,  $C = (KP) \bmod 26$  במפתח  $K = 11$ .
- ב. מהו מפתח הפענוח? פענחו את המסר המוצפן.



## שאלה מספר 2

- א. הצפינו את המסר "MAZAL TOV" באלגוריתם השחלוף  $C = (KP) \bmod 26$  במפתח  $K = 5$ .
- ב. מהו מפתח הפענוח? פענחו את המסר המוצפן.

בדוגמה שבדקנו זה עתה נתקלנו פעם נוספת בתופעה מעניינת, שכבר הכרנו. גם כשאנחנו יודעים את שיטת ההצפנה (שחלוף) ואת מפתח ההצפנה (11 או 5), גם כשאנחנו עצמנו **בצענו את ההצפנה**, לא הצלחנו למצוא **מייד** את מפתח הפענוח (ההפכי הכפלי של 11 mod 26 או של 5 mod 26). חישובו, בעצם כמעט הכל היה גלוי בפנינו: המסר, מפתח ההצפנה, המסר המוצפן ועדיין לא ידענו להסיק מיידית את מפתח הפענוח. זה נשמע מאד מוזר, אבל אלה המסקנות בהן נוכחנו, כשחיפשנו תשובה לשאלות מספר 1 ו-2.

## 2.3 איזה מערכת הצפנה אנחנו מחפשים?

נסכם את העובדות בהן נוכחנו בסעיף הקודם. מערכת הצפנה נקראת **אסימטרית** אם היא מערכת כזאת, שגם אם יודעים את כלל ההצפנה שלה-  $E_k$  ואת מפתח ההצפנה שלה-  $K$ , עדיין אין אפשרות להגיע לפענוח טקסט שהוצפן באמצעותה, **בקלות ובמהירות, כיוון שמפתח הפענוח אינו ידוע ולא פשוט למצוא אותו**. ביתר קיצור, **מערכת הצפנה אסימטרית היא מערכת, שבה כלל הפענוח אינו סימטרי לכלל ההצפנה ומפתח הפענוח שונה ממפתח ההצפנה**.

בהמשך נרחיב את הטיפול בהצפנות מן הסוג שראינו בסעיף הקודם (2.2) ונבחן האם יש להן יתרון על פני הצפנות סימטריות ואם כן, מהו. יתרון אחד, שכבר הזכרנו, עשוי להיות וויתור על סודיות המפתח. כאשר ידיעת הכלל והמפתח של ההצפנה אינה מסגירה את הפענוח, תנאי הסודיות מאבד את חשיבותו. **נתוני ההצפנה** (האלגוריתם והמפתח) **יכולים להיות גלויים** במצב זה ואפשר לפרסמם בספר טלפונים או בכל מדריך ציבורי.

במערכת ההצפנה האסימטרית, שאותה אנו רוצים לפתח, יהיו למשתמש הסמלי, שנקרא לו בני, שני מפתחות: אחד, מפתח הצפנה פומבי, אותו יפרסם ברבים ומפתח פענוח פרטי סודי. כך למשל, בעזרת המפתח הפומבי יכולה אילנית (שם סמלי למשתמש) לשלוח לבני מסרים שהוצפנו על ידה, במפתח זה (כי בני פרסם אותו כמפתח הפומבי שלו). לבני (ולכל משתמש), שפרסם מפתח הצפנה יש מפתח נוסף, מפתח פענוח. מפתח הפענוח פרטי. כך, שרק בעליו יכול לפענח את המסרים המוצפנים הנשלחים אליו, בעזרת המפתח הפרטי שלו.

היתרון של מערכת כזאת הוא, שאילנית (כמו כל אחד אחר) יכולה לשלוח לבני מסר מוצפן, לא רק **ללא תקשורת מקדימה לגבי מפתח סודי**, אלא גם **תוך שימוש בערוץ גלוי להעברת המידע הסודי**. היא עושה

זאת על ידי שימוש במפתח ההצפנה הפומבי של בני (אותו נסמן ב-  $K_{EB}$  כיוון ש:  $EB = \text{Encryption Beni}$ ). בני הוא היחיד שיכול לפענח את הטקסט המוצפן, כי רק הוא מכיר את מפתח הפענוח הפרטי שלו (אותו נסמן ב-  $K_{DB}$ ,  $DB = \text{Decryption Beni}$ ). מערכת הצפנה כזאת אנחנו מעונינים לפתח. האם זה אפשרי? קצרנו שמץ הצלחה בהצפנה על ידי כפל מודולרי. האם זה מספיק טוב? אולי יש הצפנות אסימטריות נוספות, יותר קשות לפיצוח? זה מה שנחקור בהמשך.

## 2.4 המגלים והמפתחים של ההצפנה האסימטרית

אבות הרעיון של מערכת ההצפנה האסימטרית היו שני מתמטיקאים אמריקניים, וויטפילד דיפי ומרטין הלמן (Whitfield Diffie & Martin Hellman). הם פרסמו את הרעיון בשנת 1976 ויישמו החל בשנת 1977, על ידי ריבסט, שמיר ואדלמן (Ron Rivest, Adi Shamir & Leonard Adleman). הם שהמציאו את מערכת ההצפנה האסימטרית הנקראת על שמם, מערכת RSA (בהתאם לאותיות הראשונות של שמות המשפחה שלהם). נכיר אותה בחוברת זו. מאז המצאת ה-RSA הוצעו מערכות אסימטריות נוספות, שאבטחתן מבוססת על בעיות חישוביות שונות, אבל שיטת RSA נותרה עדיין המקובלת ביותר. לסיפור הזה יש גם נקודה ישראלית: פרופסור עדי שמיר הוא ישראלי ונמנה על סגל המדענים במכון ויצמן. עם כתיבת שורות אלה פורסמה בעיתונות הידיעה כי שלישיית ממציאי שיטת ההצפנה RSA זכו בפרס טורינג, הפרס היוקרתי ביותר למדעי המחשב.

אלן טורינג (1912-1954), היה מתמטיקאי בריטי מחונן, חלוץ מדעני המחשב. היה דמות מרכזית בצוות המדענים הבריטי, שנאבק לפצח את צופן האניגמה הגרמני, במלחמת העולם השנייה. למרות גאונותו המתמטית נאלץ טורינג להתמודד עם בעיות קשות של עוינות חברתית, כיוון שהיה הומוסקסואל. בעיות אלה הביאו, בסופו של דבר, להתאבדותו. לזכרו נוסד פרס טורינג למדעי המחשב.

## 2.5 פתרונות

### פתרון שאלה מס' 1:

א. טבלת ההצפנה

|                  |     |     |     |    |     |
|------------------|-----|-----|-----|----|-----|
| P                | N   | O   | K   | E  | Y   |
| P (ערך מספרי)    | 13  | 14  | 10  | 4  | 24  |
| 11P              | 143 | 154 | 110 | 44 | 264 |
| $C=11P \bmod 26$ | 13  | 24  | 6   | 18 | 4   |
| C (אותיות)       | N   | Y   | G   | S  | E   |

ב. מפתח הפענוח הוא ההפכי הכפלי של 11 מודולו 26.  $11 \cdot 19 \bmod 26 = 1$  משמע, 19 הוא ההפכי

הכפלי המתאים

טבלת הפענוח

|                    |     |     |     |     |    |
|--------------------|-----|-----|-----|-----|----|
| C                  | N   | Y   | G   | S   | E  |
| C (ערך מספרי)      | 13  | 24  | 6   | 18  | 4  |
| 19C                | 247 | 456 | 114 | 342 | 76 |
| $P = 19C \bmod 26$ | 13  | 14  | 10  | 4   | 24 |
| P (אותיות)         | N   | O   | K   | E   | Y  |

### פתרון שאלה מס' 2:

א. טבלת ההצפנה:

|                   |    |   |    |   |    |    |    |    |
|-------------------|----|---|----|---|----|----|----|----|
| P (אותיות)        | M  | A | Z  | A | L  | T  | O  | V  |
| P (מספרים)        | 12 | 0 | 25 | 0 | 11 | 19 | 14 | 21 |
| $C=(5P) \bmod 26$ | 8  | 0 | 21 | 0 | 3  | 11 | 18 | 25 |
| C (אותיות)        | H  | A | V  | A | D  | L  | S  | Z  |

ב. מפתח הפענוח (ההפכי הכפלי של  $5 \bmod 26$ ) הוא 21. בדקו  $(21 \cdot 5) \bmod 26 = ?$

טבלת הפענוח:

|                    |    |   |    |   |    |    |    |    |
|--------------------|----|---|----|---|----|----|----|----|
| C (מספרים)         | 8  | 0 | 21 | 0 | 3  | 11 | 18 | 25 |
| $P=(25C) \bmod 26$ | 12 | 0 | 25 | 0 | 11 | 19 | 14 | 21 |
| P (אותיות)         | M  | A | Z  | A | L  | T  | O  | V  |

### 3 סיבוכיות חישובית (Computational Complexity): מושגי יסוד

#### 3.1 מה אפשר ללמוד מהמשחק "בול קליעה" (Mastermind) על סיבוכיות חישובית

יש הרבה בעיות, שפתרון הסופי מרכב משלבים רבים של פתרונות חלקיים. בכל שלב נפתר חלק מן הבעיה, נפתרת תת-בעיה, ופתרונה קובע את ההתקדמות לשלב הבא של הפתרון. למשל, אתם לבטח מכירים את המשחק "בול קליעה" (Mastermind). זהו משחק המיועד לשני משתתפים, שאחד מהם יכול להיות מחשב אישי. במשחק זה היריב שלך (או המחשב) בוחר ארבעה כדורים בצבעים שונים, מתוך ששה צבעים אפשריים (מותר לבחור אותו צבע יותר מפעם אחת). עליך לנסות לגלות את רביעיית הכדורים של היריב, את צבעו ואת מיקומו של כל אחד מארבעה הכדורים, באמצעות ניחושים. ניחוש נכון של צבע הכדור בלבד הוא "פגיעה", ניחוש נכון של צבע הכדור וגם של מיקומו הוא "בול". כל צעד (כל ניסיון לנחש את מיקומם של ארבעת הכדורים ואת צבעיהם), תוצאתו מספר "פגיעות" ומספר "בולים" (לצורך זה גם אפס הוא מספר), שידעתם עשויה לסייע בניסוח ניחוש נוסף. מומלץ מאוד להתנסות במשחק באתר:

<http://alefefes.macam98.ac.il/games/master/master.asp>

כל מי שכבר התנסה במשחק, נוכח כי הוא עשוי להסתבך מאד. מקור הסיבוך הוא בריבוי הצירופים האפשריים, ריבוי הרביעיות האפשריות של כדורים, הנבדלות בצבעי הכדורים ובמיקומם. כתוצאה מהמספר הגדול של הרביעיות האפשריות, הקושי לנחש רביעייה אחת, **צירוף אחד, מתוך רבים אפשריים**, הוא גדול. הקושי גדול כיוון שמספר הניחושים האפשריים גדול. הוא שווה למספר הרביעיות האפשריות. מהו מספר הרביעיות האפשריות? נחשב אותו. הכדורים בכל רביעייה עשויים להיות ב-6 צבעים שונים ואנו יודעים, שאין הגבלה על מספר החזרות של אותו צבע. כמה רביעיות כאלה אפשר ליצור? כבר טפלנו בבעיות דומות. למשל, כשבדקנו כמה מספרים בני 4 ספרות (כדורים) אפשר ליצור מ-6 ספרות (צבעים) שונות. נוכחנו שהתשובה לכך היא  $6^4$ .

במקרה של המשחק "בול קליעה" מספר הצירופים השונים של הכדורים הוא:  $1,296 = 6^4$ . האם זה אומר, שאם עלינו לנחש את רביעיית הכדורים, שבחר היריב, עלינו לנסות את כל 1,296 הניחושים? מי שמכיר את המשחק יודע שלא זה המצב. הרבה פעמים אנחנו מגלים את רביעיית היריב, במספר ניחושים קטן בהרבה. המספר 1296 מתאר את המצב **במקרה הגרוע ביותר**, כאשר הניחושים שלנו אקראיים ושום ניחוש אינו מושפע מהניחוש שקדם לו. האם אפשר לצמצם את מספר הניחושים? כיצד? כמו שכבר הזכרנו, כל מי שמכיר את המשחק יודע, שבדרך כלל אין הוא מנחש באקראי אלא **מעלה השערות**, המתבססות על המידע שבידיו.

בדרך כלל בכל שלב אנחנו מנסים ללמוד מתוצאות הבדיקה של ההשערה שהעלינו, אנחנו משתדלים להסיק ממנה, לפי מספר ה"פגיעות" וה"בולים" שהשגנו באמצעותה, מהי ההשערה הבאה שכדאי לנו להעלות ולנסות. בנוסף להסקת מסקנות מכל השערה בודדת, אנחנו יכולים לנסות לגבש אסטרטגיה יותר כללית: כיצד כדאי להתקדם? האם אפשר לתכנן את ההשערות? אולי כדאי לנסות ולגלות קודם כל את הצבע? אולי יותר כדאי לנסח את ההשערות לפי שיקולים אחרים? בכל מקרה, קרוב לוודאי שלא נבחר באסטרטגיה של ניחוש אקראי. האם אתם מכירים אסטרטגיה חלופית שיטתית? נסו לפתח כזאת. הנה כמה רעיונות שאולי יסייעו לכם.

יש ניסיונות מענינים של מתמטיקאים לבסס הנמקה מתמטית לאסטרטגיות משחק יעילות, שמסבירות את ההבדל **העצום** בין מספר הניחושים המוביל לניצחון בטוח, "במקרה הגרוע ביותר" (1,296), לבין מספר הניחושים בפועל של שחקן ממוצע (5-10). הנה חלק מהם:

א. לכל השערה שלנו יש מספר תשובות אפשריות. המספר הזה קבוע. איך מגיעים אליו? אם תחשבו את כל הצירופים האפשריים של "בולים", "קליעות" ו"פספוסים" בבדיקת כל השערה, תיווכחו שסכומם קבוע.

## שאלה מספר 1

השלימו את הטבלה:

| מספר ה"בולים" | מספר ה"פגיעות" | מספר ה"פספוסים" |    |
|---------------|----------------|-----------------|----|
| 0             | 0              | 4               | 1  |
| 1             | 0              | 3               | 2  |
| 0             | 1              | 3               | 3  |
| 2             | 0              | 2               | 4  |
| 1             | 1              | 2               | 5  |
| 0             | 2              |                 | 6  |
| 3             | 0              |                 | 7  |
|               |                |                 | 8  |
|               |                |                 | 9  |
|               |                |                 | 10 |
|               |                |                 | 11 |
|               |                |                 | 12 |
|               |                |                 | 13 |
|               |                |                 | 14 |

אם חישבתם נכון, נוכחתם כי סכום התשובות האפשריות להשערה הוא 15, שאחת מהן היא התשובה הנכונה (כלומר 4 "בולים"). אם מצאנו אותה, נצחנו את המשחק. (הערה: לכאורה קיימים 15 צירופים שונים של "בולים" ו"קליעות", אבל הצירוף של 3 "בולים" ו"קליעה" אחת הוא בלתי אפשרי. לא יכול להיות ש-3 כדורים הם בצבע ובמיקום נכונים והרביעי צבעו נכון אבל מיקומו לא נכון).

ב. אם לא הצלחנו בניחוש הראשון, אז אחרי בדיקת ההשערה אנחנו נשארים עם אחת מ-14 האפשרויות בלבד. כל השאר, שהיו עשויות לפתוח כוונת השערה חדשים, נדחו. בכך הצטמצם מספר הצירופים האפשריים ובכך הצטמצם מרחב החיפוש שלנו ל-93 ~ 1,296/14. גם להשערה השניה יש 14 תשובות אפשריות, גם מתוכן רק אחת מוכחת כנכונה ומספר האפשרויות מצטמצם פעם נוספת. הצמצום המקסימלי, שעשוי להתרחש בשלב זה גם הוא פי 14. 7 ~ 93/14. מכל האמור בסעיף זה נובע כי אי אפשר להגיע לפתרון בפחות מ-3 מהלכים. תהליך זה, של הצטמצמות מספר האפשרויות נמשך בכל השלבים, אם ההשערות אינן אקראיות, אלא נובעות תמיד מתוצאות הבדיקות של ההשערות שקדמו להן. אמנם אין הוא מצטמצם עד למינימום של ניחוש ב-3 מהלכים, אבל הוא הרבה יותר קטן מ-1,296, המספר המקסימלי של המהלכים, במקרה הגרוע ביותר.

ג. חישובים אחרים מורים כי המפצח, שנוקט בדרך זו, של ניסוח השערות ובדיקתן, יכול תמיד לנצח ב-5 מהלכים, לכל היותר. האסטרטגיה שמבטיחה זאת מבוססת על כך, שבכל שלב בוחר המפצח מתכונת מבחן להשערות, כך הוא צובר מידע מצירופים מסוימים של מיקום הכדורים וצבעיהם ועל ידי כך הוא יכול לצמצם את המספר המירבי של האפשרויות שנותרו.

למשל, נניח את המקרה: השערה מס' 1: ירוק, אדום, כתום, שחור, מניבה שתי "קליעות".

השערה מס' 2: לבן, אדום, כתום, שחור, מניבה שלוש "קליעות".

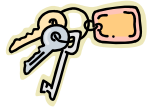
ההבדל היחיד בין שתי השורות הוא בצבעו של הכדור בעמדה הראשונה. אבל לפי התגובה, בכך נוסף כדור בעל צבע נכון. מכך אפשר להסיק בביטחון, שהצבע הלבן נכון ואילו הירוק אינו נכון. איזה מסקנה כללית אפשר להסיק מכך? זוהי דוגמה למתכונת מבחן, המסייע לצמצום מספר האפשרויות בכל שלב.

כאמור, אפשר להוכיח כי הניצחון אפשרי ב-5 מהלכים. נסו זאת.

באינטרנט מצוי חומר רב ועשיר על המשחק ועל המתמטיקה שלו. חלק מן המקורות רשום בביבליוגרפיה, בסוף החוברת.

עד כאן בדקנו מהו המספר המרבי של הצעדים הדרושים לניצחון במשחק "בול קליעה" ועל אסטרטגיות פתרון, שעשויות לשפר את מספר הצעדים, שיביא לפתרון. נראה כי שינוי נתוני הבסיס של הבעיה יגדיל את סיבוכיות הבעיה.

מה אפשר להגיד על הסיבוכיות של המשחק באופן כללי? כמה יסתבך המשחק, אם נשנה את נתוני הבסיס שלו ונגדיל את מספר הצבעים לבחירה ואת מספר הכדורים בצירוף יחיד? כיצד יגדל מספר ההשערות שיש להעלות, כדי לגלות את צירוף הכדורים הצבעוניים של היריב? למשל, מה יהיה מספר הצירופים אם נגדיל את מספר הכדורים ל-8?  $6^8 = 1,296^2 = 1,679,616$



## שאלה מספר 2

- פי כמה הגדלנו את מספר הכדורים ב"צירוף יחיד", במקרה זה?
- פי כמה גדל המספר הכולל של הצירופים האפשריים במקרה זה?
- פי כמה יגדל מספר הצירופים האפשריים, אם מספר הצבעים האפשריים יגדל פי 2?



## שאלה מספר 3

- נניח שמספר הכדורים בצירוף יחיד, גדל מ- $n$  ל- $2n$ , פי כמה יגדל המספר הכללי של הצירופים האפשריים?
- נניח שמספר הצבעים גדל מ- $m$  ל- $2m$ , פי כמה יגדל מספר הצירופים האפשריים?



## שאלה מספר 4

נוכחנו כי מספר הצירופים האפשריים של הכדורים תלוי בשני גורמים: במספר הצבעים וגם במספר הכדורים בצירוף אחד. לאיזה משני הגורמים השפעה יותר גדולה על גידול מספר הצירופים האפשריים של הכדורים?

## 3.2 מהי סיבוכיות חישובית?

המשחק "בול קליעה" הוא משחק מרתק וממכר ובנוסף לכך אפשר להפיק ממנו לקחים מתמטיים חשובים. אנחנו נתרכז במה שאפשר ללמוד ממנו לגבי מושג הסיבוכיות החישובית. אפשר לומר כי **הסיבוכיות של בעיה מתימטית קשורה למספר הצעדים הדרוש לפתרונה**. בהמשך נרחיב את חקר הסיבוכיות ונגדיר אותה ביתר דיוק.

בשאלה מספר 3 בסעיף הקודם נוכחנו כי כאשר מספר הכדורים בצירוף יחיד גדל פי 2 (מ- $n$  ל- $2n$ ) ומספר הצבעים ( $m$ ) אינו משתנה, המספר המקסימלי של ההשערות (הצירופים האפשריים), שיש לנסח כדי לגלות את הצירוף של היריב, גדל **בריבוע** (מ- $m^n$  ל- $m^{2n} = (m^n)^2$ ). כך, כאשר מספר הכדורים גדל מ-4 ל-8, גדל מספר הצירופים מ-1,296 ל- $1,296^2$  (יותר ממיליון וחצי). כלומר כתוצאה מכך, שמספר הכדורים גדל פי 2,

מספר ההשערות המירבי גדל ב"קפיצה" ליותר ממיליון וחצי. שימו לב שגם הסיבוכיות של הבעיה גדלה ב"קפיצה". גידול קטן בנתוני הבעיה הביא לגידול עצום בסיבוכיות של פתרונה.

תכונת הסיבוכיות החישובית משותפת לבעיות רבות בתחומים שונים ובין היתר לבעיות מתחום ההצפנה. למשל, בחוברת הראשונה הזכרנו מספר פעמים ש"אפשר לפצח צופן על ידי ניסוי כל מפתחות ההצפנה". האמנם אפשר? נניח שהמסר המוצפן הוא בשפה האנגלית ואלגוריתם ההצפנה הוא שחלוק מונואלפאביתי. כמה מפתחות הצפנה נצטרך לבדוק? במקרה הגרוע ביותר 26!, זה יותר מ- $10^{20}$  מפתחות (בדקו). גם אם לרשותנו מחשב שיכול לבדוק  $10^6$  מפתחות בשניה, הזמן הדרוש לבדיקת כל המפתחות הוא  $10^{14}$  שניות (בדקו), שהן יותר ממיליון שנים (בדקו). אנחנו כבר לא נהיה שם, לקרוא את המסר המפוצח. אתם רואים שגם בעיית הפיצוח של צופן שחלוק (במקרה הגרוע ביותר) היא בעלת סיבוכיות חישובית גדולה. בשתי הדוגמאות האלה (גילוי מיקום הכדורים וצבעם במשחק "בול קליעה" ופענוח צופן שחלוק), אנחנו מכירים אלגוריתם, שלכאורה יכול לפתור את הבעיה. אבל בגלל "גודל" הבעיה, הסיבוכיות של פתרונה "מביסה" את האלגוריתם. במקרה כזה אנו אומרים, שהאלגוריתם לא סביר. בסעיף הבא נגדיר את מושג הסיבוכיות החישובית ונעמיק קצת יותר לחקור אותו.

### 3.3 הגדרת מושג הסיבוכיות החישובית

הסיבוכיות החישובית נותנת מענה לשאלה, מהו היקף המשאבים הדרושים לביצוע פעולות חישוב במחשב. שני המדדים החשובים של הסיבוכיות החישובית הם גודל הזיכרון של המחשב ומספר הפעולות שמבצע המחשב בעת הרצת האלגוריתם, המבצע את החישוב. את הסיבוכיות החישובית של הזמן לפתרון בעיה, מודדים באמצעות מספר פעולות היסוד, המבוצעות על ידי המחשב, כשמריצים את האלגוריתם לפתרון הבעיה. בהמשך הדיון בסיבוכיות החישובית נתרכז רק בחקר סיבוכיות הזמן של פתרון בעיות שונות. בתחום ההצפנה מתמקדת הסיבוכיות החישובית בשתי בעיות מרכזיות:

ה"קושי" המובנה (inherent), הטבוע בבעיות.

היעילות של אלגוריתמים המשמשים לפתרון. כלומר, להצפנה ולפענוח (כדי לנתק את האלגוריתם מהביצועים של מחשב מסוים, נוהגים להגדיר מודל כללי של יעילות).

כמו שכבר אמרנו, את הסיבוכיות החישובית של פתרון בעיה במחשב, אנו מודדים על ידי מספר פעולות היסוד, המבוצעות על ידי המחשב בהרצת אלגוריתם הפתרון. פעולות היסוד נקראות "פעולות ביט". הפעולות המוגדרות הן: חיבור, חיסור, כפל של שתי ספרות בינריות, חלוקה של מספר בינרי דו-ספרתי בחד-ספרתי, או הזזה של ספרה בינרית במקום אחד.

**מספר הפעולות הדרושות להשלמת הביצוע של האלגוריתם נקרא הסיבוכיות החישובית (של האלגוריתם) ובקיצור סיבוכיות.**

### 3.4 הסיבוכיות של פעולות חשבון שונות

כולנו יודעים מניסיונו, כי בעיות חישוב הדורשות לפתרון פעולות של חיבור, חיסור, כפל וחילוק, הן בעיות פשוטות לפתרון, גם כשמדובר במספרים גדולים. בכל המקרים האלה עומדים לרשותנו אלגוריתמים מוכרים מלימודינו בבית הספר ומניסיונו הם גם יעילים למדי.

גם המחשב יכול להריץ אלגוריתמים דומים לאלה המוכרים לנו, למרות שהם לא בהכרח היעילים ביותר. מה מספר הפעולות שאנו מבצעים, כאשר אנחנו "מריצים" אלגוריתמים אלה? בביצוע ידני של 4 פעולות החשבון (חיבור, חיסור, כפל וחילוק), אנו מתייחסים למספר הפעולות על הספרות העשרוניות של המספר. כאשר אנחנו מבצעים את הפעולות האלה באמצעות מחשב, המספרים מוצגים בהצגה בינרית ואנחנו מתייחסים למספר הביטים שלהם.

**סיבוכיות החיבור** - נניח שאנחנו רוצים לבצע חיבור של שני מספרים, שכל אחד מהם הוא בן 10 ביטים, כמתואר בשרטוט:

```

. . . . .
+
. . . . .
-----
. . . . .
```

אלגוריתם החיבור מתחיל בצד ימין, לוקח זוג ביטים, אחד מן השורה העליונה והשני מן השורה התחתונה, מחבר אותם וממשיך לזוג הבא, עד לסיום פעולת החיבור. אם כל אחד משני המספרים הוא בעל 20 ביט, גם מספר הפעולות שעל האלגוריתם לבצע גדל פי 2 וגם הזמן לביצוע פעולת החיבור מתארך פי 2.

אפשר לסכם ולומר, שמספר הפעולות, שמבצע האלגוריתם כדי לחבר שני מספרים בעלי  $n$  ביטים, הוא יחסי למספר הספרות של המספרים אותם אנו מחברים או מחסרים, כלומר יחסי ל- $n$ . הזמן הדרוש לביצוע הפעולות, יחסי למספר הפעולות שמבצע המחשב. נסמן את הזמן הדרוש לביצוע הפעולות ב- $T(n)$ . כאשר מספר הביטים  $n$  גדל, למשל פי 2, גם  $T(n)$  גדל באותו יחס, כלומר פי 2.

## שאלה מספר 5

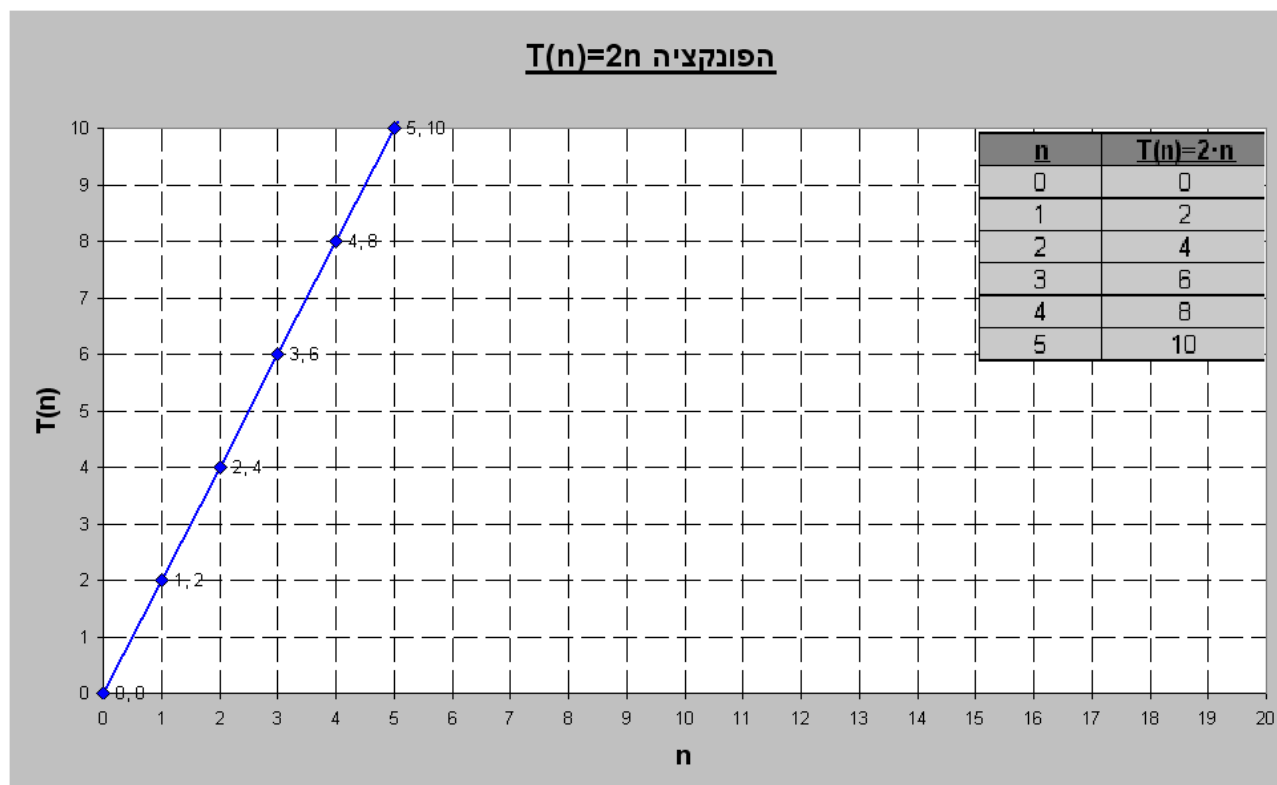
השלימו את הטבלה:

הקשר בין מספר הביטים (n) ובין הזמן הדרוש לביצוע פעולת חיבור  $T(n)$

| $T(n)$ | n=מספר הביטים |
|--------|---------------|
| 150    | 50            |
|        | 100           |
| 420    |               |
|        | 300           |
|        | 1,000         |
|        | K             |

מן הטבלה אתם רואים כי היחס בין מספר הספרות של המספרים אותם מחברים ובין זמן ההרצה של האלגוריתם המבצע את החיבור הוא קבוע. בדוגמה שהבאנו בטבלה היחס הוא 3. כאשר מספר הספרות הוא n, אזי  $T(n) = 3n$ .

נניח שנתון כי  $T(n) = 2n$ , זהו ביטוי אלגברי לפונקציה T. משמעותו שכאשר מפעילים את הפונקציה על ערכים שונים של n, הם מוכפלים ב-2.





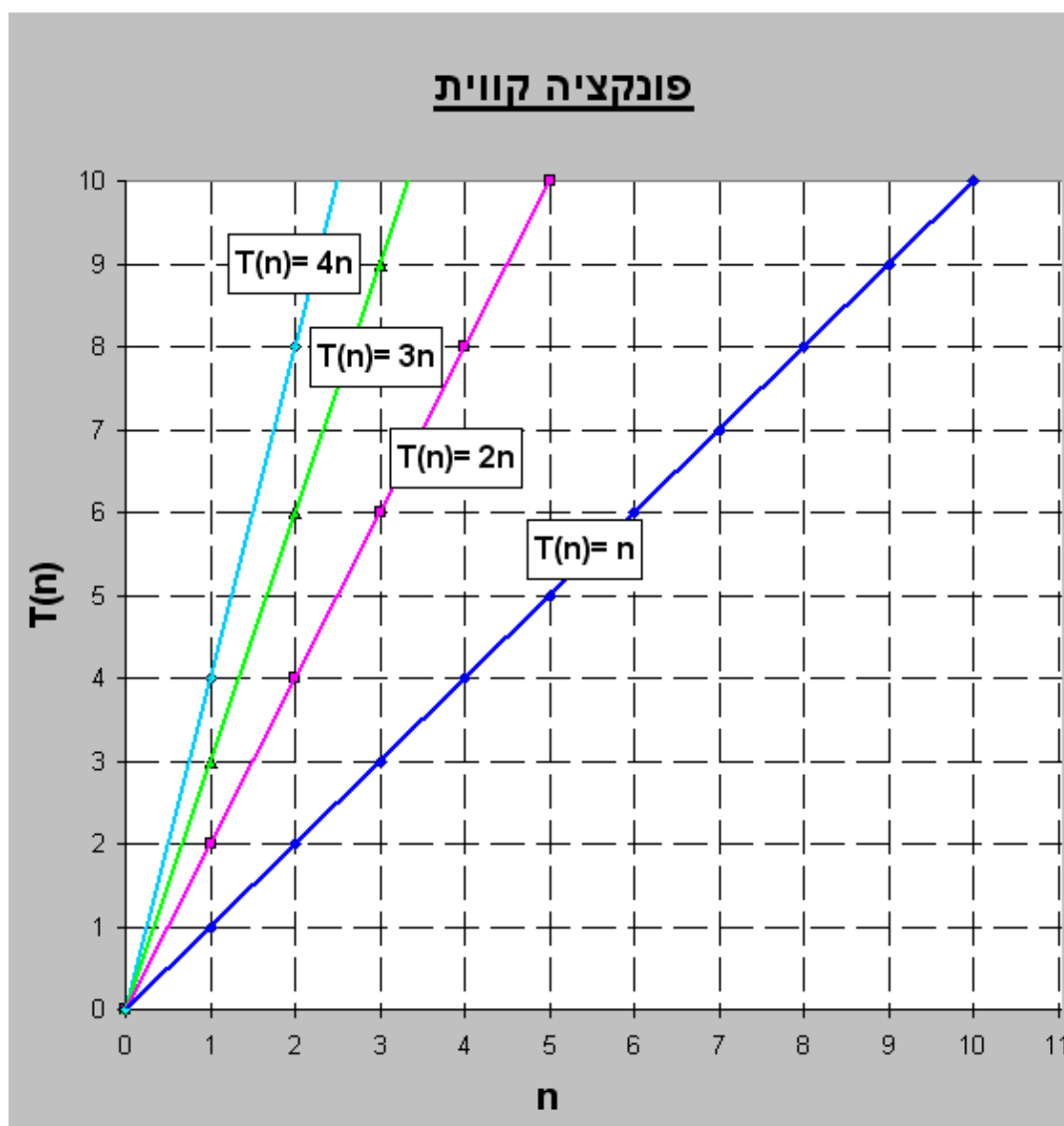
## שאלה מספר 6

ציירו את התיאור הגרפי של הפונקציה  $T(n) = 3n$ . הציר האופקי יציין את מספר הספרות והציר הניצב לו את זמן ביצוע הפעולה. השתמשו באותו קנה מידה בו שורטטה הדוגמה.

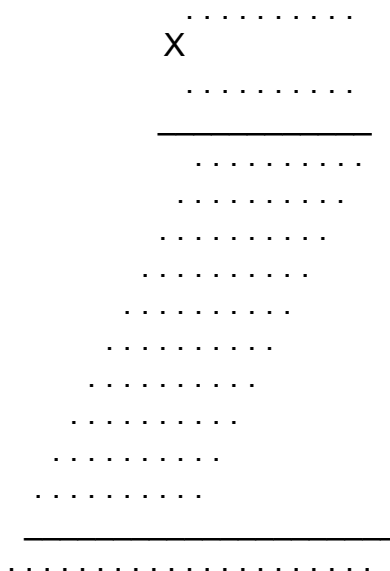
אם לא טעיתם, קבלתם גם אתם ציור של ישר. לכן ליחס כזה אנו קוראים יחס קווי ובאנגלית - ליניארי

(קווי = Line). מהו ההבדל בין שני הישרים? על מה הוא מעיד, לדעתכם?

בשרטוט הבא מובא התיאור הגרפי של פונקציות מהצורה  $T(n) = a \cdot n$ , כאשר  $a=1, 2, 3, 4$ . כל אחת מהן היא פונקציה קוויית.



**סיבוכיות הכפל** - מה מספר הפעולות שיש לבצע כשרוצים לכפול שני מספרים בני  $n$  ספרות זה בזה? ניזכר כי כשאנו רוצים לכפול שני מספרים זה בזה אנחנו צריכים לכפול כל אחת מן הספרות של אחד מן המספרים, בכל אחת מהספרות של המספר השני (בדקו זאת). השרטוט שלהלן מתאר את התבנית של ביצוע הכפל.



אנו רואים כי מספר הפעולות הדרוש לביצוע פעולת הכפל של שני מספרים, הוא יחסי **למכפלת** מספר הספרות של שני המספרים, אותם אנו כופלים זה בזה, כלומר **יחסי ל- $n^2$** . אפשר לומר כי במקרה של הכפל  $T(n) = n^2$ . לכן אנו אומרים כי היחס בין הזמן לביצוע פעולת כפל, לבין מספר הספרות של המספרים אותם כופלים, הוא ריבועי. לפעמים אומרים בקיצור היחס הוא ריבועי.

## שאלה מספר 7

השלימו את הטבלה:

הקשר בין מספר הביטים ( $n$ ) ובין הזמן הדרוש לביצוע פעולת כפל

| $n$   | $T(n)=n^2$ |
|-------|------------|
| 50    |            |
|       | 3,600      |
| 100   |            |
| 300   |            |
| 1,000 |            |



### שאלה מספר 8

ציירו את התיאור הגרפי של  $T(n) = n^2$



### שאלה מספר 9

- א. הוסיפו למערכת הצירים שבשאלה 8 את הגרף שציירתם בשאלה 6, כך תוכלו להשוות בין שני הגרפים, הקווי והריבועי, ביתר קלות.
- ב. איזו פונקציה גדלה בקצב גבוה יותר מבין השתיים?

המסקנה מן הבדיקות שבצענו לגבי מספר הפעולות הדרושות לביצוע של פעולות החיבור והכפל היא, **שמספר הפעולות הדרושות לביצוע פעולת כפל של שני מספרים בעלי מספר ספרות מסוים, גדול יותר ממספר הפעולות הדרוש לחיבור או לחיסור של שני המספרים בעלי אותו מספר ספרות.** נוכחנו בכך וגם הצגנו זאת בדרך חזותית (בתיאור גרפי), כדי להגביר את השכנוע. בעצם אין בכך משום חידוש גדול. בסך הכל קבלנו אישור מתמטי, למה שכבר ידענו מניסיונו, אם כי חשוב לציין כי הניסיון עלול גם להטעות. לבמתטיקה מוכיחים כל דבר, כך שנכונותו תהיה מעל ומעבר לכל ספק.

בלשון המושג החדש שהכרנו, מושג הסיבוכיות החישובית, נוכל לסכם ולומר **שהסיבוכיות החישובית של פעולת הכפל, גדולה יותר מן הסיבוכיות החישובית של פעולות החיבור והחיסור.** האלגוריתם לביצוע החיבור הוא קווי (זמן הרצתו קווי ביחס למספר הספרות של המספרים אותם מחברים) ואילו האלגוריתם לביצוע הכפל הוא ריבועי (זמן הרצתו ריבועי ביחס למספר הספרות). האם אפשר לצמצם את היחס הריבועי? האם אפשר להקטין את הסיבוכיות של הכפל? האם אפשר למצוא אלגוריתם לביצוע הכפל, שיהיה יותר יעיל מן האלגוריתם שזמן הרצתו ריבועי? בהמשך נחזור לשאלה זו.

## 3.5 סיכום ביניים

נסכם את כל הדוגמאות שבדקנו בסעיפים הקודמים: בדקנו את הסיבוכיות של המשחק "בול קליעה", של פיצוח צופן שחלוף (במקרה הגרוע ביותר) ואת הסיבוכיות החישובית של פעולות החיבור והכפל. מקרים אלה אפשרו לנו לערוך הכרות ראשונה עם מושג הסיבוכיות ועם מושג הסיבוכיות החישובית.

נוכחנו שפתרון של בעיות חישוביות, שנראות לכאורה פשוטות, עשוי להיות בעל סיבוכיות חישובית מפתיעה ומתסכלת בגדלה. במקרים מסוימים המשאבים החישוביים הדרושים כדי למצוא פתרון מדויק לבעיות אלה הם עצומים. הם כל כך עצומים, עד שלעיתים אין שום אפשרות להגיע לפתרון של הבעיה בפרק זמן ריאלי, גם אם מנצלים את כל יכולות החישוב של המחשב.

הסיבה לכך שהעלינו את שאלת הסיבוכיות החישובית, היא יישומיה האפשריים להצפנה בכלל ולהצפנה האסימטרית בפרט. במילים אחרות, השאלה המעניינת והחשובה היא, **האם אפשר ליישם ממצאים מחקר הסיבוכיות לפיתוח שיטות הצפנה משופרות? האם אפשר לייצר מסרים מוצפנים ברמת סיבוכיות כזאת, שליריב לא תהיה יכולת חישובית לפצח אותם במשך זמן ריאלי?**

הערה: במסגרת הדיון בסיבוכיות החישובית של פתרון בעיות שונות, חשוב להעיר, כי הידיעה או ההוכחה, שבעיה מסוימת היא חסרת פתרון תוך פרק זמן ריאלי, לשון אחרת, שמסר מסוים אינו ניתן מעשית, לפיצוח, היא גם בעלת חשיבות חיובית ולא רק חשיבות שלילית. ידיעת המגבלות מונעת מאתנו לבזבז את זמננו על משימה בלתי אפשרית ועשויה לכוון אותנו לגישות יותר "צנועות" בחיפוש אחר פתרונות חלקיים. למשל: אולי כדאי לחפש פתרונות מקורבים, אולי אפשר להסתפק בפתרון מקרים פרטיים בלבד ואולי כדאי לנסות לשנות מעט את הבעיה ולהפוך אותה ליותר פשוטה אפילו במחיר צמצום מסויים של התאמתה למצבים אמיתיים ומציאותיים.

מכל האמור לעיל ברור, כי ממצאים מחקר הסיבוכיות החישובית עשויים לסייע למתכנני אלגוריתמים, על ידי הכוונתם להתמקדות בתחומים מבטיחים ולהימנעות ממשימות בלתי אפשריות. בהמשך נראה את יישומם של רעיונות אלה בפיתוח אלגוריתמים יעילים ושיטות הצפנה חדישות.

### 3.6 היעילות של אלגוריתמים

עד כמה חשוב שאלגוריתם יהיה יעיל? היעילות של אלגוריתם היא בעלת חשיבות קריטית בכל המצבים בהם נדרשת תגובה ונדרש פתרון לבעיה ב"זמן אמת". כזה הוא המצב בבעיות של בקרת טיסה, ניווט טילים וחלליות ועוד.

אבל גם במקרים אחרים, בהם גורם הזמן אינו כל כך קריטי לכאורה, אנו יודעים כי זמן המחשב יקר ולכן ברור שהגברת היעילות (חיסכון בפעולות ובזמן המחשב), היא בעלת ערך.

### 3.6.1 איך אפשר לייעל חיפוש במילון?

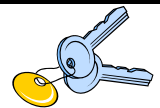
חידות ושעשועי לשון רבים מבוססים על אתגר הזיהוי של מילים שונות, שכולן בנויות מאותן האותיות. למשל:



#### שאלה מספר 10

- כל אחת מן ההגדרות הבאות מתארת שתי מילים, שמורכבות מאותן אותיות בסדר שונה. מהן שתי המילים?
- א. "עז הפנים הביא לגילוי הצופן".
  - ב. "המדינה תחבר".

למילים מן סוג הזה קוראים אנגרמות. למשל "צרפת" ו"תצרף" הן אנגרמות ואפשר להוסיף להן גם "תרצף" ו"פרצת". האם יש אנגרמות נוספות בקבוצה זו? חפשו.



#### שאלה מספר 11

- א. כמה אנגרמות, לכל היותר, יש למלה "צרפת"? כמה למלה "פצוח"? האם יש הבדל במספר האנגרמות המקסימלי של שתי המילים האלה? נמקו.
- ב. מה המספר המקסימלי של אנגרמות, שאפשר לבנות למילה בת  $k$  אותיות?

נניח שיש לנו מילון ובו 500,000 ערכים. אנחנו רוצים שבהינתן מילה, נוכל למצוא במילון את כל האנגרמות שלה. אנחנו רוצים, שבהינתן מילה, יהיה לנו **אלגוריתם** למציאת כל האנגרמות שלה. למשל, בהינתן המלה חתן האלגוריתם ייתן לנו את המילים: נתח, נחת, תנח, תחן ואחרות. בהמשך נראה כיצד בונים אלגוריתם כזה, נראה שאפשר לבנות יותר מאלגוריתם אחד למטרה זו, נבדוק את היעילות שלהם, כדי למצוא את היעיל ביותר מביניהם.

### 3.6.2 אלגוריתם חיפוש קווי

הדרך הפשוטה ביותר לחיפוש אנגרמות למילה נתונה במילון, היא לעבור על כל אחד מערכי המילון ולבדוק האם הוא אנגרמה של המילה בה מדובר. כך גם אפשר לעבור על כל ערכי המילון ולברור מתוך כל הערכים, את אלה שהם האנגרמות של המלה חתן. כשאנחנו מבצעים זאת במחשב, אנו מזינים כקלט את המילה הנתונה, חתן, בצירוף האלגוריתם המתאים (הוראה להשוואת המילה לכל ערכי המילון) ובפלט נקבל את כל האנגרמות, שרשמנו קודם ואולי נוספות. בבדיקה האם שתי מילים הם אנגרמות אחת של האחרת צריך למיין את האותיות בשתי המילים ולהשוות את התוצאה. בהמשך הדיון נתעלם מפעולת המיין של האותיות במלה ונבדוק רק את הזמן הדרוש להשוואה בין שתי מילים, לאחר מיין האותיות. נניח שבהינתן שתי מילים, פעולת ההשוואה ביניהן נמשכת 0.0002 שניות. כל מילה היא מחרוזת של ביטים, כשהמחשב "משווה" בין שתי מילים הוא בעצם משווה בין שתי מחרוזות של ביטים. **הפתרון שהצגנו, אלגוריתם לחיפוש קווי של מילה, דורש אם כן, לפחות 500,000 השוואות.** פעולת ההשוואה של כל 500,000 ערכי המילון למילה נתונה (אחת מהאנגרמות שאנו מחפשים), תמשך 100 שניות  $= 0.0002 * 500,000$ . 100 שניות הן קצת יותר מדקה וחצי. זה מהיר למדי אבל האם זה מספק אותנו? האם אפשר לשפר את זמן החיפוש? האם יש דרך יותר יעילה לחיפוש מילה במילון? נראה דרך כזאת.

### 3.6.3 אלגוריתם לחיפוש בינרי

זכרו כי המילון כולל כחצי מיליון ערכים, מסודרים לפי הא"ב ואנחנו מחפשים, למשל, את כל האנגרמות של המילה "חתן". בדרך החדשה לא נחפש מהתחלת המילון עד לסופו כמו קודם. סידור המילים במילון לפי הא"ב, מאפשר לחפש בשיטה אחרת, שנקראת חיפוש בינרי, "מאמצע לאמצע". מה פרוש? ההוראה למחשב היא לחצות את הנתונים, לבדוק את הערך האמצעי ולראות, האם המלה הנדונה נופלת לפניו או אחריו. נניח שהמחשב נותן לנו את הערך האמצעי במילון, נאמר שזו המילה כנס. מה אנו למדים מכך? שהמלה שאנחנו מחפשים, חתן, מצויה **מתחת** לערך האמצעי, היא מצויה אי שם במחצית הראשונה של רשימת הערכים במילון. לכן אין כל צורך לחפש **בכל** רשימת הערכים, מספיק לחפש מראשית הרשימה ועד אמצעיתה. **כך צמצמנו את מרחב החיפוש לחצי**, כבר אחרי הניסיון הראשון.

נמשיך לחפש, הניסיון השני של החיפוש הוא באמצע המחצית הראשונה של רשימת הערכים. נניח שמצאנו במקום זה את הערך זחל. ערך זה מחלק את המחצית הראשונה של הערכים לשני רבעים. הערך חתן נמצא ללא ספק ברבע השני. לכן אנחנו יכולים להיות בטוחים שהחיפוש השלישי יכול להצטמצם לרבע השני של רשימת הערכים. שימו לב, אחרי שתי פעולות בלבד הצטמצם מרחב החיפוש לרבע. נניח שאנו ממשיכים בדרך זו, תוך כמה פעולות, לכל היותר, נסיים את החיפוש?

$$500,000 * 1/2 = 250,000$$

$$250,000 * 1/2 = 125,000$$

המשיכו את החיפוש בדרך זו ותיווכחו, שתוך 19 בדיקות, לכל היותר, תמצאו את המילה המבוקשת (בדקו).  
 כך מצאנו תוך פרק זמן של  $0.0038 = 0.0002 \times 19$ , כארבע אלפיות שניה, אחת מן האנגרמות של האותיות ח,ג,ת.



## שאלה מספר 12

- א. כמה אנגרמות, לכל היותר, עשויות להיות למילה בת 5 אותיות שונות?
- ב. כמה זמן ימשך החיפוש אחריהן, אם זהו חיפוש בינרי?
- ג. כמה זמן ימשך החיפוש אחריהן אם זהו חיפוש קווי (הדרך הקודמת)?

נוכחנו כי החיפוש הבינרי במילון, של כל האנגרמות שאפשר ליצור ממילה נתונה, יימשך:  
 $19 \times k \times 0.0002$  שניות, כאשר  $k$  מייצג את מספר האותיות באנגרמה. לעומת זאת, החיפוש הקווי של אותן האנגרמות ימשך 100 שניות.

נוכחנו גם, שהחיפוש הבינרי של מילה בודדת הרבה יותר יעיל מהחיפוש הקווי שלה (4 אלפיות השניה בחיפוש בינרי לעומת 100 שניות בחיפוש קווי). כשחיפשנו בדרך זו קבוצה של אנגרמות, אבל חיפשנו כל אנגרמה בנפרד, נוכחנו כי היתרון של החיפוש הבינרי על החיפוש הקווי הצטמצם מאוד. האם אפשר ליעל את החיפוש הבינרי של אנגרמות? בהשקעה של זמן סביר, אפשר בהחלט. נראה זאת.

**חיפוש בינרי של אנגרמות** – לפני החיפוש בדרך החדשה יש צורך בארגון שונה של המילים במילון, לא על פי הא"ב, אלא בהתאם להשתייכותן לאותה קבוצה של אנגרמות. לשם כך נארגן את כל המילים שבמילון בקבוצות. בכל קבוצה נמצאות כל האנגרמות של אותה המילה. לכל קבוצת אנגרמות נבנה את ה"ייצוג" שלה. ה"ייצוג" זהו אנגרמה שאותיותיה מסודרות בסדר האלפביתי. למשל ה"ייצוג" של קבוצת האנגרמות שהבאנו כדוגמה יהיה חנת. מה יהיה ה"ייצוג" של קבוצת האנגרמות של המילה יצור? קבוצה זו תכלול את המילים: יצור, יצרו צורי, ירוצ, רוצי, ציור, וירצ, יוצר, ירצו (בדקו האם יש מילים נוספות), ה"ייצוג" שלה הוא **ויצר**. את כל ה"ייצוגים" נסדר לפי הא"ב ותחת כל "ייצוג" כל האנגרמות שלו. הפעולה של ארגון המילון מחדש נמשכת כ- 3.5 דקות.

איך נשתמש במילון החדש? נניח שאנחנו מחפשים את כל האנגרמות של המילה מבשיל, מהו ה"ייצוג" שלה? **בילמש**. כדי למצוא אותו אנחנו מבצעים חיפוש בינרי רק בין הייצוגים של האנגרמות. האלגוריתם שבנינו מצמצם את החיפוש אחרי מילים רבות (האנגרמות של אותה מילה) לחיפוש בינרי אחרי מילה אחת (הייצוג), שחושפת את כל השאר (האנגרמות שלה).

נוכחנו כי החיפוש הבינרי של אנגרמה על פי הייצוג שלה, יימשך  $0.0038 = 0.0002 * 19$  שניות.

נחזור על הפתרונות של החיפוש במילון ונשווה ביניהם:

הפתרון הראשון – אלגוריתם לחיפוש קווי של מילה. זמן ההרצה כ – 100 שניות. זמן ההרצה לחיפוש כל האנגרמות של מילה בת  $k$  אותיות שונות,  $100k!$  שניות.

הפתרון השני – אלגוריתם לחיפוש בינרי של מילה. זמן ההרצה  $0.0038$  שניות. זמן ההרצה לחיפוש כל האנגרמות של מילה בת  $k$  אותיות שונות,  $0.0038k!$  שניות.

הפתרון השלישי – אלגוריתם לחיפוש כל האנגרמות של אותה המילה, באמצעות הייצוג של האנגרמה. זמן ההרצה כולל מרכיב חד פעמי של ארגון המילון מחדש, כ- 3.5 דקות וחיפוש בינרי אחרי ייצוג האנגרמה המבוקשת,  $0.0038$  שניות.



### שאלה מספר 13

הארגון המחודש של המילון נמשך 3.5 דקות. האם נראה לכם שההשקעה כדאית?

ראינו כיצד מציאת אלגוריתם מוצלח, כלומר יעיל, אלגוריתם של חיפוש בינרי, מגדילה את יעילות הפתרון של הבעיה. הזמן למציאת כל האנגרמות של מילה נתונה, מתקצר מ- 100 שניות באלגוריתם חיפוש קווי, ל-  $0.0038$  שניה באלגוריתם חיפוש בינרי. השקעת הזמן לארגון מחודש של המילון שווה למשך הזמן שהיה דרוש למציאת שני ערכים באמצעות האלגוריתם הקווי. זו ללא כל ספק השקעה כדאית.

מהי הסיבוכיות בזמן של אלגוריתם החיפוש הבינרי ביחס לסיבוכיות אלגוריתם החיפוש הקווי?

הסיבוכיות של החיפוש הקווי, של ערך מסוים מבין  $n$  ערכים, היא  $n$ .

הסיבוכיות של החיפוש הבינרי של אותו ערך מבין  $n$  ערכים, היא מספר הפעמים בהם צריך לחלק את  $n$  ב-2, עד שהתוצאה קטנה מ 2. ראינו כי כאשר  $n = 500,000$ , חילקנו ב-2, 19 פעמים. אפשר לבטא זאת גם על ידי הביטוי:  $2^{19} = 527,444 \sim 500,000$

הסיבוכיות בזמן של החיפוש הבינרי במקרה שבדקנו היא 19 ובמקרה הכללי, כשמבצעים חיפוש בינרי של ערך מסוים מבין  $n$  ערכים, הסיבוכיות בזמן היא מעריך החזקה של 2, השווה ל-  $n$ .

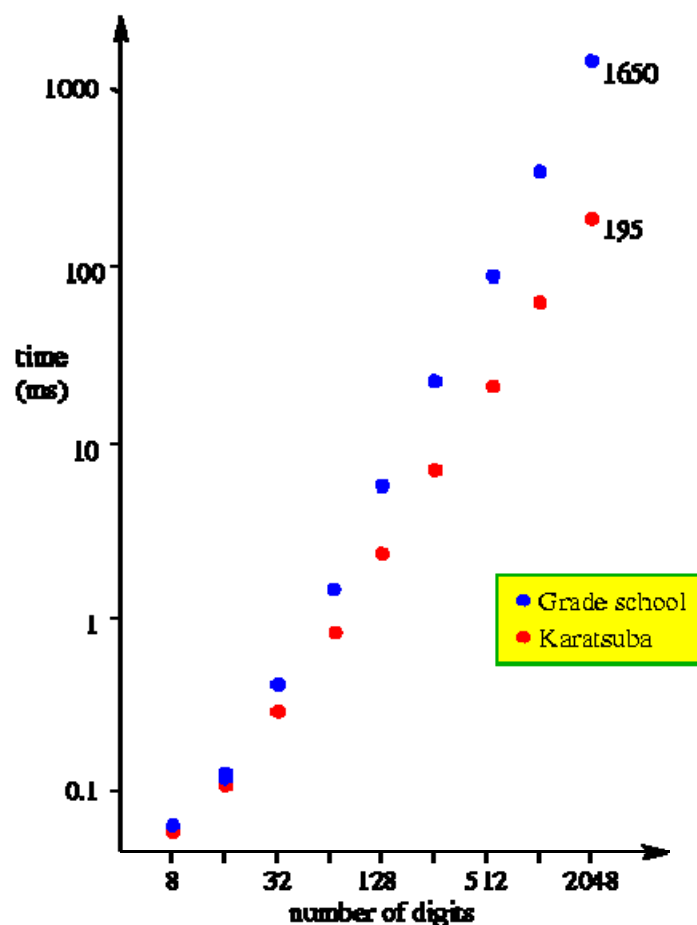
(הערה: למעריך החזקה קוראים גם הלוגריתם של  $n$  לפי בסיס 2. הוא נכתב:  $\log_2 n$ . אנחנו לא נשתמש במונח זה, אבל הוא מוזכר כאן כיוון שאתם עשויים להיתקל בו בספרות או באינטרנט. שימו לב לא לבלבל בין לוגריתם ובין אלגוריתם.)

נוכחנו אם כן, שהסיבוכיות בזמן של אלגוריתם החיפוש הבינרי קטנה יותר מזו של אלגוריתם קווי.

כשבדקנו את הסיבוכיות של פעולות החשבון ראינו כי הסיבוכיות של החיבור היא קווית ואילו הסיבוכיות של הכפל ריבועית. במילים אחרות, האלגוריתם של החיבור הוא קווי ושל הכפל ריבועי. האם אפשר לשפר את האלגוריתמים האלה, בדומה לשיפור שהצלחנו להשיג באלגוריתם החיפוש המילוני?

האם אפשר לבנות אלגוריתם חיפוש בינרי לחיבור? האלגוריתם של החיפוש הבינרי בנוי על כך שאיננו צריכים את כל ערכי המילון, אלא רק ערך מסוים. החיפוש הבינרי נותן לנו שיטה, כלומר אלגוריתם, איך לגלות ולפסול במהירות את כל הערכים המיותרים, **שלא צריך לחפש ביניהם**. אבל כשאנחנו מבצעים פעולת חיבור, **איננו יכולים להתעלם משום ספרה** ולכן האלגוריתם המתאים לנו הוא האלגוריתם הקווי, אין יעיל ממנו לצורך החיבור.

ומה לגבי פעולת הכפל? האם אפשר לשפר את אלגוריתם הכפל המוכר לנו, האלגוריתם הריבועי? האם קיים אלגוריתם, שסיבוכיות הזמן שלו קווית, לביצוע הכפל? לא נוכל להיכנס כאן לפרטי הבעיה ולפתרונה. נציין רק כי קיים אלגוריתם המשפר חלקית את האלגוריתם הריבועי המוכר לביצוע הכפל. לכל המעוניינים להעמיק בנושא, האלגוריתם נקרא על שם ממציאו Karatsuba. אלגוריתם זה יעיל לגבי מספרים גדולים. בתיאור הגרפי המופיע בדף זה, תוכלו לראות זאת. מי שמעוניין להכיר את האלגוריתם לצמצום הסיבוכיות של פעולת הכפל, ביתר פירוט, ימצא את ציון המקור לכך בנספח הביבליוגרפי.



בדקנו את היעילות של אלגוריתמים שונים. אבל האם יודעים תמיד **מהי** היעילות אותה מבקשים להשיג? האם יודעים תמיד מהו המספר **המצערי** של הצעדים הדרושים לפתרון בעיה מסוימת? האם תמיד אפשר לדעת אותו? רק אם יודעים מהי הסיבוכיות הטבועה בבעיה, אפשר גם לדעת תיאורטית מהו האלגוריתם היעיל.

### 3.7 דיון וסיכום

לצורך גיבוש וסיכום הדיון ביעילות האלגוריתמים, אנחנו נזקקים למושגים נוספים, נגדיר אותם: השתמשנו קודם לכן במושג "המקרה הגרוע ביותר". לסיבוכיות של המקרה הזה אפשר לקרוא "החסם העליון" (Upper Bound) של סיבוכיות הבעיה. אבל החסם העליון הוא לא בהכרח קבוע. אם מצאנו אלגוריתם שהסיבוכיות שלו בזמן יותר קטנה והוא "עובד", אזי הוא, כעת, החסם העליון של סיבוכיות הזמן. למשל, במקרה של החיפוש המילוני, בתחילה החסם העליון היה האלגוריתם לחיפוש קווי, אבל כשבנינו את אלגוריתם החיפוש הבינרי, הפך הוא לחסם העליון. מצד שני, אם אפשר להוכיח, מתוך הסיבוכיות הטבועה בבעיה, שאין אלגוריתם יותר טוב מהחיפוש הבינרי, אז האלגוריתם הזה הוא גם "החסם התחתון" (Lower Bound), לא יהיו טובים ממנו ולכן הוא גם האלגוריתם היעיל ביותר לפתרון הבעיה. בכל מקרה שאנחנו יודעים מהו המספר המינימלי של הצעדים הדרושים לפתרון בעיה מסוימת, יש לנו גם אפשרות להעריך את יעילותו של האלגוריתם המצוי בידינו. לשם כך אנו בוחנים את הפער בין האלגוריתם שהצלחנו לתכנן, "החסם העליון" ובין האלגוריתם הטוב ביותר האפשרי, "החסם התחתון". במילים אחרות, אנו בוחנים את הפער בין המצוי לרצוי, בין סיבוכיות הבעיה לבין יכולתנו להתמודד איתה. נחזור לתחום ההצפנה ולבעיה של פיצוח מסרים מוצפנים. במה תלוי מספר הפעולות הדרושות **לפיצוח**?

### 3.8 הסיבוכיות של שיטות הצפנה סימטריות

בחוברת הקודמת, שעסקה בהצפנה סימטרית, הכרנו שיטות הצפנה שונות ואת הבעיות הכרוכות בפיצוחן. נבחן כעת את בעיית הפיצוח של שיטות ההצפנה האלה, על פי המדד החדש שהכרנו, הסיבוכיות החישובית. לפני שניגש לבחינה מפורטת של שיטות ההצפנה הסימטרית נגדיר את "חוקי המשחק". אנו מניחים כי לידי היריב נפל מסר מוצפן. היריב ינצח, אם יצליח לחלץ את מפתח ההצפנה ואולי גם להשתמש בו כדי להצפין מסרים נוספים (מתוך הנחה שהאלגוריתם ידוע לו).

#### 3.8.1 הסיבוכיות של פיצוח צופן יוליוס קיסר

נתחיל באבי הצופנים, צופן יוליוס קיסר (הזזה עם מפתח +3). נניח שלידי היריב נפל מסר מוצפן בצופן יוליוס קיסר, שאורכו 10 תווים. היריב, שמכיר את המפתח, מבצע 10 פעולות ומפענח את המסר. כיצד תשתנה משימתו של היריב אם אורך המסר המוצפן מיליון תווים?

משימת הפענוח של מסר מוצפן בצופן יוליוס קיסר, שארכו 10 תווים, שונה ממשימת הפענוח של מסר שהוצפן באותו צופן, אבל אורכו מיליון תווים, משימת הפענוח הרבה יותר גדולה. מספר הפעולות הבסיסיות, שעל המחשב לבצע לצורך הפענוח, מבטא את נפח העבודה שעל המחשב לבצע. במקרה של צופן קיסר, המספר הוא פשוט מספר התווים שיש לפענח.

במקרה הכללי כשהמסר המוצפן הוא בן  $m$  תווים, מספר פעולות הפענוח של המחשב גם הוא  $m$ . כשהמסר גדל פי 10 גם מספר פעולות הפענוח גדל באותו יחס. אין שום הפתעות של "התפוצצות" בגידול מספר פעולות הפענוח, הוא נשאר שווה למספר התווים במסר. הזמן הדרוש לפענוח צופן קיסר בן  $m$  אותיות הוא  $T(m) = m$ .

אלגוריתם הפענוח הוא חיסור, אלגוריתם מוכר ויעיל, שמביא אותנו בבטחה אל פתרון יחיד, אל המסר המקורי.

### 3.8.2 הסיבוכיות של פיצוח צופן הזזה מונואלפאבית

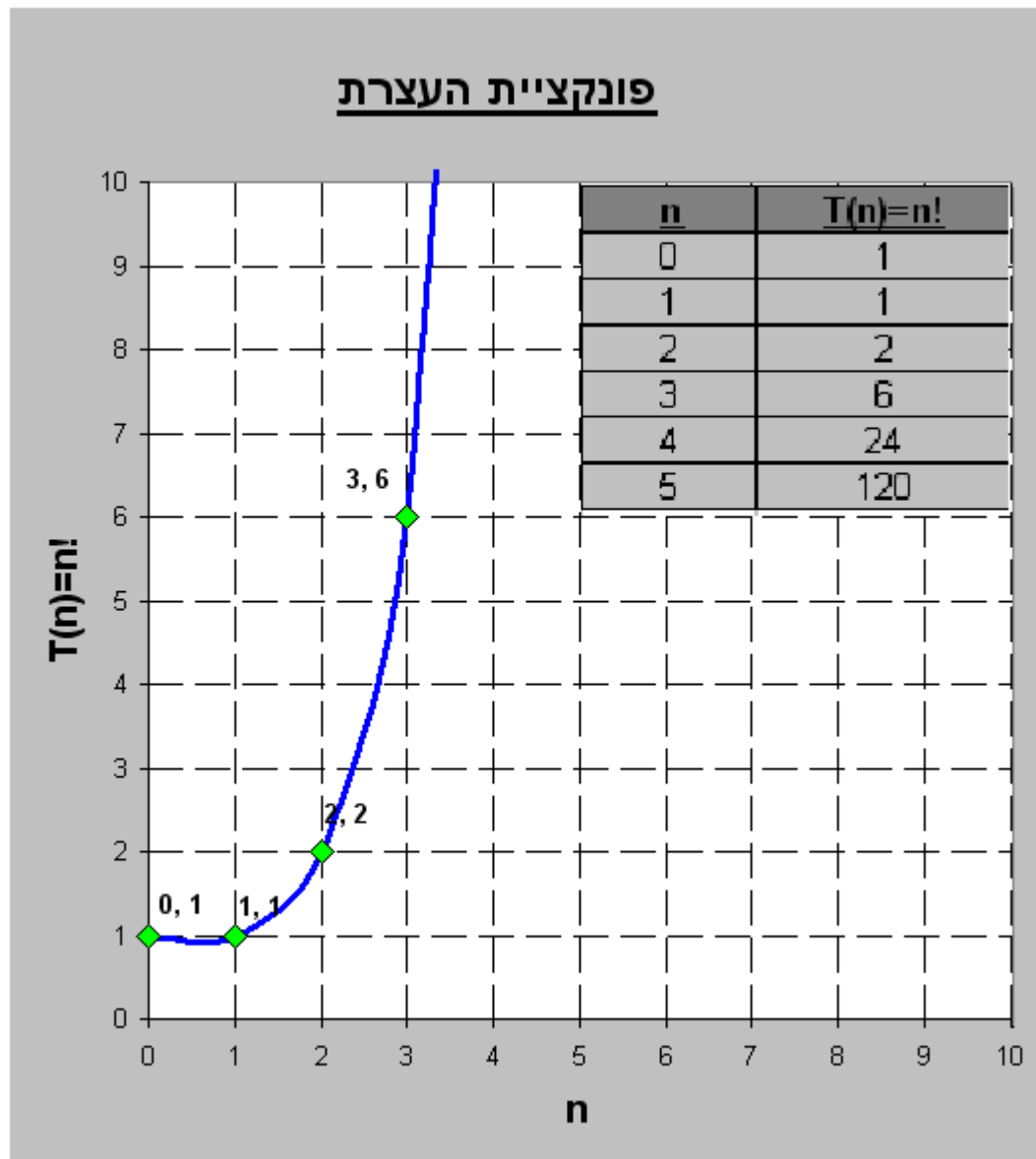
נבחן מקרה נוסף, מהי הסיבוכיות של צופן הזזה כלשהו? מה המצב כשהיריב **יודע** כי המסר המוצפן שנפל בידיו הוצפן **באלגוריתם** של הזזה, אבל אינו יודע מהו **מפתח** ההזזה? כדי לפצח את ההצפנה עליו לבצע חיפוש ממצה (brute force attack), כלומר, עליו לנסות את כל מפתחות ההזזה האפשריים. נניח שהמסר הוא בן  $m$  תווים. מה מספר פעולות הפענוח שעל המחשב לבצע, כשמדובר על מסר בן  $m$  תווים ועל  $n$  מפתחות הזזה אפשריים ( $n=22$  בעברית,  $n=26$  באנגלית,  $n=28$  בערבית,  $n=33$  ברוסית)? מספר פעולות המחשב במקרה זה הוא המכפלה  $nm$ . גם כאן האלגוריתם ידוע ולכן הפענוח (הפתרון) מובטח, אם כי הזמן הדרוש לביצועו ממושך יותר מאשר במקרה הקודם:  $T(n) = nm$ . נסכם כי: הסיבוכיות של צופן הזזה היא יחסית למכפלה של שני גורמים  $T(n) = nm$ , זוהי סיבוכיות ריבועית.

אנו רואים כי "במקרה הגרוע ביותר", הסיבוכיות של צופן הזזה היא  $T(n) = nm$ . במילים אחרות, אלגוריתם הפיצוח הוא אלגוריתם של כפל. זה החסם העליון, האם יש אלגוריתמים יותר טובים? אנחנו יודעים שכן וגם השתמשנו בהם. כשהמסר המוצפן קצר מאד אין בעיה לבצע חיפוש ממצה. אבל כשנתון לנו מסר מוצפן ארוך, שהוצפן בהזזה, נוכחנו כי יש דרכים קצרות יותר ויעילות יותר לפיצוחו. ראינו כיצד אפשר לנצל ממצאים לשוניים סטטיסטיים, כמו שכיחות של אותיות ושל מילים מסוימות, לפיצוח המסר המוצפן (בתנאי שהוא מספיק גדול). כולם הם אלגוריתמים טובים יותר מן האלגוריתם הריבועי. שימו לב שאנחנו משיגים הקטנה בסיבוכיות של פתרון בעיה, אם אנחנו מצליחים למצוא אלגוריתם בעל סיבוכיות יותר קטנה לפתרונה.

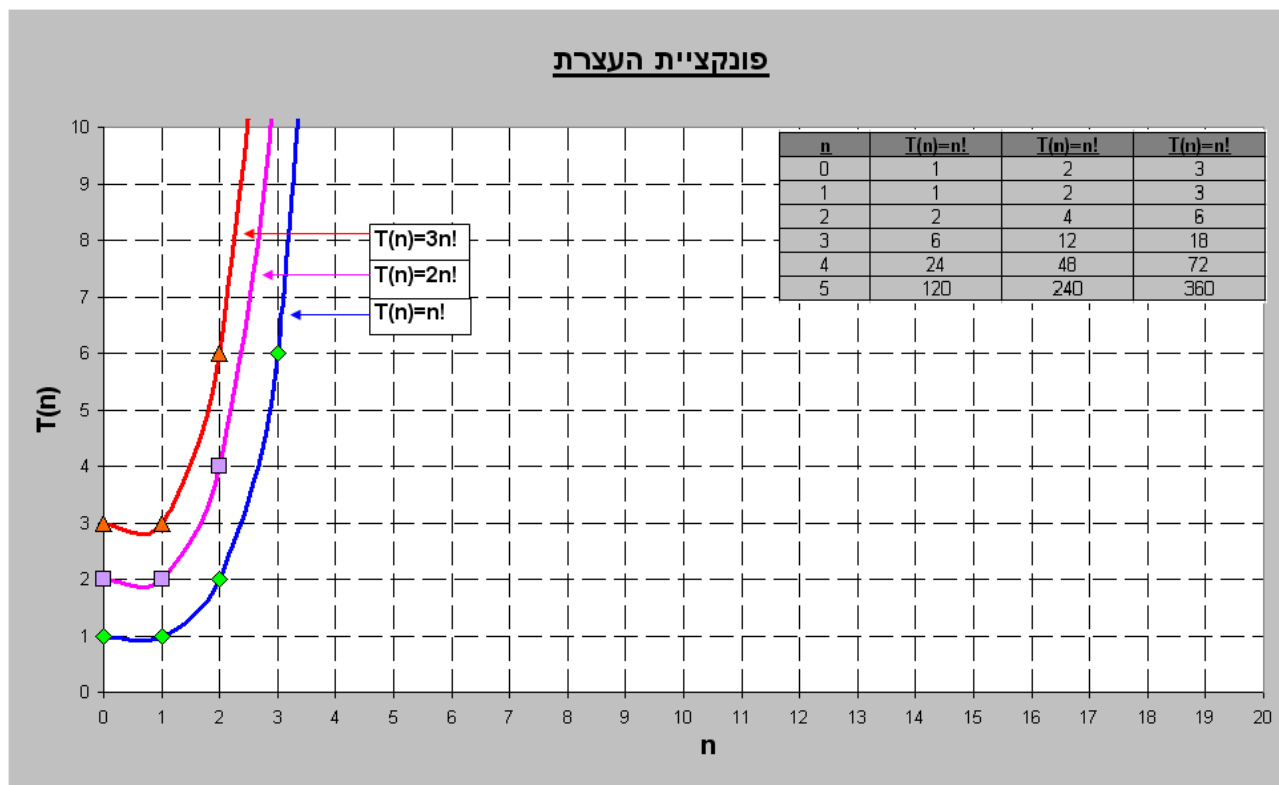
### 3.8.3 הסיבוכיות של פיצוח צופן שחלוק מונואלפאביתי

אנו יודעים כי צופן ההזה הוא מקרה פרטי של צופן שחלוק. בצופן ההזה מידת ההזה של כל אות בתהליך ההצפנה שווה ואילו בצופן שחלוק, מידת ההזה של כל אות שונה. מהי הסיבוכיות של פיצוח מסר שהוצפן בצופן שחלוק כלשהו? כמה פעולות מחשב נדרשות לפיצוחו?

למדנו כי צופני שחלוק הם צופני תמורות. ראינו שמספר מפתחות ההצפנה האפשריים, במקרה זה הוא  $n!$ . מספר המפתחות האפשריים מבטא את הסיבוכיות בזמן הפיצוח. הזמן הדרוש לחישוב כל המפתחות הוא  $T(n)=n!$ .



הערה: כפי שראינו, מספר הפעולות תלוי גם באורך המסר  $n$ . כלומר,  $T(n) = m \cdot n!$ . אולם, מתברר שהשפעתו של המקדם  $m$  על סיבוכיות הפונקציה  $n!$  היא זניחה (ראה שרטוט):



הכרנו עד עכשיו מידות שונות של סיבוכיות, הנבדלות זו מזו ב"קפיצת מדרגה", קפיצה מה"קוויות" ל"ריבועיות" ול"עצרתיות". המונח המתמטי המבטא זאת הוא "**סדר גודל**".

**סימון סדר הגודל של הסיבוכיות** – אנחנו מבדילים בין הסיבוכיות החישובית של האלגוריתמים לפתרון בעיות שונות על ידי ציון **סדר הגודל** של הסיבוכיות שסימנו  $O(n)$ :

|                   |                                                 |
|-------------------|-------------------------------------------------|
| $O(n) = \log_2 n$ | במקרה של אלגוריתם לחיפוש בינרי                  |
| $O(n) = n$        | במקרה של סיבוכיות קווית (פעולות חיבור או חיסור) |
| $O(n) = n^2$      | במקרה של סיבוכיות ריבועית (פעולת כפל)           |
| $O(n) = n!$       | במקרה של סיבוכיות עצרתית (צופני תמורות)         |

נחזור לצופני תמורות, אשר הסיבוכיות החישובית של פיצוחם היא מסדר גודל  $n!$ , כלומר  $O(n!)$ . המשמעות היא, ש"במקרה הגרוע ביותר" כשצריך לנסות את כל המפתחות האפשריים, החסם העליון של סיבוכיות הפיצוח של צופני תמורות היא  $O(n!)$ .

כשהצגנו את הדוגמה של פיצוח צופן שחלוק בראשית הפרק, נוכחנו כי אלגוריתם שהסיבוכיות שלו  $O(n!)$  אינו אלגוריתם מעשי לפיצוח צופן שחלוק. ראינו שאם מדובר בשפה האנגלית כאשר  $n = 26$ , אז  $n! \approx 400,000,000,000,000,000,000,000$  ספרות, ארבע מאות מיליון מיליארד מיליארדים. במילים אחרות, לכאורה קיים אלגוריתם לפתרון הבעיה, אבל **פתרונה בפועל, באמצעות האלגוריתם**, דורש מספר כל כך גדול של פעולות, עד כדי כך, שבעצם אינו מעשי, גם על ידי המחשבים החזקים ביותר הפועלים כיום. כבר במקרה של צופן הזה, שסיבוכיותו הרבה יותר קטנה, נזקקנו וגם מצאנו אלגוריתמים חלופיים לפיצוח מסרים מוצפנים, אלגוריתמים שמסתמכים על התכונות הלשוניות הסטטיסטיות של שפת המסר המוצפן. במקרה שהמשימה היא פיצוח צופן שחלוק מונואלפאבית, חשיבותם של הממצאים הסטטיסטיים והבלשניים, שהזכרנו בסעיף הקודם, עולה לאין ערוך והיא קריטית לפענוחו של צופן זה. גורם נוסף, לתכונות הלשוניות והסטטיסטיות של שפת המסר, שעשוי להקל על הפיצוח, הוא אם הצלחנו לשים יד על חלקים מן המסר המקורי. במקרה מוצלח כזה אפשר לבדוק את קטעי המסר המקורי מול קטעי המסר המוצפן ואולי לגלות כך חלקים של מפתח ההצפנה. במקרים שהמסר קצר מכדי להסתמך על ממצאים לשוניים – סטטיסטיים, אפשר לנסות תחבולות אחרות. היזכרו כיצד פיצחנו אנחנו מסרים מוצפנים על ידי שימוש במילות מתכונות (למשל המילה THAT, שעזרה לפצח מסרים מוצפנים בסעיף 5.3 בחוברת הראשונה). כמו שכבר הזכרנו, היתרון המיוחד של שימוש במילות המתכונות, על פני שימוש בנתונים סטטיסטיים, הוא, שהאפשרות ליישם ממצאים לשוניים סטטיסטיים תלויה **באורך המסר** ואילו האפשרות לנצל את מילות המתכונות אינה תלויה באורך המסר המוצפן, אלא רק בהימצאותה של מילת המתכונות במסר המוצפן. נוכחנו שאפשר לפצח מסרים **שהוצפנו** על ידי אלגוריתם של שחלוק, שסיבוכיות הפיצוח שלו  $O(n!)$ , על ידי אלגוריתמים **אחרים**, שסיבוכיותם יותר קטנה. שימו לב לבעיה מעניינת: שיטת הפיצוח על ידי אלגוריתם של חיפוש ממצה היא מאוד ברורה, ולהלכה מובטח שהיא מביאה לפתרון. הבעיה אתה, שבמקרה של צופן שחלוק היא אינה שיטה מעשית. הפיצוח על ידי חיפוש ממצה אינו סביר, למרות שהוא מוביל בוודאות ובדרך שיטתית לפתרון. נוהגים להגדיר אלגוריתם כזה "מוביל בוודאות לפתרון אבל אינו סביר". ומכיון שאין הוא אלגוריתם סביר, חפשנו אלגוריתמים אחרים ואמנם **מצאנו אלגוריתמים שונים, שהמשותף להם הוא הניסיון לפצח את המסר המוצפן, תוך הסתמכות על התכונות הלשוניות של המסר המקורי, שנשמרו במסר המוצפן**. האם הפיצוח אפשרי? האם אפשר להוכיח שהוא אפשרי? **עצם הפיצוח הוא ההוכחה היחידה**. נוכחנו כי בידינו אלגוריתם אחד שהוא שיטתי, האלגוריתם של "ניסוי כל המפתחות האפשריים", הוא מוביל בוודאות לפתרון אבל אינו סביר, עקב סיבוכיות הזמן העצומה של הרצתו. לעומת זאת, ניסיון הפיצוח באלגוריתם חלופי, של "בדיקת כל התכונות הלשוניות הרלוונטיות" אינו מוביל **בוודאות** לפתרון, אף פעם לא נוכל לדעת **מראש** את תוצאות הבדיקה של תכונה לשונית, זו או אחרת, שאנו מנסים לנצל לפיצוח הצופן. **אף פעם לא נדע לאן היא תביא אותנו, עד שנגיע לשם** (נבצע את הבדיקה).

מניסיונו, כתוצאה מבדיקת התכונות הלשוניות, הפכה בעיית הפיצוח של צופן השחלוף לבעיה סבירה (שפתרונה סביר). היא הייתה לא סבירה תחת האלגוריתם של החיפוש הממצה והפכה לסבירה תחת האלגוריתם הסטטיסטי - לשוני. האם זה האלגוריתם היעיל ביותר? איננו יודעים. אנחנו מסתפקים בכך שהוא סביר.

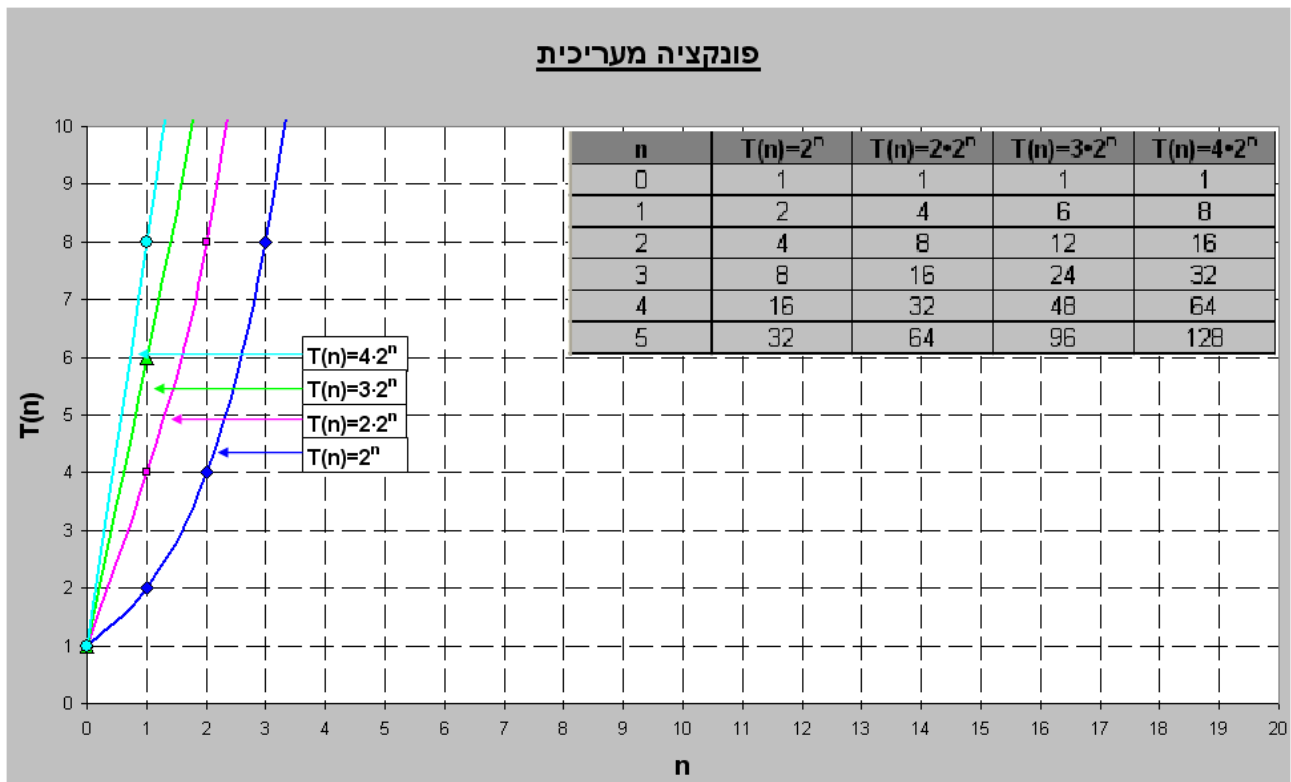
### 3.8.4 הסיבוכיות של פיצוח הצפנה באלגוריתם DES

בחוברת הקודמת הכרנו את מפתח ההצפנה DES. למדנו כי אורך מפתח ה-DES, הוא 56 תווים בינריים. ה-DES פועל על ייצוג בינרי של המסר. נוכחנו כי מספר מפתחות ההצפנה השונים, שאפשר ליצור באלגוריתם ה-DES, הוא  $2^{56}$ , ובאופן כללי, מספר המפתחות שאפשר ליצור מ- $n$  תווים בינריים הוא  $2^n$ . לכן סדר הגודל של החסם העליון של סיבוכיות הפיצוח הוא  $O(2^n)$ .

אם אורך המסר הוא  $m$  אז יש לבצע  $m \cdot 2^n$  פעולות כדי לפצח את צופן DES. זהו "המקרה הגרוע ביותר" של סיבוכיות הפיצוח של הצפנה. זהו המקרה בו עלינו לנסות את כל המפתחות האפשריים כדי למצוא את המפתח האחד שבו בוצעה ההצפנה.

לסיכום: הסיבוכיות של פיצוח ה-DES,  $O(2^n)$ . הסיבוכיות של הצפנת DES נקראת סיבוכיות מעריכית.

הערה: כפי שראינו, מספר הפעולות תלוי גם באורך המסר  $n$ . כלומר,  $T(n) = m \cdot 2^n$ . אולם, מתברר שהשפעתו של המקדם  $m$  על סיבוכיות הפונקציה  $2^n$  היא זניחה (ראה שרטוט):



בניגוד להצפנת שחלוף מונואלפביתית, שלפיצוחה מצליחים למצוא אלגוריתמים יותר טובים מ- $O(n!)$ , הרי שלפיצוח הצפנות ב-DES, ברוב המקרים אין אלגוריתמים טובים יותר מחיפוש ממצה. זהו המצב במידה ואין בידינו הצפנות רבות. אבל במקרים שבהם נפלו בידי המפצח הצפנות רבות, המצב עשוי להיות שונה. גם במאבק לפיצוח ה-DES יש נקודה ישראלית. פרופ' עדי שמיר ממפתחי RSA ופרופ' אלי ביהם מן הטכניון, הצליחו להקטין את סיבוכיות הפיצוח של DES. הם פתחו אלגוריתמים לפיצוח ה-DES, שהוא יעיל כאשר בידי המפצח הצפנות רבות. במצב זה הם הצליחו לפתח אלגוריתמים לפיצוח ה-DES שהסיבוכיות שלהם היא  $2^{40}$  ואפילו  $2^{20}$ .

### שאלה מספר 14

פי כמה קטנה סיבוכיות הפיצוח של DES, על ידי שני האלגוריתמים שנזכרו בסוף הפסקה הקודמת?

### 3.8.5 – השוואת הסיבוכיות החישובית, של פונקציות שונות

#### שאלה מספר 15

בטבלה נתון גידולו של  $n$  בפונקציות שונות:  $F(n)=n$ ,  $F(n)=n^2$ ,  $F(n)=2^n$ ,  $F(n)=n!$ . השלימו את הטבלה ורשמו בה את הגידול של כל אחת מהפונקציות  $F(n)$ , כתוצאה מהגידול של  $n$ :

| $F(n)=n!$<br>גידול עצרתי (פקטוריאלי) | $F(n)=2^n$<br>גידול מעריכי (אכספוננציאלי) | $F(n)=n^2$<br>גידול ריבועי | $F(n)=n$<br>גידול קווי | $n$                    |
|--------------------------------------|-------------------------------------------|----------------------------|------------------------|------------------------|
|                                      | 4                                         | 4                          | 2                      | 2                      |
|                                      |                                           |                            | 5                      | 5                      |
|                                      |                                           |                            | 9                      | 9                      |
| $10! = 3,628,800 \sim 10^6$          | $2^{10} = 1024 \sim 10^3$                 |                            |                        | 10                     |
|                                      |                                           |                            | 26                     | 26 (אותיות הא"ב)       |
|                                      |                                           |                            |                        | 56 (תים בינריים ב DES) |
|                                      |                                           |                            |                        | 100                    |
|                                      | $2^{1000} \sim 10^{333}$                  | 1,000,000                  | 1000                   | 1000                   |
|                                      |                                           |                            |                        | $10^4$                 |
|                                      |                                           |                            |                        | $10^6$                 |



## שאלה מספר 16

השוו את קצב הגידול של הפונקציות משאלה 15, כאשר  $n$  גדל מ-9 ל-10:  
פי כמה גדול הגידול הריבועי מהגידול הקווי, במקרה זה?

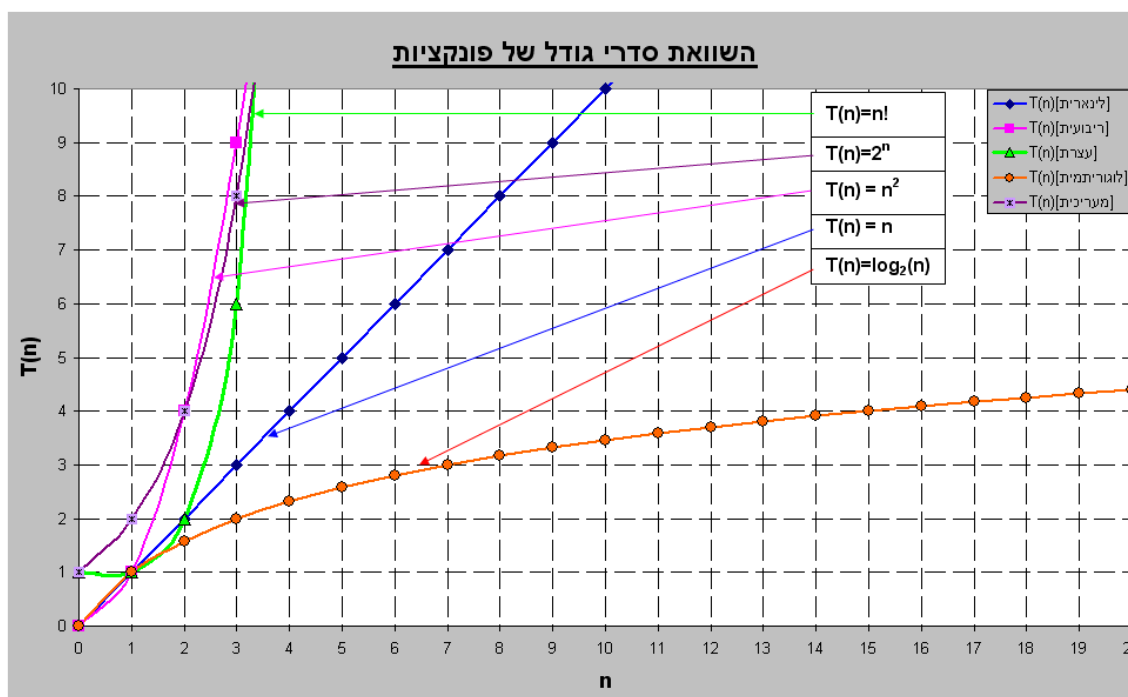
- א. הגידול המעריכי מהגידול הריבועי
- ב. הגידול המעריכי מהגידול הקווי
- ג. הגידול העצרתי מן הגידול הקווי
- ד. הגידול העצרתי מהגידול המעריכי

### 3.8.6 סיכום ביניים

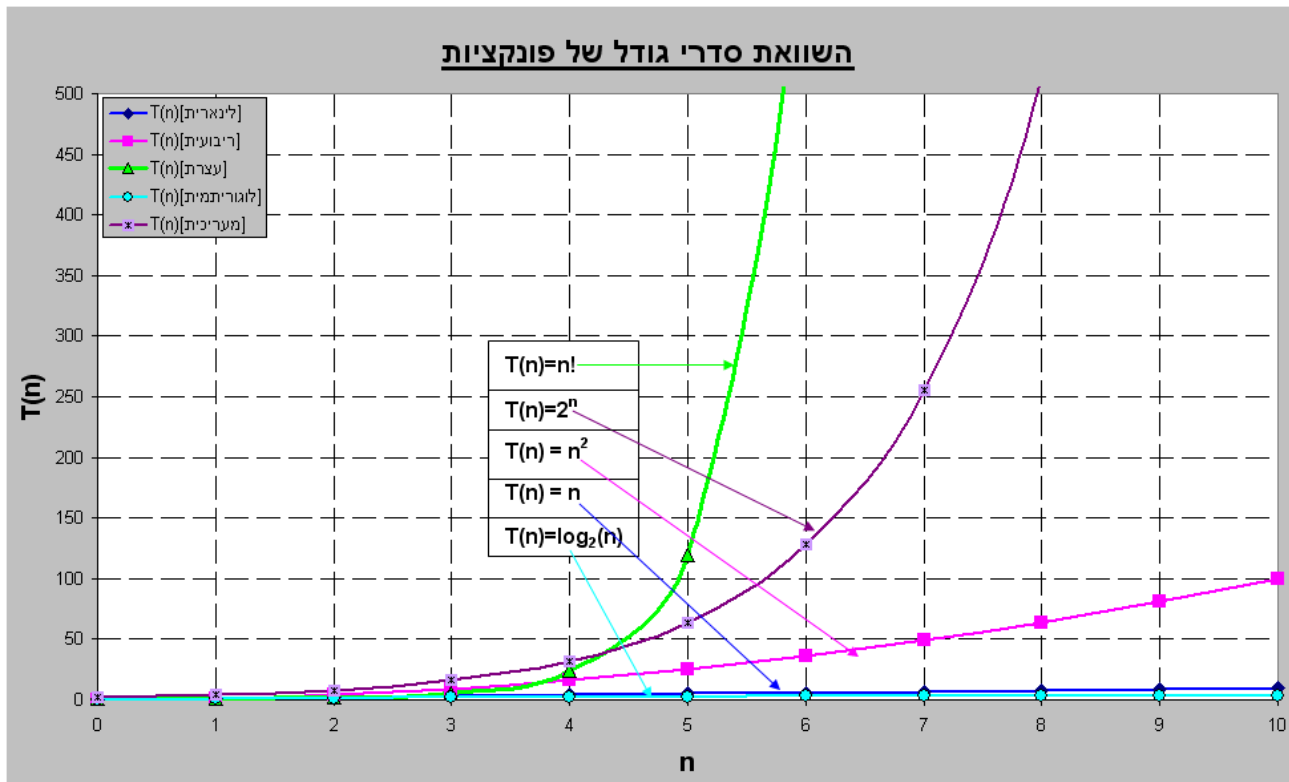
בדוגמאות השונות של שיטות הצפנה, שהובאו לעיל נתקלנו ברמות שונות של סיבוכיות, שמתייחסות ל"מקרה הגרוע ביותר". נוכחנו כי הסיבוכיות של  $n$  נובעת **מקצב הגידול** שלו. קצב הגידול של  $n$  תלוי בפונקציות הגידול השונות המופעלות עליו. כמו כן, נוכחנו בקשר שבין אלגוריתם ההצפנה (פונקצית ההצפנה) לסדר הגודל של סיבוכיות ההצפנה.

ראינו ש:  $O(\log_2 n) < O(n) < O(n^2) < O(2^n) < O(n!)$

השרטוט הבא משווה בין הפונקציות:  $T(n)=\log_2 n$ ,  $T(n)=n$ ,  $T(n)=n^2$ ,  $T(n)=2^n$ ,  $T(n)=n!$ . רואים כי קצב הגדילה של הפונקציה הרבועית, הפונקציה המעריכית ופונקצית העצרת הוא הגדול ביותר.



השרטוט הבא מבליט את השוני בקצב הגידול שבין הפונקציות הרבועית, המעריכית והעצרתית, ע"י שינוי בקנה המידה של הגרפים:



נחזור לשיטות ההצפנה שדנו בהן קודם. בכולן, למרות הסיבוכיות הגבוהה לעיתים הכרוכה בפיצוחן, הצלחנו בסופו של דבר במשימת הפענוח. אפילו בהצפנת שחלוף מונואלפיתית, שהסיבוכיות שלה בסדר גודל של עצרת. כיצד עשינו זאת? מה היו דרכי ההתמודדות, שעמדו בפנינו?

בהצפנות שפיצוחן בעל סיבוכיות גדולה מאד מתמודדים עם הסיבוכיות בעיקר בשתי דרכים:

- א. **עקיפת הקושי על ידי גילוי קיצורי דרך** (בדומה לפיתוח אסטרטגיות ניצחון במשחק "בול קליעה"). קיצורי הדרך מתאפשרים על ידי שימוש באלגוריתמים חלופיים, שהסיבוכיות שלהם יותר קטנה. האלגוריתמים האלה מתבססים על התכונות הלשוניות הסטטיסטיות של שפת המסר המוצפן. כלומר, על שכיחות שונה של אותיות מילים ותבניות לשון, שהשתמרו בהצפנה ובכך מסייעים לפענוח.
  - ב. **התמודדות עם הקושי על ידי שיפור והגדלת משאבי החישוב**, אותם משיגים על ידי פיתוח ושכלול המחשב היחיד ועל ידי פיתוח מערכות מחשבים העובדות במקביל ויוצרות כוח חישוב מוגדל.
- אבל בדיון על ההצפנות הסימטריות נתקלנו בהצפנה **חסנית פיצוח**, ההצפנה ב-One Time Pad. מהי הסיבוכיות החישובית של פיצוחה? נבחן זאת בסעיף הבא.

### 3.8.7 הסיבוכיות של פיצוח One Time PAD

נחזור ונזכר במקרה של ה-One Time Pad. מדוע, בעצם, לא הצלחנו לפצחו? האם זו, באמת, משימה בלתי אפשרית? זכרו כי בצופן זה המפתח הוא סדרה אקראית של אותיות, חסרת מובן בכל שפה שהיא. אורך המפתח כאורך המסר המוצפן. אם המסר הוא בשפה האנגלית  $n = 26$  ואורכו  $m$  אותיות, כי אז מספר המפתחות האפשריים הוא  $26^m$  ובאופן כללי,  $m^n$ . מספר המפתחות עשוי להיות עצום, אבל נוכחנו כי זו לא חייבת להיות בעיה, שתמנע את הפענוח. הקושי הוא לא בהכרח בזה. נוכחנו כי יתכן שקיימים קיצורי דרך ודרכים לעקיפת הקשיים. זכרו, מה היו קיצורי הדרך שלנו במקרים קודמים? הם נבעו כולם מניצול המידע שהצלחנו להשיג על התכונות של שפת המסר, שנשמרו גם במסר המוצפן. אבל במקרה הנדון שורש הבעיה בכך, שעם ההצפנה **נעלם כל המידע**. עקב **אקראיות** המפתחות, נעלם כל המידע על התכונות הלשוניות של המסר עם הצפנתו.

שום מידע על כך לא נשמר במסר המוצפן. איננו יודעים מהו המפתח ואין לנו שום אפשרות לגלות אותו בגלל האקראיות המוחלטת של יצירתו וכיוון שארכו כאורך המסר (ואין חזרות שמסגירות תבניות). ראינו כי התוצאה היא, שאי אפשר להכריע בין מפתחות שונים ולכן גם בין פתרונות (פענוחים) שונים בעלי משמעויות שונות, שכולם עשויים להיות אפשריים וכולם נראים הגיוניים באותה מידה.

במילים אחרות, בכל המקרים הקודמים קבלנו במהלך הפענוח צירופי אותיות **רבים** ושונים חסרי משמעות וצרוף **אחד** בעל משמעות והוא היה **הפענוח** (בהגבלה אחת שהמסר המוצפן כלל מספיק אותיות). בכל המקרים האלה הייתה **חוקיות** להצפנה (הזזה, ערבול, שחלוף) ולכן היו לנו דרכי התמודדות, באמצעותן מצאנו פתרון יחיד, **הפענוח**. אבל במקרה של ה-One Time Pad, **ההצפנה היא אקראית לחלוטין ולכן אין אלגוריתם, אפילו אלגוריתם לא יעיל, שמאפשר להגיע לפענוח בטוח. כלומר, אין אלגוריתם שמאפשר למצוא פתרון יחיד**. לכן צופן זה אינו ניתן לפיצוח, אבל הוא גם לא מעשי, במערכת רבת משתמשים, בגלל קשיי ניהולו (ריבוי המפתחות והבטחת הסודיות שלהם), אותם כבר תארנו בחוברת הקודמת.

### 3.8.8 הסיבוכיות של פיצוח צופן כפל מודולרי

לסיום בדיקת הסיבוכיות של שיטות ההצפנה שהכרנו, נותר לבדוק מהי הסיבוכיות של שיטת ההצפנה האסימטרית על ידי כפל מודולרי. נוכחנו כי בשיטה זו ידיעת אלגוריתם ההצפנה ומפתח ההצפנה לא סיפקה מיידית את מפתח הפענוח. הפענוח מבוצע על ידי כפל בהפכי הכפלי המודולרי. נוכחנו שהאלגוריתם למציאת ההפכי הכפלי עשוי להיות בניית טבלת הכפל, במודול בו עובדים ומציאת ההפכי הכפלי בטבלה זו. זה טרחני למדי במודול בן שתי ספרות ומה לגבי מודולים גדולים? האם זה האלגוריתם היעיל? אולי יש אחר יעיל ממנו?

הבעיה שלפנינו שונה מן הבעיות הקודמות. יש לנו שיטת הצפנה אבל איננו יודעים כיצד לייצר את זוג המפתחות להצפנה ולפענוח. אין לנו אפשרות לקבוע את הסיבוכיות של האלגוריתם לפני שנדע מהו האלגוריתם היעיל למציאת ההפכי הכפלי. נשאיר שאלה זו פתוחה, אך נחזור אליה בהמשך.

### 3.8.9 הערה: פונקציה חד כיוונית ודלת סתרים

בדיון המפורט על סיבוכיות חישובית ובבדיקת הסיבוכיות החישובית של ההצפנות הסימטריות, בנינו גישה חדשה לבעיית הפיצוח של מסרים מוצפנים. בחוברת הראשונה דברנו על כך ש"אפשר או אי אפשר" לפצח את המסר המוצפן. ההיכרות עם מושג הסיבוכיות הביאה אותנו לדיון שונה. לדיון בשאלה האם "סביר או לא סביר", "ישים או לא ישים" לפצח את המסר המוצפן.

תורת ההצפנה המודרנית מבוססת על הפער בסיבוכיות בין אלגוריתם ההצפנה והפענוח של המשתמש החוקי ובין אלגוריתם הפיצוח של היריב (המשתמש הלא חוקי). מטרת המצפין היא למצוא אלגוריתם הצפנה כזה, שיבטיח את הפער הזה ובכך יבטיח את אי סבירותו של הפיצוח.

אחד האלגוריתמים שמבטיחים זאת היא הפונקציה החד כיוונית. נסביר מושג חדש זה ונקשור אותו למושגים שכבר הכרנו.

את כללי ההצפנה והפענוח אפשר לראות כפונקציות. אנו יודעים כבר כי פונקציה היא כלל, שקובע התאמה בין קבוצת מספרים אחת (למשל קבוצת המספרים שמייצגים את המסר המקורי), לקבוצת מספרים אחרת (למשל קבוצת המספרים שמייצגים את המסר המוצפן). לכן אפשר לקרוא לכללי ההצפנה והפענוח גם פונקציות ההצפנה והפענוח. כך למשל אפשר לומר, כי פונקצית ההצפנה הציבורית של בני (אלגוריתם ההצפנה ומפתח ההצפנה), צריכה להיות קלה להפעלה, אבל הפעלת פונקצית הפענוח (הפונקציה ההפוכה לפונקצית ההצפנה), צריכה להיות קשה מאוד, לכל אחד חוץ מאשר לבני שמכיר את הפונקציה ההפוכה.

**אם פונקציה היא קלה להפעלה, אבל הפונקציה ההפוכה לה כל כך מסובכת, עד שאפשר לומר שמעשית אי אפשר למצוא אותה, כי אז אנו קוראים לה פונקציה חד כיוונית.** אנו רוצים בעצם, שפונקצית ההצפנה תהיה פונקציה חד כיוונית. פונקציות חד כיווניות ממלאות תפקיד מרכזי בתורת ההצפנה. הן חשובות לבניית מערכות הצפנה אסימטריות וגם בהקשרים נוספים. קיימות הרבה פונקציות מתמטיות, שבאופן מעשי הן חד כיווניות, למרות, שעדיין אין אף פונקציה, שהחד כיווניות שלה גם הוכחה. אחת הדוגמאות של פונקציה חד כיוונית היא יצירת מספר כלשהו  $N$  על ידי כפל של מספרים ראשוניים נתונים  $p$  ו- $q$ . פעולה זו היא פשוטה ומיידית. מה תהיה הפונקציה ההפוכה? פירוק לגורמים של  $N$  ומציאת  $p$  ו- $q$ .



#### שאלה מספר 17

נתון המספר 1,040,257, פרקו אותו לשני גורמים ראשוניים.

אם לא הצלחתם בפירוק לגורמים, מה שסביר למדי, הנה דלת הסתרים: אחד משני הגורמים הוא 127, מהו הגורם השני?

זו כמובן דוגמה פשוטה יחסית, אבל כשמדובר במספרים ענקיים בני מאות ספרות החד כיוויות של הפונקציה משכנעת הרבה יותר. בהמשך נטפל בפונקציה זו ובשימושיה בהצפנה המודרנית ביתר פירוט. אם רוצים לבנות מערכת הצפנה אסימטרית, לא מספיק למצוא פונקציה חד כיוונית. כבר הזכרנו כי איננו רוצים שפונקצית ההצפנה של בני (שנסמן ב- $E_B$ ), תהיה חד כיוונית **מנקודת ראותו של בני**, כיוון שהוא צריך להיות מסוגל לפענח ביעילות את המסר שקבל. לכן לבני צריך להיות **מידע סודי** שיאפשר לו **ורק לו**, היפוך קל ומהיר של  $E_B$ .

למידע הסודי הזה יש הקוראים "**דלת סתרים**". אומרים, כי פונקציה היא חד כיוונית עם דלת סתרים, אם למרות שהיא חד כיוונית, אפשר למצוא את הפונקציה ההפוכה שלה, בעזרת מידע סודי, שהוא מעין דלת סתרים לפתרון הבעיה.

### 3.9 סיכום

עד כאן תארנו מערכת הצפנה **כזאת שהיינו רוצים לבנות**. נסכם בקיצור את תכונותיה:  
**מערכת הצפנה אסימטרית, שמבוססת על שני מפתחות שונים, מפתח פומבי (ידוע לכל) ומפתח פרטי (סודי), ידוע לבעליו בלבד. מערכת הצפנה שאבטחתה נשענת על פונקצית הצפנה חד כיוונית, בעלת סיבוכיות גבוהה. לכן, גם כשיש ליריב מידע על אלגוריתם ההצפנה ואפילו על המפתח (הפומבי), הסיבוכיות היא המונעת ממנו לגלות אלגוריתם יעיל לפיצוחה של ההצפנה.**  
בהמשך נתאר את שלבי הפיתוח והבניה של מערכת כזאת.

### 3.10 פתרונות

פתרון שאלה מס' 1:

| מספר ה"פגיונות" | מספר ה"בולים" | מספר ה"פיספוסים" |    |
|-----------------|---------------|------------------|----|
| 4               | 0             | 0                | 1  |
| 3               | 0             | 1                | 2  |
| 3               | 1             | 0                | 3  |
| 2               | 0             | 2                | 4  |
| 2               | 1             | 1                | 5  |
| 2               | 2             | 0                | 6  |
| 1               | 0             | 3                | 7  |
| 1               | 1             | 2                | 8  |
| 1               | 2             | 1                | 9  |
| 1               | 3             | 0                | 10 |
| 0               | 0             | 4                | 11 |
| 0               | 2             | 2                | 12 |
| 0               | 3             | 1                | 13 |
| 0               | 4             | 0                | 14 |

\* הערה: האפשרות של 0 פספוסים, 3 "בולים" ו- 1 "פגיעה" לא תיתכן.

פתרון שאלה מס' 2:

- א. פי 2
- ב. פי  $6^4$  כלומר, בריבוע.
- ג. פי  $2^4$  כלומר, פי 16.

פתרון שאלה מס' 3:

- א. מספר הצירופים האפשריים יגדל מ-  $6^n$  ל-  $(6^n)^2 = 6^{2n}$ . הוא יגדל פי  $6^n$ , כלומר בריבוע.
- ב. מספר הצירופים האפשריים יגדל מ-  $m^4$  ל-  $16m^4 = 2^4m^4 = (2m)^4$ , פי 16.

#### פתרון שאלה מס' 4:

הגדלת מספר הכדורים לבחירה משפיעה הרבה יותר על גידול מספר האפשרויות מאשר הגדלת מספר הצבעים מתוכם נבחרים הכדורים.

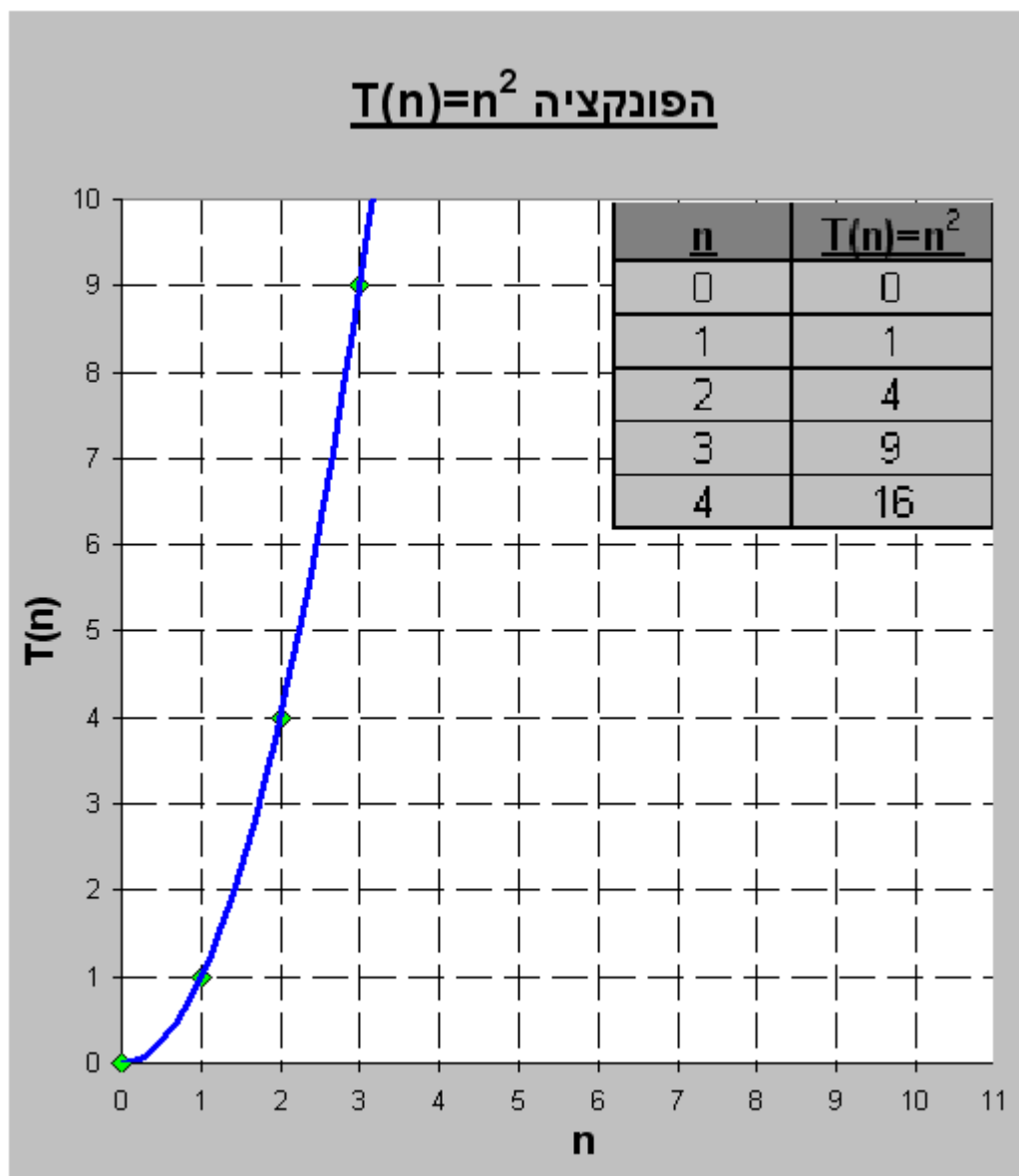
#### פתרון שאלה מס' 5:

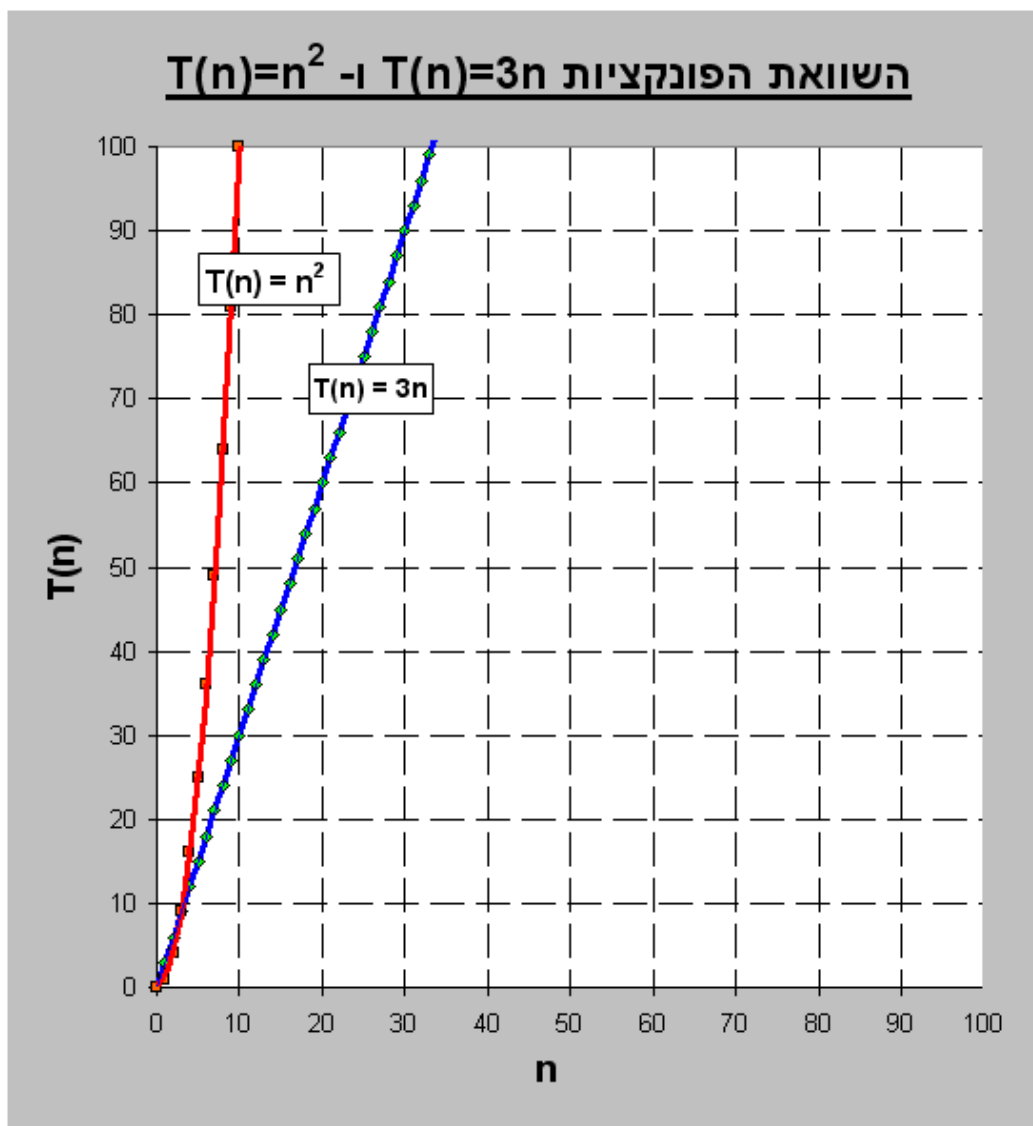
| $T(n)$ | $n = \text{מספר הביטים}$ |
|--------|--------------------------|
| 150    | 50                       |
| 300    | 100                      |
| 420    | 140                      |
| 900    | 300                      |
| 3,000  | 1,000                    |
| $3k$   | $k$                      |

#### פתרון שאלה מס' 6:

#### פתרון שאלה מס' 7:

| $T(n) = n^2$ | $n$   |
|--------------|-------|
| 2,500        | 50    |
| 3,600        | 60    |
| 10,000       | 100   |
| 90,000       | 300   |
| 1,000,000    | 1,000 |





ב. הפונקציה הריבועית גדלה בקצב גבוה יותר מהפונקציה הקווית.

**פתרון שאלה מס' 10:**

- א. חצוף, פצוח.
- ב. צרפת, תצרף.

**פתרון שאלה מס' 11:**

- א. מספר האנגרמות של מילה בת 4 אותיות שונות, כמספר התמורות של אותן אותיות,  $4!$  (כמה מצאתם אתם?).
- ב.  $k!$

### פתרון שאלה מס' 12:

- א. למילה בת 5 אותיות  $5! = 120$  אנגרמות אפשריות.  
ב. זמן החיפוש הבינרי של כל האנגרמות של מילה נתונה:  
 $45.6$  שניות  $= 0.0002 \cdot 19 \cdot 120$ , כשלושה רבעים של דקה.  
ג. החיפוש הקווי ימשך  $2 \cdot 10^{-4} \cdot 5 \cdot 10^5$  שניות  $= 0.0002 \cdot 500,000$ , שהם כמו שראינו  $100$  שניות.

### פתרון שאלה מס' 13:

### פתרון שאלה מס' 14:

החסם העליון של סיבוכיות ה-DES  $2^{56}$ ,

- א.  $2^{16} = 2^{56}/2^{40}$  הסיבוכיות קטנה פי  $2^{16}$ , פי  $65,500$  בקרוב, אך היא עדיין  $2^{40}$ , שהם בקירוב מיליון מיליונים  
ב.  $2^{36} = 2^{56}/2^{20}$  הסיבוכיות קטנה פי  $2^{36}$ , היא עדיין  $2^{20}$ , שהם בערך מיליון. משימת הפיצוח במקרה זה, עבור מחשב, שמבצע פעולה אחת ב-  $0.0002$  שניות, היא ריאלית. חשבו זאת.

### פתרון שאלה מס' 15:

### פתרון שאלה מס' 16:

- א. הגידול בפונקציה הקווית:  $f(10)-f(9)=1$   
הגידול של הפונקציה הריבועית:  $f(10)-f(9)=10^2-9^2=19$   
היחס ביניהם:  $19/1=19$   
ב. הגידול המעריכי:  $f(10)-f(9)=2^{10}-2^9=1024-512=512$ ,  
היחס בינו לבין הגידול הריבועי:  $512/19 \sim 27$   
ג.  $512/1=512$   
ד.  $f(10)-f(9)=10!-9!=3,628,800-362,880=3,265,920$   
היחס בין הגידול העצרתי לגידול הקווי:  $3,265,920/1=3,265,920$   
ה. היחס בין הגידול העצרתי לגידול המעריכי:  $3,265,920/512 \sim 60,000$

### פתרון שאלה מס' 17:

8191

## 4 איך מחליפים מידע סודי בערוצים פתוחים (גלויים)?

### 4.1 הקדמה

עד עכשיו תארנו בפרוט רב את תכונותיה של מערכת ההצפנה שאנו מנסים לפתח. כעת מתקרב רגע האמת. האם נצליח בבניה? האם אילנית (או כל אחד אחר) יכולה ליצור לעצמה מפתח שלה שיהיה פומבי, גלוי לכל? מפתח שבאמצעותו יכול כל מי שרוצה בכך, לשלוח אליה בערוצים פתוחים מידע סודי? איך מתגברים המשתמשים ברשת על בעיית ההתקשרות המקדימה? איך הם מתגברים על הבעיה, בת אלפי השנים, של כל המצפינים בשיטות הסימטריות? איך הם מגיעים להסכם מפתח בערוץ פתוח? איך מצליחים

#### המצפינים בשיטה האסימטרית להעביר מידע סודי בערוצים פתוחים?

איך הם מצליחים להעביר בביטחון, מפתח סודי לשותפי הסוד שלהם, כשההעברה מתבצעת בקווי תקשורת פתוחים ולא מאובטחים? אם הערוץ פתוח, הוא פתוח לכולם, גם ל"מאזי"(המאזינה, או כל מצותת אחר). ומה יקרה אם נתוני המפתח ייפלו לידיה של "מאזי"? המשתמשים מוכרחים להבטיח, שגם במקרה כזה היא לא תוכל לגלות שום מידע מנתונים אלה על המפתח עצמו. האם זה אפשרי?

הסיפור הקצר על "פלונית" ו"פלמוני", בתחילת החוברת, הוא משל לפתרון אפשרי אחד, לבעיה של העברת חפץ סודי בערוץ פתוח לכל. במשל הושגה המטרה על ידי שלוש "העברות" של "התיבה הנעולה" בין השולח והנמען. האם יש לכך נמשל בעולם הדיגיטלי? הנמשל לטבעת הוא המידע היקר והחיוני שאנו רוצים להעביר, הצורך להעביר מידע סודי בערוצים פתוחים. מהו הנמשל ל"נעילות" בעולם הדיגיטלי? הצפנות שיאפשרו לנו להעביר בביטחון מידע יקר.

אחד מפיתוחיה של ההצפנה האסימטרית, שנציג פה, מספק פתרון לבעיה זו. פתרון שיבטיח לבני יתרון על פני "מאזי" במצב שבו המפתח הסודי נשלח בערוץ פתוח לכל. (גם אם מאזי תתפוס את התיבה הנעולה אין היא יכולה לדעת דבר על המפתח). פתרון זה מתבסס על המושג החדש שכבר הכרנו, הסיבוכיות החישובית.

### 4.2 ההברקה של מרקל: העברת מפתח סודי בערוצים ציבוריים

עוד בהיותו סטודנט בברקלי בשנות ה-70 המוקדמות של המאה ה-20, תכנן רלף מרקל את מה שנחשב למבנה הראשון של שיטת ההצפנה האסימטרית. בשנת 1974, כשהיה עדיין סטודנט באוניברסיטת ברקלי, הגיש מרקל עבודה, שכותרתה הייתה: "תקשורת מאובטחת בערוצים לא מאובטחים" במילים אחרות: העברת מידע סודי בערוצים פתוחים. אבל הרעיון היה כנראה כל כך חדשני ומהפכני, עד שאפילו המרצה, שלו הוגשה העבודה, לא ירד לעומקה. מרקל נטש את האוניברסיטה והמשיך את עבודתו בדבקות, למרות הכישלון להציג את התוצאות כך שיובנו על ידי עמיתיו. ההברקה החדשנית של מרקל, הייתה אמורה לאפשר למשתמשים כמו בני ואילנית להחליף ביניהם מפתחות הצפנה סודיים בערוץ ציבורי. מה היה העיקרון שעליו התבסס מרקל?

הוא הניח מראש, ש"מאזי" מאזינה לקווי התקשורת של בני ואילנית ובתנאים אלה חשב על שיטה, שבה פענוח המסרים, שעוברים בין אילנית לבני, יהווה עבורם, בעיה בעלת סיבוכיות נמוכה, אבל בשביל "מאזי" (שאנו מניחים כי גם היא השיגה את המסרים המוצפנים), יהווה הפענוח בעיה, שהסיבוכיות של פתרונה הרבה יותר גדול. כתוצאה מכך יהיה פתרונה עתיר זמן.

**כיצד שולחת אילנית לבני, בערוץ פתוח לכל, מסר מוצפן סימטרית מבלי להחליף לפני כן מידע על המפתח הסודי?**

הנה כיצד זה מתבצע:

1. בני יוצר  $2^{20}$  (כמיליון) מפתחות אקראיים (נסמן את מספר המפתחות ב-  $n$ , כלומר  $n = 2^{20}$ ) כל מפתח הוא בעל 128 ביטים, שמתוכם הוא מגלה- 108 ביטים ומסתיר 20 ביטים. נסמן את המפתחות  $x_1, x_2, \dots, x_n$  השרטוט מתאר את המפתח  $x_i$ :

| $x_i$ המפתח ה- $i$             |                         |
|--------------------------------|-------------------------|
| $108 = \hat{x}_i$ ביטים גלויים | $20 = y_i$ ביטים נסתרים |

באמצעות כל אחד מן המפתחות הוא יוצר חידה, כך הוא יוצר כמיליון חידות ושולח אותן לאילנית. כל חידה שאילנית מקבלת היא במתכונת זוג סדור:

$$(108 \text{ ביטים גלויים, הצפנה סימטרית באמצעות המפתח } x_i) = (E_{x_i}(A), \hat{x}_i)$$

$A$  = הודעה מוסכמת וגלויה

$$E_{x_i} = \text{הצפנה של ההודעה המוסכמת באמצעות המפתח } x_i$$

החידה שמקבלת אילנית: "מצא את 20 הביטים החסרים". לכל חידה  $y_i$  שונה. זוהי חידה טובה, כי אילנית יכולה לדעת בביטחון האם הפתרון אליו הגיעה הוא נכון. היא יודעת זאת כיוון שהפענוח באמצעות המפתח שמצאה צריך לתת לה את ההודעה המוסכמת  $A$ .

זכרו, כיוון שהפתרון לחידה הוא מחרוזת בינארית של 20 ביטים, מספר הפתרונות האפשריים עבור  $y_i$  הוא  $2^{20}$ .

2. אילנית בוחרת באקראי את אחת החידות ומנסה לפצח אותה על ידי גילוי של 20 הביטים החסרים, שסימנם  $y_i$  כמו שכבר הזכרנו. אילנית

$$E_{\hat{x}_i y_i}(A) = E_{x_i}(A) \quad \text{מחפשת } y_i \text{ כזה, כך שיתקיים:}$$

$$E_{x_i} = \text{הצפנה סימטרית באמצעות המפתח } x_i$$

$$E_{x_i y_i} = \text{הצפנה סימטרית באמצעות המפתח } x_i y_i$$

לשם זה היא מבצעת חיפוש ממצה של המפתחות האפשריים (brute force attack). המשימה הזאת דורשת עבודה רבה אך היא בת ביצוע. אילנית צריכה לבדוק  $2^{20}$  מחרוזות אפשריות למציאת  $y_i$  שישמש אותה בשלב הבא. נזכור כי  $2^{20}$  הוא בדיוק גם מספר המפתחות  $x_i$  שבני בנה תחילה. מפני שמספר הפעולות המכסימלי שאילנית צריכה לבצע הוא כמספר המפתחות  $n$ . הסיבוכיות של פתרון הבעיה שאילנית צריכה לפתור היא מסדר  $n$ . נסמן זאת  $O(n)$ . זו בעייה שפתרונה הוא בעל סיבוכיות מסדר גודל קווי.

3. אילנית מסיימת את הפיצוח, כלומר - היא מגלה את 20 הביטים הנסתרים  $y_i$ , היא פצחה את החידה שבחירה.

כעת משימתה לשלוח לבני את המסר הסודי שלה  $(m)$ , באמצעות המפתח שזה עתה מצאה. היא שולחת לבני חידה חדשה.

היא שולחת לבני את הזוג הסדור:  $(E_{x_i}(B), E_{x_i}(m))$

$m$  = המסר הסודי של אילנית

$B$  = הודעה מוסכמת וגלויה

$E_{x_i}$  = הצפנה סימטרית באמצעות המפתח  $x_i$

$E_{x_{iyi}}$  = הצפנה סימטרית באמצעות המפתח  $\hat{X_iY_i}$

4. כעת גם לבני יש "חידה" שקבל מאילנית. איך יפתור אותה? ההודעה המוסכמת  $B$  ידועה לו וגם שאר המידע הדרוש לפתרון, בידיו. בני יבדוק ע"י חיפוש ממצה בין כל המפתחות שלו את המפתח  $x_i$  שאתו אילנית הצפינה את ההודעה המוסכמת  $B$  וגם את המסר  $m$ . מה הסיבוכיות של הבעיה של בני? גם הפעם  $O(n)$ .

**מאזי יכולה** לפצח את המערכת אבל העבודה שעליה להשקיע לשם כך הרבה יותר גדולה מעבודתם של בני ואילנית. פי כמה יותר גדולה? מה הסיבוכיות של פתרון הבעיה שלה? נבדוק זאת:

כדי לחלץ את המסר בשלב (3), על מאזי לבצע  $2^{20}$  ניסיונות פיצוח (כל המפתחות האפשריים), על כל אחת מ  $2^{20}$  ה"חידות" ששלח בני. כלומר, עליה לבצע  $2^{20} \times 2^{20} = 2^{40}$  ניסיונות פיצוח כדי לחלץ את המסר הסודי ששלחה אילנית לבני בערוץ פתוח. אפשר להסביר זאת גם באופן חזותי.

אפשר לסדר את כל ה"חידות" ששולח בני לאילנית בטבלה.  $n$  חידות ב-  $n$  מפתחות שונים. נדגים את המקרה  $n = 10$ . הטבלה תראה כמו בשרטוט בעמוד הבא:

| 10 חידות $y_i$ |   |   |   |   |   |   |   |   |   | 10 מפתחות הצפנה $x_i$ |
|----------------|---|---|---|---|---|---|---|---|---|-----------------------|
| 10             | 9 | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |                       |
|                |   |   | * |   |   |   |   |   |   | 1                     |
|                |   |   |   |   |   |   |   |   | * | 2                     |
|                |   |   |   |   | * |   |   |   |   | 3                     |
|                |   |   |   |   |   | * |   |   |   | 4                     |
|                |   |   |   |   |   |   |   | * |   | 5                     |
|                | * |   |   |   |   |   |   |   |   | 6                     |
|                |   |   |   | * |   |   |   |   |   | 7                     |
| *              |   |   |   |   |   |   |   |   |   | 8                     |
|                |   | * |   |   |   |   |   |   |   | 9                     |
|                |   |   |   |   |   |   | * |   |   | 10                    |

כל נקודה בטבלה מסמנת "חידה" מוצפנת. מספר החידה הוא מספר העמודה, בה היא נמצאת ומספר השורה הוא מפתח ההצפנה. כיוון שכל "חידה" הוצפנה במפתח אחר, כל "חידה" נמצאת בשורה שונה וכל הצפנה בעמודה שונה.

הטבלה מתארת חזותית את אוסף החידות המוצפנות, ששולח בני לאילנית. אילנית בוחרת חידה אחת (בעמודה מסוימת) ומנסה את כל המפתחות האפשריים (ממצה את כל העמודה). אילנית מבצעת מכסימום 10 בדיקות עד מציאת המפתח  $y_i$ .

אילנית שולחת לבני את המסר הסודי שלה מוצפן עם המפתח שחשפה ומסר ידוע אחר מוצפן עם מפתח החידה שבחרה  $x_i$  ( $x_i$  זכור הוא צרוף של  $\hat{x}_i$  גלוי ושל  $y_i$ ).

בני לא יודע איזה חידה בחרה אילנית. בידיו מסר ידוע מוצפן באחד מ 10 המפתחות  $x_i$  שלו. לכן בני צריך לבצע מכסימום 10 בדיקות עד מציאת החידה שבחרה אילנית. **בני יודע מהו המפתח  $y_i$  של כל חידה. זה היתרון של בני.** בעזרתו יפענח את הצופן ששלחה לו אילנית.

אולם, מאזי שהצליחה להשיג את המסר המוצפן, כמו בני - היא אינה יודעת באיזה חידה מדובר (באיזה עמודה בטבלה) אולם היא גם אינה מכירה את מפתחות ההצפנה של כל חידה (באיזו שורה בטבלה). לכן, כדי למצוא את המפתח שבעזרתו תוכל לפענח את הצופן שהשיגה, עליה לבדוק את כל ההצפנות האפשריות של כל החידות. כלומר, **עליה לבדוק את כל תאי הטבלה.** מאזי מבצעת מכסימום 100 בדיקות עד למציאת המפתח שיביא לפענוח.

אם נחזור לממדי המשימה במצב של  $2^{20}$  חידות, בלשון המתמטיקה אנו אומרים כי הסיבוכיות החישובית של פתרון הבעיה בפניה ניצבת אילנית היא  $2^{20}$  (כמיליון) ואילו הסיבוכיות החישובית של התקפתה של מאזי (הסיבוכיות של פתרון הבעיה **שלה**) היא ריבוע של הסיבוכיות של אילנית. סיבוכיות התקפתה של מאזי היא  $2^{40}$  (מיליון מיליונים).

במקרה הכללי :

אם הסיבוכיות החישובית של פתרון הבעיות של אילנית ובני היא  $O(n)$ , אז הסיבוכיות החישובית של פתרון בעייתה של מאזי היא  $O(n^2)$ . מאזי יודעת את נוסח שתי ההודעות הגלויות וגם כל המסרים המוצפנים גלויים בפניה, האם זה עוזר לה בפיצוח הצופן? האם זה מקטין את מספר המפתחות שעליה לבדוק? לא. זה לא עוזר לה לפצח את המסר המוצפן, כיוון שהקצאת המפתחות בשלב (1) הייתה אקראית לחלוטין. לכן היא נשארת עם העובדה המוצקה שערך הסיבוכיות החישובית של התקפותיה הוא הריבוע של ערך הסיבוכיות החישובית של יריביו.

(הערה: למען הדיוק, המספר המרבי של הבדיקות שהיא עשויה לבצע הוא  $n^2/4$ . הסיבה לכך היא שבכל בדיקת מפתח שמאזי מבצעת, הסיכוי שלה להצליח שווה לסיכוי שלה להיכשל ולכן אחרי  $n/2$  ניסיונות פיצוח סביר להניח שתצליח. אבל  $n^2/4 = (n/2)^2$  ולכן זהו מספר ניסיונות הפיצוח העומדים בפניה. אבל **סדר הגודל** של הסיבוכיות נשאר ריבועי וזה העיקר.

היתרון של  $n^2$  לעומת  $n$ , עשוי לספק בנסיבות מסוימות. למשל בדוגמה שהבאנו, אם אילנית ובני מסוגלים לבדוק עשרת אלפים מפתחות בשנייה (כוח חישוב של 1,544MB), אז תוך פחות משתי דקות (100 שניות), מסיים בני את הצפנת "חידותיו" ותוך פחות מ-4 דקות הוא גם מספיק לשלוח אותן. אם למאזי אותה יכולת חישובית, היא תזדקק ל-  $10^6 \times 10^2$  שניות (כיוון שמספר המפתחות שעליו לבדוק גדול פי מיליון). משימה זו תארך כשלוש שנים. כתוצאה מכך יכולים אילנית ובני לתקשר ביניהם באמצעות המפתח הסודי המבוקש, בעוד "מאזי" נאבקת לגלות מהו המפתח בו הם משתמשים. נראה שהשיטה של מרקל נחלה הצלחה.

בשיטה חדשנית זו, אילנית פתרה רק **חידה אחת**, ממיליון החידות ששלח לה בני, על ידי בדיקת **מיליון מפתחות**. כך מצאה את המפתח הסודי המשותף לה ולבני. מאזי אינה יודעת, **איזה חידה פתרה אילנית**. פריט המידע החיוני הזה, המוסתר ממאזי, מאלץ אותה לפתור **מיליון מיליונים** של חידות, משימה גדולה פי מיליון מזו של אילנית. אכן בעיה שפתרונה עתיר זמן, כמו שנוכחנו. בהמשך נכיר שיטות שונות להגדלת הסיבוכיות של הבעיות העומדות בפני היריב מחד והגדלת האבטחה של המערכת מאידך.



#### שאלה מספר 1:

כיצד מאפשרת שיטתו של מרקל לשלוח מסר מוצפן סימטרית ללא הסכם מפתח מוקדם? נסו לסכם בקצרה את העקרונות של שיטת מרקל.

החשיבות הגדולה ברעיונו המבריק של מרקל הייתה בהמצאת שיטה שאפשרה, **בפעם הראשונה, להעביר מידע סודי בערוצים פתוחים**. אבל לשיטה של מרקל מספר מגבלות.

#### 4.2.1 המגבלות של המצאת מרקל

להמצאתו של מרקל שלוש מגבלות עיקריות:

1. יחס הסיבוכיות ריבועי בלבד. פער הזמנים הנובע מכך (זמן הפיצוח), אינו מספיק. הוא לא נותן אבטחה מספקת אפילו בהווה. סביר להניח, שבעתיד, מחשבים חזקים יותר ותכנה יעילה יותר, יקצרו במאוד את זמן הפענוח. ההיסטוריה של ההצפנה רצופה בחידושים טכנולוגיים, שחיסלו יתרונות של הצפנות, שנראו אמינות ובטוחות, אך בדיעבד התברר שאמינותן הייתה זמנית בלבד כיוון שהתבססה על היכולות הטכנולוגיות, באותו זמן. לאור זה מעדיפים המצפינים יתרון גדול עוד יותר מן היתרון הריבועי. למשל, יתרון שיבטיח כאלף שנים של ניסיונות פיצוח למאזי, לעומת דקה של פענוח לאילנית. אחת הדרכים להשיג זאת היא להגדיל מאוד את מרחב החיפוש של מאזי. בני יכול לשלוח לאילנית הרבה יותר "חידות", אבל ראשית, הוא מוגבל על ידי המכשור בו הוא משתמש ושנית, הוא מחדד מגבלה נוספת, חוסר יעילות תקשורתית.
2. השיטה לוקה בחוסר יעילות תקשורתית, הנובעת מכך שהיא מעמיסה על הרשת המון מידע סרק, שכל מטרתו להסוות כמות זעירה של המידע שאותו בלבד מעונינים להעביר. בני משתמש רק במפתח אחד ממיליון, אבל מעמיס על הרשת את כל 999,999 המפתחות האחרים, שמסתירים אותו ומזרקים אחר כך.
3. מאזי יכולה לעבוד עם כמה מחשבים במקביל. על ידי כך תצמצם עוד יותר את נחיתותה. בשנים האחרונות התפתחו מאד יכולות הפיצוח על ידי צירוף משאבים חישוביים.

#### 4.3 סיכום ביניים

נסכם, מה השיג מרקל בהמצאתו? הוא יצר מצב בו לשותפי הסוד בני ואילנית יש בעיית פענוח שסדר הגודל של סיבוכיות פתרונה הוא נמוך ( $O(n)$ ), יחסית לסדר הגודל של סיבוכיות הפתרון של בעיית הפיצוח בפניה עומדת מאזי, ( $O(n^2)$ ).

במובן זה, כל שיטות ההצפנה האסימטרית עובדות בדרכים דומות. אפשר לומר כי לשותפי הסוד וליריבים יש אותה בעיה, אבל הסיבוכיות של פתרון הבעיה **שונה** לגבי השותפים ולגבי יריביהם. מציאת הפתרון על ידי השותפים היא בעלת סיבוכיות נמוכה (יחסית), אבל ליריביהם הסיבוכיות של הפיצוח גדולה מאוד ולכן פתרון הבעיה של המפצח עתיר זמן. הזמן הוא המכשול הגדול ביותר, שבפניו ניצב היריב. משימת המצפינים היא להגדיל את פערי הזמנים בין ההצפנה והפענוח. הם משיגים זאת על ידי תכנון מערכות הצפנה בהן סיבוכיות הפיצוח עולה בהרבה (בסדר גודל) על סיבוכיות ההצפנה.

### 5.1 הקדמה

בכל המפתחות, שפותחו לצורך הצפנה אסימטרית, נעשה שימוש בכלים מתמטיים דומים מאוד. לכן, לפני שנפנה לאלגוריתם מסוים, נעבור על מספר מושגי יסוד מתמטיים, שאת חלקם כבר הכרנו, אבל הפעם נעמיק את היכרותנו עמם. כבר טפלנו בהיקף מצומצם, ביסודות החשבון המודולרי ובהפכי כמושג בסיסי. כדי להתקדם בלימוד ההצפנה האסימטרית נצטרך להרחיב את ידיעותינו בתחומים אלה ובנושאים מתמטיים נוספים. לכך יוקדש הפרק הזה. בפרק שאחריו נחזור לעסוק בהצפנה ונראה, כיצד מיושמים הכלים המתמטיים האלה, לפיתוח הצפנה אסימטרית.

### 5.2 תכונת הזהות של פעולות מתמטיות

כל שיטות ההצפנה האסימטרית, שנמצאות בשימוש, מבוססות על התכונה המתמטית שנקראת **זהות**. למה הכוונה? הכל יודעים שאם נכפול מספר ב-1 תוצאת הכפל תהיה המספר עצמו. אנו קוראים לכך תכונת הזהות של הכפל, ולמספר 1 קוראים איבר הזהות של הכפל. אנו מכירים גם את תכונת הזהות של החיבור, כל מספר אם מוסיפים לו אפס, הסכום שמתקבל שווה למספר עצמו. אפס הוא איבר הזהות של החיבור. בהמשך נתרכז רק בתכונת הזהות הכפלית, כיוון שיש לה שימוש נרחב בשיטות ההצפנה האסימטרית. אנו מכירים תכונות אחדות הקשורות לתכונת הזהות של פעולת הכפל.

$$8 \times \frac{1}{8} = 1 \quad \text{אנו יודעים כי:}$$

כך למשל, אם נצא מן המספר 3, נכפול אותו קודם ב-8 (נקבל 24), אחר כך ב- $\frac{1}{8}$ , נקבל שוב את המספר ממנו התחלנו, 3. אנו אומרים כי  $\frac{1}{8}$  ו-8 הם הפכיים לגבי הכפל כיוון שמכפלתם שווה ל-1. בשביל אנשי ההצפנה הדוגמה הזאת יותר מדי פשוטה, אבל עצם ה"תחבולה" של שימוש בהפכיים הכפליים אהובה מאד עליהם.

השימוש בהפכיים כפליים פותח אפשרויות הצפנה רבות ומרתקות. אם נוכל "לכפול" את המסר, שאותו אנו רוצים להצפין, ב-1, כי אז תכונת הזהות הכפלית מבטיחה, שהערך שנקבל יהיה זהה לערכו של המסר המקורי. ומה יקרה אם נבצע זאת בשני שלבים? אם נצליח לפצל את הכפל ב-1 לשני שלבים, למשל כפל ב-8 בשלב הראשון וכפל ב- $\frac{1}{8}$  בשלב השני? בדרך זו אפשר להסוות את המספר המקורי (להצפין את המסר), על ידי הכפלתו בשלב הראשון באחד מן המספרים, ולהגיע חזרה למספר המקורי (לפענח את המסר), על ידי הכפלתו, בשלב השני, בהפכי של הכפל בשלב הראשון.

בניח למשל שלרשותה של אילנית שני מפתחות, 8 ו-  $\frac{1}{8}$  והיא היחידה עלי אדמות שיודעת כי  $\frac{1}{8}$  הוא ההפכי הכפלי של 8. במקרה כזה היא יכולה להכריז בביטחון מלא כי אלגוריתם ההצפנה הוא כפל ו"המפתח הפומבי" שלה הוא כפל ב- 8. אם בני רוצה לשלוח את המסר 5,000 הוא מצפין אותו במפתח הפומבי שפרסמה אילנית ושולח לה  $40,000 = (5,000 \times 8)$ . אילנית שרק היא יודעת, כאמור, מהו ההפכי הכפלי של המפתח הציבורי שלה, כופלת  $\frac{1}{8} \times 40,000$  ומקבלת את המסר המקורי של בני. מובן מאליו שרבים יודעים מהו ההפכי הכפלי של 8 והדוגמה ניתנה רק כדי להסביר את העיקרון. מפתח קצת יותר מסובך עשוי להיות למשל, זוג המספרים:  $\frac{2}{3}$ ,  $\frac{3}{2}$ .

## שאלה מספר 1

השלימו את הטבלה:

| זוג המפתחות<br>(ציבורי פרטי) | המסר | מפתח ההצפנה<br>(המפתח הציבורי) | המסר המוצפן | מפתח הפענוח<br>(המפתח הפרטי) | פענוח המסר<br>המוצפן |
|------------------------------|------|--------------------------------|-------------|------------------------------|----------------------|
| $8, \frac{1}{8}$             | 333  | 8                              |             | $\frac{1}{8}$                |                      |
| $\frac{3}{2}, \frac{2}{3}$   |      | $\frac{3}{2}$                  | 148,149     | $\frac{2}{3}$                |                      |

כמו שכבר אמרנו, זוהי כמובן דוגמה פשוטה שבפשוטות, מטרתה רק להמחיש את העיקרון של זוגות הפכיים ואפשרויות השימוש בהם. כמובן שבעולם המעשה זה לחלוטין אינו מספיק. המצפינים זקוקים למשהו הרבה יותר מסובך וגם הרבה יותר בטוח, שאותו נכיר בהמשך.

## 5.3 מספרים הפכיים ופעולות הפוכות

בהצפנה אנו מבצעים פעולה כלשהי, זוהי פעולת ההצפנה. המפענח צריך לבצע פעולה הפוכה מזו שביצע המצפין, כדי לבטל את ההצפנה (לפענח), המושג המתמטי הקשור לביטול הפעולה הראשונית הוא מושג ההפכי. אנו מכירים פעולות הפוכות זו לזו. ביחס לפעולת חשבון מסוימת, שהפעלת האחת מבטלת את השפעת ההפעלה של האחרת ומחזירה אותנו למצב ההתחלתי. למשל, חילוק וכפל של מספר הן פעולות הפוכות זו לזו:

$$5 \cdot 2 = 10, \quad 10 : 2 = 5$$



## שאלה מספר 2

מהי הפעולה ההפוכה:

- א. לחיסור
- ב. לחילוק
- ג. לחזקה במעריך 2?

אנו מכירים גם **מספרים הפכיים**, אלה זוגות של מספרים, שפעולת החשבון עם האחד, מבטלת את אותה פעולת החשבון עם האחר. למשל 2 ו-  $\frac{1}{2}$  הם הפכיים ביחס לכפל (הפכיים כפליים), לדוגמה:

$$5 \cdot 2 = 10 \quad 10 \cdot \frac{1}{2} = 5$$

כשמספרים הפכיים פועלים זה על זה, התוצאה המתקבלת היא איבר הזהות של הפעולה, למשל:

$$4 + (-4) = 0$$

$$\frac{2}{5} \cdot \frac{5}{2} = 1$$

כפי שהדוגמאות מראות, אם רוצים לחזור למספר המקורי לאחר שמבצעים עליו פעולה מסוימת עם מספר מסוים, אפשר לבצע זאת באחת משתי הדרכים:

**לבצע על התוצאה פעולה הפוכה עם אותו מספר שהפעלנו על המספר המקורי בנקודת ההתחלה לבצע את אותה פעולה שבצענו, אבל עם המספר ההפכי.**

כל זה פשוט למדי כשמדובר במספרים המוכרים ובפעולות המוכרות. למשל, אם נחליף את המילה "פעולה" במילה "חיבור" (+) כי אז הפעולה ההפכית היא "חיסור" (-). זה עדיין פשוט. אבל נניח שאתם יוצאים לטיול, שנקודת ההתחלה שלו היא "רחוב הרצל פינת רחוב בלפור". ההוראות הן "לכו מערבה" (זו הפעולה), "50 מטר" (זו הכמות). נניח שהתוצאה היא "רחוב הרצל פינת רחוב אחה"ע". מה תהיה **הפעולה ההפוכה**? זו שתחזיר אתכם לנקודת ההתחלה? התשובה היא, "לכו מזרחה". באיזה כמות? **באותה כמות**, "50 מטר". אבל יש עוד אפשרות לחזור לנקודת ההתחלה.

צריך לעשות את אותה הפעולה עם המספר (הכמות) ההפכי(ת). האם זה אפשרי? אנו יודעים כי במקרה זה הפעולה נשארת ללא שינוי: "ללכת מערבה". האם אפשר לצאת מנקודה כלשהי, ללכת מערבה, ולחזור בסוף המסע לנקודת ההתחלה? התשובה היא כן, בהחלט, כיוון שהארץ היא כדור, צריך פשוט ללכת וללכת (ולנסוע ולשוט ולטוס), כל הזמן מערבה, על קו הרוחב של "רחוב הרצל פינת רחוב אחה"ע". בסופו של המסע, לאחר שנקיף את כדור הארץ, באותו קו רחב (לאחר שעברנו דרך קטנה ב- 50 מטר מאורכו של קו הרוחב), נגיע עייפים אך מרוצים להרצל פינת בלפור.

הכמות ההפכית ל- 50 מטר בפעולה ללכת מערבה היא היקף כדור הארץ (באותו קו רוחב) פחות 50 מטר. זו אמנם בחירה מוזרה אבל מדגימה יפה מקרה של כמות הפכית. להזכירכם, מגלן עשה זאת כבר בשנת 1522, כשהקיף את כדור הארץ בספינתו והוא אינו היחיד.



### שאלה מספר 3

באיזה מקום על פני כדור הארץ אפשר ללכת קילומטר אחד בכיוון דרום, קילומטר אחד בכיוון מערב, קילומטר אחד בכיוון צפון ולהגיע בסוף המסע לנקודת המוצא?

### 5.3.1 הפכיים של הצפנה

גם בהצפנה אנו עוסקים בפעולות הפוכות זו לזו ובמספרים הפכיים זה לזה. שיטות ההצפנה בעזרת מפתח סימטרי משתמשות בדרך כלל לצורך פענוח בפעולות הפוכות. למשל במפתח הסימטרי DES פעולות הפענוח זהות לפעולות ההצפנה, רק סדר הפעולות בפענוח הפוך לסדר בהצפנה. אולם שיטות ההצפנה האסימטרית (הצפנה בעזרת מפתח ציבורי ופענוח במפתח פרטי), משתמשות לצורך הפענוח במספרים הפכיים. כבר למדנו שכל שיטת הצפנה כוללת שני מרכיבים:

\* הפעולה – האלגוריתם

\* הכמות לביצוע הפעולה (המספר) - המפתח



### שאלה מספר 4

נתונה נוסחת ההצפנה באלגוריתם של הזזה:  $C=P+b$

(המסר  $P$ , המסר המוצפן  $C$ , ההזזה  $b$ )

א. מה תהיה נוסחת הפענוח?

ב. מהו זוג הפעולות ההפוכות במקרה זה?

#### 5.4 חשבון מודולרי, או, העיקר מה שנשאר.

רוב שיטות ההצפנה האסימטריות, כולל ה-RSA, שהיא כאמור הנפוצה ביותר, מתבססות על חשבון מודולרי, אתו כבר עשינו היכרות ראשונה. החשבון המודולרי מסייע בבניית בעיות בעלות סיבוכיות גבוהה. בסעיף זה נראה כיצד. אבל לפני כן נחזור ונזכר בחלק מתכונות החשבון המודולרי.

למשל, כשכותבים מספר מסוים, נניח 13, במודולים שונים, יתכן שתתקבל אותה תוצאה, למרות שמדובר

|                |                 |
|----------------|-----------------|
| 13 mod 5 = 3   | במודולים שונים: |
| 13 mod 10 = 3  | וגם             |
| 13 mod 2 = 1   | למשל            |
| 13 mod 4 = 1   | אך גם           |
| 13 mod 12 = 1  | וגם             |
| 13 mod 13 = 0  |                 |
| 13 mod 14 = 13 |                 |
| 13 mod 15 = 13 |                 |



#### שאלה מספר 5

כתבו את המספר 19 במודולים שונים: 5 מודולים קטנים מ-19, מודולו 19, ו-5 מודולים גדולים מ-19.

כאשר רושמים מספרים שונים באותו מודול יתכן שיתקבלו תוצאות שוות, למשל:

$$\begin{aligned}17 \bmod 10 &= 7 \\57 \bmod 10 &= 7 \\297 \bmod 10 &= 7 \\3287 \bmod 10 &= 7 \\456,237 \bmod 10 &= 7 \\7,247 \bmod 10 &= 7\end{aligned}$$

### שאלה מספר 6

פתרו את התרגילים:

$$1 \bmod 5 =$$

$$16 \bmod 5 =$$

$$31 \bmod 5 =$$

$$106 \bmod 5 =$$

$$1006 \bmod 5 =$$

$$120,001 \bmod 5 =$$

בשאלות 6, 5, 4 בכל המקרים שבדקנו, קבלנו תמיד תשובה **יחידה וקלה לחישוב**. אבל מה היא התשובה לשאלה: איזה מספר מודולו 10 שווה 3? כמה תשובות יש לה? 13 הוא תשובה אפשרית? ו-23? ו-1233? אנחנו רואים, שכל מספר שלם, שמסתיים ב-3 הוא תשובה לשאלה, איזה מספר מודולו 10 שווה 3. במילים אחרות, לשאלה זו תשובות רבות. תכונה זו של החשבון המודולרי הביאה לשימוש הנרחב בו לבניית פונקציות בעלות סיבוכיות גבוהה וסייעה בתכנון אלגוריתמים יעילים. בהצפנה משתמשים הרבה בצירוף של חשבון מודולרי והופכיים כפליים.



### שאלה מספר 7

- א. מה מספר השאריות האפשריות במודול 10?
- ב. מה מספר השאריות האפשריות במודול n?
- ג. מה אפשר ללמוד מכך שהשארית 0?

## 5.5 חשבון מודולרי כחשבון מעגלי

המודול, כמו שכבר ראינו, הוא מעין רף עליון. התוצאה הסופית של חישוב במודול מסוים אינה יכולה להיות יותר גדולה מן המודול. לכן כשמגיעים למודול מתחילים למנות מן ההתחלה. נזכיר כי השעון הוא דוגמה טובה לחשבון מודולרי. כשמגיעים ל-12 מתחילים את מניין השעות מההתחלה. החשבון המודולרי, המשמש בבניית מערכות הצפנה אסימטריות, דומה לזה של השעון, אבל אינו זהה לו. ההבדל החשוב הוא שבהצפנה מתחילים את המנייה מ-0 ולא מ-1 (כמו בחשבון השעון) והערך המקסימלי שאפשר להגיע אליו, קטן ב-1 מערך המודול (למשל במודול 12 התוצאה המקסימלית היא 11 ולא 12, כמו בחשבון השעון). בשני המקרים יש אותו מספר מספרים: 12 במקרה של השעון, 7 במקרה של ימי השבוע. ההבדל הוא רק בשמות שלהם: 0-11 במקום 1-12, בחשבון השעון. 0-6 במקום 1-7, בחשבון ימי השבוע. בחשבון מודולרי התוצאה הסופית היא תמיד מספר שלם חיובי. אין שברים פשוטים ואין נקודה עשרונית.

מספר שלילי עשוי להתקבל רק כתוצאת ביניים. אבל בתוצאה הסופית, רק מספרים שלמים חיוביים וקטנים מהמודול הם תקפים.

למשל, נניח שבחרנו במודול 11, במקרה כזה אנו רשאים להשתמש רק במספרים מ-0 עד 10 כתשומה. בנוסף לכך גם כל התפוקות יהיו מספרים בין 0 ל-10 (הכוונה היא לתוצאה הסופית. תוצאות ביניים זמניות עשויות להיות גדולות מהמודול או גם שליליות) קל ביותר להבין זאת אם מדמים חשבון מודולרי לחשבון מעגלי, למשל:

$$9+5 = 14 \quad \text{אם בחשבון "רגיל"}$$

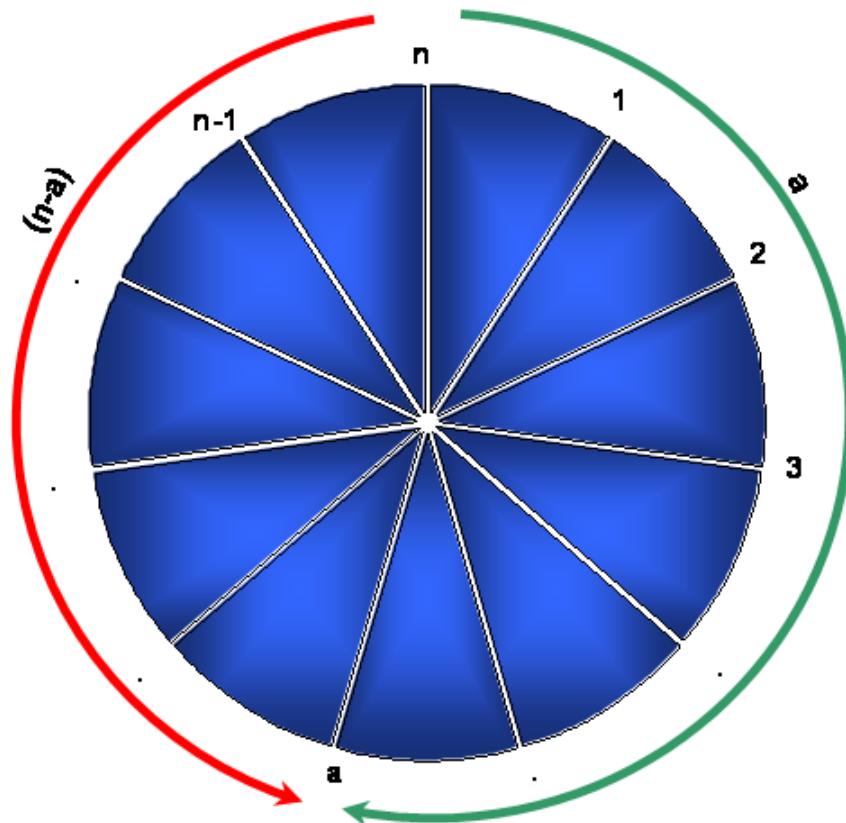
$$(9+5) \bmod 11 = 3 \quad \text{אז בחשבון מודולרי מודול 11}$$

אפשר גם, לחשב את התוצאה ה"לא מודולרית" ולבצע את מספר הצעדים המתאים לפי העיגול. למשל בכפל:

$$6*3 = 18 \quad \text{אם בחשבון "רגיל"}$$

$$(6*3) \bmod 11 = 7 \quad \text{אזי בחשבון מודולרי במודול 11}$$

$$a \bmod n = -(n-a) \bmod n$$



אנו יודעים כי לאורך מעגל אפשר לנוע בשני כיוונים. לכן כשנמצאים בנקודת הראשית, אפשר להגיע לכל נקודה על פני המעגל בשתי דרכים: בכיוון השעון ובכיוון הנגדי. עובדה זו מיוצגת על ידי הביטוי האלגברי:

$$a \bmod n = -(n-a) \bmod n$$

אלה שני תאורים חלופיים לאותה נקודה על פני מעגל שהיקפו שווה לערך המודול. תכונה זו עשויה להקל על החישובים המודולריים, כפי שנינוכח בהמשך.

דוגמה:

$$10 \bmod 11 = -1 \bmod 11$$

$$9 \bmod 12 = -3 \bmod 12$$

ומה לגבי החישוב של חזקות מודולריות? למשל, כמה הם  $7^8 \bmod 11$ ?

7 בחזקת 8 זוהי מכפלה שיש בה 8 גורמים, שכולם 7.

$$7^8 = 7 * 7 * 7 * 7 * 7 * 7 * 7 * 7$$

$$7^8 = 5,764,801$$

אם אנחנו צמודים לראיה המעגלית של החשבון המודולרי, אז כדי לחשב  $7^8 \bmod 11$  צריך להתחיל ב- 0 ולבצע 5,764,801 צעדים במעגל, שהיקפו 11 צעדים. כל הקפה דינה כ- 11 צעדים. אחרי הקפה אחת חוזרים ל- 0 ומספר הצעדים שנותרו:  $5,764,801 - 11 = 5,764,790$  וממשיכים במסע עוד סיבוב ועוד ועוד... עד תום המסע המפרך. כדי למצוא כמה סיבובים השלמנו כשהגענו לסוף המסע צריך לחשב כמה הם:  $7^8 \bmod 11$

$$7^8 = 5,764,801$$

$$5,764,801 : 11 = 542,072$$

שארית החילוק היא 9 וזו גם התשובה הסופית:  $7^8 \bmod 11 = 9$ .

**הכלל יכול, אם כן, להיות: חשבו את התוצאה הלא מודולרית של הכפל (החזקה), חלקו אותה במודול ושארית החילוק היא התשובה המודולרית.**

בהמשך נראה כיצד אפשר לקצר חישובים מייגעים כמו אלה, בעזרת החשבון המודולרי.

## 5.6 כפל מודולרי

**בכפל מודולרי, כלומר כפל במודול נתון, מספרים הפכיים, הם שני מספרים שמכפלתם שווה ל-1 במודול הנתון.** כבר הכרנו אותם בחוברת הקודמת. כעת ברור לנו מדוע המספרים, שהם בעלי התכונה הזו, הם בעלי חשיבות רבה אצל העוסקים בהצפנה. זוג של מספרים הפכיים עשוי לשמש כזוג מפתחות. כפל מודולרי באחד מהם מצפין וכפל בהפכי שלו באותו מודול, מפענח.

### 5.6.1 הפכיים (כפליים) מודולריים.

חישוב ההפכי הכפלי בכפל מודולרי הוא יותר בעייתי מחישוב ההפכי הכפלי בכפל הרגיל. נשווה את חישוב ההפכי הפשוט, של 8 למשל, לחישוב ההפכי המודולרי של 8, במודול 11, שאותו יותר מסובך לחשב.

| חישוב הפכי בחשבון "רגיל"<br>(השימוש בשברים מותר) | חישוב הפכי בחשבון מודולרי<br>(השימוש בשברים אסור) |
|--------------------------------------------------|---------------------------------------------------|
| $8 * ? = 1$                                      | $(8 * ?) \bmod 11 = 1$                            |
| $? = 1/8$                                        | $? = 7$                                           |
| $8 * 1/8 = 1$                                    | $(8 * 7) \bmod 11 = 1$                            |

| <u>כפל בהפכיים פשוטים</u> | <u>כפל בהפכיים מודולריים</u>       |
|---------------------------|------------------------------------|
| $4 \cdot 8 \cdot 1/8 = 4$ | $(4 \cdot 8 \cdot 7) \bmod 11 = 4$ |
| ובפירוט: $4 \cdot 8 = 32$ | $4 \cdot 8 \cdot 7 = 224$          |
| $32 \cdot 1/8 = 4$        | $224 \bmod 11 = 4$                 |

אפשר לסכם כי לכל פעולה מתאימים זוגות המספרים ההפכיים שלה. בכפל רגיל (לא מודולרי), אם המספר הוא  $n$ , ההפכי הכפלי שלו הוא  $1/n$ . ב"ללכת מערבה" מרחק מסוים, המספר ההפכי הוא שארית המרחק סביב כדור הארץ, על פני אותו קו רוחב. עתה הכרנו את ההפכי של הכפל המודולרי. **ההפכי הכפלי של מספר  $x$ , במודול  $n$ , הוא  $y$ , אם  $(x \cdot y) \bmod n = 1$**



### שאלה מספר 8

בדקו האם 15 הוא ההפכי הכפלי של  $3 \bmod 22$ .



### שאלה מספר 9

בנו את תמורת ההצפנה של הא"ב העברי, לפי הנוסחה:  $C = (5P) \bmod 22$



### שאלה מספר 10

- בנו את טבלת הכפל מודולו 22.
- מצאו את ההפכי הכפלי של  $5 \bmod 22$  ורשמו את תמורת הפענוח לתמורת ההצפנה שבשאלה.

בפרק 2 תארנו בפירוט רב את שיטת ההצפנה שאנו מעונינים לפתח. נוכחנו בתפקיד החשוב שיש לסיבוכיות הפיצוח של ההצפנה, כאשר בונים את ההצפנה. ראינו גם, כי החשבון המודולרי עשוי לסייע בכך, על ידי שימוש בהפכיים כפליים. בסעיף זה נטפל בהרחבה נוספת של מכפלה המודולרית.

כיצד מתקבלת מכפלה מודולרית? למשל, כיצד מקבלים מכפלה של מספר מודולו 10? מבצעים את הכפל כרגיל. אם תוצאת הכפל קטנה מ-10 היא נרשמת כ"מכפלה רגילה". למשל:  $9 = 3 * 3$ . אבל אם התוצאה שווה או גדולה מ-10, מחלקים אותה ב-10 ורשמים רק את השארית. למשל:

$$3*4 = 12$$

$$12 \bmod 10 = 2$$

טבלת כפל מודולרי (mod 10)

| X mod 10 | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
|----------|---|---|---|---|---|---|---|---|---|---|
| 0        | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 1        | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
| 2        | 0 | 2 | 4 | 6 | 8 | 0 | 2 | 4 | 6 | 8 |
| 3        | 0 | 3 | 6 | 9 | 2 | 5 | 8 | 1 | 4 | 7 |
| 4        | 0 | 4 | 8 | 2 | 6 | 0 | 4 | 8 | 2 | 6 |
| 5        | 0 | 5 | 0 | 5 | 0 | 5 | 0 | 5 | 0 | 5 |
| 6        | 0 | 6 | 2 | 8 | 4 | 0 | 6 | 2 | 8 | 4 |
| 7        | 0 | 7 | 4 | 1 | 8 | 5 | 2 | 9 | 6 | 3 |
| 8        | 0 | 8 | 6 | 4 | 2 | 0 | 8 | 6 | 4 | 2 |
| 9        | 0 | 9 | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |

נתבונן בטבלת הכפל במודול 10. מה אפשר ללמוד מן הטבלה?

איזה שורות בטבלה הן תמורות של המספרים מ-1 עד 9? מה מאפיין את המספר הראשון משמאל בכל שורה כזו? האם יש לו ול-10 מחלקים משותפים?

איזה שורות בטבלה אינן תמורות של המספרים האלה? מה מאפיין את המספר הראשון משמאל בכל שורה כזו? האם יש לו ול-10 מחלקים משותפים?

כל משבצת בטבלה שייכת לעמודה מסוימת ולשורה מסוימת. בכל משבצת רשומה המכפלה המודולרית של המספר העמוד בראש השורה למספר שנמצא בראש העמודה. ומה אם מכפלה זו היא 1? במשבצות בהן רשום המספר 1, המשמעות היא, שזוג המחלקים, שיצרו אותה, הם הפכיים. לכן אפשר לגלות את הזוגות ההפכיים על ידי הופעתו של המספר 1 בטבלה. היכן רשום בתוך הטבלה המספר 1? הוא מופיע בטבלה ארבע פעמים:

במשבצת המשותפת לשורה השניה ולעמודה הראשונה  $(1 \times 1) \bmod 10 = 1$

במשבצת המשותפת לשורה התחתונה ולעמודה הימנית  $(9 \times 9) \bmod 10 = 1$

במשבצת המשותפת לשורה השמינית ולעמודה השלישית  $(7 \times 3) \bmod 10 = 1$

במשבצת המשותפת לשורה הרביעית ולעמודה השביעית  $(3 \times 7) \bmod 10 = 1$

**כל זוג מספרים שמכפלתו המודולרית היא 1, הוא זוג של מספרים הפכיים.** האם כולם מתאימים לשמש כמפתחות הצפנה ופענוח? איזה אינם מתאימים? מדוע?

מן הטבלה אנו רואים כי המספרים 3 ו-7, הם הפכיים כפליים במודול 10. לכן הם מתאימים לשמש כזוג מפתחות במודול זה: האחד להצפנה השני לפענוח.

מה לגבי הזוגות האחרים  $(1 \times 1, 9 \times 9)$ , האם הם מתאימים לכך? חשבו מדוע. נמקו.

בסעיף קודם נוכחנו כי כשמצפינים על ידי כפל מודולרי במספר מסוים, מתבצע הפענוח על ידי כפל בהפכי הכפלי המודולרי של אותו מספר. עכשיו מצאנו גם שיטה לגילוי זוגות של הפכיים כפליים מודולריים. היא אולי קצת מסורבלת. אבל בינתיים, כל עוד אנחנו עוסקים במספרים לא גדולים, יש לנו דרך למצוא זוגות הפכיים במודולים בהם אנו עובדים.

## שאלה מספר 11

השלימו את לוח הכפל במודול 11

| X mod 11 | 1 | 2 | 3 | 4 | 5  | 6 | 7  | 8  | 9  | 10 |
|----------|---|---|---|---|----|---|----|----|----|----|
| 0        | 0 | 0 | 0 | 0 | 0  | 0 | 0  | 0  | 0  | 0  |
| 1        | 1 | 2 | 3 | 4 | 5  | 6 | 7  | 8  | 9  | 10 |
| 2        |   | 4 | 6 | 8 | 10 | 1 | 3  | 5  | 7  | 9  |
| 3        |   |   | 9 | 1 | 4  | 7 | 10 | 2  | 5  | 8  |
| 4        |   |   |   | 5 | 9  | 2 | 6  | 10 | 3  | 7  |
| 5        |   |   |   |   | 3  | 8 | 2  | 7  | 1  | 6  |
| 6        |   |   |   |   |    | 3 | 9  | 4  | 10 | 5  |
| 7        |   |   |   |   |    |   | 5  | 1  | 8  | 4  |
| 8        |   |   |   |   |    |   |    | 9  | 6  | 3  |
| 9        |   |   |   |   |    |   |    |    | 4  | 2  |
| 10       |   |   |   |   |    |   |    |    |    | 1  |



### שאלה מספר 12

סמנו בטבלה של שאלה 11 את כל ה-1ים, ורשמו את זוגות ההפכיים המופיעים בטבלה.  
האם הבחנתם בסימטריה מסוימת?

בטבלה מוצגת סדרת מספרים המוכפלת בזוג הפכיים כפליים ב-10 mod, שכבר הספקנו להכיר. בני הזוג האלה הם 3 ו-7. זכרו, כפל של כל מספר ב-10 mod  $(3 \cdot 7)$ , זהה לכפל שלו ב-1.

זהות כפליית ב-10 mod

| X | $X \cdot 3 \cdot 7 = x \cdot 21$ | $(x \cdot 21) \bmod 10$ |
|---|----------------------------------|-------------------------|
| 0 | 0                                | 0                       |
| 1 | 21                               | 1                       |
| 2 | 42                               | 2                       |
| 3 | 63                               | 3                       |
| 4 | 84                               | 4                       |
| 5 | 105                              | 5                       |
| 6 | 126                              | 1                       |
| 7 | 147                              | 7                       |
| 8 | 168                              | 8                       |
| 9 | 189                              | 9                       |



### שאלה מספר 13

בחרו זוג הפכי מן הטבלה בשאלה 11 ורשמו את טבלת הזהות הכפלית ב-11 mod

### 5.6.2 השימוש בהפכיים מודולריים להצפנה

כאמור, השימוש בזוג מספרים הפכיים מודולריים, זוהי תחבולה שכיחה, בה נוקטים העוסקים בהצפנה בימינו. לצורך ההדגמה נסתפק במספרים קטנים שהחישובים הכרוכים בהם פשוטים. אבל אפשר כמובן לבחור זוגות הפכיים, הרבה יותר קשים לגילוי מ-7 ו-3, או מהזוג שבחרתם בשאלה 12. בכל מקרה, כיוון שמספר המודולים האפשריים הוא כמספר המספרים הטבעיים (השלמים החיוביים), מספר המודולים הוא אינסופי. מספר הזוגות ההפכיים בכל מודול הוא אמנם סופי, אבל בסך הכל מספר הזוגות ההפכיים, בכל אינסוף המודולים, גם הוא אינסופי. וכך המצפינים מסוגלים לבחור זוג כזה, שאם אין יודעים איזה מספרים יצרו אותו (כמו 7 ו-3 שיצרו את 21), קשה מאד לגלות אותם. בהמשך נחלק את תהליך התקשורת המוצפנת לשני שלבים, ונראה כיצד יוצרים מפתח פרטי ומפתח ציבורי. נשתמש לכך בזוג הפכיים כפליים במודול שנבחר. אפשר, כמובן לבחור מספרים יותר גדולים מאלה שבדוגמה.

קודם השתמשנו ב-  $21 = (3 \cdot 7) \bmod 10$ , כיוון שאלה מספרים קלים לחישוב. בשאלה מספר 5 התבקשתם לבדוק את מספר התוצאות (השאריות) האפשריות במודולים שונים. למשל, כששתמשים במודול 10, התשובות מוגבלות לערכים 0-9 בלבד (כל השאריות האפשריות בחילוק ב-10). למודולים גדולים יותר, בעיקר אם הם ראשוניים, יש גם יותר זוגות הפכיים וגם יותר תוצאות אפשריות. לכן מעדיפים המצפינים מספרים גדולים יותר. (למשל אלגוריתם ה-RSA משתמש במודולים בני יותר מ-200 ספרות, כדי להגדיל את הסיבוכיות ולעשות את החיפוש עוד יותר מתסכל, עבור כל מי שאינו יודע מהם מספרי התחבולה). בהדגמה שלנו נשתמש במספרים לא כל כך גדולים. נסתפק במודולים יותר קטנים. גם הם מספיק גדולים להדגמת התחבולות המתמטיות של המפתח הציבורי ועדיין יהיה לנו קל יחסית לעבוד אתם.

### 5.6.3 איזה מספר מתאים לשמש כמפתח הצפנה?

האם כל מספר יכול לשמש כמפתח הצפנה (כיוצר תמורה), על ידי כפל מודולרי? בשאלות 7-9, ראינו שגם 3 וגם 5 התאימו לכך במודול 22. נבדוק האם המספר 11 למשל, מתאים לשמש כמפתח הצפנה במודול זה.

נוסחת ההצפנה:  $C = 11P \bmod 22$

נציב את ערכי המסר המקורי ונכפול:  $(0 \times 11) \bmod 22 = 0$

$$(1 \times 11) \bmod 22 = 11$$

$$(2 \times 11) \bmod 22 = 0$$

$$(3 \times 11) \bmod 22 = 11$$

המשיכו לבדוק 5 מקרים נוספים. איזה תוצאות קבלתם? מה משותף לתוצאות של כפולות זוגיות של 11? מה משותף לתוצאות של כפולות זוגיות?

מה קרה פה? קבוצת המספרים שקבלנו, כשניסינו להצפין על ידי כפל ב-  $11 \pmod{22}$ , כוללת רק שני מספרים, 0 ו-11 לסירוגין. וכך סדרת המספרים המציינת את אותיות המסר המקורי:

0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21

עברה למספרים:

0 11 0 11 0 11 0 11 0 11 0 11 0 11 0 11 0 11 0 11 0 11

אנחנו רואים שהכפל ב-11 הצפין אותיות שונות במקור, לאותה אות במסר המוצפן. כבר בחוברת הראשונה ראינו כיצד אפשר לתת לכל אות ייצוג מספר. כך, גם המסר המקורי וגם המסר המוצפן היו מיוצגים על ידי צירופי מספרים. במקרה של כפל ב-11 (בהצפנה בשפה העברית) יוצפנו מספרים שונים, המייצגים אותיות שונות במסר המקורי, לאותו מספר (אותה אות) במסר המוצפן.

לכן בבואנו לפענח אי אפשר יהיה לדעת לאיזה אות לפענח את המספר 11. ל-1? ל-3? אולי ל-5? ואולי זה בכלל מספר אחר? כפי שראינו, קיימות 11 אפשרויות שונות. בקיצור ההצפנה שניסינו לבצע נכשלה. קבוצת המספרים שקבלנו אינה תמורה של הקבוצה המקורית. זכרו כי תמורה של  $n$  אותיות חייבת לכלול את כל  $n$  האותיות של השרשרת המקורית, אלא בסדר שונה מהמקור. זה היה המצב כשכפלנו ב-3 וגם כשכפלנו ב-5.

בהצפנה לפי:  $C = 3P \pmod{22}$

קבלנו מן השרשרת המקורית:

[0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21]

את התמורה:

[0 3 6 9 12 15 18 21 5 8 11 14 17 20 1 4 7 10 13 16 19]

בשרשרת המקורית יש 22 מרכיבים ובתמורה שלה מופיעים כל אותם המרכיבים **והם בלבד**, אלא שהם מסודרים בסדר שונה. במילים אחרות, לכל מספר בשרשרת המקורית, מתאים מספר אחד ורק אחד בתמורת ההצפנה, שקבלנו על ידי כפל ב-3. המספר 2 בשרשרת המקורית למשל, מתאים ל-6 **בלבד** ולהפך, המספר 6 בתמורת ההצפנה מתאים ל-2 **בלבד**. המספר 16 בשרשרת המקורית מתאים ל-4 בתמורת ההצפנה **ורק** ל-4.

כבר למדנו כי להתאמה כזאת בין שתי קבוצות של מספרים, קוראים התאמה חד-חד ערכית. ראינו גם שאם בין המספרים בשרשרת המקורית ובין אלה שבתמורתה, קיימת התאמה חד-חד ערכית, אזי גם בין אותיות המסר המוצפן לבין אותיות המסר המקורי קיימת התאמה חד-חד ערכית, זה היה המצב בהצפנה מונואלפבתית. נוכחנו כי רק התאמה חד-חד ערכית בין אותיות המסר המקורי לבין אותיות המסר המוצפן, מאפשרת פענוח חד משמעי של המסר המוצפן. שאלנו איזה מספר יכול לשמש כמפתח הצפנה ונוכחנו כי 3 למשל, מתאים לכך, כיוון שהוא יוצר תמורה במודול 22. ראינו כי ההצפנה והפענוח הן תמורות שונות של אותיות הא"ב, כלומר קיימת ביניהן התאמה חד-חד ערכית. בפתח סעיף זה שאלנו איזה מספר מתאים לשמש כמפתח הצפנה של כפל במודול 22. ראינו כי גם 5 וגם 3 מתאימים לכך, כיוון שכפל מודולרי בהם יוצר התאמה חד-חד ערכית בין אותיות המסר המקורי לאלה של המסר המוצפן. המספר 11, לעומת זאת, אינו יכול לשמש כמפתח הצפנה במודול 22. הוא אינו יוצר התאמה חד-חד ערכית של אותיות המסר ואותיות המסר המוצפן. הוא הצפין מחצית מאותיות המסר המקורי לאותה אות במסר המוצפן. בניסיון הפענוח, אות אחת של המסר המוצפן תוכל להתפענח ל- 11 אותיות שונות במסר המקורי. נסכם איפוא: במצב שלא קיימת חד-חד ערכיות, בין ההצפנה לפענוח, ההצפנה אינה מעשית כיוון שהפענוח בלתי אפשרי.

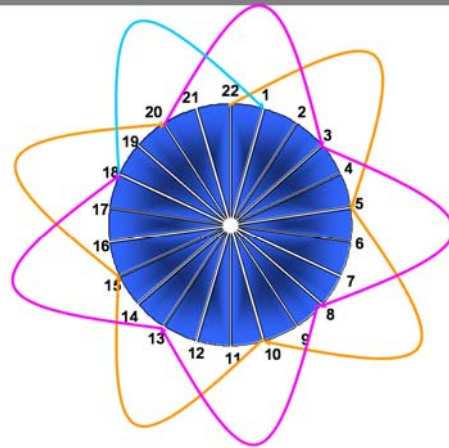
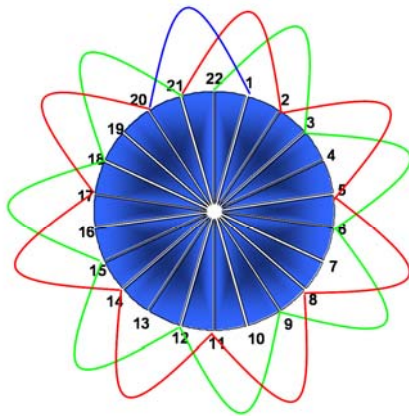
איך אפשר להסביר את התוצאות שקבלנו? מדוע המספרים 3 ו- 5 התאימו לשמש כמפתחות הצפנה ואילו המספר 11 לא התאים לכך? איזה תכונה של המספר קובעת האם הוא מתאים לשמש כמפתח הצפנה? בסעיף הבא נברר זאת.

## 5.7 מספרים ראשוניים ומספרים זרים

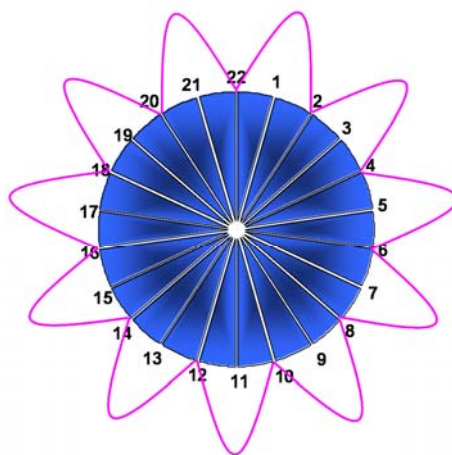
כידוע, לכל מספר חיובי שלם וגדול מ- 1 יש שני מחלקים לפחות (שני מספרים בהם הוא מתחלק ללא שארית): הוא עצמו והמספר 1. **למספר ראשוני יש בדיוק שני מחלקים.** למשל, 7 הוא מספר ראשוני כיוון שיש לו שני מחלקים בלבד 1 ו- 7. רק בהם הוא מתחלק. לעומת זאת, 45 אינו ראשוני, כיוון שבנוסף להתחלקותו ב- 1 וב- 45, הוא מתחלק ב- 3, ב- 5 ובמספרים נוספים.

**מספרים זרים** - שני מספרים נקראים זרים אם אין להם מחלק משותף, חוץ מ- 1. למשל, 38 ו- 55 הם מספרים זרים. אמנם אף אחד מהם אינו ראשוני, כלומר, לכל אחד מהם יש יותר משני מחלקים, אבל אין להם מחלקים משותפים פרט ל- 1. המחלקים של 38 הם 1, 2, 19, ואילו המחלקים של 55 הם 1, 5, 11. המחלק המשותף של שניהם הוא 1 בלבד, לכן הם מספרים זרים. לעומת זאת, 22 ו- 55 אינם זרים כי שניהם מתחלקים ב- 11.

קודם שאלנו מדוע המספרים 3 ו-5 מתאימים כמפתחות הצפנה במודול 22 ואילו המספר 11 אינו מתאים? שימו לב לכך, של-3 ול-22 אין מחלקים משותפים. גם ל-5 ול-22 אין מחלקים משותפים. 22 לא מתחלק ב-3 וגם לא ב-5, המספרים 3 ו-5 זרים ל-22 (למודול). נדגים זאת בשרטוט הבא:



לעומת זאת, 2 ו-22 לא זרים, ניתן לראות זאת בשרטוט הבא:



אבל ל-22 ול-11 יש גורם משותף, 11 ומשום כך הם לא זרים. כיצד יראה הפרח שהיקפו 22 ובו עלה הכותרת בן 11 קפיצות?

אנו רואים אם כן, כי רק מספרים שהם זרים למודול שאתו עובדים, יוצרים הצפנה חד-חד ערכית. לכן רק הם מתאימים לשמש כמפתחות הצפנה במודול זה.



### שאלה מספר 14

- א. מהם המספרים הזרים ל- 22 וקטנים ממנו?  
 ב. רשום את הזוגות ההופכיים בכפל מודולו 22, לפי טבלת הכפל מודולו 22 שבשאלה 10.  
 ג. אילו זוגות מתאימים לשמש מפתחות הצפנה במודולו 22 ומדוע?

מהם המחלקים הראשוניים של 22? 2 ו- 11. לכן כל המספרים הזוגיים וכל הכפולות של 11 אינם זרים ל- 22 ולא יוכלו לשמש כמפתח הצפנה במודול 22. כל שאר המספרים יתאימו לכך. האמנם כל השאר? גם אם הם גדולים מ- 22? ננסה.



### שאלה מספר 15

הצפינו לפי המפתח  $C=25P \bmod 22$ . השוו את התוצאות לאלה שמקבלים כשמציפינים לפי הנוסחה  $C=3P \bmod 22$ . מה אפשר ללמוד מכך? האם יש טעם לחפש מפתחות הצפנה מן הסוג  $C=bP \bmod 22$  כאשר  $b>22$ ?

$$= 3P \bmod 22 \quad 25P \bmod 22 = (22 + 3) P \bmod 22 = 22P \bmod 22 + 3P \bmod 22 = 0 + 3P \bmod 22$$
  
 ובמקרה הכללי, נניח ש:  $b = 22+a$  (כיוון ש-  $b>22$ )  
 ואז:  $bP \bmod 22 = (22+a) \bmod 22 = a \bmod 22$ .  
 אבל כל המספרים הקטנים מ- 22 (כולל  $a$ ), כבר נבדקו.  
 לכן אין טעם לחפש מפתחות הצפנה מן הסוג:  $C = bP \bmod 22$ , כאשר  $b>22$ .  
 הגדלת המפתח-  $b$ , אינה מוסיפה, אם כן, דבר. הסיבה לכך היא, שכל התוצאות הן במודול 22.



### שאלה מספר 16

מהם כל מפתחות ההצפנה האפשריים לא"ב האנגלי, שנוסחתם  $C=bP \bmod 26$ ?  
 סדרו אותם בזוג.

## 5.8 מציאת ההפכי הכפלי

### 5.8.1 הקדמה

נניח שיש לנו מפתח הצפנה  $e$ , במודול  $m$ , מה יהיה מפתח הפענוח המתאים לו? הוא יהיה ההפכי הכפלי של  $e$  במודול  $m$ . נסמן אותו ב-  $d$ . כבר ראינו כי אפשר למצוא אותו בעזרת טבלת כפל מודולרי במודול  $m$ . כשחקרנו את טבלת הכפל המודולרי גלינו כי כל זוג של מחלקים, שהם זרים למודול ומכפלתם שווה לאחד במודול  $m$ , מתאימים לשמש כזוג מפתחות של הצפנה  $e$  ו-  $d$ . כעת נלמד שיטה למציאת ההפכי הכפלי בעזרת האלגוריתם של אוקלידס.

### 5.8.2 האלגוריתם של אוקלידס לחישוב מחלק משותף מקסימלי של שני מספרים שלמים

יש אומרים כי האלגוריתם של אוקלידס הוא אבי אבותיהם של כל האלגוריתמים, כיוון שהוא האלגוריתם העתיק ביותר, ששרד עד ימינו. אוקלידס פרסם גרסה של האלגוריתם בספרו "יסודות", בשנת 300 לפנה"ס. אך ההיסטוריונים משוכנעים כי האלגוריתם הומצא עוד 200 שנה קודם לכן. בכל מקרה הוא ידוע כבר הרבה שנים. כיצד פועל האלגוריתם של אוקלידס?

זוכרים את ההליך הרגיל של חילוק ארוך של מספר שלם  $a$  במספר שלם  $b$ ? למדתם אותו מזמן אבל לבטח לא תתקשו להיזכר כי הליך זה נמשך עד שהשארית קטנה מהמחלק.

למשל, אם:  $a = 648$

ו:  $b = 7$

החישוב ייתן את התוצאה:  $648 = 7 \times 92 + 4$

קבלנו את המנה:  $q = 92$

ואת השארית:  $r = 4$

אפשר לנסח זאת כמשפט כללי:

אם  $a$  הוא מספר שלם ו-  $b$  הוא שלם גדול מאפס קטן מ  $a$ , אזי אפשר למצוא תמיד מספרים שלמים  $q$  ו-  $r$ ,

כך ש:  $a = bq + r$  (1) כאשר  $r$  מקיים את אי השוויון:  $0 \leq r < b$

הערה: אם  $b$  מחלק של  $a$  אז  $r=0$ .

(ההוכחה למשפט אוקלידס נמצאת בנספח)

מן העובדה הפשוטה הזאת אפשר להסיק מסקנות חשובות. אנחנו נראה אחת מהן, השיטה למציאת המחלק המשותף המקסימלי של שני מספרים.

נניח שנתונים שני שלמים  $a$  ו-  $b$ , שאחד מהם אינו אפס ונניח שקיימת קבוצה של מספרים, שכולם מחלקים את  $a$  ואת  $b$ . קבוצה זו היא כמובן סופית. ננמק זאת: נניח ש-  $a \neq 0$ , ברור שהמחלק הגדול ביותר שלו הוא  $a$  עצמו, אותם שיקולים קיימים גם לגבי  $b$ . לכן מספר המחלקים סופי. נסמן את המחלק הגדול ביותר של  $a$  ו-  $b$ , המחלק המשותף המקסימלי, ב-  $d$ .

הסימון המתמטי של המחלק המשותף המקסימלי של  $a$  ו- $b$ :  $d = (a,b)$  ובמילים:  $d$  הוא המחלק המשותף הגדול ביותר של  $a$  ו- $b$  (לפעמים נקרא ל- $d$ , "מ.מ.מ.").

דוגמאות לחישוב המחלק המשותף המקסימלי:

א. נתון  $a = 12, b = 8$

על ידי ניסוי נמצא  $4 = (12,8)$

ב. נתון  $a = 9, b = 5$

על ידי ניסוי נמצא  $1 = (9,5)$

כשמדובר במספרים גדולים, החיפוש על ידי ניסוי ארוך ומייגע. האלגוריתם של אוקלידס מספק דרך קצרה ובטוחה. הוא מבוסס על העובדה שמכל יחס שצורתו:

$$(2) \quad a = bq + r$$

$$(3) \quad (a,b) = (b,r) \quad \text{נובע:}$$

ובניסוח מילולי:

המחלק המשותף המקסימלי של  $a$  ו- $b$ , שווה למחלק המשותף המקסימלי של  $b$  ו- $r$ .

נחזור לדוגמאות הקודמות:

א.  $a=12, b=8$

$$12=8 \cdot 1 + 4$$

$$(12,8)=(8,4)=4$$

ב.  $a=9, b=5$

$$9=5 \cdot 1 + 4$$

$$(9,5)=(5,4)=1$$

נראה כי אם  $u$  מחלק משותף של  $a$  ו- $b$ , אז אפשר לרשום את  $a$  ו- $b$  כמכפלות של  $u$ :  $a = su$   $b = tu$  כאשר  $s$  ו- $t$  שלמים.

כך מתקיים למשל בדוגמה הבאה:

נניח ש-  $b = 28$  ו-  $a = 63$

$$63=28 \cdot 2 + 7$$

$$(63,28)=(28,7)=7$$

בדוגמה זו המחלק המשותף המקסימלי של  $a$  ו- $b$  הוא 7 וניתן לרשום את  $a$  ו- $b$  כמכפלות של 7:

$$28 = 4 \cdot 7 \quad \text{ו-} \quad 63 = 9 \cdot 7$$

נוכיח את הטענה הכללית, שהמחלק המשותף המקסימלי  $u$  של  $a$  ו- $b$ , הוא גם המחלק המשותף המקסימלי של  $b$  ו- $r$ :

נניח כי  $u$  מחלק משותף של  $a$  ו- $b$  אז:

$$u \text{ מחלק גם את } r \text{ כיוון שניתן לרשום את } r \text{ כמכפלה של } u: \quad r = a - bq = su - qt = (s - qt)u$$

**לכן כל מחלק משותף של  $a$  ו- $b$ , הוא גם מחלק משותף של  $b$  ו- $r$ .**

ולהיפך גם כן נכון. נוכיח זאת:

נניח כי  $v$  מחלק משותף של  $r$  ו- $b$ , אז ניתן לרשום את  $r$  ו- $b$  כמכפלות של  $v$ :

$$b = s_1 v \quad r = t_1 v$$

והוא גם מחלק את  $a$  כיון ש:  $a = bq + r = s_1 vq + t_1 v = (s_1 q + t_1)v$

**לכן כל מחלק משותף של  $r$  ו- $b$  הוא גם מחלק משותף של  $a$  ו- $b$ .**

לכן, קבוצת כל המחלקים המשותפים של  $a$  ו- $b$ , זהה לקבוצת המחלקים המשותפים של  $b$  ו- $r$ .

לכן, גם המחלק המשותף המקסימלי של  $a$  ו- $b$  מוכרח להיות זהה למחלק המשותף המקסימלי של  $b$  ו- $r$ , כמו שנטען למעלה בשורה (3).

מיד נראה שימוש של תכונה זו:

מהו המחלק המשותף המקסימלי של 1804 ו-328?

$$1804 = 328 \cdot 5 + 164 \quad \text{על ידי חילוק ארוך נמצא:}$$

$$(1804, 328) = (328, 164) \quad \text{על סמך (3) אנו מסיקים ש:}$$

שימו לב שהבעיה המקורית הוחלפה בבעיה המערבת מספרים יותר קטנים. לכן אנו יכולים להמשיך לבצע את החילוק במספרים החדשים ולרשום:

$$328 = 164 \cdot 2 + 0$$

$$(328, 164) = (164, 0) = 164 \quad \text{כלומר:}$$

$$(1804, 328) = (328, 164) = (164, 0) \quad \text{ולכן:}$$

וזו התוצאה המבוקשת.

באופן כללי, כשנתונים שלמים  $a$  ו- $b$ ,  $b \neq 0$  ואנו מחפשים את המ.מ.מ. שלהם, אזי אפשר להפעיל חילוק חוזר שלהם כדי לקבל את המחלק המשותף המקסימלי:

(4)

|                      |                   |
|----------------------|-------------------|
| $a = bq_1 + r_1$     | $(0 < r_1 < b)$   |
| $b = r_1q_2 + r_2$   | $(0 < r_2 < r_1)$ |
| $r_1 = r_2q_3 + r_3$ | $(0 < r_3 < r_2)$ |
| $r_2 = r_3q_4 + r_4$ | $(0 < r_4 < r_3)$ |
| וכו'.....            | וכו'.....         |

כמו שראינו בדוגמה, התהליך נמשך כל עוד השאריות  $r_1, r_2, r_3, r_4, \dots$  אינן 0. אם תבחנו את האי שוויונות שבטור הימני תוכלו להיווכח כי לפנינו טור יורד של מספרים חיוביים.

$$(5) \quad b > r_1 > r_2 > r_3 > r_4 > \dots > 0$$

ולכן אחרי  $b$  צעדים לכל היותר תהיה השארית 0. בדרך כלל זה יקרה אחרי הרבה פחות צעדים, כיון שבדרך כלל ההפרש בין שתי שאריות עוקבות גדול מ-1.

בסוף הדרך נקבל:

$$r_{n-2} = r_{n-1}q_n + r_n$$

$$r_{n-1} = r_n q_{n+1} + 0$$

כשזה קורה, אנו יודעים שמצאנו את המחלק המשותף המקסימלי:  $(a,b) = r_n$  במילים אחרות,  $(a,b)$  הוא השארית החיובית האחרונה בסדרה (5).

זה נובע מיישום חוזר של השוויון (3) על האי שוויונות (4), כיוון שמשורות עוקבות של (4) נקבל:

$$(a,b) = (b,r_1), \quad (b,r_1) = (r_1,r_2), \quad (r_1,r_2) = (r_2,r_3), \quad (r_2,r_3) = (r_3,r_4), \quad \dots, (r_{n-1},r_n) = (r_n,0) = r_n$$


### שאלה מספר 17

חשבו בעזרת האלגוריתם של אוקלידס את המחלק המשותף המקסימלי של זוגות המספרים הבאים:

1. 105, 385
2. 393, 345
3. 187, 77

איך כל זה מתקשר לכללי החשבון המודולרי? איך זה יעזור לנו למצוא הפכי כפלי של מספר במודול מסוים? את זאת נראה בסעיף הבא.

### 5.8.3 השימוש באלגוריתם של אוקלידס למציאת ההפכי הכפלי

זכור:  $(a,b) = (b,r)$

כאשר  $r$  הוא שארית החלוק של  $a$  ב-  $b$  לכן:

$$r = a \bmod b$$

לכן  $(a,b) = ((a \bmod b), b)$

ממערכת המשוואות המסומנת למעלה ב- (4) נגזרת תכונה חשובה של  $(a,b)$ :

אם:  $d = (a,b)$  כי אז קיימים שני שלמים, חיוביים או שליליים,  $k$  ו-  $l$  כך ש:  $d = ka + lb$  (6)

(נזכור כי  $d$  הוא גם השארית האחרונה השונה מאפס באלגוריתם של אוקלידס.)

נראה כי מתכונה זו נובעת האפשרות למציאת ההפכי הכפלי המודולרי.

כדי להראות זאת נבחן את סדרת השאריות העוקבות המסומנות ב- (5).

בדוד השארית במשוואה הראשונה ב- (4)  $a = bq_1 + r_1$

$$r_1 = a - q_1 b$$

$$r_1 = k_1 a + l_1 b$$

$$k_1 = 1, \quad l_1 = -q_1$$

$$b = r_1 q_2 + r_2$$

$$r_2 = b - r_1 q_2$$

$$r_2 = b - r_1 q_2 = b - (k_1 a + l_1 b) q_2 = (-q_2 k_1) a + (1 - q_2 l_1) b = k_2 a + l_2 b \quad \text{השארית הבאה:}$$

$$K_2 = q_2 k_1, l_2 = (1 - q_2 l_1) \quad \text{במקרה זה:}$$

אפשר לחזור על התהליך עם כל השאריות העוקבות:  $r_3, r_4, \dots, r_n$

$$r_n = k a + l b \quad \text{ונקבל מתוך אותם השיקולים:}$$

$$r = k a + l b \quad \text{כלומר, נקבל את (6):}$$

נבהיר על ידי דוגמה מספרית:

נחפש את:  $(61, 24)$  באמצעות האלגוריתם של אוקלידס:

$$61 = 24 \cdot 2 + 13$$

$$24 = 13 \cdot 1 + 11$$

$$13 = 11 \cdot 1 + 2$$

$$11 = 2 \cdot 5 + 1$$

$$2 = 1 \cdot 2 + 0$$

מסקנה: המחלק המשותף המקסימלי הוא  $(61, 24) = 1$ . אנו מחפשים את שני המספרים השלמים  $I, K$  שלפי

$$1 = K \cdot 61 + I \cdot 24 \quad \text{טענה (6) יתנו:}$$

נבודד את השאריות בכל שלב:

$$13 = 61 - 2 \cdot 24 \quad \text{מן המשוואה הראשונה נקבל:}$$

$$11 = 24 - 13 = 24 - (61 - 2 \cdot 24) = -61 + 3 \cdot 24 \quad \text{נמשיך בתהליך ונרשום את השארית הבאה:}$$

$$2 = 13 - 11 = (61 - 2 \cdot 24) - (-61 + 3 \cdot 24) = 2 \cdot 61 - 5 \cdot 24 \quad \text{את זו שאחריה:}$$

$$1 = 11 - 5 \cdot 2 = (-61 + 3 \cdot 24) - 5(2 \cdot 61 - 5 \cdot 24) = -11 \cdot 61 + 28 \cdot 24 \quad \text{והאחרונה:}$$

$$I = 28, K = -11 \quad \text{מצאנו:}$$

כיצד זה עוזר לנו למצוא את ההפכי הכפלי במודול מסוים? למשל ההפכי הכפלי של  $24 \bmod 61$ .

כבר ראינו כי  $(61, 24) = 1$  ומצאנו שני מספרים שלמים  $28, -11$  שמקיימים את השיויון:

$$28 \cdot 24 - 11 \cdot 61 = 1$$

$$(24 \cdot 28) \bmod 61 - (11 \cdot 61) \bmod 61 = 1 \bmod 61 \quad \text{אפשר לרשום גם:}$$

$$(11 \cdot 61) \bmod 61 = 0 \quad \text{אבל:}$$

$$1 \bmod 61 = 1 \quad \text{ו:}$$

$$(24 \cdot 28) \bmod 61 = 1 \quad \text{ולכן קבלנו ש:}$$

אבל מהי המשמעות של המשוואה האחרונה? משמעותה היא ש-  $24$  ו-  $28$  הם הפכיים כפליים מודול  $61$

ובהכללה, מצאנו דרך לאיתור ההפכי הכפלי מודול  $X$  של מספר זר ל-  $X$ .

דוגמה:

נבחר שני מספרים זרים, למשל:  $7, 40$ .

מהו ההפכי הכפלי של  $7 \bmod 40$ ?

### שלב ראשון: מוצאים את (7,40).

מפני שהם זרים, אנו יודעים כי המחלק המשותף המקסימלי שלהם הוא 1. מבצעים חלוק חוזר:

$$40 = 7 \cdot 5 + 5$$

$$7 = 5 \cdot 1 + 2$$

$$5 = 2 \cdot 2 + 1$$

$$2 = 1 \cdot 2 + 0$$

### שלב שני: הצגת השאריות כסכום מכפלות שלמות של 40,7:

מציגים את השאריות כביטוי שתלוי במספרים 7,40 לשם מציאת ההצגה כסכום מהצורה  $1 = k \cdot 40 + l \cdot 7$

$$5 = 40 - 5 \cdot 7$$

$$2 = 7 - 1 \cdot 5 = 7 - (40 - 5 \cdot 7)$$

$$1 = 5 - 2 \cdot 2 = (40 - 5 \cdot 7) - 2(7 - (40 - 5 \cdot 7)) = 3 \cdot 40 - 17 \cdot 7$$

$$l = -17, K = 3 \quad \text{מצאנו:}$$

### שלב שלישי: חישוב ההפכי של 7 מודולו 40

$$3 \cdot 40 - 17 \cdot 7 = 1$$

$$(-17 \cdot 7) \bmod 40 = 1$$

מצאנו שההפכי הכפלי של  $7 \bmod 40$  הוא -17. מה פרושה של התוצאה? הלא אמרנו כי בחשבון מודולרי התוצאות הסופיות הם תמיד שלמים חיוביים? זכרו כי במודול 40 מבוצעות כל הפעולות על פני מעגל שהיקפו 40 יחידות. הנקודה -17 על פני מעגל זה היא גם הנקודה +23, הכל תלוי בכיוון התנועה שלנו על פני המעגל. במלים אחרות ההפכי הכפלי של 7 מודולו 40 הוא 23. ואמנם  $(7 \cdot 23) \bmod 40 = 1$ .

לסיכום, איזה "חדשות" מבשר לנו האלגוריתם של אוקלידס? החדשות ה"טובות" הן בעצם גילוי. כעת יש בידינו שיטה טובה למציאת הפכי כפלי, במסגרת מאמצינו לפתח שיטות הצפנה אסימטריות. החדשות ה"רעות" הן, שלא נוכל יותר להשתמש בכפל מודולרי כאלגוריתם הצפנה. האלגוריתם של אוקלידס מבטיח למאזי הצלחה מהירה ופשוטה בפיצוח המסרים המוצפנים של בני ואילנית. ההצפנה על ידי כפל מודולרי היא אמנם אסימטרית והצפנות אסימטריות אנחנו מעונינים לפתח, אבל הסיבוכיות של פצוח הצפנה על ידי כפל מודולרי אינה מספקת כלל וכלל לאור פתוח האלגוריתם של אוקלידס.



### שאלה מספר 18

מצא בעזרת האלגוריתם של אוקלידס את ההפכי הכפלי של  $19 \bmod 40$ .

## 5.9 זהויות מעריכיות

### 5.9.1 מהי זהות מתמטית?

זהות מתמטית היא שוויון בין שתי צורות הצגה של אותו ביטוי מתימטי. הזהות מביעה את יכולתנו לומר אמירה מתמטית אחת בשתי דרכים שונות. למשל השוויון:

$$5 \cdot 2a = 10a$$

זו זהות. לא משנה איזה מספר נציב במקום  $a$ , לכל הצבה ישמר בין שני אגפי המשוואה השוויון.

$$X^a * X^b = X^{a+b} \quad \text{גם השוויונות המעריכיים הבאים הם זהויות:}$$

$$(X^a)^b = X^{a \cdot b}$$

$$(a+b) \bmod n = a \bmod n + b \bmod n \quad \text{וגם השוויונות המודולריים:}$$

$$(a \cdot b) \bmod n = a \bmod n * b \bmod n$$

$$(m^e \bmod n)^d \bmod n = m^{ed} \bmod n$$

שני האגפים מבטאים אותו הדבר בדרכים שונות. כלומר, השוויון מהווה זהות, לא משנה איזה מספרים נציב בשניהם, השוויון ביניהם לא יופר.



### שאלה מספר 19

בדקו את נכונות הזהות המספרית:  $(2^4 \bmod 11)^5 \bmod 11 = (2^{4 \cdot 5}) \bmod 11$

חישוב חזקות עלול להיות ארוך ומייגע. נראה כיצד אפשר לקצרו בעזרת זהויות מעריכיות ובעזרת חוקי החישוב של החשבון המודולרי.

### 5.9.2 קיצורי דרך בעזרת החשבון המודולרי

$$7^8 \bmod 11 \quad \text{ניזכר בחישוב מסעיף 5.5:}$$

$$7^8 = (7^4)^2 = ((7^2)^2)^2 \quad \text{אנו יודעים כי:}$$

$$7^8 \bmod 11 = (((49)^2)^2) \bmod 11 \quad \text{ולכן:}$$

$$49 \bmod 11 = 5 \quad \text{כיוון ש:}$$

$$((5^2)^2) \bmod 11 = 3^2 \bmod 11 = 9 \quad \text{אז:}$$

התוצאה זהה לזו שקבלנו כאשר חשבנו אותה על ידי החילוק הארוך שאנו מכירים. אבל התהליך הרבה יותר פשוט. שיטת חישוב זו נקראת ריבוע חוזר (repeating squaring). היא שימושית ומועילה, כיוון שהיא מקצרת ומפשטת את החישוב המודולרי של חזקות בעלות מעריכים גדולים. כמו שראיתם הקיצור מושג על ידי ביצוע המודול אחרי כל כפל.

נבחן דוגמאות נוספות:

כמה הם  $23^{16} \bmod 30$ ?

כיוון ש:  $16 = 2 \cdot 2 \cdot 2 \cdot 2$

נכתוב:  $23^{16} = 23^{2 \cdot 2 \cdot 2 \cdot 2} = (((23^2)^2)^2)^2$

לכן:

$$\begin{aligned} 23^{16} \bmod 30 &= (((23^2)^2)^2)^2 \bmod 30 = (((-7^2)^2)^2)^2 \bmod 30 \\ &= (((49)^2)^2)^2 \bmod 30 = (((-11)^2)^2)^2 \bmod 30 = ((121)^2)^2 \bmod 30 \\ &= ((1)^2)^2 \bmod 30 = 1 \\ 23^{16} \bmod 30 &= 1 \end{aligned}$$

התשובה הסופית:



### שאלה מספר 20

כמה הם  $23^{25} \bmod 30$ ?

רמז: הציגו את  $23^{25}$  כ-  $23^{16+8+1}$ . הפעילו ריבוע חוזר על כל חלק, הכפילו את התוצאות.

בדוגמאות שפתרנו הפעלנו תחילה את השיטה של ריבוע חוזר רק על מעריכים שהיו חזקות של 2. אבל 25 אינו חזקה של 2, מה עשינו? הצגנו אותו כסכום של חזקות של 2 והפעלנו על כל אחד מאברי הסכום את שיטת הריבוע החוזר. בעצם הצגנו את מעריך החזקה בייצוג בינרי:

$$25 = 1 \cdot 2^4 + 1 \cdot 2^3 + 0 \cdot 2^2 + 0 \cdot 2^1 + 1 \cdot 2^0$$



### שאלה מספר 21

כמה הם  $17^{39} \bmod 30$ ?

האם הביטויים המעריכיים עשויים להביא תועלת נוספת, פרט לקיצורי דרך חישוביים? לאחר שנוכחנו כי הסיבוכיות של הכפל המודולרי אינה מספקת לביצוע הצפנה, נבחן כעת את הסיבוכיות שאפשר ליצור באמצעות ביטויים מעריכיים. האם הם יתאימו למטרות הצפנה? האם אפשר לבצע הצפנות אסימטריות בעזרת ביטויים מודולרים מעריכיים? בהמשך נבדוק זאת.

## 5.10 תרומתם של פרמה ואוילר לפיתוח ההצפנה האסימטרית

### 5.10.1 המשפט הקטן של פרמה

פייר דה פרמה (1601 – 1665) היה עורך דין צרפתי עד גיל 30. אחר כך בעקבות ספר מתמטיקה עתיק שהתגלגל לידייו וכנראה שבה אותו, הפכה המתמטיקה לתחביבו הרציני. הוא התפתח לאחד מגדולי המתמטיקאים של כל התקופות. בין יתר תרומותיו המתמטיות, תרם גם לפיתוח האריתמטיקה המודולרית. הוא מצא, שאם עובדים עם מודול ראשוני, אזי פעולות החישוב הן "נוחות". הוא הוכיח ש:

אם רוצים לחשב מספר  $m$  במודול של מספר ראשוני  $p$ , כאשר  $m < p$ , כי אז:  $m^{(p-1)} \bmod p = 1$ .

המשפט הזה נקרא, אמנם, "המשפט הקטן של פרמה" (הוא נסח גם משפט שזכה לכינוי "המשפט הגדול", שלא נעסוק בו) אבל חשיבותו גדולה מאוד. איך הוא הופך את הפעולות ל"נוחות"? מה התועלת בכך? איך נחשב, למשל:  $7^{10} \bmod 11$ ?

האם יש קיצורי דרך? יש ויש, בעזרת תגליתו של פרמה. אנחנו יודעים ש-11 ראשוני ואנחנו יודעים ש:  $10 = 11 - 1$ . לכן אין צורך לבצע שום חישוב נוסף, אפשר לכתוב בביטחון:  $7^{10} \bmod 11 = 1$ .

#### שאלה מספר 22



חברו 8 תרגילים, שעושים שימוש במשפט הקטן של פרמה. השלימו את הטבלה:  
זכרו כי  $p$  ראשוני ו-  $1 \leq m < p$

#### שאלה מספר 23



הראו:

- א.  $7^{12} \bmod 11 = 7^2 \bmod 11$
- ב.  $5^{27} \bmod 124 = 5^3 \bmod 124$
- ג.  $5^{120} \bmod 24 = 5^2 \bmod 24$
- ד.  $7^{50} \bmod 48 = 7^{10} \bmod 48 = 1$

#### שאלה מספר 24



חברו 3 תרגילים נוספים במתכונת זו. פתרו אותם.

## 5.10.2 משפט אוילר

ליאונרד אוילר (1707 – 1783) הוא אחד מענקי המתמטיקה, שחיו אי פעם. הוא גילה ששוויון דומה לזה, שמתקיים במשפט הקטן של פרמה, מתקיים, גם אם בוחרים בתור מודול  $n$ . מספר שהוא **מכפלה של שני ראשוניים**,  $p$  ו- $q$ . אוילר קבע כי:

$$m^{(p-1)(q-1)} \bmod n = 1 \quad \text{אז } 1 \leq m < n \text{ ו- } m \text{ זרים, כי אז } m^{(p-1)(q-1)} \bmod n = 1$$

זהו משפט אוילר וחיבותו לפיתוח ההצפנה האסימטרית עצומה. בהמשך נבין מדוע. כדי להבין את קביעתו

של אוילר נבחר שני מספרים ראשוניים, למשל:  $p=11, q=5$ .

מכפלתם:  $n=5*11=55$

ואז:  $(p-1)(q-1)=(5-1)(11-1)=4*10=40$

כעת, מבלי לבצע כל חישוב נוסף אנו יכולים לקבוע את הערך המספרי של  $38^{40} \bmod 55$

התשובה היא:  $38^{40} \bmod 55 = 11$ .

שימו לב, כי כדי ש"תחבולה" זו תעבוד  $m$  ו- $n$  צריכים להיות זרים.

התנאי הנוסף שצריך להתקיים הוא:  $1 \leq m < n$ .

בדוגמה שהבאנו, התנאים האלה מתקיימים.  $m$  בדוגמה הוא 38. ומהו  $n$ ? 55. האם 38 ו-55 הם זרים? מהם המחלקים הראשוניים של 38? מהם המחלקים הראשוניים של 55? האם יש להם מחלקים משותפים? האם הם זרים? בדקו ותיווכחו שהתשובה חיובית. אתם יכולים להיזכר בנימוקים אלה, על ידי עיון חוזר בסעיף 5.7.

נחזור אל השאלה מהי חיבותו של משפט אוילר בהצפנה אסימטרית? כדי להתקדם לתשובה, נפתח מעט את משפט אוילר על ידי כפל שני האגפים ב- $m$ :

$$m^{(p-1)(q-1)} m \bmod n = 1 * m \quad \text{נקבל}$$

$$m^{(p-1)(q-1)+1} \bmod n = m \quad \text{או}$$

שימו לב: על ידי פעולה מתמטית, העלאה בחזקה של  $m$  במעריך  $(p-1)(q-1)+1$  במודול  $n$ , חזרנו לנקודה ממנה יצאנו, חזרנו ל- $m$ .

המתמטיקאים נוהגים לסמן ב- $\phi(n)$  את המכפלה  $(p-1)(q-1)$ , כאשר  $n$  הוא המודול ו- $n = p*q$ .

המעריך  $(p-1)(q-1)+1$  הוא חשוב מאד כיוון שהוא שימושי מאוד. מדוע, בעצם, הוא כל כך שימושי?

כיוון שנזכרנו, שאם יוצאים ממספר מסוים  $m$ , אז באמצעותו של המעריך הזה, אפשר לחזור אל אותו המספר, גם אחרי פעולות מתמטיות רבות.

מה הקשר להצפנה? אם רק נצליח לפצל את הפעולות המתמטיות לשני שלבים הפכיים, כי אז נוכל לצאת מ- $m$  (מסר כלשהו המיוצג על ידי מספרים) ולהציפו ולפענח אותו, בעזרת תגליותיהם של פרמה ואוילר. בהמשך נעשה זאת: נראה כיצד נוצל הידע המתמטי, שנמצא כעת בידינו, לפיתוח מערכות הצפנה אסימטרית.

### 5.10.3 דוגמה מספרית לשימוש במשפט אוילר

נחשב, למשל, חזקות של 7 מודולו 55.

$$7^2 = 7 * 7$$

נתחיל עם

$$7^3 = 7^2 * 7$$

כדי לחשב  $7^3$  אם יודעים כמה זה  $7^2$

באופן דומה אפשר להמשיך ולחשב את החזקות של 7 (או של כל מספר אחר) מודולו 55 (או כל מודול אחר). לא נכנס כעת לפרטי החישובים, נציין שתי תוצאות הנובעות ממשפט אוילר, ללא צורך בחישוב נוסף:

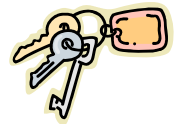
$$7^{40} \bmod 55 = 1$$

$$7^{41} \bmod 55 = 7$$

כאשר היינו צריכים למצוא כמה הם  $7^{40}$  ידענו מייד את התשובה, על פי משפט אוילר היא הייתה 1. שימו לב לעובדה החשובה ביותר, גם במקרה של  $7^{41}$  ידענו את התשובה מבלי לחשב. אבל מה הייתה התשובה?

$$7^{41} \bmod 55 = 7^{40} \bmod 55 * 7 \bmod 55 = 1 * 7 = 7 \quad \text{היא הייתה 7 כי:}$$

כך קיבלנו את המספר ממנו יצאנו, חזרנו לנקודת ההתחלה.



#### שאלה מספר 25

פתרו את התרגילים הרשומים בטבלה. חברו 6 תרגילים פשוטים נוספים, שעושים שימוש במשפט אוילר. רשמו את הנוסחה ואת התוצאה הסופית המתאימה, ללא חישוב.

## 5.11 פתרונות

### פתרון שאלה מספר 1:

| זוג המפתחות<br>(ציבורי פרטי) | המסר   | מפתח ההצפנה<br>(המפתח הציבורי) | המסר המוצפן | מפתח הפענוח<br>(המפתח הפרטי) | פענוח המסר<br>המוצפן |
|------------------------------|--------|--------------------------------|-------------|------------------------------|----------------------|
| 8, 1/8                       | 333    | 8                              | 2,664       | 1/8                          | 333                  |
| 3/2, 2/3                     | 98,766 | 3/2                            | 148,149     | 2/3                          | 98,766               |

### פתרון שאלה מספר 2:

- א. חיבור.
- ב. כפל.
- ג. הוצאת שורש ריבועי.

### פתרון שאלה מספר 3:

בקוטב הצפוני

### פתרון שאלה מספר 4:

- א.  $P = C - B$
- ב. חיבור וחיסור

### פתרון שאלה מספר 5:

|                  |                   |
|------------------|-------------------|
| $19 \bmod 1 = 0$ | $19 \bmod 19 = 0$ |
| $19 \bmod 2 = 1$ | $19 \bmod 20 = 1$ |
| $19 \bmod 3 = 1$ | $19 \bmod 21 = 2$ |
| $19 \bmod 4 = 3$ | $19 \bmod 22 = 3$ |
| $19 \bmod 5 = 4$ | $19 \bmod 23 = 4$ |
| $19 \bmod 6 = 1$ | $19 \bmod 38 = 0$ |

### פתרון שאלה מספר 6:

התשובה בכל התרגילים היא 1.

### פתרון שאלה מספר 7:

א.  $10 : 0, 1, 2, \dots, 9$

ב.  $n$

ג. שארית אפס מורה כי במספר מתחלק במודול – ללא שארית.

### פתרון שאלה מספר 8:

כן, כיוון ש:  $(3 \cdot 15) \bmod 22 = 45 \bmod 22 = 1$

### פתרון שאלה מספר 9:

|   | א | ב | ג  | ד  | ה  | ו | ז | ח  | ט  | י | כ  | ל  | מ  | נ  | ס  | ע  | פ  | צ  | ק  | ר  | ש  | ת  |
|---|---|---|----|----|----|---|---|----|----|---|----|----|----|----|----|----|----|----|----|----|----|----|
| P | 0 | 1 | 2  | 3  | 4  | 5 | 6 | 7  | 8  | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 |
| C | 0 | 5 | 10 | 15 | 20 | 3 | 8 | 13 | 18 | 1 | 6  | 11 | 16 | 21 | 4  | 9  | 14 | 19 | 2  | 7  | 12 | 17 |

### פתרון שאלה מס' 10:

א. טבלת הכפל מודולו 22

|    | 0 | 1  | 2  | 3  | 4  | 5  | 6  | 7  | 8  | 9  | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 |
|----|---|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|
| 0  | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  |
| 1  | 0 | 1  | 2  | 3  | 4  | 5  | 6  | 7  | 8  | 9  | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 |
| 2  | 0 | 2  | 4  | 6  | 8  | 10 | 12 | 14 | 16 | 18 | 20 | 0  | 2  | 4  | 6  | 8  | 10 | 12 | 14 | 16 | 18 | 20 |
| 3  | 0 | 3  | 6  | 9  | 12 | 15 | 18 | 21 | 2  | 5  | 8  | 11 | 14 | 17 | 20 | 1  | 4  | 7  | 10 | 13 | 16 | 19 |
| 4  | 0 | 4  | 8  | 12 | 16 | 20 | 2  | 6  | 10 | 14 | 18 | 0  | 4  | 8  | 12 | 16 | 20 | 2  | 6  | 10 | 14 | 18 |
| 5  | 0 | 5  | 10 | 15 | 20 | 3  | 8  | 13 | 18 | 1  | 6  | 11 | 16 | 21 | 4  | 9  | 14 | 19 | 2  | 7  | 12 | 17 |
| 6  | 0 | 6  | 12 | 18 | 2  | 8  | 14 | 20 | 4  | 10 | 16 | 0  | 6  | 12 | 18 | 2  | 8  | 14 | 20 | 4  | 10 | 16 |
| 7  | 0 | 7  | 14 | 21 | 6  | 13 | 20 | 5  | 12 | 19 | 4  | 11 | 18 | 3  | 10 | 17 | 2  | 9  | 16 | 1  | 8  | 15 |
| 8  | 0 | 8  | 16 | 2  | 10 | 18 | 4  | 12 | 20 | 6  | 14 | 0  | 8  | 16 | 2  | 10 | 18 | 4  | 12 | 20 | 6  | 14 |
| 9  | 0 | 9  | 18 | 5  | 14 | 1  | 10 | 19 | 6  | 15 | 2  | 11 | 20 | 7  | 16 | 3  | 12 | 21 | 8  | 17 | 4  | 13 |
| 10 | 0 | 10 | 20 | 8  | 18 | 6  | 16 | 4  | 14 | 2  | 12 | 0  | 10 | 20 | 8  | 18 | 6  | 16 | 4  | 14 | 2  | 12 |
| 11 | 0 | 11 | 0  | 11 | 0  | 11 | 0  | 11 | 0  | 11 | 0  | 11 | 0  | 11 | 0  | 11 | 0  | 11 | 0  | 11 | 0  | 11 |
| 12 | 0 | 12 | 2  | 14 | 4  | 16 | 6  | 18 | 8  | 20 | 10 | 0  | 12 | 2  | 14 | 4  | 16 | 6  | 18 | 8  | 20 | 10 |
| 13 | 0 | 13 | 4  | 17 | 8  | 21 | 12 | 3  | 16 | 7  | 20 | 11 | 2  | 15 | 6  | 19 | 10 | 1  | 14 | 5  | 18 | 9  |
| 14 | 0 | 14 | 6  | 20 | 12 | 4  | 18 | 10 | 2  | 16 | 8  | 0  | 14 | 6  | 20 | 12 | 4  | 18 | 10 | 2  | 16 | 8  |
| 15 | 0 | 15 | 8  | 1  | 16 | 9  | 2  | 17 | 10 | 3  | 18 | 11 | 4  | 19 | 12 | 5  | 20 | 13 | 6  | 21 | 14 | 7  |
| 16 | 0 | 16 | 10 | 4  | 20 | 14 | 8  | 2  | 18 | 12 | 6  | 0  | 16 | 10 | 4  | 20 | 14 | 8  | 2  | 18 | 12 | 6  |
| 17 | 0 | 17 | 12 | 7  | 2  | 19 | 14 | 9  | 4  | 21 | 16 | 11 | 6  | 1  | 18 | 13 | 8  | 3  | 20 | 15 | 10 | 5  |
| 18 | 0 | 18 | 14 | 10 | 6  | 2  | 20 | 16 | 12 | 8  | 4  | 0  | 18 | 14 | 10 | 6  | 2  | 20 | 16 | 12 | 8  | 4  |
| 19 | 0 | 19 | 16 | 13 | 10 | 7  | 4  | 1  | 20 | 17 | 14 | 11 | 8  | 5  | 2  | 21 | 18 | 15 | 12 | 9  | 6  | 3  |
| 20 | 0 | 20 | 18 | 16 | 14 | 12 | 10 | 8  | 6  | 4  | 2  | 0  | 20 | 18 | 16 | 14 | 12 | 10 | 8  | 6  | 4  | 2  |
| 21 | 0 | 21 | 20 | 19 | 18 | 17 | 16 | 15 | 14 | 13 | 12 | 11 | 10 | 9  | 8  | 7  | 6  | 5  | 4  | 3  | 2  | 1  |

ב. ההפכי הכפלי של 5 מודולו 22 הוא 9 כי:  $(5 \cdot 9) \bmod 22 = 1$

תמורת ההצפנה היא:  $C = 5p \bmod 22$

ותמורת הפענוח תתקבל לפי הנוסחה:  $P = 9C \bmod 22$

### פתרון שאלה מספר 11:

| $X \bmod 11$ | 0 | 1  | 2  | 3  | 4  | 5  | 6  | 7  | 8  | 9  | 10 |
|--------------|---|----|----|----|----|----|----|----|----|----|----|
| 0            | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  |
| 1            | 0 | 1  | 2  | 3  | 4  | 5  | 6  | 7  | 8  | 9  | 10 |
| 2            | 0 | 2  | 4  | 6  | 8  | 10 | 1  | 3  | 5  | 7  | 9  |
| 3            | 0 | 3  | 6  | 9  | 1  | 4  | 7  | 10 | 2  | 5  | 8  |
| 4            | 0 | 4  | 8  | 1  | 5  | 9  | 2  | 6  | 10 | 3  | 7  |
| 5            | 0 | 5  | 10 | 4  | 9  | 3  | 8  | 2  | 7  | 1  | 6  |
| 6            | 0 | 6  | 1  | 7  | 2  | 8  | 3  | 9  | 4  | 10 | 5  |
| 7            | 0 | 7  | 3  | 10 | 6  | 2  | 9  | 5  | 1  | 8  | 4  |
| 8            | 0 | 8  | 5  | 2  | 10 | 7  | 4  | 1  | 9  | 6  | 3  |
| 9            | 0 | 9  | 7  | 5  | 3  | 1  | 10 | 8  | 6  | 4  | 2  |
| 10           | 0 | 10 | 9  | 8  | 7  | 6  | 5  | 4  | 3  | 2  | 1  |

### פתרון שאלה מספר 12:

זוגות ההפכיים הכפליים מודולו 11:  $(1,1)$   $(6,2)$   $(3,4)$   $(5,9)$   $(7,8)$   $(10,10)$   
קיימת סימטריה של פיזור ההפכיים יחסית לאלכסון.

### פתרון שאלה מספר 13:

הזוג הנבחר לדוגמה:  $(3,4)$  טבלת הזהות הכפלית ב-  $\bmod 11$ :

| x | $x \cdot 3 \cdot 4$ | $(x \cdot 12) \bmod 11$ |
|---|---------------------|-------------------------|
| 0 | 0                   | $0 \bmod 11 = 0$        |
| 1 | 12                  | $12 \bmod 11 = 1$       |
| 2 | 24                  | $24 \bmod 11 = 2$       |
| 3 | 36                  | $36 \bmod 11 = 3$       |
| 4 | 48                  | $48 \bmod 11 = 4$       |
| 5 | 60                  | $60 \bmod 11 = 5$       |
| 6 | 72                  | $72 \bmod 11 = 6$       |
| 7 | 84                  | $84 \bmod 11 = 7$       |
| 8 | 96                  | $96 \bmod 11 = 8$       |
| 9 | 108                 | $108 \bmod 11 = 9$      |

**פתרון שאלה מספר 14:**

- א. 1, 3, 5, 7, 9, 13, 15, 17, 19, 21  
 ב. (3, 15) (5, 9) (13, 17) (17, 21)

**פתרון שאלה מספר 15:**

הצפנה ע"י כפל ב- 3 מודולו 22

| X  | $3x \bmod 22$ |
|----|---------------|
| 0  | 0             |
| 1  | 3             |
| 2  | 6             |
| 3  | 9             |
| 4  | 12            |
| 5  | 15            |
| 6  | 18            |
| 7  | 21            |
| 8  | 2             |
| 9  | 5             |
| 10 | 8             |

הצפנה ע"י כפל ב- 25 מודולו 22

| x  | $25x \bmod 22$ |
|----|----------------|
| 0  | 0              |
| 1  | 3              |
| 2  | 6              |
| 3  | 9              |
| 4  | 12             |
| 5  | 15             |
| 6  | 18             |
| 7  | 21             |
| 8  | 2              |
| 9  | 5              |
| 10 | 8              |

**פתרון שאלה מספר 16:**

כל המספרים הזרים ל- 26: 1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25  
 זוגות המפתחות האפשריים: (3,9) (5,21) (7,15) (11,19)

**פתרון שאלה מספר 17:**

1.  $(105, 385) = 35$   
 2.  $(393, 345) = 3$   
 3.  $(187, 77) = 11$

### פתרון שאלה מספר 18:

שלב א':

$$40 = 19 \cdot 2 + 2 \quad (40, 19) \text{ מוצאים}$$

$$19 = 2 \cdot 9 + 1$$

$$2 = 1 \cdot 2 + 0$$

שלב ב':

$$2 = 40 - 2 \cdot 19 \quad \text{מציגים את השאריות:}$$

$$1 = 19 - 9 \cdot 2 = 19 - 9(40 - 19 \cdot 2) = 19 \cdot 19 - 8 \cdot 40$$

שלב ג':

$$(19 \cdot 19) \bmod 40 - (8 \cdot 40) \bmod 40 = 1 \quad \text{מחשבים את ההפכי:}$$

$$(19 \cdot 19) \bmod 40 = 1$$

ההפכי הכפלי של 19 מודולו 40 הוא 19.

### פתרון שאלה מספר 19:

$$(2^4 \bmod 11)^5 \bmod 11 = (16 \bmod 11)^5 \bmod 11 = 5^5 \bmod 11 = 3125 \bmod 11 = 1$$

$$2^{4 \cdot 5} \bmod 11 = 2^{20} \bmod 11 = 1,048,576 \bmod 11 = 1$$

### פתרון שאלה מספר 20:

$$23^{25} = 23^{(16+8+1)} = 23^{16} \cdot 23^8 \cdot 23 = 23^{2 \cdot 2 \cdot 2 \cdot 2} \cdot 23^{2 \cdot 2 \cdot 2} \cdot 23$$

$$23 \bmod 30 = 23$$

$$\begin{aligned} 23^{2 \cdot 2 \cdot 2} \bmod 30 &= ((23^2)^2)^2 \bmod 30 = (((-7)^2)^2)^2 \bmod 30 = ((49)^2)^2 \bmod 30 = ((19)^2)^2 \bmod 30 \\ &= ((-11)^2)^2 \bmod 30 = 121^2 \bmod 30 = 121 \bmod 30 \cdot 121 \bmod 30 = 1 \cdot 1 = 1 \end{aligned}$$

$$23^{16} \bmod 30 = (23^8 \cdot 23^8) \bmod 30 = 1 \cdot 1 = 1$$

$$23^{25} \bmod 30 = 23$$

### פתרון שאלה מספר 21:

אפשר לרשום את 39 בהצגה בינרית:

$$39 = 2^5 + 2^2 + 2^1 + 2^0$$

$$17^{39} = 17^{(32+4+2+1)} = 17^{32} * 17^4 * 17^2 * 17$$

$$17^2 \bmod 30 = (-13)^2 \bmod 30 = 169 \bmod 30 = 19$$

$$17^4 \bmod 30 = 19^2 \bmod 30 = (-11)^2 \bmod 30 = 1$$

$$17^{32} \bmod 30 = (17^4)^8 = 1$$

$$17^{39} \bmod 30 = (1 * 1 * 19 * 17) \bmod 30 = (19 * 17) \bmod 30 = (-11) (-13) \bmod 30$$

$$= 141 \bmod 30 = 21$$

$$17^{39} \bmod 30 = 21$$

### פתרון שאלה מספר 22:

| m  | p  | $m^{(p-1)} \bmod p = 1$         |
|----|----|---------------------------------|
| 2  | 7  | $2^6 \bmod 7 = 64 \bmod 7 = 1$  |
| 4  | 5  | $4^4 \bmod 5 = 256 \bmod 5 = 1$ |
| 2  | 5  | $2^4 \bmod 5 = 16 \bmod 5 = 1$  |
| 10 | 13 | $10^{12} \bmod 13 = 1$          |
| 3  | 11 | $3^{10} \bmod 11 =$             |
| 2  | 3  |                                 |
| 3  | 7  |                                 |
| 5  | 11 |                                 |

### פתרון שאלה מספר 23:

$$7^{12} = 7^{10} * 7^2 \quad \text{א.}$$

$$7^{10} \bmod 11 = 1 \quad \text{אבל לפי משפט פרמה:}$$

$$7^{12} \bmod 11 = 7^2 \bmod 11 \quad \text{לכן:}$$

$$5^3 \bmod 124 = 1 \quad \text{ב. רמז:}$$

$$5^2 \bmod 24 = 1 \quad \text{ג. רמז:}$$

$$7^2 \bmod 48 = 1 \quad \text{ד. רמז:}$$

פתרון שאלה מספר 24:

פתרון שאלה 25:

| p | q  | n  | p-1 | q-1 | m | $m^{(p-1)(q-1)} \bmod n = 1$                                 |
|---|----|----|-----|-----|---|--------------------------------------------------------------|
| 3 | 5  | 15 | 2   | 4   | 4 | $4^8 \bmod 15 = ((4^2)^2)^2 \bmod 15 = (1^2)^2 \bmod 15 = 1$ |
| 3 | 7  | 21 | 2   | 6   | 2 | $2^{12} \bmod 21 =$                                          |
| 5 | 11 | 55 | 4   | 10  | 2 | $2^{40} \bmod 55 =$                                          |
| 5 | 7  | 35 | 4   | 6   | 2 | $2^{24} \bmod 35 =$                                          |
| 3 | 7  | 21 | 2   | 6   | 2 | $2^{12} \bmod 21 =$                                          |
| 5 | 11 | 55 | 4   | 10  | 2 | $2^{40} \bmod 55 =$                                          |

## 6 הצפנה אסימטרית

כעת אנחנו מצוידים בעקרונות המתמטיים הדרושים להבנת הצפנות אסימטריות – הצפנות בהן מפתחות ההצפנה והפענוח שונים זה מזה וידיעת האחד אינה מסגירה את האחר.

**RSA** הוא האלגוריתם המקובל ביותר של ההצפנה האסימטרית. כמו שכבר הזכרנו, שמו התקבל מצרף האותיות הראשונות בשמות המשפחה של ממציאיו: **R.L.Rivest, A.Shamir, L.M.Adelman**. בהמצאתם, לפיתוח אלגוריתם ההצפנה שלהם, הם השתמשו בעובדות, המתמטיות שגילו אוילר ופרמה, (שאם בוחרים כמודול מספר ראשוני, או מכפלה של שני מספרים ראשוניים, כמו שראינו בסעיפים 5.10.1 ו- 5.10.2, כי אז פעולות החישוב מתנהגות בצורה "נוחה"), לפיתוח האלגוריתם של ההצפנה.

### 6.1 מפתחות נפרדים להצפנה ולפענוח

בשיטת ההצפנה האסימטרית מפתח אחד מצפין ואחר, שונה ממנו, מפענח. כיצד זה פועל? איך אפשר שמפתח אחד יכול רק להצפין, אך אינו יכול לפענח? כיצד מבצע המפתח האחר את הפענוח? הרעיון נשמע כאילו הוא נוגד את ההיגיון. ואמנם, במאמרו מ-1976, כתב וויטפילד דיפי, שפיתח שיטה לניסוח הסכם על מפתח סודי בערוצים פתוחים, "זו פעם ראשונה מזה 3000 שנה של חקר ההצפנה, שעולה רעיון מעין זה." חזונו של דיפי היה חזון נועז ומקורי, אבל הוא לא הצליח לממש אותו. הוא לא הצליח לבנות מערכת הצפנה, שתעבוד על פי חזונו. אולם מאמרו של דיפי התגלגל לידי רונלד ריבסט ב-MIT, ועורר בו התלהבות גדולה. הוא שכנע את עדי שמיר ממכון ויצמן, ששהה ב-MIT באותו זמן ואת ליאונרד אדלמן, גם הוא מ-MIT, לסייע לו במציאת המתמטיקה הדרושה, כדי להפוך רעיון זה למציאות שיטת RSA, שפיתחה השלישייה המבריקה הזאת, פתרה הן את הבעיה של אימות הזהות של המתקשר בקצה השני שלהקו והן את בעיית חילופי המפתח.

בנוסף לפתרון שתי הבעיות האלה, האלגוריתם RSA פתר בעיה נוספת, בעיית ריבוי המפתחות. בסעיף 11.2 בחוברת הראשונה, בדיון על מגבלות ההצפנה הסימטרית, הראינו את חומרתה של הבעיה. הראינו כי  $n$  משתמשים זקוקים ל- $n(n-1)/2$  מפתחות, כדי לתקשר ביניהם ללא מגבלות. במערכת הצפנה אסימטרית, שעובדת עם האלגוריתם RSA, הם נזקקים רק ל- $n$  זוגות של מפתחות. לדוגמה, אלף ( $10^3$ ) משתמשים במערכת הצפנה סימטרית, זקוקים לחצי מליון מפתחות בקירוב ( $1000*999/2$ ).

אפשר לנסח את הכלל כי היחס בין מספר המפתחות לו נזקקים המשתמשים בשתי השיטות הוא:

$$\frac{\frac{n(n-1)}{2}}{2n} = \frac{n(n-1)}{4n} = \frac{n-1}{4}$$

כאשר מדובר ב- $10^3$  משתמשים, מספר המפתחות לו יזדקקו אם הם מצפינים בשיטה הסימטרית, גדול פי 250 ממספר המפתחות הדרושים בשיטת הצפנה אסימטרית. (הערה: בהמשך נטפל בבעיה זו בפירוט נוסף וביתר דיוק). בכל אופן, כל הסיבות שמנינו הפכו את RSA לשיטת ההצפנה המקובלת ביותר בעידן הדיגיטלי.

## 6.2 אלגוריתם RSA: שימוש בפונקצית RSA להצפנה אסימטרית

### 6.2.1 הקדמה

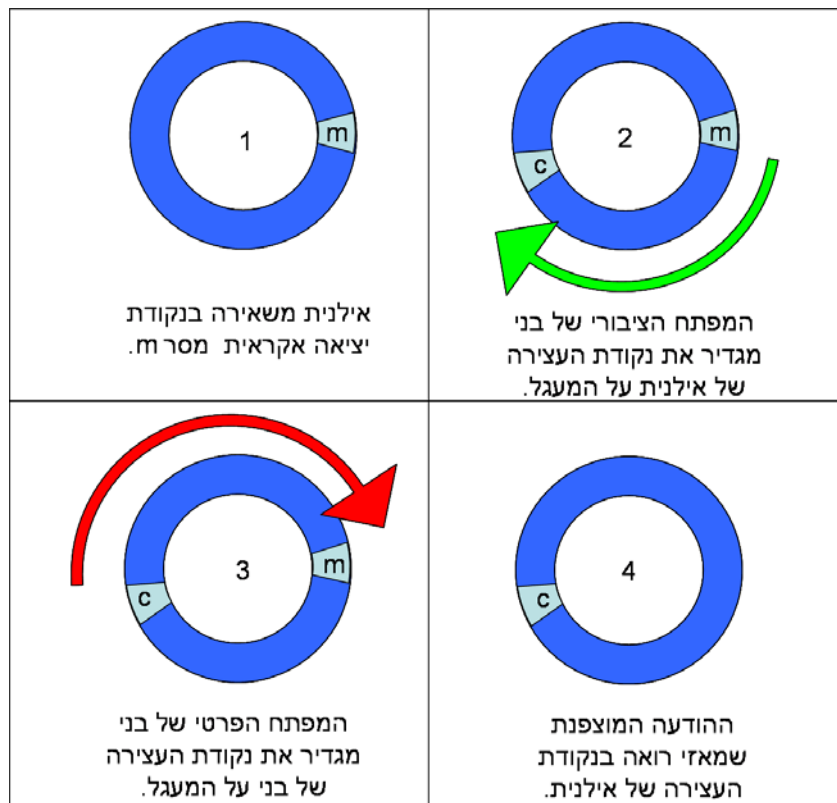
בראשית הפרק הכרנו זוגות שונים של מפתחות אסימטריים. זוגות של מפתחות (מספרים), שהם הפכיים כפליים, במודול מסוים. ראינו שהאלגוריתם של הכפל המודולרי אינו בעל סיבוכיות מספקת ליצירת הצפנות, ברגע שגילינו את האלגוריתם של אוקלידס, שגובר עליו. בסעיפים הבאים נכיר אלגוריתם הצפנה נוסף ומקובל ביותר, ה-RSA, ונראה על מה מבוססת הסיבוכיות שלו ומה הבעיות של תכנון אלגוריתם לפענוח RSA. ההצפנה באלגוריתם RSA מבוססת על חשבון מודולרי, על פונקציות מעריכיות וגם על תורת המספרים הראשוניים. אחרי אלפי שנים של שעשועים במספרים הראשוניים, שריתקו מתמטיקאים בכל הדורות רק מטעמי סקרנות, נמצא למספרים האלה שימוש בעל ערך עצום.

### 6.2.2 משל להמחשת ההצפנה באלגוריתם של RSA

כמו שאמרנו, RSA הוא אלגוריתם הצפנה אסימטרי. את המתמטיקה שלו אפשר לדמות לכזו שמתרחשת על מסילה מעגלית. על המסילה המעגלית נוסעת רכבת מיוחדת. זו הרכבת **היחידה** שיכולה לנוע על המסילה. הרכבת הזו נעה **רק קדימה** ולעולם לא תנוע לאחור. אורך המסילה אלפי מטרים ולארכה, בכל מטר, מונחת תיבה. מספר עצום של תיבות, לאורכו של המסלול המעגלי. מסילה כזו יש לכל אחד מהמשתמשים באלגוריתם ההצפנה שאנו עומדים להכיר, שנקרא RSA. כדי לנוע ברכבת, מספיק לדעת להשתמש במפתח הציבורי של בעל המסילה. המפתח הציבורי קובע איזה מרחק על המסילה, צריך הנוסע לעבור.

כשאלנית רוצה לשלוח מסר לבני, היא ניגשת למסילה שלו, היא יכולה לגשת לכל אחת מן התיבות המונחות לאורך המסילה, לא חשוב לאיזו מהן. היא בוחרת, באקראיות מוחלטת, תיבה מסוימת, שנסמן אותה באות  $m$ , ומשאירה בה את המסר. בנקודה זו עולה אילנית על הרכבת ("כרטיס הנסיעה" שלה הוא המפתח הציבורי של בני, השימוש במפתח הפומבי של בני משול בסיפור שלנו לנסיעה ברכבת בהתאם לכרטיס שמנפיק בני). היא נוסעת מרחק מסוים - עד לנקודה C (הנקבעת על ידי מפתח זה). בנקודה זו, יורדת אילנית מן הרכבת.

בדיוק באותה נקודה בה ירדה אילנית מן הרכבת, עולה בני על הרכבת. הוא עובר מרחק מסוים (על פי הוראת המפתח הפרטי שלו) ויורד מן הרכבת. התחבולה היא, שהמפתח הפרטי והציבורי מתאימים זה לזה כך, **שסכום המרחקים שעברו אילנית ובני בנסיעתם, שווה לארכה הכולל של המסילה. לכן בני מסיים את נסיעתו (ויורד מן הרכבת), באותה נקודה, שבה אילנית החלה את נסיעתה (עלתה על הרכבת), ב-m. ביחד השלימו הקפה. בני יורד מן הרכבת בדיוק ליד התיבה בה הטמינה אילנית את המסר. התבוננו בשרטוט שמדגים זאת.**



מאזי רוצה, כמובן, "לפתוח" את התיבה  $m$  ולגלות את המוצפן בה. האם היא יכולה לעשות זאת? נניח ש"מאזי" רואה את אילנית יורדת ב- $C$ , (היא יודעת מהו המפתח הציבורי של בני וגם המסר המוצפן זמין לה) אבל היא אינה יודעת היכן **החלה** אילנית את מסעה (היא אינה יודעת את  $m$ ). היא יכולה אמנם לפתוח את כל התיבות שלאורך המסילה, עד שתמצא את  $m$ , אבל יש מיליונים כאלה והבדיקה תמשך פרק זמן כל כך ארוך, שכל חייה לא יספיקו לכך. היא גם אינה יכולה לעלות על הרכבת ולנסוע חזרה בעקבותיה של אילנית, כיוון שהרכבת לעולם לא נעה אחורנית. אילו ידעה מאזי את ממדי המסילה, אולי יכלה לחשב, על ידי שימוש במפתח הציבורי, איך תשוב על עקבותיה, גם ללא הרכבת ותחלץ את המסר ששלחה אילנית לבני. אבל אורך מסלול הנסיעה של אילנית עצום ולרשותה של מאזי רק סרגל, שארכו מוגבל מאוד. זה ייארך לה הרבה יותר מדי זמן, לבצע את כל המדידות הדרושות. **הסיבוכיות של הבעיה גדולה מאד.** הסיבוכיות, היא שמונעת ממאזי לגלות את  $m$ . עד כאן המשל של מסילת הרכבת, ומהו הנמשל? שיטת ההצפנה של ה-RSA ומשפטי פרמה ואוילר, עליהם היא מתבססת.

### 6.2.3 אוילר ופרמה על המסילה המעגלית

כיצד יסייעו לנו משפטי פרמה ואוילר (סעיפים 4.10.1, 4.10.2), בניווט המסע על המסילה המעגלית? נסכם בקיצור את המשל. אילנית התחילה את מסעה ב-  $m$ , נסעה מרחק מסוים  $(y)$ , בהתאם להוראת המפתח הציבורי של בני וירדה ב-  $c$ . בני עלה ב-  $c$ , נסע מרחק מסוים  $(x)$ , בהתאם להוראת המפתח הפרטי שלו וסיים את מסעו ב-  $m$  – נקודת ההתחלה. והנמשל, כאמור, הצפנה אסימטרית בעזרת משפטי אוילר ופרמה. נראה, שאפשר למצוא הקבלה מרתקת בין נתוני המסע ובין העובדות שגילינו בדוגמה המספרית (בסעיף 4.10.3), כשחישבנו את החזקות של 7 במודול 55 בעזרת משפט אוילר. נסכם את ההקבלה בטבלה:

| המשל: הנסיעה על המסילה המעגלית          | הנמשל: חישוב החזקות של 7 ב- $\text{mod } 55$         |
|-----------------------------------------|------------------------------------------------------|
| אורך הקפה אחת של המסילה                 | ערכו של המודול – $n = 55$                            |
| נקודת העלייה של אילנית על הרכבת         | הייצוג המתמטי של המסר – $m = 7$ (בסיס החזקה)         |
| כרטיס הנסיעה של אילנית                  | המפתח הציבורי של בני – $e = 3$ (מעריך החזקה)         |
| הנסיעה (בהתאם לכרטיס)                   | ביצוע האלגוריתם (פעולת החזקה)                        |
| אורך המסע של אילנית                     | ערכה של החזקה ב"חשבון רגיל" – $y=7^3=343$            |
| נקודת הסיום של אילנית על המסילה המעגלית | התשובה המודולרית של החזקה – $343 \text{ mod } 55=13$ |

אם "נוסעים בכרטיס 5", פרוש הדבר ( $e=5$ ),  $7^5=7*7*7*7*7$ ,  $7^5 \text{ mod } 55 = 16,807 \text{ mod } 55 = 32$ , כלומר, מסיימים ב- 32 על המסילה, מאותם שיקולים שקודם סיימנו ב- 13. **אם "נוסעים בכרטיס 41", מסיימים את המסע בנקודת ההתחלה, ב- 7. כיוון ש-  $7^{41} \text{ mod } 55=7$ .**

אבל איך יודעים שצריך "לנסוע בכרטיס 41", כדי להגיע לנקודת ההתחלה? האם אתם זוכרים מהו המיוחד למספר 41 בדוגמה שבדקנו? נזכר כיצד קבלנו אותו: המודול בו חישבנו את החזקות של 7 היה 55.

המודול הזה התקבל ממכפלת שני הראשוניים  $p=11$ ,  $q=5$ .  
וראינו שלפי אוילר ופרמה,  $m^{(p-1)(q-1)}=1$   
ולכן  $m^{(p-1)(q-1)+1}=m$

כלומר, ה"כרטיס" (המעריך),  $(p-1)(q-1)+1$ , הוא שמחזיר אותנו לנקודת ההתחלה (המסר המקורי).

**אבל בדוגמה שבדקנו  $41=(p-1)(q-1)+1$ .**

**לכן, המעריך 41 הוא שיחזיר אותנו לנקודת המוצא, למסר המקורי.**

אם רק נצליח לפצל, או לפרק את המסע של בני ואילנית לשני שלבים, (כפל מודולרי בזוג מספרים הפכיים), כך שסכום ה"כרטיסים" (המפתחות) שלהם יהיה 41, הם יהיו שני המפתחות שלנו, האחד להצפנה והאחר לפענוח.

## 6.2.4 פיצול המסע ובניית מפתחות

הנה כיצד אפשר לפרק את המסע לשני חלקים:

\* נמצא שני מספרים, נסמן את האחד  $e$  ואת האחר  $d$ ,

$$e \cdot d = (p-1)(q-1) + 1 \quad \text{כך ש:}$$

\* אילנית עולה ב-  $m$ , יש לה כרטיס  $e$ , היא נוסעת  $m^e$  ומגיעה ל-  $c$ . בני עולה במקום שאילנית סיימה

את מסעה, יש לו כרטיס  $d$ , הוא נוסע  $c^d$ , ומגיע בחזרה ל-  $m$ . מניין אנחנו יודעים זאת?

\* הביטוי המתמטי לפעולה של אילנית:  $m^e \bmod n \rightarrow c$

\* הביטוי המתמטי לפעולה של בני:  $c^d \bmod n \rightarrow m$

\* אמרנו שבני עלה ב-  $c$ , הנקודה בה ירדה אילנית. הוא נסע  $c^d$

\* אנחנו יודעים כי הנקודה בה ירדה אילנית  $c = m^e \bmod n$

\* לכן נוכל לרשום במקום  $c$ ,  $m^e \bmod n$

\* לפי חוקי החזקות של הכפל המודולרי, נקבל  $c^d = (m^e \bmod n)^d = (m^e)^d$

\* היינו  $m^{e \cdot d} \bmod n$

\* אבל  $e \cdot d = (p-1)(q-1) + 1$

\* לכן המרחק שבני נוסע הוא  $m^{(p-1)(q-1)+1}$

ואז הוא מגיע ל:  $m^{(p-1)(q-1)+1} \bmod n$

\* מה זה????? זה פשוט  $m$  עצמו (כמו שלמדנו ממשפטי פרמה ואילר).

כשבני מבצע את החישובים, הוא לא ממש מחליף, את  $c$  ב-  $m^e$ . הוא פועל על  $c$  וזה כמו לפעול על  $m^e$  כיוון

שהם זהים זה לזה.

$$\begin{aligned} C = m^e & \xrightarrow{e \cdot d = (p-1)(q-1) + 1} m^{e \cdot d} = m^{(p-1)(q-1) + 1} \\ C^d & \xrightarrow{\quad} (m^e)^d \xrightarrow{\quad} m^{ed} \xrightarrow{\quad} m^{(p-1)(q-1) + 1} \\ & m^{(p-1)(q-1) + 1} \bmod n = m \bmod n \\ & c^d \bmod n = m \end{aligned}$$

לכן

## 6.2.5 הדוגמה המספרית

נחזור לדוגמה המספרית  $p=5, q=11, n=55$

$$(p-1)(q-1) + 1 = 41$$

אנחנו רוצים למצוא את  $e$  ו-  $d$  כך ש:  $e \cdot d = 41$

כאן מצפות לנו חדשות רעות. אין בנמצא זוג מספרים שמכפלתם שווה ל- 41, כיוון ש- 41 הוא מספר ראשוני. האם פרוש הדבר הוא, שאיננו יכולים להשתמש ב-  $p$  וב-  $q$  שמצאנו? אנחנו בהחלט יכולים להשתמש בהם, כיוון שיש דרך לעקוף את הקושי.

זכרו שאנחנו עוסקים בחשבון מודולרי. ובחשבון מודולרי, כשמגיעים למודול מתחילים מהתחלה. כלומר, שאם נבחר את 40 כמודול, אזי נקבל  $41 \bmod 40 = 1$ .

במילים אחרות, צריך לחפש  $d$  ו- $e$  כאלה, כך ש:

$$(e * d) \bmod 40 = 1$$

כלומר, צריך לחפש זוג מספרים, שהם הפכיים כפליים במודול 40. בחוברת הקודמת מצאנו הפכיים כפליים, מודולריים, ששמשו כמפתחות הצפנה. מצאנו אותם על ידי בניית לוח הכפל במודול זה. אחר כך בסעיף 4.8, למדנו למצוא הפכי כפלי בעזרת האלגוריתם של אוקלידס. כזכור לכם, רק מספרים, שהם הפכיים כפליים זרים למודול (סעיף 4.9), מתאימים לשמש כמפתחות הצפנה. לכן נחפש את הזוג של ההפכיים הכפליים במודול 40, בלוח הכפל של המספרים הזרים ל-40. כיוון ש:  $40 = 2 * 2 * 2 * 5$  יכלול לוח הכפל שנבנה רק מספרים קטנים מ-40, שאינם כפולות של 2, או של 5.

לוח הכפל של המספרים הזרים ל-40, במודול 40

|    | 0 | 1  | 3  | 7  | 9  | 11 | 13 | 17 | 19 | 21 | 23 | 27 | 29 | 31 | 33 | 37 | 39 |
|----|---|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|
| 0  | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  |
| 1  | 0 | 1  | 3  | 7  | 9  | 11 | 13 | 17 | 19 | 21 | 23 | 27 | 29 | 31 | 33 | 37 | 39 |
| 3  | 0 | 3  | 9  | 21 | 27 | 33 | 39 | 11 | 17 | 23 | 29 | 1  | 6  | 13 | 19 | 31 | 37 |
| 7  | 0 | 7  | 21 | 9  | 23 | 37 | 11 | 39 | 13 | 27 | 1  | 29 | 3  | 17 | 31 | 19 | 33 |
| 9  | 0 | 9  | 27 | 23 | 1  | 19 | 37 | 33 | 11 | 29 | 7  | 3  | 21 | 39 | 17 | 13 | 31 |
| 11 | 0 | 11 | 33 | 37 | 19 | 1  | 23 | 27 | 9  | 31 | 13 | 17 | 39 | 21 | 3  | 7  | 29 |
| 13 | 0 | 13 | 39 | 11 | 37 | 23 | 9  | 21 | 7  | 33 | 19 | 37 | 17 | 3  | 29 | 1  | 27 |
| 17 | 0 | 17 | 11 | 39 | 33 | 27 | 21 | 9  | 3  | 37 | 31 | 19 | 13 | 7  | 1  | 29 | 13 |
| 19 | 0 | 19 | 17 | 13 | 11 | 9  | 7  | 3  | 1  | 39 | 37 | 33 | 31 | 29 | 27 | 23 | 21 |
| 21 | 0 | 21 | 23 | 27 | 29 | 31 | 33 | 37 | 39 | 1  | 3  | 7  | 9  | 11 | 13 | 17 | 19 |
| 23 | 0 | 23 | 29 | 1  | 7  | 13 | 19 | 31 | 37 | 3  | 9  | 21 | 27 | 33 | 39 | 11 | 17 |
| 27 | 0 | 27 | 1  | 29 | 3  | 17 | 31 | 19 | 33 | 7  | 21 | 9  | 23 | 37 | 11 | 39 | 13 |
| 29 | 0 | 29 | 7  | 3  | 21 | 39 | 17 | 13 | 31 | 9  | 27 | 23 | 1  | 19 | 37 | 33 | 11 |
| 31 | 0 | 31 | 13 | 17 | 39 | 21 | 3  | 7  | 29 | 11 | 33 | 37 | 19 | 1  | 23 | 27 | 9  |
| 33 | 0 | 33 | 19 | 31 | 17 | 3  | 29 | 1  | 27 | 13 | 39 | 11 | 37 | 23 | 9  | 21 | 7  |
| 37 | 0 | 37 | 31 | 19 | 13 | 7  | 1  | 29 | 23 | 17 | 11 | 39 | 33 | 27 | 21 | 9  | 3  |
| 39 | 0 | 39 | 37 | 33 | 31 | 29 | 27 | 13 | 21 | 19 | 17 | 13 | 11 | 9  | 7  | 3  | 1  |



## שאלה מספר 1

- א. סמנו את כל ה-1ים בלוח הכפל המודולרי.
- ב. כמה זוגות של הפכיים כפליים מצאתם?
- ג. האם קיימת חוקיות בסידורם בלוח הכפל המודולרי?

נניח שנבחר בזוג ההפכי 3 ו-27.

$$(3 \cdot 27) \bmod 40 = 1$$

הכל נראה תקין, אבל רגע אחד, איך קפצנו מ- $\bmod 55$  ל- $\bmod 40$ ? זוהי בדיוק התחבולה של ה-RSA, השימוש בשני מודולים, האחד ליצירת המפתחות והאחר להצפנה ולפענוח. המודול להצפנה ולפענוח הוא  $p \cdot q$  והמודול ליצירת זוג המפתחות הוא  $(p-1)(q-1)$ .

## 6.2.6 תאור האלגוריתם RSA

- צעד ראשון: בוחרים שני מספרים ראשוניים  $p$  ו- $q$ .
- צעד שני: כופלים את הראשוניים זה בזה,  $n = p \cdot q$ .
- צעד שלישי: כופלים אותם בדרך שונה  $\phi(n) = (p-1)(q-1)$ .
- צעד רביעי: השימוש ב- $\phi$  מגדיר את זוג המספרים (המפתחות)  $e$  ו- $d$ .
- צעד חמישי: מפרסמים את המפתח הציבורי  $(n, e)$  ושומרים את המפתח הפרטי  $d$ .
- צעד שישי: הצפנה - לשם הצפנה של  $m$  צריך להתקיים  $m < n$ ,  $m$  ו- $n$  זרים. מחשבים  $c = m^e \bmod n$ .
- צעד שביעי: פענוח - לשם פענוח של  $c$  משתמשים במפתח הפרטי  $d$ . מחשבים  $m = c^d \bmod n$ .

בדוגמה שראינו:  $p=5, q=11, \phi=40, n=55, e=3, d=27$

כלומר, מודול ההצפנה הוא 55. המודול ליצירת המפתחות הוא 40. המפתחות הם 3 ו-27 (3 הוא חלק מהמפתח הציבורי ו-27 הוא חלק מהמפתח הפרטי). זכרו שכאשר דברנו על הפכיים, הכרנו פעולות הפוכות זו לזו ומספרים הפכיים, ביחס לפעולה מסוימת. בדוגמה שהצגנו עשינו שימוש במספרים הפכיים ביחס לפעולה:

3 ו-27 הם הפכיים ביחס לכפל  $\bmod 40$ .

$$(3 \cdot 27) \bmod 40 = 1$$

ברגע שיצרנו את המפתחות אין יותר צורך במספר 40, אפשר לזרוק אותו. אבל יש להבטיח, כמובן, שאף אחד לא ימצא אותו.

## שאלה מספר 2

בטבלה הבאה יש תרגילי הצפנה ופענוח באמצעות אלגוריתם RSA, השלימו אותה. (זכרו לבחור  $m < n$ ):

| p | q | n | $\Phi(n)$ | e | d | m | $m^e \bmod n = c$ | $c^d \bmod n = m$ |
|---|---|---|-----------|---|---|---|-------------------|-------------------|
| 2 | 7 |   |           |   |   | 2 |                   |                   |
| 5 | 3 |   |           |   |   | 3 |                   |                   |
|   |   |   |           |   |   |   |                   |                   |

### 6.2.7 הצפנת אותיות באלגוריתם RSA

נשתמש בדוגמה המספרית מהסעיף הקודם לשם הצפנה באלגוריתם RSA. כעת אנחנו כבר יודעים את כל הדרוש לשם כך. נצפין, למשל, את האות T. לשם כך מקודדים אותה למספר ומצפינים את המספר.

כיוון שזו האות ה-20 בא"ב האנגלי, נשנה אותה למספר 19 (כאשר  $A=0$ ) ואותו נצפין.

ניקח  $q, p$ , שני מספרים ראשוניים: 5, 11.

$$n = p * q = 55$$

$$\phi(n) = (p - 1) (q - 1) = 40$$

$$m = 19, e = 3, d = 27$$

במקרה זה

$$m^e \bmod n = C$$

**הצפנה מחשבים את C:**

$$19^3 \bmod 55 = 39$$

כלומר

קבלנו את המסר המוצפן  $C = 39$

אם לחזור למשל המסילה המעגלית, היקפו של סיבוב אחד הוא 55 יחידות (זהו המודול). אילנית התחילה בנקודה כלשהי-19 "נסעה בכרטיס 3" וסיימה בנקודה 39. זה מצלצל מוזר, אבל תזכרו שהרכבת המיוחדת שלנו מבצעת פעולות מיוחדות - פעולות מודולריות.

$$C^d \bmod n = m$$

**בפענוח מחשבים את m:**

$$C = 39, d = 27$$

במקרה שלנו:

$$39^{27} \bmod 55$$

אנחנו צריכים לחשב

התוצאה אמורה להיות זהה למסר המקורי. כלומר, צריך להתקיים:

$$39^{27} \bmod 55 = 19$$

נבדוק זאת. לביצוע החישוב אפשר להיעזר בטבלת חזקות של 39, המופיעה בעמוד זה.

$$X^a * X^b = X^{a+b}$$

כדי לצרף אותן זכרו את הזהויות המעריכיות:

$$(X^a * X^b) \bmod n = X^a \bmod n * X^b \bmod n$$

$$(a * b) \bmod n = a \bmod n * b \bmod n$$

ואת הזהות המודולרית:

### חזקות נבחרות של 39

| מה מחשבים<br>$39^{a+b} = 39^a * 39^b$ | $39^a \bmod 55 * 39^b \bmod 55$ | תוצאת הכפל | התשובה המודולרית<br>$39^{a+b} \bmod 55$ |
|---------------------------------------|---------------------------------|------------|-----------------------------------------|
| $39^1 = 39$                           | 39                              | 39         | $39 \bmod 55 = 39$                      |
| $39^2 = 39^1 * 39^1$                  | $39 * 39$                       | 1521       | $1521 \bmod 55 = 36$                    |
| $39^4 = 39^2 * 39^2$                  | $36 * 36$                       | 1296       | $1296 \bmod 55 = 31$                    |
| $39^8 = 39^4 * 39^4$                  | $31 * 31$                       | 961        | $961 \bmod 55 = 26$                     |
| $39^{16} = 39^8 * 39^8$               | $26 * 26$                       | 676        | $676 \bmod 55 = 16$                     |

הסתכלו במה שרשום בטבלה. איך חישבנו למשל,  $39^8$ ?  
 על סמך הזהויות המעריכיות, אפשר לכתוב זאת גם כ-  $39^{4+4} = 39^4 * 39^4$   
 אבל  $39^4 \bmod 55 = 31$   
 ולכן  $39^8 \bmod 55 = (39^4 * 39^4) \bmod 55 = 39^4 \bmod 55 * 39^4 \bmod 55 =$   
 $= 31 \bmod 55 * 31 \bmod 55 = (31 * 31) \bmod 55$   
 בעזרת הטבלה נחשב גם  $39^{27}$   
 $39^{27} = 39^{16} * 39^8 * 39^2 * 39$   
 $39^{27} \bmod 55 = (16 * 26 * 36 * 39) \bmod 55$   
 $= 584,064 \bmod 55 = 19$

נסכם שוב את התהליך: אילנית התחילה את מסעה (את ההצפנה), על המסילה המעגלית (המודול) של בני  $(n=55)$ , בנקודה 19 (המסר המקורי  $m=19$ ), היא "נסעה בכרטיס 3" (הצפינה על ידי המפתח הציבורי של בני  $e=3$ ).

אורך המסע שעשתה על המסילה המעגלית,  $m^e = 19^3$ , הנקודה הסופית אליה הגיעה היא  $19^3 \bmod 55 = 39 = c$ . המספר 39 הוא המסר המוצפן.

בני התחיל את מסעו (את הפענוח) ב- 39 (המסר המוצפן), "נסע בכרטיס 27" (פענח על ידי המפתח הפרטי  $d=27$ ), על אותה המסילה המעגלית (מודול 55). אורך המסע שבצע (תוצאת ביניים)  $39^{27}$ , הוא סיים את המסע (את הפענוח) ב- 19 (התשובה המודולרית של החזקה,  $39^{27} \bmod 55 = 19$ ) בנקודת ההתחלה (במסר המקורי,  $m$ ).

## 6.2.8 משל המסילה והאלגוריתם של RSA

קעת כבר גיליתם בודאי, כי הפעולות שבצענו, אינן נסיעות לאורך חלקי מסילה. כל פעולה היא בדרך כלל, סיבובים רבים במסילה המעגלית. הרבה סיבובים שלמים ועוד קצת. התוספת הקטנה הזאת היא החשובה. אם משלימים סיבוב, חוזרים לנקודת ההתחלה. גם אם משלימים 100 או 1000 סיבובים, חוזרים לנקודת ההתחלה. במילים אחרות, דין סיבוב אחד כדין 100 או 1000 סיבובים. אבל כל מסע מסתיים בתוספת קטנה לכל הסיבובים. אם נחבר את התוספת הקטנה של המפתח הציבורי לתוספת הקטנה של המפתח הפרטי, התוצאה תהיה תמיד סיבוב שלם, כלומר חזרה לנקודת ההתחלה - לטקסט המקורי.

זהו האלגוריתם של RSA. נחזור בקצרה על כל שלביו:

1. בוחרים שני מספרים ראשוניים  $p$  ו- $q$ .
2. כופלים אותם זה בזה, נקרא לתוצאה  $n$ .
3. בוחרים כמערך ציבורי מספר זר ל- $(p-1)$  ול- $(q-1)$  ונקרא לו  $e$ . הזוג  $(e, n)$  הוא המפתח הציבורי.
4. מוצאים  $d$ , כך ש:  $d \cdot e \bmod (p-1)(q-1) = 1$ .  $d$  הוא המפתח הפרטי.
5. מפרסמים בציבור את  $n$  ואת  $e$ , ומחזיקים בסוד את  $d$  ואת  $p$  ו- $q$ .
6. בוחרים  $m < n$  וזר לו. כשמציפים את  $m$ , הטקסט המוצפן הוא  $C = m^e \bmod n$ .
7. כשמפענחים את  $C$ , מחלצים את  $m$  על ידי  $m = C^d \bmod n$ .

וביתר פירוט:

$$C^d \bmod n = (m^e \bmod n)^d \bmod n = m^{ed} \bmod n = m^{(p-1)(q-1)+1} \bmod n = m$$

**נסכם את השלבים:**

שנו לאות פענחו במפתח פרטי הצפינו במפתח ציבורי שנו למספר התחילו באות  
 $s \xrightarrow{\hspace{1cm}} 19 \xrightarrow{\hspace{1cm}} 39 \xrightarrow{\hspace{1cm}} 19 \xrightarrow{\hspace{1cm}} s$

עליכם לזכור כי בתהליך מעורבים שני מודולים. כשבונים את  $d$  (המפתח הפרטי הסודי), משתמשים ב- $\bmod (p-1)(q-1)$ . וכשמציפים משתמשים ב- $\bmod p \cdot q$ .

## 6.3 פתרונות

### פתרון שאלה מספר 1:

ב. 16.

ג. הזוגות שאינם באלכסון סימטריים ביחס לאלכסון וכל אחד מהם מופיע פעמיים.

### פתרון שאלה מספר 2:

| p | q | n  | $\Phi(n)$ | e | d | m | $C = m^e \bmod n$  | $m = C^d \bmod n$  |
|---|---|----|-----------|---|---|---|--------------------|--------------------|
| 2 | 7 | 14 | 6         | 5 | 5 | 2 | $2^5 \bmod 14 = 4$ | $4^5 \bmod 14 = 2$ |
| 5 | 3 | 15 | 8         | 5 | 5 | 3 | $3^5 \bmod 8 = 3$  | $3^5 \bmod 8 = 3$  |

## 7 הגורמים שמשפיעים על מידת הבטיחות של RSA

עקבנו אחר כל השלבים של ביצוע הצפנת RSA. כעת נבחן מה מידת עמידותה של הצפנה זו בפני ניסיונות לפיצוחה.

### 7.1 מהם הצעדים הדרושים לפיצוח שיטת ההצפנה RSA

נניח ש"מאזי" גלתה את המסר המוצפן C. היא יודעת מהו n ומהו e, כלומר, היא יודעת מהו המפתח הפומבי. היא יודעת גם כי אלגוריתם ההצפנה הוא RSA. יש לה מידע רב. האם תוכל לחלץ את m, כיצד? הדרך היחידה הידועה לחשב את m (המסר), מ-C (המסר המוצפן), היא להשתמש במפתח הפרטי d. אבל כיוון שהוא סודי, "מאזי" אינה יודעת מהו. האם תוכל לגזור את d מ-n ו-e? האם תוכל לשבור את שיטת ההצפנה של RSA? נבחן בפירוט את בעייתה של מאזי:

#### מה רוצה "מאזי"?

(1) מאזי רוצה לגלות את m

היא יודעת ש:  $m = c^d$

ואת c היא יודעת.

(2) מאזי רוצה לגלות את d

היא יודעת ש:

$$(e \cdot d) \bmod (p-1)(q-1) = 1$$

ואת e היא יודעת

מה היא צריכה לעשות? לגלות את  $(p-1)(q-1)$

מה היא צריכה לעשות? לגלות את p ואת q

(3) מאזי רוצה לגלות את  $(p-1)(q-1)$

(4) מאזי רוצה לגלות את p ואת q

היא יודעת ש:  $pq = n$

הצפנה חלק ב

לפי (2), אם מאזי יודעת את  $(p-1)(q-1)$  אזי היא יכולה לפרק את n לגורמים. כלומר, היא יכולה לפצח את RSA.

דוגמה:

**בניח שמאזי יודעת ש:**  $n = 221$  ו-  $(p-1)(q-1) = 192$ . איך היא יכולה לגלות את p ואת q?  
כלומר, איך היא יכולה לפרק את n לגורמים?

פתרון:

$$n = pq = 221 \quad \text{נתון:}$$

$$\varphi(n) = (p-1)(q-1) = 192$$

$$(p-1)(q-1) = pq - p - q + 1 = pq - (p+q) + 1 = n - (p+q) + 1 = 192$$

$$p+q = n - 192 + 1 = 221 - 192 + 1 = 30$$

$$pq = p(30-p) = 30p - p^2 = 221$$

$$p^2 - 30p + 221 = 0$$

p ו- q מקיימים את מערכת המשוואות:

$$\begin{cases} p+q=30 & (1) \\ p^2-30p+221=0 & (2) \end{cases}$$

המשוואה השנייה שקבלנו היא משוואה ריבועית ולפתרונה יש נוסחה כללית, שאולי כבר הספקתם להכיר. מי שאינו מכיר יוכל למצוא את ההוכחה לפתרון בנספח. למשוואה שני פתרונות:

$$P_1 = \frac{30 + \sqrt{900 - 884}}{2} = \frac{30 + 4}{2} = 17$$

$$P_2 = \frac{30 - \sqrt{900 - 884}}{2} = \frac{30 - 4}{2} = 13$$

אם  $p=17$ , אז לפי משוואה (1),  $q=13$ .

אם  $p=13$ , אז לפי משוואה (1),  $q=17$ .

לפיכך, זוג הפתרונות שלנו הוא 13, 17.

כמו כן:

$$pq = 17 \times 13 = 221 = n$$

$$(p-1)(q-1) = 16 \times 12 = 192$$

נוכחנו שאם מאזי יודעת את  $(p-1)(q-1)$  היא יכולה לפרק את n לגורמים.

**אבל אם מאזי אינה יודעת את  $(p-1)(q-1)$** , מה הסיכוי שלה לפרק את  $n$  לגורמים, אם  $n$  הוא מספר בן מאות או אלפי ביטים? מה הסיכוי, אם כל מה שהיא יודעת על זוג הגורמים הוא, שהם מספרים ראשוניים גדולים מאד וקרובים זה לזה במספר הספרות שלהם? מידת הקושי של משימתה היא הקובעת את הבטיחות של הצפנת RSA.

אבל הקושי של משימתה של מאזי תלוי ביכולתם של המצפינים למצוא מספרי ענק ראשוניים. שתי הבעיות אינן פשוטות, בלשון המעטה. פתרונותיהם בעלי סיבוכיות גבוהה. מי ינצח בקרב בין המצפינים למפצחים? זה שיצליח לבנות אלגוריתם בעל סיבוכיות נמוכה יותר משל יריבו, לפתרון הבעיה.

## 7.2 משימות המצפינים והמפצחים בשיטת RSA

כדי לברר את גורמי הבטיחות של RSA, אנחנו צריכים לחקור כעת, מהי הסיבוכיות של משימות המצפינים, כשהם יוצרים את המפתח, לעומת אלה של המפצחים, בשיטת RSA.

### 7.2.1 מהי משימתם הראשונה של המצפינים בשיטת RSA?

ראינו, שכדי לבנות את מערכת ההצפנה RSA, המצפינים צריכים למצוא שני מספרים ראשוניים גדולים מאוד  $p$  ו- $q$ . שני המספרים הראשוניים הגדולים קרובים זה לזה במספר הספרות שלהם. מכפלתם  $n$  היא אחד מנתוני המפתח הציבורי. נוכחנו כי הבעיה של מציאת זוג ראשוניים גדולים, קרובים זה לזה, אינה קלה, בהמשך דיוננו ננסה לגלות מהי הסיבוכיות של פתרונה.

### 7.2.2 מהי משימתם של אלה שמנסים לפצח הצפנת RSA?

ראינו שהמפצחים, שרוצים לגלות את  $p$  ו- $q$  (הגורמים של המכפלה- $n$ ), צריכים לפרק לגורמים את  $n$ . גם כאן עומד הניסיון לעזרתנו. אנו יודעים מניסיונו, כי לא כל מספר פריק קשה לפרק לגורמים. אם הגורמים הם מספרים קטנים, הפרוק לגורמים פשוט וקל. אבל כאשר המספר הפריק גדול מאד (בן מאות ספרות), כאשר הוא מתפרק רק לשני גורמים, כאשר זוג הגורמים הם מספרים קרובים במספר הספרות שלהם, כלומר ששניהם מספרים גדולים, אזי המשימה הרבה יותר קשה. בהמשך נברר גם את הסיבוכיות של פירוק לגורמים.

נסכם את מצב המצפינים והמפצחים בשיטת RSA:

בעיית המצפינים, כשהם יוצרים את המפתח, היא למצוא ראשוניים גדולים בעלי התכונות שהזכרנו. בעיית המפצחים היא לפרק מספר גדול לשני גורמים ראשוניים.

האבטחה של מערכות ההצפנה תלויה לחלוטין בשאלות התאומות: מחד, עד כמה קל לזהות ראשוני ומאידך, מה מידת הקושי של פירוק מספר פריק אקראי, לזוג גורמים ראשוניים, קרובים זה לזה בגודלם. הפתרונות של שתי הבעיות התאומות הם בעלי סיבוכיות, אבל לא אותה סיבוכיות. מתברר שקיים הבדל גדול בין הסיבוכיות של מציאת ראשוניים גדולים ובין הפירוק לגורמים של מספרים שנוצרו על ידי מכפלת ראשוניים גדולים.

מערכת ההצפנה של RSA מבוססת על ההבדל הגדול בסיבוכיות של פתרון שתי הבעיות האלה. בניסוח מקוצר נוהגים לומר, כי שיטת RSA מבוססת על ההבדל הגדול שבין הסיבוכיות של הפירוק לגורמים ובין הסיבוכיות של בדיקת ראשוניות. בהמשך נבחן את מידות הסיבוכיות של פתרון שתי הבעיות האלה.

### 7.3 הסיבוכיות של פרוק לגורמים

כדי לפרק מספר  $n$  לגורמים, צריך למצוא את כל המחלקים הראשוניים שלו. פרוק מספר כמו 15 נעשה בקלי קלות. אנו יודעים, כי הוא מתחלק ללא שארית ב-3 וב-5. אבל תארו לעצמכם שצריך לפרק לגורמים מספר גדול הרבה יותר.



#### שאלה מספר 1

פרקו לגורמים ראשוניים את המספר 13,860



#### שאלה מספר 2

פרקו לזוג גורמים את המספר 3,599



#### שאלה מספר 3

פרקו לזוג גורמים את המספר 32,399

אתם רואים שאם יש למספר הנבדק הרבה גורמים קטנים, הפירוק לגורמים שלו קל יותר, מאשר פרוק לגורמים של מספר שנבנה משני גורמים ראשוניים בלבד. למשל, מה דעתכם על הסיבוכיות של הפירוק לגורמים של המספר 6,320,491,217? זהו מספר בן 10 ספרות בלבד, אבל, אפשר להוכיח, שכבר הפרוק

לגורמים שלו מהווה בעיה לא פשוטה כלל. אם נרצה לפרק לגורמים מספר בן 300 ספרות, הסיבוכיות, כמובן, הרבה הרבה יותר גדולה. אנו נזדקק לשם כך למיליוני שנים, במחשבים המוכרים לנו. אנו נאלצים להכיר בכך, שבמונחים שכבר הכרנו, בעיית הפרוק לגורמים של מספר גדול היא בלתי סבירה. לכן יכולים המצפינים לפרסם בביטחון את  $n$  והמפצחים חורקים שיניים, אך אינם מצליחים לפרק אותו לזוג הגורמים הראשוניים מהם נוצר.

חשוב לציין, כי בעקבות התרחבות השימוש ב-RSA, חלה התפתחות עצומה בפיתוח אלגוריתמים של פרוק לגורמים ובפיתוח מבנים של מערכות מחשבים העובדים במקביל על אותה בעיה. כיום מכירים אלגוריתמים של פירוק לגורמים, שהם הרבה יותר טובים מאלה שהכירו בעבר, אבל כולם עדיין לא סבירים. לכן פתרון בעיית הפרוק לגורמים נותר, עדיין, לא סביר.

זהו אם כן מצבם הקשה של המפצחים, אבל מה לגבי המצפינים? כמו שראינו גם הם ניצבים בפני בעיה. הם צריכים לבחור שני מספרים ראשוניים גדולים. לשם כך הם צריכים לקבוע האם מספר מסוים בו הם רוצים להשתמש הוא ראשוני. מה מידת הסיבוכיות של הבעיה שלהם? מהי הסיבוכיות של בדיקת ראשוניות של מספר? נבדוק זאת בסעיף הבא.

## 7.4 על מספרים ראשוניים ועל הסיבוכיות של בדיקת ראשוניות

### 7.4.1 היכרות עם המספרים הראשוניים

מספרים ראשוניים גדולים הם לחם חוקם של המצפינים ב-RSA. לכן לפני שנדון בשיטות לבדיקת ראשוניות, נפתח בדיון כללי על המספרים הראשוניים ונשפר את היכרותנו עמם.

לחקר הראשוניים מקום חשוב בתורת המספרים. תחום זה נחשב בעבר, ל"טהור" לחלוטין (חסר משמעויות יישומיות). אך כיום, כמו שכבר נוכחנו, הוא תופס מקום חשוב ביותר במדעי המחשב.

ראינו שלכל המספרים הראשוניים תכונה משותפת, הם מתחלקים בעצמם וב-1 בלבד.

בדומה ליסודות הכימיים ולחלקיקים האלמנטריים בפיסיקה, המספרים הראשוניים הם אבני היסוד של המספרים השלמים. כל המספרים השלמים הלא ראשוניים, המספרים הפריקים, ניתנים להיכתב כמכפלות של ראשוניים.

אבל, בעוד שהכימאים מטפלים ב-100 יסודות (בקירוב) בלבד, מתברר, שהמתמטיקאים נאלצים לטפל באספקה אינסופית של מספרים ראשוניים. כבר לפני 2000 שנה הוכיח אוקלידס כי מספר הראשוניים הוא אינסופי, ומאז נתונים המתמטיקאים במרדף, שגם לו אין סוף, לאיתורם.

הנימוק של אוקלידס, למציאותם של אינסוף ראשוניים, מאלף. הוכחתו נסמכת על כך, שמסקנתה סותרת את הנחת המוצא שלה ולכן גוררת את שינוי הנחת המוצא. מהלכה כדלקמן: נניח שקיים מספר **סופי** של ראשוניים, נסמן את הגדול שבהם ב- $p$ . נכפיל את כל הראשוניים עד  $p$  זה בזה. למספר הענק שקבלנו נוסיף 1 ונסמנו ב- $N$ . מה אפשר לדעת על  $N$ ? הוא גדול מ- $p$  כיוון ש- $p$  הוא רק אחד הגורמים של  $N$ .  $N$  אינו יכול להיות ראשוני כיוון שאז הוא הראשוני הגדול ביותר וזה סותר את הנחת היסוד שלנו. אבל  $N$  גם לא יכול

להיות מספר פריק, בגלל הדרך שבה בנינו אותו (אם ננסה לפרק אותו לגורמים, על ידי חילוקו בכל אחד מן הראשוניים המוכרים, נקבל תמיד שארית 1). בכך נסתרה הנחת המוצא כי מספר הראשוניים סופי. המסקנה היא – **מספר הראשוניים אינסופי**.

לכאורה, אם מספר הראשוניים הוא כל כך גדול, אז מציאת ראשוני אחד אינה צריכה להוות בעיה. אבל מתברר שכאן מתעוררת בעיה נוספת. נבדוק אותה.

#### שאלה מספר 4

רשמו את המספרים הראשוניים עד 100.

#### שאלה מספר 5

השלימו את הטבלה

| מספר הראשוניים | המספרים בין: |
|----------------|--------------|
|                | 1-10         |
|                | 11-20        |
|                | 21-30        |
|                | 31-40        |
|                | 41-50        |
|                | 51-60        |
|                | 61-70        |
|                | 71-80        |
|                | 81-90        |
|                | 91-100       |
|                | 101-110      |

#### שאלה מספר 6

- באיזה עשרות הצפיפות של הראשוניים היא הגדולה ביותר?
- באיזה עשרות היא השניה בגודלה?
- באיזה עשרות היא הקטנה ביותר?

מן הבדיקות המעטות שערכתם לא יכולתם להיווכח, שיש חוקיות לפיזורם של המספרים הראשוניים, בין השלמים. אבל כשמבצעים בדיקות רבות, אפשר לגלות חוקיות מסוימת. היא רשומה בטבלה שלהלן:

| השלמים מ...עד... | מספר הראשוניים מביניהם |
|------------------|------------------------|
| 1-10             | 4                      |
| 1-100            | 26                     |
| 1-1000           | 168                    |
| 1-10,000         | 1229                   |
| 1-100,000        | 9,592                  |

אחד מגדולי המתמטיקאים, גאוס (Karl Fridrich Gauss 1777-1855) מצא חוקיות כזו. הוא הראה ששיעור הראשוניים יורד על פי נוסחה כמתואר בטבלה הבאה:

| המספרים מ...עד... | שיעור הראשוניים מביניהם |
|-------------------|-------------------------|
| $1-10^1$          | 1:2.5                   |
| $1-10^2$          | 1:4                     |
| $1-10^3$          | 1:6                     |
| $1-10^4$          | 1:8.1                   |
| $1-10^5$          | 1:10.4                  |
| $10^n$            | $1:2.3n \sim$           |

אחרי גאוס הוכנסו בנוסחה זו שיפורים אבל אנחנו נסתפק בה.

## שאלה מספר 7

- א. מהו, לפי גאוס, מספר הראשוניים הקטנים מ- $10^6$ ,  $10^{10}$ ,  $10^{20}$ ?
- ב. מהו, לפי גאוס, מספרם של הראשוניים בין השלמים הקטנים מ- $10^{12}$ ?

לכן, אם נבחר מספר אקראי, שמספר הספרות שלו  $n$ , הסיכוי שהוא ראשוני אינו זניח והוא יחסי למספר הספרות שלו. גודלו של הסיכוי הוא  $1/2.3n$ , הסיכוי למציאת מספר ראשוני בן 1000 ספרות, הוא  $1/2300$ . בעיית ההצפנה היא בניית ראשוני יחיד ולכן המידע על גודל הסיכוי למציאתו הוא חשוב. מהוכחתו של אוקלידס נובעת שיטה אחת לבניית ראשוניים: הכפלת ראשוניים עד ערך מסוים והוספת 1 למכפלה. האם בשיטה זו המספר שמתקבל הוא באמת תמיד ראשוני?



## שאלה מספר 8

נסו לבנות מספרים ראשוניים בשיטתו של אוקלידס:

- א. על ידי מכפלת שלושת הראשוניים הראשונים ותוספת 1 למכפלה.
- ב. על ידי מכפלת ארבעת הראשוניים הראשונים ותוספת 1 למכפלה.
- ג. על ידי מכפלת חמשת הראשוניים הראשונים ותוספת 1 למכפלה.
- ד. על ידי מכפלת ששת הראשוניים הראשונים ותוספת 1 למכפלה.
- ה. על ידי מכפלת שבעת הראשוניים הראשונים ותוספת 1 למכפלה.

האם השיטה עובדת?

כבר מן הבדיקות המעטות שערכנו אפשר להיווכח, כי שיטתו של אוקלידס, לא יוצרת תמיד מספרים ראשוניים.

מתברר כי תחום המספרים הראשוניים, גם אם הוא נראה פשוט, בהחלט אינו כזה. זהו תחום מורכב, אך גם מרתק. הרבה שאלות, שקשורות אליו, לא מצאו עדיין תשובה. הנה מספר שאלות כאלה:  
האם קיימת שיטה כללית **אמינה**, ליצירת מספרים ראשוניים?

כשנתון מספר ראשוני, מה מרחקו מן הראשוני הבא אחריו? במילים אחרות, השאלה שכבר העלינו, האם יש **תבנית** לפיזורם של הראשוניים בין השלמים?

אנחנו מכירים זוגות של ראשוניים סמוכים זה לזה (כמו 3 ו-5, 41 ו-43, 191 ו-193), האם מספר הזוגות הראשוניים סופי? האם הוא אינסופי?

איש טרם מצא את התשובות, ואלה רק חלק מן השאלות הרבות וההשערות שמצפות להוכחה. לכן אמרנו, שתחום המספרים הראשוניים הוא נרחב ומרתק. אך במסגרת הדיון בהצפנת RSA נתרכז רק בשתי שאלות מתוכן:

א. איך **יוצרים** (מוצאים) מספר ראשוני?

שיטת RSA בנויה על הצפנה באמצעות ראשוניים גדולים. כבר נזכרנו כי אין מחסור בראשוניים, מספרם אינסופי, אבל המצפינים נזקקים לשיטה שתייצר מספרים ראשוניים. מהי הסיבוכיות של אלגוריתם לייצור מספרים ראשוניים?

ב. כשנתון מספר, איך אפשר **לבדוק** האם הוא ראשוני?

נניח שיש לנו שיטה, שאמורה לייצר מספרים ראשוניים גדולים. איך אפשר להיות בטוחים, שהמספרים שנוצרו הם אמנם ראשוניים? כדי להיות בטוחים בכך יש לבדוק זאת, כלומר - לבדוק ראשוניות של מספר. מהי הסיבוכיות של בדיקת ראשוניות?

## 7.4.2 בדיקת ראשוניות של מספר

נניח שאנחנו רוצים לבדוק האם 97 הוא ראשוני. נבחן את כל המחלקים שלו. נתחיל מהקטן ביותר. האם 97 מתחלק ב-2? כיוון ש-97 אי זוגי ברור שהתשובה שלילית. האם הוא מתחלק ב-3? לא (בדקו), מה לגבי 4? האם 97 מתחלק ב-4? כיוון ש-4 הוא כפולה של 2 התשובה שלילית ואין צורך לבדוק. ומה לגבי 5? הבדיקה מורה שהתשובה שלילית. מה לגבי 6? האם 97 מתחלק ב-6? ללא בדיקה אפשר לקבוע שהתשובה שלילית (חשבו מדוע אפשר לקבוע זאת ללא בדיקה). מה לגבי 9? האם גם כאן אפשר לדעת את התשובה (השלילית) ללא בדיקה? עד מתי צריך להמשיך לבדוק? למשל, האם יש טעם לבדוק האם 97 מתחלק ב-10? התשובה שלילית. נסביר מדוע. נניח ש-97 כן מתחלק ב-10. במקרה כזה קיים שלם  $a$  כך ש:  $10a = 97$ , אבל במקרה כזה  $a$  מוכרח להיות קטן מ-10 ואנחנו כבר בדקנו את כל המספרים הקטנים מ-10 ונוכחנו שאינם מחלקים של 97. המסקנה מן הבדיקה האחרונה היא שמספיק לבדוק התחלקות של מספר  $n$ , רק עד  $\sqrt{n}$ . השורש הריבועי של 97 קטן מ-10 ולכן אם בדקנו את כל המספרים בין 2 ל-10 ונוכחנו כי אף אחד מהם אינו מחלק את 97, אנו יכולים להכריז בביטחון מלא, כי 97 הוא ראשוני.

נבדוק דוגמה נוספת. למשל, מה לגבי 44,197? האם הוא ראשוני? כמה בדיקות צריך לבצע כדי להחליט בוודאות?  $\sqrt{44,197} = 210.24$

כלומר צריך לבצע יותר מ-210 בדיקות, כדי לקבוע האם המספר ראשוני או פריק. בעזרת מחשבון אפשר להתמודד עם הבעיה ולגלות כי המספר פריק. אפשר לפרקו לאחר מאמץ מסוים, ל-193 ו-229 שניהם ראשוניים.

נראה שיש לנו אלגוריתם לפתרון שאלת הראשוניות של מספר. האם הוא יעיל גם לגבי מספרים יותר גדולים? הרבה יותר גדולים?

זכרו כי המצפינים ב-RSA מעונינים אך ורק בראשוניים ענקיים, בני מאות ספרות. ההצלחה באיתור ובחקר הראשוניים הענקיים, שנחבאים בין המספרים הפריקים, דורשת סבלנות רבה, מזל, נחישות ומספר כלים מתורת המספרים.

כמובן, שצידי המספרים הראשוניים הגדולים יכולים לבדוק את הראשוניות של המספר  $N$  כמו שבדקנו את הראשוניות של 97: לחלקו בשיטתיות בכל השלמים החל מ-2. אם  $N$  אינו מתחלק באף אחד מהם ללא שארית, אזי הוא ראשוני. ראינו, שיש לבדיקה קיצורים: אין צורך לעבור מעבר לשורש הריבועי של המספר הנבדק, כיוון שמחלקיו של מספר מופיעים תמיד בזוגות. אם אחד מהם גדול מן השורש הריבועי, בן זוגו קטן מן השורש וכבר נתגלה בשלב קודם של הבדיקה. אין גם צורך לבדוק כפולות של הגורמים שכבר נבדקו. קיצור דרך נוסף הוא, כמובן, בדיקת התחלקות רק באי זוגיים (מעבר לבדיקה ב-2).

אבל במקרה של המספרים הראשוניים הענקיים, גם אחרי כל הקיצורים, שיטה זו היא עדיין בלתי סבירה. למחשב שיכול לבצע מליארד ניסיונות חילוק בשניה, יידרשו לביצוע המשימה יותר שנים מגילו הנוכחי של היקום. ניסיונות החילוק יעילים במספרים קטנים. אבל, גם מספר בן 100 ספרות כבר אינו נכלל בקטגוריה זו, אלא אם יש לו במקרה, גורם קטן או שהוא בעל מבנה מיוחד.

אנחנו רואים כי הסיבוכיות של בדיקת הראשוניות עצומה וכל האלגוריתמים העומדים לרשותנו הם לא סבירים. האם אפשר להקטין את הסיבוכיות של בדיקת הראשוניות? האם אפשר למצוא אלגוריתמים בעלי סיבוכיות קטנה יותר לבדיקת ראשוניות? מה יכול להיות הכיוון לחיפוש האלגוריתם?

שימו לב, אנחנו מעונינים לבדוק רק ראשוניות, אבל בפועל מבצעים פירוק של המספר הנבדק לגורמים, על ידי פעולות חילוק רבות מספור, שמגדילות את הסיבוכיות של הפתרון. הרי, בעצם, כלל לא חשוב לנו לדעת לאיזה גורמים המספר מתפרק. לנו מספיק לדעת האם המספר ראשוני או שאינו ראשוני. האלגוריתם שהפעלנו לא רק מספק תשובה לשאלת הראשוניות, אלא נותן גם את כל הגורמים של המספר, אם הוא אינו ראשוני. מכאן הסיבוכיות העצומה שלו.

האם אפשר למצוא אלגוריתמים, שיצביעו על ראשוניות של מספר מבלי למצוא, באותו זמן, את הגורמים שלו, אם אינו ראשוני? אלגוריתם כזה יספק לנו את כל המידע הדרוש, אך קרוב לוודאי שהסיבוכיות שלו תהיה קטנה יותר, ולכן בדיקת הראשוניות באמצעותו תהיה מהירה יותר. זהו אלגוריתם שיבדוק רק ראשוניות של מספר, מבלי לפרקו לגורמים. בהמשך נכיר אלגוריתם כזה.

### 7.4.3 תרומתו של פרמה לבדיקת ראשוניות של מספר

כבר במאה ה-17 סיפק פֶרְמָה בסיס לבדיקת ראשוניות של מספר, מבלי לפרקו לגורמים. מתברר שאחד היישומים של "המשפט הקטן של פרמה", שכבר הספקנו להכיר, יכול לשמש גם לבדיקת ראשוניות. נסביר זאת:

המשפט הקטן של פרמה אומר כי: אם  $p$  ראשוני אז לכל  $m$  קטן מ- $p$ , מתקיים  $m^{p-1} \bmod p = 1$ . גרסא אחרת של המשפט אומרת כי: אם  $p$  הוא מספר ראשוני ו- $m$  הוא כל מספר שלם קטן ממנו, כי אז:

$$m^{p-m} \bmod p = 1$$

במילים אחרות נוכל לומר ש:  $m^{p-m} \bmod p = 1$  מתחלק ב- $p$  ללא שארית.

למשל: אם  $m=2$ ;  $p=7$ ,

המשפט הקטן של פרמה אומר ש-7 מחלק, ללא שארית, את  $2^7 - 2$ .

$$2^7 - 2 = 128 - 2 = 126$$

נבחן זאת:

$$126 / 7 = 18$$

והתוצאה

אחרי שהכרנו את השיטה של הריבוע החוזר, יש בידינו כלי לעבוד גם עם חזקות בעלות מעריכים גדולים.



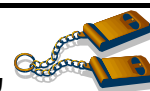
### שאלה מספר 9

אנחנו הכרנו את המשפט הקטן של פרמה בניסוח:  $m^{(p-1)} \bmod p = 1$   
נסו לקבל את הניסוח "הישן" מתוך הניסוח שזה עתה פגשנו:  $(m^p - m) \bmod p = 0$



### שאלה מספר 10

האם 9 ראשוני? בדקו בעזרת המשפט הקטן של פרמה.



### שאלה מספר 11

בדקו את נכונות של המשפט הקטן של פרמה לגבי המספר 13.



### שאלה מספר 12

בדקו, בדרך זו, האם 11 מקיים את המשפט הקטן של פרמה.

נסכם: כל מספר ראשוני מקיים את המשפט הקטן של פרמה. האם גם ההפך נכון? האם כל מספר שמקיים את המשפט הקטן של פרמה הוא ראשוני? אם המשפט ההפוך נכון, אזי אפשר לשנות את המשפט הקטן של פרמה, למשפט המשמש לבדיקת ראשוניות.

אבל המשפט ההפוך אינו נכון תמיד. נכון שאם השארית אינה אפס, אז המספר פריק (זוהי בדיקה לפריקות של מספר). אבל, וזהו אבל גדול, כיוון שמתברר, ששארית החילוק היא אמנם אפס עבור כל הראשוניים, אבל לא רק עבורם. יש מקרים שבהם השארית אפס אבל  $p$  פריק. כלומר, אם השארית לא אפס המספר לא ראשוני ואם השארית אפס, ברוב המקרים המספר ראשוני, אבל לא תמיד, לעיתים הוא פריק. המסקנה מכל האמור היא, שהתאפסות שארית החילוק היא תנאי הכרחי, אבל לא מספיק לקביעת הראשוניות.

הפריקים האלה (ששארית החילוק שלהם אפס וכך הם "מתחזים" לראשוניים) נקראים ראשוניים לכאורה. למשל, אחד "המתחזים" הוא 341. כאשר בודקים את המספר  $p = 341$ , מוצאים, שהביטוי  $2^{341} - 2$  מתחלק ב-341 (שארית החילוק אפס). למרות ש-341 פריק, הוא כפולה של 11 ו-13. אם כן, משפט פרמה לא פתר את הבעיה, אבל הוא פתח כוון לפתרונה. האלגוריתמים המודרניים לבדיקת ראשוניות נשענים על המשפט הקטן שלו. הם מתבססים עליו אך גם נבדלים ממנו הבדל יסודי: הם אינם קובעים שמספר הוא ראשוני, אלא רק שהוא ראשוני, עם סיכויי זעיר לטעות. בסעיף הבא נכיר אותם.

#### 7.4.4 אלגוריתמים הסתברותיים לבדיקת ראשוניות

נכיר את עקרון הפעולה של האלגוריתמים המודרניים לבדיקת ראשוניות. שימו לב, שסיבוכיות בדיקת הראשוניות של מספר תלויה בצורת הניסוח של השאלה אותה בודקים.

בסעיף הקודם ראינו, שהמשפט הקטן של פרמה מספק תנאי הכרחי אך בלתי מספיק לקביעת ראשוניות של מספר. לעומת זה הוא מספק תנאי הכרחי ומספיק ל"אי ראשוניות" (לפריקות) של מספר. לכן בבדיקת שארית החילוק של  $b^p - b$  ב- $p$ , אם השארית אינה אפס, אנחנו אומרים כי  $b$  הוא "עד מאשר" לאי ראשוניות של  $p$  (לפריקותו של  $p$ ).

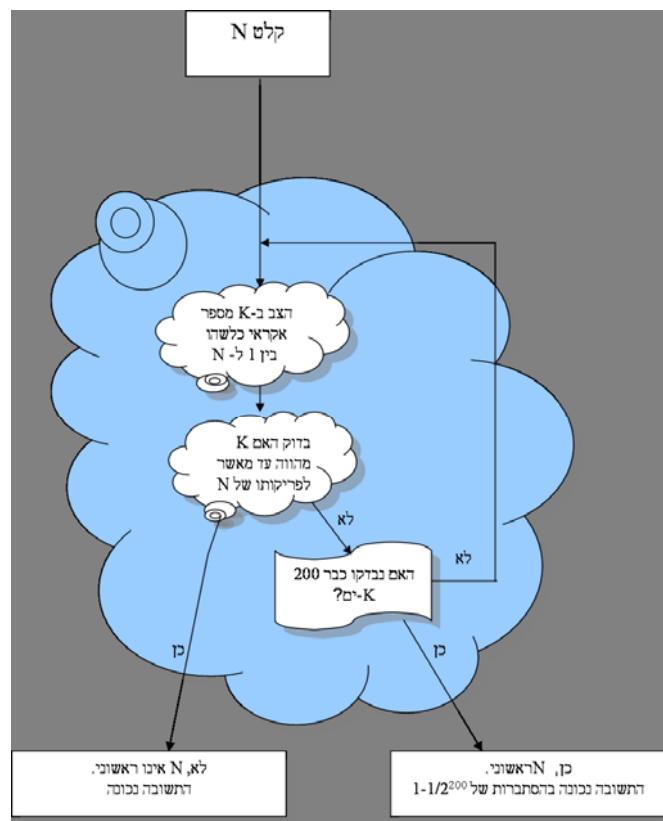
לכן אם הנוסח של השאלה לבדיקת הראשוניות הוא על דרך השלילה: "האם המספר אינו ראשוני" (פריק)? כי אז ברגע שמצאנו גורם אחד שמחלק את המספר הנבדק קיבלנו אישור מלא ל"אי ראשוניות" (לפריקות) של המספר. בניסוח אחר אפשר לומר כי **לקביעת הפריקות של מספר מספיקה תשובה חיובית אחת, מספיקה "עדות מאשרת" אחת. אבל לקביעת ראשוניות יש צורך לבצע "חיפוש ממצה" בין כל המחלקים האפשריים.** האם זה עוזר לנו? בינתיים לא. הלא אנחנו צריכים לבדוק ראשוניות. לכן, כל מה שנאמר עד עתה לגבי העדר אלגוריתמים סבירים לבדיקת ראשוניות של מספר הוא עדיין בגדר "חדשות רעות". בינתיים, בקרב על בדיקת ראשוניות, הסיבוכיות הביסה את האלגוריתמים.

האם יש גם "חדשות טובות" לגבי בדיקת ראשוניות? בראשית הפרק כשהצגנו את מושג הסיבוכיות אמרנו, כי לידיעה שלבעיה מסוימת אין פתרון סביר, יש גם משמעות חיובית. אמרנו כי היא מכוונת אותנו לפשרות, שאם נקבל אותן אנו עשויים להגיע לפתרון, אולי מוגבל, אבל בהישג יד. מתברר שזהו המצב לגבי בדיקת ראשוניות של מספר. לא קיים אלגוריתם סביר לקביעת ראשוניות של מספר **בוודאות**, גם משפט פרמה לא סיפק אותו. במשפט פרמה ראינו, שאם השארית אפס, אז אולי המספר פריק ואולי הוא ראשוני. מה הסיכוי שהמספר ראשוני? האם יש דרך להגדיל אותו? זה היה כיוון החקירה שבסופה הצליחו החוקרים לפתח אלגוריתם סביר לקביעת ראשוניות של מספר, **לא בוודאות אבל בהסתברות גבוהה.**

באמצע שנות ה-70 התגלו שני **אלגוריתמים הסתברותיים סבירים**, לבדיקת ראשוניות. גם כאן יש נקודה ישראלית כיוון שאחד הידועים שבהם פותח על ידי פרופסור מיכאל רבין הישראלי. אלגוריתמים אלה מסוגלים לבדוק ראשוניות של מספר בן 150 ספרות, תוך שניות ספורות, בהסתברות זניחה לטעות.

נתאר בקצרה את עקרונות פעולתו של אלגוריתם כזה. הוא מבוסס על חיפוש אקראי אחרי "עדים מאשרים" ל"אי ראשוניות" (פריקות) של המספר הנבדק. אם האלגוריתם מצא מספר המחלק את המספר הנבדק, כי אז מחלק זה הוא "עד מאשר" לכך. במקרה כזה האלגוריתם עוצר וקובע **בביטחון** כי המספר הנבדק אינו ראשוני. בהעדר "עד מאשר" האלגוריתם ממשיך לחפש. אולם החיפוש מתוכנן כך, שלא ימשך ללא הגבלה (עבור כל  $0 < m < p$ ), אלא יפסק אחרי פרק זמן סביר בהכרזה: "המספר הנבדק הוא ראשוני, עם סיכוי קלוש לטעות".

אנחנו לא נביא את התיאור המתמטי המפורט של האלגוריתם, אלא רק את התיאור הכללי של כמה מאפיינים שלו. חשוב להדגיש כי ה"עדים הפוטנציאליים" (לבדיקת הפריקות של  $p$ ) נבחרים באקראי. בחירתו של "עד" נעשית בדרך שמבטיחה כי אם הוא מאשר את הפריקות של  $p$ , אז לפחות מחצית המספרים בין 1 ל- $p$ , גם מאשרים זאת. המסקנה היא שאם ה"עדים" נבחרים בדרך זו, אם "עד" אינו מאשר פריקות, הסיכוי לטעות קטן מחצי. אם שני "עדים" בלתי תלויים (אקראיים), אינם מאשרים פריקות, אז הסיכוי לטעות קטן מרבע, וכן הלאה. כל "עד" אקראי נוסף, שקובע כי " $p$  אינו פריק", מקטין את הסיכוי לטעות פי 2. ברור שכל שמבצעים יותר בדיקות ומקבלים תשובות שליליות ("המספר אינו פריק"), כך מצטמצם הסיכוי לטעות. אחרי 200 בדיקות, הסיכוי לטעות קטן מ- $\left(\frac{1}{2}\right)^{200}$ . אחרי  $n$  בדיקות שתוצאותיהן שליליות, הסיכוי לטעות קטן מ- $\left(\frac{1}{2}\right)^n$ . האיור הבא מתאר את שלבי הבדיקה של האלגוריתם ההסתברותי לבדיקת ראשוניות.



לפי תרשים של דוד הראל מתוך ספרו "אלגוריתמיקה"

מן השרטוט אתם רואים כי האלגוריתם מבצע לכל היותר 200 בדיקות. האם לדעתכם זה מספק? הסיכוי

$$\left(\frac{1}{2}\right)^{200} \approx \left(\frac{1}{10}\right)^{60}, \text{ אנחנו יודעים כי: } \left(\frac{1}{2}\right)^{200} \text{ לטעות הוא}$$

במילים אחרות, הסיכוי לטעות אחרי 200 בדיקות שליליות, הוא יותר קטן מהחלק של מיליון בחזקת עשר. זו תוצאה מספקת לחלוטין. למעשה, גם 50 בדיקות כבר מבטיחות סיכוי מספיק קטן לטעות (בערך החלק המיליון בחזקת 6).

שימו לב שאם, לפני שסיימנו 200 בדיקות אקראיות, אחת הבדיקות מגלה שהמספר אינו ראשוני, כי אז זוהי תוצאה וודאית ולא הסתברותית. לכן היא גם סופית. אחרי שהתקבלה אין צורך בבדיקות נוספות. לאלגוריתם כזה אנו קוראים אלגוריתם מוטה לשלילה, כיוון שכל התשובות החיוביות שהוא יוצר ("לפי הבדיקה המספר ראשוני") הן הסתברותיות, אבל התשובה השלילית ("לפי הבדיקה המספר אינו ראשוני") היא וודאית. אלגוריתם זה מקל מאד, על המצפינים בשיטת RSA, למצוא ראשוניים גדולים. לעומת זאת, הוא אינו מקל על המפצחים בניסיונותיהם לפרק מספרי ענק לגורמים.

נסיים סעיף זה בהתפתחות מפתיעה. בקיץ 2002 פרסמו שלושה אנשי מחשבים הודיים, M. Agrawal, N. Kayal & N. Saxena, אלגוריתם חדש ומפתיע לבדיקת ראשוניות. האלגוריתם שלהם הוא לא הסתברותי אלא דטרמיניסטי והסיבוכיות שלו יחסית לאורך המספר הנבדק (מספר הביטים שלו). היישומים של אלגוריתם זה הם פחות יעילים מאלה של האלגוריתמים ההסתברותיים ולכן אין לו עדיין שימוש. למרות זאת הפך פרסומו לסנסציה, כיוון שרבים ובהם גם עיתונאים, כתוצאה מחוסר הבחנתם בין פירוק לגורמים ובדיקת ראשוניות, מהרו להסיק שהנה מגיע קצו של ה-RSA. כששכחה הסנסציה, התברר כי הספדתו של אלגוריתם ההצפנה RSA הייתה מוקדמת וחסרת בסיס.

#### 7.4.5 השוואת הסיבוכיות של בדיקת ראשוניות עם זו של הפירוק לגורמים

ננסה לסכם מהם יחסי הכוחות בין המצפינים למפצחים בשיטת RSA. יחסי כוחות אלה הם תוצאה של הבדלי הסיבוכיות של פתרון הבעיות התאומות: בדיקת ראשוניות ופירוק לגורמים. במצב הדברים כיום, האלגוריתמים ההסתברותיים לבדיקת ראשוניות הם סבירים, כיוון שכתוצאה מאופיים ההסתברותי הסיבוכיות שלהם קטנה בהרבה. לעומת זאת, האלגוריתמים של הפירוק לגורמים הם בלתי סבירים, למרות ההתקדמות הגדולה בפיתוחם, בזכות השימוש הגובר בהעלאה מהירה בחזקה של מספרים. הסיבוכיות הנוכחית של האלגוריתמים של הפירוק לגורמים נותרה, בסופו של דבר, הרבה יותר גבוהה מזו של האלגוריתמים המודרניים לבדיקת ראשוניות. לסיכום אפשר לומר כי בדיקת ראשוניות היא כיום בעיה "קלה", אך הפירוק לגורמים, ככל הידוע לנו, הוא עדיין בעיה "קשה" וחסרת פתרון סביר.

## 7.5 מידת הבטיחות של הצפנת RSA

כשדורשים בטיחות של מערכת הצפנה, דורשים כמובן, את קיומן של התכונות הבאות:

- ♦ גם כשידוע למאזי המפתח הפומבי, אין לה אפשרות לגלות את המפתח הפרטי.
  - ♦ גם כשידוע למאזי המסר המוצפן, אין לה אפשרות ישימה חישובית, לגלות את המסר המקורי, או חלקים ממנו.
  - ♦ מאזי אינה יכולה לגלות האם מספר מסרים מוצפנים, הם בעצם הצפנות שונות של אותו מסר מקורי. למשל, גם כששולחים מסר זהה למספר נמענים, אין לה אפשרות לגלות זאת.
- לבטיחות של מערכת הצפנה עשויות להיות שתי רמות: בטיחות בלתי מותנית ובטיחות חישובית.

### 7.5.1 בטיחות בלתי מותנית

בטיחות בלתי מותנית של מערכת הצפנה, זוהי בטיחות מוחלטת, שמתקיימת גם כאשר אין כל הגבלה על מספר פעולות החישוב שהיריב יכול לבצע. במילים אחרות, מערכת הצפנה היא בעלת בטיחות בלתי מותנית (מוחלטת), אם היא חסינת פיצוח גם כאשר ליריב מקורות חישוב (זמן מחשב) אינסופיים (לא מוגבלים). אנחנו הכרנו מערכת הצפנה אחת, שהיא בעלת התכונה של בטיחות מוחלטת, הצפנה באמצעות Onetime pad.

### 7.5.2 בטיחות חישובית

**מידת הבטיחות החישובית** מתייחסת למאמץ החישובי הדרוש לפיצוחה של מערכת הצפנה. בפועל נאמר על מערכת שהיא "מאובטחת חישובית", אם השיטה הידועה כטובה ביותר לשבירתה של המערכת דורשת זמן מחשב שארכו בלתי סביר. כלומר, הבטיחות החישובית היא בטיחות מותנית. היא תלויה ביחס בין גודלם של שני גורמים: סיבוכיות הפיצוח של המסר המוצפן והמשאבים החישוביים הזמינים למפצח. איזה מגבלות של המערכת עלולים לפגום בבטיחות החישובית שלה? נתאר דוגמא אחת. בדוגמה זו מאזי יודעת כי למסר המוצפן רק שני פענוחים אפשריים. זה המצב במקרים שונים של הצפנות מן הסוג של, "כן" או "לא". למשל אם מאזי יודעת שהמסר מתייחס להוראת פעולה בבורסה, שיש לה רק שתי אפשרויות "לקנות" או "למכור". במצב כזה כשמרחב ההודעות כל כך מצומצם, הצפנת RSA למשל, כפי שהכרנו אותה, אינה מספקת בטיחות. בהמשך נסביר זאת ביתר פירוט. כדי להתגבר על הכשל הבטיחותי שתיארנו, צריך להבטיח שני סוגים של בטיחות חישובית. בהמשך נתאר אותם ונראה דוגמה של שיטת הצפנה שמבטיחה את השגתם עבור כל הצפנות RSA.

### 7.5.3 בטיחות סמנטית

מערכת הצפנה היא בעלת בטיחות סמנטית, אם המידע הזמין למאזי על המסר המקורי, **לאחר** שראתה את המסר המוצפן, אינו עולה על המידע הזמין, שהיה לה **לפני** שראתה את המסר המוצפן. במילים אחרות, כיוון שמסרים מיוצגים על ידי ביטויים מתמטיים, אנחנו יכולים לומר שכל החישובים שהיריב יכול לבצע על ערכי הפונקציות של המסר, **אחרי** שהשיג את המסר המוצפן, אינם שונים במאום מאלה שהיה יכול לבצע, **לפני** שהצליח להשיג את המסר המוצפן. בקיצור, המסר המוצפן הוא חסר ערך עבורו, הוא אינו יכול לחלץ ממנו שום מידע חדש, הנוגע למסר המקורי. **הבעיות שלו אינן נובעות מהעדר מידע (הוא מכיר את אלגוריתם ההצפנה ואפילו את מפתח ההצפנה), אלא מהסיבוכיות החישובית של פיצוח ההצפנה וממגבלות משאבי החישוב הזמינים לפתרונו.** בהמשך נראה כיצד בונים הצפנות בעלות בטיחות סמנטית.

### 7.5.4 העדר אפשרות להבחין בין מסרים

זהו סוג נוסף של בטיחות המסר. כשבטיחות זו קיימת, היריב אינו יכול למצוא שני מסרים שונים, שהוא מסוגל להבדיל בין ההצפנות שלהם. למה הכוונה? נניח שבידי היריב שני מסרים,  $m_1$  ו- $m_2$ , ובידיו גם הצפנה, שהוא יודע כי היא של אחד מהמסרים, אבל הוא אינו מסוגל להבחין לאיזה מסר שייכת ההצפנה שבידיו. על הצפנה שמבטיחה זאת, אומרים כי היא ניחנה בתכונה של חוסר אפשרות להבחין בין שני מסרים.

אבל אם, למשל, היריב **יודע** כי ההצפנה מתייחסת **רק** לשתי הודעות מסוימות (שגם הן ידועות לו), משהו בנוסח של "כן" או "לא", כפי שכבר הזכרנו, כי אז יש לו אפשרות (שנתאר אותה בהמשך) לשייך את המסר המוצפן לאחד משני המסרים המקוריים. **העובדה, שאפשר להבחין בין שני מסרים ולשייך את ההצפנה לאחד מהם (בניגוד לדרישה של חוסר ההבחנה בין מסרים, שתוארה בפסקה הקודמת), מהווה פגיעה אנושה בבטיחות המערכת.**

### 7.5.5 סיכום ביניים

אפשר להוכיח כי הבטיחות הסמנטית (חוסר האפשרות **לחשב** מידע הקשור למסר) וחוסר האפשרות להבחין בין מסרים, מבטאים את אותה התכונה. לכן אומרים כי אלה תכונות שקולות (אקוויולנטיות). כמו שהזכרנו קודם, שתי התכונות האלה, גם כשהן מתקיימות, אינן מקנות למערכת ההצפנה בטיחות מוחלטת, אלא בטיחות חישובית בלבד.

### 7.5.6 הבטיחות של הצפנת RSA

ומה לגבי בטיחותה של מערכת ההצפנה של RSA? אנחנו כבר נוכחנו כי היא אינה מספקת בטיחות בלתי מותנית (מוחלטת), למסרים המוצפנים בה. ה-RSA הפשוט גם אינו בעל התכונה של העדר הבחנה בין מסרים. נראה שאם משתמשים בשיטת RSA כהלכה, היא מספקת בטיחות חישובית, הנשענת על ההבדל בסיבוכיות בין פרוק לגורמים ובין בדיקת ראשוניות. זוהי דרך נוספת לבטא את מידת הבטיחות החישובית של מערכת הצפנה, בדרך זו קושרים את בעיית הבטיחות של המערכת לבעיה אחרת מוכרת. בעיה שידועה כקשה לפתרון. בהמשך נפרט חלק מבעיות הבטיחות של השימוש בפונקציית RSA להצפנה. נדגים גם כיצד אפשר להתמודד עם בעיות אלה.

אם מאזי משיגה את המסר המוצפן  $C$ , שאילנית שלחה לבני, ומאזי יודעת שהטקסט נשלח לבני, אז יש לה נקודת מוצא להתקפה על המסר המוצפן. זכרו כי מאזי מכירה את מפתח ההצפנה הציבורי של בני וגם את אלגוריתם ההצפנה (RSA). האם יעזור לה המידע הזה לפענח את הטקסט המוצפן שבידיה? הפירוק לגורמים של  $n$  מתוך מפתח ההצפנה של בני אינו סביר, כפי שאנחנו יודעים. האם יש לה דרך פיצוח נוספת? היא יכולה לנסות ולהצפין הרבה מאוד טקסטים אפשריים, באמצעות המפתח הציבורי של בני- $E_B$ , עד שבסופו של דבר היא תמצא מסר  $P$  כזה, שהצפנתו על ידי  $E_B$  תהיה  $C$ . כלומר יתקיים:  $C = E_B(P)$ . כלומר,  $P$  הוא הפענוח של  $C$ .

האם הפיצוח בדרך זו מעשי? אם המסר המוצפן ששלחה אילנית לבני הוא אקראי לגמרי ולמאזי אין כל מידע על תכנו האפשרי, כי אז אין לה כל נקודת אחיזה לפיצוח. איזה טקסטים תנסה להצפין בעזרת המפתח הציבורי של בני? על מזג האוויר? על מצב שוק המניות? על ריגול תעשייתי? על מסיבת הפתעה במשפחה? במצב זה, כשהמסר אקראי לחלוטין אין למאזי כל סיכוי לפצח את תוכנו של המסר המוצפן. אבל נניח שמאזי יודעת כי המסר המוצפן מתייחס לעסקה מסוימת בין אילנית לבני, והמסר אמור לציין את הסכמתה או אי הסכמתה של אילנית לביצוע העסקה.

במקרה כזה, כשלמאזי יש מידע במה מדובר וכאשר המסר מתייחס למצב של "כן" או "לא", מצב שכבר תיארנו, אז משימת הפיצוח מצטמצמת ולכן אפשרית. מאזי יודעת שהיא יכולה להסתפק בבדיקת שתי אפשרויות בלבד והיא פשוט מנסה אותן. כבר נוכחנו קודם כי זהו מצב שבו קשה להבטיח בטיחות סמנטית, מאזי אכן יכולה להפיק מן המסר המוצפן מידע על המסר המקורי. לכן חשוב מאוד לא להצפין מידע של "כן" או "לא", על ידי קידוד ישיר.

לסיכום, השימוש בפונקציית RSA להצפנה מספק בטיחות חישובית אם המסר אותו רוצים להצפין הוא אקראי אבל השימוש ב-RSA, להצפנת מסרים של "כן" או "לא" (מצב של מרחב הודעות מצומצם), אינו יוצר הצפנות בעלות בטיחות חישובית מספקת.

המסקנה ממגבלות הבטיחות של RSA, כפי שתיארנו אותן בפסקה הקודמת, היא שבכל המקרים בהם מרחב ההודעות מצומצם, על בני ואילנית (וכל המשתמשים) למצוא דרכים להגן על ההודעות מפני מאזי (או כל יריב אחר). הנה דוגמה אחת כיצד הם יכולים להשיג הגנה כזאת.

### 7.5.7 הצפנה הסתברותית

ראינו קודם כיצד מאזי, שהצליחה לשים את ידה על מסר מוצפן, מנסה לפענח אותו על ידי הצפנת מסרים משוערים שונים, מתוך תקווה שאחת ההצפנות תהיה זהה לזו הנמצאת בידה. נוכחנו גם כי שיטה זו עשויה להצליח כאשר מרחב ההודעות קטן.

מטרת ההצפנה ההסתברותית היא להבטיח, שמתוך המסר המוצפן, אי אפשר יהיה לחשב שום מידע על המסר המקורי (ללא קשר לגדלו של מרחב ההודעות). משיגים את המטרה על ידי הצפנה בנתוני פונקצית RSA, אבל ההצפנה שונה במקצת מזו שהכרנו. ההצפנה היא הסתברותית. כלומר, **בהצפנה כזו לאותו מסר עשויות להיות הצפנות רבות ושונות זו מזו** (עבור אותם נתוני מפתח  $e, d, n$ ) ולכן אין זה ישים חישובית, לבדוק האם מסר מוצפן נתון הוא הצפנה של מסר מסוים. נראה כיצד אפשר לבצע זאת.

#### הצפנה של מסר $m$ :

נתון  $m$  שאורכו  $K$  תווים בינריים. רוצים לייצר מפתח אקראי שישמש מפתח הצפנה של המסר  $m$ , בשיטת Onetime pad. לכן, נייצר מפתח שאורכו כאורך המסר  $m$ . אלגוריתם ההצפנה עם המפתח יהיה חיבור בינרי של המסר  $m$  עם המפתח.

שלב א' - ייצור המפתח:

בוחרים מחרוזת בינרית אקראית  $X_0$ . מחשבים  $X_0^e \bmod n$  ומניחים בצד את הביט האחרון. חוזרים על הפעולה כאשר הכלל הוא:  $X_i = X_{i-1}^e \bmod n = (X_0^e)^i \bmod n$ . חוזרים על הפעולה  $K$  פעמים (ערכו של  $K$  כמספר תווי המסר  $m$ ), כאשר  $e$  ו- $n$  הם נתוני המפתח הפומבי של RSA. ב- $K$  הביטים ששמנו בצד משתמשים כ- Onetime pad.

שלב ב' - הצפנה:

מחברים למסר  $m$  את המפתח  $K$  (פעולה של חיבור בינרי). כך הוצפן המסר  $m$ .

שלב ג' - שליחה:

שולחים את הזוג הסדור  $(X_k, \text{המסר המוצפן})$ .

#### פענוח של המסר המוצפן:

שלב א' - מציאת מפתח ה Onetime pad:

הנמען של המסר המוצפן שקבל גם את מילת המפתח מוצפנת  $k$  פעמים -  $X_k$ , משחזר מ- $X_k$  את  $X_{k-1}$  וכך הלאה עד  $X_0$ . בכל צעד נעשה שמוש במפתח הפרטי של הנמען  $d$ , כך שמתקיים:  $X_i = X_{i+1}^d \bmod n$ . תוך כדי שחזור  $X_i$ , שמים בצד את הספרה הבינרית האחרונה וכך "צוברים" את מפתח ההצפנה. שלב ב' - פענוח המסר המוצפן:

לאחר שנמצא המפתח להצפנה, יעשה חיסור בינרי של המפתח מהמסר המוצפן, וכך מפוענח הצופן.

ניתן להראות כי שיטה זו, של הצפנה הסתברותית משיגה הצפנה עם בטיחות סמנטית, וכמו כן חוסר אפשרות להבחין בין מסרים, עבור כל מרחב הודעות.

### 7.5.8 פתרון מוצלח

פתרון מוצלח הוא לשלב בין שתי השיטות ולמצות את היתרונות של שתיהן. כך משיגים את יתרון האבטחה של ההצפנה האסימטרית ואת יתרון מהירות של ההצפנה הסימטרית. דוגמה להליך אחד באמצעותו אפשר להשיג זאת, הוא הליך שנקרא מעטפה דיגיטלית. כשאיננו רוצה לשלוח לבני מסר בהליך זה, היא מצפינה את המסר במפתח **סימטרי**, ב-DES למשל, וכך היא מאיצה את מהירות ההצפנה.

היא מצפינה במפתח הציבורי של בני, מפתח **אסימטרי**, רק את מפתח ההצפנה. את מפתח ההצפנה היא מצפינה בהליך שמבטיח בטיחות סמנטית, כפי שתיארנו בסעיף הקודם. כך היא מגדילה את אבטחת המסר, אך מצליחה לשמור על מהירות ההצפנה. כך מנצלת איננו את היתרונות של שתי שיטות ההצפנה. זוהי המעטפה הדיגיטלית. בני מפענח את מפתח DES המוצפן במפתח הפרטי שלו, ואז משתמש במפתח הסימטרי שפענח, לפענוח המסר עצמו.

## 7.6 פתרונות

### פתרון שאלה מספר 1:

$$2^3 * 3^2 * 5^2 * 7 * 11 = 13,860$$

### פתרון שאלה מספר 2:

$$59 * 61 = 3,599$$

### פתרון שאלה מספר 3:

$$179 * 181 = 32,399$$

### פתרון שאלה מספר 4:

1,2,3,5,7,11,13,17,19,23,29,31,37,41,43,47,53,59,61,67,71,73,79,81,83,89,97

### פתרון שאלה מספר 5:

| המספרים בין: | מספר הראשוניים |
|--------------|----------------|
| 1-10         | 5              |
| 11-20        | 4              |
| 21-30        | 2              |
| 31-40        | 2              |
| 41-50        | 3              |
| 51-60        | 2              |
| 61-70        | 2              |
| 71-80        | 3              |
| 81-90        | 3              |
| 91-100       | 1              |
| 101-110      | 4              |

### פתרון שאלה מספר 6:

- א. בעשרת הראשונה, כלומר בתחום 1-10, יש הכי הרבה מספרים ראשוניים.  
ב. בעשרות 11-20, 101-110, הצפיפות השניה בגודלה.  
ג. בעשרת התשיעית, כלומר בתחום 91-100, יש הכי מעט ראשוניים.

### פתרון שאלה מספר 7:

א.  $2.3 * 20 = 46, 2.3 * 10 = 23, 2.3 * 6 = 13$

ב.  $1:12 * 2.3 = 1:27.6$

### פתרון שאלה מספר 8:

א.  $1 * 2 * 3 + 1 = 7$

ב.  $1 * 2 * 3 * 5 + 1 = 31$

ג.  $1 * 2 * 3 * 5 * 7 + 1 = 211$

ד.  $1 * 2 * 3 * 5 * 7 * 11 + 1 = 2,311$

ה.  $1 * 2 * 3 * 5 * 7 * 11 * 13 + 1 = 3,0031 = 59 * 509$

### פתרון שאלה מספר 9:

$$m^p \bmod p = m \bmod p$$

$$m * m^{(p-1)} \bmod p = m \bmod p$$

$$m^{(p-1)} \bmod p = 1$$

### פתרון שאלה מספר 10:

נקח:  $m = 2$ ,  $m$  קטן מ-9. לפי משפט פרמה, אם 9 ראשוני אז  $2^9 - 2$  כפולה של 9.

$$2^9 - 2 = 512 - 2 = 510$$

510 אינו מתחלק (ללא שארית) ב-9, לכן 9 אינו ראשוני.

### פתרון שאלה מספר 11:

13 הוא ראשוני ולכן צריך לקיים את משפט פרמה:

נקח:  $m = 2$ ,  $m$  קטן מ-13.

$$2^{13} - 2 = 8192 - 2 = 8190$$

$$8190 / 13 = 630$$

13 הוא ראשוני לכן 8190 מתחלק ב-13 ללא שארית.

### פתרון שאלה מספר 12:

$$2^{11} - 2 = 2048 - 2 = 2046$$

$2046 \bmod 11 = 0$ , מקיים את המשפט הקטן של פרמה.

## 8 הערות סיכום

### 8.1 יתרונות ההצפנה האסימטרית על פני ההצפנה הסימטרית

היתרון העיקרי של ההצפנה האסימטרית הוא בהגדלת הביטחון והנוחות, שנובעת משתי סיבות עיקריות:

א. **ביטול הצורך בהסכם מפתח:** בשיטת הצפנה זו, יש מפתחות נפרדים להצפנה ולפענוח. לכן אין צורך בהסכם מפתח, שמקדים את שליחת המסר המוצפן. לבעליו של המפתח הפרטי (מפתח הפענוח) אין אף פעם צורך להעביר את המפתח שלו או לגלותו לאדם אחר. כל מי שמעונין לשלוח לו מסר מוצפן עושה זאת באמצעות המפתח הפומבי (מפתח ההצפנה), הגלוי לכל. במצב כזה, בעיית השמירה על סודיות המפתח מצטמצמת מאוד. כל משתמש צריך לדאוג רק לסודיות המפתח הפרטי שלו. המפתח הזה מספיק לו לכל ההתקשרויות עם המשתמשים האחרים. לעומת זאת בהצפנה הסימטרית, כיוון שאותו מפתח משמש להצפנה ולפענוח, מוכרחים כל שני מתקשרים לבצע הסכם מפתח מקדים, הם מוכרחים להעביר את המפתח ביניהם (על ידי שליח, או בערוץ תקשורת אחר), לפני שליחת המסר המוצפן. תמיד קיימת הסכנה שתוך כדי העברת המפתח הוא יפול בידי היריב. גם אם נתעלם מחוסר הנוחות של השיטה, הבעיה של שמירת בטיחות המפתחות היא חמורה ומתמדת.

ב. **צמצום מספר המפתחות** - היתרון השני הוא בצמצום מספר המפתחות של מערכת ההצפנה האסימטרית, לעומת מספר המפתחות במערכות הצפנה סימטריות. בדיון קודם על מגבלות ההצפנה הסימטרית נזכרנו, כי במערכת סימטרית של  $n$  משתמשים, בה כל משתמש מתקשר עם כל האחרים, מספר המפתחות הדרוש הוא  $n(n-1)/2$ , ואילו במערכת הצפנה אסימטרית, בעלת אותו מספר משתמשים, מספר המפתחות הדרושים הוא  $2n$ . למשל, במצב של 1,000 משתמשים, במערכת סימטרית, יש צורך בחצי מיליון מפתחות. במערכת האסימטרית, יש לכל משתמש זוג מפתחות בלבד. בסך הכל יש במערכת 1,000 מפתחות פומביים, שאין כל צורך לשמור על סודיותם ו- 1,000 מפתחות פרטיים. כלומר, צריך לשמור על הסודיות של 1,000 מפתחות מול 500,000 מפתחות. בסך הכל צריך לנהל 2,000 מפתחות במקום חצי מיליון מפתחות. לכן בעיות הניהול ואבטחת המפתחות בשיטה האסימטרית הרבה יותר פשוטות.

### 8.2 מגבלות ההצפנה האסימטרית לעומת ההצפנה הסימטרית

**מהירות** - להצפנה האסימטרית יש מגבלת מהירות. שיטות רבות של הצפנה סימטרית מהירות באופן משמעותי מן השיטות האסימטריות הרווחות.

## נספח א': הוכחה לנוסחת פתרונות המשוואה הריבועית

$$ax^2 + bx + c = 0$$

$$x^2 + \frac{b}{a}x + \frac{c}{a} = 0$$

$$x^2 + \frac{b}{a}x = \left(x + \frac{b}{2a}\right)^2 - \left(\frac{b}{2a}\right)^2$$

$$\left(x + \frac{b}{2a}\right)^2 - \left(\frac{b}{2a}\right)^2 + \frac{c}{a} = 0$$

$$\left(x + \frac{b}{2a}\right)^2 = \left(\frac{b}{2a}\right)^2 - \frac{c}{a}$$

$$x + \frac{b}{2a} = \pm \sqrt{\left(\frac{b}{2a}\right)^2 - \frac{c}{a}}$$

$$x = -\frac{b}{2a} \pm \sqrt{\frac{b^2}{4a^2} - \frac{c}{a}}$$

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

## נספח ב': הוכחת משפט אוקלידס

"לכל  $a$  שלם קיימים  $b, q$  שלמים קטנים ממנו כך ש:  $a = bq + r$  כאשר:  $0 \leq r < b$ ".

אפשר להוכיח את המשפט מבלי להזדקק להליך של החילוק הארוך. שימו לב לכך, שלגבי כל שלם  $a$  קיימות שתי אפשרויות:

- א.  $a$  הוא כפולה של  $b$  ומתקיים:  $a = bq$
  - ב.  $a$  נמצא בין שתי כפולות עוקבות של  $b$  ומתקיים:  $bq < a < b(q+1)$
- במקרה הראשון מתקיימת טענת המשפט כי:  $a = bq + r$  כאשר  $r = 0$
- ובמקרה השני נקבל מן האי שוויון השמאלי  $bq < a$
- $$0 < a - bq$$
- ומן האי שוויון הימני נקבל  $a < b(q + 1)$
- $$a - bq < b$$

כלומר:  $0 < a - bq < b$

ידוע כי:  $a - bq = r$

לכן  $0 \leq r < b$ .

## ביבליוגרפיה

דוד הראל - פרקי יסוד במדעי המחשב. משרד הבטחון ההוצאה לאור 1992.

דוד הראל - אלגוריתמיקה : יסודות מדעי המחשב. האוניברסיטה הפתוחה 2001.

Ivars Peterson - The Mathematical Tourist, W. H. Freeman & Company New York 1998

D. R. Stinson - Cryptography Theory and Practice. CRC Press LLC, 1995

H. X. Mel and D. Baker - Cryptography Decrypted. Addison Wesley, 2001

S. Singh - The Code Book. Anchor Books New York 1999

S. Singh - The code Book, How to Make it, Break it, Hack it, Crack it.

Delacorte Press 2001. (זוהי מהדורה מקוצרת לנוער של הספר הקודם של אותו סופר)

S. Flannery - In Code A Mathematical Journey. Workman Publishing New York 2000

Alfred J.Menzes,Paul C.van Ooschot, Scott A. Vanstone - Handbook of Applied Cryptography. Carcr.math.uwaterloo.ca/hac

Richard A. Mollin - An Introduction to Cryptography. Chapman & Hall/CRC 2001

### מקורות באינטרנט סיבוכיות חישובית – "בול קליעה"

Invitation to Master Mind by Don Greenwell

<http://www.maa.org/editorial.knot/Mastermind.html>

Break the Hidden Code by Toby Nelson <http://www.tnelson.demon.co.uk/mastermind/>

Mastering Mastermind by Ivars Peterson

[http://www.maa.org/mathland/mathtreck\\_10\\_11\\_99.html](http://www.maa.org/mathland/mathtreck_10_11_99.html)

### סיבוכיות – סדר גודל

Big O notation [http://www.wikipedia.org/wiki/Big\\_O\\_notation](http://www.wikipedia.org/wiki/Big_O_notation)

### סיבוכיות של פעולות חשבון

Great Theoretical Ideas in Computer Science, Steven Rudich, Carnegie Melon University

<http://www.2.cs.cmu.edu/afs/cs.cmu.edu/academic/class/15251/Site>

## סדרת הרצאות ומצגות:

- מצגת מספר 1 – חיפוש בינרי של אנגרמות
- מצגת מספר 2 – אלגוריתמים של חיבור ושל כפל.
- מצגת מספר 9 – האלגוריתם של Karatsuba

## סיבוכיות של בדיקת ראשוניות ושל פרוק לגורמים

How Many Primes Are There? <http://www.utm.edu/research/primes/howmany.shtml>

MATH WORLD- Primality Testing is Easy

[http://mathworld.wolfram.com/news/2002-08-07\\_primalitytest/](http://mathworld.wolfram.com/news/2002-08-07_primalitytest/)

A Prime Solution by R. Ramachandran <http://www.flonnet.com/fl1917/19171290.htm>

The Primes is in P Little FAQ [http://crypto.cs.mcgill.ca/~stiglic/PRIMES\\_P\\_FAQ.html](http://crypto.cs.mcgill.ca/~stiglic/PRIMES_P_FAQ.html)

Finding Primes & Proving Primality

[http://www.utm.edu/research/primes/prove/prove4\\_3.html](http://www.utm.edu/research/primes/prove/prove4_3.html)

Fermat Little Theorem Converse

[http://mathworld.wolfram.com/Fermats\\_Little\\_Theorem\\_Converse.html](http://mathworld.wolfram.com/Fermats_Little_Theorem_Converse.html)

Has factoring been getting easier? <http://denis.arnaud.free.fr/zds/appendix/nod56.html>

What are the best factoring methods in use today? (57)

What are the prospects for theoretical factoring breakthrough? (58)

## בטיחות של הצפנה

<http://www-cse.ucsd.edu/users/mihir/papers/gb.html>

(פרק מספר 1 ופרק מספר 7)

