

הצפנה סימטרית



תמר ריינר

הצפנה סימטרית



תמר ריינר

הצפנה סימטרית

כתיבה: **תמר ריינר** מנהלת הערוצים, הטלוויזיה החינוכית
מנהל פרויקט **כדאי לדעת**: פרופ' אילון סולן
ייעוץ מדעי: פרופ' נצה מובשוביץ-הדר, הטכניון, פרופ' מוני נאור, מכון ויצמן למדע
עריכת לשון: ד"ר דנה ברעם
ריכוז אדמיניסטרטיבי: גלית הרצברג
עיצוב גרפי ועימוד: ניצן-שמיר מעצבים
איור עטיפה: shutterstock
כתובת אתר **כדאי לדעת**: goodtoknow.tau.ac.il

תודות ל"מדעטק-המוזאון הלאומי למדע טכנולוגיה וחלל בטכניון" שאישר את ההוצאה לאור של חוברת זו במסגרת פרויקט "כדאי לדעת", לנועם מזור מביה"ס למדעי המחשב בכתיבת המבוא והסיכום של החוברת, ולמכון ו"מכון צ'ק-פוינט לאבטחת מידע", ביה"ס למדעי המחשב, אוניברסיטת תל-אביב על מימון ההפקה של החוברת הנ"ל.

זכויות הקניין הרוחני, לרבות זכויות היוצרים והזכות המוסרית של היוצרים בחומר זה, מוגנות.

השימוש בחוברות, שמירתן במאגרי מידע והפצתן מותר לצורך שימוש לא מסחרי בלבד. בעת שמירה במאגרי מידע, יש לציין במפורש שהחוברת שייכת לפרויקט "כדאי לדעת" ולצרף קישור לאתר הפרויקט. השימוש לכל מטרה מסחרית וליצירה של חומרים נגזרים אסור ללא קבלת רשות מפורשת בכתב מהנהלת הפרויקט.

תוכן

4	תודות
5	מבוא
8	1. צופני שחלוף קלים
8	1.1. מהו צופן שחלוף?
9	1.2. צופני הזזה - צופן יוליוס קיסר
10	מהו מספר ההזזות האפשרי של האלף-בית?
11	1.3. בניית מכשיר להצפנת יוליוס קיסר
13	1.4. החשבון המודולרי של צופן יוליוס קיסר
13	שלב א: המרת אותיות במספרים
13	שלב ב: הזזה מודולרית
17	הצפנה באמצעות חיבור מודולרי
18	1.5. סיכום ביניים של צופן יוליוס קיסר
19	2. צפנים של ערבול
19	2.1. מהו צופן ערבול?
19	ערבול באמצעות היפוך סדר האותיות במסר
20	2.2. צופן זיגזג
22	2.3. צופן השביל המתפתל
23	מסלול מתפתל ספירלי
24	הערות
25	2.4. תמורה כמושג מתמטי
27	תמורות שיש בהן חזרות
27	2.5. הסימון המתמטי לתמורה והשימוש בו
29	3. מקצה שיפורים לצופן יוליוס קיסר
29	3.1. מספר התמורות במעגל
31	3.2. שימוש בכפל מודולרי להצפנה
32	פענוח בעזרת ההופכי הכפלי
35	3.3. הצפנה סימטרית ואסימטרית
35	3.4. מגבלות הצופן המוגן-אלף-ביתי
37	סיכום
38	נספח א מילון מונחים
42	נספח ב מעגלי הצפנה
46	קישורים לאתרי אינטרנט בנושא מכונת האניגמה
47	פתרונות
57	ביבליוגרפיה

תודות

החוברת "הצפנה סימטרית" היא הראשונה מתוך שתי חוברות בנושא הצפנה שנכתבו עבור פרויקט האולימפידיע של מדע-טק בשנת 2003, פרויקט שמטרתו לעודד את המצוינות בקרב תלמידי חטיבות הביניים. חוברת שנייה, "הצפנה אסימטרית", נכתבה אף היא עבור פרויקט האולימפידיע. אני אסירת תודה לפרופסור מוני נאור, שנאות לתרום מזמנו, ואני מודה לעצותיו החשובות שסייעו לי למצוא את דרכי בשפע החומר, הסבוך לעיתים. אני מודה לפרופסור נצה מובשוביץ-הדר, שבלעדיה 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.

תודה לאנשי המוזאון הלאומי למדע בחיפה, שעצותיהם תרמו לשיפור החומר:

לפרופסור יורם זבירין, מנהל המוזאון, שלמרות עיסוקיו הרבים טרח לקרוא בקפדנות את החומר והעיר את הערותיו.

ליעל אדרי, רכזת פרויקט האולימפידיע במוזאון, שעברה בקפדנות על הטיוטות, חשפה נקודות תורפה והציעה שיפורים משמעותיים, ואף תכננה ושרטטה את כל השרטוטים מאירי העיניים. הדיאלוג הענייני בינינו השביח את המוצר הסופי.

לדליה כץ, מנהלנית המוזאון, על נכונותה לסייע תמיד, למיכל טל, שטרחה ללא ליאות על עיצובו הנאה של החומר ועל הדפסת המהדורה הראשונה, ולטלי זמירין, המעצבת הגרפית, על עיצוב הכריכה.

תודה לעוד רבים בצוות המוזאון, שתקצר היריעה מלנקוב בשמם, על שיתוף הפעולה ועל מאור הפנים. תודה ל"קשר חם" - המרכז לקידום, שיפור ורענון החינוך המתמטי בישראל, שבסיועו התאפשרה הוצאת המהדורה הנוכחית המתוקנת.

לכולם תודתי, והשגאות - אם יש - עליי.

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

בתקווה שתיהנו
ובברכת "תחלצום הנפצה",
תמר ריינר
ינואר 2008

מדי יום אנחנו שולחים הודעות - בדואר האלקטרוני או בדרכים אחרות באמצעות המחשב, בווטסאפ או במסרונים. מהרגע שבו ההודעות עוזבות את המחשב או את הטלפון שלנו ומגיעות למחשב או לטלפון של בן שיחנו, הן עוברות בתווך שאליו חשופים אנשים נוספים. הודעת דוא"ל שאנחנו כותבים במחשב עוברת דרך השרת של ספק האינטרנט שלנו ודרך מחשבים אחדים עד שהיא מגיעה למחשב של ספק האינטרנט של בן-שיחנו ומשם למחשב שלו. גם הודעת ווטסאפ עוברת מהטלפון שלנו לאנטנה של חברת התקשורת שמספקת לנו שירות, למחשבים של חברת התקשורת, ומשם דרך רשת האינטרנט - כלומר, דרך מחשבים נוספים - לחברת התקשורת שמספקת שירות לבן-שיחנו ולטלפון שלו. במהלך הדרך הארוכה שעוברת ההודעה עד שהיא מגיעה ליעדה, יכולים לקרוא אותה אנשים רבים. רבות מההודעות שאנחנו שולחים הן פרטיות, ואיננו מעוניינים שאחרים יוכלו לקרוא אותן. כיצד, אם כן, נוכל להעביר את ההודעה בתווך ציבורי מבלי שתיחשף לעיני זרים?

מאז ומתמיד חששו שליטי מדינות ומצביאים צבאיים מהתוצאות החמורות שעלולות להיות לנפילה של מסרים סודיים לידי גורמים עוינים. לכן ניסו לפתח שיטות שונות להסתרת מסרים חשובים באמצעות שימוש בצפנים ובכתבי סתר. כבר לפני 2500 שנה רצה יוליוס קיסר להעביר מסרים צבאיים מבלי שייפלו לידי האויב, והוא ניסה לפתור בעיה זו בעזרת הצפנה: שני הצדדים - שולח ההודעה ומקבלה - מסכימים לפני משלוח ההודעה על סוד משותף, שנקרא "מפתח". בעזרת המפתח הסודי, שולח ההודעה יכול לשנות את ההודעה שהוא רוצה לשלוח - כלומר להצפין אותה - כך שהיא תיראה חסרת משמעות לכל אדם שיראה אותה, מלבד למי שידע מהו המפתח. אדם שאינו מכיר את המפתח יכול לנסות לנחש מהו, אך אם מספר המפתחות האפשריים גדול, הסיכוי שהוא ינחש נכונה קטן, ולכן הסיכוי שיוכל לשחזר את ההודעה אינו גדול.

לאורך ההיסטוריה התפתחו דרכים שונות להצפין מסרים. תורת ההצפנה חוקרת את הדרכים האלו, והיא חוקרת גם את הדרכים לשחזר את ההודעה מהצופן ללא ידיעת המפתח, תהליך הנקרא "שבירת הצופן". כך הלך והתפתח תחום ההצפנה, עד שהיה למדע של ממש, הנקרא בלועזית **קריפטוגרפיה**. מדע ההצפנה מקיף מגוון של שיטות לשיבוש מסרים ולהסתרתם מפני כל מי שהמסרים לא נועדו לו. לצורך זה הוקמו מחלקות ייעודיות שעסקו בהמצאה וביצירה של צפנים, וכן הועסקו מפצחי צפנים, שכל תפקידם היה לגלות את סודותיו המוצפנים של הצד האחר.

ההיסטוריה של ההצפנה היא סיפור ההתמודדות בת אלפי השנים בין יוצרי הצפנים לבין מפצחיהם. לתחרות המוחות הזאת הייתה השפעה גדולה על מהלך ההיסטוריה האנושית. למשל, ארצות הברית הצטרפה למלחמת העולם הראשונה אחרי שהמודיעין הבריטי הצליח לשבור את הצופן של מברק שנשלח מגרמניה למקסיקו, שבו הציעה גרמניה למקסיקו לכרות עימה ברית ולתקוף את ארצות הברית. במהלך מלחמת העולם השנייה, הבריטים והגרמנים שברו אלה את הצפנים של אלה, וקריאת ההודעות המוצפנות אפשרה לשני הצדדים לפגוע זה בזה ביעילות רבה יותר. מפורסמת במיוחד היא הפרשה המרתקת של מכונת ההצפנה הגרמנית אניגמה, שהייתה בשימוש בשנות השלושים והארבעים של המאה העשרים והשפיעה השפעה דרמטית על מהלך המערכה באירופה במלחמת העולם השנייה. אלה הן דוגמאות ספורות מבין רבות.

בעוד בעבר שימשו הצפנות בעיקר מדינות וצבאות, היום יש להן שימושים אזרחיים ופרטיים רבים מאוד. אנו חיים כיום בחברה גדושה במידע בכל תחומי החיים, והגישות למקורות מידע ואפשרויות השימוש בסוגים שונים של מידע גדולות יותר מאי פעם. פעולות של יום-יום כמו שיחות בטלפון, שימוש בכרטיסי אשראי, ביצוע עסקאות באמצעות האינטרנט - כל אלה ורבות נוספות אינן חסינות מפני ציתות או התערבות זדונית אחרת. הצפנה היא דרך יעילה מאוד להבטיח את חסיון המידע של הפרטים ושל גופים עסקיים ואחרים, והיום יישומים רבים מצפינים באופן אוטומטי את המידע הנשלח באמצעותם. ככל שהמחשבים חזקים ומהירים יותר, כך אנו יכולים להשתמש בשיטות הצפנה מתוחכמות יותר וגם לשבור צפנים במהירות גדולה יותר. אפשר לומר כי הקריפטוגרפיה - מדע התקשורת הסודית - מאפשרת את שגשוגם של הכלכלה ושל שוק הכספים בעידן המודרני.

אולם ההתפתחות הטכנולוגית המרשימה בתחום זה מעוררת בעת האחרונה גם בעיות רציניות. מתברר שהיכולת להעביר מסרים מוצפנים באינטרנט עלולה להיות מנוצלת על ידי גורמים העוינים את הסדר החברתי, למשל קבוצות טרור. ומנגד, גורמי ביטחון פנים מגבירים את הציתות ואת המעקב אחרי כל האזרחים במאבקם נגד הטרוריסטים. אנו צופים בפגיעה בחירויות הפרט, בפגיעה בחסיון המידע. האם ראוי לפגוע בחירויות אלה כדי לא לסכן את ביטחון המדינה? זהו חומר למחשבה.

בחוברת זו נכיר משפחה של שיטות הצפנה פשוטות, שנקראות הצפנות סימטריות. הצפנות כאלה היו בשימוש מאז ימי יוליוס קיסר ועד הרבע האחרון של המאה העשרים. כל המצפינים במשך כל השנים הללו הכירו את ההצפנות הסימטריות והשתמשו רק בהן. נכיר שתי שיטות להצפנה סימטרית. השיטה הראשונה היא שיטת הערבול, שבה אותיות המסר המקורי מעורבלות - המסר המוצפן מכיל את כל אותיות המסר המקורי אבל בסדר שונה. כדי לפענח את הצופן יש לגלות מהו הסדר המקורי

של האותיות. שיטת ההצפנה השנייה שנכיר היא שיטת השחלוף, שבה כל אות במסר המקורי משנה את זהותה, אבל סדר האותיות אינו משתנה. כדי לפענח יש לגלות את זהותה המקורית של כל אות. בהמשך נבין מדוע קוראים להצפנות אלה הצפנות סימטריות, ונכיר גם את המגבלות שלהן, שהובילו לפיתוח צפנים אסימטריים. בחוברת השנייה בנושא הצפנות נציג את עקרון ההצפנה האסימטרית, שהיא שיטת ההצפנה של העולם המודרני, ונכיר אחת מהן - שיטת RSA.

חלקים ניכרים בתורת ההצפנה מבוססים על פרקים במתמטיקה, והעקרונות המתמטיים יוצגו כאן אף הם. בחוברת מפורטות דוגמאות ויש בה תרגילים רבים. כדי שתוכלו לבדוק את עצמכם, תמצאו בסוף החוברת פתרונות לתרגילים.

1. צופני שחלוף קלים

1.1. מהו צופן שחלוף?

בהצפנה על פי צופן שחלוף (substitution) מוחלפת כל אות במסר המקורי באות אחרת או בסמל, וכך מתקבל המסר המוצפן. מכאן השם צופן שחלוף. סדר האותיות אינו משתנה בתהליך ההצפנה. אחת משיטות השחלוף הפשוטות והעתיקות, הנקראת אתב"ש, מופיעה כבר בספר ירמיהו בתנ"ך. כדי להצפין בשיטה זו כותבים את האלף-בית בשתי שורות: בעליונה מן ההתחלה לסוף כמקובל, ובתחתונה במהופך - מן הסוף להתחלה, כפי שמופיע בטבלה שלהלן. המפתח הוא אפוא:

א	ב	ג	ד	ה	ו	ז	ח	ט	י	כ	ל	מ	נ	ס	ע	פ	צ	ק	ר	ש	ת
ת	ש	ר	ק	צ	פ	ע	ס	נ	מ	ל	כ	י	ט	ח	ז	ו	ה	ד	ג	ב	א

בהצפנה מחליפים כל אות בטקסט המקורי באות המופיעה בדיוק מתחתיה, וכך מתקבל המסר המוצפן.

לדוגמה, המסר: אִם אֵין אִני לִי מִי לִי

יִכתֵּב בִּאתֵּב"ש: תִּי תִמֵּט תִטֵּמ כִּמ יִמ כִּמ

לטבלה אנו קוראים מפתח ההצפנה. המפתח מורה לנו באיזה אות יש לשחלף כל אחת מאותיות המסר המקורי כדי להצפינו. כפי שהזכרנו, המפתח שהכרנו זה עתה נקרא מפתח אתב"ש. האם ברור לכם מדוע?

כדי להקשות על הפענוח, נהוג לשבור את החלוקה למילים ולקבץ את אותיות המסר המוצפן בקבוצות של 4 או 5 אותיות. כשנעשה זאת במסר המוצפן נקבל: תִיתֵמ טִתֵטֵמ כִמיֵמ כִמ.

שאלה 1

נתון המסר: צמעצ גפלכ צבנס ייפד בלזא

המסר הוצפן בצופן שחלוף במפתח אתב"ש. פענחו אותו.

מעניין לציין שבתנ"ך מופיע השימוש בצופן שחלוף במפתח אתב"ש שלוש פעמים, כולן בספר ירמיהו: בפרק כה פסוק כו נאמר: "... וּמָלֵךְ שִׁשְׁכָּה, יִשְׁתָּה אַחֲרֵיהֶם". איזו ארץ היא ששך? בהצפנת אתב"ש, בבל היא ששך. ואכן בפרק נא פסוק מא נאמר: "אֵיךְ נִלְכְּדָה שִׁשְׁכָּה, וַתִּתְּפֹשׂ תְּהִלַּת כָּל-הָאָרֶץ; אֵיךְ הָיְתָה לְשִׁמָּה בְּבֶל, בְּגוֹיִם". פסוק זה מאשר כי אמנם ששך היא בבל במפתח אתב"ש. לא ברור מדוע בחר ירמיהו להשתמש באתב"ש. באותו פרק נא, בפסוק הפותח נאמר: "הִנְנִי מַעִיר עַל-בְּבֶל, וְאֶל-יֹשְׁבֵי לֵב קָמִי--רוּחַ, מִשְׁחִית". מפרשים כי "לב קמי" היא "כשדים" באתב"ש (בדקו). הפרשנים משערים כי המניע ל"הצפנה" הוא ספרותי בלבד, מכיוון שלא נמצא צורך אחר כלשהו לכך.

שאלה 2 מה לא תעשה לחברך?

התשובה המוצפנת: תאצב טפתז כמלת כאזב צכסש גל
רמז: התשובה הוצפנה בצופן שחלוף במפתח אתב"ש.

מפתח שחלוף עברי אחר הוא אלב"מ. בשחלוף במפתח אלב"מ מחלקים את אותיות האלף-בית לשתיים: א עד כ, ל עד ת. את שתי הסדרות רושמים בטבלה בת שתי שורות:

א	ב	ג	ד	ה	ו	ז	ח	ט	י	כ
ל	מ	נ	ס	ע	פ	צ	ק	ר	ש	ת

כך יוצרים זוגות של אותיות, ומצפינים על פי הכלל שכל אות בטקסט המקורי מוחלפת באות המופיעה בדיוק מתחתיה או מעליה: א ו-ל מחליפות זו את זו, ב ו-מ מחליפות זו את זו וכך הלאה.

שאלה 3 מהי מסכה?

התשובה המוצפנת: עקאח עשקש סיאע וגשב יעלס במפק טמהז בפ
רמז: התשובה הוצפנה בצופן שחלוף במפתח אלב"מ.

1.2. צופני הזזה - צופן יוליוס קיסר

צופני הזזה (shift) הם סוג של צופני שחלוף. הם ידועים בשם צופני יוליוס קיסר, מכיוון שהוא היה הראשון שהשתמש בהם להעברת מסרים סודיים לשלטונות רומא, כבר לפני 2500 שנה. בצופני הזזה, ההסכמה בין המצפינים למפענחים פשוטה וקלה, ולכן השימוש בהם נוח. מפתח הצופן הוא מספר המוסכם רק בין שולח המסר לנמען. המספר מצביע על גודל ההזזה.

כך למשל, אם מפתח ההזזה הוא +1, אזי לצורך ההצפנה מחליפים כל אות באלף-בית בזו שאחריה. נוח לרשום את מפתח ההזזה בשתי שורות. מספר המפתח מציין מהו שיעור ההזזה של האלף-בית בשורה התחתונה ביחס לעליונה.

נתבונן למשל בשתי שורות האלף-בית הלטיני:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G

האותיות בשורה התחתונה מוזזות שמאלה ב-7 מקומות ביחס לשורה העליונה. האות A נמצאת מעל H וכל השאר הוזזו בהתאם: B מעל I, C מעל J, וכן הלאה. זהו צופן הזזה של +7. כדי להצפין מסר בצופן זה, מוצאים את האות של הטקסט המקורי בשורה העליונה, המסודרת בסדר הרגיל, ומחליפים אותה בזו שתחתיה, שהיא האות הנמצאת 7 מקומות קדימה בסדר האלף-בית.

הנה דוגמה: הטקסט המקורי הוא SAMUEL. מזיזים כל אות 7 צעדים קדימה, ומתקבל הטקסט המוצפן ZHTBLS. כדי לפענח, רושמים במקום כל אחת מאותיות המילה המוצפנת, שנמצאות בשורה התחתונה, את זו הנמצאת בדיוק מעליה.

שאלה 4  הטקסט FIEYXC מוצפן בהזזה, במפתח הזזה +4. מהו המסר המקורי?

שאלה 5  נסו להצפין את המסר "הפגישה מחר בחצות ליד הגשר", בצופן הזזה במפתח +2.

להלן המפתח:

א	ב	ג	ד	ה	ו	ז	ח	ט	י	כ	ל	מ	נ	ס	ע	פ	צ	ק	ר	ש	ת
ג	ד	ה	ו	ז	ח	ט	י	כ	ל	מ	נ	ס	ע	פ	צ	ק	ר	ש	ת	א	ב

שאלה 6  המסר שלהלן הוצפן בצופן הזזה במפתח +3:

PHHW BRX LQ RUODQGR

מהו המסר המקורי?

לעיתים קורה שבהצפנה הופכת מילה אחת לאחרת ולא לצירוף סתמי של אותיות. למשל המילה "כלב" בהזזה של +10 תהפוך ל"שתל". COLD הופכת בהזזה של +3 ל-FROG. כאן קיבלנו זאת במקרה, אבל זהו מקרה מוצלח, מכיוון שאם נראה שיש משמעות למסר המוצפן, הוא אינו מעורר חשד שהוא בעצם מוצפן.

שאלה 7 

- מהי ההצפנה של "אבן" בצופן הזזה במפתח הזזה של +10?
- מה יתקבל מהמילה PECAN אם תוצפן בצופן הזזה במפתח של +4?
- מה יתקבל מהמילה SLEEP אם תוצפן בצופן הזזה במפתח של +9?

מהו מספר ההזזות האפשרי של האלף-בית?

נחזור ליוליוס קיסר. נניח שהוא שולח לאחד ממפקדי השטח את המסר "נתקוף מייד עם שחר". הוא מצפינו ומקבל "פגטר עממז קע בכא". אם חלילה המסר המוצפן נופל בידי האויב, מתחיל מרוץ לפענוחו. אבל ברור לגמרי שאם המסר לא יפוענח עד זריחת החמה, פענוחו לאחר מכן יהיה כבר חסר ערך לאויב. מכאן ברור שחשוב להצפין בשיטה שהפענוח שלה דורש זמן רב, וכך, גם אם לבסוף המסר

יפוענח בהצלחה, הוא כבר יהיה חסר ערך. צופן הזה אינו מסובך לפיצוח, וזהו חסרונו העיקרי. אם האויב שתפס את המסר משער כי הוא הוצפן בהזזה, כדי לפצח אותו צריך פשוט לנסות את כל מפתחות ההזזה האפשריים, ומספרם אינו גדול. מהו מספר מפתחות ההזזה האפשריים בעברית? מה מספרם באנגלית?

דוגמה: נניח שנפל לידי האויב המסר המוצפן "ייממפחט". על האויב לבנות לעצמו את טבלת הפענוחים האפשריים:

המסר המוצפן	י	י	מ	מ	פ	ח	ט
הזזה 1	ט	ט	ל	ל	ע	ז	ח
הזזה 2	ח	ח	כ	כ	ס	ו	ז
הזזה 3	ז	ז	י	י	נ	ה	ו
הזזה 4	ו	ו	ט	ט	מ	ד	ה
הזזה 5	ה	ה	ח	ח	ל	ג	ד
הזזה 6	ד	ד	ז	ז	כ	ב	ג
הזזה 7	ג	ג	ו	ו	י	א	ב
הזזה 8	ב	ב	ה	ה	ט	ת	א
הזזה 9	א	א	ד	ד	ח	ש	ת
הזזה 10	ת	ת	ג	ג	ז	ר	ש
הזזה 11	ש	ש	ב	ב	ו	ק	ר

אחרי עשרה ניסיונות פענוח שנתנו צירופים חסרי משמעות של אותיות, התקבל בהזזה ה-11 ביטוי בעל משמעות, שהוא כנראה המסר המקורי.

1.3. בניית מכשיר להצפנת יוליוס קיסר

כדי להקל על הצפנה ופענוח בשיטת השחלוף באמצעות הזזה, נבנה מכשיר, שבעזרתו נוכל לקבל את כל המפתחות בבת אחת. לצורך זה השתמשו בשני זוגות העיגולים המודפסים על דפים נפרדים בנספח ב בחוברת בעמוד 42 - זוג אחד להצפנה בעברית והאחר להצפנה באנגלית. חברו את שני העיגולים במרכזיהם בעזרת סיכה כך שיהיה להם ציר מרכזי משותף ותוכלו לסובב את האחד ביחס לשני. כל סיבוב של העיגול הקטן ביחס לגדול נותן מפתח הזזה.



רשמו בעזרת מכשיר ההצפנה המעגלי שבניתם את מפתח ההצפנה בהזזה של +7 בעברית, ואת מפתח ההצפנה בהזזה של +20 באנגלית. רשמו כל מפתח בעזרת טבלה בת שתי שורות: בשורה העליונה רשמו את האותיות לפי הסדר המקובל מ-א עד ת ומ-A עד Z, ובתחתונה רשמו את האותיות המוזזות.

שאלה 9

הצפינו במפתח הזזה של +4 את המסר: "שונא מתנות יחיה - אבל ממה".

שאלה 10

הצפינו בצופן יוליוס קיסר (צופן הזזה במפתח +3) את אמרתו המפורסמת: "באתי ראיתי ניצחתי".

שאלה 11

פענחו את המסר המוצפן: שלולד כדפסחכ כוטחכ ימחדנ
רמז: המסר הוצפן בצופן הזזה במפתח +20.

שאלה 12

אמרתו המפורסמת של יוליוס קיסר, שהובאה בשאלה 10, נאמרה במקור בלטינית: VENI VIDI VICI
הצפינו אותה בצופן קיסר.

שאלה 13

נתון מסר שהוצפן בצופן הזזה במפתח של +11:

HP LCP CPLOJ EZ LEELNV NZYQTCX

מה הוא אומר?

שאלה 14

א. כשמצפינים באמצעות הזזה בעברית,

האם יש הבדל בין הצפנה בהזזה במפתח של +20 להצפנה בהזזה במפתח של -2? היעזרו במפתח ההצפנה המעגלי.

ב. כשמצפינים באמצעות הזזה באנגלית,

אילו מפתחות הזזה נותנים תוצאות זהות להזזה במפתח +19? היעזרו במפתח ההצפנה המעגלי.

אנו רואים כי לצופן ההזזה יש תכונות מתמטיות מעניינות. בכיר כעת תכונות מתמטיות נוספות של צופן ההזזה.

1.4. החשבון המודולרי של צופן יוליוס קיסר

עד כה ראינו איך אפשר לעבוד עם צופן יוליוס קיסר - צופן של שחלוף בהזזה - ולהצפין באמצעות שימוש באותיות חלופיות. אבל אפשר גם להמיר את האותיות במספרים וכך לסבך את הצופן ולהקשות עוד יותר את הפענוח שלו.

שלב א: המרת אותיות במספרים

אפשר להתייחס לאלף-בית בסדר הטבעי שלו כאילו הוא התקבל באמצעות הצפנת הזזה במפתח 0, אך מובן שלמעשה לא מדובר בהצפנה וגם לא בהזזה. הצפנת הזזה במפתח +1 מעבירה את האות א לאות ב וכן הלאה. הצפנת הזזה במפתח +2 מעבירה את האות א לאות ג וכן הלאה. בעברית יש 21 מפתחות הזזה שונים. לכן נסמן את האות ב ב-1, את האות ג ב-2 וכן הלאה, כדי לציין שמדובר בהחלפה של האות א לפי הזזה של 1 או של 2 וכן הלאה עד 21.

נקבל אפוא בעברית את מפתחות ההזזה האפשריים בטבלה זו:

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

באלף-בית הלטיני נקבל באותו אופן סימול של 25 מפתחות ההזזה האפשריים:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

שלב ב: הזזה מודולרית

ברישום בטבלאות שלעיל, לכל אות באלף-בית מותאם מספר. לראשונה 0 ולאחרונה 25 אם מדובר באנגלית, או 21 אם מדובר בעברית. כל אחד מהמספרים האלה משמש בהצפנה כערך המספרי של האות שמעליו.

נעבור עכשיו לתהליך ההצפנה.

הצפנת אות בצופן הזזה במפתח של +6 היא בעצם תוספת של 6 לערך המספרי של אותה אות. למשל באלף-בית העברי האות שהערך שלה 2 (כלומר ג), תהפוך לאות שערכה 8 (כלומר ט), ובאנגלית - האות c שערכה 2 תהפוך ל-i שערכה 8.

מה יקרה לאות העברית שערכה 20 בהזזה זו? בהזזה של 6 הופכת האות ש לאות ה. התרגום למספרים נותן ביטוי מתמטי שנראה מוזר במקצת: $20+6=4$. זוהי תוצאה של החשבון המעגלי. כדי להמחיש זאת תוכלו להיעזר שוב במכשיר ההצפנה המעגלי שבניתם.

שאלה 15

א. איזה מסר בעברית מייצגים המספרים:

21,5,17,7,1,19,7,12,5,15,9,2,9,21,5,11,11,5,17,4

ב. הצפינו אותו בצופן הזה, במפתח +15. רשמו את המסר המוצפן במספרים ובאותיות.

החישובים שערכנו בשאלה 15 הם דוגמה לחשבון שנקרא **חשבון מודולרי**. איזה מן חשבון זה? זהו חשבון שבו התוצאה של פעולת חישוב אינה יכולה לעלות על מקסימום מספרי מסוים, מכיוון שאז היא חסרת משמעות. למספר זה אנו קוראים מודול (modulus). בכל פעם שמגיעים למודול, מתחילים לספור מ-0, מן ההתחלה. זוהי מתמטיקה של חשבון מעגלי. מהו המודול במקרה שלנו? התשובה היא: 22 אם מדובר בעברית, 26 אם מדובר באנגלית.

אנחנו משתמשים בחשבון מודולרי בחיי היום-יום בחשבון השעון ובחשבון ימי השבוע. למשל, חשבון השעון הוא בעצם חשבון מודולרי במודול 12. אם השעה כעת שמונה בבוקר, כי אז בעוד שבע שעות תהיה השעה שלוש אחר הצהריים. לפי החשבון המוזר הזה צריך לרשום $3 = 8+7$. כדי להימנע מביטויים מוזרים כאלה אנו כותבים זאת כך: $(8+7) \bmod 12 = 3$

כך קוראים זאת: שמונה ועוד שבע מודול 12 שווה שלוש.

שאלה 16

השלימו את הטבלה:

השעה כעת	מה תהיה השעה בעוד	הביטוי המודולרי	התשובה
10	10 שעות	$(10+10) \bmod 12 = 8$	8
11	16 שעות		
7	24 שעות		
2	9 שעות		
	10 שעות		2
3			1
8	100 שעות		

בנו את טבלת החיבור מודול 12

+mod 12	0	1	2	3	4	5	6	7	8	9	10	11
0												
1												
2												
3												
4												
5												
6												
7								2				
8												
9											7	
10				1								
11												

חשבון ימי השבוע - (מודול 7)

כמה הם: $(4+5) \bmod 7$?

לפי הכלל שלמדנו: $(4+5) \bmod 7 = 2$

מודול 7 גם הוא מודול מוכר ושימושי. השאלה המילולית המתאימה לתרגיל האחרון עשויה להיות: "אם היום יום רביעי, איזה יום יהיה בעוד 5 ימים?" והתשובה המתקבלת בחישוב מודול 7: יום שני.

שאלה 18

א. אם היום יום ראשון, איזה יום יהיה בעוד 9 ימים? בעוד 30 יום?

ב. השלימו את הטבלה:

אם היום יום...	איזה יום יהיה בעוד...	הביטוי המודולרי	התשובה
שני	10 ימים	$(2+10) \bmod 7 = 5$	יום חמישי
ראשון	200 ימים		
רביעי	45 ימים		
שלישי	1000 ימים		
	14 יום		שבת
חמישי			שני

שאלה 19

בנו את טבלת החיבור מודול 7.

+mod 7	0	1	2	3	4	5	6
0							
1							
2							
3							
4							
5							
6							

שאלה 20

שאלה זו דומה לשאלה 14, אלא שהפעם התשובה לשאלה צריכה להיכתב בשפת הסמלים של המתמטיקה המקובלת בחשבון מודולרי.

א. כשמציפינים באמצעות הזזה בעברית, האם יש הבדל בין הצפנה בהזזה במפתח של +20 להצפנה בהזזה במפתח של -2?

ב. כשמציפינים באנגלית, אילו מפתחות הזזה נותנים תוצאות זהות להזזה במפתח +19?

הצפנה באמצעות חיבור מודולרי

נחזור לנושא ההצפנה. בחישובי ההצפנה והפענוח, המודול באנגלית הוא 26 ובעברית 22.

אם נסמן את הערך המספרי של האות במסר ב-P (plain text),

את גודל ההזזה ב-s (shift),

ואת הערך המספרי של האות המוצפנת ב-C (cipher text),

כי אז אנו יכולים לכתוב את נוסחת ההצפנה כך:

בהצפנת הזזה באנגלית: $(P+s) \bmod 26 = C$

בהצפנת הזזה בעברית: $(P+s) \bmod 22 = C$



שאלה

הכינו טבלת הצפנה לפי חיבור מודול 22:

+mod 22	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
0																						
1																						
2																						
3																						
4																						
5																						
6																						
7																						
8																						
9																						
10																						
11																						
12																						
13																						
14																						
15																						
16																						
17																						
18																						
19																						
20																						
21																						

שאלה 22

אחת מאמרותיו הידועות של צ'רצ'יל תורגמה לעברית והוצפנה בצופן שחלוף באמצעות הזזה, לפי המפתח: $(P+6) \bmod 22 = C$

האמרה המוצפנת היא:

5,6,5,11,12,13,17,17,11,16,15,15,19,19,15,6

10,9,15,13,15,10,11,12,10,15,20,11,3,5,17,11,21,0

10,18,11,17,21,5,11,16,16,5,7,19,15,3,11,5,20,18,5,0,11,0,6

מהי האמרה של צ'רצ'יל?

להמרת האותיות במספרים יש יתרונות אחדים. העבודה במספרים מאפשרת להיעזר במחשבים אלקטרוניים, והשימוש בהם מקצר ומייעל מאוד את תהליכי ההצפנה והפענוח. שימוש במחשבים מאפשר גם להשתמש בפונקציות (נוסחאות) מתמטיות ליצירת הצפנות מתוחכמות ומסובכות. כל זה מקל לבנות מערכות מאובטחות ויעילות. טיפול במספרים מספריים הוא מהיר ויעיל, גם אם ההצפנות מורכבות ומשתמשים בהן במספרים ענקיים. כדי להדגים זאת נמיר את האותיות במספרים.

1.5. סיכום ביניים של צופן יוליוס קיסר

א. לצפנים יש בדרך כלל שני מרכיבים - הוראת פעולה ומפתח. להוראת הפעולה קוראים גם אלגוריתם. במקרה של צופן יוליוס קיסר האלגוריתם הוא "להזיז". המפתח מפרט בכמה יש להזיז כדי להחליף אות אחת באחרת. בשאלה 9 למשל המפתח הוא +4, ובשאלה 10 המפתח הוא +3. באתב"ש האלגוריתם הוא "לשחלף", אבל כמו שראינו יש שחלופים אפשריים רבים. מפתח אתב"ש מפרט את כלל השחלוף במקרה הפרטי של "שחלף את האות א באות ת" וכן הלאה. גם באלב"מ האלגוריתם הוא "לשחלף" אבל מפתח השחלוף שונה: "שחלף את האות א באות ל" וכן הלאה. בהמשך נכיר שיטות הצפנה נוספות, נכיר את האלגוריתם האופייני לכל שיטה ואת המפתחות השונים המתאימים לכל אלגוריתם.

ב. ראינו כיצד אפשר להמיר אותיות במספרים לצורך ההצפנה. כך יכולנו לבטא את אלגוריתם ההזזה בנוסחה מתמטית. נוכחנו כי נוסחאות ההזזה הן נוסחאות חיבור מסוג מיוחד - חיבור מודולרי. זהו חיבור מעגלי, שבו סכום המחברים אינו יכול להיות גדול מערך המודול. המספרים שמחברים בהצפנה מייצגים אותיות, וערכו של המודול שווה למספר האותיות באלף-בית שאותן אותיות שייכות לו.

אחרי שהכרנו את החיבור המודולרי ואת שימושו בהצפנות הזזה, נעלה שאלה חדשה: האם יש גם כפל מודולרי? האם אפשר לנצל כפל כזה להצפנה? כדי שנוכל לענות על כך, נכיר שיטת הצפנה נוספת - הצפנת ערבול.

2. צפנים של ערבול

2.1. מהו צופן ערבול?

בצופן ערבול - או בשמו הלועזי צופן טרנספוזיציה (transposition) - האלגוריתם (שהוא כאמור הוראת הפעולה) הוא: "יש לשנות את **מקומן** של אותיות המסר, אבל **אין לשנות את האותיות עצמן**".

מסר המוצפן בשיטה זו יכיל בדיוק את אותן האותיות המופיעות במסר המקורי, אבל בסדר חדש. הסדר החדש נקבע באמצעות מפתח הערבול. מי שיודע מהו האלגוריתם וגם מהו המפתח, יוכל להחזיר את אותיות המסר המוצפן לסדר המקורי שלהן ללא כל קושי, וכך לפענח את המסר המוצפן. מי שיודע מהו האלגוריתם אך אינו יודע מהו המפתח, ייאלץ להתאמץ כדי לגלות את המפתח. רק אם יצליח לפצח את הצופן, יוכל לפענח את המסר.

ערבול באמצעות היפוך סדר האותיות במסר

מבין כל צופני הערבול, המפתח הפשוט ביותר הוא הכלל: יש לכתוב את המסר המקורי בסדר הפוך - מן הסוף להתחלה. לדוגמה:

אם המסר בעברית הוא	סוכן 724 יצא לדרכו
המסר המוצפן הוא	וכרדל אצי 427 נכוס
המסר המקורי באנגלית הוא	AGENT 427 IS ON HIS WAY
המסר המוצפן הוא	YAW SIH NO SI 724 TNEGA

דוגמאות להצפנות ערבול

1. המסר המוצפן: תוצחב שגפינ
המסר המקורי: ניפגש בחצות
2. המסר המוצפן: רחמ כל הכחמ ינא
המסר המקורי: אני מחכה לכ מחר

שימו לב שההצפנה מתעלמת מן האותיות הסופיות. הנוסח המדויק במסר האחרון: אני מחכה לך מחר.

מהו המסר המקורי?

2.2. צופן זיגזג

	ᵀ		ᵒ		ᵑ		ᶄ		ᶃ		ᶂ		ᵀ		ᶆ
ᵐ		ᵀ		ᵒ		ᵑ		ᶄ		ᶃ		ᶂ		ᵒ	

הפענוח

הפענוח קל ממש כמו ההצפנה - פשוט עובדים בסדר הפוך: ראשית מאחדים את כל האותיות לרצף אחד, אחר כך מחלקים את הטקסט לשניים ורושמים אותו בשתי שורות, כך:

איגע קחתי

נמיר מרימ

כעת קוראים את האותיות לסירוגין, אחת מן השורה העליונה ואחת מן השורה התחתונה וחוזר חלילה. לבסוף נותר רק לזהות את המילים שבמסר המקורי, ועל פי המשמעות שלהן להוסיף רווחים ביניהן.

אם מספר האותיות של המסר המיועד להצפנה אינו זוגי, אפשר להוסיף בסופו אות דמה אחת, כדי שיהיה אפשר לחלק אותו לשתי שורות בעלות אותו מספר אותיות. אם מספר האותיות אינו כפולה של ארבע, אפשר לבחור בחלוקה אחרת ל"מילים" או להוסיף עוד אותיות דמה, כך שמספר האותיות יתחלק ב-4.

הערות

אפשר להקשות את הפענוח באמצעות היפוך סדר האותיות בשורות המסר המוצפן. גם הפענוח ישתנה בהתאם. אפשר גם להצפין את המסר המקורי בדיגזג של שלוש שורות או יותר. למשל:

			ת			ק				ג				א
מ		י		ר		מ		ר		י		מ		נ
		י			ח				ע				י	

המסר המוצפן הוא: אגקת נמיר מרימ יעחי

שאלה 24 מה אמר האיש שנפל מבניין בן 20 קומות, כשהגיע לקומה החמישית?

התשובה המוצפנת: עעשו כבדל צילא גשדכ יהלס רארכ דורת

למה התכוון האיש?

רמז: התשובה הוצפנה באמצעות צופן זיגזג בן שתי שורות.

שאלה 25 מדוע נעים לדבר אל הקיר?

התשובה המוצפנת: היאפ מיוו רתהנ מלקר פעאנ סתאמ שארו

ובכן - מדוע?

רמז: התשובה הוצפנה באמצעות צופן זיגזג בן שתי שורות.

בכל צופן של ערבול אנו מערבלים את אותיות המסר כדי להצפינו. נכיר צורת ערבול נוספת.

2.3. צופן השביל המתפתל

בצופן השביל המתפתל, הטכניקה של ערבול אותיות המסר משוכללת יותר מאשר בצופן הזיגזג. בצופן זה משתמשים בטבלה ריבועית או מלבנית, שיש בה מספר קבוע מראש של שורות ושל עמודות.

לדוגמה, כדי להצפין את המסר "חכו לי ביום שני בעוד שבוע", סופרים תחילה את מספר האותיות במסר (20 אותיות) ובונים טבלה בהתאם (במקרה זה של 4 שורות ו-5 עמודות). משבצים את האותיות בטבלה על פי סדר כתיבתן במסר המקורי ומקבלים:

ח	כ	ו	ל	י
ב	י	ו	מ	ש
נ	י	ב	ע	ו
ד	ש	ב	ו	ע

בשלב הבא יוצרים שרשרת מן האותיות שבטבלה, לפי מסלול שהוסכם עליו מראש בין שולח המסר לבין הנמען. הנמען אמור להיות מסוגל לפענח אותו בקלות. מובן שלא כדאי להתחיל את השרשרת בשורה הראשונה מימין לשמאל, כי במקרה זה יתחיל הטקסט המוצפן במילים "חכו לי", ואז יש חשש שגם קורא לא רצוי יוכל להסתייע בכך כדי לפענח את המסר המוצפן. מסלול טוב עשוי להיות כזה המסומן באמצעות החיצים. כדי להדגים זאת הוספנו רישום מספרי של שלבי המסלול בטבלה השמאלית.

					←	←
20	13	12	5	4	↑ ח	↓ ל
19	14	11	6	3	↑ ב	↓ מ
18	15	10	7	2	↑ נ	↓ ע
17	16	9	8	1	↑ ד	↓ ו
					←	←

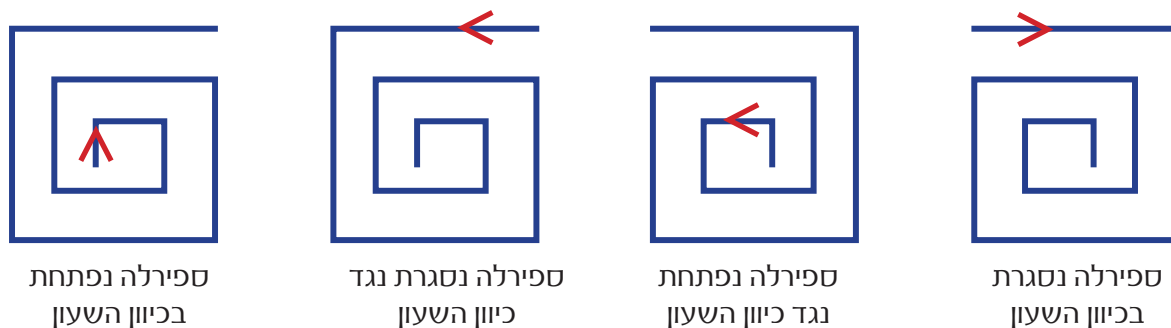
כדי להצפין, מעתיקים את האותיות שבטבלה הימנית, לפי סדר המספרים בטבלה השמאלית. מתחילים במשבצת הימנית התחתונה ומתקדמים בהתאם למספרים, למעלה, שמאלה והלאה, עד סוף המסלול. מחלקים את האותיות לקבוצות בנות 4 אותיות ומקבלים: דנבח כייש בבוו למעו עושי.

הפענוח

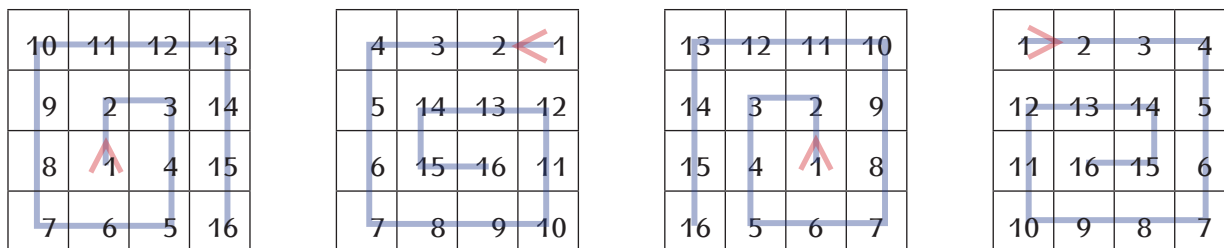
כדי לפענח, יש לשרטט טבלה זהה לטבלת ההצפנה ולמלא את המשבצות הריקות באותיות המסר המוצפן, לפי הסדר שהוסכם עליו מראש: רושמים את האות הראשונה במשבצת הימנית התחתונה וממשיכים לרשום את יתר האותיות לפי המסלול המתפתל שהוסכם עליו לצורך ההצפנה. אחרי שעושים זאת, אפשר לפענח את המסר המקורי - פשוט קוראים את האותיות מימין לשמאל, מן השורה העליונה לשורה התחתונה.

מסלול מתפתל ספירלי

מסלול מתפתל אחר להצפנה עשוי להיות המסלול הספירלי. התנועה במסלול הספירלי יכולה להיות בכיוון השעון או נגד כיוון השעון. התנועה יכולה להיות ממרכז הספירלה להיקפה או להיפך - מן ההיקף אל המרכז, הכול בהתאם למה שהוסכם מראש. התבוננו באיור 1, שמודגמות בו האפשרויות השונות. באיור 2 מייד בהמשך מופיעות ארבע טבלאות, שמוצג בהן סדר ההצפנה המתאים לכל ספירלה באיור 1.



איור 1: ארבע ספירלות שונות: נפתחות ונסגרות, בכיוון השעון ובכיוון נגדי לכיוון השעון



איור 2: ארבע טבלאות שמראות את סדר ההצפנה המתאים לכל ספירלה מהאיור הקודם

שאלה 26

הצפינו בעזרת טבלאות ההצפנה שבאיור 2 את המסר "שים שלום על כל ישראל", בכל ארבע האפשרויות.

שאלה 27

הסכמת עם שותפי הסוד שלך על הצפנה במסלול ספירלי בכיוון השעון, בטבלה של 4 שורות ו-5 עמודות. נקודת ההתחלה היא באמצע השורה השנייה מלמעלה. המסר המוצפן שקיבלת הוא: וייב עמלו כחבנ דשבו עושי מהו המסר המקורי?

שאלה 28

איך ייראה בהצפנה זו מסר מוצפן של ההודעה: "המחשב שלנו נפגע על ידי ווירוס", אם הוצפן בטבלה של 4 שורות ו-6 עמודות במסלול ספירלי בכיוון השעון, שמתחיל בפינה השמאלית התחתונה?

שאלה 29

שאלת את שותפך לסוד מהי אינפלציה. הסכמתם על תשובה מוצפנת בטבלה של 6 שורות ו-7 עמודות, מימין לשמאל ומלמעלה למטה. המסר הוצפן במסלול ספירלי נגד כיוון השעון, ותחילתו בפינה השמאלית התחתונה. התשובה המוצפנת: תידמ רתוב ייאכ אשרל אפדנ מישי דחיש כחדא ינפל וכלס כמוכ מהי אינפלציה לפי שותפך לסוד?

הערות

אם רוצים לסבך את הערבול עוד יותר, אפשר לצרף שני מסלולים שונים. למשל, אפשר לכתוב את המסר המקורי במסלול המתפתל, להציין אותו לפי המסלול הספירלי, ואחרי הפענוח לקרוא את המסר המקורי במסלול המתפתל. צריך רק לזכור כלל אחד חשוב והכרחי: כל שיטה שבוחרים בה, חייבת להיות ידועה גם לשולח וגם לנמען. ככל שהיא מסובכת יותר, קשה יותר לקרוא בלתי רצוי ("אויב") לפענח אותה.

אפשר לשנות את ממדי הטבלה בכל מסר. למשל, בראשית המסר המוצפן אפשר להוסיף מספר שיציין את מספר השורות בטבלה, ובסוף המסר מספר שיציין את מספר העמודות בטבלה. מובן שזה עלול לרמוז לקורא הבלתי רצוי מהי שיטת הערבול של המסר. אפשר לבחור בשיטות ערבול נוספות רבות, ובלבד שמקיפידים על הכלל החשוב וההכרחי - **כל המשתמשים ורק הם** יודעים מהו כלל ההצפנה.

2.4. תמורה כמושג מתמטי

עד עתה הכרנו צופני ערבול אחדים שונים זה מזה: צופן שורה, צופן זיגזג, צופן השביל המתפתל, צופן מתפתל ספירלי. במהותם כולם מתארים הצפנות המתקבלות באמצעות שינוי סדר האותיות במסר. שינוי כזה של סדר האותיות מבלי להחליף את האותיות עצמן, נקרא **תמורה של האותיות**. תמורה היא מושג מקובל במתמטיקה. נסביר אותו.

כשנתונה שרשרת מסודרת של n איברים ומשנים את הסדר שלהם, מקבלים תמורה של מרכיבי השרשרת. התמורה כוללת את כל מרכיבי השרשרת המקורית. התמורות נבדלות ביניהן בסדר המרכיבים. מעתה נבין כי צופן של ערבול הוא בעצם צופן של תמורות, וכל אחד מכללי היצירה של תמורות הוא מפתח.

ובכן, כמה מפתחות יש למסר בן n אותיות? נתחיל מדיון ב- n אותיות שונות זו מזו:

א. כמה תמורות יש למסר בן שתי אותיות? תשובה: שתי תמורות, למשל אב, בא.

ב. כמה תמורות יש למסר בן שלוש אותיות? כל אחת משלוש האותיות עשויה לשמש אות ראשונה. כלומר, יש שלוש אפשרויות לבחירת האות הראשונה. לכל אחת מהן מתאימות שתי תמורות של שתי האותיות הנותרות, כפי שראינו בסעיף א. כך נקבל: אבג, אגב, באג, בגא, גאב, גבא, ובסך הכול שש אפשרויות $2 \cdot 3 = 6$.

ג. ובמקרה של ארבע אותיות, מהו מספר התמורות? בדומה לשיקולים הקודמים, יש ארבע אפשרויות לבחירת האות הראשונה. לגבי שלוש הנותרות, נוכחנו כבר בסעיף ב כי מספר האפשרויות הוא שש, ובסך הכול $2 \cdot 3 \cdot 4 = 24$.

ד. ובמקרה שבמסר יש חמש אותיות? בדקו בעצמכם. האם קיבלתם 120? נמקו זאת.

ה. עכשיו נעבור למקרה הכללי: כמה תמורות יש למסר בן n אותיות? נבחן זאת צעד אחר צעד. יש n אפשרויות לבחירת האות הראשונה מתוך מבחר של n האותיות הנתונות. לכל אחת מ- n האפשרויות האלה יש $(n-1)$ אפשרויות לבחירת האות השנייה, כי אותה אפשר לבחור כעת רק מתוך $(n-1)$ האותיות שנותרו. לבחירת האות השלישית נותרו $(n-2)$ אפשרויות, וכך הלאה. לבסוף, כשמגיעים לאות השלישית מן הסוף נותרו שלוש אפשרויות לבחירה, לאות שלפני אחרונה נותרו רק שתיים, ולאחרונה אפשרות אחת בלבד. המספר האמור של אפשרויות הבחירה של האותיות בכל שלב הוא בהתאם לכל אחת מן האפשרויות בשלב שקדם לו. לכן המספר הכולל של האפשרויות המתקבלות הוא מכפלת מספר האפשרויות לכל אות במספר האותיות בשלב הקודם. כך למשל, בשני השלבים הראשונים מספר האפשרויות הוא $(n-1)n$, בשלושת השלבים הראשונים מספר האפשרויות הוא $(n-2)(n-1)n$. בסך הכול מספר התמורות שאפשר ליצור מ- n איברים הוא:

$$1 \cdot 2 \cdot 3 \dots \cdot (n-3) \cdot (n-2) \cdot (n-1) \cdot n$$

במתמטיקה מקובל לקרוא למכפלה של n מספרים שלמים עוקבים n עצרת. מסמנים עצרת בסימן קריאה: $n!$.

את מספר התמורות של n איברים מסמנים ב- P_n . כפי שנוכחנו, מספר התמורות שווה למכפלת המספרים הטבעיים מ-1 עד n , כלומר $n!$.

$$n(n-1)(n-2)(n-3) \cdot \dots \cdot 3 \cdot 2 \cdot 1 = n! = P_n$$

נחזור לנושא ההצפנה. אפשר לומר לסיכום, כי לכל מסר בן n אותיות שונות יש $n!$ הצפנות שונות בשיטת התמורה, כלומר הערבול.

גם כל פענוח אפשר לראות כתמורה. מה הקשר בין שתי התמורות? מה הקשר בין תמורת ההצפנה לתמורת הפענוח? ההצפנה משנה את המסר באמצעות שינוי סדר האותיות שבו, ובלשון מתמטית אפשר לומר - באמצעות יצירת תמורה של אותיות המסר. הפענוח **מבטל את השינוי ומחזיר את המצב לקדמותו**, כלומר משנה את סדר האותיות במסר המוצפן לסדר ההתחלתי שלהן במסר המקורי. הפענוח גם הוא תמורה, תמורה של המסר המוצפן. זוהי תמורה מיוחדת, **הופכית לתמורת ההצפנה**. לכן מקובל לומר בלשון מתמטית שפעולת הפענוח היא פעולה הופכית לפעולת ההצפנה. דוגמה נוספת לזוג של פעולות הופכיות זו לזו היא למשל חיבור וחיסור. מהי הפעולה ההופכית לכפל? בהמשך נרחיב ונעמיק את הדיון בנושא הפעולות ההופכיות זו לזו.

שאלה 30

- כמה מפתחות שונים להצפנת ערבול (תמורות) יש למסר: "אתה צועד לפנים"?
- הצפינו מסר זה באמצעות שלושה מפתחות (תמורות) הצפנה שונים.

עד כה טיפלנו בתמורות של מסרים שאין בהם אותיות חוזרות. כעת נבדוק כיצד משפיעות האותיות החוזרות במסר על מספר התמורות לערבול. בדקו זאת במסרים בשאלות אלה:

שאלה 31

- גג
- דוד
- חיים

א. אי אפער

ב. משה גנב ושקרן

ג. הידד לנודדים

תמורות שיש בהן חזרות

בשאלה האחרונה עסקנו במסרים שהכילו אותיות חוזרות. בלשון מתמטית, זוהי בעיה של תמורות שיש בהן חזרות. השאלה היא מה מספר התמורות של n אותיות, שלא כולן שונות זו מזו? אנחנו כבר יודעים שאם כל n האותיות שונות, אזי מספר התמורות הוא $n!$. אבל אם a אותיות מתוכן זהות, הן יכולות ליצור $a!$ תמורות ביניהן, שכולן זהות. כך הן מקטינות את מספר התמורות הכללי פי $a!$.

לכן מספר התמורות של n אותיות אשר a מתוכן זהות הוא: $\frac{n!}{a!} = Q_n$

ואם יש לנו שתי קבוצות של אותיות זהות, האחת בת a אותיות והשנייה בת b אותיות, כי אז קטן סך התמורות גם פי $b!$. והתוצאה: $\frac{n!}{a!b!} = Qn$

בדקו שנית את התוצאות שקיבלתם בשאלות 31 ו-32. האם הן מתאימות לנוסחה של מספר התמורות שיש בהן חזרות?

2.5. הסימון המתמטי לתמורה והשימוש בו

דוגמה:

נתון המסר: שבת מלכה

נסמן את אותיות המסר במספרים סידוריים משמאל לימין:

ש ב ת ס ל כ ה

אפשר לראות את המסר המקורי כתמורה אחת של האותיות המרכיבות אותו. לכל אות מתאימים מספר סידורי המציין את מקומה במסר המקורי. התמורה מוגבלת משני הצדדים באמצעות סוגריים מרובעים. אפשר לראות כל ערבול כתמורה של האותיות ושל המספרים שציינו את מקומן במסר המקורי.

הסידור המקורי, כאמור: $[1 \ 2 \ 3 \ 4 \ 5 \ 6 \ 7]$

כיכוד ייראה המסר אם יוצפן בהתאם לתמורה:

נכתוב את המסר המוצפן בשלבים:

במקום הראשון מופיעה בו האות שמספרה 7 במסר המקורי. זוהי האות ש.

לכן נכתוב **ש** במקום הראשון:

במקום השני בתמורת ההצפנה מופיעה האות הרביעית של המסר המקורי.

לכן נכתוב מ:

[מ]

חוזרים ומפעילים את אותם שיקולים לגבי המקום השלישי, הרביעי וכן הלאה, ומקבלים לבסוף את

[ש מ ל ב ה ת כ]

תמורת ההצפנה, כלומר את המסר המוצפן:

[5 1 3 6 2 4 7]

תמורת הפענוח המתאימה תהיה:

איך מצאנו זאת?

[ש ב ת מ ל כ ה]

כזכור המסר המקורי הוא:

[1 2 3 4 5 6 7]

וסדר האותיות בו:

[2 5 1 6 3 4 7]

התבוננו שנית בתמורת ההצפנה:

שימו לב כי האות ש, לא שינתה את מקומה בתמורת ההצפנה. היא נשארה במקום שמספרו 7 לכן תישאר באותו מקום גם בתמורת הפענוח. האות ב במסר המקורי מספרה 6. בתמורת ההצפנה היא נמצאת במקום הרביעי, וכדי לפענח צריך להחזירה למקומה במסר המקורי. לכן כתבנו בתמורת הפענוח את הספרה 4 משמאל לספרה 7, ומתחת לה בהתאמה את האות ב משמאל לאות ש. במסר המקורי מספרה של האות ת הוא 5, ואילו בתמורת ההצפנה היא נמצאת במקום השני. כדי להחזירה למקומה במסר המקורי נרשום בתמורת הפענוח את הספרה 2 משמאל ל-4 ואת האות ת משמאל לאות ב. חוזרים על אותם שיקולים, וכך מגיעים לתמורת הפענוח וממנה בחזרה למסר המקורי. שימו לב לקשר בין תמורת ההצפנה לתמורת הפענוח, קשר שבגללו אנו אומרים כי הן הופכיות זו לזו.

שאלה 33

נתון מסר בן 9 אותיות. נסמן אותן במספרים סידוריים מימין לשמאל.

[7 4 8 1 3 6 9 2 5]

נתונה תמורת ההצפנה:

ל י ח מ ד ה צ ד נ

נתון המסר המוצפן:

מהו המסר המקורי?

3. מקצה שיפורים לצופן יוליוס קיסר

עד תקופת ימי הביניים רק מעטים ידעו לקרוא ולכתוב, ולבטח שלא ידעו להצפין ולפענח מסרים כתובים. אולם אחרי המצאת הדפוס בידי יוהן גוטנברג במאה השש-עשרה, השיגו יותר ויותר אנשים שליטה בקריאה ובכתיבה, וצופני ההזזה הפשוטים נעשו מהר מאוד בלתי בטוחים לשימוש. כפי שנוכחנו, מכיוון שמספר מפתחות ההזזה אינו גדול - 25 באנגלית ו-21 בעברית - פיצוח צפנים אלה אינו קשה למי שידע צורת אות. גורם נוסף שבגללו הצפנת ההזזה פשוטה לפענוח, הוא הסדר הקבוע והידוע של אותיות האלף-בית, שכן פענוח של אות אחת מגלה מייד את מפתח הצופן של כל שאר האותיות.

מה אפשר לעשות כדי להתגבר על כך? אפשר **לערבל** את האותיות בערבול **שאינו הזזה** לפני הצפנתן (לפני ההזנתן). כמה מפתחות יתווספו לנו בדרך זו? ראינו כי כל ערבול הוא תמורה וכל תמורה היא מפתח, לכן מספר המפתחות הנוספים יהיה כמספר התמורות של אותיות האלף-בית - 22! בעברית, 26! באנגלית. בכל מקרה נוספים כמה מיליון מיליונים, ודי בכך. זוהי בעצם הצפנה דו-שלבית: ערבול שאינו הזזה בשלב הראשון, והזזה בשלב השני.

למען הדיוק, יש לציין כי מתוך מיליוני התמורות שנוספו לנו יש לנכות את מספר ההזזות של אותיות האלף-בית - 22 בעברית, 26 באנגלית. התמורות שתישארה - עדיין מדובר במיליוני מיליונים - יהיו כולן ערבולים שאינם הזזות.

3.1. מספר התמורות במעגל

אם עובדים עם מכשיר ההצפנה המעגלי (בדומה לזה שבניתם בסעיף 1.3) ומערבלים את אותיות המעגל הפנימי, האם מספר הערבולים (התמורות) שלהן שונה ממספר התמורות של אותן אותיות המסודרות בשורה? מה דעתכם, האם הוא גדול יותר או קטן יותר? נבדוק: בניח שנתונות n אותיות, המסודרות במעגל. כמה תמורות אפשר ליצור? תארו לעצמכם שמזיזים את האותיות. אם הן "מחוללות" במעגל שני צעדים ימינה, שלושה שמאלה - אלה אינן תמורות שונות, מכיוון שסדר האותיות בין לבין עצמן אינו משתנה. אבל אם נקבע אות אחת במקומה, מה מספר התמורות שאפשר ליצור מהשאר? נותרו $(n-1)$ אותיות, שכל אחת מהן חופשית לנוע בנפרד בלי קשר לאחרות. לכן מספר התמורות שאפשר ליצור מ- n אותיות המסודרות במעגל הוא $(n-1)!$. אפשר להגדיל לעשות - אפשר לערבול את המעורבל: אפשר להצפין את המסר באמצעות כמה ערבולים עוקבים. וכך מי שאינו מכיר את המפתח יתקשה יותר לפענח אותו, והפענוח יהיה מסובך יותר ובעיקר ממושך יותר. כבר נוכחנו כי במקרים רבים פענוח מאוחר של המסר עשוי להיות חסר ערך.

במהלך הפרק הכרנו כמה ממגבלותיו של צופן יוליוס קיסר וגילינו שאפשר להתמודד איתן באמצעות **צירוף של ערבולים** (שאינם הזזות) **ושל הזזות** (שהן סוג של ערבולים). בפרק הבא נכיר כלים מתמטיים המאפשרים ליצור ערבולים.

שאלה 34 נתונות הספרות 1, 2, 3, 4, 5.

- א. כמה מספרים שונים אפשר ליצור בעזרתן, בתנאי שבכל מספר יופיעו כל הספרות ללא חזרות?
- ב. בכמה מהם הספרה 4 מופיעה ראשונה משמאל?
- ג. בכמה מהם הספרה 4 איננה הראשונה משמאל?

שאלה 35 נתונות הספרות 1, 2, 3, 4, 5.

- א. כמה מספרים המתחלקים ב-5 אפשר ליצור מהן?
- ב. כמה מספרים זוגיים אפשר ליצור מהן?

שאלה 36

בכמה אופנים שונים אפשר להושיב שישה אנשים סביב שולחן עגול בכל אחד מהתנאים האלו:

- א. ללא הגבלות;
- ב. אדם אחד חייב להישאר במקומו;
- ג. כל האנשים חופשיים לשנות את מקומותיהם, אבל צבעו של אחד הכיסאות שונה מזה של כל האחרים;
- ד. שניים מן האנשים לא יישבו זה ליד זה בשום מצב.

שאלה 37

- על מדף בספרייה מונחים 12 ספרים: 3 ספרי ביולוגיה, 5 ספרי גאוגרפיה, 3 ספרי כימיה וספר גאומטריה אחד. כל הספרים באותו תחום הם עותקים זהים של אותו ספר. בכמה אופנים שונים אפשר לסדר את הספרים על המדף, בשני מצבים אלה:
- א. ללא כל הגבלה;
 - ב. כל הספרים הזהים יוצבו צמודים זה לזה.

שאלה 38

כמה "מילים" בנות 4 אותיות (גם חסרות מובן) אפשר ליצור מ-10 אותיות שונות בתנאים אלו:

- א. כל אות מופיעה במילה רק פעם אחת, למשל אגרח היא "מילה";
- ב. מספר החזרות של אות במילה אינו מוגבל, למשל גגג היא "מילה".

3.2. שימוש בכפל מודולרי להצפנה

ראינו כיצד אפשר להצפין מסר מילולי באמצעות שימוש בפעולת חיבור מודולרי. האם אפשר להצפין גם באמצעות כפל מודולרי? מה יקרה אם במקום להוסיף מספר קבוע לערך המספרי של כל אחת מאותיות המסר, נכפול כל אחד מהערכים המספריים הללו במספר קבוע ונכתוב את התוצאה מודול 22 (או 26)?

ננסה למשל להצפין את אותיות האלף-בית האנגלי לפי נוסחת הצפנה זו:

$$(3P) \bmod 26 = C$$

כלומר, נכפול ב-3 מודול 26. נרכז את התוצאות בטבלה. נרשום את האותיות ואת המספרים המייצגים אותן במסר המקורי ובהצפנתו:

במסר המקורי	ההצפנה	במסר המוצפן	במסר המקורי	ההצפנה	במסר המוצפן
A = 0	$(0 \times 3) \bmod 26 = 0$	A = 0	N = 13	$(13 \times 3) \bmod 26 = 13$	N = 13
B = 1	$(1 \times 3) \bmod 26 = 3$	B = 3	O = 14	$(14 \times 3) \bmod 26 = 16$	O = 16
C = 2	$(2 \times 3) \bmod 26 = 6$	C = 6	P = 15	$(15 \times 3) \bmod 26 = 19$	P = 19
D = 3	$(3 \times 3) \bmod 26 = 9$	D = 9	Q = 16	$(16 \times 3) \bmod 26 = 22$	Q = 22
E = 4	$(4 \times 3) \bmod 26 = 12$	E = 12	R = 17	$(17 \times 3) \bmod 26 = 25$	R = 25
F = 5	$(5 \times 3) \bmod 26 = 15$	F = 15	S = 18	$(18 \times 3) \bmod 26 = 2$	S = 2
G = 6	$(6 \times 3) \bmod 26 = 18$	G = 18	T = 19	$(19 \times 3) \bmod 26 = 5$	T = 5
H = 7	$(7 \times 3) \bmod 26 = 21$	H = 21	U = 20	$(20 \times 3) \bmod 26 = 8$	U = 8
I = 8	$(8 \times 3) \bmod 26 = 24$	I = 24	V = 21	$(21 \times 3) \bmod 26 = 11$	V = 11
J = 9	$(9 \times 3) \bmod 26 = 1$	J = 1	W = 22	$(22 \times 3) \bmod 26 = 14$	W = 14
K = 10	$(10 \times 3) \bmod 26 = 4$	K = 4	X = 23	$(23 \times 3) \bmod 26 = 17$	X = 17
L = 11	$(11 \times 3) \bmod 26 = 7$	L = 7	Y = 24	$(24 \times 3) \bmod 26 = 20$	Y = 20
M = 12	$(12 \times 3) \bmod 26 = 10$	M = 12	Z = 25	$(25 \times 3) \bmod 26 = 23$	Z = 23

ערכנו את הפעולה - כפל ב-3 מודול 26 - על קבוצת מספרים זו:

0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25

וקיבלנו את הקבוצה מסודרת כך:

0 3 6 9 12 15 18 21 24 1 4 7 10 13 16 19 22 25 2 5 8 11 14 17 20 23

אפשר לראות שבעצם קיבלנו תמורה של סדרת המספרים מ-0 עד 25, ובהתאמה קיבלנו תמורה של אותיות האלף-בית שהמספרים האלה מסמלים אותן. בתמורה שקיבלנו מופיעים כל המספרים שבשרשרת המקורית והם בלבד. בדקו זאת. לכן, מכיוון שכל מספר מייצג אות, לכל אות במסר המקורי מתאימה אות אחת ורק אחת במסר המוצפן.

קבוצת אותיות זו:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

הוצפנה ל:

A	D	G	J	M	P	S	V	Y	B	E	H	K	N	Q	T	W	Z	C	F	I	L	O	R	U	X
0	3	6	9	12	15	18	21	24	1	4	7	10	13	16	19	22	25	2	5	8	11	14	17	20	23

שאלה 39

הצפינו את המסר: "העקביות היא מפלטם האחרון של חסרי הדמיון",

לפי מפתח הצפנה $C = (3P) \bmod 22$.

רמז: לשם כך יש להשלים תחילה את הטבלה הבאה:

	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
$(3P) \bmod 22$	0	3	6																			
C	א	ד	ז																			

פענוח בעזרת ההופכי הכפלי

איך נבנה את טבלת הפענוח המתמטית? אם היה מדובר בחשבון רגיל ולא בחשבון מודולרי, הרי מכיוון שההצפנה נעשתה באמצעות כפל ב-3, את הפענוח אפשר לעשות באמצעות **הפעולה ההופכית לכפל**: חילוק ב-3 או כפל במספר הופכי ל-3, שהוא $\frac{1}{3}$. אבל אנחנו עוסקים בחשבון מודולרי, ותוצאת הכפל היא במודול 26. **מהו ההופכי הכפלי ל-3 במודול 26?**

ראינו שבהצפנה (בדקו שוב בטבלה): $(1 \cdot 3) \bmod 26 = 3$.

כדי לפענח אנו מחפשים: $(? \cdot 3) \bmod 26 = 1$.

נזכיר שוב את משמעות המשוואות. בהצפנה של 1 כפלנו ב-3 ורשמנו את התוצאה מודול 26. התוצאה הייתה 3. כלומר, 1 הוצפן ל-3. כדי לפענח אנו צריכים לקבל בחזרה 1. אנחנו מחפשים מספר שאם נכפול אותו ב-3, התוצאה במודול 26 תהיה 1. כלומר, השארית בחילוק ב-26 היא 1. נתחיל מהסוף: איזה מספר שהוא כפולה של 3 משאיר שארית 1 בחילוק ב-26?

$27 \bmod 26 = 1$	התשובה (אחת התשובות האפשריות) היא כמובן 27:
$(9 \cdot 3) \bmod 26 = 1$	כיוון ש-27 הוא גם כפולה של 3, הפתרון הוא:
$((1 \cdot 3) \times 9) \bmod 26 = 1$	ראינו כי:
	כלומר, ההופכי הכפלי של 3 מודול 26 הוא 9.
$?((2 \cdot 3) \times 9) \bmod 26 = 2$	נבדוק זאת במקרה נוסף - של 2. האם:
$(2 \cdot 3) \bmod 26 = 6$	ראינו בהצפנה כי:
$(? \cdot 6) \bmod 26 = 2$	כדי לפענח אנחנו צריכים לפתור:
$28 + 26 = 54$	ננסה פעם נוספת, מה לגבי 54?
$54 \bmod 26 = 2$	לכן 54 מתאים מבחינת השארית:
$6 \cdot 9 = 54$	והוא גם כפולה של 6:
$(6 \cdot 9) \bmod 26 = 2$	לכן,
	בשני המקרים שבדקנו נוכחנו כי 9 הוא ההופכי הכפלי של 3 מודול 26.
	בדקו דוגמאות נוספות. האם גם הן מאשרות ש-9 הוא ההופכי הכפלי של 3 במודול 26?
$(13 \cdot 9) \bmod 26 = ?$	
$(8 \cdot 9) \bmod 26 = ?$	
$(22 \cdot 9) \bmod 26 = ?$	
$3P \bmod 26 = C$	נוכל לסכם: כשכלל ההצפנה היה
$9C \bmod 26 = P$	אזי בכל המקרים שבדקנו כלל הפענוח היה
$(3P)9 \bmod 26 = P$	כלומר,
	בדקו את נכונות הנוסחה לגבי שאר המקרים.

השלימו את טבלת הפענוח השלמה בעזרת הנוסחה.

$P = \text{הערך המקורי} = \text{המסר}$	כפל מודול 26 = אלגוריתם ההצפנה	כפל בהופכי הכפלי מודול 26 = אלגוריתם הפענוח
0	$(0 \cdot 3) \bmod 26 = 0$	$(0 \cdot 9) \bmod 26 = 0$
1	$(1 \cdot 3) \bmod 26 = 3$	$(3 \cdot 9) \bmod 26 = 1$
2	$(2 \cdot 3) \bmod 26 = 6$	$(6 \cdot 9) \bmod 26 = 2$
3	$(3 \cdot 3) \bmod 26 = 9$	
4	$(4 \cdot 3) \bmod 26 = 12$	$(12 \cdot 9) \bmod 26 = 4$
5		$(15 \cdot 9) \bmod 26 = 5$
6	$(6 \cdot 3) \bmod 26 = 18$	$(18 \cdot 9) \bmod 26 = 6$
7	$(7 \cdot 3) \bmod 26 = 21$	$(21 \cdot 9) \bmod 26 = 7$
8	$(8 \cdot 3) \bmod 26 = 24$	
9	$(9 \cdot 3) \bmod 26 = 1$	$(1 \cdot 9) \bmod 26 = 9$
10	$(10 \cdot 3) \bmod 26 = 4$	$(4 \cdot 9) \bmod 26 = 10$
11	$(11 \cdot 3) \bmod 26 = 7$	$(7 \cdot 9) \bmod 26 = 11$
12		$(10 \cdot 9) \bmod 26 = 12$
13	$(13 \cdot 3) \bmod 26 = 13$	$(13 \cdot 9) \bmod 26 = 13$
14	$(14 \cdot 3) \bmod 26 = 16$	
15	$(15 \cdot 3) \bmod 26 = 19$	$(19 \cdot 9) \bmod 26 = 15$
16		$(22 \cdot 9) \bmod 26 = 16$
17	$(17 \cdot 3) \bmod 26 = 25$	
18	$(18 \cdot 3) \bmod 26 = 2$	
19	$(19 \cdot 3) \bmod 26 = 5$	
20	$(20 \cdot 3) \bmod 26 = 8$	
21		
22		
23		
24		
25		

3.3. הצפנה סימטרית ואסימטרית

מה המסקנות מכל החישובים שערכנו? נוכחנו כי כשמצפינים באמצעות כפל מודולרי הפענוח מסתבך. אי אפשר לפענח באמצעות המספר ההופכי וגם לא באמצעות הפעולה ההופכית שאנחנו מכירים. נוכחנו כי כשמצפינים באמצעות פעולות של החשבון הרגיל וגם באמצעות חיבור מודולרי, הרי אם יודעים מהו מפתח ההצפנה, יודעים גם מהו מפתח הפענוח - הוא פשוט ההופכי למפתח ההצפנה. אבל כשמצפינים בעזרת **כפל מודולרי**, אי אפשר לדעת בקלות מהו מפתח הפענוח גם כשיודעים מהו מפתח ההצפנה, מכיוון שמציאת ההופכי איננה מיידיית. כדי לגלות את מפתח הפענוח, נדרשנו לערוך חישובים רבים, גם כשלצורך ההצפנה השתמשנו במספר קטן של חישובים.

קיבלנו כאן הצפנה מסוג חדש. זוהי הצפנה שגם כשיודעים מהו האלגוריתם שלה ומהו המפתח שלה, בכל זאת אין יודעים לפענח אותה, וזאת בניגוד להצפנות הקודמות שהכרנו, שבהן ידיעת האלגוריתם והמפתח אפשרה פענוח מיידי. הצפנה שבה אם ידועים אלגוריתם ההצפנה ומפתח ההצפנה ידוע גם מפתח הפענוח נקראת **הצפנה סימטרית** - אותו מפתח משמש הן להצפנה הן לפענוח. לעומת זאת, **הצפנה אסימטרית** היא הצפנה שבה גם אם ידועים לנו אלגוריתם ההצפנה ומפתח ההצפנה, איננו יכולים לדעת מהו מפתח הפענוח.

החוברת הנוכחית עוסקת בהצפנה סימטרית: בכל ההצפנות שהכרנו, כשניתנו האלגוריתם והמפתח של ההצפנה, הפענוח היה ברור ומיידי. כל ההצפנות היו הצפנות **סימטריות**, פרט למקרה האחרון שבדקנו. במקרה אחרון זה ניסינו להצפין בעזרת כפל מודולרי, וקיבלנו הצפנה שונה - **הצפנה אסימטרית**: לא יכולנו לדעת מהו מפתח הפענוח אף שאלגוריתם ההצפנה וגם מפתח ההצפנה היו ידועים לנו. מה חשיבותה של הצפנה זו? ראינו שיש הכרח לשמור על סודיות המפתח וראינו שיש בעיות הנובעות מכך. האם שיטת ההצפנה האסימטרית יכולה לתרום לשיפור בתחום זה? זהו חומר למחשבה. נעסוק בו בהרחבה בחוברת הבאה. אבל בינתיים נוסיף ונעמיק לחקור את ההצפנה הסימטרית. נכיר חולשות נוספות שלה ונחפש דרכים נוספות לשפר אותה.

3.4. מגבלות הצופן המונו-אלף-ביתי

נחזור לדון בצופן קיסר ובדרכים שבאמצעותן אפשר לשפר אותו ולהפוך אותו למתוחכם יותר. עד כה הכרנו דרכים שונות ליצור תמורות של אותיות המסר וערבולים שונים שלהן, באמצעות הזזות ובאמצעות כפל של אותיות המסר המקורי. מובן שגם צירופים של שיטות ההצפנה השונות הם אפשריים, כולם מספקים מפתחות להצפנה. ראינו כי בעזרת שיטות אלה אפשר ליצור מספר עצום (מיליונים) של מפתחות (תמורות) הצפנה. אבל מתברר שאפילו שפע מפתחות זה אינו מספק את האבטחה הדרושה. כעת נבין מדוע.

לצופן קיסר יש מגבלה גדולה הנוצעת בהיותו צופן חד-חד-ערכי. נסביר זאת. התבוננו באלף-בית ובערכיו המספריים, שהסכמנו עליהם בסעיפים קודמים:

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

נצפין באמצעות הנוסחה: $3P \bmod 26 = C$

בהצפנה זו כפלנו ב-3 וקיבלנו מן השרשרת המקורית את התמורה:

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

בשרשרת המקורית יש 22 מרכיבים, ובתמורה שלה נמצאים **אותם המרכיבים והם בלבד**, אלא שהם מסודרים בסדר שונה. פירוש הדבר הוא שלכל מספר בשרשרת המקורית מתאים מספר אחד ורק אחד בתמורת ההצפנה. למשל, המספר 2 בשרשרת המקורית מתאים **אך ורק ל-6**, ולהפך - המספר 6 בתמורת ההצפנה מתאים ל-2 **בלבד**. המספר 16 בשרשרת המקורית מתאים אך ורק ל-4 בתמורת ההצפנה, ולהפך - 4 מתאים אך ורק ל-16. להתאמה כזאת בין שתי קבוצות של מספרים אנחנו קוראים התאמה חד-חד-ערכית.

מה חשיבותה של ההתאמה החד-חד-ערכית להצפנה ולפענוח? אנחנו כבר יודעים כי כל מספר בשרשרת או בתמורות שלה מייצג אות במסר. המספרים בשרשרת המקורית מייצגים את אותיות המסר המקורי, ובתמורה של השרשרת כל מספר מייצג את אחת מן האותיות במסר המוצפן. אם יש התאמה חד-חד-ערכית בין המספרים בשרשרת המקורית לבין אלה שבתמורתה, אזי גם בין אותיות המסר המוצפן לבין אותיות המסר המקורי יש התאמה חד-חד-ערכית. מדוע זה חשוב כל כך? תארו לכם מצב שבו אות מסוימת במסר המוצפן מצפינה שתי אותיות של המסר המקורי. איך נוכל לפענח אותה? איך נדע לאיזה משתי האותיות שהיא מצפינה צריך לפענח אותה? רק התאמה חד-חד-ערכית בין אותיות המסר המקורי לבין אותיות המסר המוצפן מאפשרת לפענח את המסר המוצפן פענוח חד-משמעי.

בהצפנה המבטיחה התאמה חד-חד-ערכית בין אותיות המסר לאותיות המסר המוצפן מוחלפת כל אות במסר באות אחת ורק אחת במסר המוצפן. הוא הדין גם בפענוח. כל אות במסר המוצפן מתפענחת לאות אחת ורק אחת במסר המקורי. לצופן חד-חד-ערכי מקובל לקרוא **צופן מונו-אלף-ביתי** (monoalphabetic).

אולי זה ייראה מוזר, אבל מתברר שתכונתו ההכרחית והחשובה ביותר של הצופן היא גם המגבלה הגדולה ביותר שלו. מדוע בעצם - מדוע המונו-אלף-ביתיות של צופן היא מגבלה? אנו יודעים שלכל שפה יש תכונות ותבניות לשוניות אופייניות שאינן משתנות בהצפנה מונו-אלף-ביתית. אחת מן התכונות האלה היא שכיחות אופיינית של אותיות מסוימות במילים של אותה שפה. אותיות המופיעות פעמים רבות יותר מן האחרות הן למשל האות י בעברית והאות e באנגלית. יש גם צירופי אותיות וגם מילים מסוימות שהם שכיחים יותר מאחרים. אפשר לגלות את התכונות הללו בשיטות סטטיסטיות, והן יכולות לסייע לפיצוח טקסטים מוצפנים בצופן מונו-אלף-ביתי. בחוברת הבאה נראה זאת.

בחוברת זו למדנו מהי הצפנה, והכרנו דרכים אחדות להצפנת הודעות בשיטת ההצפנה הסימטרית. הכרנו צפנים סימטריים: צופני שחלוף (למשל צופן אתב"ש), צופני הזזה (למשל צופן קיסר) וצופני ערבול, שבהם מערבלים את אותיות המסר אך לא משנים אותן.

כמו כן הכרנו את התורות המתמטיות שהצפנות סימטריות מתבססות עליהן - תורת החשבון המודולרי ותורת חשבון התמורות. נוסף על כך למדנו כיצד אפשר לפצח הצפנות כאלה בעזרת ידע על שפת הדיבור שבה נכתב המסר המקורי.

עם זאת, עדיין לא הכרנו את כל שיטות ההצפנה הסימטרית, ועל שיטות נוספות נלמד בחוברת הבאה.

עוד הכרנו סוג נוסף של צפנים שהתפתחו במהלך המאה האחרונה - צפנים אסימטריים. בהבדל מצפנים סימטריים, שבהם שולח המסר ומקבל המסר חייבים לחלוק סוד משותף (מפתח ההצפנה והפענוח), בהצפנות אסימטריות מפתח הפענוח ידוע אך ורק למקבל המסר. צורת הצפנה כזאת נמצאת בשימוש נרחב באינטרנט, כי יש לה יתרונות רבים שנכיר בחוברת הבאה.

אנחנו מקווים שהחוברת עניינה אתכם ושתמשיכו לקרוא חוברות בסדרה.

חוברות נוספות אפשר למצוא באתר האינטרנט שלנו שכתובתו: [/https://goodtoknow.tau.ac.il](https://goodtoknow.tau.ac.il)

נספח א

א. מילון מונחים עברי-אנגלי

1. אורך המפתח - key length
2. אלגוריתם ההצפנה - encryption algorithm
3. דֵס - DES (Data Encryption Standard)
4. הצפנה/צופן - encryption = encipherment = encode
5. הצפנה אסימטרית - asymmetric key cryptography
6. הצפנה סימטרית - symmetric key cryptography
7. מסר - plaintext
8. מסר מוצפן - cipher text
9. מפתח הצפנה - key
10. פענוח - decryption = decipherment = decode
11. צופן/הצפנה - cipher
12. צופן הזזה - shift cipher
13. צופן מונו-אלף-ביתי - mono alphabetic cipher
14. צופן ערבול - transposition cipher
15. צופן שחלוף - substitution cipher
16. קוד - code
17. קריפטוגרפיה - cryptography
18. קריפטולוגיה - cryptology

key length	1. אורך המפתח
בהצפנות בכלל ובהצפנות ממחשבות בפרט משתמשים במפתחות שהם מספרים. אורך המפתח מציין את מספר הספרות או הביטים שבונים אותו. אורך המפתח מצביע על המספר הגדול ביותר שאפשר להשתמש בו לשם בניית המפתח, וכך הוא מגדיר את מספר המפתחות האפשריים. ככל שאורך המפתח גדול יותר, כך רב יותר מספר המפתחות האפשריים ומתארך זמן פיצוח הצופן.	
encryption algorithm	2. אלגוריתם ההצפנה
כל כלל או תהליך הצפנה כללי, המוגדר בדיוקנות באמצעות בחירת מפתח.	
(Data Encryption Standard) DES	3. דֵס
תקן להצפנה סימטרית, שפותח בידי IBM ואומץ לשימוש בארצות הברית בשנת 1976.	
encryption = encipherment = encode	4. הצפנה
שינוי המסר המקורי למסר מוצפן באמצעות החלפת כל אות במסר באות אחרת או בסמל אחר.	
asymmetric key cryptography	5. הצפנה אסימטרית
שיטת הצפנה שבה מפתחות ההצפנה והפענוח שונים זה מזה, וידיעת מפתח ההצפנה אינה מסגירה את מפתח הפענוח.	
symmetric key cryptography	6. הצפנה סימטרית
שיטת הצפנה שבה מפתחות ההצפנה והפענוח זהים זה לזה. המונח מתאים לכל שיטות ההצפנה המסורתיות, כלומר כל אלה שהיו נהוגות לפני 1970.	
plaintext	7. מסר
המידע המקורי	
cipher text	8. מסר מוצפן
המסר לאחר הצפנתו	
key	9. מפתח הצפנה
האלמנט שהופך את אלגוריתם ההצפנה הכללי לשיטת הצפנה ייחודית, ספציפית. הנחת המצפינים היא, שחוזק המפתח הוא הקובע את חוסן ההצפנה. גם אם האויב יודע מהו אלגוריתם ההצפנה, הוא לא יוכל לפצח את המסר המוצפן אם מפתח ההצפנה חזק. לכן חשוב כל כך לשמור על סודיות המפתח.	
decryption = decipherment = decode	10. פענוח
הפיכה חוזרת של הטקסט המוצפן לטקסט המקורי.	
cipher	11. צופן
כל שיטת הצפנה להסתרת משמעות המסר באמצעות החלפת כל אות במסר המקורי באות אחרת. לשיטה יש בבסיסה מידה מסוימת של גמישות. במונח "גמישות" הכוונה היא שבהצפנות שונות עשויה אותה אות במסר המקורי להתחלף באותיות שונות במסר המוצפן. את הגמישות קובע המפתח.	
shift cipher	12. צופן הזזה
כל אות במסר המקורי מוחלפת באות אחרת, אבל סדר האותיות אינו משתנה. צופן ההזזה הראשון היה צופן יוליוס קיסר (צופן קיסר): שיטת הצפנה שבה כל אות במסר המקורי הוחלפה בזו הנמצאת שלושה מקומות אחריה.	

mono alphabetic cipher	13. צופן מונו-אלף-ביתי
בהצפנה בצופן כזה, כל אות במסר המקורי מוצפנת לאות אחת ורק אחת במסר המוצפן. כלומר, אות המופיעה במסר פעמים אחדות תוחלף בכל פעם באותה אות בדיוק. הוא הדין גם בפענוח. במתמטיקה נהוג לומר כי יש התאמה חד-חד-ערכית בין אותיות המסר המקורי לאותיות המסר המוצפן.	
transposition cipher	14. צופן ערבול
בהצפנה, אותיות המסר המקורי משנות את מקומן בלבד, מתערבלות, אבל הן אינן משתנות - כל אותיות המסר המקורי נמצאות גם במסר המוצפן.	
substitution cipher	15. צופן שחלוף
זהו צופן הזזה, שבו מידות ההזזה של אותיות המסר המקורי שונות. צופן הזזה הוא מקרה פרטי של צופן שחלוף, שבו נעשית מידה זזה של הזזה על כל אותיות המסר.	
code	16. קוד
1. דרך לייצוג מידע לפי טבלת קידוד ידועה. הטבלה חייבת לתאר התאמה חד-חד-ערכית. לדוגמה, קוד ASCII מקודדים לפי טבלת קוד ASCII, קוד מורס מקודדים לפי טבלת קוד מורס. 2. קידוד הוא גם כתיבת תוכניות בשפת המחשב. 3. צופן המורה על החלפת מילה או משפט במסר המקורי, בתו אחד או בקבוצת תווים, במסר המוצפן.	
cryptography	17. קריפטוגרפיה
מדע ההצפנה והסתרת המשמעות של המסר. משתמשים במונח זה גם כמונח נרדף לקריפטולוגיה.	
cryptology	18. קריפטולוגיה
המדע של כתבי הסתר וההצפנות למיניהם. מונח נרדף לקריפטוגרפיה.	

ב. מילון מונחים אנגלי-עברי

המספור מתאים למספור המונחים במילון המונחים העברי אנגלי

asymmetric key cryptography .5

cipher .11

cipher text .8

code .16

cryptology .18

cryptography .17

decryption .10

DES .3

encryption algorithm .2

encryption - encipherment - encode .4

key .9

key length .1

mono alphabetic cipher .13

plaintext .7

shift cipher .12

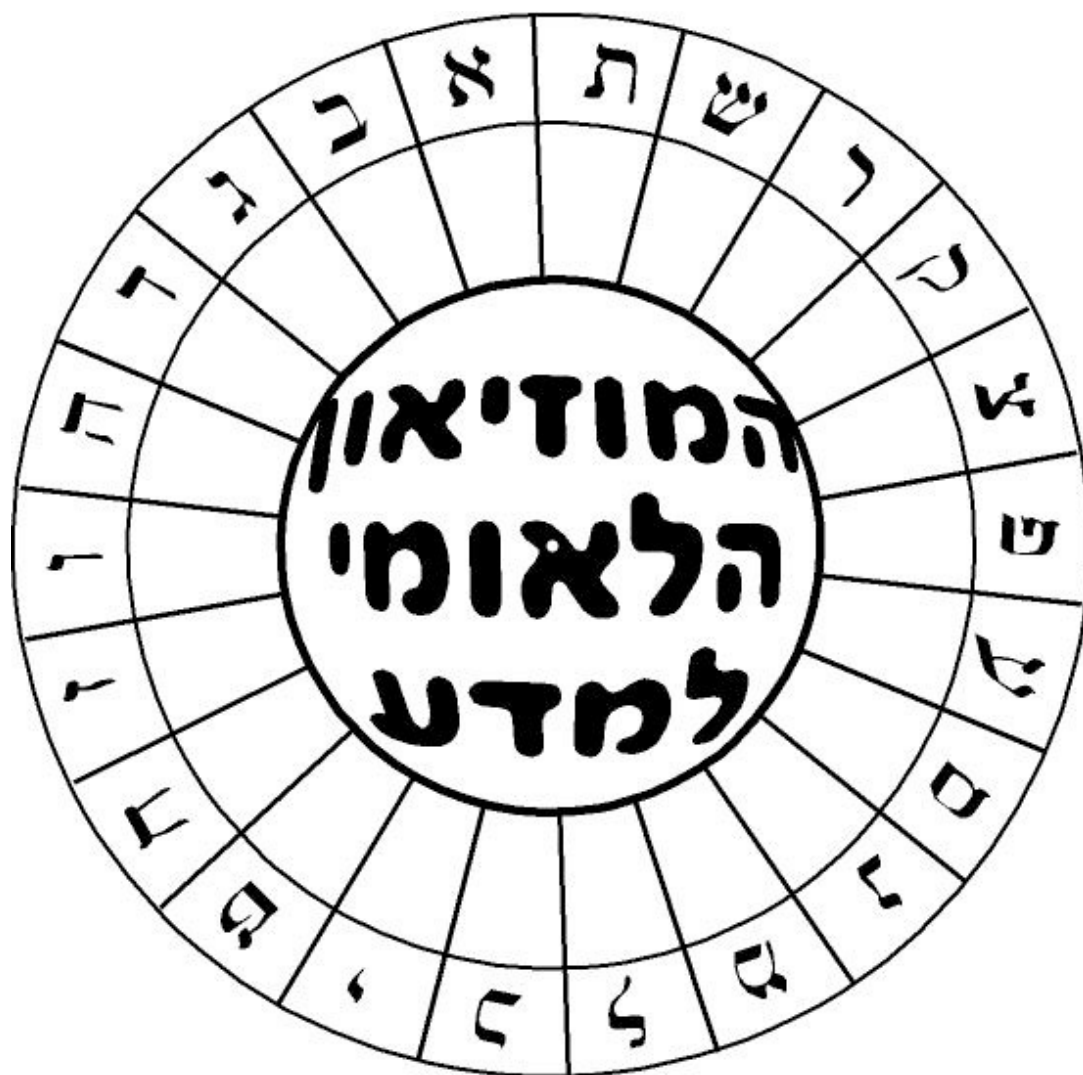
symmetric key cryptography .6

substitution cipher .15

transposition cipher .14

נספח ב

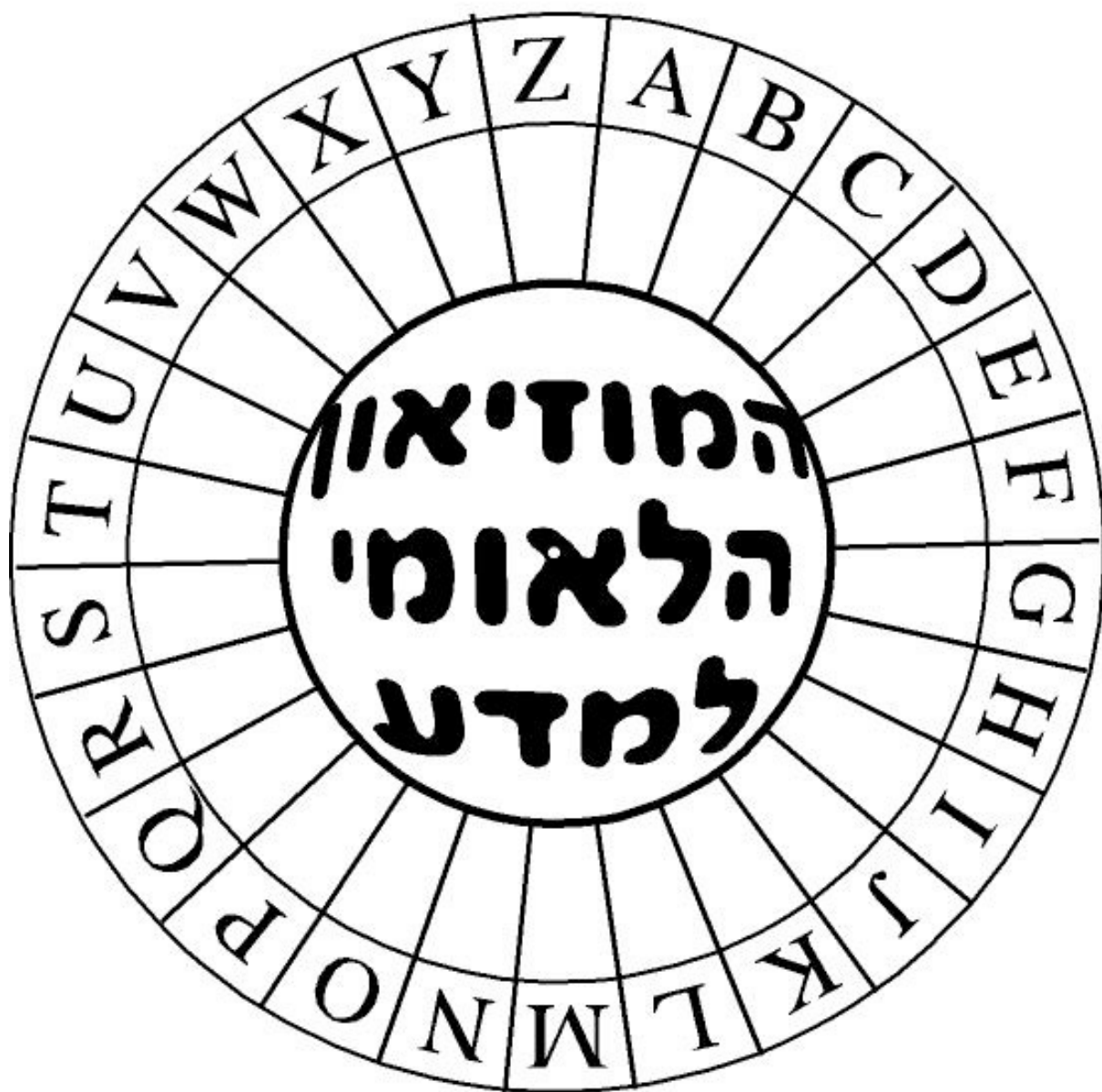
א. מעגלי הצפנה בעברית





ב. מעגלי הצפנה באנגלית





קישורים לאתרי אינטרנט בנושא מכונת האניגמה

<http://www.pbs.org/wgbh/nova/decoding/enigma.html>

אתר מומלץ של הטלוויזיה הציבורית של ארצות הברית, שיש בו חומר מדעי והיסטורי רב בנושא האניגמה.

[/https://www.bletchleypark.org.uk](https://www.bletchleypark.org.uk)

אתר בריטי המתמקד בסיפורה של האחוזה שבה פעלו מפצחי צופן האניגמה.

פתרונות

שאלה 1 

היזהרו כל השטח ממוקש כעת.

שאלה 2 

את השנוא עליך אל תעשה לחברך.

שאלה 3 

החלק היחיד של הפנים שהאדם בוחר בעצמו.

שאלה 4 

BEAUTY

שאלה 5 

זקהלאז סית דירחב נלו זהאת.

שאלה 6 

MEET YOU IN ORLANDO

שאלה 7 

א. כלב

ב. TIGER

ג. BUNNY

שאלה 8

מפתח של +7 בעברית:

א	ב	ג	ד	ה	ו	ז	ח	ט	י	כ	ל	מ	נ	ס	ע	פ	צ	ק	ר	ש	ת
ח	ט	י	כ	ל	מ	נ	ס	ע	פ	צ	ק	ר	ש	ת	א	ב	ג	ד	ה	ו	ז

מפתח של +20 באנגלית:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T

שאלה 9

גיצה פדציד נלנט - הוע פפט?

שאלה 10

הדגמ אדמגמ פמשכגמ

שאלה 11

אנחנו מוקפים מחכים לסיוע.

שאלה 12

YHQL YLGL YLFL

שאלה 13

WE ARE READY TO ATTACK CONFIRM

שאלה 14

ג. אין הבדל. מפתחות זהים בהצפנה בשיטת הזזה במפתח +20 ובמפתח -2 בעברית:

{20, 42, 64, 86, ...} וגם {-2, -24, -46, -68, ...}

ב. מפתחות זהים בהצפנה בשיטת הזזה במפתח של +19 באנגלית:

{19, 45, 71, ...} וגם {-33, -59, -85, ...}

שאלה 15

א. הצוללות יגיעו מחר בחצות.

ב. 14,20,10,0,16,12,0,5,20,8,2,17,2,14,20,4,4,20,10,19

רכשה השבצגטישואמפאכשם

שאלה 16

השעה כעת	מה תהיה השעה בעוד	הביטוי המודולרי	התשובה
		$(11+16) \bmod 12 = 3$	3
		$24 \bmod 12 = 0$	7
		$\bmod 12 = 11 \ (9+2)$	11
4		$(x+10) \bmod 12 = 2$	
	10 שעות	$(3+x) \bmod 12 = 1$	

שאלה 17

+mod 12	0	1	2	3	4	5	6	7	8	9	10	11
0	0	1	2	3	4	5	6	7	8	9	10	11
1	1	2	3	4	5	6	7	8	9	10	11	0
2	2	3	4	5	6	7	8	9	10	11	0	1
3	3	4	5	6	7	8	9	10	11	0	1	2
4	4	5	6	7	8	9	10	11	0	1	2	3
5	5	6	7	8	9	10	11	0	1	2	3	4
6	6	7	8	9	10	11	0	1	2	3	4	5
7	7	8	9	10	11	0	1		3	4	5	6
8	8	9	10	11	0	1	2	3	4	5	6	7
9	9	10	11	0	1	2	3	4	5	6		8
10	10	11	0		2	3	4	5	6	7	8	9
11	11	0	1	2	3	4	5	6	7	8	9	10

שאלה 18

א. תשעה ימים אחרי יום ראשון יהיה יום שלישי. גם בעוד 30 יום יהיה יום שלישי.

ב.

אם היום יום...	איזה יום יהיה בעוד...	הביטוי המודולרי	התשובה
		$(200+1) \bmod 7 = 5$	יום חמישי
		$(45+4) \bmod 7 = 0$	יום שבת
		$(1000+3) \bmod 7 = 2$	יום שני
שבת		$14 \bmod 7 = 0$	
	ארבעה ימים	$(x+5) \bmod 7 = 2$	

שאלה 19

+mod 7	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	4	5	6	0	1
3	3	4	5	6	0	1	2
4	4	5	6	0	1	2	3
5	5	6	0	1	2	3	4
6	6	0	1	2	3	4	5

שאלה 20

א. אין הבדל.

ב. שתי קבוצות המספרים $20 \bmod 22 = \{20, 42, 64, 86, \dots\}$

וגם $-2 \bmod 22 = \{-2, -24, -46, -68, \dots\}$

$$20 \bmod 22 = -2 \bmod 22$$

נכון לומר כי:

באופן כללי:

$$x \bmod 22 = (x-22) \bmod 22$$

אם x מפתח ההצפנה בשיטת הזזה בעברית:

ואם מעגלי ההצפנה עושים סיבובים שלמים זה ביחס לזה:

$$x \bmod 22 = (x-22+22n) \bmod 22$$

עבור סיבובים בכיוון השעון

$$x \bmod 22 = (x-22-22n) \bmod 22$$

ועבור סיבובים נגד כיוון השעון

ג. באנגלית - אם נסמן את מפתח ההזזה ב- x , נכון לכתוב: $x \bmod 26 = (x-26) \bmod 26$

עבור n סיבובים שלמים בכיוון השעון: $(x+19) \bmod 26 = (x+19+26n) \bmod 26$

ועבור n סיבובים שלמים נגד כיוון השעון: $(x+19) \bmod 26 = (x+19-26n) \bmod 26$

שאלה 21

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

שאלה 22

אינני יכול לחזות את פעולת רוסייה. זוהי חידה אפופת מסתורין בתוככי תעלומה.

שאלה 23

א. יש לי משהו חשוב למסור לך.

ב. אני מגיע מחרתיים חכו לי.

שאלה 24

עד עכשיו הכל בסדר לא צריך לדאוג.

שאלה 25

הקיר אפפע מאינ וסות ראתמ השנא מרלו

הקיר אף פעם אינו סותר את מה שנאמר לו.

שאלה 26

ש	י	מ	ש
ל	ו	מ	ע
ל	כ	ל	י
ש	ר	א	ל

א. שמיש ללשר אליע מוכל - ההצפנה בספירלה נסגרת עם כיוון השעון;

ב. שימש עילא רשלל ומלכ - ההצפנה בספירלה נסגרת נגד כיוון השעון;

ג. למוכ ראלי עשמי שללש - ההצפנה בספירלה נפתחת עם כיוון השעון;

ד. כומל ארשל לשימ שעיל - ההצפנה בספירלה נפתחת נגד כיוון השעון.

שאלה 27

י	ל	ו	כ	ח
ש	מ	ו	י	ב
ו	ע	ב	י	נ
ע	ו	ב	ש	ד

חכו לי ביום שני בעוד שבוע

שאלה 28

ש	ב	ש	ח	מ	ה
ג	פ	נ	ו	נ	ל
י	ד	י	ל	ע	ע
ס	ו	ר	י	ו	ו

המסר המוצפן במסלול ספירלי: סיגש בשחמ הלעו וירח דפנו נעלי

שאלה 29

טבלת ההצפנה

18	17	16	15	14	13	12
19	34	33	32	31	30	11
20	35	42	41	40	29	10
21	36	37	38	39	28	9
22	23	24	25	26	27	8
1	2	3	4	5	6	7

כ	א	ש	ר	ל	א	פ
א	ח	ד	א	י	נ	ד
י	כ	ס	פ	מ	פ	נ
י	ש	ל	כ	ו	ל	מ
ב	י	ח	ד	י	ש	י
ו	ת	ר	מ	ד	י	ת

פענוח: כאשר לאף אחד אין די כסף מפני שלכולם ביחד יש יותר מדי.

שאלה 30

א. מספר המפתחות כמספר התמורות, מכיוון שכל אות מופיעה במסר רק פעם אחת:

$$n! = 12! = 479,001,600$$

שאלה 31

מדובר במקרים של תמורות עם חזרות.

א. 1

$$\frac{6!}{2!} = 3 \quad \text{ב.}$$

$$\frac{4!}{2!} = 12 \quad \text{ג.}$$

שאלה 32

א. במסר בן 6 אותיות ללא חזרות, מספר התמורות הוא $6! = 720$.

במסר "אי אפשר" יש שתי חזרות של האות א, ולכן מספר תמורות ההצפנה הוא $\frac{6!}{2!} = 360$.

ב. במסר בן 11 אותיות ללא חזרות, מספר התמורות הוא $11! = 39,916,800$.

במסר "משה גב ושקן" יש שתי חזרות של האות ש ושתיים של נ, ולכן מספר התמורות הוא

$$\frac{11!}{2! \cdot 2!} = 9,979,200$$

ג. במסר בן 11 אותיות ללא חזרות, מספר התמורות הוא $11! = 39,916,800$.

במסר "הידד לנוודים" יש שתי חזרות של האות י וארבע חזרות של ד, ולכן מספר התמורות הוא

$$\frac{11!}{2! \cdot 4!} = 831,600$$

שאלה 33

צריך למצוא את תמורת הפענוח, שהיא: [6 2 5 8 1 4 9 7 3]

ולפענח את המסר: ה י ד ד ל מ נ צ ח

שאלה 34

א. $5! = 120$

ב. $4! = 24$

ג. $5! - 4! = 96$

שאלה 35

א. מספרם של כל המספרים המסתיימים ב-5 הוא $4!$.

ב. המספרים הזוגיים מסתיימים ב-2 או ב-4. מספרם $2 \cdot 4! = 48$.

שאלה 36

א. מספר התמורות של שישה איברים במעגל הוא $5! = 120$.

ב. $5! = 120$

ג. מקום האיש הראשון ביחס לכיסא שצבעו שונה יכול להיות באחד משישה מקומות, ולכן $6! = 720$.

ד. $\frac{5!}{4!} = 5$

שאלה 37

א. מספר הסידורים האפשריים של 12 ספרים שונים הוא $12! = 479,001,600$. אולם לא כל הספרים

שונים זה מזה, ולכן בתנאי השאלה יש לחלק תשובה זו ב- $3! \cdot 5! \cdot 3!$. התשובה הסופית היא

$110,880$.

ב. מכיוון שיש 4 סוגים שונים של ספרים, מספר הסידורים האפשריים הוא $4! = 24$.

שאלה 38

א. $10! / (10-4)! = 3,628,800 / 720 = 5040$

ב. $10^4 = 10,000$

שאלה 39

מבכדוער מוא סהלרס מאתנעצ כל תשנו מיסעוצ

1. D. R. Stinson: Cryptography Theory and Practice. CRC Press LLC, 1995.
 2. H. X. Mel and D. Baker: Cryptography Decrypted. Addison Wesley, 2001.
 3. R. F. Churchhouse: Codes and Ciphers (Julius Caesar, the Enigma and the Internet) Cambridge University Press 2002.
 4. M. Gardner: Codes Ciphers and Secret Writing. Dover Publication New York, 1984.
 5. S. Singh: The Code Book. Anchor Books New York 1999.
- ספר זה התפרסם גם בעברית:
- ס' סינג: סודות ההצפנה. ספרי עליית הגג - ידיעות אחרונות - ספרי חמד, 2003.
6. 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).
 7. S. Flannery: In Code A Mathematical Journey. Workman Publishing New York 2000.
 8. F. B. Wrixson: Codes, Ciphers & Other Cryptic & Clandestine Communication. Black Dog and Leventhal Publishers, 1998.
 9. A. J. Menzes, P. C. van Ooschot, S. A. Vanstone: Handbook of Applied Cryptography. Carcr.math.uwaterloo.ca/hac.

חברות "כדאי לדעת" מציגות מגוון נושאים אקדמיים וסוגיות מתקדמות בשפה שווה לכל נפש. מטרתן לחשוף את הקוראים לתחומים חדשים ולאתגר את חשיבתם. בחוברת זו נלמד על משפחה של שיטות הצפנה, שנקראות הצפנות סימטריות. הצפנות אלה היו ההצפנות היחידות בשימוש מאז ימי יוליוס קיסר ועד לרבע האחרון של המאה ה-20.

נכיר שתי שיטות להצפנה סימטרית. השיטה הראשונה היא שיטת הערבול, שבה אותיות המסר המקורי מעורבלות והמסר המוצפן מכיל את אותיות המסר המקורי בסדר שונה. כדי לפענח את המסר המוצפן יש לגלות את הסדר המקורי של האותיות. שיטת ההצפנה השניה שנכיר היא שיטת השחלוף. בהצפנה על ידי שחלוף כל אות במסר המקורי מוחלפת על ידי אות אחרת. כדי לפענח את המסר המוצפן יש לגלות את זהותה המקורית של כל אות. לסיום, נבין מדוע קוראים להצפנות אלה הצפנות סימטריות ונכיר את המגבלות שלהן.



תוכנית בנו ארבל לתלמידים צעירים מצטיינים במתמטיקה
בית הספר למדעי המתמטיקה
הפקולטה למדעים מדויקים ע"ש ריימונד וברלי סאקלר
אוניברסיטת תל אביב



goodtoknow.tau.ac.il