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

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

הצפנה

חלק א'– הצפנה סימטרית

כתיבה: תמר ריינר
בסיוע: יעל אדרי

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

מהדורה שניה, חיפה פברואר 2008

<u>תודות</u>

שתי החוברות 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 האולימפידע של מדע-טק בשנת 2003. פרוייקט שמטרתו עידוד המצויינות בקרב תלמידי חט"ב.

כשהציעה לי פרופסור נצה מובשוביץ-הדר לכתוב חומר לימוד בנושא ההצפנה, עבור משתתפי האולימפידע, 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 האולימפידע 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 האולימפידע 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 האולימיידע, 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, שטרחה 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

1 הקדמה

מאז ומתמיד היו שליטי מדינות ומצביעים צבאיים, מודעים לתוצאות החמורות, שעלולות להיות לנפילת מסרים סודיים לידי גורמים עוינים. לכן ניסו לפתח שיטות שונות להסתרת מסרים חשובים, שהעבירו זה לזה, על ידי שימוש בצפנים ובכתבי סתר. כך הלך והתפתח תחום ההצפנה, עד שהיה למדע של ממש. תחום ההצפנה מקיף מגוון של שיטות לשיבוש מסרים והסתרתם, מפני כל מי שהמסרים לא נועדו לו. לצורך זה פותחו מחלקות שלמות, שעסקו בהמצאה וביצירה של צפנים. במקביל לכך העסיק היריב או האויב, מפצחי צפנים, אנשים שכל תפקידם היה לגלות את סודותיו המוצפנים של הצד השני.

אפשר להמשיל את מפצחי הצפנים לאלכימאים, חוקרי החומר שחיו בימי הביניים וקדמו לכימאים של ימינו. הם האמינו בקיומו של חומר פלאי, שקראו לו אבן החכמים, ההופך כל חומר לזהב. הם בילו שנים רבות בניסיונות מתסכלים לגלותו. פיצוח הצופן משול לגילוי אבן החכמים. הוא נותן משמעות לאוסף סמלים, חסר פשר לכאורה. ממש כמו אבן החכמים שאמורה הייתה להפוך חומרים "נחותים" לזהב. קיים כמובן הבדל עקרוני בין האלכימאים למפצחי הצופנים. אבן החכמים היא מושג שווא, חזיון תעתועים. אבל פיצוח צופנים הוא משימה אמיתית, אם כי היא עשויה להיות מאד מפרכת.

ההיסטוריה של ההצפנה היא סיפור ההתמודדות בת אלפי השנים בין יוצרי הצפנים לבין מפצחיהם. לתחרות המוחות הזאת הייתה השפעה גדולה על מהלך ההיסטוריה האנושית. החל מיוליוס קיסר, שכבר לפני 2500 שנה, שלח לשלטונות רומא מסרים מוצפנים משדה הקרב, ועד לפרשה המרתקת של מכונת ההצפנה הגרמנית - אניגמה, שהייתה בשימוש בשנות ה- 30 וה- 40, של המאה ה- 20, והשפיעה באופן דרמטי על מהלך המערכה באירופה במלחמת העולם השניה. אלה רק שתי דוגמאות מבין רבות אחרות.

כיום אנו חיים בחברה גדושת מידע. הנגישות למקורות מידע והשימוש בסוגים שונים של מידע, רחבים יותר מאי פעם ומחלחלים לכל תחומי החיים. פעולות של יום יום כמו שיחות טלפון, שימוש בכרטיסי אשראי, ביצוע עסקות באמצעות האינטרנט ופעולות רבות נוספות כולן אינן חסינות מפני ציתות או התערבות זדונית אחרת. ההצפנה היא דרך יעילה מאוד לאבטחת חסיון המידע של היחיד ושל גופים עסקיים ואחרים.

מדע ההצפנה נקרא בלועזית קריפטוגרפיה. 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 עויינים לסדר החברתי, למשל על ידי קבוצות טרור, המתקשרות בדרך זו. גורמי בטחון פנים, במאבקם נגד הטרוריסטים, מגבירים את הציתות והמעקב אחרי כל האזרחים. מה עם חירויות הפרט? מה עם חסיון המידע? האם הם עלולים לסכן את בטחון המדינה? - חומר למחשבה.

לומדות ולומדים יקרים,

בחוברת שלפניכם תלמדו על משפחה של שיטות הצפנה, שנקראות הצפנות סימטריות. הצפנות כאלה היו בשימוש מאז ימי יוליוס קיסר, לפני 2500 שנה ועד לרבע האחרון של המאה ה- 20, לפני כ- 25 שנה. כל המצפינים במשך כל השנים האלה הכירו והשתמשו רק בהצפנות סימטריות. בהמשך לימוד החומר, בחוברת השניה, תכירו את העקרון של ההצפנה האסימטרית, שהיא שיטת ההצפנה של העולם המודרני. שיטות הצפנה רבות מבוססות על עיקרון זה. אנחנו נלמד על אחת מהן, על שיטת RSA.

בחוברת הראשונה תכירו שתי שיטות להצפנה סימטרית: שיטת הערבול בה אותיות המסר המקורי מעורבלות והמסר המוצפן מכיל את אותיות המסר המקורי אבל בסדר שונה. כדי לפענח יש לגלות את הסדר המקורי של האותיות. שיטת ההצפנה השניה שתכירו היא שיטת השחלוף. בהצפנה על ידי שחלוף 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 א-סימטריים.
חלקים ניכרים בתורת ההצפנה מבוססים על פרקים במתמטיקה. חוברת הלימוד תציג אותם בפניכם. החוברת יכולה לשמש גם ללימוד עצמי. היא מפורטת ומכילה תרגילים ודוגמאות. הקפידו לבצע את כולם. כדי שתוכלו לבדוק את עצמכם, תמצאו בסוף החוברת תשובות.

בתקווה שתיהנו.

ובברכת "תחלצום הנפצה",

תמר ריינר

2 צפני שחלוף (Substitution) קלים

2.1 מהו צופן שחלוף?

בהצפנה על פי צופן שחלוף, מוחלפת כל אות במסר המקורי באות אחרת, (או בסמל אחר), כך מתקבל המסר המוצפן. מכאן השם צופן שחלוף. סדר האותיות אינו משתנה בתהליך ההצפנה. אחת משיטות השחלוף הפשוטות והעתיקות, מופיעה כבר בספר ירמיהו בתנ"ך ונקראת אתב"ש. כדי להצפין בשיטה זו כותבים את הא"ב בשתי שורות, העליונה מן ההתחלה לסוף, כמקובל והתחתונה במהופך, מן הסוף להתחלה. זה רשום 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

ההצפנה מבוצעת על ידי החלפת כל אות בטקסט המקורי, באות שתחתיה וכך מתקבל המסר המוצפן.

לדוגמא, המסר: אם אין אני לי מי לי

ייכתב באתב"ש: תי תמט תטם כמ ימ כמ

לטבלה אנו קוראים מפתח ההצפנה. המפתח מורה לנו באיזה אות לשחלף כל אחת מאותיות המסר המקורי, על מנת להצפינו. כמו שכבר הזכרנו, המפתח שהכרנו זה עתה, נקרא מפתח אתב"ש. האם ברור לך מדוע?

כדי להקשות על הפענוח, נהוג לשבור את החלוקה למילים ולקבץ את אותיות המסר המוצפן בקבוצות של 4 או 5 אותיות. כשנבצע זאת על המסר המוצפן נקבל: תיתמ טתטמ כמימ כמ

שאלה מספר 1:

נתון המסר: צמעצ גפלכ צבנס ייפד בלזא

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

מעניין לציין שבתנ"ך מופיע השימוש בצופן שיחלוף במפתח אתב"ש שלוש פעמים, כולן בספר ירמיהו: בפרק כ"ה פסוק כ"ו נאמר: "...ומלך ששך ישתה אחריהם". איזו ארץ היא ששך? בהצפנת אתב"ש, בבל היא ששך. ואכן בפרק נ"א פסוק מ"א, נאמר: "איך נלכדה ששך ותתפוס תהילת כל הארץ! איך הייתה לשמה בבל בגויים". פסוק זה מאשר כי אמנם ששך היא בבל במפתח אתב"ש. לא ברור מדוע בחר ירמיהו להשתמש באתב"ש. באותו פרק, בפסוק הפותח נאמר: "...הנני מעיר על בבל ועל יושבי לב קמי רוח משחית". מפרשים כי "לב קמי" היא "כשדים" באתב"ש (בדקו). הפרשנים משערים כי המניע ל"הצפנה" הוא ספרותי בלבד, כיוון שלא ניתן לשער קיומו של צורך אחר לכך.

שאלה מספר 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 הא"ב לשתיים: א' עד כ', ל' עד ת'. רושמים זאת 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: א' ו- ל' מחליפות זו את זו, ב' ו- מ' מחליפות זו את זו וכך הלאה.

שאלה מספר 3:

מהי מסכה?

התשובה המוצפנת: עקאח עשקש סיאע וגשב יעלס במפק טמהז בפ

רמז: התשובה הוצפנה בצופן שחלוף במפתח אלב"מ

2.2 צופני הזזה (Shift) - צופן יוליוס קיסר

צופני הזזה הם סוג של צפני שחלוף. הם ידועים בשם צפני יוליוס קיסר, כיוון שהוא היה הראשון שהשתמש בהם, להעברת מסרים סודיים לשלטונות רומא, כבר לפני 2500 שנה. צפני הזזה הם פשוטים להסכמה בין המצפין והמפענח ולכן השימוש בהם נוח. מפתח הצופן הוא מספר, הידוע רק לשולח המסר ולנמען. מספר זה מצביע על גודל ההזזה.

כך למשל, אם מפתח ההזזה הוא 1+, אז לצורך ההצפנה מחליפים כל אות בא"ב, בזו שאחריה. נוח לרשום את מפתח ההזזה בשתי שורות. מספר המפתח מציין מהו שיעור ההזזה של הא"ב בשורה התחתונה, ביחס לעליונה.

נתבונן למשל, בשתי שורות הא"ב 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 ל- H וכל השאר הוזזו בהתאם כך שהאות B מעל ל- I, C מעל ל- J, וכך 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 ה-א"ב..

דוגמא: הטקסט המקורי: SAMUEL, מזיזים כל אות 7 צעדים קדימה. הטקסט המוצפן המתקבל: ZHTBLS.

כדי לפענח, רושמים במקום כל אחת מאותיות המלה המוצפנת, שנמצאות בשורה השניה, את זו הנמצאת בדיוק מעליה.

2.2.1 שאלות

שאלה מספר 4:

הטקסט FIEYXC מוצפן בהזזה, מפתח ההזזה 4+. מהו המסר המקורי?

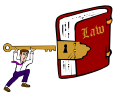
שאלה מספר 5:

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



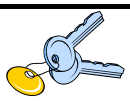
שאלה מספר 6:

המסר שלהלן הוצפן בצופן הזזה במפתח 3+:

PHHW BRX LQ RUODQGR

מהו המסר המקורי?.

לעתים קורה, שבהצפנה הופכת מלה אחת לאחרת ולא לצירוף סתמי של אותיות. למשל המלה "כלב" בהזזה של 10 תהפוך ל"שתל". COLD הופכת בהזזה של 3 ל- FROG. כאן קבלנו זאת במקרה. אבל זה מקרה מוצלח, כיוון שאם המסר המוצפן נראה כבעל משמעות הוא אינו מעורר חשד שהוא בעצם מסר מוצפן.



שאלה מספר 7:

א. מהי ההצפנה של "אבן" בצופן הזזה במפתח הזזה של 10+?

ב. מה יתקבל מ-- PECAN אם יוצפן בצופן הזזה במפתח של 4+?

ג. מה יתקבל מ-- SLEEP אם יוצפן בצופן הזזה במפתח של 9+?

2.2.2 מהו מספר ההזזות האפשרי של הא"ב?

נחזור ליוליוס קיסר, נניח שהוא שולח לאחד ממפקדי השטח את המסר, "נתקוף מיד עם שחר". הוא מצפינו ומקבל "פגתטר עמז קע בכא". אם חלילה המסר המוצפן נופל בידי האויב, מתחיל מרוץ לפיענוחו. אבל ברור לגמרי, שאם המסר לא יפוענח עד זריחת החמה, פיענוחו אחרי-כן יהיה כבר חסר ערך לאויב. מכאן רואים, שחשוב להצפין בשיטה שהפיענוח שלה דורש זמן רב. וכך, גם אם לבסוף מתבצע הפענוח בהצלחה, הוא כבר חסר ערך. צופן ההזזה אינו ממש מסובך לפיצוח וזה חסרונו העיקרי. אם האויב שתפס את המסר משער כי הוא הוצפן על ידי הזזה, אז כדי לפצח אותו, צריך פשוט לנסות את כל מפתחות ההזזה האפשריים ומספרם אינו גדול. מה מספר מפתחות ההזזה האפשריים בעברית? מה מספרם באנגלית?

דוגמא: נניח שנפל לידי האויב המסר המוצפן: "יימפחט". על האויב לבנות לעצמו את טבלת הפיענוחים האפשריים:

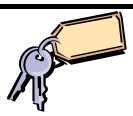
המסר המוצפן	**י**	**י**	**מ**	**מ**	**פ**	**ח**	**ט**
הזזה 1	ט	ט	ל	ל	ע	ז	ח
הזזה 2	ח	ח	כ	כ	ס	ו	ז
הזזה 3	ז	ז	י	י	נ	ה	ו
הזזה 4	ו	ו	ט	ט	מ	ד	ה
הזזה 5	ה	ה	ח	ח	ל	ג	ד
הזזה 6	ד	ד	ז	ז	כ	ב	ג
הזזה 7	ג	ג	ו	ו	י	א	ב
הזזה 8	ב	ב	ה	ה	ט	ת	א
הזזה 9	א	א	ד	ד	ח	ש	ת
הזזה 10	ת	ת	ג	ג	ז	ר	ש
הזזה 11	ש	ש	ב	ב	ו	ק	ר

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

2.3 בנית מכשיר להצפנת "יוליוס קיסר"

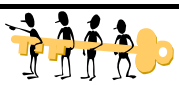
כדי להקל על הצפנה ופיענוח, בשיטת השחלוף על ידי הזזה, נבנה מכשיר, שבעזרתו נוכל לקבל את **כל** המפתחות בבת אחת. לצורך זה השתמשו בשני זוגות העיגולים, המודפסים על דפים נפרדים בנספח ב' בחוברת הלימוד. זוג אחד להצפנה בעברית והאחר להצפנה באנגלית. חברו את שני העיגולים במרכזיהם על ידי סיכה כך שיהיה להם ציר מרכזי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

2.3.1 שאלות



שאלה מספר 8:

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 האותיות לפי הסדר המקובל מ- א' עד ת', או מ- A עד Z ובתחתונה רשמו את האותיות המוזזות.



שאלה מספר 9:

הצפינו במפתח הזזה של 4+ את המסר: שונא מתנות יחיה – אבל ממה?

שאלה מספר 10:

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

שאלה מספר 11:

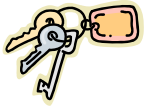
פענחו את המסר המוצפן: שלולד כדפסחכ כוטחכ ימחדנ

רמז: המסר הוצפן בצופן הזזה במפתח 20+.

שאלה מספר 12:

אימרתו המפורסמת של יוליוס קיסר, שהובאה בשאלה 10, נאמרה במקור בלטינית: VENI VIDI VICI

הצפינו אותה בצופן קיסר.



שאלה מספר 13:

נתון מסר שהוצפן בצופן הזזה במפתח של 11+:

HP LCP CPLOJ EZ LEELNV NZYQTCX

מה הוא אומר?

שאלה מספר 14:

א. כשמצפינים על ידי הזזה, בעברית,

האם יש הבדל בין הצפנה בהזזה במפתח של 20+ ובין הצפנה בהזזה במפתח של 2-? (העזרו במפתח ההצפנה המעגלי)

ב. כשמצפינים באנגלית,

אילו מפתחות הזזה נותנים תוצאות זהות להזזה במפתח 19+? (העזרו במפתח ההצפנה המעגלי)

אנו רואים כי לצופן ההזזה תכונות מתמטיות מעניינות. בקטע הבא נכיר תכונות מתמטיות נוספות של צופן ההזזה.

2.4 החשבון המודולרי של צופן יוליוס קיסר (צופן שחלוף על ידי הזזה)

עד כאן ראינו איך אפשר לעבוד עם צופן "יוליוס קיסר" (צופן של שחלוף על ידי הזזה) ולהצפין עלידי שימוש באותיות חלופיות. אבל אפשר גם להמיר את האותיות במספרים וכך לתת לצופן תוספת סיבוך ולהקשות עוד יותר על הפענוח שלו.

2.4.1 שלב א: המרת אותיות במספרים

אפשר להתייחס לא"ב בסדר הטבעי, כאילו זו הצפנת הזזה במפתח אפס. כמו שכבר הזכרנו, זו אינה הצפנה וגם לא הזזה של ממש. הצפנה בהזזה במפתח 1+, מעבירה את האות א' לאות ב' וכו'. 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 וכו', 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 הבאה:

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

בא"ב 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

2.4.2 שלב ב: הזזה מודולרית

ברישום בטבלאות שלעיל, לכל אות בא"ב 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 בא"ב העברי: האות 2 (=ג), תהפוך ל- 8 (=ט). ובאנגלית c=2 תהפוך ל- i=8

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

שאלה מספר 15:

א. איזה מסר בעברית מיוצג על ידי 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 הזזה, במפתח 15+. רשמו את המסר המוצפן במספרים ובאותיות.

החישובים שבצענו בשאלה 15ב' הם דוגמא לחשבון שנקרא **חשבון מודולרי**. איזה מן חשבון זה? זהו חשבון, שבו התוצאה של פעולת חישוב אינה יכולה לעלות על מקסימום מספרי מסוים, כיוון 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.

אנו 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 אחה"צ. לפי החשבון המוזר הזה צריך לרשום 8+7=3. כדי להימנע מביטויים מוזרים כאלה אנו כותבים זאת כך:

$$(8+7) \bmod 12=3$$

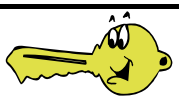
קוראים זאת: שמונה ועוד שבע מודולו 12 שווה שלוש.

2.4.3 שאלות

שאלה מספר 16:

מלאו 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		



שאלה מספר 17:

בנו את טבלת החיבור מודולו 12

+mod12	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 – (מודולו 7)

כמה הם: $(4+5) \bmod 7$?

לפי הכלל שלמדנו: $(4+5) \bmod 7 = 2$

מודולו 7 גם הוא מודול מוכר ושימושי. השאלה המילולית, שמתאימה לתרגיל האחרון עשויה להיות:

"אם היום יום רביעי, איזה יום יהיה בעוד 5 ימים?" והתשובה ע"י חישוב מודולו 7: "יום שני".

שאלה מספר 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) mod 7=5	יום חמישי
ראשון	200 ימים		
רביעי	45 ימים		
שלישי	1000 ימים		
	14 יום		שבת
חמישי			שני

שאלה מספר 19:

בנו את טבלת החיבור מודולו 7.

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

שאלה מספר 20:

שאלה זו היא אותה שאלה כמו שאלה מספר 14 אלא, שהפעם, התשובה לשאלה צריכה להכתב בשפת הסמלים של המתמטיקה המקובלת בחשבון מודולרי.

א. כשמצפינים על ידי הזזה, בעברית, האם יש הבדל בין הצפנה בהזזה במפתח של 20+ ובין הצפנה בהזזה במפתח של 2-?

ב. כשמצפינים באנגלית, אילו מפתחות הזזה נותנות תוצאות זהות להזזה במפתח 19+?

2.4.4 הצפנה על ידי חיבור מודולרי

נחזור לנושא ההצפנה. בחישובי ההצפנה והפיענוח, המודול הוא 26 (באנגלית) או 22 (בעברית).

אם נסמן את: הערך המספרי של האות במסר P= (plain text)

גודל ההזזה s = (shift)

הערך המספרי של האות המוצפנת C = (cipher text)

כי אז אנו יכולים לכתוב את נוסחת ההצפנה בצורה שלהלן:

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

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

2.4.5 שאלות

שאלה מספר 21:

הכינו טבלת הצפנה לפי חבור מודולו 22:

+mod22	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 מספר 22:

אחת מאמרותיו הידועות של צ'רצ'יל תורגמה לעברית והוצפנה בצופן שחלוף על ידי הזזה, לפי המפתח:

$$(P+6) \bmod 22 = C$$

האימרה 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 האימרה של צ'רצ'יל?

להמרת האותיות במספרים, יש יתרונות אחדים. העבודה במספרים מאפשרת להיעזר במחשבים אלקטרוניים בתחום זה. השימוש במחשבים מקצר ומייעל מאוד את תהליכי ההצפנה והפיענוח. השימוש במחשבים מאפשר גם שימוש בפונקציות (נוסחאות) מתמטיות, ליצירת הצפנות מתוחכמות ומסובכות. כל זה מקל על יצירת מערכות מאובטחות ויעילות. טיפול במסרים מספריים הוא מהיר ויעיל, גם כשההצפנות מורכבות ומשתמשות במספרי ענק. כדי להדגים זאת נמיר את האותיות למספרים.

2.5 סיכום ביניים של צופן יוליוס קיסר

א. לצופנים 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 8 למשל, המפתח 4. אבל בשאלה 9, המפתח 3. באתב"ש האלגוריתם הוא "שחלף", אבל כמו שראינו יש הרבה שחלופים אפשריים. מפתח אתב"ש מפרט את כלל השחלוף במקרה הפרטי, "שחלף א' עם ת'" וכו'. גם באלב"מ האלגוריתם הוא "שחלף" אבל המפתח של השחלוף שונה, "שחלף א' עם ל'" וכו'. בהמשך נכיר שיטות הצפנה נוספות, נכיר את האלגוריתם האופייני לכל שיטה ואת המפתחות השונים המתאימים לכל אלגוריתם.

ב. כשעסקנו בצופן יוליוס קיסר, ראינו כיצד אפשר להמיר אותיות במספרים לצורך ההצפנה. על ידי כך יכולנו לבטא את אלגוריתם ההזזה בנוסחה מתמטית. נוכחנו כי נוסחאות ההזזה הן נוסחאות חיבור מסוג מיוחד, חיבור מודולרי. זהו חיבור מעגלי, שבו סכום המחוברים לא יעלה אף פעם על המודול. המספרים שמחברים בהצפנה מייצגים אותיות וערכו של המודול שווה למספר האותיות בא"ב אליו שייכות אותן האותיות. אחרי שהכרנו את החיבור המודולרי ואת שימושו בהצפנות הזזה, נעלה שאלה חדשה: האם קיים גם כפל מודולרי? האם אפשר לנצל אותו להצפנה? כדי שנוכל לענות על כך נכיר שיטת הצפנה נוספת.

3 צפנים של ערבול (Transposition)

3.1 מהו צופן ערבול?

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

המסר המוצפן בשיטה זו, יכיל בדיוק את אותן האותיות כמו המסר המקורי, אבל בסדר חדש. הסדר החדש נקבע על ידי מפתח "הערבול". זה שיודע מהו האלגוריתם וגם מהו המפתח, יוכל להחזיר את אותיות המסר המוצפן, ללא כל קושי, לסדר המקורי שלהן וכך לפענח את המסר המוצפן. זה שיודע מהו האלגוריתם (יודע שהמסר עורבל), אך אינו יודע מהו המפתח, יאלץ להתאמץ כדי לגלות אותו. רק אם יצליח "לפצח" את הצופן, יוכל לפענח את המסר.

3.1.1 ערבול על ידי היפוך סדר האותיות במסר

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

אם המסר הוא: סוכן 427 יצא לדרכו

המסר המוצפן הוא: וכרדל אצי 724 נכוס

באנגלית:

המסר המקורי: AGENT 427 IS ON HIS WAY

וכדי להצפינו כותבים: YAW SIH NO SI 724 TNEGA

3.1.2 דוגמאות להצפנות ערבול

1. המסר המוצפן: תוצחב שגפנ

   המסר המקורי: נפגש בחצות

2. המסר המוצפן: רחמ כל הכחמ ינא

   המסר המקורי: אני מחכה לכ מחר.

(שימו לב שההצפנה מתעלמת מן האותיות הסופיות. הנוסח המדויק: אני מחכה לך מחר)

שאלה מספר 23:

א. נתון המסר המוצפן: כל רוסמל בושח והשמ יל שי

ההצפנה בוצעה על כתיבת אותיות המסר המקורי מן הסוף להתחלה.

מהו המסר המקורי ?

ב. נתון המסר המוצפן: יל וכח מייתרחמ עיגמ ינא

אלגוריתם ההצפנה הוא ערבול והמפתח, רישום אותיות המסר המקורי בסדר הפוך.

מהו המסר המקורי ?

3.1.3 בעיה למחשבה

שימו את המשפטים המוצפנים מול מראה. האם אפשר לפענח אותם בעזרת הבבואה שלהם? מה ההבדל בין תמונתו של המסר המוצפן במראה לבין המסר המקורי? איזה מאותיות המסר המוצפן מתפענחות בבבואתן ואיזה אינן מתפענחות?

3.1.4 פלינדרום

יש מלים, שהמשמעות שלהם אינה תלויה בכוון הקריאה שלהם. למשל המלים: יהי, ביב, הגיגה (מחשבתה, הרעיון שלה). יש גם משפטים כאלה. נסו למשל את ההוראה באנגלית: PULL UP IF I PULL UP. האם היא תשתנה אם תכתבו אותה מן הסוף להתחלה? בדקו זאת.

מלים או משפטים מסוג זה נקראים פלינדרומים. חיפוש פלינדרומים עשוי להיות שעשוע מהנה. נסו זאת.

3.2 צופן "זיגזג"

עד עתה הכרנו צפני ערבול שבהם אותיות המסר המוצפן נכתבו בשורה, כמו האותיות במסר המקורי רק בסדר שונה. אפשר לקרוא לצפנים כאלה צפני שורה. כעת נכיר צפני ערבול נוספים.

נתייחס אל המסר "אני מגיע רק מחרתיים", להצפנתו פועלים כך: קודם כל מונים את מספר האותיות (המסר כולל 16 אותיות). בשלב הבא, כותבים את המסר בזיגזג, בשתי שורות, כך:

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

לסיום ההצפנה מעתיקים את שתי השורות, בזו אחר זו.

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

לבסוף מחלקים את המסר המוצפן לקבוצות של 4 אותיות, מעין "מילים" ומתקבלת הצורה הסופית של הטקסט המוצפן: איגע קחתי נמיר מרימ

3.2.1 הפענוח

הפענוח קל, ממש כמו ההצפנה, פשוט עובדים בסדר הפוך: ראשית מאחדים את כל האותיות לרצף אחד, אחר כך מחלקים את הטקסט לשני חצאים 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 המלים שבמסר המקורי ועל פי המשמעות שלהן, להכניס את הרווחים ביניהן.

אם מספר האותיות של המסר המיועד להצפנה, אינו זוגי, אפשר להוסיף בסופו אות דמה אחת, כדי שיהיה אפשר לחלקו לשתי שורות שבשתיהן 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.

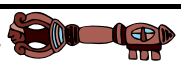
3.2.2 הערות

אפשר להקשות על הפענוח על ידי היפוך סדר האותיות בשורות המסר המוצפן. גם הפענוח ישתנה בהתאם. אפשר גם להצפין את המסר המקורי בזיגזג של שלוש שורות (או יותר). למשל:

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

המסר המוצפן הוא: אגקת נמיר מרימ יעחי

3.2.3 שאלות



שאלה מספר 24:

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

התשובה המוצפנת: עעשו כבדל צילא גשדכ יהלס ראכר דורת

למה התכוון האיש?.

(רמז: התשובה הוצפנה על ידי צופן זיגזג בן שתי שורות.)

שאלה מספר 25:

מדוע נעים לדבר אל הקיר?

התשובה המוצפנת: היאפ מיוו רתהנ מלקר פעאנ סתאמ שארו

ובכן – מדוע?

(רמז: התשובה הוצפנה על ידי צופן זיג זג בן שתי שורות)

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

3.3 צופן השביל המתפתל

בצופן השביל המתפתל הטכניקה של ערבול אותיות המסר משוכללת יותר מאשר בצופן הזיגזג. בצופן זה משתמשים בטבלה ריבועית או מלבנית ובה מספר קבוע מראש של שורות ועמודות.

לדוגמא, כדי להצפין: **"חכו לי ביום ששי בעוד שבוע"**

סופרים תחילה את מספר האותיות (במסר 20 אותיות) ובונים טבלה (במקרה זה של 4 על 5 משבצות) בהתאם. בהמשך משבצים את האותיות בטבלה על פי סדר כתיבתן במסר המקורי ומקבלים:

ח	כ	ו	ל	י
ב	י	ו	מ	ש
ש	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, שאמור להיות מסוגל לפענח אותו בקלות. כמובן שלא כדאי להתחיל את השרשרת בשורה הראשונה, מימין לשמאל, כי במקרה זה יתחיל הטקסט המוצפן במלים "חכו לי" ,ואז יש סכנה שגם קורא לא רצוי יוכל להסתייע בכך כדי לפענח את המסר המוצפן. מסלול טוב עשוי להיות כזה המסומן על ידי החצים. כדי להדגיש זאת הוספנו רישום מספרי של שלבי המסלול בטבלה השמאלית.

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

ח↑	כ↓	ו↑	ל↓	י↑
ב↑	י↓	ו↑	מ↓	ש↑
ש↑	י↓	ב↑	ע↓	ו↑
ד↑	ש↓	ב↑	ו↓	ע↑

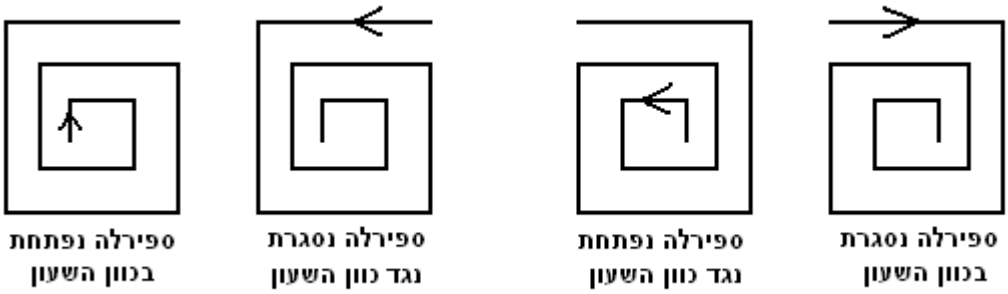
כדי להצפין, מעתיקים את האותיות, שבטבלה הימנית, לפי הסדר של המספרים בטבלה השמאלית. (מתחילים במשבצת הימנית התחתונה ומתקדמים בהתאם למספרים, למעלה, שמאלה והלאה, עד סוף המסלול), מחלקים אותן לקבוצות של 4 אותיות ומקבלים: **דשבח כייש בבוו למעו עושי**

3.3.1 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, על ידי קריאת האותיות מימין לשמאל, מן השורה העליונה לשורה התחתונה.

3.3.2 מסלול מתפתל ספירלי

מסלול מתפתל אחר להצפנה, עשוי להיות המסלול הספירלי. התנועה במסלול הספירלי, יכולה להיות בכיוון השעון או נגד כוון השעון. התנועה יכולה להיות ממרכז הספירלה להיקפה או להיפך, מן ההיקף אל המרכז של הספירלה (הכל לפי מה שהוסכם מראש). התבוננו ב**איור 3.1** מודגמות האפשרויות השונות.



ארבע ספירלות שונות, "נפתחות" או "נסגרות", בכוון השעון ובכיוון נגדי לכיוון השעון

1	2	3	4
12	13	14	5
11	16	15	6
10	9	8	7

13	12	11	10
14	3	2	9
15	4	1	8
16	5	6	7

4	3	2	1
5	14	13	12
6	15	16	11
7	8	9	10

10	11	12	13
9	2	3	14
8	1	4	15
7	6	5	16

ארבע טבלאות שמראות את סדר ההצפנה שמתאים לכל ספירלה מהאיור הקודם.

3.3.3 שאלות

שאלה מספר 26:

הצפינו בעזרת טבלות ההצפנה, שבסוף הסעיף הקודם, את המסר "שים שלום על כל ישראל", בכל 4 האפשרויות.

שאלה מספר 27:

הסכמת עם שותף הסוד שלך על הצפנה במסלול ספירלי, בכוון השעון, בטבלה של 4 שורות ו- 5 עמודות, ההתחלה היא באמצע השורה השניה מלמעלה.

המסר המוצפן שקבלת הוא: וייב עמלו כחבש דשבו עושי

מהו המסר המקורי?

שאלה מספר 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, שמתחיל בפינה השמאלית התחתונה, בכוון השעון?

שאלה מספר 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, שתחילתו בפינה השמאלית התחתונה וכוונו נגדי לזה של השעון.

התשובה המוצפנת: תידם רתוב ייאכ אשרל אפדנ מישי דחיש כחדא ינפל וכלס פמוכ

מהי אינפלציה לפי שותפך לסוד?

3.3.4 הערות

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

אפשר לשנות את ממדי הטבלה בכל מסר. במקרה כזה אפשר להוסיף בראשית המסר המוצפן מספר, שיציין את מספר השורות בטבלה ובסוף המסר מספר, שיציין את מספר העמודות בטבלה. כמובן שזה עלול להיות רמז ל"אויב", מהי שיטת הערבול של המסר. אפשר לבחור בשיטות ערבול נוספות רבות, ובלבד ששומרים על התנאי, החשוב וההכרחי – **כל** המשתמשים **ורק הם** יודעים מהו כלל ההצפנה**.**

3.4 תמורה כמושג מתמטי

עד עתה הכרנו מספר צפני ערבול, הם נראים שונים זה מזה וגם נקראים בשמות שונים: צופן שורה, צופן "זיגזג", צופן המסלול המתפתל, ספירלה ועוד. במהותם כולם מתארים הצפנות המושגות על ידי שנוי סדר האותיות במסר. שנוי סדר האותיות בינן לבין עצמן, נקרא **תמורה של האותיות.** "תמורה" היא מושג מקובל במתמטיקה, נסביר אותו.

כשנתונה שרשרת מסודרת של *n* אברים 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. כל 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 כראשונה 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 הכל 2x3=6.

ג. ובמקרה של ארבע אותיות, מהו מספר התמורות? בדומה לשיקולים הקודמים, קיימות ארבע אפשרויות לבחירת האות הראשונה, לגבי שלוש הנותרות, נוכחנו כבר (בסעיף ב') כי מספר האפשרויות הוא שש ובסך הכל 2x3x4=24.

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

ה. עכשיו נעבור למקרה הכללי: כמה תמורות יש למסר בן *n* אותיות? נבחן זאת צעד אחר צעד. קיימות *n* אפשרויות לבחירת האות הראשונה (מתוך מבחר של n האותיות הנתונות). לכל אחת מן האפשרויות האלה קימות (*n-1*) לבחירת האות השניה, כי אותה כבר אפשר לבחור מתוך(*n-1*) האותיות שנותרו. לבחירת האות השלישית נותרו (*n-2*) אותיות וכך הלאה. לבסוף, כשמגיעים לאות השלישית מן הסוף, נותרו שלוש אפשרויות. במקום הלפני אחרון נותרו רק שתי אותיות לבחירה ובאחרון, אחת בלבד. מספר אפשרויות הבחירה של האותיות בכל שלב הן לכל אחת מן האפשרויות בשלב שקדם לו. לכן מספר האפשרויות שמתקבלות בשני השלבים הראשונים, למשל, הוא *n(n-1)*, בשלושת השלבים הראשונים מספר האפשרויות הוא *n(n-1)(n-2)*. בסך הכל מספר התמורות שאפשר ליצור מ- *n* אברים הוא:

1x2x3...x(n-3)(n-2)(n-1) n

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

את מספר התמורות של *n* אברים, מסמנים ב- *Pn*. כפי שנוכחנו הוא שווה למכפלת המספרים הטבעיים מ- 1 עד n, כלומר *n!*.

n (n-1)(n-2)(n-3)x...x3x2x1=n!=Pn

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

גם כל פענוח אפשר לראות כתמורה.מה הקשר בין שתי התמורות? מה הקשר בין תמורת ההצפנה לתמורת הפענוח? ההצפנה משנה את המסר, על ידי שנוי סדר האותיות בו. בלשון מתמטית נגיד על ידי יצירת תמורה של אותיות המסר. הפענוח **מבטל את השינוי ומחזיר את המצב לקדמותו**. 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. דוגמא נוספת לזוג של פעולות הופכיות, זו לזו, היא למשל החיבור והחיסור. מהי הפעולה ההופכית לכפל? בהמשך נרחיב ונעמיק את הדיון בנושא הפעולות ההופכיות זו לזו .

3.4.1 שאלות

שאלה מספר 30:

א. כמה מפתחות שונים להצפנת ערבול (תמורות), יש למסר: "אתה צועד לפנים"?

ב. הצפינו את המסר הנ"ל, באמצעות שלושה מפתחות (תמורות) הצפנה שונים.

עד כה טפלנו בתמורות של מסרים, שאין בהם אותיות חוזרות. כעת נבדוק כיצד משפיעות האותיות החוזרות במסר על מספר התמורות לערבולו? בדקו זאת במסרים הבאים:

שאלה מספר 31:

כמה תמורות יש למילים:

א. גג

ב. דוד

ג. חיים

שאלה מספר 32:

כמה תמורות יש למסרים:

א. אי אפשר

ב. משה גנב ושקרן

ג. הידד לנודדים

3.4.2 תמורות עם חזרות

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

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

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

בדקו שנית את התוצאות שקבלתם בשאלות 28 ו- 29. האם הן מתאימות לנוסחה של מספר התמורות עם חזרות?

3.5 הסימון המתמטי לתמורה והשימוש בו

דוגמא:

נתון המסר: שבת מלכה

נסמן את אותיותיו במספרים סידוריים משמאל לימין: [1 2 3 4 5 6 7]

ש ב ת מ ל כ ה

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

הסידור המקורי, כאמור: [1 2 3 4 5 6 7]

כיצד ייראה המסר אם יוצפן בהתאם לתמורה: [2 5 1 6 3 4 7]?

נכתוב את המסר המוצפן בשלבים:

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

לכן נכתוב **ש** במקום הראשון: [ש]

במקום השני בתמורת ההצפנה מופיעה האות הרביעית של המסר המקורי.

לכן נכתוב **מ:** [מ]

חוזרים ומפעילים את אותם השיקולים, לגבי המקום השלישי, הרביעי וכו' ומקבלים לבסוף את תמורת ההצפנה (המסר המוצפן): [ש מ ל ב ה ת כ]

תמורת הפענוח המתאימה תהיה: [7 4 2 6 3 1 5]

איך מצאנו זאת?

כזכור המסר המקורי: [ש ב ת מ ל כ ה]

וסדר האותיות בו: [7 6 5 4 3 2 1]

התבוננו שנית בתמורת ההצפנה: [7 4 3 6 1 5 2]

שימו לב כי האות ש', לא שנתה 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 במקום הרביעי כדי לפענח צריך להחזירה למקומה במסר המקורי, לכן כתבנו בתמורת הפענוח את הספרה 4 משמאל למספר 7 ומתחת לה בהתאמה, את האות ב' משמאל לאות ש'. האות ת' במסר המקורי מספרה 5. בתמורת ההצפנה היא 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 השיקולים וכך מגיעים לתמורת הפענוח וממנה חזרה למסר המקורי. שימו לב לקשר בין תמורת ההצפנה לתמורת הפענוח, קשר שבגללו אנו אומרים כי הן הופכיות זו לזו.

שאלה מספר 33: נתון מסר בן 9 אותיות. נסמן אותן במספרים סידוריים מיחין לשמאל

נתונה תמורת ההצפנה: *[5 2 9 6 3 1 8 4 7]*

נתון המסר המוצפן: *ל י ח מ ד ה צ ד נ*

מהו המסר המקורי?

4 מקצה שיפורים לצופן קיסר

4.1 הקדמה

עד לתקופת ימי הביניים רק מעטים ידעו לקרוא ולכתוב, ולבטח שלא ידעו להצפין או לפענח מסרים כתובים. אולם עם המצאת הדפוס באירופה, על ידי יוהן גוטנברג במאה ה- 16, השיגו יותר ויותר אנשים שליטה בקריאה ובכתיבה וצפני ההזזה הפשוטים הפכו מהר מאוד לבלתי בטוחים לשימוש. כפי שנוכחנו, כיוון שמספר מפתחות ההזזה אינו גדול (25 בשפה האנגלית ו- 21 בעברית), פיצוחם אינו קשה למי שיודע צורת אות. גורם נוסף שהופך את הצפנת ההזזה לפשוטה לפענוח על ידי גורם עוין, הוא הסדר הקבוע והידוע של אותיות הא"ב. בגללו, **פענוח של אות אחת מגלה מייד את מפתח הצופן של כל שאר האותיות.**

מה אפשר לעשות כדי להתגבר על כך? אפשר **לערבל** את האותיות, **ערבול שאינו הזזה**, לפני הצפנתן (לפני הזזתן). כמה מפתחות זה מוסיף לנו? ראינו כבר, כי כל ערבול הוא תמורה וכל תמורה היא מפתח, לכן מספר המפתחות הנוספים כמספר התמורות של אותיות הא"ב, !22 בעברית, !26 באנגלית. בכל מקרה זה כמה מיליון מיליוני מיליונים, וזה מספיק. זוהי בעצם הצפנה דו שלבית: ערבול שאינו הזזה בשלב הראשון, והזזה בשלב השני. (הערה: למען הדיוק יש לציין כי ממיליוני התמורות שנוספו לנו, יש לנכות את מספר ההזזות של אותיות הא"ב, 22 בעברית, 26 אם מדובר באנגלית. התמורות שתשארנה, כולן ערבולים שאינם הזזות. עדיין מיליוני מיליונים.)

4.2 מספר התמורות במעגל

אם עובדים עם מכשיר ההצפנה המעגלי (זה שבניתם בסעיף 2.3) ומערבלים את אותיות המעגל הפנימי, האם מספר הערבולים (התמורות) שלהן, שונה ממספר התמורות של אותן אותיות המסודרות בשורה? מה דעתכם, האם הוא יותר גדול? יותר קטן? נבדוק: נניח 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, כיוון שסדר האותיות בינן לבין עצמן לא השתנה. אבל אם נקבע אות אחת במקומה, מה מספר התמורות שאפשר ליצור מהשאר? נותרו *(n-1)* אותיות חופשיות לנוע כל אחת בנפרד, ללא קשר לאחרות ולכן מספר התמורות האפשרי, שאפשר ליצור מ- *n* אותיות, המסודרות במעגל הוא *!(n-1)*. אפשר להגדיל לעשות, אפשר לערבל את המעורבל. אפשר להצפין על ידי מספר ערבולים של המסר וכך הופך הפענוח, לזה שאינו מכיר את המפתח, ליותר מסובך ובעיקר יותר ממושך. כבר נוכחנו כי במקרים רבים מתקיים הפסוק - "עבר זמנו בטל קרבנו", פענוח מאוחר של המסר עלול להיות חסר ערך.

במהלך הפרק הכרנו כמה ממגבלותיו של צופן יוליוס קיסר וגילינו כיצד ניתן להתמודד איתן, על ידי **צירוף ערבולים** (שאינם הזזות) **והזזות** (שהן סוג של ערבולים). בפרק הבא נכיר כלים מתמטיים ליצירת הערבולים.

4.2.1 שאלות

שאלה מספר 34:

נתונות הספרות 1, 2, 3, 4, 5:

א. כמה מספרים שונים אפשר ליצור בעזרתן (בכל מספר כל הספרות ללא חזרות)?

ב. בכמה מהם הספרה 4, ראשונה משמאל?

ג. בכמה מהם 4 איננה הראשונה משמאל?

שאלה מספר 35:

נתונות הספרות מן השאלה הקודמת (1, 2, 3, 4, 5):

א. כמה מספרים שמתחלקים ב- 5 אפשר ליצור מהן?

ב. כמה מספרים זוגיים אפשר ליצור מהן?

שאלה מספר 36:

בכמה אופנים שונים אפשר להושיב 6 אנשים סביב שולחן עגול?

א. ללא הגבלה.

ב. יש אדם אחד שאינו זז ממקומו.

ג. אם כל האנשים חופשיים לשנות את מקומותיהם, אבל אחד הכיסאות הוא בצבע שונה מזה של כל האחרים?

ד. אם שניים מן האנשים מסרבים לשבת זה ליד זה?

שאלה מספר 37:

על מדף בספריה מונחים 12 ספרים: 3 ספרי ביולוגיה, 5 ספרי גיאוגרפיה, 3 ספרי כימיה וספר אחד בגיאומטריה. כל הספרים באותו תחום הם עותקים זהים זה לזה, של אותו ספר. בכמה אופנים שונים אפשר לסדר את הספרים על המדף?

א. ללא הגבלה?

ב. כך שכל הספרים הזהים יהיו ניצבים צמודים זה לזה?

שאלה מספר 38:

כמה "מלים" בנות 4 אותיות (גם חסרות מובן), אפשר ליצור מ- 10 אותיות שונות?

א. כל אות מופיעה במילה רק פעם אחת (למשל אגרח היא "מילה")?

ב. מספר החזרות של אות במילה אינו מוגבל (למשל גגגג היא "מילה")?

4.3 שימוש בכפל מודולרי להצפנה

ראינו כיצד ניתן להצפין מסר מילולי על ידי שימוש בפעולת חיבור מודולרי. האם אפשר להצפין גם על ידי כפל מודולרי? מה יקרה אם במקום להוסיף מספר קבוע לערכה המספרי של כל אחת מאותיות המסר, נכפול כל אחד מהם במספר קבוע ונכתוב את התוצאה מודולו 22 (או 26)?

ננסה למשל, להצפין את אותיות הא"ב האנגלי לפי נוסחת ההצפנה הבאה:

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

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	(0x3)mod26=0	A=0	N=13	(13x3)mod26=13	N=13
B=1	(1x3)mod26=3	B=3	O=14	(14x3)mod26=16	O=16
C=2	(2x3)mod26=6	C=6	P=15	(15x3)mod26=19	P=19
D=3	(3x3)mod26=9	D=9	Q=16	(16x3)mod26=22	Q=22
E=4	(4x3)mod26=12	E=12	R=17	(17x3)mod26=25	R=25
F=5	(5x3)mod26=15	F=15	S=18	(18x3)mod26=2	S=2
G=6	(6x3)mod26=18	G=18	T=19	(19x3)mod26=5	T=5
H=7	(7x3)mod26=21	H=21	U=20	(20x3)mod26=8	U=8
I=8	(8x3)mod26=24	I=24	V=21	(21x3)mod26=11	V=11
J=9	(9x3)mod26=1	J=1	W=22	(22x3)mod26=14	W=14
K=10	(10x3)mod26=4	K=4	X=23	(23x3)mod26=17	X=17
L=11	(11x3)mod26=7	L=7	Y=24	(24x3)mod26=20	Y=20
M=12	(12x3)mod26=10	M=12	Z=25	(25x3)mod26=23	Z=23

כתוצאה מן הפעולה שבצענו (כפל ב- 3 מודולו 26) קבלנו מקבוצת המספרים:

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

את הקבוצה המסודרת 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 קבלנו תמורה של סדרת המספרים מ- 0 ועד 25, ובהתאמה קבלנו תמורה של אותיות הא"ב, שהמספרים האלה מסמלים אותן. בתמורה שקבלנו, מופיעים כל המספרים שבשרשרת המקורית והם בלבד.(בדקו זאת!) כיוון שכל מספר מייצג אות, אז אותו הדבר חל גם עליהן, כלומר לכל אות במסר המקורי, מתאימה אות אחת ורק אחת במסר המוצפן.

קבוצת האותיות:

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 מספר 39:

הצפינו את המסר:

"העקביות היא מפלטם האחרון של חסרי הדמיון",

לפי מפתח הצפנה C = 22 mod(3P).

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)mod22	0	3	6																			
C	א	ד	ז																			

4.3.1 הפענוח בעזרת ההופכי הכפלי

איך נבנה את טבלת הפענוח המתמטית? אם היה מדובר בחשבון רגיל (ולא בחשבון מודולרי), אז כיוון שההצפנה בוצעה על ידי כפל ב- 3, הפענוח יכול להתבצע על ידי **הפעולה ההופכית לכפל**, על ידי **חילוק ב- 3**, **או על ידי כפל במספר הופכי ל- 3, כפל ב-** $\frac{1}{3}$. אבל אנחנו עוסקים בחשבון מודולרי ותוצאת הכפל היא במודול 26. **מהו ההופכי הכפלי ל- 3, מודול 26?**

ראינו שבהצפנה (חיזרו ובדקו בטבלה): 3 = (1x3) mod 26.

כדי לפענח אנו מחפשים: 1 = (?x3) mod 26.

נזכיר שוב את המשמעות של 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?

התשובה (אחת התשובות האפשריות) היא כמובן 27: 1 = 27 mod 26

כיוון ש- 27 הוא גם כפולה של 3, הפתרון הוא: 1 = (9x3) mod 26,

ראינו כי: 1 = ((1x3)x9)mod 26.

כלומר, ההופכי הכפלי של 3 מודול 26 הוא 9.

נבדוק זאת במקרה נוסף, של 2. האם: 2 = ((2x3)x9)mod 26?

ראינו בהצפנה כי: 6 = (2x3) mod 26

כדי לפענח אנחנו צריכים לפתור: 2 = (?x6) mod 26

נחזור על ההסבר. אנחנו מחפשים מספר שאם נכפול אותו ב- 6 (הערך המוצפן), ונחלק ב- 26, התוצאה תהיה 2 (הערך המקורי). ננסה 28. הוא אמנם משאיר שארית 2 במודול 26, אבל הוא אינו כפולה של 6, לכן אינו מתאים.

ננסה פעם נוספת, מה לגבי 54? 28+26=54,

לכן 54 מתאים מבחינת השארית: 54 mod 26 = 2,

והוא גם כפולה של 6: 6x9=54.

לכן, (6x9) mod 26 = 2.

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?

(13x9) mod 26=?

(8x9)mod 26=?

(22x9)mod 26=?

נוכל לסכם: כשכלל ההצפנה היה 3P mod 26=C,

אז בכל המקרים שבדקנו, כלל הפענוח היה 9C mod 26=P.

כלומר, ((3P)9)mod 26 = P.

בדקו את נכונות הנוסחה לגבי שאר המקרים.

השלימו את טבלת הפענוח השלמה בעזרת הנוסחה.

כפל בהופכי הכפלי מודול 26 = אלגוריתם הפיענוח	כפל מודול 26 = אלגוריתם ההצפנה	P = הערך המקורי = המסר
(0x9)mod 26 = 0	(0x3)mod 26 = 0	0
(3x9)mod 26 = 1	(1x3)mod 26 = 3	1
(6x9)mod 26 = 2	(2x3)mod 26 = 6	2
	(3x3)mod 26 = 9	3
(12x9)mod26 = 4	(4x3)mod 26 = 12	4
(15x9)mod 26 = 5		5
(18x9) mod 26 = 6	(6x3)mod 26 = 18	6
(21x9)mod 26 = 7	(7x3)mod 26 = 21	7
	(8x3)mod 26 = 24	8
(1x9)mod 26 = 9	(9x3)m0d 26 = 1	9
(4x9)mod 26 = 10	(10x3)mod 26 = 4	10
(7x9)mod 26 = 11	(11x3)mod 26 = 7	11
(10x9)mod 26 = 12		12
(13x9)mod 26 = 13	(13x3)mod 26 = 13	13
	(14x3)mod 26 = 16	14
(19x9)mod 26 = 15	(15x3)mod 26 = 19	15
(22x9)mod 26 = 16		16
	(17x3)mod 26 = 25	17
	(18x3)mod 26 = 2	18
	(19x3)mod 26 = 5	19
	(20x3)mod 26 = 8	20
		21
		22
		23
		24
		25

4.4 הצפנה סימטרית ואסימטרית

מה המסקנות מכל החישובים שביצענו? נוכחנו כי כשמצפינים על ידי כפל מודולרי הפענוח מסתבך. אי אפשר לבצע אותו, על ידי המספר ההופכי וגם לא על ידי הפעולה ההופכית, שאנו מכירים. נוכחנו כי כשמצפינים על ידי פעולות של החשבון הרגיל (או גם על ידי חיבור מודולרי), אז אם יודעים את מפתח ההצפנה, יודעים גם את מפתח הפענוח (שהוא פשוט ההופכי למפתח ההצפנה). אבל כשמצפינים בעזרת כפל **מודולרי**, **אי אפשר לדעת בקלות מהו מפתח הפענוח גם כשיודעים מהו מפתח ההצפנה,** כיוון שמציאת ההופכי אינה מיידית. כדי לגלות את מפתח הפענוח, נדרשנו לבצע חישובים רבים, גם כשלצורך ההצפנה השתמשנו במספר קטן של חישובים.

קבלנו כאן הצפנה מסוג חדש. הצפנה שגם כשיודעים את האלגוריתם שלה ואת המפתח שלה, עדיין אין יודעים לפענח אותה. זאת בניגוד להצפנות הקודמות שהכרנו, בהן ידיעת האלגוריתם והמפתח אפשרה פענוח מיידי. להצפנה שבה ידיעת אלגוריתם ההצפנה ומפתח ההצפנה, פירושה ידיעת מפתח הפענוח קוראים **הצפנה סימטרית.** להצפנה שבה ידיעת אלגוריתם ההצפנה ומפתח ההצפנה אינה מגלה את מפתח הפענוח קוראים **הצפנה אסימטרית**.

שמה של החוברת הנוכחית הוא הצפנה סימטרית, כעת גם ברור מדוע. בכל ההצפנות שהכרנו ובכל התרגילים, כשניתנו האלגוריתם והמפתח של ההצפנה, הפענוח היה ברור ומיידי. כל ההצפנות היו הצפנות **סימטריות**, פרט למקרה האחרון שבדקנו. במקרה זה נסינו להצפין בעזרת כפל מודולרי וקבלנו הצפנה שונה, **הצפנה אסימטרית**. בהצפנה הזאת, לא יכולנו לדעת את מפתח הפענוח, למרות שידענו הן את אלגוריתם ההצפנה והן את מפתח ההצפנה. מה חשיבותה של תגלית זו? ראינו את ההכרח של שמירת סודיות המפתח ואת הבעיות הנובעות מכך. האם שיטת ההצפנה האסימטרית יכולה לתרום לשיפור בתחום זה?- חומר למחשבה. נרחיב בו בחוברת הבאה. אבל בינתיים נוסיף ונעמיק לחקור את ההצפנה הסימטרית. נכיר חולשות נוספות שלה ונחפש דרכים נוספות לשיפורה.

4.5 מגבלות הצופן המונו-אלפביתי

נחזור לדון בצופן קיסר ובדרכים שונות לתחכומו ולשיפורו. בדיוננו הקודם בנושא, הכרנו דרכים שונות ליצירת תמורות של אותיות המסר, ערבולים שונים שלהן, על ידי הזזות ועל ידי כפל אותיות המסר המקורי. כמובן 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 המפתחות הזה, אינו מספק את האבטחה הדרושה. כעת נבין מדוע.

לצופן קיסר מגבלה רצינית הנעוצה בעובדה שהוא חד-חד-ערכי. נסביר זאת. התבוננו בא"ב ובערכיו המספריים שעליהם הסכמנו 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 על ידי הנוסחה: $3P \bmod 26 = C$

בהצפנה זו קבלנו 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 22 מרכיבים ובתמורה שלה **אותם המרכיבים והם בלבד**, אלא שהם מסודרים בסדר שונה. פרוש הדבר הוא שלכל 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 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 מייצג כל מספר אחת מן האותיות במסר המוצפן. אם בין המספרים בשרשרת המקורית ובין אלה שבתמורתה, קיימת התאמה חד-חד-ערכית, אז גם בין אותיות המסר המוצפן לבין אותיות המסר המקורי קיימת התאמה חד-חד-ערכית. מדוע זה כל כך חשוב? 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 פענוח חד-משמעי של המסר המוצפן.

הצפנה שמבטיחה התאמה חד-חד-ערכית בין אותיות המסר לאותיות המסר המוצפן משמעותה היא, כי בעת ההצפנה, מוחלפת כל אות במסר, על ידי אות 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-אלפביתי (monoalphabetic).** זוהי מילה לועזית שמבטאת את העובדה, שמדובר בהתאמה חד-חד-ערכית, בין אותיות המסר המקורי לאותיות המסר המוצפן.

אולי זה ייראה מוזר, אבל מתברר שתכונתו ההכרחית והחשובה ביותר של הצופן היא גם המגבלה הגדולה ביותר שלו. מדוע בעצם? מדוע המונו-אלפביתיות של צופן היא מגבלה? התשובה לכך נובעת מן העובדה, שלכל שפה תכונות ותבניות לשוניות אופייניות שאינן משתנות בהצפנה מונו-אלפביתית. אחת מן התכונות האלה היא שכיחות אופיינית של אותיות מסוימות במילים של אותה שפה, (אותיות שמופיעות הרבה יותר מן האחרות הן למשל האות י' בעברית, או האות e באנגלית). גם צירופי אותיות וגם מלים מסוימות הם יותר שכיחים מאחרים. תכונות אלה ניתנות לגילוי בשיטות סטטיסטיות ויכולות לסייע, לפיצוח טקסטים מוצפנים בצופן מונו-אלפביתי בפרק הבא נראה זאת.

5. איך מפצחים צפני שחלוף מונו-אלפביתיים?

5.1 עקרון קרקהוף - מה קובע את חוזק ההצפנה?

עמידותו של צופן כנגד פיצוח, כלומר **מידת הקושי הכרוכה בפיצוחו**, תלויים במפתח הרבה יותר מאשר באלגוריתם. יותר מזה, בדרך כלל מניח המצפין, כי יריבו יודע מהו אלגוריתם ההצפנה, אבל אין היריב יודע מהו מפתח ההצפנה. במצב זה, גם אם היריב יתפוס את המסר המוצפן, עדיין כל משימת הפיצוח לפניו. עדיין הוא צריך לבדוק את כל המפתחות האפשריים, המתאימים לאלגוריתם, כדי לפענח את המסר המוצפן. אם המסר הוצפן על ידי אלגוריתם של הזזה, מספר המפתחות האפשריים אינו גדול, רק 25 (אם מדובר בשפה האנגלית). אבל אם מדובר על אלגוריתם של שחלוף, מספר המפתחות הוא כל התמורות האפשריות של 26 האותיות, כלומר !26. זה מספר עצום של מפתחות. מספר בן 27 ספרות. 400,000,000,000,000,000,000,000,000. גם אם היריב יודע **בוודאות** כי המסר המוצפן שנפל בידיו הוצפן באלגוריתם של שחלוף, ידיעתו אינה מקטינה כהוא זה, את המספר העצום של המפתחות שעליו לבדוק כדי לפענח את המסר המוצפן. **במילים אחרות, סודיות האלגוריתם אינה חשובה, אבל לסודיות המפתח חשיבות קריטית.**

הראשון שקבע זאת היה הבלשן ההולנדי אוגוסט קרקהוף (Auguste Kerckhoff), בשנת 1883. הוא ניסח את "עקרון קרקהוף" לפיו: " אבטחתה של שיטת הצפנה אסור שתהיה תלויה בשמירה על סודיות אלגוריתם ההצפנה. האבטחה תלויה רק בשמירה על סודיות המפתח". כשמדברים על חוזק של הצפנה, מתכוונים לחוזקה על פי עקרון זה.

5.2 שימוש בתכונות השפה לפיצוח צפנים

פיצוח של צפני שחלוף זו מיומנות, שדורשת מידה רבה של ידע וניסיון, כדי שהביצוע יהיה מהיר. כבר הזכרנו קודם לכן, כי תכונות רבות של השפה הכתובה נשמרות בהצפנה מונו-אלפביתית והאויב העירני יזדרז לעשות בהן שימוש. היתרון של השימוש בשיטה זו הוא קיצור הדרך. איננו מפענחים את המסר המוצפן על ידי **תקיפת מפתח ההצפנה** (כי נוכחנו שזה עלול לקחת זמן רב), אלא על ידי **תקיפת המסר המוצפן** עצמו. כדי להצליח צריך להכיר את התכונות של השפה בה הוצפן המסר.

5.2.1 תכונות מעניינות של השפה האנגלית

בדיקות של טקסטים רבים בשפה האנגלית, העלו את הממצאים הבאים:

1. האות השכיחה ביותר (שמופיעה יותר מכל אות אחרת, כמעט בכל טקסט), היא E. אחריה על פי מידת שכיחותן באות, מימין לשמאל: N, O, A, T.
2. האות השכיחה ביותר בסוף מילה, היא E.
3. האות השכיחה ביותר בראשית מילה, היא T.
4. יש שתי מילים בנות אות אחת והן: I ו- A.
5. המילה השכיחה ביותר, בת שתי אותיות, היא OF ואחריה TO ו- IN.
6. המילה השכיחה ביותר, בת שלוש אותיות, היא THE ואחריה AND.
7. המילה השכיחה ביותר, שיש בה ארבע אותיות, היא THAT (שימו לב, שהיא מתחילה ומסתיימת באותה אות).
8. אחרי האות Q תבוא תמיד U.
9. העיצור (consonant) השכיח ביותר אחרי תנועה (vowel), הוא N.
10. האותיות הכפולות על פי מידת שכיחותן, מימין לשמאל הן :
    LL, EE, SS, OO, TT, FF, RR, NN, PP, CC,.

כל התכונות שמנינו כאן לא משתנות בהצפנה מונו-אלפביתית, אלא רק מופיעות ב"תחפושת" של אות אחרת. בעלי ניסיון בפענוח יגלו בטקסט המוצפן רמזים מבטיחים. בניסיון לפצח צפנים, יש חשיבות לכל פרט שעשוי לשמש כרמז לפיצוח הצופן. אחדות מהאותיות במסר המוצפן, ניתנות לפענוח על סמך שכיחותן. אחרי קביעת השכיחות, מה שנותר לעשות, הוא להשוות את נתוני שכיחות האותיות בטקסט המוצפן לממצאים הסטטיסטיים של שפת המסר. זה כמובן לא מבטיח באופן מוחלט את נכונות הפענוח, שהרי עדיין מדובר בנתונים סטטיסטיים ולא בעובדות מוצקות.

חשוב לציין כי במקרים רבים המסרים המוצפנים הם קצרים מאד ואז אין כל אפשרות להסתמך על נתוני שכיחות הופעתה של אות זו או אחרת בטקסט.

בנספח ג' מופיעה היסטוגרמת שכיחויות של אותיות ה א"ב האנגלי שהתקבלה מקובץ שהכיל 114,485 תווים. ההיסטוגרמה נבנתה בעזרת תוכנה שנקראת CrypTool.exe. התוכנה מופצת חינם באינטרנט, ופותחה ע"י מספר מתמטיקאים עבור הבנק הגרמני, מתוך מטרה לעורר אמון בין לקוחות הבנק לגבי יחס רציני של הבנק לכל מה שנוגע להצפנה, וכך קדם הבנק את היקף העסקאות שנעשות דרך האינטרנט עם הבנק הגרמני.

5.2.2 מילות מתכונת

רמז נוסף וסיוע ניכר לפיצוח צפנים, בא מגילוי דפוסים מסוימים של מילים מיוחדות הנקראות מילות מתכונת. מילת מתכונת היא מילה, שבה לפחות אות אחת ,מופיעה יותר מפעם אחת. לעובדה זאת, חשיבות רבה במרוץ לפיצוח צפנים. למשל, נניח שאתם רואים במסר מוצפן את המילה XPP (מתכונת של שוויון שתי האותיות האחרונות). קרוב לודאי, שזו מילה שכיחה כמו ALL, SEE, או TOO, אם כי זו עשויה להיות גם מילה פחות שכיחה כמו: ODD, ADD, INN, EGG, ZOO ואחרות.

המילה המוצפנת XYZX (מתכונת של שוויון האות הראשונה והאחרונה במילה), סביר שתתפענח כ- THAT. מילה מוצפנת בת חמש אותיות, כמו BOCKC סביר להניח שתתפענח ל- THERE, או WHERE, או THESE. אבל היא עשויה לייצג גם מלים פחות שכיחות כמו NIECE, או ROSES, או NOSES ועוד. המתכונת ABCDB היא כנראה WHICH. ROMMRJ, היא מילת מתכונת עם שתי אותיות חוזרות: R ו- M. ההימור הטוב ביותר הוא LITTLE, אבל כמובן, שזה עדיין הימור בלבד.

כל המפצחים המיומנים של צפנים, יזהו במהירות מילות מתכונת כמו TOMORROW, PEOPLE, BANANA, BEGINNING, COMMITTEE ורבות אחרות. אם המסר המוצפן זו ציטטה, שצמוד לה שם המחבר, כי אז מפצח מיומן יזהה, על סמך החזרות של האות D, כי RBKJDRLDKMD הוא SHAKESPEARE ולא אחר.

אחד הכלים השימושיים ביותר, של כל מפצח צפנים חובב, זו טבלת שכיחות של מילות מתכונת. חשוב לארגן את הטבלה כך, שיהיה אפשר למצוא את המתכונת במהירות וגם את המלים שעשויות להתאים לה. הטכניקה לפענוח מסרים מוצפנים, כוללת ניסוח השערות ואחר כך בחירת ההשערה, שנראית המבטיחה ביותר לגבי מלים מסוימות. בשלב הבא מחליפים את האותיות המוצפנות באלה שפוצחו בעזרת ההשערה, בשאר המלים של המסר המוצפן. לאחר מכן בוחנים את התוצאות, האם הן מתקבלות על הדעת, או שההשערה הובילה לצירופי אותיות, שאינם מתקבלים על הדעת. אם אמנם התקבלו צירופי אותיות מתקבלים על הדעת, יש יסוד להניח שפיצוח הצופן עלה יפה. אולם אם התקבלו צירופי אותיות חסרי משמעות, זו הוכחה לכך, שההשערה שגויה וצריך לנסות השערה חדשה. בסעיף הבא ננסה את כוחנו בפענוח טקסט מוצפן.

5.3 דוגמא לפענוח מסר המוצפן בהצפנה מונו-אלפביתית

המסר המוצפן הבא הוא ציטטה מכתביו של סופר נודע:

ZU HO UD CUZ ZU HO ZSGZ AE ZSO JKOEZAUC

ננסה את כוחנו בפענוחה. אנו יודעים, כי הציטטה הוצפנה באלגוריתם של שחלוף, אך אין אנו יודעים מה היה מפתח ההצפנה ואין לנו זמן לבדוק מיליוני מיליונים של מפתחות. לכן נחפש דרך לעקוף את הקושי הזה. כיוון שהמסר המוצפן קצר מאוד, לא נוכל להסתמך על חקר שכיחותן של האותיות המופיעות בו, כמו שכבר הערנו בסעיף 5.2.1. לכן כדאי לחפש דרך אחרת. התחלה טובה, יכולה אולי להיות, ממילת המתכונת ZSGZ. כפי שראינו, סביר להניח שהיא מתפענחת כ- THAT, כיוון שזו מילה נפוצה. ננסה ונראה מה נקבל.

ZU HO UD CUZ ZU HO ZSGZ AE ZSO JKOEZAUC

שלבי הפתרון:

1. נבחן קודם כל את ההשערה ZSGZ=THAT נעשה זאת על ידי כך שנכתוב מעל כל Z במסר המוצפן, T, מעל כל S במסר המוצפן, נכתוב H, ומעל כל G נכתוב A. רשמנו זאת בטבלה:

T											**T**		**T**						**T**	**H**	**A**	**T**					**T**	**H**						**T**			
Z	U		H	O		U	D		C	U	Z		Z	U		H	O		Z	S	G	Z		A	E		Z	S	O		J	K	O	E	Z	A	U	C

2. השערה נוספת שנראית סבירה היא, ש- O מתפענחת כ- E. נוסיף זאת בטבלה: (להוסיף טבלה)
3. בינתיים עוד קשה לראות לאן זה מוביל, אבל כדאי להמשיך. על פי ההשערה הראשונה שלנו, המלה ZU, שהיא מילה בת שתי אותיות ומופיעה פעמיים בטקסט, מתחילה באות T, ננסה לבדוק השערה נוספת: ZU=TO. נבחן זאת על ידי כך שנרשום בטבלה, מעל לכל האותיות U בטקסט המוצפן, את האות O. נקבל:

T	**O**			**E**		**O**				**O**	**T**		**T**	**O**			**E**		**T**	**H**	**A**	**T**					**T**	**H**	**E**				**E**		**T**		**O**	
Z	U		H	O		U	D		C	U	Z		Z	U		H	O		Z	S	G	Z		A	E		Z	S	O		J	K	O	E	Z	A	U	C

4. נבחן השערה נוספת. המלה הרביעית היא בת 3 אותיות, ששתיים מהן אולי כבר פוענחו, על ידי ההשערות הקודמות. אלה האותיות OT. לגבי האות הראשונה שלה, קיימות אפשרויות רבות. נבחן אותן. האות הראשונה היא C, היא לא יכולה להתפענח כ- H, כיוון שכבר השתמשנו ב- H, כפענוח של S ומדובר בצופן מונו-אלפביתי. נשים לב שהאות C במסר המוצפן מופיעה גם בסיומת של המילה האחרונה, שם מופיעות לפי ההשערות הקודמות גם האותיות _T_O . אנו יודעים כי הסיומת TION היא סיומת שנפוצה במילים רבות. זה נותן יסוד להשערה, ש- C מתפענחת כ- N ו- A מתפענחת כ- I. מכאן נקבל שהמילה הרביעית במסר המוצפן- CUZ, מתפענחת למילה בת משמעות NOT. לכן גם ההשערה הזאת נראית מבטיחה. נוסיף זאת בטבלה:

T	**O**			**E**		**O**			**N**	**O**	**T**		**T**	**O**			**E**		**T**	**H**	**A**	**T**					**T**	**H**	**E**				**E**		**T**		**O**	**N**
Z	U		H	O		U	D		C	U	Z		Z	U		H	O		Z	S	G	Z		A	E		Z	S	O		J	K	O	E	Z	A	U	C

אם אמנם, C=N ו- A=I , על פי הנימוקים שהעלינו, כי אז נקבל:

T	**O**			**E**		**O**			**N**	**O**	**T**		**T**	**O**			**E**		**T**	**H**	**A**	**T**		**I**			**T**	**H**	**E**				**E**		**T**	**I**	**O**	**N**
Z	U		H	O		U	D		C	U	Z		Z	U		H	O		Z	S	G	Z		A	E		Z	S	O		J	K	O	E	Z	A	U	C

5. לאור ההצלחות שמסתמנות, נעלה השערה נוספת. במילה AE במסר המוצפן, נותר לפענח את האות E. המילה אינה יכולה להיות IT, כיוון שב- T כבר השתמשנו כפענוח של Z. המילה המוצפנת AE, נמצאת בין THAT ל-THE. אנו מחפשים מילה כזו, שתיצור צירוף בעל משמעות של שלוש המילים THE __ THAT. המילה IS עשויה להתאים. לכן השערתנו היא ש- E במסר המוצפן מתפענח ל- S.

T	**O**			**E**		**O**			**N**	**O**	**T**		**T**	**O**			**E**		**T**	**H**	**A**	**T**		**I**	**S**		**T**	**H**	**E**				**E**	**S**	**T**	**I**	**O**	**N**
Z	U		H	O		U	D		C	U	Z		Z	U		H	O		Z	S	G	Z		A	E		Z	S	O		J	K	O	E	Z	A	U	C

בשלב זה כבר אפשר להשלים את הפענוח:

TO BE OR NOT TO BE THAT IS THE QUESTION

הציטטה לקוחה מתוך "המלט", מחזהו המפורסם של ויליאם שייקספיר, המחזאי הבריטי הנודע.
אילו היינו מניחים, באחד השלבים, הנחה שונה מזו שהנחנו, לא היינו מגיעים לפענוח הטקסט המוצפן. היינו נותרים עם צירוף אותיות חסר משמעות והיינו נאלצים לחזור אחורנית ולנסות השערה חדשה, במקום זו שהכזיבה. וכך עד שהיינו מעלים השערות נכונות ומפענחים את מילותיו המעמיקות והיפות של שייקספיר.

שאלה מספר 40:

נתון מסר מוצפן – C, שהוצפן בהצפנת שחלוף מונואלפאביתית :

C R C N A O E B X C P D X A D Y A W O P C A D C V H M A

Q C N E K W O A N A Z Y A M W H C V C O E B X C P C V H M

A N U D X C P Q C N E K W

פענחו אותו וגלו את המסר המקורי P. לרשותכם מספר רמזים, המרוכזים בטבלה:

Cipher Text	Plain Text
A	A
N	N
DXAD	THAT
Q	G

6 הערת סיכום

פיצוח מסר מוצפן עשוי להיות שעשוע גדול. ככל שתרבו לעסוק בכך, תגדל מיומנות הפיצוח שלכם. הדרך הטובה לתרגל פיצוח מסרים מוצפנים היא לבקש ממישהו, שיצפין מסר כלשהו וייתן לכם להתמודד עם הפענוח. כותב המסר עשוי לחשוב, שמסר ארוך, יהיה יותר קשה לפענוח, מאשר מסר קצר, אבל כמובן, שזה לא תמיד נכון. לעיתים, דווקא ההפך הוא הנכון. מסר מוצפן בן מילה אחת, כגון COME, הוא בלתי ניתן לפיענוח. הוא עשוי להיות כל מילה בת 4 אותיות שונות!!!

מתמטיקאי אמריקני ומייסד הענף המתמטי "תורת התקשורת", ששמו Claude E. Shannon קבע, שאם המסר המוצפן מכיל 30 אותיות או יותר מזה, כמעט וודאי שהוא בעל פתרון יחיד. אבל אם הוא מכיל 20 אותיות או אף פחות מכך, כי אז אפשר, בדרך כלל, למצוא לו יותר משני פתרונות!!!

בהמשך חקירותיכם ובהמשך לניסיונות פענוח נוספים תגלו, כי כשאתם עובדים על מסר מוצפן ארוך ובוחנים רמזים רבים, שמאוששים זה את זה, מגיע בסוף הרגע המרגש, שבו אתם **בטוחים**, כי השערתכם נכונה וכעת זה רק עניין של זמן להשלמת הפתרון. במצב דומה נמצא גם המדען החוקר.

על כך בסעיף הבא.

7 המדען כמפצח צפנים

יש דמיון רב בין תהליך הפענוח ותחושת הסיפוק כשנמצא הפתרון הנכון, לבין עבודת המדען ושיטת המחקר המדעית. גם בעבודת המדען מגיע הרגע, שבו הוא חש כי יש בידיו מספיק ראיות, כדי לנסח (כהשערה) תיאוריה מדעית חדשה.

המתמטיקאי והפילוסוף הגרמני ווילהלם גוטפריד לייבניץ, שחי במאה ה- 17, אמר כבר אז, כי פענוח מסר מוצפן כמוהו כפתרון בעיה מדעית. אם, למשל, ידועות למדען שלוש עובדות, שלכאורה אינן קשורות זו לזו והוא מנסה לתת להן הסבר אחד (משותף), הוא עשוי, לחשוב על תריסר תיאוריות, שיכולות להתאים. ממש כמו שהמפענח עשוי לחשוב על תריסר פענוחים אפשריים למילה קצרה. אבל כשנתון מספר רב של תצפיות, שצריך להסבירן, זה דומה למצב בו נתון מסר מוצפן ארוך, שצריך לפענח אותו. לא קל לפתח תיאוריה, שתסביר מספר רב של עובדות, שקודם לכן נראו בלתי מוסברות ואולי אפילו מסתוריות וחסרות קשר. כשממציאים תיאוריה כלשהי והיא אמנם מסבירה את מאות העובדות, אפשר לומר שיש יסוד איתן להאמין בנכונותה, כשם שיש יסוד איתן לנכונותו של פתרון למסר מוצפן ארוך, ככל שמספר המלים המשמעותיות בפענוח גדל והולך.

ובכל זאת קיים הבדל בין השניים. תהליך הפענוח של צופן הוא סופי. הוא דורש, לכל היותר, את בדיקת כל המפתחות האפשריים. זה עלול להיות תהליך ארוך, אבל הוא סופי. לעומת זאת, תהליך המחקר המדעי וקביעת נכונותה של תיאוריה מדעית, הוא אינסופי. אין זה משנה כמה ניסויים כבר אוששו את נכונות התיאוריה, מספיק ניסוי אחד בלבד כדי להפריכה, ואף פעם אין בטחון מוחלט שניסוי כזה לא יתבצע אי פעם, תמיד קימת האפשרות שאירוע כזה עוד יקרה.

אפשר לומר כי חוקי המדע הם "מילות המתכונת" של היקום. "הספר הגדול של הטבע", כתב גלילאו גלילי, "כתוב בסמלים מתמטיים". המדענים הם מפצחי כתב החידה הענק ועוסקים בפענוח איטי, אך מתמיד של אינסוף סודותיו המוצפנים של הטבע.

גליליאו גלילי חי ופעל בסוף המאה ה- 16 ובראשית המאה ה- 17. הוא נחשב למייסד המדידה בניסויים פיזיקליים. הוא בצע ניסויים רבים למדידת מהירות הנפילה של גופים שונים, בקרבת כדור הארץ. ה"אגדה" מספרת כיצד הפיל עצמים שונים, ממרומי מגדל פיזה הנטוי. הוא היה מן הבודדים שהעז להצהיר (דבר שכל ילד בימינו יודע בביטחון), כי הארץ היא המקיפה את השמש, הצהרה שנחשבה בזמנו לכפירה נוראה בכתבי הקודש. על כך הושם במעצר, הובא למשפט ונדון למוות על המוקד. כל הלחצים האלה הביאו את גליליאו לחזור בו מהצהרתו על תנועת הארץ. אך ברגעיו האחרונים הצהיר את הצהרתו המפורסמת ביותר: "בכל זאת נוע תנוע".

7.1 הצופן הגנטי.

אחת התגליות המדעיות הגדולות ביותר במאה ה- 20, הייתה פענוח צופן שקיים בטבע, הצופן הגנטי. זהו הצופן הנמצא ב- DNA, שבגרעין התא החי ונושא את כל המידע לבניית היצורים החיים. לצופן הגנטי 4 אותיות בלבד, כל אחת מציינת חומר כימי שונה. ארבעת החומרים (הבסיסים החנקניים), מסודרים לאורכה של מולקולת ה- DNA בשלשות. השלשות הן ה"מילים" של הקוד הגנטי, הן בונות "משפטים" באורך שלא יאומן ובהם כל הוראות הפעולה לתא החי. כל שלשה של אותיות (בסיסים) מקודדת חומצה אמינית. החומצות האמיניות בונות את החלבונים, והחלבונים הם המשפטים בקוד הגנטי.

שאלה מספר 41:

א. *כמה חומצות אמיניות שונות ("מילים" בנות 3 אותיות בקוד הגנטי), ניתן לקודד מ- 4 האותיות של הצופן הגנטי?*

ב. *כמה "משפטים" בקוד הגנטי המורכבים מ- 5 חומצות אמיניות שונות, ניתן לייצר בתנאים הבאים:*

1. *ללא כל הגבלה.*
2. *כל חומצה אמינית מופיעה רק פעם אחת בחלבון.*
3. *כל המשפטים מורכבים מ- 5 חומצות אמיניות ויתכנו חזרות של אותה חומצה אמינית.*
4. *כמו ב- 3, אבל כל חומצה אמינית מופיעה רק פעם אחת בחלבון.*

זו הייתה סטייה קצרה מהצפנה ופענוח מסמכים כתובים, כדי להכיר כמה מן הפענוחים הגדולים של רזי הטבע. נחזור אל הצופנים – והפעם אל יותר מורכבים ומעניינים.

8 צפנים פולי-אלפביתיים

8.1 הקדמה

הכרנו את חולשתו הבסיסית של הצופן המונו-אלפביתי, זהו **צופן חד-חד-ערכי**. לכן אם מגלה המפצח כי במילה מסוימת, האות צ' מצפינה את האות א', אז על ידי כך הוא יכול לרשום בביטחון, א' במקום צ' בכל המילים של הטקסט המוצפן. כל הצפנים שראינו עד עתה היו כולם מונו-אלפביתיים. צפנים כאלה כפי שראיתם, אינם קשים לפיצוח, בעיקר אם המסר ארוך, או אם עומדים לרשות המפענח, מסרים רבים לפענוח. כיוון שהצבא והממשלה של כל אומה, ניצבים בפני הצורך לשגר מסרים ברמת סודיות גבוהה, הם מוכרחים להשתמש בצפנים, הרבה יותר קשים לפיצוח, מצפני השחלוף המונו-אלפביתיים. צפנים כאלה הם הצפנים הפולי-אלפבתיים. (פולי =הרבה). כלומר, צפנים כאלה שבהם לכל אורך הטקסט המוצפן, עשויים סמלים שונים להיות תולדת הצפנה של אותה אות בטקסט המקורי ואותו סמל בטקסט המוצפן, עשוי להיות תולדת הצפנה של אותיות שונות בטקסט המקורי. במילים אחרות אפשר לומר כי צפנים אלה אינם חד-חד-ערכיים. הצפנים הפולי-אלפביתיים עשויים להיות מסובכים מאוד ולכן קשים מאוד לפיצוח. אבל אסור שיהיו יותר מדי מסובכים, כיוון שאז גם ההצפנה וגם הפענוח שלהם ייקחו יותר מדי זמן. בפרק הבא נכיר דוגמאות של צפנים מקבוצה זו - צפנים פשוטים אך יעילים.

8.2 צופן פולי-אלפביתי לפי מילת מפתח

אחת השיטות להתגבר על מגבלות הצופן המונואלפאביתי היא על ידי שימוש במילת מפתח, כלומר מילה המשמשת כמפתח ההצפנה. כתוצאה מכך מקבלים צופן שאינו מונו-אלפביתיים. נדגים הצפנה באמצעות מילת מפתח. נצפין את המסר:

MEET YOU IN ORLANDO

נצפין אותו בהזזה על פי מילת המפתח HOME. כדי לבצע זאת ממספרים את האותיות לפי סדר הופעתן בא"ב. האות E מופיעה ראשונה, האות H שניה, M שלישית ו- O רביעית. ממספרים אותן בהתאם. מקבלים את המפתח המספרי 2431:

2	4	3	1
H	O	M	E

נכתוב את המפתח מעל מילות המסר, המיועד להצפנה, מספר פעמים כדרוש (כמו בשורה העליונה בטבלה). נצפין אותו על ידי הזזת כל אחת מאותיותיו, לפי המספר הרשום מעליה. כך מוחלפת כל אות במסר (שרשום בשורה האמצעית בטבלה), באות הנמצאת בא"ב, בהזזה של המספר שמעליה. בסופו של התהליך נקבל בשורה התחתונה של הטבלה את המסר המוצפן הבא:

2	4	3	1		2	4	3		1	2		4	3	1	2	4	3	1
M	E	E	T		Y	O	U		I	N		O	R	L	A	N	D	O
O	I	H	U		A	S	X		J	P		S	U	M	C	R	G	P

האם הצופן הזה הוא מונו-אלפביתי? נבדוק. האות E שבמסר, מוצפנת פעם כ- H ופעם כ- I. האות O מוצפנת פעמיים כ- S ופעם כ- P. האות U מצפינה גם את T וגם את R. האות P מצפינה גם את N וגם את O. אנו רואים שהצופן הזה אינו מונו-אלפביתי. זהו צופן פולי-אלפביתי. כלומר בצופן כזה אות אחת במסר המקורי, עשויה להיות מוצפנת לאותיות שונות במסר המוצפן ואותיות שונות במסר המקורי יכולות להיות מוצפנות לאותה אות במסר המוצפן. לפיכך קבלנו שיטת הצפנה שאינה חד-חד-ערכית, אינה מונו אלפאביתית. היא נקראת פולי-אלפאביתית רב-ערכית.

לשימוש במילות מפתח יש יתרונות ניכרים. את מלות המפתח קל מאוד לזכור ולכן אפשר לשנות את המפתח לעתים קרובות, אפילו כל שבוע, או כל יום. כל מה שצריך, זה להסכים עם הנמען על מילת מפתח חדשה. השימוש במלות מפתח או במשפטי מפתח, כדי להשיג צופן חד רב ערכי, זו טכניקה בעלת ערך רב וידועה עוד מימי קדם.

8.2.1 שאלות

שאלה מספר 42:

סב שלח לנכדו חידה: - מה זה אפור, בעל 4 רגליים, זנב ומזוודה?

הנכד שלח תשובה מוצפנת באנגלית, בהזזה, מילת המפתח היא: JANET .

התשובה המוצפנת: DNSW XHHS KSJP RCYU JT

מהי תשובתו של הנכד?

שאלה מספר 43:

מה אמר הצב לארנב, כאשר התחרו ביניהם בריצה?

קריאתו המוצפנת של הצב היא: יינע ודאג עזמי אנתק נלתר

רמז: ההצפנה היא בטבלה של 4 שורות ו- 5 עמודות. המסר המקורי נרשם בטבלה, במסלול ספירלי, נגד כיוון השעון החל מן המשבצת הימנית העליונה. מילת המפתח היא "מרדכי". היא נרשמה מעל לטבלה, כל אות מעל עמודה אחרת. האות מ' מעל לעמודה הימנית וכך הלאה. אחר כך שנו את הסדר של עמודות הטבלה וסדרו אותן לפי ערכן המספרי של אותיות מילת המפתח. כל עמודה נרשמה לפי הסדר וכך התקבל המסר המוצפן. לכם לא נותר אלא לפענח אותו.

8.3 צופן פולי-אלפביתי לפי תאריך

דוגמא נוספת לצופן פולי-אלפביתי, הוא צופן הזזה לפי תאריך. השימוש בו מאפשר לשנות את מידת ההזזה של כל אות מאותיות המסר המקורי. אפשר להשתמש בתאריך בו נשלח המסר כמפתח ההצפנה. למשל, נניח שאתם שולחים מסר ב- 21.2.03 וללא הנקודות, 21203 מפתח ההצפנה הוא, כל אות במסר תוזז, בהתאם לספרת התאריך שמעליה.

דוגמא:

2140 32 1 40 3 21 403

המסר המקורי: THIS IS A SUNNY DAY

רושמים את המפתח מעל למסר המקורי ומזיזים בהתאם, כל אחת מאותיותיו.

המסר המוצפן הוא: VIMS LUBW URQZ HAB

כדי לפענח רושמים את ספרות המפתח מעל אותיות המסר המוצפן ומזיזים כל אות לאחור. אם מגיעים ל- Z, תוך כדי ההזזה, חוזרים ומתחילים מ- A (כדי להקל על ארגון הנתונים רשמו אותם בטבלה).

שימו לב שהצופן האחרון שהכרנו אינו מונו-אלפביתי. למשל האות I במסר המקורי מוצפנת פעם כ- M ופעם כ- L. האות S מוצפנת פעם כ- S, פעם כ- U ופעם כ- W. האות B במסר המוצפן מייצגת פעם A ופעם Y. כל זה מקשה מאוד על פענוח המסר. כמובן שאין צורך להשתמש דווקא בתאריך כמפתח. כל צירוף מספרים יתאים לכך ובלבד שהשולח והנמען יודעים אותו ואף אחד חוץ מהם אינו יכול להשיגו. אנו משתמשים **במילת** מפתח, רק כדי להקל על זכירת מספר המפתח.

שאלה מספר 44:

השתמשו בתאריך הלידה שלכם כמפתח כדי להצפין את המסר:

YOU MUST COME NO LATER THAN TOMORROW MORNING

כאמור, את מילת המפתח אפשר ורצוי לשנות לעתים קרובות. אבל בדרך כלל לא קל להפגיש את המצפין עם הנמען לעתים תכופות, זה עלול לעורר בעיות. הצורך בשליחת מסרים מוצפנים עולה **כיוון שאין אפשרות להיפגש פנים אל פנים,** ולהעביר בדרך זו את המידע הסודי.

אחת הדרכים להימנע מפגישה היא, להשתמש בספר או בכתב עת, שמספקים את מלות המפתח. ברור שיש לבחור ספר שלשני הצדדים יש גישה לאותה מהדורה שלו, להסכים על ההליך לבחירת מילת מפתח ראשונה, לציין את מספר העמוד בו היא מופיעה, מספר השורה מראש העמוד ומספר המילה בשורה, ולהסכים על ההליך להחלפתה בפרקי זמן קצובים.

8.4 צפנים פולי-אלפבתים קשים לפיצוח

8.4.1 הצופן של PORTA

בצופן זה אנו מצפינים זוגות של אותיות מן הטקסט המקורי על ידי סמל יחיד בטקסט המוצפן. השיטה הומצאה על ידי האיטלקי Porta, מאנשי האשכולות של תקופת הרנסנס, סופר, מדען וגם קוסם. בהיותו בן 28, בשנת 1563, הוציא פורטה לאור, ספר על מבנה צפנים שונים, שכלל גם צופן מסוג זה. ככל הידוע, היה הוא הראשון בסוגו, שפורסם. כדי להשתמש בצופן של פורטה, נזדקק לטבלה של 26 שורות ו- 26 עמודות ובסה"כ 676 משבצות. היא מגדירה את מפתח ההצפנה (התבוננו בדוגמת הטבלה שבעמוד הבא). אותיות הא"ב הלטיני כתובות בשוליים של הטבלה. פעם מעל לשורה הראשונה ופעם משמאל לעמודה השמאלית. את 676 תאי הטבלה תוכלו למלא בסמלים, בכל דרך שתבחרו: אותיות, מספרים, או סמלים אחרים. התנאי היחיד הוא, אסור שיהיו בטבלה שתי משבצות זהות זו לזו. בדוגמא שלנו השתמשנו במספרים מ-1 עד 676 (הערה: להצפנה בעברית, בשיטת פורטה דרושה טבלה של 22x22 משבצות והא"ב ייכתב בשוליים העליונים והימניים).

נעבור עכשיו לתהליך ההצפנה. נניח שאנו רוצים להצפין את המילה THEY. ראשית מחלקים אותה לזוגות של אותיות: TH - EY. להצפנת TH מחפשים את התא שנמצא בנקודת החיתוך של השורה T והעמודה H, מוצאים שרשום בו: 502. באופן דומה בצומת של השורה E ושל העמודה Y, נמצא המספר 129. חשוב לזכור: האות הראשונה של הזוג מסמלת תמיד את השורה והאות השניה את העמודה. המילה THEY תוצפן אפוא כ-502,129. כדי לפענח מחליפים כל מספר בזוג האותיות של השורה והעמודה, המתאימות למשבצת שבה מופיע המספר. האות הראשונה מסמנת את השורה והשניה את העמודה. אם מספר האותיות במסר אי זוגי, מוסיפים בסופו אות דמה אחת.

	A	B	C	D	E	F	J	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	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	26
B	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52
C	53	54	55	56	57	58	59	60	61	62	63	64	65	66	67	68	69	70	71	72	73	74	75	76	77	78
D	79	80	81	82	83	84	85	86	87	88	89	90	91	92	93	94	95	96	97	98	99	100	101	102	103	104
E	105	106	107	108	109	110	111	112	113	114	115	116	117	118	119	120	121	122	123	124	125	126	127	128	129	130
F	131	132	133	134	135	136	137	138	139	140	141	142	143	144	145	146	147	148	149	150	151	152	153	154	155	156
G	157	158	159	160	161	162	163	164	165	166	167	168	169	170	171	172	173	174	175	176	177	178	179	180	181	182
H	183	184	185	186	187	188	189	190	191	192	193	194	195	196	197	198	199	200	201	202	203	204	205	206	207	208
I	209	210	211	212	213	214	215	216	217	218	219	220	221	222	223	224	225	226	227	228	229	230	231	232	233	234
J	235	236	237	238	239	240	241	242	243	244	245	246	247	248	249	250	251	252	253	254	255	256	257	258	259	260
K	261	262	263	264	265	266	267	268	269	270	271	272	273	274	275	276	277	278	279	280	281	282	283	284	285	286
L	287	288	289	290	291	292	293	294	295	296	297	298	299	300	301	302	303	304	305	306	307	308	309	310	311	312
M	313	314	315	316	317	318	319	320	321	322	323	324	325	326	327	328	329	330	331	332	333	334	335	336	337	338
N	339	340	341	342	343	344	345	346	347	348	349	350	351	352	353	354	355	356	357	358	359	360	361	362	363	364
O	365	366	367	368	369	370	371	372	373	374	375	376	377	378	379	380	381	382	383	384	385	386	387	388	389	390
P	391	392	393	394	395	396	397	398	399	400	401	402	403	404	405	406	407	408	409	410	411	412	413	414	415	416
Q	417	418	419	420	421	422	423	424	425	426	427	428	429	430	431	432	433	434	435	436	437	438	439	440	441	442
R	443	444	445	446	447	448	449	450	451	452	453	454	455	456	457	458	459	460	461	462	463	464	465	466	467	468
S	469	470	471	472	473	474	475	476	477	478	479	480	481	482	483	484	485	486	487	488	489	490	491	492	493	494
T	495	496	497	498	499	500	501	502	503	504	505	506	507	508	509	510	511	512	513	514	515	516	517	518	519	520
U	521	522	523	524	525	526	527	528	529	530	531	532	533	534	535	536	537	538	539	540	541	542	543	544	545	546
V	547	548	549	550	551	552	553	554	555	556	557	558	559	560	561	562	563	564	565	566	567	568	569	570	571	572
W	573	574	575	576	577	578	579	580	581	582	583	584	585	586	587	588	589	590	591	592	593	594	595	596	597	598
X	599	600	601	602	603	604	605	606	607	608	609	610	611	612	613	614	615	616	617	618	619	620	621	622	623	624
Y	625	626	627	628	629	630	631	632	633	634	635	636	637	638	639	640	641	642	643	644	645	646	647	648	649	650
Z	651	652	653	654	655	656	657	658	659	660	661	662	663	664	665	666	667	668	669	670	671	672	673	674	675	676

שאלה מספר 45:

איזו מילה מוצפנת על ידי השלשות: 313,363

שאלה מספר 46:

בטבלה הבאה, בנו מפתח לצופן Porta להצפנה בעברית. הצפינו את המסר "אין ברירה".

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

כדי להקשות את הפענוח על ידי היריב כדאי לרשום את המספרים בטבלה לא לפי סדרם הטבעי, או להשתמש בסמלים אחרים. דרך אחרת היא להשאיר את סדר המספרים ללא שינוי, אבל לערבל את האותיות בשוליים. כשמערבלים את המספרים קשה יותר לפענח, כשמערבלים את האותיות יותר קשה להצפין ולכן זה לא משיג את מטרת ההצפנה. אם מערבלים גם את האותיות וגם את המספרים, אז גם ההצפנה וגם והפענוח יהיו מסובכים ופחות יעילים.

8.4.2 הצופן של Playfair

הצופן של Playfair דורש יותר עבודה מזה של Porta, גם בהצפנה וגם בפיענוח, אבל הוא נשען על שימוש בטבלה הרבה יותר פשוטה. הצופן נקרא על שם הברון Lyon Playfair, אנגלי בן המאה ה- 19. למעשה הומצא הצופן על ידי חברו של הברון Charles Wheatstone. וויטסטון היה מדען בריטי, שהתפרסם כבונה של כלי נגינה וכממציאה של עוד שיטת קידוד שיטה טלגרפית, שהומצאה יותר מאוחר, באופן בלתי תלוי על ידי האמריקני סמואל מורס. את הקוד הטלגרפי, כמו זה של מורס, אפשר לראות כצפן לא סודי, בו מוחלפות האותיות על ידי סמלים במתכונת של קווים ונקודות. טבלת ההתאמה ("ההצפנה") גלויה ומפורסמת לציבור. הסיפור הקצר מצביע על חוסר מזלו של וויטסטון. למרבית הצער שתי ההצפנות שהמציא אינן נקראות על שמו ואחרים זכו בתהילה, שהגיעה לו.

בכל אופן, צופן Playfair היה בשימוש בצבא הבריטי שנים רבות, בעיקר במלחמת הבורים, שהתחוללה בדרום אפריקה בשנים 1899-1902 בין הבריטים לבין המתיישבים ההולנדים ,שנקראו בורים. יותר מאוחר, במלחמת העולם השניה, גם האוסטרלים השתמשו בו.

טבלת Playfair עשויה להיות ריבועית או מלבנית. אנו נשתמש בטבלה של 4 על 8. ב-32 התאים שלה, נרשום את אותיות הא"ב וספרות מ- 2 עד 7 (1 מושמט כיוון שהוא דומה יותר מדי ל- l). פיזור האותיות והספרות בתאי הטבלה נעשה באופן אקראי וללא חזרות. למשל:

4	H	M	V	L	3	Y	D
X	K	B	5	P	Z	E	O
N	7	W	U	F	T	6	J
G	R	2	Q	C	A	I	S

צופן Playfair פועל גם הוא, כמו צופן Porta, על זוגות של אותיות. המסר בצופן Playfair מוצפן על ידי כך שלוקחים בכל פעם, זוג של אותיות ומצפינים אותו לפי שלושה חוקים בסיסיים:

1. אם שתי האותיות, של המסר המקורי, נמצאות באותה השורה, כל אחת מהן מוצפנת לזו שמימינה. את השורה יש לראות כטבעת. כלומר, האות שבקצה הימני של השורה, תוצפן לאות הראשונה משמאל באותה שורה. דוגמא: P, O, שבשורה השניה, יוצפנו Z, X.
2. אם שתי האותיות נמצאות באותה העמודה, כל אחת מהן מוצפנת לזו שמתחת לה. גם את העמודה רואים כטבעת. כלומר, האות שבתחתית העמודה, תוצפן לאות שבראש העמודה,
   דוגמא: האותיות K, R שבעמודה השניה, יוצפנו H, 7.
3. אם שתי האותיות של המסר המקורי נמצאות בעמודות שונות ובשורות שונות, אז כל אות תוחלף על ידי אות שנמצאת באותה שורה, בעמודה של האות השניה.

נבהיר בדוגמא: נניח שבמסר המקורי מופיע זוג האותיות H, T, המופיעות בשורות שונות ובעמודות שונות. T נמצאת בשורה השלישית בטבלה.כדי להצפין אותה נלך בשורה של T שמאלה עד לעמודה של H. H נמצאת בעמודה השניה, בשורה השלישית בעמודה זו נמצא 7 לכן 7 יצפין את T. כעת נצפין את H: H נמצאת בשורה הראשונה ו- T בת זוגה נמצאת בעמודה השישית. במשבצת המפגש של השורה הראשונה והעמודה השישית, נמצאת הספרה 3, היא המצפינה את H.

4. אם באותו זוג נמצאות שתי אותיות זהות, מפרידים ביניהן על ידי האות X.
5. אם בסוף החלוקה של המסר המקורי לזוגות נותרת אות בודדת, מצמידים גם אליה X.

לדוגמא נצפין: I WILL ARRIVE AT FOUR P.M.

נחלק את אותיות המסר לזוגות.

IW IL LA RX RI VE AT FO UR PM

שימו לב שהיה צורך להוסיף X בין RR, שנפלו באותו זוג, אבל לא בין LL, שנפלו בזוגות שונים. (בדוגמא שלנו לא נזקקנו לכך). נצפין את המסר המקורי לפי חוקי ההצפנה שהכרנו לעייל ונארגן את אותיות המסר המוצפן ברביעיות. המסר המוצפן יראה כך: (בדקו).

26CY 3CGK 2SY5 3AJP 7QBL

הפענוח יבוצע בהתאם לאופן הכתיבה של הטקסט, מלבד שינוי קטן, במקרה שזוג האותיות, במסר המוצפן, נמצאות באותה השורה או באותה העמודה בטבלה. במקרה כזה, אם האותיות נמצאות באותה שורה, צריך לקחת במקומן את האותיות,שנמצאות משמאלן בטבלה. אם האותיות נמצאות באותה עמודה, צריך לקחת במקומן את האותיות שנמצאות מעליהן.

זה צופן מופלא, קל לשימוש וקשה לפיענוח. David Kahn בספרו "מפצחי הצופן", מספר על צופן זה סיפור משעשע. כש- Playfair וויטסטון ניסו לעניין את משרד החוץ הבריטי בצופן, נאמר להם שהצופן קשה ללימוד. וויטסטון הציע שיוכיח כי הדבר אינו נכון על ידי כך, שילמד את הצופן תוך רבע שעה לתלמיד בי"ס יסודי, בעל אינטליגנציה ממוצעת. "זה אפשרי" נאמר לו בחיוך, "אבל אנחנו מדברים על הסגל הדיפלומטי".

8.4.3 צופן Vigenere של Lewis Carroll

הצופן הגאוני הזה, נקרא על שמו של Blaise de Vigenere, צרפתי בן המאה ה- 16, שהמציא צפנים רבים וגם כתב על כך. וואריאציות שונות על הרעיונות הבסיסיים שלו, נתגלו מאוחר יותר, באופן בלתי תלוי, על ידי אחרים. הגרסה שמובאת כאן הומצאה על ידי לואיס קרול, המתמטיקאי מאוניברסיטת אוקספורד, שמוכר יותר כסופר שכתב את הספרים "עליסה בארץ הפלאות" ו"עליסה בארץ המראות". לואיס קרול פרסם את הצופן שלו בעילום שם בשנת 1868.

הצופן של קרול, נשען על טבלה של 26 על 26 משבצות, המובאת להלן בעמוד הבא. היא שווה בגדלה לטבלה של Porta, אבל יותר קל למלא אותה, כיוון שהאותיות נכתבות לפי הסדר שלהן בא"ב, במתכונת שקל לזכור אותה, בכל המשבצות בטבלה. בשורה הראשונה הסדר המקובל A עד Z. בכל שורה אחר כך מוזז הא"ב שמאלה. בכל שורה באות אחת שמאלה, יחסית לשורה שמעליה.

הצופן דורש מילת מפתח. בהוראות הקצרות של קרול, הוא השתמש במילה VIGILANCE, כשהדגים את השיטה באמצעות המסר: MEET ME ON TUESDAY EVENING AT SEVEN

מילת המפתח נכתבת מעל למסר במספר החזרות הדרוש.

V	I	G	I		L	A		N	C		E	V	I	G	I	L	A		N	C	E	V	I	G	I		L	A		N	C	E	V	I
M	E	E	T		M	E		O	N		T	U	E	S	D	A	Y		E	V	E	N	I	N	G		A	T		S	E	V	E	N

האות שמעל M, שהיא האות הראשונה במסר המקורי, היא V. מוצאים את העמודה, שבראשה V, יורדים בעמודה זו, עד שמוצאים את השורה M. בנקודת המפגש של השורה והעמודה נמצאת האות H. זוהי האות הראשונה בטקסט המוצפן. האות הבאה במסר היא E ומעליה אות המפתח I. במפגש של השורה E והעמודה I נמצאת האות M. לכן זו האות השניה במסר המוצפן. חוזרים באופן דומה, על התהליך לגבי כל אות במסר המקורי והאות המתאימה של מילת המפתח שמעליה. בסופו של תהליך ההצפנה נקבל את המסר המוצפן:

HMKB XEBP XPMY LLYR XIIQ TOLT FGZZ Y

כמובן שאפשר להוסיף שלוש אותיות דמה להשלמת הרביעייה האחרונה.

תהליך הפענוח הוא כזה: ראשית כותבים את מילת המפתח מעל הטקסט המוצפן, מספר פעמים כדרוש. האות שמעל H היא V. מוצאים את העמודה V, יורדים בה עד למשבצת H מתקדמים, שמאלה עד קצה השורה ומגיעים ל- M. היא האות הראשונה בשורה וגם האות המסמנת את השורה. M היא האות הראשונה במסר המפוענח, המסר המקורי. חוזרים על התהליך עד לפענוח המלא של המסר המוצפן

לואיס קרול כתב: "אין כל אפשרות לפענח את המסר ללא מילת המפתח, גם אם יודעים את הטבלה."

אף כי דבריו של קרול מוגזמים מעט והצופן הזה ניתן לפיצוח על ידי מומחים, המלאכה אינה קלה כלל ועיקר. משום כך, בגרסות שונות שלו הוא ממשיך להיות אחד הצפנים הפופולריים ביותר, שהומצאו אי פעם.

בעמוד הבא תמצאו את טבלת ההצפנה של לואיס קרול.

	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	
A	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	**A**
B	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	a	**B**
C	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	**C**
D	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	**D**
E	e	f	g	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	f	g	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	g	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**
H	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	**H**
I	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	h	**I**
J	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	**J**
K	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	**K**
L	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	**L**
M	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	**M**
N	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	**N**
O	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	**O**
P	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	**P**
Q	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	**Q**
R	r	s	t	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	s	t	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	t	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**
U	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	**U**
V	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	u	u	**V**
W	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	t	v	**W**
X	x	y	z	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	y	z	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	z	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**
	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**	

יש דרך נוספת להשתמש בטבלה ובמילת המפתח. אולי תעדיפו אותה על זו של קרול, כיוון שבה תהליך הפענוח זהה לתהליך ההצפנה. שיטה זו נקראת שיטת Beaufort, על שם ממציאה, אדמירל בצי הבריטי בשנת 1857 מכר את שיטתו לבריטניה, כשיטה למשלוח מסרים סודיים על ידי הטלגרף או על ידי גלויות דואר. הוא מכר את שיטתו במחיר סמלי של 6 פני.

נדגים כיצד פועלת השיטה על ידי בחינת ההצפנה של M (האות הראשונה במסר) ו- V (האות הראשונה במילת המפתח). מוצאים את M בעמודה שמחוץ לטבלה ומתקדמים ימינה בשורה עד שמגיעים ל- V. עולים עד שמגיעים ל- J בראש העמודה. J תהיה האות הראשונה בטקסט המוצפן. בפיענוח מוצאים את J בעמודה השמאלית, מתקדמים ימינה עד ל- V ועולים עד M בראש העמודה.

8.4.4 מכונת האניגמה

מכונת האניגמה היא מכונת הצפנה פוליאלפבתית שפתחו הגרמנים בימי מלחמת העולם השניה. האניגמה הצפינה על ידי שחלופים וערבולים חוזרים. היא נתנה בידי הגרמנים יתרון גדול, שסיכן את הצי הבריטי זמן רב. הבריטים, האמריקאים ואחרים השקיעו מאמצים עצומים בפענוחה. סיפור חילוצה של מכונת האניגמה מצוללות גרמנית טבועות ופענוח הצופן של האניגמה, הם מן הפרשיות החשובות והמרתקות,שסייעו להכרעת המערכה באירופה במלחמת העולם השניה.

מכונת האניגמה הייתה מורכבת משלושה רוטורים שהסתובבו במהירות קבועה יחסית האחד לשני. כל רוטור ביצע שחלוף של אותיות הא"ב הלועזי. מפני שכל אחד מהם גם הסתובב, השחלוף והסבוב ביחד יצרו הצפנה פולי-אלפבתית, כמו השמוש במילת מפתח יחד עם הצפנת הזזה שיוצרים ביחד הצפנה פולי-אלפבתית.

ברשת האינטרנט תוכלו למצוא מידע רב על האניגמה, כמו למשל סימולציה של מכונת האניגמה בכתובת: http://homepages.tesco.net/~andycarlson/enigma/enigma_j.html.

כדאי לקרוא ולהרחיב את הידיעה על מכונת הצפנה זו לפי רשימת הקישורים שבנספח ו'.

בעברית יצא לאור, בהוצאת "יבנה" הספר "אניגמה – סיפור הקרב על הצופן". הספר מרתק, כדאי מאוד לקרוא אותו. כתב אותו יו – סיבאג מונטיפיורי, יהודי בריטי ממשפחת מונטיפיורי הידועה. מעניין לדעת, שפרוייקט פיצוח האניגמה בבריטניה התרחש באחוזת המשפחה בפארק בלייצ'לי.

9 הצופן שאינו ניתן לפיצוח- One Time Pad

החולשה הבסיסית של צופן הזזה עם מילות מפתח (גם כאלה הלקוחות מספר) היא, שבדרך כלל המסר והמפתח הם באותה שפה. זה "גורר העתקות" של תבניות לשון בסיסיות, שנמצאות בטקסט המקורי אל הטקסט המוצפן ומספק רמזים למפענח. אפילו אם שפת המפתח שונה משפת המסר, משימת הפענוח אפשרית, אם כי קשה. בסופו של דבר המפענח מנחש את שפת המפתח ומפענח את המסר, כיוון שיש דמיון רב בתבניות לשון ותכונות לשוניות אחרות גם בין השפות ולא רק בתוך השפה. כיצד אפשר להתגבר על שרידותן העקשנית של התכונות הלשוניות? אפשר להתגבר על כך, אם המפתח לא מבוסס על שום שפה טבעית. המפתח יכול להיות צרוף אקראי של אותיות כך שמספר האותיות במפתח, שווה למספר אותיות הטקסט ועושים בהן (באותיות המפתח) שימוש חד פעמי. במקרה כזה השגנו "הצפנה מנצחת" - בנינו מפתח חד פעמי, שאינו ניתן לפיצוח. במילים אחרות, כדי להגיע למערכת חסינת פיצוח, צריך לבחור צופן הזזה, שהמפתח שלו מורכב ממספרים (אותיות), שנבחרו אקראית. **אורך המפתח צריך להיות כאורך הטקסט המקורי.**

הצופן הזה נקרא One Time Pad, או צופן Vernian. הוא הומצא על ידי איש צבא אמריקאי בשנת 1917. הרוסים השתמשו בצופן זה לתקשורת הרדיו הסודית שלהם. כמו כן השתמשו בה בתקופת המלחמה הקרה, בשנות ה- 50 וה- 60 של המאה ה- 20. בקו (הטלפון) החם בין הבית הלבן בוושינגטון לקרמלין במוסקבה. הצופן הזה הוא בלתי מנוצח, כיוון שההסתברות להצגתה של אות מסוימת בטקסט המקורי על ידי אות אחרת בטקסט המוצפן אינה קבועה, היא משתנה כל הזמן. בשיטת הצפנה זו גם אי אפשר לגלות תבניות לשוניות, כיוון שכל בחירה של מפתח היא אקראית.

כמה מפתחות אקראיים, שונים זה מזה, אפשר ליצור מ- 26 האותיות של השפה האנגלית? נפתור את השאלה במספר שלבים. בשלב הראשון נשנה אותה מעט, במקום לדון באותיות ומפתחות, נתייחס לספרות ולמספרים. אנחנו יכולים לשאול למשל, כמה מספרים **בני שתי ספרות** אפשר ליצור על ידי שימוש בכל 10 הספרות (עם מספר חזרות בלתי מוגבל של כל ספרה)? התשובה כמעט מיידית, אלה כל המספרים בין אפס ל- 99.

נרשום אותם: 00, 01, 02, 03, 04.....,99

כמה מספרים כאלה יש? 100 כמובן.

ואפשר כמובן לרשום זאת: $100=\mathbf{10}^{2}$

כמה מספרים **בני 3 ספרות** אפשר ליצור מעשר הספרות? התשובה היא: $\mathbf{10}^{3}$, כל המספרים בין 000 ל- 999.כמה מספרים **בני 12 ספרות** אפשר ליצור? - כל המספרים בין אפס ל- 999,999,999,999 בסך הכל $\mathbf{10}^{12}$.

זהו מספר בן 12 ספרות, מיליון מיליונים, שנקרא טריליון.

נכליל את ממצאינו מן השלב הראשון: אפשר לומר שאם *n* מציין את מספר הספרות במספר, אז מספר המספרים השונים, בני *n* ספרות, שאפשר ליצור הוא: 10^n.

כעת נעבור לשלב השני. נשאל את אותה השאלה, אבל נחליף את הספרות בסמלים אחרים, באותיות למשל. נשאל כמה "מילים" שונות זו מזו, שאורך כל אחת מהן *n* אותיות, אפשר ליצור, בשפה האנגלית? במקום "מילים" אפשר גם לומר מפתחות הצפנה. בכך חזרנו לשאלת המוצא: כמה מפתחות שונים זה מזה, שאורכם *n* אותיות אפשר ליצור, בשפה האנגלית? כיוון שמספר האותיות בשפה האנגלית הוא 26, מספר המפתחות האפשריים שאורכם *n*, הוא 26^n. כך, שעבור *n* גדול, הפיצוח של ההצפנה אינו ישים. למשל אם הטקסט בן 56 אותיות, כי אז מספר המפתחות האפשריים הוא 26^{56}, שזה בערך 10^{79}, כלומר מספר בעל 80 ספרות.

כפי שאתם רואים מקבלים שמספר המפתחות האפשריים הוא בן 80 ספרות בקירוב. אחד מהם אנחנו מחפשים, אבל הסיכוי למצוא אותו אפסי. כיוון שב- One Time Pad הופעתן של כל האותיות היא אקראית, אזי אין זה חשוב כמה אותיות של המפתח כבר ראינו, אין שום דרך לנבא מה תהיה האות הבאה, היא יכולה להיות כל אחת מהן. במילים אחרות, כל המפתחות אפשריים באותה מידה. המשמעות של עובדה זו היא, שלבעיית הפענוח אין פתרון יחיד אלא פתרונות רבים.

פירושו של הדבר הוא, שמסר שהוצפן על ידי One Time Pad, עשוי להתפענח **למסרים שונים** (על ידי שימוש במפתחות שונים), **כולם מסרים בעלי אותו מספר אותיות,** אבל כיוון שלמפתח ההצפנה של המסר אין שום תכונה המבדילה אותו ממפתחות אחרים, **אין כל אפשרות להחליט איזה נוסח מנוסחי הפענוח הוא המסר המקורי**. אין כל אפשרות לזהות אותו. אלא אם כן, באורח מאוד יוצא דופן, רק אחד מכל אלה הוא בעל משמעות וכל מיליוני האחרים הם חסרי משמעות.

עובדה זו מודגמת בטבלה. שימו לב לפרטיה:

בשורה הראשונה מופיע מסר מוצפן C ובשורה השניה ייצוגו המספרי. בשורה השלישית מפתח הצפנה אפשרי K_1, שאולי באמצעותו הוצפן המסר. בשורה הרביעית מופיע ייצוגו המספרי של המפתח K_1. בשורה החמישית רשום הייצוג המספרי של הפענוח בהתאם לנוסחה:

$$P_1 = C\text{-}K_1$$

בשורה השישית רשום הפענוח הסופי (באותיות).

שימו לב כי החישוב של הפענוח לפי הנוסחה עשוי לתת תוצאת ביניים שלילית. למשל בטור השמאלי:

$$C = Q = 16, \quad K_1 = Y = 24$$

$$P_1 = Q - Y = 16 - 24 = -8 = 26\text{-}8 = 18 = S$$

(הערה – קל להבין את הביטוי הזה אם זוכרים כי אפשר לראות בחשבון המודולרי חשבון מעגלי)

(1)	C אותיות	Q	Q	N	A	F	C	U	M	E	Y	B	E	X	L	Q
(2)	Cמספרי	16	16	13	0	5	2	20	12	4	24	1	4	23	11	16
(3)	K_1 אותיות	Y	Q	B	M	I	U	D	F	C	B	D	P	I	L	J
(4)	K_1 מספרי	24	16	1	12	8	20	3	5	2	1	3	15	8	11	9
(5)	P_1אותיות	S	A	M	T	S	I	R	H	C	X	Y	P	P	A	H
(6)	P_1 מספרי	18	0	12	19	18	8	17	7	2	23	24	15	15	0	7
(7)	K_2 אותיות	M	F	F	N	Y	U	I	P	N	Y	X	T	V	R	D
(8)	K_2 מספרי	12	5	5	13	24	20	8	15	13	24	23	19	21	17	3
(9)	P_2 מספרי	4	11	8	18	18	8	12	23	17	0	4	11	2	20	13
(10)	P_2 אותיות	E	L	I	S	S	M	X	R	A	E	L	C	U	N	

(1) למשל, המסר המוצפן - C:

Q	L	X	E	B	Y	E	M	U	C	F	A	N	Q	Q

(3) הוצפן ב-One Time Pad. אם המפתח הוא K_1:

J	L	I	P	D	B	C	F	D	U	I	M	B	Q	Y

(6) המסר המקורי הוא P_1:

H	A	P	P	Y	X	C	H	R	I	S	T	M	A	S

(7) אבל אם המפתח הוא K_2:

D	R	V	T	X	Y	N	P	I	U	I	N	F	F	M

(10) אז המסר המקורי הוא P_2:

N	U	C	L	E	A	R	X	M	I	S	S	I	L	E

אז מהו המסר המקורי? **אי אפשר לדעת !**. כל המפתחות שאורכם 15 אותיות באים בחשבון, כולם סבירים באותה מידה ומספרם יותר מ- 10^{21} (26^{15}). יש לשער כי רובם יתנו מסרים חסרי משמעות, אבל עדיין יהיו רבים בעלי משמעות ולא נוכל לדעת מהו המסר המקורי. לכן אפשר לטעון את הטענה הגורפת שצופן ה- One Time Pad הוא חסין פיצוח לחלוטין.

9.1 שאלות

שאלה מספר 47:

נתון הטקסט המוצפן:

H	M	P	Z	X	S	M	D	J	K	O	E	B
9	8	2	11	11	14	21	15	23	7	1	26	19

א. מהו הטקסט המקורי אם שיטת ההצפנה הייתה One time Pad ומפתח ההצפנה K_1 היה:

3	20	7	23	6	16	15	25	21	17	1	10	10

ב. מהו הטקסט המקורי אם מפתח ההצפנה K_2 היה:

הערה: בטקסט המוצפן רשומות המילים ללא רווחים. בשני המקרים הטקסט המקורי הוא בן 3 מילים והוא הוצפן בשיטת הזזה עם One time pad.

שאלה מספר 48:

נתון הטקסט המוצפן "גלזוז משלחנ", מהו הטקסט המקורי?

פענחו אותו בעזרת שני המפתחות:

א. מפתח א': (6, 2, 14, 7, 0, 7, 0, 1, 6, 11).

ב. מפתח ב': (8, 10, 4, 15, 0, 19, 14, 20, 11, 19)

אם אמנם, הצופן של ה- One Time Pad הוא כל כך מאובטח, מדוע אין משתמשים בו לכל ההצפנות? הסיבה היא שהצופן הזה עשוי להתאים רק למערכות תקשורת המשרתות מספר קטן של משתמשים, שנזקקים רק למעט התקשרויות ביניהם. אבל היישום של שיטה זו במערכות תקשורת מודרניות, שהן עתירות משתמשים והתקשרויות הוא איטי ומסורבל מאוד. כיון שהמפתח מיועד לשימוש חד-פעמי בלבד, אז במהלך הקשר (session) המוצפן, צריך לייצר לכל תנועה של מידע מהמקור ליעד ומן היעד למקור, מפתח חדש. למשל, במערכת סחר אלקטרוני, הקשר (session) בין הלקוח לסוחר, ברכישת כל מוצר, מורכב מפעולות רבות של מעבר מידע בין הלקוח לסוחר:

* הקונה מבקש מוצר מהסוחר,
* הסוחר שולח טופס בקשת פרטים אישיים (פרטי זיהוי, חשבון בנק ואופן תשלום) מהלקוח,
* הקונה שולח לסוחר את הטופס מלא בנתונים,
* הסוחר מעביר את נתוני הלקוח לחברת האשראי לשלם אמות אשראי,
* חברת האשראי מחזירה תשובה לסוחר,
* הסוחר שולח תשובה ללקוח.

תארו לעצמכם את מסלול הייסורים, שכל משתמשי הסחר האלקטרוני היו חייבים לעבור, אילו הסוחרים היו מבצעים כך את קשרי הלקוחות שלהם והיו נאלצים להצפין בכל שלב במפתח שונה.

לסיכום, הצפנת המידע שעובר בתקשורת במערכת סחר אלקטרוני בשיטה של one time pad, מחייבת ייצור של מספר רב של מפתחות עבור כל session ולכן אינה ישימה. היא גם אינה ישימה במערכות מידע בהן נפח המידע שעובר בתקשורת הוא גדול (כי אז אורך המפתח היה עצום).

10 מחשוב ההצפנה ופיתוח DES

10.1 הקדמה - מספרים בינריים ואותיות מחשב

כמו בשאר תחומי החיים, גם בהצפנה הביא השימוש במחשב לקפיצת מדרגה בתהליכי ההצפנה והפענוח. גם התחכום שלהם וגם המהירות בה ניתן לבצע אותם, גדלו מאוד. כדי להצפין ולפענח בעזרת המחשב צריך לתרגם את כל תווי המסר לשפת המחשב. שפת המחשב היא מספרית. בסעיף קודם כבר ראינו כיצד ממירים אותיות למספרים הרגילים, הנכתבים בעזרת 10 הספרות. אבל בשפת המחשב שתי ספרות בלבד, 0 ו- 1, המציינות שני מצבים אפשריים במעגל החשמלי: קיום זרם חשמלי (1), או העדרו (0). לכן אנו קוראים לה: שפה בינרית. את נתוני המסר אנו מזינים לזיכרון של המחשב. אפשר להמשיל את זיכרון המחשב למיליוני מעגלים חשמליים ובהם נורות זעירות, שכל אחת מהן עשויה להימצא באחד משני מצבים בלבד, דולקת או כבויה. מצבים אלה מצוינים על ידי הספרות 0 ו-1 ולכן כל הנתונים המוזנים למחשב (נתוני הקלט), וכל התוצאות של פעולות המחשב עליהם (נתוני הפלט), מנוסחים בשפה הבינרית.

קודם המרנו את האותיות למספרים הרשומים בשיטה העשרונית. כדי להזין את המספרים העשרוניים (שמייצגים את האותיות) למחשב, עלינו לתרגם אותם לשפה הבינרית, שאותה המחשב מכיר.

לצורך חישובים בשיטה הבינרית, נציין חלק מחוקי החיבור והכפל. חוקים אלה רשומים בטבלה:

<u>לוח החיבור בשיטה הבינרית:</u>

+	0	1
0	0	1
1	1	10

על סמך לוח החיבור, נוכל לרשום את הייצוג הבינרי של עשרת המספרים העשרוניים הראשונים.
הרישום מרוכז בטבלה:

ייצוג עשרוני	ייצוג בינרי
0	0
1	1
2	10
3	11
4	100
5	101
6	110
7	111
8	1000
9	1001
10	1010

<u>לוח הכפל בשיטה הבינרית:</u>

X	0	1
0	0	0
1	0	1

מספרים בייצוג בינרי מקובל לסמן עם המספר "2" בצדם הימני התחתון. מספרים בייצוג עשרוני מקובל לסמן עם המספר "10" בצידם הימני התחתון.
במה דומות ובמה נבדלות שתי השיטות? למשל, מה קובע את ערכה של ספרה כלשהי במספר? נבדוק למשל את המספר 333_{10} (המספר העשרוני 333), הספרה 3 מופיעה בו 3 פעמים, אך מציינת בכל פעם מספר שונה: פעם 3 אחדות, פעם 3 עשרות ופעם 3 מאות, הכל לפי מקומה של הספרה במספר. ומה המצב בשיטה הבינרית? למשל במספר 111_2, הספרה 1 מופיעה בו 3 פעמים אך בכל פעם ערכה שונה, בהתאם למקומה במספר. קוראים לתכונה הזאת **ערך המקום** והיא משותפת לשתי השיטות. אפשר לרשום זאת כך:
בשיטה העשרונית:

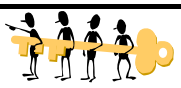
$$333_{10} = 3\times100_{10} + 3\times10_{10} + 3\times1_{10} = 3\times10^2_{10} + 3\times10^1_{10} + 3\times10^0_{10}$$

בשיטה הבינרית:

$$111_2 = 1\times100_2 + 1\times10_2 + 1\times1_2 = 1\times10_2^2 + 1\times10_2^1 + 1\times10_2^0 = 1\times2_{10}^2 + 1\times2_{10}^1 + 1\times2_{10}^0 = 1\times4_{10} + 1\times2_{10} + 1_{10} = 7_{10}$$

מה אפשר להסיק מן הצורה שבה רשמנו את המספרים כסכומים של מכפלות? בשיטה העשרונית רושמים את המספר כסכום. כל איבר של הסכום הוא מכפלה של אחת מספרות המספר **בחזקה של 10**, בהתאם למקומה של הספרה במספר. גם בשיטה הבינרית רושמים את המספר כסכום של מכפלות, אבל כל אחד מאברי הסכום הוא מכפלה של אחת מספרות המספר **בחזקה של 2,** בהתאם למקומה של הספרה במספר.

לסיכום, בשתי השיטות ערך הספרות במספר נקבע על ידי **מקומן** בו. אבל **הערך** של המקום **שונה בשתי השיטות.** בשיטה העשרונית הוא נקבע על ידי חזקות של 10, בשיטה הבינרית על ידי חזקות של 2.



שאלה מספר 49:

המשיכו ורשמו בשיטה הבינרית את המספרים 20_{10} - 11_{10}.

שאלה מספר 50:

א. כתבו בשיטה העשרונית את המספרים הבאים: 1111_2, 1101_2, 10001_2, 10101_2

ב. כתבו בשיטה הבינרית את המספרים הבאים: 32_{10}, 16_{10}, 24_{10}, 35_{10}, 55_{10}, 64_{10}, 128_{10}

שאלה מספר 51:

נתונה השיטה הרומית לכתיבת מספרים. בשיטה זו:

I = 1, V = 5, IV = 4, VI = 6, X =10, IX = 9, XI = 11, L = 50, C = 100, D = 500, M = 1000

א. כתבו בשיטה הרומית: 8, 14, 29, 101, 140, 555, 1244

ב. האם השיטה הרומית מבוססת על ערך המקום? נמקו.

10.2 התקן האמריקאי ASCII

רוב המחשבים משתמשים להמרת תווי המסר לנתוני קלט למחשב, בתקן אמריקאי, שנקרא ASCII (American Standard Code for Information Interchange). תקן ASCII הוא למעשה שיטת התאמה, שמתאימה לכל תו שרוצים להזין למחשב, מספר מסוים בין 1 ל- 256. מספר זה (בין 1 ל- 256) מיוצג בינרית על ידי 8 ספרות 0 ו- 1. (בנספח ד' מופיעה טבלת קוד ASCII מלאה). כמה מפתחות שמכילים 8 ספרות של 0 ו- 1, רק בסדר שונה, אפשר ליצור? – כדי להשיב על כך נתחיל במקרה יותר פשוט.

שאלה מספר 52:

א. כמה מספרים שונים בני שתי ספרות אפשר ליצור, מהספרות 1 ו- 0, כשאפשר לחזור ולבחור אותה ספרה ללא הגבלה?

רמז: כיוון שאנו מתירים נוכחות אפס במקום השמאלי הקיצוני, אז למקום הראשון אפשר לבחור שתי ספרות, 0 או 1. גם למקום השני אפשר לבחור שתי ספרות, כיוון שאנחנו מתירים חזרות על אותה ספרה.

ב. כמה מספרים בני 3 ספרות אפשר ליצור מהספרות 0 ו- 1 באותם תנאים?

נחזור לקוד ASCII, המורכב מצרופים שונים של 8 ספרות 0 ו- 1. כמה צרופים כאלה אפשר ליצור? כמספר המספרים בני 8 ספרות שאפשר ליצור מן הספרות 0 ו- 1, 2^8 =2x2x2x2x2x2x2x2 , שהם 256.

לסיכום, בקוד ASCII כל אות מיוצגת על ידי צירוף ייחודי של 8 ספרות (או תווים) 0 ו-1. כל תו, 0 או 1 נקרא ביט (בעברית סיבית). בטבלה רשומות מספר דוגמאות להמרה של אותיות לצופן ASCII השלימו את הטבלה.

טבלת קוד ASCII חלקית

האות	ייצוג עשרוני	ייצוג בינרי	האות	ייצוג עשרוני	ייצוג בינרי
A	97_{10}	1100001_2	N	110_{10}	1101110_2
B	98_{10}	1100010_2	O	111_{10}	1101111_2
C	99_{10}	1100011_2	P	112_{10}	1110000_2
D	100_{10}	1100100_2	Q	113_{10}	1110001_2
E	101_{10}		R	114_{10}	
F	102_{10}		S	115_{10}	
G	103_{10}		T	116_{10}	
H	104_{10}		U	117_{10}	
I	105_{10}		V	118_{10}	
J	106_{10}		W	119_{10}	
K	107_{10}		X	120_{10}	
L	108_{10}		Y	121_{10}	
M	109_{10}		Z	122_{10}	1111010_2

שאלה מספר 53:

כתבו בקוד בינרי את קוד ASCII של המילים: Good Morning.

10.3 DES (Data Encryption Standard)

שיטות ממוחשבות ליצירת מפתחות סודיים משתמשות בהרבה מחזורים של שחלוף וערבול. השיטה הנפוצה ביותר, הנהוגה כיום ליצירת מפתחות סודיים בדרך זו, ה- DES, מבצעת 16 מחזורים של שחלוף וערבול על קבוצות של 8 אותיות. כל קבוצה כזאת נקראת בלוק. ה- DES, אם כן, הוא אלגוריתם הצפנה סימטרי (להזכירכם, זו הצפנה שבה ידיעת מפתח ההצפנה מביאה לגילוי מיידי של מפתח הפענוח), ששייך למשפחה של הצפנות על בלוקים של מידע בעלי אורך קבוע. על כל בלוק מופעל אלגוריתם קבוע של הצפנה.
לצופן כזה קוראים צופן בלוקים (Block Cipher).

שאלה מספר 54:

כמה ביטים יש בבלוק של 8 אותיות?

10.4 הרקע לפיתוח ה- DES

בסוף שנות ה- 60 של המאה ה- 20 החל עידן חדש בהצפנה, כאשר חברות נזקקו לדרכים מאובטחות להעברת מסמכים וקבצים. מוסדות ציבוריים, בעיקר המוסדות הפיננסיים, נזקקו לתקן הצפנה בדוק ואמין, בו יוכלו להשתמש בביטחון מלא, להחלפת נתונים. לחברות רבות היו מחשבים שיכלו לבצע הצפנות, אבל כדי שכל אחת מהן תוכל לקיים תקשורת ברמת אבטחה ידועה ומוסכמת על כולן, חסר היה תקן. חסרה שיטת הצפנה מקובלת, מוסכמת אוניברסלית. ב- 1974 החליטה NSA (National Security Agency) בארה"ב, על ה- DES, שיטת הצפנה שהוצעה על ידי IBM, כתקן הצפנה מחייב.

השיטה ידועה גם בשם: DEA (Data Encryption Algorithm). ב- 1977 הוחלט כי השיטה תעמוד לביקורת של NSA, מידי 5 שנים.

10.5 תיאור ה- DES

1. האלגוריתם מתוכנן להצפין בלוק נתונים, באורך קבוע של 64 ביטים, ועל כל בלוק מופעל אותו אלגוריתם שאינו תלוי בבלוקים עצמם. לכן ה- DES הוא דוגמא לצופן בלוקים. צופן שבו תווי המידע, נחלקים לקבוצות (בלוקים) באורך קבוע.
2. אורך המפתח ב- DES הוא 64 ביטים.
3. שני אנשים שרוצים לתקשר באמצעות DES, צריכים להסכים על מפתח סודי. כל יתר הנתונים הקשורים ב- DES הם מידע ציבורי. האלגוריתם ידוע לפרטיו וניתן לרכוש ללא הגבלה חומרה ותוכנה שמבצעות הצפנה DES.
4. תאור האלגוריתם:
   - 4.1 למפתח הסודי K, בוחרים המשתמשים 7 תווים של 8 ביטים, בסך הכל 56 ביטים. ה- DES מוסיף 8 ביטים נוספים, המשמשים לביקורת וכך מתקבל מפתח של 64 ביטים.
   - 4.2 בעזרת K, יוצרים תמורה התחלתית על בלוק הנתונים בן 64 הביטים.
   - 4.3 מבצעים 16 מחזורים של ערבול ושחלוף של בלוק הנתונים.
   - 4.4 על הבלוק הסופי (אחרי המחזור ה- 16), מבצעים תמורה הופכית לתמורה ההתחלתית.
   - 4.5 64 הביטים שהתקבלו הם המסר המוצפן.

5. הפענוח מבוצע באמצעות מפתח ההצפנה, על ידי חזרה על הליכי ההצפנה בסדר הפוך, והם:
   5.1 מבצעים תמורה התחלתית על בלוקים של הצופן.
   5.2 מבצעים 16 מחזורים של ערבול ושחלוף הפוכים לאלה שבוצעו בהצפנה.
   5.3 מבצעים תמורה הפוכה על כל בלוק של הנתונים.

בנספח ז' ישנה סכמה של אלגוריתם DES.

10.6 עד כמה ה- DES הוא חסין פיצוח?

המפתח של DES הוא בן 56 ביטים. כמה מפתחות שונים אפשר ליצור מ- 56 ביטים? התשובה נשענת על שיקולים שהכרנו בסעיף 9, בדיון בשיטת ה- One time Pad, השאלה היא כמה מספרים בני 56 ספרות אפשר ליצור משתי ספרות, והתשובה היא 2^{56}. זה מספר עצום: $7x10^{16} \sim 2^{56}$. ל- DES יש 70 קוודריליון, שבעים אלף מיליון מיליונים, מפתחות אפשריים! הוא חסין פיצוח במונחי הקריפטוגרפיה (תורת ההצפנה) המסורתית. אבל למרות "גילו הצעיר" (ה- DES הוא בן 30 בלבד), כבר אין הוא בטוח במידה מספקת.

גם 70 קוודריליון מפתחות פוטנציאליים אינם מספיקים בימינו למניעת הפיצוח. ניתוח סטטיסטי של שכיחות האותיות, השיטה שהכרנו בסעיף 5.2, נשקם העיקרי של מפצחי מסרים מוצפנים במשך דורות, אינו מסייע בהתקפה על שיטה כ- DES. זו שיטה כל כך מאובטחת עד שלמפצחים לא נותרת ברירה, פרט לתקיפת המפתח. כלומר ניסוי כל המפתחות האפשריים.

מדוע שיטת הפיצוח הזו (של ניסוי כל המפתחות), מקטינה את חסינותו של ה- DES לפיצוח כיוון שהיא תלויה במהירות הפיצוח של כל מפתח והתפתחות הטכנולוגיה מקטינה בהתמדה את משך הזמן של הפיצוח הממצה (Brute Force Attacks).כלומר,את הזמן הדרוש לפיצוח של כל המפתחות האפשריים.

נסביר זאת ביתר פירוט: המפצח אינו מכיר את המפתח, הוא מנסה לגלותו, לפצח אותו. כל ניסוי יכול להצליח אך יכול גם להיכשל. הסיכוי להצליח והסיכוי להיכשל שווים זה לזה. לכן מספר ניסיונות הפיצוח, שיהא עליו לבצע הוא בממוצע, מחצית ממספר המפתחות האפשריים. במקרה שלנו, 35 קוודריליון, 35 אלף מיליון מיליונים ניסיונות. לביצוע המשימה יש צורך במחשבי-על חזקים ויקרים. אולם מצב זה משתנה בהתמדה, כיוון שעוצמת המחשבים עולה ומחירם יחסית לה יורד.

ב- 1977, נחשב מפתח של 56 ביטים (באורך 56 ביטים), להגנה טובה. מספר הצירופים של 56 "אפס"ים ו"אחד"ים הוא 2^{56} וזה סדר גודל של 10^{15}, כמו שכבר ראינו. אפשר לחשב ולראות, שמחשב המבצע 10^6 (מיליון) פעולות בשניה, יזדקק ל- 10^9 שניות, שהן בערך אלף שנים, כדי לנסות את כל המפתחות האפשריים.

גורדון מור (Gordon Moore), ממייסדי אינטל טען כי הודות להתפתחות הטכנולוגית מוכפל כוחו של המחשב מידי 18 חודשים, מבלי שהדבר ישפיע על מחירו. מה המסקנה לגבי פיצוח ה- DES? אם בשנות ה 70 נזקקו המחשבים ל 1,000 שנה כדי לפצח את כל המפתחות האפשריים של DES, הרי אפשר היה לראות את DES כבטוח. אבל ב- 25 השנים שעברו מאז גדלה מאוד גם עוצמת המחשבים. ב- 1997 הצליחו לפצח את DES ב- 96 ימים. שנה לאחר מכן הצליחו לעשות זאת ב- 41 יום. ארבעה חודשים לאחר מכן הצליחו לפצח את DES ב- 56 שעות תוך שימוש במחשב, שעלותו הייתה רבע מיליון דולר. חצי שנה לאחר מכן בינואר 1999 חזר אותו צוות על הפיצוח, הפעם תוך פחות מ- 24 שעות. כיום המפצחים טוענים כי מחשב שעלותו 10^7 (עשרה מיליון דולר), יפצח את DES במספר דקות. במצב דברים זה, ברור שאי אפשר עוד להסתמך על DES במסחר האלקטרוני. יש הכרח לפתח פתרונות הצפנה יותר יעילים. נכיר כאלה בחוברת הבאה.

11 סיכום

11.1 תכונות ההצפנה הסימטרית

הכרנו בחוברת זו שיטות הצפנה שונות. נוכחנו כי חוזק האבטחה של מערכת הצפנה תלוי במספר המפתחות שהאלגוריתם שלה מייצר (עקרון קרקהוף). בהצפנת ההזזה (שהראשון להשתמש בה היה יוליוס קיסר), רק 25 מפתחות, אם מדובר באנגלית, או 21 מפתחות אם מדובר בעברית. ברור שאלה הצפנות חלשות, אפשר לפצח כל אחת מהן על ידי פחות מ- 30 ניסיונות. הגידול בחוזק האבטחה מושג על ידי תמורות הא"ב (שחלופים וערבולים). מספר המפתחות האפשריים (באנגלית) !26, כמספר התמורות של אותיות הא"ב האנגלי. כדי לייעל את תהליכי ההצפנה והפענוח מפתחים מכונות הצפנה וראינו כי גם המחשב נרתם למאמץ של פיתוח מספר רב של מפתחות. מדוע כל שיטות ההצפנה המתוחכמות האלה עדיין אינן מספקות?

לכל המפתחות שהכרנו בחלק זה (פרט לכפלי המודולרי וההופכי שלו), שתי תכונות:

סימטריה: מפתח ההצפנה זהה למפתח הפענוח ופעולת הפענוח הפוכה לפעולת ההצפנה. מתכונה זו נובעת תכונה נוספת,

סודיות: כיוון שמפתח ההצפנה והפיענוח זהים, מפתח ההצפנה מוכרח להיות סודי. גם אם מניחים ששיטת ההצפנה אינה סודית, המפתח עצמו ידוע אך ורק לשולח המסר ולנמען. חשיפת המפתח על ידי האויב מגלה את המסר ומחסלת את אבטחת המערכת.

כל מערכות ההצפנה הקלאסיות, שהיו בשימוש יותר מאלפיים שנה, מבוססות על מפתחות סימטריים, ולכן בהכרח סודיים וזה גם מקור המגבלות שלהן.

11.2 מגבלות ההצפנה הסימטרית

I. **הצורך בהסכם מוקדם:** הצפנת המסרים בשיטה הסימטרית, מחייבת את השולח ואת הנמען להסכים **מראש** על המפתח. במערכות הצפנה כאלה, כדי להסכים על המפתח, יש הכרח בהתקשרות מקדימה בין השולח (המצפין), לבין לנמען, בערוץ חסוי ומאובטח, **עוד לפני העברת המסר עצמו**. אבל אחת הבעיות בעולם התקשורת, הוא המרחק הרב בין השולח לנמען. המרחק הרב מקשה מאוד על ביצוע "ההסכם המוקדם", על מפתח סודי משותף לשולח ולנמען, כך שלא יתגלה על ידי גורם לא רצוי.

II. **ריבוי המפתחות:** במערכת הצפנה סימטרית, לכל זוג של משתמשים, יש מפתח הצפנה משלו. זהו המפתח שישמש את הזוג במהלך ההצפנה וגם במהלך הפיענוח. כמה מפתחות דרושים למערכות הצפנה סימטריות רבות משתמשים? שני משתמשים זקוקים למפתח אחד. לכמה מפתחות זקוקים שלושה משתמשים (א', ב', ג')? נניח שהסכם מפתח דינו כלחיצת יד. א' לוחץ יד עם ב' ו- ג' (בוצעו הסכמים על שני מפתחות), ב' ו- ג' לחצו ידיים (בוצע הסכם מפתח נוסף). בסך הכל, שלושה משתמשים, שכל אחד מהם מעונין לתקשר עם שני האחרים, זקוקים לשלושה מפתחות.

מה במקרה הכללי של *n* משתמשים שכל אחד מהם מעוניין לתקשר בהצפנה עם כל האחרים? הראשון מסכים על מפתחות עם *n-1* המשתמשים האחרים (כולם פרט לו עצמו). על כמה מפתחות נותר למשתמש השני להסכים? עם המשתמש הראשון הוא כבר הסכים על מפתח. עם עצמו אין לו צורך להסכים. לכן *נותרו n-2* משתמשים, שעליו להסכים אתם על מפתחות הצפנה. מאותם שיקולים למשתמש השלישי נותר להסכים *על n-3* מפתחות, לרביעי על *n-4* וכך הלאה. כשהגענו למשתמש השלישי מן הסוף, עם כמה משתמשים נותר לו להסכים על מפתח? רק עם שני האחרונים. השני מן הסוף? רק עם אחד, עם האחרון. אז על כמה מפתחות הוסכם בסך הכל?

$$1+2+3+\ldots+(n-4)+(n-3)+(n-2)+(n-1)$$

זהו מספר המפתחות, להם זקוקים *n* משתמשים, כדי לתקשר ביניהם ללא מגבלה (כל אחד עם כל האחרים). כיצד לחשב מספר זה? כדי להקל על החישוב נחבר את אברי הסדרה בזוגות:

הראשון עם האחרון	n	=	$(n-1)$	+ 1
השני עם השני מן הסוף	n	=	$(n-2)$	+ 2
השלישי...	n	=	$(n-3)$	+ 3

וכך הלאה, זוג אחר זוג וכל זוג סכומו *n*. כמה זוגות כאלה יש?

מחצית ממספר אברי הסדרה, $\frac{(n-1)}{2}$.

הסכום של הסדרה שווה למכפלה של ערכו של כל זוג- *n*, במספר הזוגות: $\frac{(n-1)}{2}$

ולכן המספר הכולל של המפתחות במערכת סימטרית הוא:

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

כדי לדון במשמעות של העובדה הזאת, השלימו את הטבלה הבאה:

מספר משתתפים בהצפנה סימטרית	מספר המפתחות לו הם זקוקים
10	
50	
100	
500	
1000	
50.000	
100,000	
1,000,000	
N	$\frac{n\cdot(n-1)}{2}$

אנחנו רואים לפי החישובים בטבלה, כי מיליון משתמשים זקוקים ל:

$$\frac{1{,}000{,}000\times 999{,}000}{2}\sim\frac{1{,}000{,}000\times 1{,}000{,}000}{2}=\frac{1{,}000{,}000^2}{2}=500{,}000{,}000{,}000$$

ובמילים, מיליון משתמשים במערכת הצפנה סימטרית, זקוקים לחמש מאות מיליארד מפתחות. מיליון משתמשים זה מספר סביר כשמדובר ברשתות אינטרנטיות. **אבל ניהול של 500 מיליארד מפתחות הוא בלתי ישים לחלוטין.**

לסיכום, שתי הבעיות, בעיית ההסכם המוקדם ובעיית ריבוי המפתחות, הן המגבלות של מערכות הצפנה סימטריות. הן הופכות את ניהול מערכת המפתחות למשימה מסובכת מאוד וכשהמערכת רבת משתמשים, לבלתי ישימה. שורש הבעיה בסימטריות של המערכת. האם קיימת אפשרות אחרת? האם אפשר לפתח מערכות הצפנה אחרות, שלא יסבלו ממגבלות אלה?

היזכרו מה קרה כשניסינו לפענח מסר שהוצפן על ידי כפל מודולרי (סעיפים 4.4 ,4.3.1 ,4.3), קבלנו מפתח פענוח מיוחד, שונה ממפתח ההצפנה. קבלנו הצפנה אסימטרית.

בחוברת הבאה נכיר הצפנות אסימטריות, שפותחו ברבע האחרון של המאה העשרים ונבחן דרכים חדשות לבניית הצפנות חזקות ולהתמודדות עם הבעיות של ניהול המפתח.

נספח א':

I. מילון מונחים – עברי-אנגלי

1. אורך המפתח – Key Length
2. אלגוריתם ההצפנה - Encryption Algorithm
3. דס - 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. מפתח פומבי - Public Key
11. מפתח פרטי - Private Key
12. פענוח - Decryption = Decipherment = Decode
13. צופן/הצפנה- Cipher
14. צופן הזזה - Shift Cipher
15. צופן מונואלפבתי - Mono Alphabetic Cipher
16. צופן ערבול - Transposition Cipher
17. צופן פוליאלפבתי - Poly Alphabetic Cipher
18. צופן שחלוף- Substitution Cipher
19. קוד – Code
20. קוד אסקי - ASCII Code (American Standard Code for Interchanging Information)
21. קריפטואנליזה – Cryptanalysis
22. קריפטוגרפיה - Cryptography
23. קריפטולוגיה - Cryptology

1. אורך המפתח - Key Length

בהצפנות בכלל ובפרט בהצפנות הממוחשבות, עובדים עם מפתחות שהם מספרים. אורך המפתח מציין את מספר הספרות, או הביטים שבונים אותו. אורך המפתח מצביע על המספר הגדול ביותר בו ניתן להשתמש ליצירת המפתח וכך מגדיר את מספר המפתחות האפשריים. ככל שאורך המפתח גדול, כך רב יותר מספר המפתחות האפשריים ומתארך זמן הפיצוח על ידי האויב.

2. אלגוריתם ההצפנה - Encryption Algorithm

כל כלל או תהליך הצפנה כללי, המוגדר בדייקנות על ידי בחירת מפתח.

3. דס - DES (Data Encryption Standard)

תקן להצפנה סימטרית. פותח על ידי IBM ואומץ לשימוש בארה"ב בשנת 1976.

4. הצפנה - Encryption = Encipherment = Encode

שינוי המסר המקורי למסר מוצפן, על ידי החלפת כל אות במסר באות אחרת או בסמל אחר.

5. הצפנה אסימטרית - Asymmetric Key Cryptography

שיטת הצפנה שבה מפתחות ההצפנה והפיענוח שונים זה מזה, וידיעת מפתח ההצפנה אינה מסגירה את מפתח הפיענוח.

6. הצפנה סימטרית - Symmetric Key Cryptography

שיטת הצפנה שבה מפתחות ההצפנה והפיענוח זהים זה לזה. המונח מתאים לכל שיטות ההצפנה המסורתיות. כלומר כל אלה שהיו נהוגות לפני 1970.

7. מסר - Plaintext

המידע המקורי.

8. מסר מוצפן - Ciphertext

המסר לאחר הצפנתו.

9. מפתח הצפנה - Key

האלמנט שהופך את אלגוריתם ההצפנה הכללי, לשיטת הצפנה ייחודית (ספציפית). הנחת המצפינים היא, שחוזק המפתח הוא הקובע את חוסן ההצפנה. גם אם האויב יודע את אלגוריתם ההצפנה, הוא לא יוכל לפצח את המסר המוצפן, אם מפתח ההצפנה חזק. לכן חשוב כל כך לשמור על סודיות המפתח.

10. מפתח פומבי - Public Key

מונח מתחום ההצפנה האסימטרית. זהו מפתח ההצפנה בו משתמש השולח בכדי להצפין מידע שנשלח ליעדו. בשיטת ההצפנה האסימטרית, המפתח הפומבי גלוי ונגיש לכולם.

11. מפתח פרטי - Private Key

מונח מתחום ההצפנה האסימטרית. זהו מפתח הפיענוח בו משתמש מקבל המסר המוצפן. המפתח הפרטי ידוע רק לבעליו.

12. פענוח - Decryption = Decipherment = Decode

הפיכה חוזרת של הטקסט המוצפן לטקסט המקורי.

13. צופן - Cipher

כל שיטת הצפנה להסתרת משמעות המסר, על ידי החלפת כל אות במסר המקורי באות אחרת. לשיטה מידה מסוימת של גמישות בבסיסה. במונח גמישות הכוונה היא שבהצפנות שונות, עשויה אותה אות, במסר המקורי, להתחלף באותיות שונות במסר המוצפן. הגמישות נקבעת על ידי המפתח.

14. צופן הזזה - Shift Cipher

כל אות במסר המקורי מוחלפת על ידי אות 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 וכך התקבל המסר המוצפן.

15. צופן מונואלפבתי - Mono Alphabetic Cipher

בהצפנה כל אות במסר המקורי, מוצפנת לאות אחת ורק אחת במסר המוצפן.כלומר, אות שמופיעה במסר מספר פעמים, תוחלף בכל פעם באותה אות. הוא הדין גם בפיענוח. במתמטיקה נהוג לומר כי קימת התאמה חד-חד-ערכית בין אותיות המסר המקורי לאותיות המסר המוצפן.

16. צופן ערבול - Transposition Cipher

בהצפנה, אותיות המסר המקורי משנות את מקומן, מתערבלות. אבל כל אות שומרת על זהותה. כל אותיות המסר המקורי נמצאות גם במסר המוצפן

17. צופן פוליאלפבתי - Poly Alphabetic Cipher

כל אות במסר המקורי עשויה להיות מוצפנת ליותר מאות אחת במסר המוצפן.

18. צופן שחלוף - Substitution Cipher

הוא צופן הזזה, שבו מידות ההזזה של אותיות המסר המקורי שונות. צופן הזזה הוא מקרה פרטי של צופן שחלוף, שבו מבוצעת על כל אותיות המסר, מידה שווה של הזזה.

19. קוד - Code

i. **דרך לייצוג מידע** לפי טבלת קידוד ידועה. הטבלה חייבת לתאר התאמה חד-חד-ערכית. לדוגמא, קוד ASCII (מקודדים לפי טבלת קוד ascii), קוד מורס (מקודדים לפי טבלת קוד מורס)..

ii. קדוד זוהי כתיבת תכניות בשפת המחשב.

iii. צופן המורה על החלפת מילה או משפט במסר המקורי, בתו אחד או בקבוצת תווים, במסר המוצפן.

20. קוד אסקי - ASCII Code (American Standard Code for Interchanging Information)

תקן אמריקאי לקידוד נתונים (אלפביתיים ואחרים) למספרים.

21. קריפטואנליזה - Cryptanalysis

המדע של גילוי משמעותו של המסר המקורי, מתוך המסר המוצפן, ללא ידיעת מפתח ההצפנה.

22. קריפטוגרפיה - Cryptography

מדע ההצפנה והסתרת המשמעות של המסר. משתמשים במושג גם כמושג נרדף לקריפטולוגיה.

23. קריפטולוגיה - Cryptology

המדע של כתבי הסתר וההצפנות השונות. מושג נרדף לקריפטוגרפיה.

II. מילון מונחים – אנגלי-עברי

(המספור מתאים למספור המונחים במילון המונחים העברי אנגלי).

20. ASCII Code
14. Alphabetic Cipher
5. Asymmetric Key Cryptography
13. Cipher
8. Cipher text
19. Code
23. Cryptology
22. Cryptography
21. Cryptanalysis
12. Decryption
3. DES
2. Encryption Algorithm
4. Encryption – Encipherment – Encode
9. Key
1. Key Length
15. Mono Alphabetic Cipher
7. Plaintext
17. Poly Alphabetic Cipher
11. Private Key
10. Public Key
14. Shift Cipher
6. Symmetric Key Cryptography
18. Substitution Cipher
16. Transposition Cipher

נספח ב'

I. מעגלי הצפנה בעברית

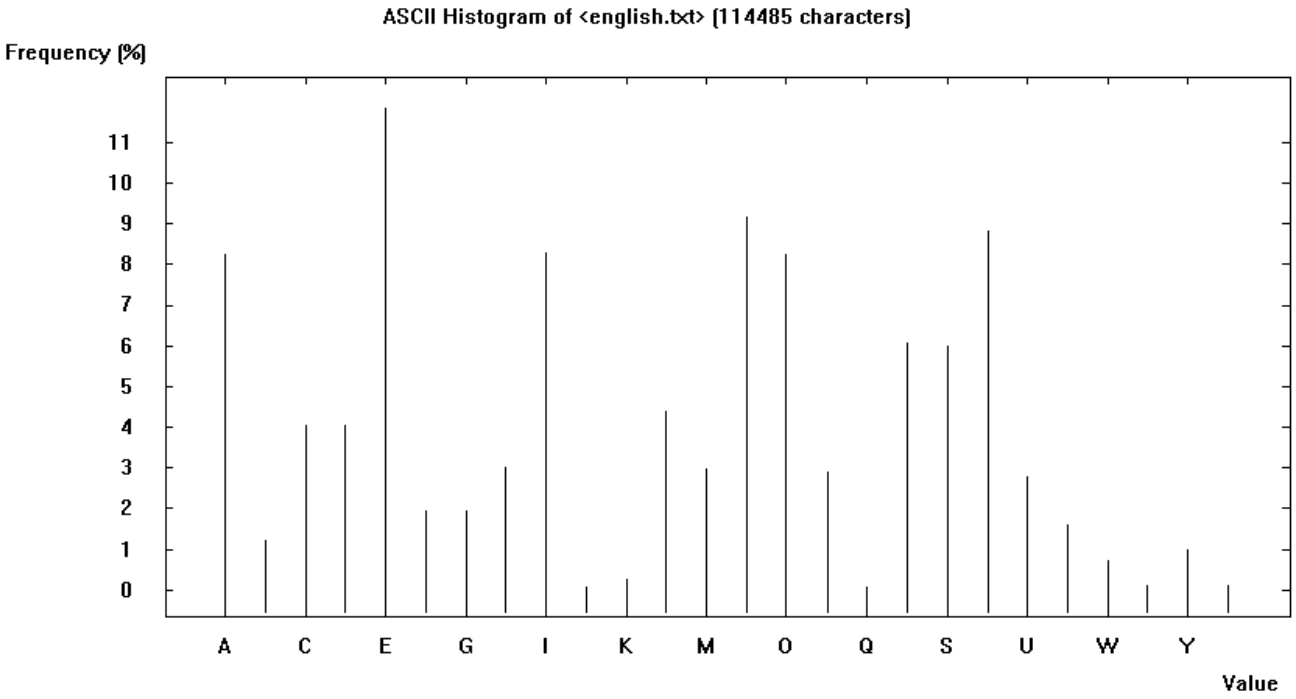

המודיאון
הלאומי
למדע

II. מעגלי הצפנה 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
המודיאון
הלאומי
למדע

נספח ג'

היסטוגרמת שכיחויות של אותיות הא"ב האנגלי בקובץ טקסט נתון בן 114,485 תווים



נספח ד':

טבלת קוד ASCII מלאה

Char = תו על המקלדת

Dec = הייצוג העשרוני של קוד ASCII

Dec	Char	Dec	Chr	Dec	Chr	Dec	Chr	Dec	Chr	Dec	Chr	Dec	Chr	Dec	Chr
0	NUL (null)	32	Space	64	@	96	`	128	Ç	161	í	190	╛	219	█	248	°
1	SOH (start of heading)	33	!	65	A	97	a	129	ü	162	ó	191	┐	220	▄	249	∙
2	STX (start of text)	34	"	66	B	98	b	130	é	163	ú	192	└	221	▌	250	·
3	ETX (end of text)	35	#	67	C	99	c	131	â	164	ñ	193	┴	222	▐	251	√
4	EOT (end of transmission)	36	$	68	D	100	d	132	ä	165	Ñ	194	┬	223	▀	252	ⁿ
5	ENQ (enquiry)	37	%	69	E	101	e	133	à	166	ª	195	├	224	α	253	²
6	ACK (acknowledge)	38	&	70	F	102	f	134	å	167	º	196	─	225	ß	254	■
7	BEL (bell)	39	'	71	G	103	g	135	ç	168	¿	197	┼	226	Γ	255	
8	BS (backspace)	40	(	72	H	104	h	136	ê	169	⌐	198	╞	227	π		
9	TAB (horizontal tab)	41	)	73	I	105	i	137	ë	170	¬	199	╟	228	Σ		
10	LF (NL line feed, new line)	42	*	74	J	106	j	138	è	171	½	200	╚	229	σ		
11	VT (vertical tab)	43	+	75	K	107	k	139	ï	172	¼	201	╔	230	µ		
12	FF (NP form feed, new page)	44	,	76	L	108	l	140	î	173	¡	202	╩	231	τ		
13	CR (carriage return)	45	-	77	M	109	m	141	ì	174	«	203	╦	232	Φ		
14	SO (shift out)	46	.	78	N	110	n	142	Ä	175	»	204	╠	233	Θ		
15	SI (shift in)	47	/	79	O	111	o	143	Å	176	░	205	═	234	Ω		
16	DLE (data link escape)	48	0	80	P	112	p	144	É	177	▒	206	╬	235	δ		
17	DC1 (device control 1)	49	1	81	Q	113	q	145	æ	178	▓	207	╧	236	∞		
18	DC2 (device control 2)	50	2	82	R	114	r	146	Æ	179	│	208	╨	237	φ		
19	DC3 (device control 3)	51	3	83	S	115	s	147	ô	180	┤	209	╤	238	ε		
20	DC4 (device control 4)	52	4	84	T	116	t	148	ö	181	╡	210	╥	239	∩		
21	NAK (negative acknowledge)	53	5	85	U	117	u	149	ò	182	╢	211	╙	240	≡		
22	SYN (synchronous idle)	54	6	86	V	118	v	150	û	183	╖	212	╘	241	±		
23	ETB (end of trans. block)	55	7	87	W	119	w	151	ù	184	╕	213	╒	242	≥		
24	CAN (cancel)	56	8	88	X	120	x	152	ÿ	185	╣	214	╓	243	≤		
25	EM (end of medium)	57	9	89	Y	121	y	153	Ö	186	║	215	╫	244	⌠		
26	SUB (substitute)	58	:	90	Z	122	z	154	Ü	187	╗	216	╪	245	⌡		
27	ESC (escape)	59	;	91	[	123	{	156	£	188	╝	217	┘	246	÷		
28	FS (file separator)	60	<	92	\	124	|	157	¥	189	╜	218	┌	247	≈		
29	GS (group separator)	61	=	93	]	125	}	158	₧								
30	RS (record separator)	62	>	94	^	126	~	159	ƒ								
31	US (unit separator)	63	?	95	_	127	DEL	160	á								

Source: www.asciitable.com

נספח ה'

קישורים לאתרי באינטרנט בנושא מכונת האניגמה

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

אתר של הטלוויזיה הציבורית של ארה"ב. הרבה חומר מדעי והיסטורי. מומלץ

http://www.codesandciohers.org.uk/enigma/enigma1.htm

http://www.codesandciphers.org.uk/enigma/retrospec.htm

אתר בריטי. נותן מעט רקע כללי בהצפנת שחלוף ומטפל בפרוט במפרט הטכני של האניגמה

http://www.bletchleypark.org.uk/history

אתר בריטי. מתמקד בסיפורה של האחוזה בה פעלו מפצחי האניגמה.

http://www.geocities.com/CapeCanaveral/Hangar/4040/bombe.html

אתר של סוכנות החלל. חומר על פעולתן של ה"פצצות", מכונות הפענוח שבנה אלן טיורינג, לפיצוח האניגמה

http://www.cs.miami.edu/~harald/enigma/enigma.html

אתר אמריקאי, מיאמי פלורידה, מסביר את ההצפנה והפענוח של האניגמה

http://www.cl.cam.ac.uk/Research/Security/Historical/azzole1.html

מאמר על פיצוח האניגמה

http://home.us.net/~encore/Enigma/text.html

מאמר של כותב פולני על האניגמה

http://webhome.idirect.com/~jproc/crypto/enigma.html

תאור של מכונת האניגמה

http://webhome.idirect.com/~jproc/crypto/enigs1.html

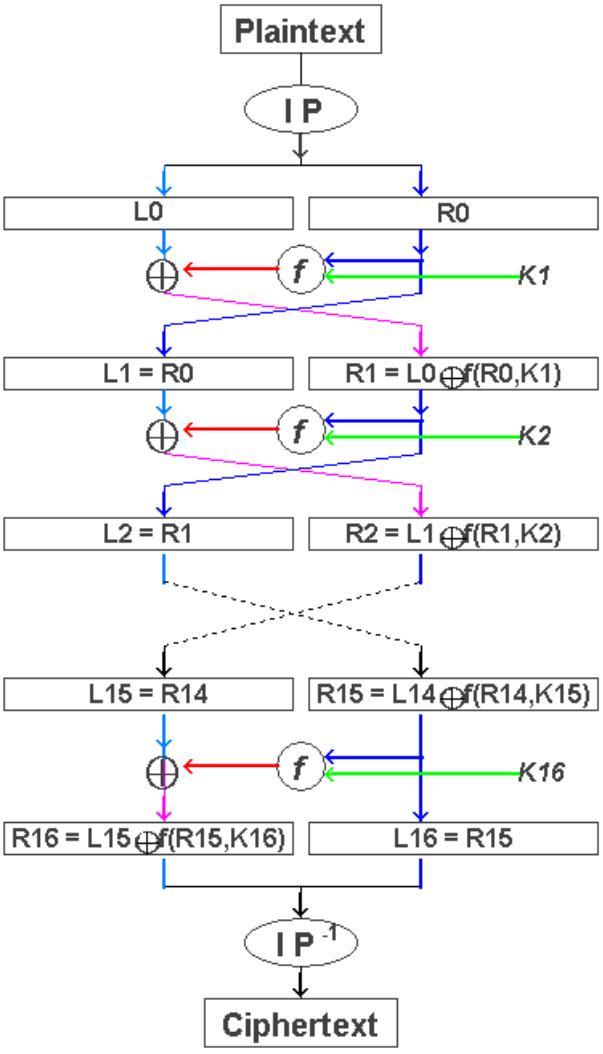
סיפור האניגמה מנקודת הראות של הפולנים, שהיו הראשונים שהחלו בפיצוחה

http://webhome.idirect.com/~jproc/crypto/enigs2.html

סיפור האניגמה מנקודת הראות של הצרפתים, שהשתתפו במאמץ הפיצוח

http://www.cs.oberlin.edu/classes/cs115/lect130n.html

נספח ו': סכמה של אלגוריתם DES



הסכמה מתארת הצפנה של מסר Paintext בעזרת אלגוריתם DES עם מפתח K.

IP = תמורת אתחול קבועה (initial permutation)

IP^{-1} = תמורה הפוכה לתמורה IP (inverse permutation)

הפעלת IP על מסר באורך של 64 bit, נותנת מחרוזת תווים התחלתית.

מחלקים מחרוזת זו לשתי מחרוזות L0 ו- R0 , כל אחת באורך 32 bit.

מבצעים 16 פעמים את הפעולה הבאה:

$1<=i<=16$ $L_i = R_{i-1}$ וכן $R_i=L_{i-1} \oplus f(R_{i-1},K_i)$.

כאשר פונקצית ה $\oplus$ מוגדרת כך:

$\oplus$	0	1
0	0	1
1	1	0

ופונקצית f היא פונקציית Feistel Cipher שבה כל Ki מתקבל מבצוע תמורה על מפתח ההצפנה הסימטרית K.

נספח ז'

פתרונות

שאלה מספר 1:

היזהרו כל השטח ממוקש כעת.

שאלה מספר 2:

את השנוא עליך אל תעשה לחברך

שאלה מספר 3:

החלק היחיד של הפנים שהאדם בוחר בעצמו.

שאלה מספר 4:

BEAUTY

שאלה מספר 5:

זקהלאז סית דירחב נלו זהאת.

שאלה מספר 6:

MEET YOU IN ORLANDO

שאלה מספר 7:

א. כלב.

ב. TIGER

ג. BUNNY

שאלה מספר 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 מספר 9:

גיצה פדציד נלנט - הוע פפט?

שאלה מספר 10:

הדגמ אדמגמ פמשכגמ

שאלה מספר 11:

אנחנו מוקפים מחכים לסיוע

שאלה מספר 12:

YHQL YLGL YLFL

שאלה מספר 13:

WE ARE READY TO ATTACK CONFIRM

שאלה מספר 14:

א. אין הבדל. מפתחות זהים בהצפנה בשיטת הזזה עם מפתח 20+בעברית :
{20,42,64,86,….} וגם {-2,-24,-46,-68,…}.

ב. מפתחות זהים בהצפנה בשיטת הזזה עם מפתח של 19+ באנגלית :
{19,45,71,…} וגם {-33,-59,-85,…}.

שאלה מספר 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

רכשההשסבצגטישואמפאכשס

שאלה מספר 16:

השעה כעת	מה תהיה השעה בעוד	הביטוי המודולרי	התשובה
		(11+16)mod12=3	3
		24mod12=0	7
		(9+2)mod12=11	11
4		(x+10)mod12=2	
	10 שעות	(3+x)mod12=1	

שאלה מספר :17

+mod12	**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 מספר 18:

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 מספר 19:

+mod7	**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 מספר 20:

א. אין הבדל

ב. שני קבוצות המספרים {20,42,64,86,….}= 20mod22 וגם {-2,-24,-46,-68,…} = -2mod22
מספקות אותו מפתח להצפנה בשיטת ההזזה.

נכון לומר כי : 20mod22=-2mod22.

באופן כללי :

אם X מפתח ההצפנה בשיטת הזזה בעברית, אז: xmod22=(x-22)mod22

ואם מעגלי ההצפנה עושים n סבובים שלמים זה ביחס לזה אז:

עבור n סבובים בכיוון השעון xmod22=(x-22+22n)mod22

ועבור n סיבובים נגד כיוון השעון xmod22=(x-22-22n)mod22

ג. באנגלית - אם נסמן את מפתח ההזזה ב-x, נכון לכתוב : xmod26=(x-26)mod26

עבור n סיבובים שלמים בכיוון השעון אז: (x+19)mod26 = (x+19+26n)mod26

ועבור n סיבובים שלמים נגד כיוון השעון אז: (x+19)mod26 = (x+19-26n)mod26

שאלה מס' 21:

התלמידים ימלאו טבלה שבחוברת.

שאלה מספר 22:

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

שאלה מספר 23:

א. יש לי משהו חשוב למסור לך.

ב. אני מגיע מחרתיים חכו לי

שאלה מספר 24:

עד עכשיו הכל בסדר, לא צריך לדאוג.

שאלה מספר 25:

הקיר אפפע מאינ וסות ראתמ השנא מרלו

הקיר אף פעם אינו סותר את מה שנאמר לו

שאלה מספר 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 בספירלמ נפתחת נגד כיוון השעון)

שאלה מספר 27:

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

חכו לי ביום ששי בעוד שבוע

שאלה מספר 28:

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

המסר המוצפן במסלול ספירלי : סיגש בשחמ הלעו וירו דפנו נעלי

שאלה מספר 29:

טבלת ההצפנה

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→

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

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

שאלה מספר 30:

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

n! = 12! = 479,001,600

ב.

שאלה מספר 31:

מדובר במקרים של תמורות עם חזרות: א. 1

ב. $\frac{6!}{2!}=3$

ג. $\frac{4!}{2!}=12$

שאלה מספר 32:

א. ללא חזרות, מספר האותיות 6, מספר התמורות 720=!6.

עם שתי חזרות של האות א', $\frac{6!}{2!}=360$. זהו מספר תמורות ההצפנה.

ב. ללא חזרות, מספר האותיות 11, מספר התמורות 39,916,800=!11.

עם שתי חזרות של האותיות ש', נ', מספר התמורות $\frac{11!}{2!\cdot 2!}=9,979,200$

ג. ללא חזרות, מספר האותיות 11, מספר התמורות 39,916,800=!11.

עם שתי חזרות של האות י' ו- 4 חזרות של ד', $\frac{11!}{2!\cdot 4!}=831,600$.

שאלה מספר 33:

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

ולפענח את המסר: ה י ד ד ל מ נ צ ח

שאלה מספר 34:

א. 5!=120

ב. 4!=24

ג. 5!-4!=96

שאלה מספר 35:

א. כל המספרים המסתיימים ב- 5 מספרם 4!.

ב. המספרים הזוגיים מסתיימים ב- 2 או ב- 4. מספרם 2x4!=48.

שאלה מספר 36:

א. מספר התמורות של ששה אברים במעגל, 5!=120

ב. 5!=120

ג. מקום האיש הראשון יחסית לכסא לצבעו שונה יכול להיות באחד מששה מקומות ולכן: 6!=720

ד. $\frac{5!}{4!}=5$

שאלה מספר 37:

א. מספר הסידורים האפשריים ל- 12 ספרים שונים הוא 12!=479,001,600, אולם בתנאי השאלה יש לחלק את התשובה הזו ב 3!x5!x3!. התשובה הסופית 110,880

ב. כיוון שקיימים 4 סוגים שונים של ספרים, מספר הסידורים האפשריים 4!=24

שאלה מספר 38:

א. 10!/(10-4)!=3,628,800/720=5040

ב. 10^4=10,000

שאלה מספר 39:

מבכדוער מוא סהלרס מאתנעצ פל תשנו מיסעוצ

שאלה מספר 40:

EVEN A CIPHER THAT WAS CREATED BY A GENIUS CAN ALWAYS BE DECIPHERED BY ANOTHER GENIUS

שאלה מספר :41

א. 4^3

ב. 1. 64^5 2. $\frac{64!}{(64-5)!}$ 3. 5^5 4. $5!$

שאלה מספר 42:

מספור אותיות המפתח:

J	A	N	E	T
3	1	4	2	5

C צופן	T	J	P	R	C	Y	U	J	S	K	S	H	H	S	W	X	H	S	N	D
	19	9	15	17	2	24	20	9	18	10	18	7	7	18	22	23	7	18	13	3
K מספר ההזזות בהצפנה לפי מילת המפתח	4	1	3	1	4	2	5	3	5	2	5	3	1	4	2	5	3	4	1	3
K- מספר ההזזות בפיענוח לפי מילת המפתח	-4	-1	-3	-1	-4	-2	-5	-3	-5	-2	-5	-3	-1	-4	-2	-5	-3	-4	-1	-3
P מספרי	15	8	17	19	0	13	14	6	13	8	14	4	6	14	20	18	4	14	12	0
P אותיות	P	I	R	T	A	N	O	G	N	I	O	E	G	O	U	S	E	O	M	A

A MOUSE GOING ON A TRIP

שאלה מספר 43:

מ	ר	ד	כ	י
4	5	1	3	2

א	נ	י	ע	ו
נ	ל	י	ז	ד
ת	ת	נ	מ	א
ק	ר	ע	י	ג

אני עוד אגיע רק תן לי זמן

שאלה מספר 44:

שאלה מספר 45:

MANY

שאלה מספר 46:

שאלה מספר 47:

א. SEND MORE MONEY

ב. RUN TO EXCERCISE

שאלה מספר 48:

הטקסט המוצפן	ג	ל	ז	ו	ז	מ	ש	ל	ח	נ
מפתח הצפנה- א	11	6	1	0	7	0	7	14	2	6
א. טקסט מקורי- א	נ	צ	ח	ו	נ	מ	ז	ה	י	ר
מפתח הצפנה- ב	19	11	20	14	19	0	15	4	10	8
ב. טקסט מקורי- ב	ת	ב	ו	ס	ה	מ	ו	ח	צ	ת

שאלה מספר :49

11_{10}	12_{10}	13_{10}	14_{10}	15_{10}	16_{10}	17_{10}	18_{10}	19_{10}	20_{10}
1011_2	1100_2	1101_2	1110_2	1111_2	10000_2	10001_2	10010_2	10011_2	10100_2

שאלה מספר 50:

א.

$$1111_2 = 1\times 2^3_{10} + 1\times 2^2_{10} + 1\times 2^1_{10} + 1\times 2^0_{10} = 15_{10}$$
$$1101_2 = 1\times 2^3_{10} + 1\times 2^2_{10} + 1\times 2^0_{10} = 13_{10}$$
$$10001_2 = 1\times 2^4_{10} + 1\times 2^0_{10} = 17_{10}$$
$$10101_2 = 1\times 2^4_{10} + 1\times 2^2_{10} + 1\times 2^0_{10} = 21_{10}$$

ב.

$$32_{10} = 1\times 2^5_{10} = 100000_2$$
$$16_{10} = 1\times 2^4_{10} = 10000_2$$
$$24_{10} = 1\times 2^4_{10} + 1\times 2^3_{10} = 11000_2$$
$$35_{10} = 1\times 2^5_{10} + 1\times 2^1_{10} + 1\times 2^0_{10} = 100011_2$$
$$55_{10} = 1\times 2^5_{10} + 1\times 2^3_{10} + 1\times 2^2_{10} + 1\times 2^0_{10} = 101101_2$$
$$64_{10} = 1\times 2^6_{10} = 1000000_2$$
$$128_{10} = 1\times 2^7_{10} = 10000000_2$$

שאלה מספר 51:

א. VIII, XIV, XXIX, CI, CXL, DLV, MCCXLIV,

ב. השיטה הרומית אינה מבוססת על ערך המקום ככלל, אלא רק במספר מקרים בהם כתיבת ספרה מימין או משמאל לספרה הסמוכה, משנה את ערך המספר (למשל IX = 9, XI = 11). שימו לב כי אין אפס בין הספרות הרומיות.

שאלה מספר 52:

א. מספר המספרים הדו-ספרתיים, שאפשר ליצור משתי ספרות הוא $2x2=2^2$. לכל אחת מן הספרות.

ב. במספר התלת ספרתי אפשר לבחור שתי ספרות ולכן סך כל הבחירות הוא $2x2x2=2^3$.

(000, 001, 010, 011, 100, 101, 110, 111)

שאלה מספר 53:

	G	O	O	D	M	O	R	N	I	N	G
קוד ASCII	103_{10}	111_{10}	111_{10}	99_{10}	109_{10}	111_{10}	114_{10}	110_{10}	105_{10}	110_{10}	103_{10}
קוד ASCII בינרי	1100111_2	1101111_2	1101111_2	1100100_2	$110011o1_2$	1101111_2	1110010_2	1101110_2	1101001_2	1101110_2	1100111_2

שאלה מספר 54:

בבלוק של 8 אותיות, שכל אחת מיוצגת על ידי 8 ביטים בינריים, יש 8x8=64 ביטים.

נספח ח'

ביבליוגרפיה

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

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 של אותו סופר)

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. Alfred J.Menzes,Paul C.van Ooschot, Scott A. Vanstone - Handbook of Applied Cryptography.
Carcr.math.uwaterloo.ca/hac