מערך שיעור – סודות ההצפנה

נכתב בהשראת הספר וחוברת הפעילויות **סודות ההצפנה לילדים** מאת ד"ר סתיו אלבר.

סקירה כללית

- **קהל יעד:** תלמידי יסודי.
- **משך זמן:** כ-90 דקות.
- **טיפ למדריך/ה:** מרגיש ארוך מדי? אין בעיה! המערך מודולרי – אפשר בקלות לפצל אותו לכמה שיעורים, לקצר את הפעילויות או לבחור רק את החלקים שהכי מתאימים.

מטרות

- היכרות עם מושגי יסוד: הצפנה, פענוח ומפתח סודי.
- הבחנה בין סוגי צפנים: צופן שחלוף (Transposition) וצופן החלפה (Substitution).
- התנסות מעשית בצפנים קלאסיים (סקייטל, אתב"ש, קיסר, החלפה).
- הבנת שיטה בסיסית לפיצוח צפנים: חיפוש ממצה.

ציוד נדרש

- לוח מחיק וטושים.
- גלילי נייר טואלט (באותו קוטר).
- רצועות נייר ארוכות וצרות (מומלץ לגזור מראש דף A4 לרוחב לרצועות בעובי 2-3 ס"מ).
- נייר דבק.
- דסקיות הצפנה.
- סיכות מתפצלות.

חלק 1: פתיחה – מי אוהב סודות? (10 דקות)

מטרה: יצירת עניין, חיבור הנושא לעולמם של הילדים והגדרת מושגי יסוד.

1. **דיון:** "מי אוהב סודות? אם הייתם רוצים לשלוח הודעה סודית לחבר שאף אחד אחר לא יבין, איך הייתם עושים את זה?" (אספו רעיונות).
2. **חיבור לחיי היומיום:** הסבירו שכולנו משתמשים בסודות כל יום. "כשאנחנו פותחים את הטלפון עם קוד, שולחים הודעות בווטסאפ, או נכנסים למשחק עם סיסמה – יש קסם בלתי נראה ששומר עלינו."
3. **הגדרת מושגים:**
   - **הצפנה (Encryption):** השם של הקסם הזה. הופכת הודעה רגילה לכתב סתרים (הודעה שאי אפשר להבין).
   - **פענוח (Decryption):** התהליך ההפוך, הפיכת כתב הסתרים חזרה להודעה המקורית.
   - **מפתח (Key):** הסוד שבעזרתו מצפינים ומפענחים. זה כמו מפת אוצר: רק מי שיש לו את המפה הנכונה יכול למצוא את האוצר.

חלק 2: מסע בזמן – צופן אתב"ש (5 דקות)

מטרה: התנסות בצופן החלפה פשוט ועתיק.

1. **הקדמה היסטורית:** הסבירו שאנשים תמיד חיפשו דרכים להסתיר מידע, הרבה לפני המצאת המחשב.
2. **צופן אתב"ש:** "אפילו בתנ"ך מסתתרים צפנים! המפורסם הוא אתב"ש. זהו **צופן החלפה** – כלומר, מחליפים כל אות באות אחרת לפי כלל קבוע."
3. **הסבר הכלל:** כל אות מוחלפת באות המקבילה לה מהסוף של הא"ב. מחליפים את האות הראשונה (א') באחרונה (ת'), את השנייה (ב') בלפני אחרונה (ש'), וכן הלאה.
4. **שאלה למחשבה:** למה הצופן נקרא כך?
5. **הדגמה על הלוח:** צור ביחד עם הילדים את טבלת ההחלפה המלאה.
   - א ↔ ת
   - ב ↔ ש
   - ...
6. **תרגול קצר:** בקשו מהילדים לפענח הודעה מוצפנת.

חלק 3: פעילות מעשית – בונים סקייטל ספרטני (20 דקות)

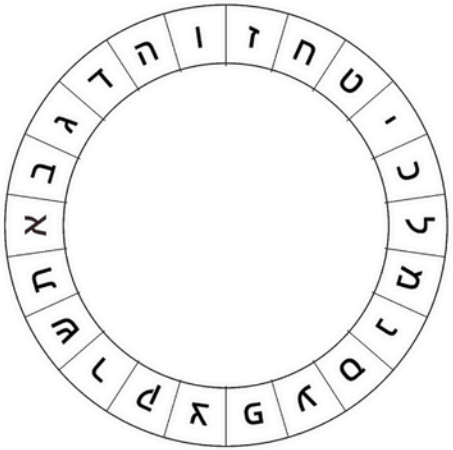
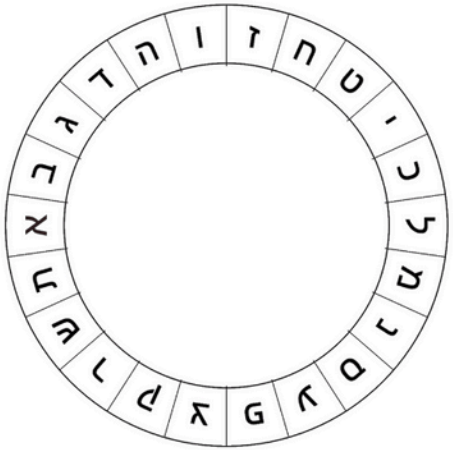
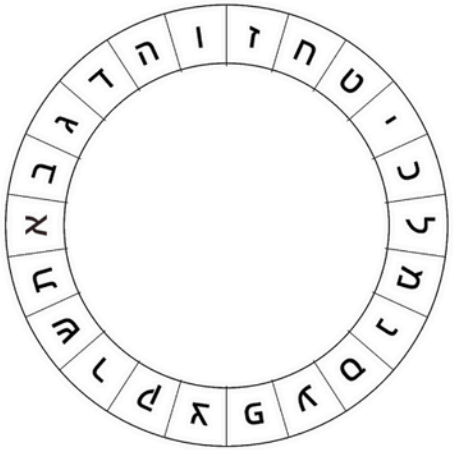
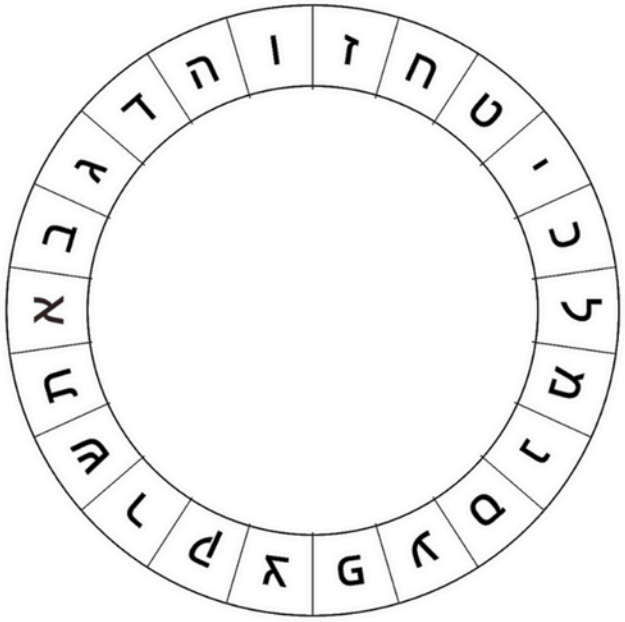
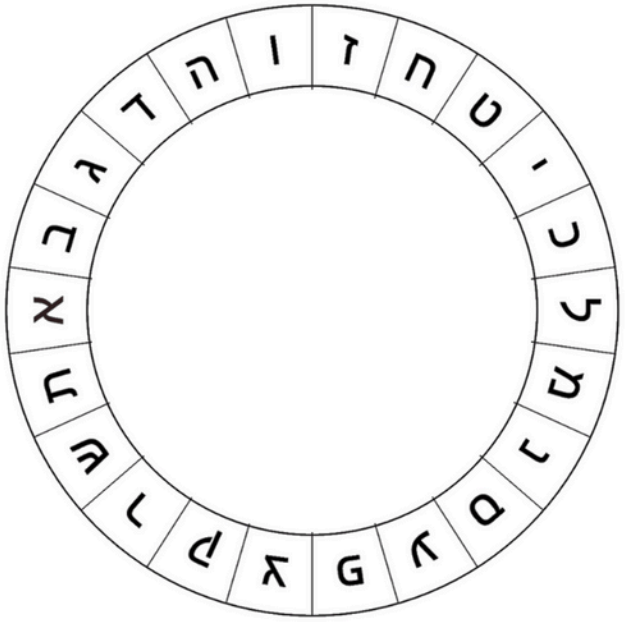
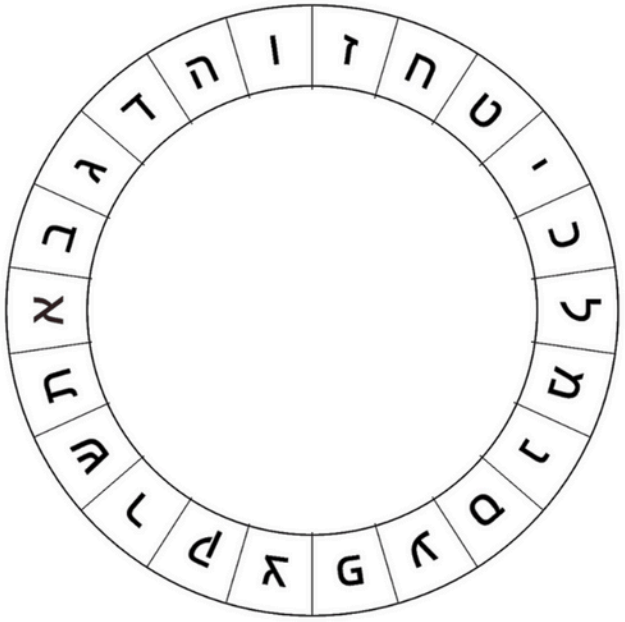
מטרה: התנסות מעשית בצופן שחלוף (שינוי סדר האותיות) והבנת חשיבות המפתח הפיזי.

1. **סיפור רקע:** "דרך אחרת להצפין היא לא להחליף את האותיות, אלא לבלבל את הסדר שלהן. זה נקרא **צופן שחלוף**. ביוון העתיקה, הלוחמים הספרטנים השתמשו בשיטה מתוחכמת שנקראת **סקייטל** (Scytale)."
2. **הסבר העיקרון:** הספרטנים היו כורכים רצועת עור סביב גליל עץ בעובי סודי, וכותבים את המסר. כשפרשו את הרצועה, האותיות התערבבו.
3. **פעילות בנייה והתנסות (בזוגות או שלישיות):**
   - חלקו לכל קבוצה גליל נייר טואלט, רצועת נייר ונייר דבק.
   - הדגימו כיצד ללפף את הרצועה סביב הגליל. **חשוב:** ללפף חזק, בלי רווחים ובלי חפיפות. הדביקו את הקצוות.
   - כתבו הודעה סודית קצרה **לאורך** הגליל, שורה אחר שורה.
   - הסירו את הרצועה מהגליל. ראו איך האותיות התבלבלו!
   - החליפו רצועות בין הקבוצות. בקשו מהם לפענח על ידי ליפוף הרצועה סביב הגליל שלהם.
4. **דיון והרחבה:**
   - שאלו: "מה היה המפתח הסודי כאן?" (תשובה: קוטר הגליל).
   - עובדת בונוס: "כדי להקשות על האויב, לפעמים הספרטנים השתמשו במקלות עם **קוטר משתנה** (כמו חרוט). זה הפך את הפיצוח לכמעט בלתי אפשרי בלי המקל המדויק!"

חלק 4: הצופן הסודי של יוליוס קיסר (20 דקות)

מטרה: למידה והתנסות בצופן הזזה (סוג של צופן החלפה) באמצעות דסקיות ההצפנה.

1. **דיון:** "יוליוס קיסר, מנהיג רומאי מפורסם, היה צריך לתקשר עם המפקדים שלו בשדה הקרב. איך הוא יכול היה לעשות זאת? מה היה קורה אם השליח ששלח עם ההודעה היה נתפס?"
2. **היכרות:** "קיסר המציא צופן שבו 'מזיזים' כל אות קדימה באלף-בית מספר קבוע של צעדים. מספר הצעדים הזה הוא **המפתח הסודי**."
3. **התנסות עם דסקיות ההצפנה:**
   - תנו לתלמידים לגזור את הדיסקיות. הסבירו: דסקית גדולה (חיצונית) = הודעה רגילה, דסקית קטנה (פנימית) = כתב סתרים.
   - רצוי לחבר את הדיסקיות במרכז באמצעות סיכה מתפצלת.
   - **הדגמת כיוונון (קריטי):** "בואו נבחר מפתח 3. אנחנו רוצים ש-א' תהפוך ל-ד'. סובבו את הדסקית הקטנה עד שהאות **ד'** (פנימית) תהיה בדיוק מתחת לאות **א'** (חיצונית)." (ודאו עם הילדים).
   - **תרגול הצפנה (חיצוני לפנימי):** "כדי להצפין, מוצאים את האות בחיצונית וכותבים את מה שמתחתיה בפנימית."
     - דוגמה (מפתח 3): הצפינו את המילה 'סוד'. (ס->צ, ו->ט, ד->ז. תוצאה: **צטז**).
   - **תרגול פענוח (פנימי לחיצוני):** "כדי לפענח, עושים הפוך."
4. **שאלה לדיון:** "כמה מפתחות אפשריים יש לצופן קיסר?" (תשובה: 21. כי 22 מחזיר אותנו להתחלה).

חלק 5: פיצוח קיסר – חיפוש ממצה (15 דקות)

מטרה: הבנת המושג "חיפוש ממצה" (Brute Force) והתנסות בפיצוח צופן ללא מפתח.

1. **הצגת הבעיה:** "מה אם קיבלנו הודעה מוצפנת בצופן קיסר, אבל המפתח אבד?"
2. **חיפוש ממצה (Brute Force):** "כמו במנעול קומבינציה, אם אנחנו לא יודעים את הקוד, ננסה את כל הצירופים האפשריים (בסוף המנעול ייפתח). לשיטה הזו קוראים **חיפוש ממצה**."
3. **יישום:** "בצופן קיסר זה קל! יש רק 21 מפתחות. אפשר לנסות את כולם די מהר!"
4. **פעילות אתגרית – פיצוח הצופן:**
   - כתבו על הלוח הודעה מוצפנת.
   - הנחיה: "השתמשו בדסקיות. נסו לסובב צעד אחד (מפתח 1) ונסו לפענוח ולקרוא. לא הגיוני? נסו עוד צעד (מפתח 2), וכן הלאה."

חלק 6: צופן החלפה הכללי (15 דקות)

מטרה: הכרת צופן החלפה – הצופן הכי מפורסם בעולם.

1. **המעבר מצופן קיסר:** "ראינו שצופן קיסר קל לפיצוח כי יש לו רק 21 מפתחות. אבל מה אם היינו רוצים צופן חזק יותר?"
2. **הסבר צופן החלפה כללי (Substitution Cipher):** "במקום רק להזיז את האלף-בית בסדר קבוע, אפשר להחליט שכל אות תוחלף באות אחרת לגמרי, בלי שום היגיון." (הדגימו על הלוח: א -> ח, ב -> ק, ג -> י...).
3. **עוצמת הצופן:** "כמה מפתחות אפשריים יש לצופן כזה? המון! המספר הוא בערך 1 עם 21 אפסים אחריו (1,000,000,000,000,000,000,000)."
4. **המסקנה:** "אי אפשר להשתמש ב'חיפוש ממצה' כאן. זה ייקח יותר מדי זמן, אפילו למחשב הכי חזק בעולם."
5. **צרו יחד טבלת החלפה, הצפינו ופענחו הודעות.**
6. **שאלה לדיון:** האם בכל זאת יש משהו שיכול לעזור לנו לפענח הודעות בלי לדעת את המפתח?

חלק 7: סיכום השיעור (5 דקות)

1. **חזרה קצרה (חידון קצר):**
   - "מה ההבדל בין סקייטל לקיסר?" (סקייטל מבלבל סדר, קיסר מחליף אותיות).
   - "מה זה חיפוש ממצה? מתי יעיל להשתמש בו?"
   - "איזה צופן הכי קל לפיצוח למדנו היום?"
2. **סיכום.**