

המפצחים: מכונת האניגמה

ליאור ויצהנדלר

מסענו בעולם הקריפטוגרפיה מוביל אותנו למכונה המפורסמת מכול, שפיצוחה הוביל לפיתוח המחשב האלקטרוני הראשון. סודות ההצפנה: כתבה חמישית בסדרה

זוהי הכתבה החמישית בסדרת כתבות העוסקות בצפנים, אך היא עומדת בזכות עצמה.

הפרקים הקודמים: **צופן קיסר, ניתוח תדירויות, צופן ויז'נר, שיטת קסיסקי.**

בסדרת כתבות זו, העוסקת בשיטות הצפנה ופיצוח צפנים, דנו עד כה בצפנים ופיצוחים שנעשו באמצעות דף ועט – או קלף ונוצה. כעת נדלג לשנת 1918, אז מהנדס החשמל הגרמני ארתור שרביוס (Scherbius) המציא את מכונת האניגמה, שהייתה מכשיר ההצפנה החשמלי הראשון. שרביוס שיווק אותה בתחילה לבנקים ולמוסדות אחרים שהיו זקוקים לתקשורת מאובטחת. בתחילת שנות ה-30 אימץ אותה לצרכיו גם הצבא הגרמני.

בשנות המלחמה שימשה המכונה להעברת מאות ואף אלפי הודעות חסויות ביממה בשירות הממשלה הנאצית וסוכנויות הביון והצבא של הרייך השלישי. בתוך כך נוספו לה שכלולים חדשים. בכתבה נתמקד באופן פעולתה של המכונה, אך סיפור פיצוחה הוא מרתק לא פחות. פרק אחד וחשוב בו שייך למתמטיקאי הבריטי ומפצח הצפנים **אלן טיורינג**, שתכנן את מכונת החישוב שממנה התפתח בהמשך המחשב האלקטרוני.



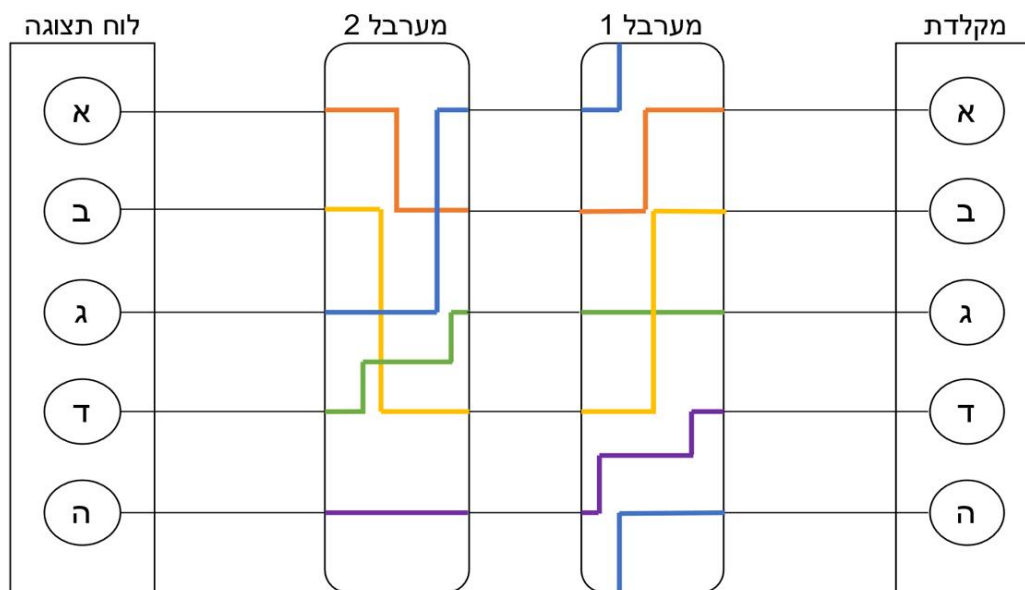
מכונת אניגמה שהייתה בשימוש הצי הגרמני במלחמת העולם השנייה | Cordelia
Molloy, Science Photo Library

אופן הפעולה

מכונת האניגמה נראית כמעט כמו מכונת כתיבה רגילה, פרט לכך שכאשר לוחצים על אות מסוימת נדלקת בלוח התצוגה האות שמחליפה אותה בקוד המוצפן. המכונה כללה כמה מרכיבים שהשתלבו יחד כדי להוסיף מורכבות להצפנה.

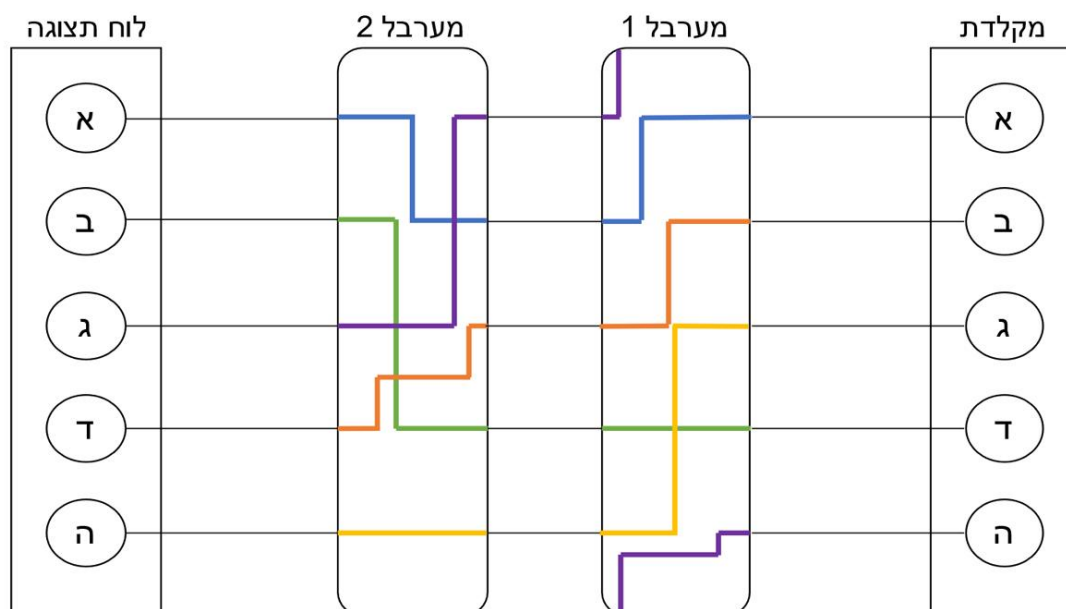
1. המערבלים

כל מערבבל במכונת האניגמה היה טבעת בעלת חיווט חשמלי פנימי שתפקידו לחבר בין אותיות שונות, כמו צופן החלפה פשוט. הייחוד הוא בכך שבכל פעם שלוחצים על אות במקלדת המערבלים מסתובבים בפסיעות מוגדרות ועל ידי כך משנים את אופן הצפנת האות הבאה.



דוגמה למכונה של חמש אותיות ושני מערבלים: המצב ההתחלתי | איור: ליאור ויצהנדלר

אפשר להמשיל את אופן תזוזת המערבלים למנגנון של שעון. בכל פעם שמוקלדת אות, מערבל 1 מסתובב פסיעה אחת; כשהוא מסיים סיבוב שלם, שבאיור למעלה אורכו הוא חמש פסיעות (הקלדות), מערבל 2 מצטרף אליו וזו גם הוא פסיעה אחת. אם נקליד על אות מסוימת במכונה המאירת למעלה, מצב המערבלים ישתנה לסידור המתואר למטה.

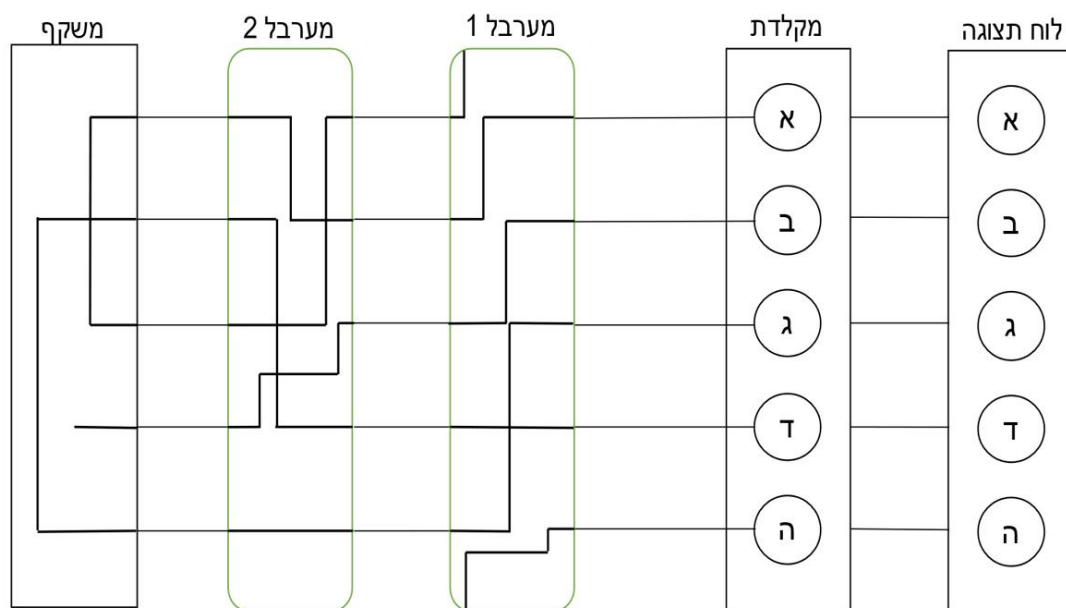


מכונה אחרי הקלדת האות הראשונה | איור: ליאור ויצהנדלר אותה

כל מערבול אפשר לסובב למצב התחלתי מסוים המיוצג על ידי האות המתאימה לו. מספר המצבים האפשרי זהה למספר האותיות במכונה, כלומר חמישה במכונה הפשוטה מאוד שבאיור או 26 במכונה המבוססת על האלפבית הלטיני. למשל, מצב התחלתי אפשרי של המערבלים במכונה שלנו יכול להיות "ב'-ה'", או למשל R-C-G במכונת אניגמה גרמנית. אמיתית עם שלושה מערבלים. כמורכבות נוספת, יש מערבלים עם חיוטים פנימיים שונים. לכן גם סדר המערבלים במכונה משמעותי, וחיוני שהמצפין והמפענח ירכיבו אותם במכונה באותו סדר בדיוק.

2. המשקף

המשקף הוא רכיב נוסף שנמצא מייד אחרי המערבלים. אחרי שהאות החשמלי עובר דרך המערבלים הוא מגיע למשקף, שמחזיר אותו למערבלים עם הזחה נוספת. במכונה המקורית, להבדיל מהאיור הבא, אות לא יכלה להשתקף מחדש לעצמה. בדיעבד זה היה פגם עיצובי במכונה, שאפשר למפצחי הצפנים הפולנים לפרוץ את ההצפנה שלה.

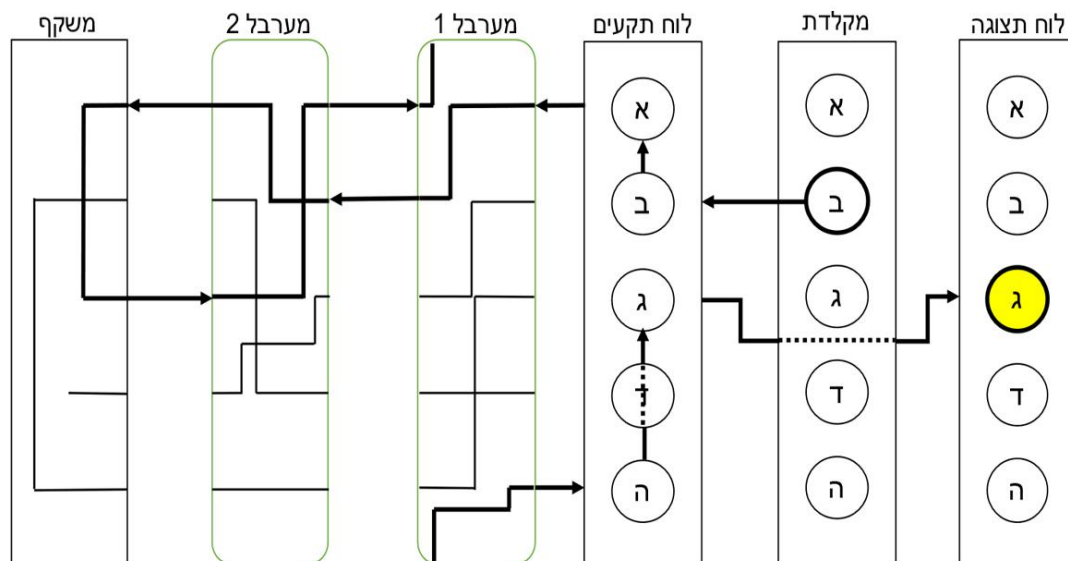


מנגנון האניגמה עם המשקף | איור: ליאור ויצהנדלר

3. לוח התקעים

לוח התקעים הוא מרכיב נוסף במכונה שמאפשר להחליף בין זוגות של אותיות. פעולת ההחלפה נעשית מייד אחרי ההקלדה ולפני המעבר במערבלים, ופעם נוספת לפני הצגת אות

בלוח התצוגה. ההחלפה הזאת היא הדדית, כלומר אם א' מחליפה את ב' אז גם ב' מחליפה את א'.



דוגמה למעבר האות החשמלי בסידור מסוים (קונפיגורציה) של רכיבי המכונה. בלחיצה על האות ב' האות החשמלי מגיע ללוח התקעים ומוחלף באות א', לאחר מכן הוא עובר דרך המערבלים, המשקף, חוזר למערבלים, עובר החלפה נוספת בלוח התקעים ולבסוף נדלקת האות ג' בלוח התצוגה | איור: ליאור ויצהנדלר.

סיבוכיות

הצבא הגרמני השתמש במכונה עם חמישה מערבלים שונים שאותם יכלו להכניס לכל אחד משלושה חרירי מערבלים. כמו כן בלוח התקעים היה אפשר לחבר בין עשרה צמדי אותיות שונים. מספר הסידורים האפשריים (קונפיגורציות) הוא בסביבות 10^{20} סידורים שונים של האלפבית! תארו לעצמכם איזו משימה אדירה ולא מעשית הייתה לנסות את כל הסידורים האפשריים כדי לקרוא את ההודעה. פיצוח הקוד התאפשר בסופו של דבר רק בזכות כמה חולשות במכונה ובשימוש האנושי בה, שמפצחי הצפנים נאחזו בהם.

פיצוח האניגמה

הראשון שפיצח את ההצפנה של מכונת האניגמה, בגלגולה המוקדם, היה המתמטיקאי הפולני מריאן רייבסקי (Rejebski), שעבד במטה ההצפנה של צבא פולין. לידי הפולנים נפלה מכונת אניגמה גרמנית, ומלאכת הפיצוח שלה הוטלה על רייבסקי.

הגרמנים השתמשו במכונה כך: כל חודש חולקו למשתמשי האניגמה הקונפיגורציות היומיות (הסידורים האפשריים או המפתחות) לכל אותו החודש. המפתח היומי לא שימש לשליחת ההודעות אלא לצורך שליחת "מפתח הודעה".

- ראשית השולח כייל את המכונה לפי המפתח היומי.
- לאחר מכן הוא החליט על מצב התחלתי חדש עבור המערבלים, למשל TGN, הקליד אותו פעמיים רצוף (TGNTGN) ושלח את הרצף שקיבל לנמען ההודעה.
- הנמען פענח את ההודעה לפי המפתח היומי וקיבל את מפתח ההודעה.
- בסופו של התהליך התקשורת ביניהם התבצעה באמצעות מפתח ההודעה. שניהם כיילו את המכונות שלהם לפי המפתח החדש ורק אז נשלחה ההודעה האמיתית.

למה הגרמנים עשו את זה? ככל שהטקסט ארוך יותר, קל יותר למפצח הצפנים **לזהות את המפתח**. בנוהל הזה כל מפתח הודעה משמש לשליחת הודעה אחת בלבד, במקום שכל ההודעות מאותו יום יוצפנו על ידי אותו מפתח יומי וכך יקלו מאוד על המפענחים. את המפתח החלופי שלחו כאמור פעמיים, כדי לפצות על טעויות אנוש ובעיות תקשורת – וזו בדיוק הייתה נקודת התורפה שרייבסקי חיפש.

הוא התחיל בניתוח מפתחות ההודעה עבור הודעות מוצפנות שיורטו ביום מסוים. נניח שעבור שלוש הודעות שכאלה הוא קיבל:

6	5	4	3	2	1	
E	G	B	N	O	T	הודעה 1
Z	X	K	C	P	Q	הודעה 2
R	W	S	J	M	Y	הודעה 3

לפי הנוהל שתיארנו, כיוון שהרצף נשלח פעמיים, האות הראשונה והרביעית (זוג 1) נובעות מהקלדת אותה אות. אותו דבר נכון גם לאות השנייה והחמישית (זוג 2) והשלישית והשישית (זוג 3). אם כן, לפי ההודעה הראשונה האותיות T, B, קשורות. רייבסקי אסף מאות הודעות שכאלה ביום ועבור כל זוג הוא הרכיב טבלה המתארת את הקשרים בין האותיות. לדוגמה עבור זוג 1 תיתכן הטבלה:

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

מהטבלה הזאת אפשר להרכיב שרשראות שמתארות קשרים בין אותיות, לדוגמה, C קשורה ל-G, שקשורה ל-X, שקשורה ל-R, שקשורה ל-P, שקשורה ל-H, שחוזרת מחדש ל-C.

8 חוליות	$A \rightarrow Y \rightarrow S \rightarrow W \rightarrow N \rightarrow E \rightarrow L \rightarrow Z \rightarrow A$
12 חוליות	$B \rightarrow F \rightarrow V \rightarrow O \rightarrow Q \rightarrow K \rightarrow D \rightarrow U \rightarrow M \rightarrow I \rightarrow J \rightarrow T \rightarrow B$
6 חוליות	$C \rightarrow G \rightarrow X \rightarrow R \rightarrow P \rightarrow H \rightarrow C$

רייבסקי הסיק שני דברים חשובים: הראשון, אורך השרשראות האלה הוא טביעת אצבע ייחודית של כל סידור של המערבלים. הדבר השני הוא שלוח התקעים לא ישפיע על אורך השרשראות. נסו להחליף בין זוג אותיות ותגלו שזה כך.

כלומר אורך השרשראות נובע אך ורק מכיול המערבלים, וכיוון שבשלב ההוא היו במכונה רק שלושה מערבליים, מספר האפשרויות שצריך לבדוק מצטמצם ל-105,456. עבור כל אפשרות כזאת בדקו רייבסקי וצוותו מה יהיו אורכי השרשראות עבור שלושת הזוגות והרכיבו מאגר נתונים. המשימה הזאת נמשכה שנה שלמה, אך אחריה כל מה שרייבסקי היה צריך לעשות כדי לזהות את המפתח היומי היה להרכיב טבלה, לנתח את אורך השרשראות ולחפש במאגר את הכיול המתאים.

בהמשך, אחרי שהגרמנים סיבכו את המכונה עוד קצת, רייבסקי תכנן ובנה את מכונות ה"בומב" (Bombe), שחיפשו בעצמן את הכיול המתאים במאגר הנתונים. לאחר מכן נותר להקליד הודעה מוצפנת ולהסיק את הסידור של לוח התקעים על ידי השלמת מילים.



עמד בראש צוות מפענחים בריטיים שהצליח לקרוא את ההודעות המוצפנות של הגרמנים. פסל בדמותו של אלן טיורינג, מוצב בבלצ'לי פארק | Lenscap Photography, Shutterstock

מבצע הפענוח של בלצ'לי פארק ואלן טיורינג

אולם הגרמנים לא טמנו את ידם בצלחת והוסיפו בהדרגה למכונות האניגמה החדשות עוד מערבליים ועוד כבלי חיבור ללוח התקעים. לפולנים פשוט חסרו האמצעים הדרושים לבדיקת מספר כה רב של כיוולי מערבליים. כאן הבריטים תפסו את המושכות. במשך תקופה מסוימת הם המשיכו לפענח הודעות לפי הטכניקה הפולנית, ביחידת מפענחי הצפנים שפעלה בבלצ'לי פארק באנגליה. אך המכונות נהיו יותר ויותר מסובכות, וצוות המפענחים שבראשו עמד אלן טיורינג הסתייע בקיצורי דרך נוספים כדי להמשיך לקרוא את ההודעות המוצפנות.

בהמשך פיתח טיורינג, בין השאר בהשראת מכונת ה"בומב" של רייבסקי, מכונה משוכללת יותר שיכלה להתמודד עם מציאת הכיול היומי. שיטת הפיצוח החדשה כבר לא השתמשה בזיהוי שרשראות מפתחות ההודעה, אך גם היא נעזרה בחיפוש אחרי חזרות שקיימות בטקסט המוצפן. פיתוח המכונה חייב שורה של פריצות דרך בתיאוריה של מדעי המחשב,

ואלה תרמו רבות לטיורינג ועמיתיו באנגליה ובארצות הברית בפיתוח המחשבים
האלקטרוניים הראשונים אחרי המלחמה.

**באתר מוזיאון המדע בירושלים מצוי סימולטור של האניגמה. מצפין
ההודעה השתמש במערבלים V, IV, II, שמצבם התחילי הוא R, K, V
בהתאמה. כמו כן חובר זוג האותיות A-B. פענחו את ההודעה הבאה:
LMLA HDCTJVGS PTIWPK**

מקור הכתבה

<https://davidson.weizmann.ac.il/online/askexpert/%D7%94%D7%9E%D7%A4%D7%A6%D7%97%D7%99%D7%9D-%D7%9E%D7%9B%D7%95%D7%A0%D7%AA-%D7%94%D7%90%D7%A0%D7%99%D7%92%D7%9E%D7%94#>