

## צופן האניגמה ופענוחו מנחם לדור

אניגמה הוא כינויה של מכונת ההצפנה ששימשה את הדרגים הגבוהים של הצבא הגרמני בזמן מלחמת העולם השנייה. במאמר זה נספר קצת על המכונה ועל תהליך שבירת הצופן.

הצפנה (קריפטוגרפיה בלע"ז) היא תהליך בו שולח המסר מחליף את הטקסט שברצונו לשלוח באמצעות תהליך הידוע למקבל המסר. המטרה היא שגם אם גורם שלישי כלשהו יצליח לקלוט את הטקסט בזמן העברתו (בדרך כלל האלחוטית) הוא לא יוכל להבין את תוכן השדר. דוגמה פשוטה: בעבר, השתמשו בנוסחה שתמציתה החלפת כל אות באלפבית באות השלישית הבאה אחריה. בשיטת הצפנה זו המילה "בולאות" תהפוך להיות "הטסדטג".



נושא פענוח הצפנים הפך אקוטי מאז החלו בתשדורות אלקטרוניות

שיטת ההצפנה שתוארה לעיל הינה קלה לפיענוח על ידי ניתוח של תדירות ההופעה של כל אות בשפה. אם נניח ש-'ו' היא האות השכיחה ביותר בשפה העברית, הרי שכתוצאה מכך תהיה 'ט' האות השכיחה ביותר בטקסט ששלחנו. עם קצת סטטיסטיקה והכרת השפה, נוכל מהר מאוד לחזור מ"הטסדטג" ל"בולאות". מכאן, שהמשימה העיקרית של מי שרוצה לבנות מכונת הצפנה חכמה הוא שבמסר המוצפן תופענה כל אותיות האלפבית בתדירות פחות או יותר שווה. והמשימה השנייה נוגעת לזמן הפענוח של המסר: שמצד אחד מכונת הצפנה חכמה תאפשר לנמען של השדר

לפענח אותו במהרה (לאור חשיבות השדר). מצד שני המטרה היא שלאויב הקולט את התשדורת, ייקח כמה שיותר זמן לפענח את השדר – אם בכלל. אם ייקח לאויב שנה שלמה כדי לפענח את השדר הרי שכלל הנראה הוא כבר יהיה חסר משמעות מבחינה אופרטיבית (גדוד הטנקים כבר תקף מזמן או הצוללת כבר שינתה את מיקומה).



מכונת אנגימה עם ארבעה רוטורים על גבי "הבול שלי".

כל עוד תשדורות הועברו באופן פיסי, פענוח ההצפנה נעשה רק על ידי תפיסתו של השליח וקריאת השדר. הנושא קיבל תנופה באמצע המאה ה-19 עם התפתחות רשת הטלגרף, ובעיקר בתחילת המאה ה-20 (ומלחמת העולם הראשונה) עם כניסת הרדיו לשימוש ומעבר הצבאות לתקשורת אלחוטית.

העיקרון של מכונת האניגמה פותח על ידי מהנדס חשמל גרמני בשם **ארתור שרביוס** במהלך שנות ה-20 של המאה העשרים. העיקרון מתבסס על בנית גלגלי אותיות (רוטורים), שליד כל אות ישנו פין, המופנה לצד ימין של הטבעת או לשמאלה. ניתן לחבר חשמלית בין הפינים של גלגל א' לאלו של גלגל ב' ולאלו של גלגל ג'. שלושה רוטורים כאלו (ולעיתים יותר) הוכנסו לתוך המכונה. למכונה הייתה מקלדת, כמו של מכונת כתיבה. הקשה על אות

מסוימת העביר זרם חשמלי דרך שלושת הרוטורים אל יחידת קצה שהחזירה את הפולס החשמלי דרך שלושת הרוטורים בכיוון ההפוך. בחלונית קטנה הופיעה האות המוצפנת, וכך הוצפן שדר שלם שהועבר אחר כך אלחוטית בקוד מורס. לאחר הצפנה של כל אות, נע קדימה כל גלגל במספר משתנה של מקומות. אף כי רוב המכונות הכילו שלושה גלגלים כאלו, לכל מכונה היו צמודים מספר גלגלים, ומפעם לפעם היו מחליפים ביניהם. בצורתה הפשוטת ביותר סיפקה המכונה כ-107,000 פרומוטציות (אפשרויות) שונות ועם הזמן נוספו למכונה תכונות שהגדילו משמעותית את מספר הקומבינציות האפשריות, עד כ-150 טריליון  $(150 \times 10^{12})$ . הפענוח נעשה בדרך זהה – הקלדת האות המוצפנת הציגה את האות המקורית, ומכאן קלות הפעלתה. המעוניינים בפרטים נוספים מופנים לערך "אניגמה" בוויקיפדיה, המכסה את הנושא היטב וכתוב בצורה בהירה.



לאנגימה הייתה מקלדת כשל מכונת כתיבה

מובן כי "שבירה" של צופן כזה אינו יכולה להיעשות על ידי בני אדם עם "נייר ועפרון". הרכב הגלגלים בו נעשה שימוש באותו יום, ונקודת ההתחלה של כל גלגל היו נקודות המפתח לתהליך הפענוח. הראשון שהבין היטב את מבנה המכונה ודרך פעולתה



(וכנראה שהיה לו עותק מוקדם שלה) היה מתימטיקאי פולני בשם **מריאן רייבסקי**. אולם הכרה 'תיאורטית' של המכונה (ונציין שהיא עברה שינויי מבנה שלא כולם נודעו לרייבסקי) לא הספיקה כדי לקרוא שדרים שהוצפנו באמצעותה: כפי שצינו לעיל, תצורת הרוטורים ונקודת ההתחלה שלהם היו קריטיים. אבל כדי שגם הצד המקבל את השדר ידע לפענח אותו, גם הוא היה צריך לדעת את הנתונים הללו. ולכן, נקבע נוהל, כי בתחילת השדר יצוינו האותיות לפיהן הוחל בהצפנה.

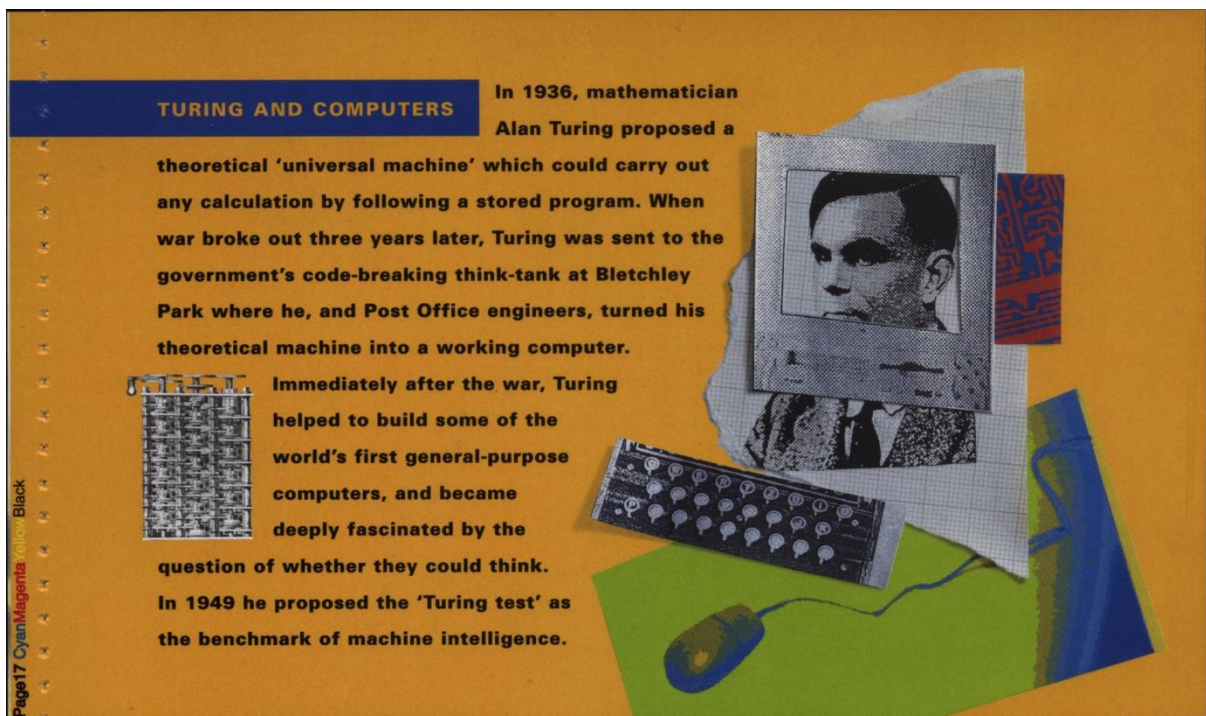


מריאן רייבסקי הבין את העקרון המתמטי של פעולת האניגמה. דבר בוליס.

רייבסקי נעזר במידע נוסף שקיבל מהמודיעין הצרפתי ומצא שיטה לפיה, בהינתן מספר גדול של שדרים שנשלחו באותו יום, ניתן לקבוע את אותיות ההתחלה. ועדיין, גם עם הידע הזה, המלאכה הייתה ארוכה ומייגעת כדי לפענח את השדר במהירות מספקת כך שלפענוח תהיה לו משמעות אופרטיבית בשדות הקרב. עם התקדרות ענני המלחמה, שיתף רייבסקי את שירותי המודיעין הצרפתיים והאנגליים בידיעותיו, עם תחילת המלחמה הוברחו רייבסקי ואנשי צוותו מפולין, דרך רומניה לדרום צרפת.

לפענוח צופן האניגמה הייתה חשיבות עליונה – היא הייתה בשימוש בדרגי הצבא הגבוהים ביותר וכן על ידי צי הצוללות הגרמניות. ככל ש"המלחמה על האוקיאנוס האטלנטי" התקדמה, והצוללות הגרמניות טבחו בשירות האספקה מארצות הברית לבריטניה, הלכה וגדלה החשיבות של פענוח האניגמה (ראה מאמרו של **ג'ידי רענן** בנושאונט מספר 9 ו-10). האנגלים השקיעו רבות בהשגת מידע על המכונה (אפילו על ידי תפיסת צוללת או שתיים והטבעתה מיד אחר כך). אולם העבודה הסיזיפית של פענוח השדרים היומיים המשיכה להתקיים.

וכאן נכנס לתמונה אחד מגדולי המתימטיקאים בכל הזמנים – אלן טיורינג. הוא נולד בלונדון בקיץ 1912. ב-1931 החל את לימודי המתמטיקה בקיימברידג' ומהר מאוד בלט בכישרונו האדיר. הוא תקף את הבעיות המתמאטיות הסבוכות ביותר של התקופה, וב-1936 פרסם מאמר ("On Computable Numbers"), המהווה עד היום את הבסיס של תורת המחשבים, ובו הגדיר את מה שמכונה "מכונת טיורינג". המטרה הייתה ליצור הגדרה מתמטית מדויקת של אלגוריתם או "תהליך מכני". עוצמתו של הרעיון נעוצה בפשטות הקיצונית שלו וקובעת כי מכונת טיורינג, חרף פשטותה, מסוגלת לבצע כל חישוב או אלגוריתם שהוא בר-ביצוע במחשב כלשהו. מבחינה זו, מכונת טיורינג שקולה לכל מחשב, ולכן משמשת עד היום במדעי המחשב כבסיס לחקר יכולותיו ומגבלותיו של מחשב כלשהו.

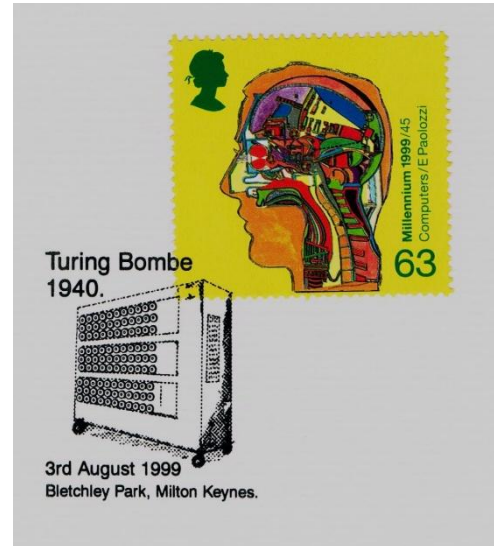


אלן טיורינג ומכונת טיורינג. דפית מתוך קונטרס יוקרה בריטי.

עם פרוץ מלחמת העולם, גויס טיורינג והוצב בפארק בלצ'לי (Bletchley Park), מקום בו פעל בית הספר הממשלתי לקידוד ופענוח. שמו של המקום מעיד, אולי, על מקום אקדמי באופיו, אך למעשה היה זה מרכז פענוח לכל דבר: בצד אחד נכנסו שדרים מוצפנים ובצד השני יצאו שדרים מפוענחים... טיורינג למד את מכונת ההצפנה, הבין את עקרון פעולתה ואת מורכבותה וניגש לממש את התיאוריה שהגדיר. הוא תכנן את הבומב (Bombe) ואחר כך את הקולוסוס – Colossus.

הבומב היתה מכונה אלקטרו-מכנית שאפשרה בדיקה יחסית מהירה – מכנית במקום אנושית – של חלופות שונות על מנת לזהות את נקודות ההתחלה היומיות. המודלים הראשונים של הבומב נבנו כבר ב-1939 ו-1940. הקולוסוס הייתה מכונה מורכבת הרבה יותר: בניית הדגם הראשון הסתיימה רק בסוף 1943, והוא נכנס לשירות כחודשיים מאוחר יותר. זהו בעצם מחשב ייעודי, שסרק את מיליוני הקומבינציות האפשריות, כדי להגיע אל התצורה היומית. לאחר שפוענח הצירוף היומי כבר הייתה





מכונות הפיענוח: הבומב (מימין) והקולוסוס (משמאל).

הדרך קלה לקרוא שדרים בגרמנית. זה נראה לנו פשוט, אך הדבר היה מורכב, מסובך, מיגע ולקח הרבה מאוד זמן. כאמור, הקולוסוס היה מחשב יעודי (ובמהלך מלחמת העולם נבנו עשרה כאלו), שאיכלס חדר שלם והורכב מ-1500 נורות חשמליות. מאחר ובדואר עסקי, מעניין לציין כי שתי המכונות הללו – הבומב והקולוסוס – נבנו במעבדות המחקר של משרד הדואר והטלפוניה הבריטי, על בסיס פיתוחים שנעשו עבור מרכזיות טלפוניה.



שימוש בכתובת עלומה על גבי מכתב המיועד למעשה ליחידה הסודית בפארק בלצ'לי



פרס טיורינג – הנובל של מדעי המחשב

הפעילות בפארק בלצ'לי הייתה סודית ביותר. בין השאר, קבלת הדואר עבור המוצבים בבסיס לא נעשתה באופן ישיר מטעמי ביטחון שדה, אלא על ידי שימוש בכתובת עלומה בלונדון. המכתב הנראה לעיל נשלח מציריך אל "מועדון איגוד דוברי אנגלית" בלונדון. במועדון – ארגון קצינים שרבים כמותו פעלו

בבירה האנגלית – שונתה הכתובת לתיבת דואר 111 בבלצ'לי. לאחר מלחמת העולם החליטו הבריטים להמשיך ולשמור על הסוד הכמוס במשך למעלה משלושים שנים נוספות. יש הסבורים, כי זאת אחת הסיבות שתעשיית המחשבים הבריטית לא הצליחה להתרומם מיד לאחר המלחמה (כפי שקרה בארצות הברית). כיום ניתן לבקר באתר, הנמצא כ-90 קילומטר מצפון ללונדון – טיול שאני ממליץ עליו בחום.

הסודיות היתרה לא הייתה סודיות מיותרת: רבים – **וצ'רצ'יל** ביניהם – חשבו שזו הייתה היחידה הצבאית החשובה ביותר של כל כוחות הברית במלחמת העולם השנייה. פיצוח קוד האנגימה השפיע באופן קריטי על תנועת השיירות באוקיאנוס האטלנטי ועל יכולתה של בריטניה לשרוד את המצור.

אלן טיורינג היה מתימטיקאי כל כך חשוב שהוכרז על שמו 'פרס טיורינג' המזוהה כיום כ'נובל של מדעי המחשב'. חלוקת הפרס החלה בשנת 1968, וכאן יש קצת מקום לגאווה: פרופ' **מיכאל רבין** (האוניברסיטה העברית, 1976), פרופ' **אמיר פנואלי** (מכון ויצמן, 1996), פרופ' **עדי שמיר** (מכון ויצמן, 2002), פרופ' **יהודה פרל** (UCLA, ישראלי בוגר הטכניון, 2011) ופרופ' **שפי גולדווסר** (מכון ויצמן/MIT, 2012) הם בין זוכי הפרס. ישראל ניצבת במקום החמישי במספר הזוכים, עם חמישה זוכים, אחרי ארצות הברית (41) ובריטניה (6).

מנחם לדור היה יושב הראש הראשון של איל"ת, וכיום הוא מכהן כסגן יושב הראש של האגודה. בשנים האחרונות הוא אוסף ומציג את "תולדות המידע והעברתו". בין נושאי האיסוף שלו נכללים גם ה"מחשב" ו"ריגול". מנחם הוא שופט תימאטי בינלאומי. כתובתו: ladorm@gmail.com