



אב תשפ"ג
יולי 2023

אניגמה

מאת: אל"ם בדימוס דניאל רוזן

מבוא

זהו סיפורה של ה'אניגמה' (Enigma), מכונה אלקטרומכנית להצפנת טקסט בשיטה 'אקראית' לכאורה' ששימשה את כוחות הביטחון הגרמנים במלחמת העולם השנייה. הבריטים הצליחו לפענח את הצופן שהמכונה ייצרה – ופרשה זו, מהסודות הכמוסים של המלחמה, נשמרה בקנאות שנים רבות. זה סיפור מרתק, עליו נכתבו ספרים, הומחזו מחזות ונערכו סרטים רבים.

ההיסטוריונים מעריכים שהמידע שהופק מפענוח הצפנים הגרמניים תרם מהותית לניצחון בנות הברית על גרמניה הנאצית, וקיצר את המלחמה בשנתיים לפחות.

מאמר זה מתאר את מכונת ה'אניגמה', מציג את ציר הזמן והאירועים המרכזיים בתהליכי פענוחה, ומפנה לביבליוגרפיה בנושא.

עקרון הפעולה של 'אניגמה'

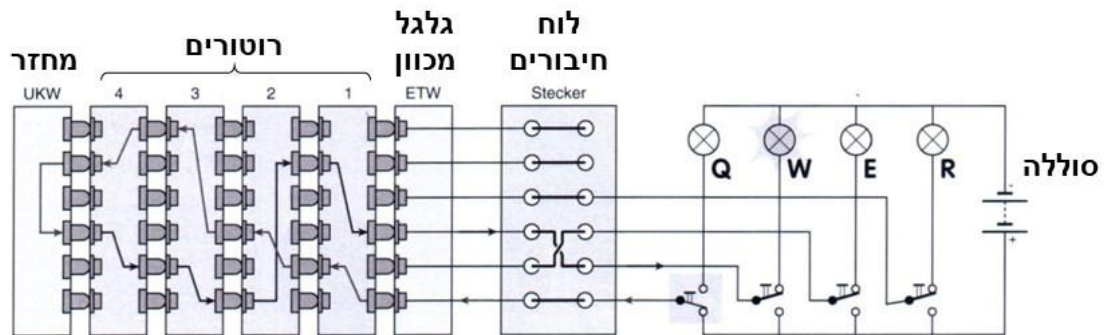
ההצפנה והפענוח במכונת 'אניגמה' מבוססים על לוח מקשים ולוח נוריות. הקשת אות גלויה גורמת להארת נורית המסמנת את האות המוצפנת. הקשת אות מוצפנת גורמת להארת נורית המסמנת את האות הגלויה.

המעגל החשמלי בין המקש לנורית נסגר דרך מספר רוטורים (Rotors) המורכבים על ציר משותף. הרוטור הימני מתקדם צעד אחד בכל לחיצה על מקש אות, וכאשר הפסיעה מגיעה לחרץ (Notch) ברוטור, הרוטור לשמאלו מתקדם צעד אחד או שני צעדים, וכך משתנה המצב היחסי בין הרוטורים אחרי הקשת כל אות. הרוטור עצמו מורכב משתי דיסקיות עגולות, בכל אחת 26 מגעים, עם תיול חשמלי בין שתייהן. בדגם M4, הדגם המשוכלל של ה'אניגמה' ששירת את הצי הגרמני משנת 1942, היו חמישה רוטורים שונים, שמוספרו באותיות רומיות I עד V, מהם בחרו שלושה לכל הרכב רוטורים, ועוד שני רוטורים שנועדו לרוטור הרביעי (הרוטור השמאלי) שכונו β (Beta) או γ (Gamma), והיו 'דקים' בהשוואה ליתר הרוטורים (הם כונו Zusatzwalze או Griechenwalze), ואחד מהם שימש בכל הרכב.¹ התיול בין דיסקיות כל רוטור, 26 חיבורים פנימיים, שונה לפי מספר הרוטור. משני צידי הרוטורים המסתובבים יש דיסקיות קבועות: הראשונה (מימין) מכונה ETW (Eintrittswalze) או גלגל מכון (Stator), האחרונה (משמאל) מכונה UKW (Umkehrwalze) או מְחַזֵּר (Reflector).² בין המקשים והנוריות לבין מערכת הרוטורים מותקן לוח חיבורים (Steckerbett) עם מגשרים.

¹ הוספת הרוטור הרביעי התאפשרה באמצעות הקטנת המחזור, אך המקום שנותר היה צר, ולא התאים לרוטור רגיל.

² מכונת 'אניגמה' שיוצרו לגורמים שונים בכוחות הביטחון הגרמניים היו עם תיול שונה של הגלגל המכוון ושל המחזור.

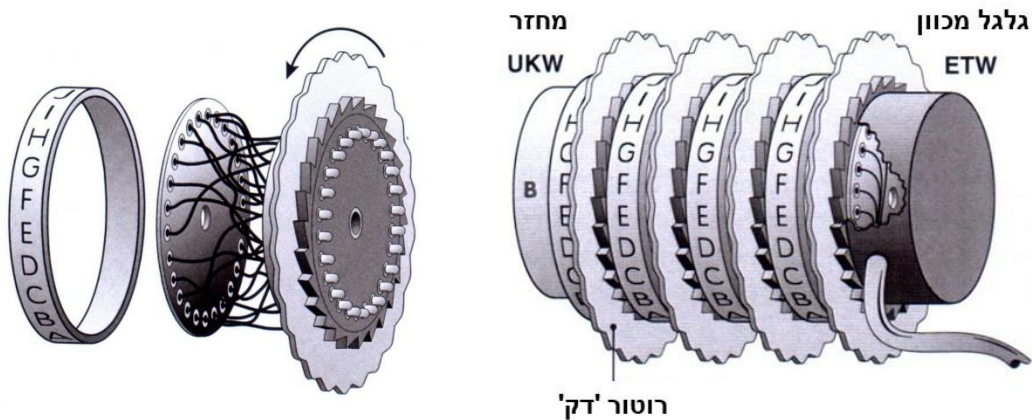
המעגל החשמלי של מכונת 'אניגמה' מתואר באיור מס' 1 ומערכת הרוטורים מתוארת באיור מס' 2.



איור מס' 1: מעגל חשמלי עקרוני של 'אניגמה' דגם M4

בדוגמה: לחיצה על האות Q מפעילה את הנורה W

מקור: Paul Reuvers & Marc Simons, *ENIGMA – E*, Crypto Museum, Netherlands, 2003

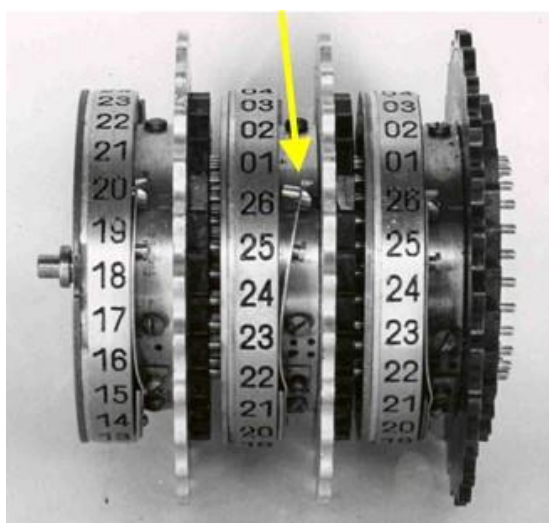


מבנה רוטור

מערכת הרוטורים

איור מס' 2: מערכת הרוטורים של 'אניגמה' דגם M4

מקור: Paul Reuvers & Marc Simons, *ENIGMA – E*, Crypto Museum, Netherlands, 2003



מיקום יחסי של טבעת הרוטור

בדוגמה זו, של 'אניגמה' M3: 20 26 26

הפין קפיצי – מושכים אותו החוצה, ומסובבים את הטבעות עד שהוא מגיע למקום הנדרש

מקור:

National Security Agency, National Cryptologic Museum, 2008.1003.1043

מפתח ההצפנה כולל את בחירת הרוטורים, מיקום יחסי של הטבעת בכל רוטור, וסדר הרכבתם, תצורת הגישורים בלוח החיבורים ומצב התחלתי של הרוטורים.³ הגרמנים נהגו לבחור באופן אקראי את מצב הרוטורים לכל הודעה שהוצפנה, והאותיות הראשונות ששודרו היה מצב הרוטורים של ההודעה, כשהם מוצפנים במצב ההתחלתי של הרוטורים, והם שודרו פעמיים (כדי להתמודד עם טעויות בקליטה).

עד שנת 1936 הוחלפו מפתחות אחת לשלושה חודשים. לאחר מכן הוחלפו מפתחות אחת לחודש, ובהמשך מדי יום, ולקראת סוף המלחמה: פעמיים ביום ואף כל שעה.⁴



מכונת אניגמה M4

מקור: National Security Agency, National Cryptologic Museum, 210211-D-IM742-2001

כמות הצירופים האפשריים

בהכירנו את המכונה, ניתן לחשב את כמות הצירופים האפשריים להצפנת כל אות, שהיא מכפלת הצירופים של חלקי המכונה השונים.

³ בדרך כלל היו 10 מגשרים, וקטע זה של המפתח כלל 10 צמדי אותיות – מאין ולאן יש לחבר מגשר.

⁴ Tom Perera & Dan Perera, *Inside Enigma*, Second Edition, Radio Society of Great Britain, 2019, p. 95

המרכיב הראשון הוא כמות הצירופים של המגשרים בלוח החיבורים : בלוח החיבורים 26 שקעים, בהם ניתן להתקין מ"ס עד 13 מגשרים. כמות המגשרים מסומנת ב- p . כמות הצירופים בכמות מגשרים p היא :

$$\frac{26!}{(26 - 2 \times p)! \times p! \times 2^p}$$

ובהתאם לכמות המגשרים, נקבל את התוצאה הבאה :

כמות צירופים	כמות מגשרים p
1	0
325	1
44,850	2
3,453,450	3
164,038,875	4
5,019,589,575	5
100,391,791,500	6
1,305,093,289,500	7
10,767,019,638,375	8
53,835,098,191,875	9
150,738,274,937,250	10
205,552,193,096,250	11
102,776,096,548,125	12
7,905,853,580,625	13

וכמות הצירופים האפשריים הכוללת של המגשרים בלוח החיבורים היא סיכום של כל אלה, דהיינו :

$$\sum_{p=0}^{13} \frac{26!}{(26 - 2 \times p)! \times p! \times 2^p} = 532,985,208,200,576$$

המרכיב השני הוא כמות הצירופים של מערכת הרוטורים. במכונה עם שלושה רוטורים, כמות הצירופים היא :

$$26! \times (26! - 1) \times (26! - 2) = 65,592,937,459,144,468,297,405,473,480,371,753,615,896,841,298,988,710,328,553,805,190,043,271,168,000,000$$

ובמכונה עם ארבעה רוטורים, כאשר לא ניתן להתקין את הרוטור הרביעי במקום אחד משלושת הרוטורים הקודמים, כמות הצירופים היא :

$$26! \times (26! - 1) \times (26! - 2) \times 26! = 24,453,071,587,484,435,966,565,383,350,966,637,647,029,992,367,895,564,609,744,699,959,788,953,452,189,042,702,687,102,042,112,000,000,000,000$$

המרכיב השלישי הוא כמות הצירופים של מיקום הרוטורים ההתחלתי, שהוא :

$$26^4 = 456,976$$

המרכיב הרביעי הוא המיקום היחסי של החריצים, שכן במכונת 'אניגמה' M4 היה חריץ נוסף, שניתן לשנות את מיקומו. לצורך זה יש להתחשב רק ברוטור הראשון והשני, ולכן כמות הצירופים הנוספים היא :

$$26^4 = 456,976$$

המרכיב החמישי הוא כמות הצירופים של המחזור, שיש לו 26 מגעות, אך רק צד בודד. מספר הצירופים האפשריים הוא :

$$\frac{26}{(13! \times 2^{13})} = 7,905,853,580,625$$

מספר הצירופים הכולל הוא מכפלה של כל המרכיבים, והוא 3×10^{14} ל'אניגמה' עם שלושה רוטורים M3, או 2×10^{145} ל'אניגמה' עם ארבעה רוטורים M4.

באופן מעשי, המפענחים התמודדו עם מספר צירופים קטן יותר. הגרמנים נהגו להשתמש ב-10 מגשרים בלבד. תיול הרוטורים היה ידוע, ולכן נשאר לקבוע רק את סדר הנחתם, וגם תיול המחזור היה ידוע. הדבר צמצם את כמות הצירופים לסדר גודל של 1×10^{23} – עדיין מספר גדול מאוד.⁵

בפועל, כמות הרוטורים הייתה במידה רבה אשליה, שכן רוב ההודעות ששודרו היו קצרות, והרוטור השלישי ביצע פסיעה רק אחת לחמש עד שמונה הודעות; גם כמות הצירופים של לוח המגשרים היא אשליה, שכן הוא מוסיף הצפנה בקוד החלפה אלפא-ביתי קבוע, שניתן לפענח בקלות; 'תורת ההפעלה' הגרמנית צמצמה עוד יותר את כמות הצירופים, כך למשל: עד שנת 1936 השתמשו רק בשישה מגשרים, איסור על הכנסת רוטור ספציפי למיקום מסוים במשך יומיים מהיום האחרון בו עשו זאת, הצפינו פעמיים את מצב הרוטורים בתחילת ההודעה (נוהל שבוטל במאי 1940);⁶ והחולשה המרכזית: האות המוצפנת הייתה תמיד שונה מהאות הגלויה, כך שאם היה למפענח רמז (או ניחוש) לאות הגלויה, הוא ידע (או ניחש) לאיזה אות מוצפנת מתורגמת אותה גלויה.

ציר הזמן

תיאור כרונולוגי של התפתחות ה'אניגמה' ואירועי פענוחה משלים את התאור ה'טכני' של המכונה, ומציג תמונה מעניינת על המאמץ לפענוח ה'אניגמה' ועל חשיפתו, שנים רבות לאחר סיום מלחמת העולם השנייה :

שנה	אירוע
1918	• ארתור שרביוס (Arthur Scherbius) רשם פטנט על מנגנון ההצפנה של ה'אניגמה' במשרד הפטנטים הגרמני. • בשנים הבאות נרשמו פטנטים נוספים, על שיפורים שונים במנגנון ההצפנה. • בשנות העשרים (עד שנת 1932) הייתה המכונה זמינה כמוצר מסחרי, אך הפעילות לא זכתה להצלחה עסקית.
1926	• הצבא הגרמני רכש את הפטנטים של שרביוס, ביצע במכונה שינויים, החל להצטייד בה וגיבש נהלי תפעול. • השינויים העיקריים שהצבא הגרמני עשה במכונה היו שינוי תיול הרוטורים והוספת לוח המגשרים.
1928	• רוב התעבורה המוצפנת הצבאית הגרמנית הוצפנה ב'אניגמה'. • השירותים החשאיים הפולנים, שחששו מפלישה גרמנית, החלו לעסוק בפענוח צופן ה'אניגמה'.
1932	• הבריטים החלו להתעניין ב'אניגמה', ללא הצלחה. • הכשלון בשבירת הצופן הביא לכך שהמודיעין הבריטי התבסס על מדל'ית (מודיעין ללא-תכנים), דהיינו: ניתוח תעבורה גרמנית ומיקום מוערך של הגורמים המשדרים.

⁵ Ray Miller, *The Cryptographic Mathematics of Enigma*, Center for Cryptologic History, National Security Agency, 2019

⁶ Olaf Ostwald, *Cryptographic design flaws of early Enigma*, Crypto Museum, 2023

שנה	אירוע
1933	- הפולנים פענחו את ה'אניגמה'. הם הצליחו לפענח את תיול הרוטורים, להבין את מבנה המכונה ולייצר רפליקות ששימשו לפענוח ההודעות. - נהלי התפעול הגרמניים, שמשותף פעולה גרמני העביר למודיעין הצרפתי בסוף שנת 1931, סייעו מאוד, שכן הפענוח הפולני התבסס על 'אינדיקטורים' – הצפנה פעמיים של מצב הרוטורים בתחילת ההודעה (הפולנים התבססו על כך שהאות הרביעית זהה לאות הראשונה, האות החמישית זהה לאות השנייה, והאות השישית זהה לאות השלישית).
1934	היטלר מונה לקנצלר גרמניה בבחירות בינואר 1933, ובשנת 1934 הכריז על עצמו כדיקטטור (Führer).
1938	- הגרמנים השתלטו על אוסטריה וסיפחו אותה לגרמניה (אנשלוס). - הפולנים בנו מכונות אלקטרומכניות לפענוח צופן ה'אניגמה', שנקראו Bomba, שעברו על 17,000 צירופים אפשריים כדי לזהות את מפתח הצופן – המצב ההתחלתי של הרוטורים, שהשתנה בכל הודעה.
1939	- הגרמנים הוסיפו שני רוטורים. הפולנים הצליחו לאתר את תיול הרוטורים, אך לא הייתה להם דרך לקבוע איזה הם שלושת הרוטורים הנמצאים בשימוש, והם הפסיקו לקרוא את ההודעות הגרמניות. - ביולי הזמינו הפולנים את גורמי המודיעין הבריטים והצרפתים, מסרו בידיהם את סוד פענוח צופן ה'אניגמה', ונתנו להם רפליקות של המכונה. - ב־1 בספטמבר פלשו הגרמנים לפולין. המפענחים הפולנים נמלטו לצרפת, שם המשיכו בחשאי את עבודתם. - בריטניה וצרפת הכריזו מלחמה על גרמניה.
1940	- במרכז פענוח הצפנים הבריטי בלצ'לי פארק (Bletchley Park) פעל צוות בראשות אלן טיורינג (Alan Turing) וגורדון וולשמן (Gordon Welchman), שהצליח לפענח את צופן ה'אניגמה', ובאוגוסט העמיד גרסה שלהם של המכונה הפולנית, בשם Bombe, והצליחו לפענח חלק נכבד מהתעבורה הגרמנית.⁷ - המכונה הבריטית לא התבססה רק על ה'אינדיקטורים', אלא גם על מילים ידועות בטקסט (כמו שמות יחידות, שמות מקומות, מונחים צבאיים), שכונו Cribs. - גרמניה פלשה לצרפת ולנורבגיה. - הבריטים לא הצליחו לפענח את ההודעות הצי הגרמני.
1941	- המשחתת הבריטית HMS Bulldog תפסה בחודש מאי את הצוללת הגרמנית U-110 וחילצה ממנה מסמכים סודיים, מכונת 'אניגמה' וספרי מפתחות צופן.⁸ - המידע איפשר לבריטים לפענח את ההודעות הצי הגרמני. - בדצמבר שידרה בטעות צוללת גרמנית הודעה במכונת M4, וכשעמדה על טעותה שידרה את אותה ההודעה במכונה M3. הטעות איפשרה לבריטים לפענח את התיול של הרוטור הרביעי.
1942	- בפברואר עבר הצי הגרמני ממכונת 'אניגמה' M3 למכונת M4. הבריטים הפסיקו לפענח את תעבורת הצי הגרמני. - המשחתת הבריטית HMS Petard הטביעה בחודש אוקטובר את הצוללת הגרמנית U-559. הצוללת טבעה באיטיות וצוות השתלטות בריטי חילץ ממנה בגבורה מכונת 'אניגמה' וספרי מפתחות צופן.⁹ המידע שנאסף איפשר לחדש את פענוח ההודעות הצי הגרמני.

⁷ עבודתו המקורית של אלן טיורינג, בסיווג 'סודי ביותר', בשם Turing's Treatise on the Enigma, זמינה בארכיון הלאומי הבריטי, ראו: <https://www.archives.gov/files/press/press-releases/2015/images/turing-enigma-treatise.pdf>

⁸ הצוללת הגרמנית תקפה שיירה של בנות הברית סמוך לגרנלנד, אותרה בסונאר, נפגעה מפצצות עומק, ועלתה לפני הים. הצוות הגרמני נטש והצוללת הייתה על סף טביעה. רב החובל הגרמני נהרג. רב החובל הבריטי הבחין שהצוללת לא טובעת, ושלח צוות להשתלט עליה. הצוללת נגררה לאיסלנד אך טבעה בדרכה. תפיסת מכונת ה'אניגמה' וספרי הצופן נשמרה כסוד כמס, ונשיא ארה"ב רוזוולט עודכן רק בינואר 1942.

⁹ מטוס סיור ימי בריטי זיהה את הפריסקופ של הצוללת מול חופי מצרים. כוח של חמש משחתות בריטיות רדף אחר הצוללת במשך 16 שעות, פגע בה בפצצות עומק, והיא נאלצה לעלות לפני הים, שם טובעה באש תותחים. הצוות הגרמני נטש אך לא פתח כראוי את פתחי חדירת המים להטבעת הספינה, והצוללת טבעה באיטיות. צוות בריטי, באומץ לב ראוי לציון, חילץ ממנה את מכונה ה'אניגמה' והמסמכים הסודיים טרם טביעתה. שני מלחים בריטים לא הצליחו לצאת מהצוללת הטובעת וירדו עמה למצולות.

שנה	אירוע
1943	במאי השלימו האמריקאים פיתוח מכונת Bombe משלהם, 'חזקה' ומהירה יותר מהמכונה הבריטית.
1944	שיא פעילות מרכז פענוח הצפנים הבריטי בלצ'לי פארק, עם כ-10,000 איש.
1945	היטלר התאבד באפריל. גרמניה נכנעה בספטמבר.
1946	הפעילות בבלצ'לי פארק הסתיימה, אך הסוד נשמר בהוראת ראש הממשלה הבריטי וינסטון צ'רצ'יל. הימים היו ימי 'המלחמה הקרה', והיה חשוב שהסוד לא יגיע לסובייטים.
1967	הפולני Wladyslaw Kozaczuk פרסם ספר (Bitwa o tajemnice – קרב הסודות) המתאר את הפעילות הפולנית בפענוח ה'אניגמה' ושיתוף הפעולה עם הבריטים והצרפתים.
1974	הבריטי Frederick William Winterbotham, שהיה אחראי על הפצת מודיעין שהופק מפענוח ה'אניגמה' ושמירת הסוד, פרסם זיכרונות, בו תיאר את פעילות פענוח הצפנים והשלכותיה.

מפתח 'אניגמה' 649 של חיל האוויר הגרמני
 שים לב: אסור שמפתחות יפלו לידי האויב. השמד מיד בעת סכנה
 (המגשרים במחזר לא היו ב'אניגמה' המקורית, ונוספו בתחילת שנת 1944)
 מקור: Crypto Machine, אתר מרשתת של Jerry Proc, חובב רדיו קנדי באות הקריאה VE3FAB



מפקד הקורפוס הממוכן ה-19, גנרל-אוברסט היינץ גודריאן, צרפת, 1940
 שני קשרים מפעילים מכונת 'אניגמה' M3 וקשר שלישי מפעיל את מכשיר הקשר ברכב הפיקוד,
 תחת עינו הבוחנת של הגנרל

מקור : 2008.1002.1402, National Security Agency, National Cryptologic Museum

לאחר מלחמת העולם השנייה התברר כי פענוח האניגמה היה תלוי בשערה

שיתוף הפעולה ההדוק בין בריטניה לארה"ב בתחום מודיעין אותות ופענוח צפנים במלחמת העולם השנייה התנהל במסגרת סוכנות חשאית שכונתה TICOM (Target Intelligence Committee).¹⁰ לקראת תום המלחמה הפעילה סוכנות זו צוותים מיוחדים שהצטרפו לכוחות הקדמיים של צבאות בנות הברית ושקדו על איתור סודות הצבא הגרמני, מעצר וחקירה של אנשי צבא גרמנים שעסקו בנושא ואיתור מסמכים וציוד. השירות הקריפטולוגי במטה הכללי הגרמני, OKW/Chi, ש'התפורר' לקראת סוף המלחמה וארכיונו נעלם, היה היעד העיקרי של הסוכנות.¹¹ פעילות זו הייתה חשאית ונשמרה בסוד עד שנת 2009, אז פורסמו לציבור מסמכים רבים.¹²

בשנת 2007 שחרר משרד ההגנה האמריקאי מחקר המבוסס על מסמכי TICOM, הדן בשאלה מה ידעו ב' OKW/Chi על חולשות ה'אניגמה'.¹³

הגרמנים חקרו את בטחון האניגמה משנות ה-20, ובשנת 1932 מיסדו את הפעלת ה'אניגמה' עם שלושה זוגות מגשרים.

בשנת 1939, לאחר הפלישה הגרמנית לפולין, התברר לגרמנים ממסמכי שלל כי הפולנים פענחו את האניגמה מספר שנים לפני המלחמה. מחקירת קצינים פולנים שבויים שעסקו בנושא (שידעו שהודעות ה'אניגמה' פוענחו, אך לא ידעו כיצד הדבר נעשה) למדו הגרמנים את הכינוי הפולני החשאי לפעילות – WICHER. הגרמנים זיהו כי בפענוח עסקו מספר מתמטיקאים פולנים צעירים, אך לא הצליחו לאתרם.

מידור חמור, בין המטה הכללי OKW ומפקדת כוחות היבשה OKH, שנקבע בצו שהיטלר הוציא בשנת 1940, גרם לכך שהמסמכים הפולנים שנתפסו לא הועברו ל'OKW/Chi', לו הייתה רק תמונה מוגבלת וחלקית של ההישג הפולני. המידע לא ערער את ביטחון OKW/Chi ב'אניגמה', אך כצעד 'זהירות מונעת' בוצעו שינויים תפעוליים (ביטול ההצפנה הכפולה של מצב הרוטורים בתחילת ההודעה ומעבר משישה לעשרה זוגות מגשרים). מידור זה הביא לכך שלמפקדת הצי הגרמני OKM לא הועבר מידע כלשהו על WICHER.

עם כיבוש צרפת במאי-יוני 1940 נעשה מאמץ מודיעיני לאתר את היכולות הצרפתיות והקשר בין הצרפתים לפולנים ולבריטים, אך מאמץ זה לא הניב תוצאות ממשיות. אחר כיבוש 'צרפת החופשית' של וישי בנובמבר 1942 לא נעשה מאמץ מודיעיני נוסף.

¹⁰ מודיעין אותות (SIGINT – Signals Intelligence) הוא כינוי כולל למודיעין המופק מאמצעי תקשורת ואמצעים אלקטרוניים, הכולל מודיעין תקשורת (COMINT – Communications Intelligence), המודיעין המופק מיידות התקשורת של היריב, ומודיעין אלקטרוני (ELINT – Electronics Intelligence), המודיעין המופק מקרינה אלקטרומגנטית של היריב שאיננה לצרכי תקשורת.

¹¹ Randy Rezabek. *TICOM: The Last Great Secret of World War II*, Intelligence and National Security, 27:4, Routledge, 2012, 513-530

¹² בשנת 2011 שחרר ה-NSA 50 אלף מסמכים, הזמינים בארכיון האמריקאי NARA (National Archives and Records Administration), בהם כ-600 מסמכים של TICOM. מסמכים רבים זמינים באתר האינטרנט של ההיסטוריון Randy Rezabek, בארכיון האינטרנט, ראו <https://archive.org/details/ticom>

¹³ Joseph A. Meyer, Der Fall WICHER: German Knowledge of Polish Success on ENIGMA, NSA Technical Journal, Spring 1975 - Vol. XX, No.2. p. 9, DOCID: 3838699. ראו: <https://media.defense.gov/2021/Jul/02/2002755854/-1/-1/0/DER-FALL-WICHER.PDF>

מפקד חיל הקשר הגרמני הגנרל פֶּלְגִיבֶּל,¹⁴ שהיה ממונה גם על נושא האזנה ופענוח צפנים, הורה בשנת 1943 לחקור שוב את הקצינים הפולנים שהיו מעורבים בפעילות WICHER. החקירות איששו את יכולת הפולנים לפענח הודעות 'אניגמה' עד שנת 1939 (עד אשר הגרמנים הוסיפו למכונה שני רוטורים והגדילו את מספר המגשרים משלושה לשישה), אך לא חשפו את סוד קיומה של מכונת ה-Bomba הפולנית.¹⁵ הגרמנים הגיעו למסקנה שאכן הודעות 'אניגמה' פוענחו בעבר, אך הסיכון איננו עוד, ומספר הצירופים הגבוה של המכונה מעניק ביטחון גבוה. נראה שמומחי הצופן הגרמנים הבכירים לא סברו שקבוצת מתמטיקאים פולנים צעירים יכולים למצוא חולשה במכונה ולפענחה במספר צירופים קטן.

אירועים שונים הביאו לכך שהחשד הגרמני שבנות הברית קוראות תעבורה גרמנית מוצפנת הלך וגדל, אך הדבר יוחס לבגידה ודליפת מפתחות צופן. הגרמנים נקטו צעדים יוצאי דופן לשפר את ביטחון ונוהלי תקשורת הרדיו, לקיים מעקב ביטחוני הדוק אחרי כל האנשים שהיו קשורים בייצור, חלוקת ואחזקת מפתחות צופן, ולחלק תעבורה בין מספר מפתחות הצפנה, כדי לצמצם את הנזק של 'זליגת' מפתח.

הצלחות בנות הברית בלחימה כנגד הצי הגרמני יוחסה אף היא לבגידה ולמכ"ם, אך החשש לביטחון הצופן הלך וגדל, והביא להוספת הרוטור הרביעי במכונות 'אניגמה' של הצי הגרמני בשנת 1942.

המודיעין הגרמני (Abwehr) העביר באוגוסט 1943 דו"ח מודיעין מסוכן גרמני שפעל במפקדת הצי האמריקאי בווישינגטון, ממנו למדו הגרמנים כי הצי האמריקאי קורא את הפקודות הנשלחות לצוללות גרמניות. מידע זה לא הועבר למטה הכללי הגרמני OKW.

משנת 1944, הגרמנים פעלו בהנחה שתעבורת 'אניגמה' מפוענחת בידי בנות הברית, אך חשדו שהסיבה לכך היא בגידה והעברת מפתחות לאויב. התעבורה ב'אניגמה' הוגבלה לסיווג 'שמור', ונאסר להצפין באמצעותה מידע בסיווג 'סודי' או 'סודי ביותר', ולשלוח באמצעותה פקודות מבצע. המידע המסווג הועבר בטלפרינטרים שהוצפנו במכונות לורנץ (צופן Tunny), שהגרמנים בטחו בו.

החקירות של TICOM בתום המלחמה גילו כי המחקרים התיאורטיים של הגרמנים חשפו את כל החולשות של ה'אניגמה', אך הדבר לא הרשים אותם, שכן הם לא ראו דרך מעשית בה האויב יוכל להשתמש בחולשות אלה.¹⁶ הגרמנים התכוונו ליישם שיפור ב'אניגמה' (Variable Notch Rotor) ולאחר מכן לעבור מ'אניגמה' למכונת הצפנה חדשה (Cipher Device 39), צעדים שאם היו מתבצעים לא היו ניתנים לפענוח, אך הם לא הספיקו לעשות זאת.¹⁷

שיתוף פעולה בין הגורמים הגרמנים שעסקו בנושא, חקירות גרמניות נמרצות יותר בפולין ובצרפת, לאחר כיבושם, וענווה מקצועית (במקום עודף ביטחון עצמי) היו משנים את התמונה. פענוח צופן ה'אניגמה' היה נתון בסכנה, תלוי בשערה.

¹⁴ פריץ אריך פלגייבל (Fritz Erich Fellgiebel) (1886–1944). מפקד חיל הקשר הגרמני משנת 1940. היה בין הקצינים השותפים לקשר נגד היטלר ב-20 ביולי 1944 והוצא להורג בעקבות כשלון הקשר.

¹⁵ ראו:

European Axis Signal Intelligence in World War II as Revealed by "TICOM" Investigations and by Other Prisoners of War Investigations and Captured Material, Principally German, Volume 2 – Notes on German High Level Cryptography and Cryptanalysis, Army Security Agency, 1 May 1946. DOCID: 3560816 (hereinafter **TICOM Vol. 2**), p. 5.
https://media.defense.gov/2021/Jul/14/2002762718/-1/-1/0/VOLUME_2_NOTES_ON_GERMAN.PDF

¹⁶ חקירת ד"ר בוגיש (Buggisch), TICOM Vol. 2 P. 12.

¹⁷ TICOM Vol. 2, pp. 13–14

ערב מלחמת סיני (1956), הצפנה ופענוח של מברקים בחטיבות הלוחמות בצה”ל התבססו על מפתחות חד-פעמיים והצפנה ידנית.¹⁸ ההצפנה והפענוח הידניים של התעבורה ברשתות הרדיו היו ‘צוואר בקבוק’ שעיקב את העברת המברקים, וכדי לפתור בעיה זו הצטייד חיל הקשר בכ-50 מכונות הצפנה ‘אניגמה’ עם שלושה רוטורים M3. המכשירים הוסבו לשפה העברית, יוצרו עבורם מפתחות להצפנה ופענוח (בחירת הרוטורים וסדר התקנתם, הנחיות למיקום ראשוני של הרוטורים וחיבורי לוח החיבורים בחזית המכשיר), הוכנו נהלים מתאימים, וצפנים הוכשרו להשתמש בהם.¹⁹

ערב מלחמת סיני התברר כי תפעול המכשיר מסורבל ואיננו מקנה יתרון מול ההצפנה הידנית, וייתכן כי מומחי הצופן של חיל הקשר סברו כי הטכנולוגיה של ה‘אניגמה’, הגם שהיא מספקת מספר גדול מאוד של צירופים, לא מספקת צופן חזק דיו, ולכן הוחלט לא לבצע בצה”ל שימוש מבצעי במכונות אלה.²⁰ המכונות אוחסנו ומעולם לא נעשה בהם שימוש (פרט לניסוי של העברת כמות מברקים קטנה בין ארבעה משרדי קשר נייחים במשך ארבעה ימים בנובמבר 1956).²¹



איור מס' 3: אניגמה בצה”ל, מוסבת לעברית – טג-356

¹⁸ דניאל רוזן, מרדכי פופר, **כסף החרטום – ראשית השימוש בכתב-סתרים בצה”ל**, העמותה להנצחת חללי חיל הקשר והתקשוב, כסלו התשפ”ב – ינואר 2021.

¹⁹ המספרים הסידוריים של מכונות ה‘אניגמה’ הבודדות ורכיביהם ששרדו הם מסדרות כמותן נמצאות במוזיאון צבא נורווגיה באוסלו (Forsvarsmuseet).

²⁰ נזכיר כי מספר בכירים במערכת הישראלית שירתו בזמן מלחמת העולם השנייה בתפקידים בכירים במערך הבריטי שפענח את צופן ‘אניגמה’. בין בכירים אלה: ולטר איתן, שהיה המנכ”ל הראשון של משרד החוץ, ופרופסור יוסף (גיו) גיליס, ממקימי הפקולטה למתמטיקה במכון ויצמן למדע ברחובות.

²¹ ארכיון צה”ל ומערכת הביטחון 404-652/1958.

אירוע ההצטיידות במכונות הצפנה אלה ערב מלחמת סיני מעלה סימן שאלה – עד כמה היו מומחי חיל הקשר, בשנותיו הראשונות, מודעים לחולשות של מנגנוני כתב־סתרים 'אקראיים לכאורה' בטכנולוגיות האלקטרומכניות של אותה תקופה,²² ולאפשרות פענוח המידע העובר בהם?

מחקר עדכני בנושא 'אניגמה'

נושא צופן ה'אניגמה' ממשיך לעניין קהל גדול של חוקרים, אנשים תאבי דעת וחובבים, ברחבי העולם. בכנסים הדנים בקריפטולוגיה מועלים תדירות נושאים ורעיונות חדשים, ואנשים רבים פועלים לאתר מכונות אניגמה ישנות ולשפץן.

במרשתת זמינות סימולציות תוכנה של מכונת 'אניגמה', המאפשרות ל'השתעשע' בפענוח והצפנה של ידיעות מתקופת מלחמת העולם, ולרכוש בקיאות ברזי המכשיר.

ניתן לרכוש ערכות (Kits) להרכבה עצמית של רפליקות, אלקטרומכניות או אלקטרוניות, של מכונת 'אניגמה'.

הערות

כאשר פרצה מלחמת העולם השנייה, כוחות הביטחון הבריטיים השתמשו בצפנים מיושנים שהגרמנים פענחו. רק בשנת 1941 הגיעו הבריטים לרמת סודיות נאותה של הצפנים שבשימושם.²³ למתמטיקאים ולמתורגמנים יהודים היה תפקיד נכבד בפעילות פענוח ה'אניגמה' בבלצ'לי פארק. חלק מקבוצה זו אף הקימו תא ציוני, והצהירו בגלוי על כוונתם להגר לפלשתינה בתום המלחמה.²⁴ בנוסף לתעבורת ה'אניגמה', הבריטים פענחו מכשירי הצפנה נוספים בשירות הגרמנים. מחשב ה'קולוסוס', המחשב המתוכנת הראשון בעולם, שימש לפענוח צפני הפיקוד העליון הגרמני, צופן Tunny (צופן 'לורנץ').

הבריטים פענחו גם את צפני שירות הקשר של 'ההגנה' והמחלקה המדינית של הסוכנות, ומשנת 1944 היו אלה 'יעד מועדף', ומקור המודיעין העיקרי שלהם על פעילות היישוב ועל ההעפלה.²⁵ התפרסם כי מערב גרמניה, אוסטריה ונורבגיה השתמשו במכונות 'אניגמה' כמעט עשור מתום מלחמת העולם.²⁶

²² באותה תקופה, השימוש במכונות הצפנה אלקטרומכניות המבוססות על מנגנונים 'אקראיים לכאורה' היה נפוץ בצבאות העולם: האמריקאים השתמשו במכונות SIGABA/M-134, M-209 ו-C-52, הבריטים השתמשו במכונות Typex, הסובייטים השתמשו במכונות Fialka M-125.

²³ John Ferris, *Behind the Enigma, the Authorised History of GCHQ*, Bloomsbury, 2020, pp. 220-230.

²⁴ רוברט הניגאן, *הסיפור הסודי של שוברי הצפנים היהודים שתרמו לניצחון במלחמת העולם השנייה*, ג'ואיש כרוניקל, 26 בינואר 2017, תרגום: דניאל רוזן, העמותה להנצחת חללי חיל הקשר והתקשוב, אב התשפ"ב – אוגוסט 2022.

²⁵ דניאל רוזן, *העליונות המודיעינית הבריטית והתבססותה על פענוח צופני 'ההגנה'*, (טרם פורסם).

²⁶ Tom Perera & Dan Perera, *Inside Enigma*, Second Edition, Radio Society of Great Britain, 2019, p. 117

לקריאה נוספת

מקצת מהפרסומים הרבים על האניגמה, המציגים מידע אמין ומעניין :

Ray Miller, *The Cryptographic Mathematics of Enigma*, Center for Cryptologic History, National Security Agency, 2019.

תיאור מתמטי מקיף של ה'אניגמה', המבחין בין כמות המצבים התיאורטית לבין כמות המצבים המעשית אתן התמודדו המפענחים.

Jennifer Wilcox, *Solving the ENIGMA: History of the Cryptanalytic Bombe*, Center for Cryptologic History, National Security Agency, 2015.

תיאור היסטורי מפורט של הפעילות לפענוח צופן ה'אניגמה'.

David P. Mowry, *German Cipher Machines of World War II*, Center for Cryptologic History, National Security Agency, 2014.

תיאור מכונות ההצפנה האלקטרומכניות בשימוש כוחות הביטחון הגרמנים במלחמת העולם השנייה.

Władysław Kozaczuk, *Enigma: How the German Machine Cipher Was Broken, and How It Was Read by the Allies in World War Two*, edited and translated by Christopher Kasoarek, Second Edition, Frederick, Maryland: University Publications of America, 1984.

תרגום ספר שפורסם בפולנית בשנת 1967. המחבר, קולונל בשירותי הביטחון הפולניים, מתאר את המאמץ הפולני לפענוח ה'אניגמה' ואת שיתוף הפעולה עם השירותים החשאיים הבריטים והצרפתיים.

Frederick William Winterbotham, *The Ultra Secret*, Weidenfeld and Nicolson, London, 1974.

הספר הראשון בשפה האנגלית על ה'אניגמה'. המחבר היה קצין חיל האוויר הבריטי בדרגת Group Captain (דרגה בין מפקד טייסת וקומודור) שהיה אחראי על הפצת המודיעין שנרכש מפענוח צפני ה'אניגמה' ושמירת הסוד. למחבר לא הייתה גישה למסמכים מסווגים והספר נכתב מזיכרון, ויש בו מספר אי דיוקים.

Gordon Welchman, *The Hut Six Story: Breaking the Enigma Codes*, McGraw Hill, 1982.

זיכרונות המתמטיקאי הבריטי שפיקד על 'צריף 6', הגוף בבלצ'לי פארק שהיה אחראי על פענוח ה'אניגמה', מתחילת המלחמה ועד שנת 1943.

Tom Perera & Dan Perera, *Inside Enigma*, Second Edition, Radio Society of Great Britain, 2019.

פרופ' פררה התמחה בנושא ה'אניגמה', וספרו מציג תיאור מקיף של התפתחות המכונה, ממוצר מסחרי למכשיר הצפנה צבאי, ואת הגרסאות השונות של מכונות 'אניגמה' בכוחות הביטחון הגרמניים. בנוסף מתאר הספר מכונות הצפנה אלקטרומכניות דומות בשימוש הבריטים, האיטלקים, היפנים, האמריקאים והשווייצרים, ומכונות הצפנה של הגוש הסובייטי מתקופת 'המלחמה הקרה'.

Robert J. Hanyok, *Eavesdropping on Hell*, Center for Cryptologic History, National Security Agency, 2005.

תיאור מה ידע מודיעין התקשורת של בנות הברית על השואה ומחנות ההשמדה ממברקי 'אניגמה' שפוענחו. מסמך היסטורי חשוב ומעניין לקורא הישראלי.