אדר תשפ״ה
מרץ 2025

מכונות הצפנה אלקטרומכניות במלחמת העולם השנייה

מאת: אל״מ בדימוס דניאל רוזן

מבוא

סיפור ה׳אניגמה׳ (Enigma), מכונת הצפנה אלקטרומכנית בשימוש גרמניה הנאצית במלחמת העולם השנייה, ופענוח תעבורת ה׳אניגמה׳ בידי בנות הברית, זכו לתשומת לב רבה, אך זו לא הייתה מכונת הרוטורים האלקטרומכנית היחידה שצפניה פוענחו.

מכונות הצפנה אלקטרומכניות שיצרו מנגנונים ׳אקראיים לכאורה׳ בטכנולוגיה של מערכת רוטורים מסתובבים היו נפוצות בתקופת מלחמת העולם השנייה ובתחילת תקופת המלחמה הקרה. מאמר זה מציג סקירה תמציתית של מכונות ההצפנה העיקריות בטכנולוגיה זו.

גרמניה הנאצית השתמשה במכונות ׳אניגמה׳ (Enigma), Lorenz SZ40/42 ו־Siemens T52;[1] ארה״ב השתמשה במכונות SIGABA/M-134 ו־M-209; בריטניה השתמשה במכונות TypeX; משנת 1943 השתמשו ארה״ב ובריטניה במכונות CCM;[2] היפנים השתמשו במכונות Shiki Ōbun Injiki 91/97.

הצופן הלך והתפתח במהלך מלחמת העולם השנייה, שכן רדיו היה אמצעי תקשורת מרכזי והצדדים הלוחמים ייחסו חשיבות למודיעין תקשורת, ידעו על מאמצי מודיעין התקשורת של האויב, הבינו את השימוש שהאויב יכול לעשות במידע המועבר ברדיו ונקלט על ידו, וניסו לאתר ולהתמודד עם חולשות ציוד ההצפנה ששימש אותם.[3]

שיתוף הפעולה ההדוק בין בריטניה לארה״ב בתחום מודיעין אותות ופענוח צפנים במלחמת העולם השנייה התנהל במסגרת סוכנות חשאית שכונתה TICOM (Target Intelligence Committee). 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

---

1 מכונות ההצפנה Lorenz SZ40/42 ו־Siemens T52 שימשו להצפנת תעבורת טלפרינטרים. הטלפרינטר הגרמני העיקרי נקרא T-32, והגרסאות הצבאיות שלו כונו T-36 ו־T-37; אלה היו למעשה טלפרינטר Model 14 אמריקאי, שכן חברת Lorenz הגרמנית (שייצרה טלפרינטרים משנת 1906) נרכשה בשנת 1930 בידי חברת ITT (International Telephone and Telegraph) האמריקאית, ובשנת 1932 החלה לייצר ברישיון טלפרינטר Model 14 של חברת Teletype האמריקאית. הטלפרינטרים פעלו בקוד בודו (Baudot) של חמש סיביות, בקצב 50 בוד.
ראו: דניאל רוזן, **טלפרינטרים בצה״ל**, העמותה להנצחת חללי חיל הקשר והתקשוב, אלול תשפ״ד – ספטמבר 2024.
המסמך זמין ב: https://www.amutakesher.org.il/_Uploads/dbsAttachedFiles/IDF_Teleprinters_1.00.pdf
ראו עוד:
David P. Mowry, *German Cipher Machines of World War II*, National Security Agency (NSA), 2014.
המסמך זמין ב:
https://www.nsa.gov/portals/75/documents/about/cryptologic-heritage/historical-figures-publications/publications/wwii/german_cipher.pdf

2 Review of Security of Naval Codes and Cyphers 1939-1945, The National Archives (TNA) ADM 1/27186

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

סוף המלחמה וארכיונו נעלם, היה היעד העיקרי של הסוכנות.[4] פעילות זו הייתה חשאית ונשמרה בסוד עד שנת 2009, אז פורסמו לציבור מסמכים רבים.[5] זה מקור המידע העיקרי על הצופן של גרמניה הנאצית.

אניגמה

אניגמה היא מכונה אלקטרומכנית להצפנת טקסט בשיטה 'אקראית לכאורה' ששימשה בדרגים הטקטיים בכוחות הביטחון הגרמנים במלחמת העולם השנייה. הבריטים הצליחו לפענח את הצופן שהמכונה ייצרה – ופרשה זו, מהסודות הכמוסים של המלחמה, נשמרה בסוד בקנאות שנים רבות. זה סיפור מרתק, עליו נכתבו ספרים, הומחזו מחזות והופקו סרטים.[6]

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

מכונת ה'אניגמה' מבוססת על פטנט שנרשם בשנת 1918. בשנות העשרים (עד שנת 1932) הייתה המכונה זמינה כמוצר מסחרי, שלא זכה להצלחה עסקית. הצבא הגרמני רכש את הפטנט בשנת 1926, והכניס במכונה שיפורים. רוב התעבורה הצבאית הגרמנית הוצפנה ב'אניגמה' כבר בשנת 1928.

ההצפנה והפענוח במכונת 'אניגמה' היו תהליך ידני המבוסס על לוח מקשים ולוח נוריות. הקשת אות גלויה גרמה להארת נורית המסמנת את האות המוצפנת. הקשת אות מוצפנת גרמה 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 לחריץ (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 שתיהן. 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.[7] התיול בין דיסקיות כל רוטור, 26 חיבורים פנימיים, שונה לפי מספר הרוטור. משני צידי הרוטורים המסתובבים יש דיסקיות קבועות: הראשונה (מימין) מכונה ETW (Eintrittswalze)

---

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

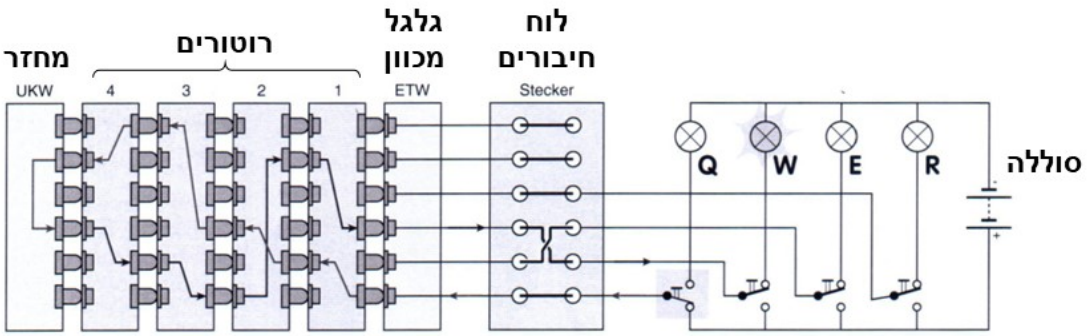
5 בשנת 2011 שחרר ה־NSA 50 אלף מסמכים, הזמינים בארכיון האמריקאי NARA (National Archives and Records Administration), בהם כ־600 מסמכים של TICOM. מסמכים רבים זמינים באתר האינטרנט של ההיסטוריון Randy Rezabek, בארכיון האינטרנט, ראו https://archive.org/details/ticom
הדו"ח המסכם של TICOM, ממאי 1946, זמין ב:
https://www.nsa.gov/Helpful-Links/NSA-FOIA/Declassification-Transparency-Initiatives/Historical-Releases/European-Axis-SIGINT/

6 ראו: דניאל רוזן, **אניגמה**, העמותה להנצחת חללי חיל הקשר והתקשוב, אב תשפ"ג – יולי 2023.
המסמך זמין ב: https://www.amutakesher.org.il/_Uploads/dbsAttachedFiles/Enigma_1.01.pdf

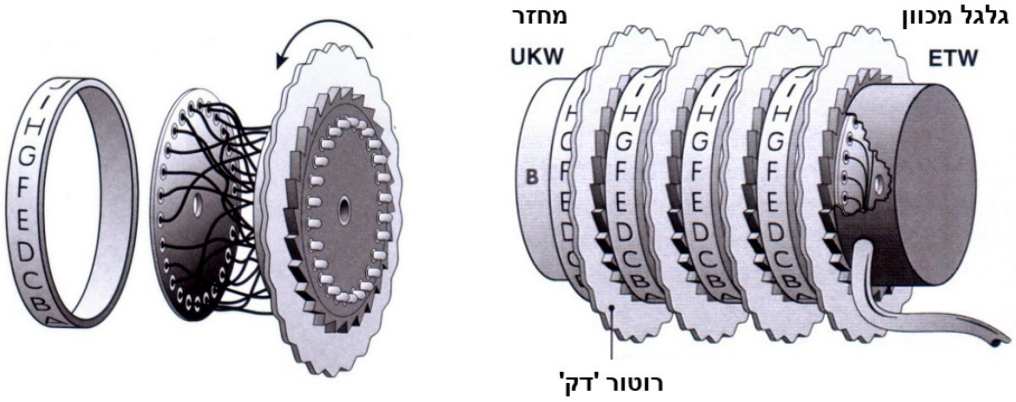
7 הוספת הרוטור הרביעי התאפשרה באמצעות הקטנת המחזר, אך המקום שנותר היה צר, ולא התאים לרוטור רגיל.

או גלגל מכוון (Stator), האחרונה (משמאל) מכונה UKW (Umkehrwalze) או מַחְזֵר (Reflector). [8] בין המקשים והנוריות לבין מערכת הרוטורים מותקן לוח חיבורים (Steckerbrett) עם מגשרים.

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



מערכת הרוטורים מבנה רוטור

איור מס' 2: מערכת הרוטורים של 'אניגמה' דגם M4
מקור: Paul Reuvers & Marc Simons, *ENIGMA – E*, Crypto Museum, Netherlands, 2003

מספר הצירופים התיאורטי האפשרי של מכונת 'אניגמה' הוא מכפלה של כמות הצירופים בלוח החיבורים, כמות הצירופים של מערכת הרוטורים, כמות הצירופים של מיקום הרוטורים ההתחלתי, המיקום היחסי של החריצים ברוטורים (שהיה ניתן לשינוי) וכמות הצירופים במחזר, והוא 3×10^{114} ל'אניגמה' עם שלושה רוטורים M3, או 2×10^{145} ל'אניגמה' עם ארבעה רוטורים M4.

מפתח ההצפנה כולל את בחירת הרוטורים, מיקום יחסי של הטבעת בכל רוטור, וסדר הרכבתם, תצורת הגישורים בלוח החיבורים ומצב התחלתי של הרוטורים.[9] הגרמנים נהגו לבחור באופן

[8] מכונות 'אניגמה' שיוצרו לגורמים שונים בכוחות הביטחון הגרמניים היו עם תיול שונה של הגלגל המכוון ושל המחזר.

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

אקראי את מצב הרוטורים לכל הודעה שהוצפנה, והאותיות הראשונות ששודרו היו 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.[10]

הפולנים פענחו את צופן ה'אניגמה' משנת 1933 עד שנת 1939. שינויים טכניים של הגרמנים (הוספת שני רוטורים חדשים) עצרו את פענוח ההודעות. ביולי 1939 העבירו הפולנים לבריטים ולצרפתים את סודות פענוח האניגמה. הבריטים הצליחו לפענח חלק ניכר מהתעבורה הגרמנית כבר באוגוסט 1940, והצליחו לפענח את צופן האניגמה עד סוף המלחמה (פרט להפרעות חלקיות של מספר חודשים בתחילת שנת 1941 ובמהלך חלק משנת 1942).

החקירות של TICOM בתום המלחמה גילו כי המחקרים התיאורטיים של הגרמנים חשפו את החולשות של ה'אניגמה', אך הדבר לא הרשים אותם, שכן הם לא ראו דרך מעשית בה האויב יוכל להשתמש בחולשות אלה.[11] 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.[12]

מכונת אניגמה M4

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

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

[11] חקירת ד"ר בוגיש (Buggisch), 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. Ref ID: 3560816 (hereinafter **TICOM Vol. 2**), p. 12.
https://media.defense.gov/2021/Jul/14/2002762718/-1/-1/0/VOLUME_2_NOTES_ON_GERMAN.PDF

[12] TICOM Vol. 2, pp. 13-14

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 : National Security Agency, National Cryptologic Museum, 2008.1002.1402

Lorenz SZ40/42

מכונת ההצפנה Lorenz SZ40, מכונת הצפנה אלקטרומכנית מבוססת רוטורים לתעבורת טלפרינטרים, הייתה בשימוש נרחב בצבא גרמניה הנאצית משנת 1941, לתעבורת טלפרינטרים בסיווג גבוה בין המטה הכללי OKW (Oberkommando der Wehrmacht) למפקדות הכפופות לו, בעיקר

בערוצי רדיו בתדר גבוה (2 עד 30 מה״ץ).[13] המכונה שודרגה פעמיים במהלך המלחמה (דגם SZ42a ודגם SZ42b). שם הקוד הבריטי למכונה זו היה TUNNY.

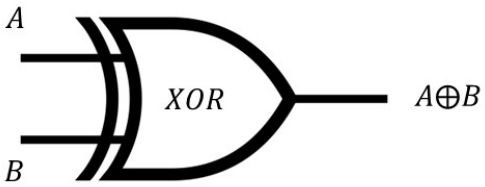
המכונה הייתה מבוססת על 12 רוטורים שיצרו בכל צעד חמש סיביות, להצפנת חמש הסיביות של האות הגלוי.[14] בהיקף כל רוטור היו פינים, שניתן היה להציבם במצב גבוה (שהפך סיבית ׳0׳ לסיבית ׳1׳ וסיבית ׳1׳ לסיבית ׳0׳) או במצב נמוך (שלא שינה את ערך הסיבית – ׳1׳ נשאר ׳1׳, ׳0׳ נשאר ׳0׳). חמשת הרוטורים הראשונים כונו Psi, הרוטור השישי והשביעי כונו Mu וחמשת הרוטורים הנוספים כונו Chi. בשנת 1941 שינו הגרמנים את מצבי הרוטורים Psi ו־Chi אחת לחודש ואת מצבי הרוטורים Mu כל יממה. בשנים מאוחרות יותר שינו את מצבי כל הרוטורים כל יממה.[15]

חמשת הרוטורים Chi התקדמו צעד אחד בכל אות. חמשת הרוטורים Psi התקדמו בצעדים שנקבעו בידי שני הרוטורים Mu.

כמות הצעדים בכל רוטור הייתה שונה, לפי הטבלה הבאה:

כינוי הרוטור	M	L	K	J	I	H	G	F	E	D	C	B	A
כמות צעדים (פינים)	23	26	29	31	41	61	37	59	53	51	47	43	

שיטת ההצפנה הייתה צירוף בינרי בין מפתח ההצפנה לבין ההודעה בדרך של ביצוע פעולת XOR בנפרד על כל אחת מחמש הסיביות של קוד בוד – סיבית מפתח הצפנה מול סיבית הודעה גלויה לצרכי הצפנה, מול סיבית הודעה מוצפנת לצרכי פענוח. פעולת ה־XOR נעשתה בין חמשת הרוטורים Psi וחמשת הרוטורים Chi.



A	B	$A \oplus B$
0	0	0
0	1	1
1	0	1
1	1	0

שער XOR: טבלה לוגית (טבלת אמת), סימול לוגי

זרם הסיביות האקראי לכאורה שהמכונה יוצרת, לצורך ההצפנה/פענוח, הוא:

$$\text{זרם סיביות אקראי לכאורה} = \text{מפתח } Psi \otimes \text{מפתח } Chi$$

תיאורטית, מספר הצירופים האפשריים היה:

$$43 \times 47 \times 51 \times 53 \times 59 \times 37 \times 61 \times 41 \times 31 \times 29 \times 26 \times 23 = 1.6 \times 10^{19}$$

---

13 לתעבורה ברמת סיווג גבוהה במיוחד השתמשו הגרמנים משנת 1944 בהצפנה עם מפתח חד־פעמי, באמצעות מכונת הצפנה Siemens T-43.

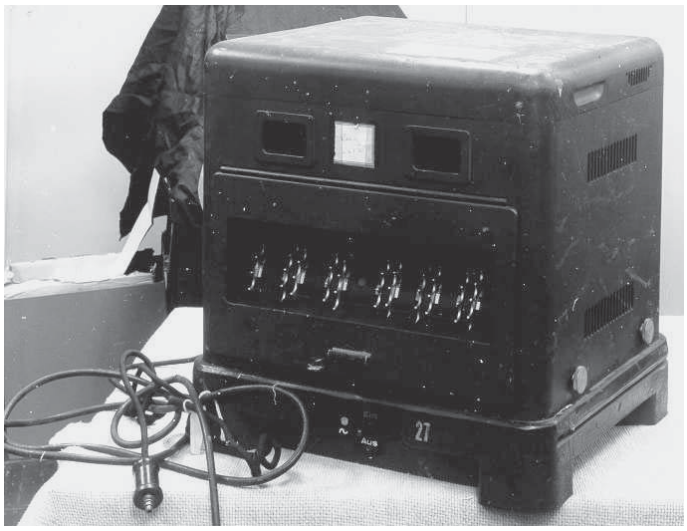
14 לפרטים על מבנה המכונה ראו: TICOM document No. 663
המסמך זמין ב: https://www.cryptomuseum.com/crypto/lorenz/sz40/files/T663_SZ42_Vol_1.pdf
למידע על מפתחות צופן ראו: TICOM document No. 665
המסמך זמין ב: https://www.cryptomuseum.com/crypto/lorenz/sz40/files/T665_SZ42_Vol_3.pdf
להוראות שימוש ראו: TICOM document No. 667
המסמך זמין ב: https://www.cryptomuseum.com/crypto/lorenz/sz40/files/T667_SZ42_Vol_2.pdf
תיאור פענוח הצופן מוצג במסמך: NSA 3838670, ששוחרר לפרסום בדצמבר 2007.
המסמך זמין ב: https://media.defense.gov/2021/Jul/02/2002755804/-1/-1/0/TUNNY-MACHINE.PDF

15 TICOM Vol. 2, pp.20-23

הבריטים פענחו את מנגנון ההצפנה בשנת 1941, ומשנת 1942 קראו את התעבורה שעשתה שימוש במכונות אלה.[16] הפענוח התבסס על ניצול טעויות מפעילים (למשל: שידור שתי הודעות באותו מצב התחלתי של הרוטורים, או העברת המצב ההתחלתי של הרוטורים בתקשורת גלויה), ועל כך שהאות המוצפן שמר על סטטיסטיקת השימוש באותיות האלף־בית ה'צמודות' בשפה הגרמנית.

הבריטים פענחו את הצופן של מכונה זו וקראו את התעבורה ששודרה באמצעותה באמצעות שימוש במחשב ה'קולוסוס', המחשב המתוכנת הראשון בעולם. ההישג הבריטי בפענוח צופן זה היה אף חשוב יותר מההישג של פענוח תעבורת ה'אניגמה'. מאביב 1942 TUNNY סיפקה לבריטים מידע אמין ומשמעותי, בעל ערך אסטרטגי ייחודי, על פעילות הגרמנים ותוכניותיהם.[17]

הבריטים חשפו את הסוד של Tunny לציבור הרחב רק בשנת 2000.[18]



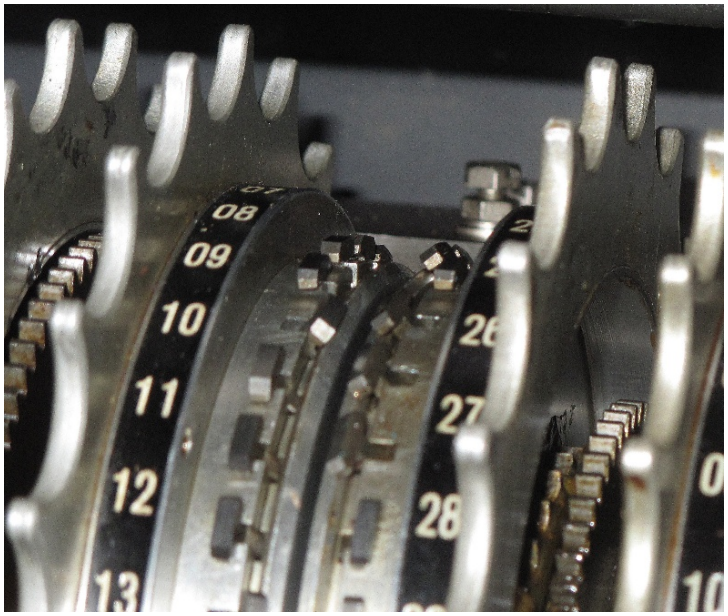
מכונת הצפנה Lorenz SZ40
באדיבות NSA

מכונת הצפנה Lorenz SZ40
באדיבות NSA

16 Captain Jerry Roberts, *Lorenz: Breaking Hitler's Top Secret Code at Bletchley Park*, The History Press, 2017

17 כדוגמה: מידע מקיף על היערכות הגרמנים לפלישת בנות הברית לאירופה, או ההישג הבריטי בזיהוי הצלחת הגרמנים לפענח את הצפנים ששימשו שיירות באוקיינוס האטלנטי (Naval Cypher No. 3 and No. 4) באוגוסט 1942.
Ralph Erskine, *Tunny Reveals B-Dienst Successes Against the 'Convoy Code'*, Intelligence & National Security 18(6), December 2013, pp 868-889.

18 *General Report on Tunny, with Emphasis on Statistical Methods*, TNA HW 25/4, HW 25/5



הצבת הפינים על רוטור
מקור: Ted Coles

Siemens T52

מכונת ההצפנה Siemens T52, מכונת הצפנה אלקטרומכנית מבוססת רוטורים לתעבורת טלפרינטרים, פותחה בשנת 1930 בחברת Siemens & Halske בברלין, שירתה בעיקר את חיל האוויר הגרמני (Luftwaffe), והופעלה בעיקר על קווים פיזיים.[19] למכונות אלה היו ארבע גרסאות: T52a/b, T52c/ca, T52d ו־T52e. הגרמנים כינו את המכונה Geheimschreiber. שם הקוד הבריטי למכונה זו היה Sturgeon.[20]

המכונה התבססה על טלפרינטר T-36 תוצרת Siemens שנוספה לו תיבת הצפנה עם עשרה רוטורים. המכונה הייתה כבדה מאוד, ומשקלה, כשהיא ארוזה בתיבת הובלה, היה מעל 100 ק״ג.[21]

כמות הצעדים בכל רוטור הייתה שונה, לפי הטבלה הבאה:

כינוי הרוטור	K	I	H	G	F	E	D	C	B	A
כמות צעדים (פינים)	47	53	59	61	64	65	67	69	71	73

19 לאחר המלחמה עשו מספר מדינות שימוש במכונה זו, כולל הצי ההולנדי ומשרד החוץ הצרפתי.

20 Frode Weierud, Bletchley Park's *Sturgeon, The Fish That Laid No Eggs*, in: B.Jack Copeland (Ed.), COLOSSUS, Oxford University Press, 2006, pp.307-327.
Or: Frode Weierud, *BP's Sturgeon, The Fish That Laid No Eggs*, CERN, Switzerland, 2006 (hereinafter: Weierud, *Sturgeon*)

ראו:
https://www.researchgate.net/publication/346818035_Bletchley_Park's_Sturgeon-The_Fish_That_Laid_No_Eggs

21 חברת Siemens & Halske רשמה בשנת 1933 פטנט בארה״ב על המכונה (Secret Telegraph System, פטנט מספר 1,912,983), רישום הפטנט מתאר את פרטי מבנה המכונה.
המסמך זמין ב: https://www.cryptomuseum.com/crypto/siemens/t52/files/us1912983.pdf
תיאור המכונה בגרמנית זמין ממקורות שונים, כולל:
חוברת טכנית משנת 1937:
https://www.cryptomuseum.com/crypto/siemens/t52/files/Geheimzusatz_FSM_T52_OKM_1937.pdf
חוברת דגם T-52d מדצמבר 1944:
https://www.cryptomuseum.com/crypto/siemens/t52/files/T52d_TechDoc_1944.pdf
תיאור מפורט של המכונה בשפה האנגלית מדצמבר 1984, ממקור לא ידוע, מוצג במסמך:
https://www.cryptomuseum.com/crypto/siemens/t52/files/T52e_TechDesc_EN.pdf

הרוטורים נבחנו בנקודה מוקדמת לנקודה הראשית (נקודה 25, 24, 23, 22, 22 , 20, 20, 19 ו־16 בהתאמה), ורוטור קפץ צעד היה ותוצאת פעולת OR עם הרוטורים בשני צדדיו הייתה '1'. מערכת ממסרים ולוח חיבורים איפשרו שליטה בלוגיקה זו. [22]

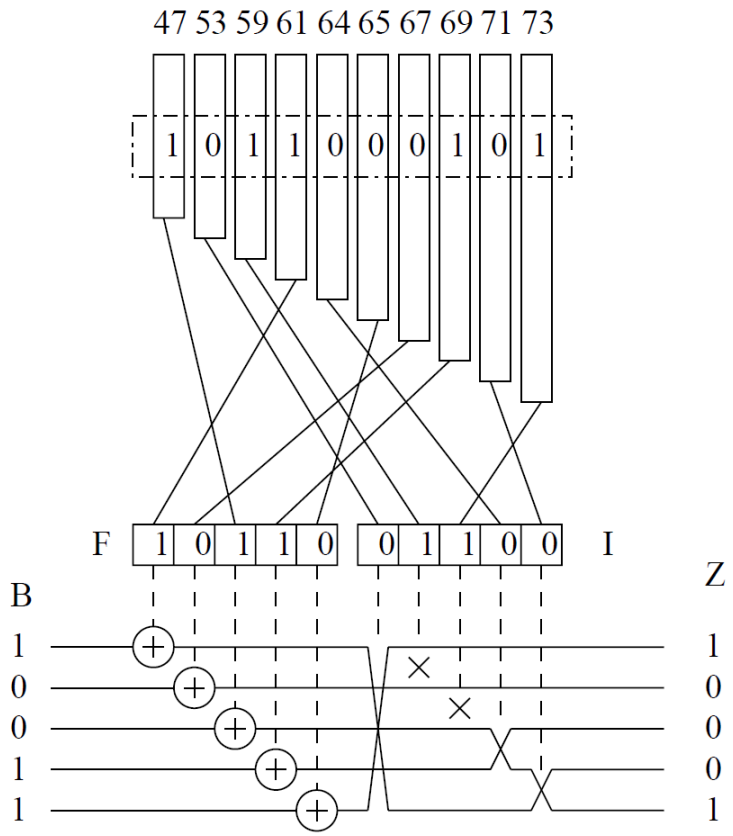
ההצפנה/פענוח מבוססת על כך שחמשת הרוטורים הראשונים מבצעים פעולה של XOR על האות הגלוי/מוצפן, וחמשת הרוטורים הנוספים מבצעים על תוצאה זו פעולת תמורה (Permutation).

השבדים האזינו לקווים שחיברו בין גרמניה לנורבגיה והחלו לפענח את תעבורת ה־T-52 ממאי 1940. הגרמנים איתרו את חולשות המכונה וקיבלו מידע מודיעיני על הפענוח בידי השבדים, ובשנת 1943 שינו את המכונה (הדגם המשופר כונה T52d). השבדים לא הצליחו להמשיך לקרוא את התעבורה.

הבריטים התקשו להאזין לקווים הפיזיים באירופה, אך פענחו תעבורה שהוצפנה במכונה זו בקיץ 1942, כאשר הגרמנים השתמשו במכונה להצפנת קשר אלחוטי בתג״ם בין סיציליה ללוב.

מכונת הצפנה
Siemens T52
באדיבות
Crypto Museum

[22] TICOM Vol. 2, pp.23-26



מרשם חשמלי עקרוני של מכונת הצפנה T52
מקור: Weierud, *Sturgeon*

TypeX

הבריטים כוננו בשנת 1926 ועדה בין־משרדית לבחון מכונה אלקטרומכנית שתחליף הצפנה ידנית. הוועדה פעלה עד שנת 1933, אך לא הגיעה להסכמות באשר למענה ראוי. חיל האוויר המלכותי פעל לפתרון עצמאי, מבוסס על מכונת 'אניגמה' מסחרית, ודגמים ראשונים, TypeX Mark I, הופעלו בשנת 1937. 500 יחידות של דגם משופר, TypeX Mark II, הוכנסו לשימוש בשנת 1938,[23] ובמהלך השנים יוצרו 8,200 מכונות מדגם זה, ועוד 3,000 מכונות בגרסה ניידת, דגם TypeX Mark VI.[24]

בהצפנה, המפעיל הקיש את הטקסט הגלוי בלוח המקשים; מדפסת אחת הדפיסה את הטקסט המוצפן על סרט נייר אחד ומדפסת שנייה הדפיסה את הטקסט הגלוי על סרט נייר שני (לצורך ביקורת). בפענוח, המפעיל הקיש את הטקסט המוצפן בלוח המקשים, מדפסת אחת הדפיסה את הטקסט הגלוי המפוענח על סרט נייר אחד ומדפסת שנייה הדפיסה את הטקסט המוצפן שהוקש על סרט נייר שני.

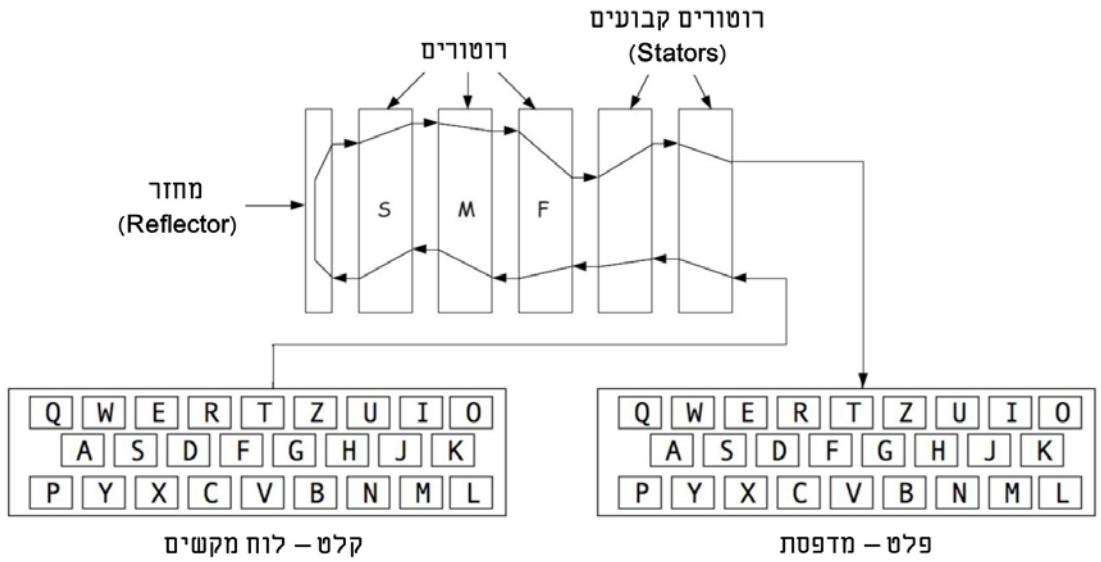
ההחלטה הבריטית לשלב במכונת ההצפנה מדפסות (במקום להשתמש בטלפרינטרים חיצוניים), סיבכה את המכונה, והפכה את ייצורה ליקר.

מכונת TypeX הייתה שונה מה'אניגמה' המסחרית, שכן היו לה חמישה רוטורים. שלושת הרוטורים השמאליים נעו בדומה לרוטורים ב'אניגמה', ושני הרוטורים הימניים היו קבועים (והחליפו את לוח

[23] ה־TypeX הייתה מכונה מורכבת וגדולה, וייצורה היה יקר. להשוואה: באותה עת היו לגרמנים 10,000 מכונות 'אניגמה'.

[24] לתקשורת טלפרינטר ברמת סיווג גבוהה השתמשו הבריטים בהצפנה עם מפתח חד־פעמי, באמצעות מכונות הצפנה BID 30/5-UCO.

החיבורים של ה'אניגמה'). הרוטורים עצמם היו שונים מאלה של ה'אניגמה': ברוטור של 'אניגמה' היה חריץ (Notch) בודד. ברוטורים של TypeX היו בין 3 ל־9 חריצים, ולכן הרוטורים נעו במהירות גדולה יותר מאשר ב'אניגמה'.[25] עם זאת – בניתוח רמת ההצפנה, מכונת TypeX לא סיפקה הצפנה חזקה יותר מזו של ה"אניגמה'.



מכונת הצפנה TypeX – מרשם עקרוני[26]

במהלך המלחמה בוצעו במכונה מספר שינויים, שהעיקריים בהם, בשנת 1943, היו מערכות רוטורים עם תיול פנימי שונה ומחזר (Reflector) שניתן היה לשנות בו תיול (Rewireable). עד אז הייתה המכונה חלשה מבחינת חוזק ההצפנה.

הגרמנים תפסו מכונת TypeX בעת פינוי הכוחות הבריטיים מדנקרק בשנת 1940, וייתכן כי תפסו מכונה בטוברוק בשנת 1942. הבריטים הגיעו למסקנה כי הגרמנים כשלו בניסיונותיהם לפענח את הצופן של TypeX. הנושא היה שנוי במחלוקת עד שבשנת 1947 אותר הארכיון של סוכנות ההאזנה הצבאית הגרמנית, שהוחבא באוסטריה, והמסמכים שנמצאו בו איששו את הכשלון הגרמני.[27]

הבריטים השתמשו במכונות TypeX עד אמצע שנות ה־50. הצי הקנדי השתמש במכונות אלה עד 1962, ומשרד החוץ הקנדי – עד 1968.

---

25 ראו: *Type X Machine Mk VI*, Ministry of Aircraft Production
המסמך זמין ב: https://www.cryptomuseum.com/crypto/uk/typex/files/Typex_Manual_VI.pdf
Maintenance of TYPEX Machines Marks IB, II, III and VI by Code and Cypher Personal, Air Ministry
המסמך זמין ב: https://www.cryptomuseum.com/crypto/uk/typex/files/Typex_Manual_IB_II_III_VI.pdf

26 Kelly Chang, Richard M. Low, Mark Stamps, *Cryptanalysis of TypeX*, Cryptologia, Volume 38, Issue 2, April 2014, pp. 116-132.
המאמר זמין ב: https://www.cryptomuseum.com/crypto/uk/typex/files/kelly_et_al.pdf

27 Interrogations of prisoners of war from the German Army Y Service, TNA HW 40/169

מכונת הצפנה TypeX Mark II
באדיבות Brent Bevan

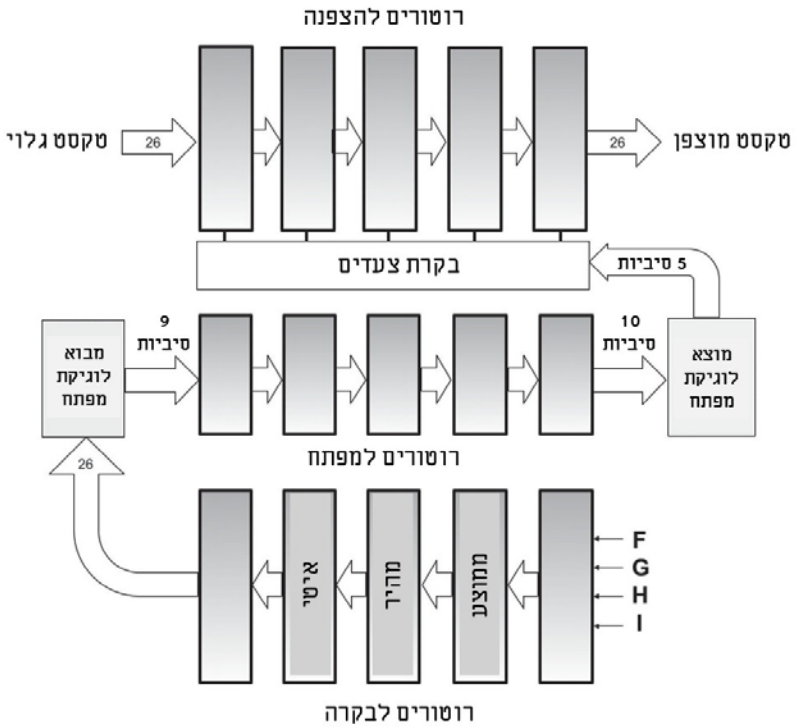
מכונת הצפנה TypeX Mark VI
באדיבות Bonhams, London

SIGABA

בשיתוף פעולה בין הצבא לצי של ארה״ב פותחה מכונת הצפנה שהצי כינה ECM (Electric Cipher Machine) II והצבא כינה בשם SIGABA.[28] עד שנת 1943 השתמשו ב־5,000 מכונות הצפנה אלה, ועד סוף המלחמה השתמשו ב־10,000 מכונות.[29]

בהצפנה, המפעיל הקיש את הטקסט הגלוי בלוח המקשים, ומכונת SIGABA הדפיסה טקסט מוצפן על סרט נייר. בפענוח, המפעיל הקיש את הטקסט המוצפן בלוח המקשים, והמכונה הדפיסה את הטקסט הגלוי המפוענח על סרט נייר. מונה סימן את מספר האותיות בהודעה (מספר זה נרשם בכותרת ההודעה בעת שידורה, כדי לאפשר בדיקה שההודעה נקלטה במלואה).

מנגנון ההצפנה התבסס על שלוש קבוצות של חמישה רוטורים, שתי קבוצות עם רוטורים של 26 מצבים וקבוצה אחת עם רוטורים למפתח (Index), עם 10 מצבים. עשרת הרוטורים התחלפו ביניהם לפי המפתח התקופתי, וניתן היה להתקין כל רוטור בשני מצבים – ישר או הפוך – כדי להגדיל את מרחב המצבים). קבוצה אחת של חמישה רוטורים הצפינה את אות הטקסט, בדומה להצפנה ב׳אניגמה׳. מערכת שינוי המצב היחסי בין הרוטורים הייתה מורכבת פי כמה בהשוואה ל׳אניגמה׳, SZ-40, T-52 או TypeX, וכללה מנגנון הצפנה מורכב, ששינה את המצב היחסי בין הרוטורים המשמשים להצפנה אחרי כל אות.



מנגנון ההצפנה של מכונת SIGABA – מרשם פונקציונלי

מקור: George Lasry, *Cracking SIGABA in less than 24 hours on a consumer PC*, Cryptologia 47(1), pp. 1–37.

[28] לתקשורת טלפרינטר ברמת סיווג גבוהה השתמשו כוחות ארה״ב בהצפנה עם מפתח חד־פעמי, באמצעות מכונת הצפנה SGITOT.

[29] Timothy J. Mucklow, *The SIGABA/ECM II Cipher Machine, "A Beautiful Idea"*, Center for Cryptologic History, National Security Agency, 2015 (hereinafter: Mucklow, *SIGABA*)

המסמך זמין ב:

https://www.nsa.gov/portals/75/documents/about/cryptologic-heritage/historical-figures-publications/publications/technology/The_SIGABA_ECM_Cipher_Machine_A_Beautiful_Idea3.pdf

מספר הצירופים התיאורטי האפשריים נקבע לפי חמשת הרוטורים ששימשו להצפנה וחמשת הסיביות ששימשו לבקרת צעדי הרוטורים. היות וניתן היה לבחור מתוך 10 רוטורים, וכל רוטור ניתן היה להרכיב ישר או הפוך, וניתן היה לקבוע להם מצבים התחלתיים שונים, מספר צירופי הרוטורים האפשרי הוא:

$$10! \times 2^{10} \times 26^{10} = 2^{78.8}$$

ומאחר שיש 5! מצבים למוצא לוגיקת המפתח, ובהתחשב במצבים ההתחלתיים האפשריים, מספר המצבים התיאורטי הוא:

$$5! \times 2^5 \times 10^5 = 2^{28.5}$$

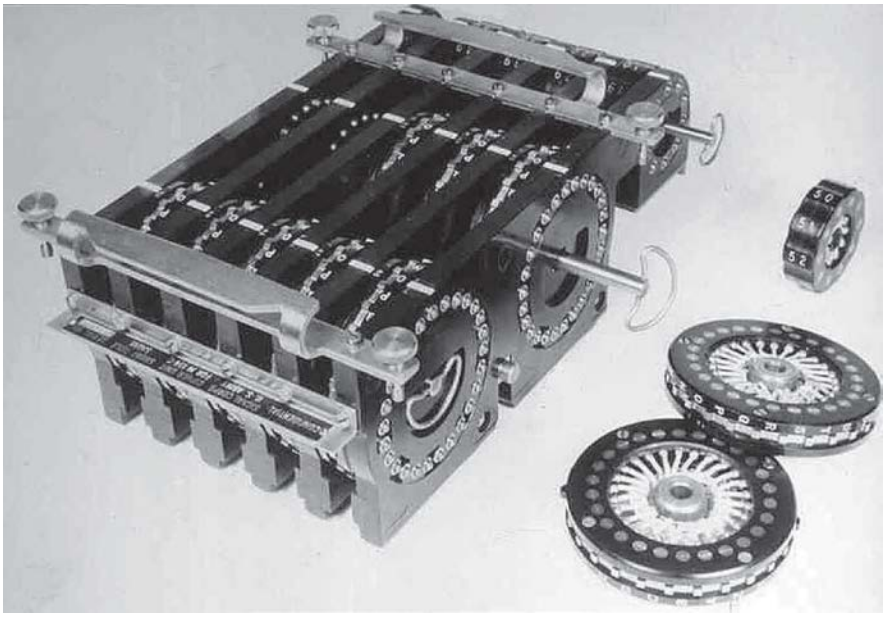
וכמות הצירופים התיאורטית האפשרית היא:

$$2^{(78.8+28.5)} = 2^{107.3} = 2 \times 10^{32}$$

וכאשר לוקחים בחשבון שהיריב איננו מכיר את תיול הרוטורים, מספר הצירופים התיאורטי הכללי גדל, והוא:

$$(26!)^{10} \times (10!)^5 = 2^{992.8}$$

מנגנון הצופן השתנה במהירות והיה אקראי במידה גבוהה פי כמה בהשוואה למנגנון של ה'אניגמה', שהמגרעת העיקרית שלו הייתה תנועה איטית של רוטורים ותבניות (Patterns) בולטות, שאיפשרו את פענוחו. הצופן של ה־SIGABA היה 'חזק' פי כמה בהשוואה ל'אניגמה'.[30]



מערכת הרוטורים של מכונת SIGABA באדיבות NSA

[30] להשוואה: למנגנון DES (Data Encryption Standard) מודרני יש 2^{56} מצבים תיאורטיים אפשריים. למנגנון AES (Advanced Encryption Standard) מתקדם יש 2^{128}, 2^{192} או 2^{256} מצבים, בהתאם לאורך המפתח.

מכונת הצפנה
SIGABA/EC
M II
באדיבות NSA

בפברואר 1945 היה חשש (שהתבדה) שמכונת SIGABA נגנבה מדיביזיית החי״ר השמינית בצרפת, ולכן כל הרוטורים בכל המכונות הוחלפו ברוטורים עם תיול אחר.[31]

מנגנון ההצפנה של מכונת SIGABA נחשב בזמנו ל׳חזק׳ ובטוח, יותר מכל המכונות האחרות בטכנולוגיה של רוטורים מסתובבים, אך כיום ברור שיש לו חולשות, ויש הטוענים שהוא ניתן לפענוח תוך כיממה בעוצמת חישוב של מחשב אישי מודרני.[32]

CCM (Combined Cipher Machine)

עוד בשנת 1941 הגיעו ארה״ב ובריטניה להבנה כי עליהן להשתמש בצופן משותף בתקשורת ביניהם. ארה״ב לא הייתה מוכנה לחלוק עם הבריטים את השימוש במכונות SIGABA, ומכונות TypeX הבריטיות לא התאימו לייצור המוני. הפשרה שנבחרה הייתה שימוש במתאמים (Attachments) משלושה טיפוסים, שהורכבו על מכונות SIGABA ועל מכונות TypeX: Mk1 להתקנה ארעית על מכונת SIGABA קיימת, MkII להרכבה קבועה על מכונת SIGABA, ו־MkIII להרכבה ארעית על מכונת TypeX. המתאמים התבססו על עשרה רוטורים, מהם בחרו חמישה לכל הרכב.[33]

---

31 ההיסטוריה של ה־SIGABA מתוארת בהרחבה בשלושה כרכים של מסמך NSA, *History of Converter M-134-C*, כנראה משנת 1949. המסמכים זמינים ב:
כרך 1, Red ID A522328:
https://www.nsa.gov/Portals/75/documents/news-features/declassified-documents/friedman-documents/patent-equipment/FOLDER_123/41768449080756.pdf
כרך 2, Ref ID A523186:
https://www.nsa.gov/Portals/75/documents/news-features/declassified-documents/friedman-documents/patent-equipment/FOLDER_123/41768399080751.pdf
כרך 3, Ref ID A523210:
https://www.nsa.gov/Portals/75/documents/news-features/declassified-documents/friedman-documents/patent-equipment/FOLDER_123/41768519080763.pdf

32 George Lasry, *Cracking SIGABA in less than 24 hours on a consumer PC*, Cryptologia 47(1), 2021, pp. 1–37.
המאמר זמין ב: https://www.tandfonline.com/doi/full/10.1080/01611194.2021.1989522#abstract

33 ראו: Colonel E.B.W. Cardiff, NATO Memorandum, *CCM System for NATO*, SGM-1922-51, 10 November 1951
המסמך זמין ב: https://www.cryptomuseum.com/crypto/uk/typex/files/nato_ccm_19511110.pdf

כל הציוד יוצר בארה״ב, מאחר שלבריטים לא היו משאבים תעשייתיים זמינים. הציים של ארה״ב ובריטניה החלו להשתמש במכונות אלה בנובמבר 1943, וכל הכוחות המזויינים של ארה״ב ובריטניה החלו להשתמש במכונות אלה באפריל 1944. [34]

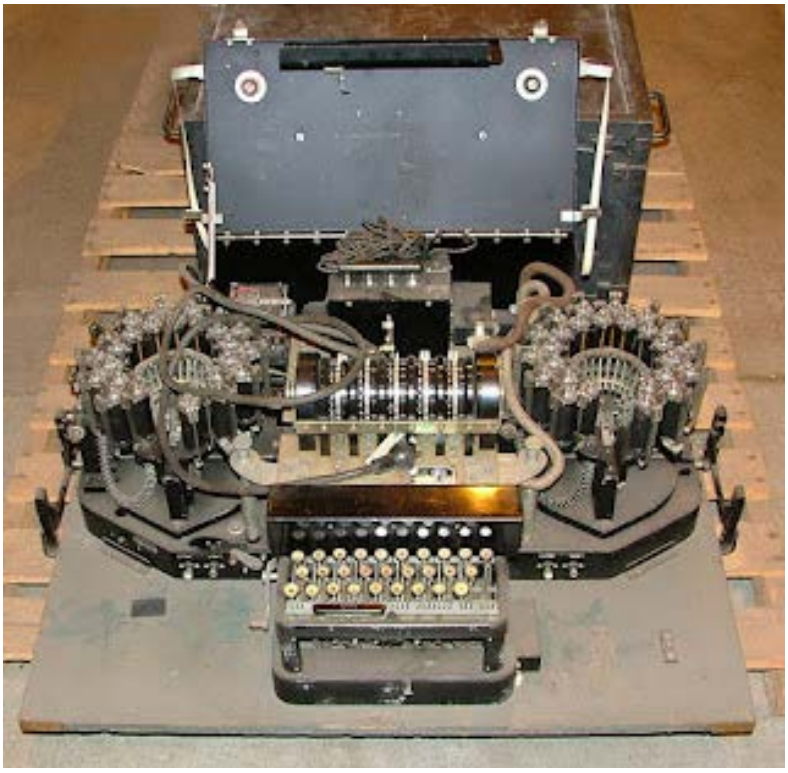
המתאמים התבססו על שימוש בחמישה רוטורים (מתוך עשרה אפשריים) וארבעה אלקטרומגנטים, לקידום הרוטורים. הרוטור האמצעי התקדם צעד אחד בכל לחיצה על לוח המקשים. מגעי הרוטור האמצעי (רוטור 3) שלטו על צעדי הרוטורים 2 ו־4. מגעי רוטור 2 שלטו על תנועת רוטור 1, ומגעי רוטור 4 שלטו על תנועת רוטור 5.

בשנת 1951 החליטה נאט״ו להשתמש במכונות אלה להצפנה ברמה משנית (למפקדות דיביזיה ולספינות מלחמה). נאט״ו השתמשה במכונות אלה עד 1956, עת הוחלפו במכונות הצפנה KL-7. [35] במהלך השנים בוצעו מספר שינויים במכונה, כולל הגדלת מספר הרוטורים מעשרה לעשרים, ושינוי במנגנון השליטה על צעדי הרוטורים.

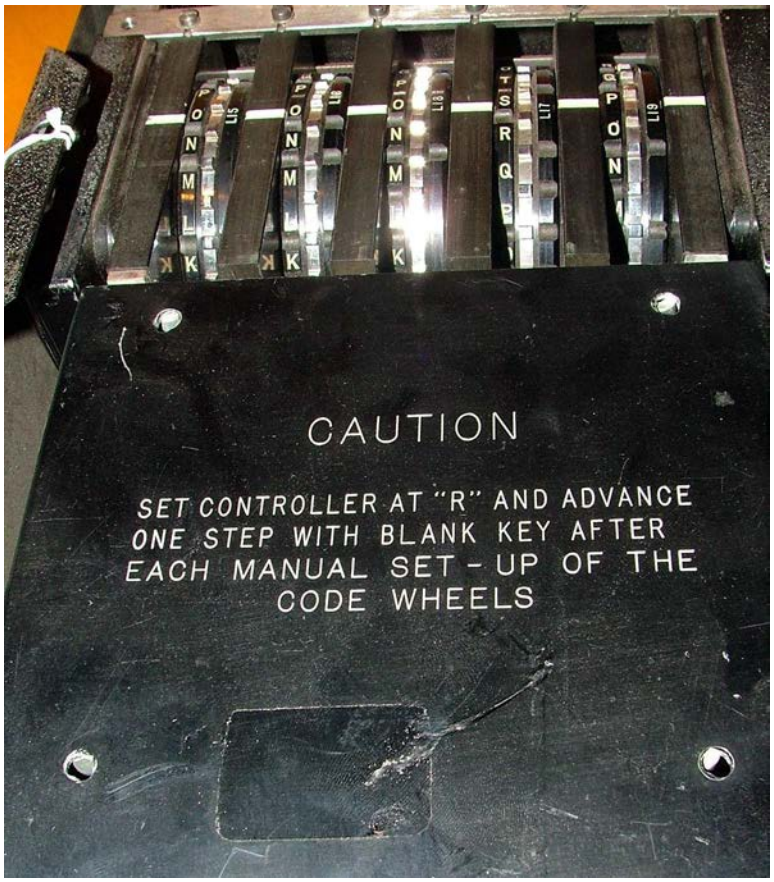
מכונת הצפנה
CCM MkII (CSP1700)
באדיבות
Crypto Museum

[34] *History of Invention and Development of the Mark II ECM*, October 1943, NSA, Ref ID: A273704
המסמך זמין ב:
https://www.nsa.gov/Portals/75/documents/news-features/declassified-documents/friedman-documents/patent-equipment/FOLDER_116/41766759080586.pdf

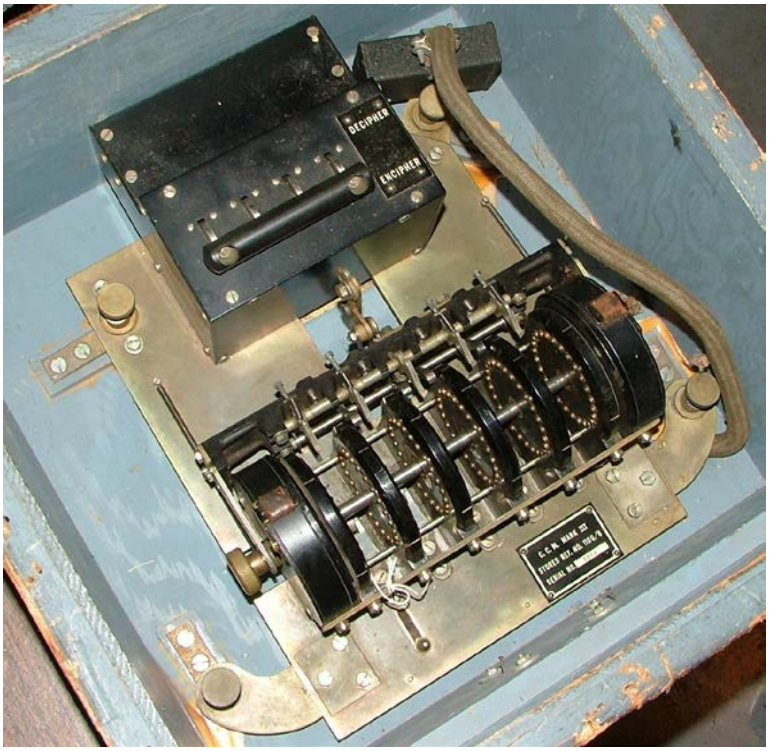
[35] מכונת הצפנה בטכנולוגיה דומה עם שמונה רוטורים, אחד מהם סטטי.



מכונת TypeX עם מתאם CCM MkIII (CSP 1800)
באדיבות NSA



מתאם CCM למכונת (CSP1700),SIGABA CCM Mk II
באדיבות NSA



מתאם CCM למכונת TypeX, CCM Mk III (CSP 1800), בהתקן הובלה
באדיבות NSA

הפעלת מכונת TypeX Mark II עם מתאם CCM
באדיבות Imperial War Museum, A 23510

91/97 Shiki Ōbun Injiki (Angooki Taipu A/B)

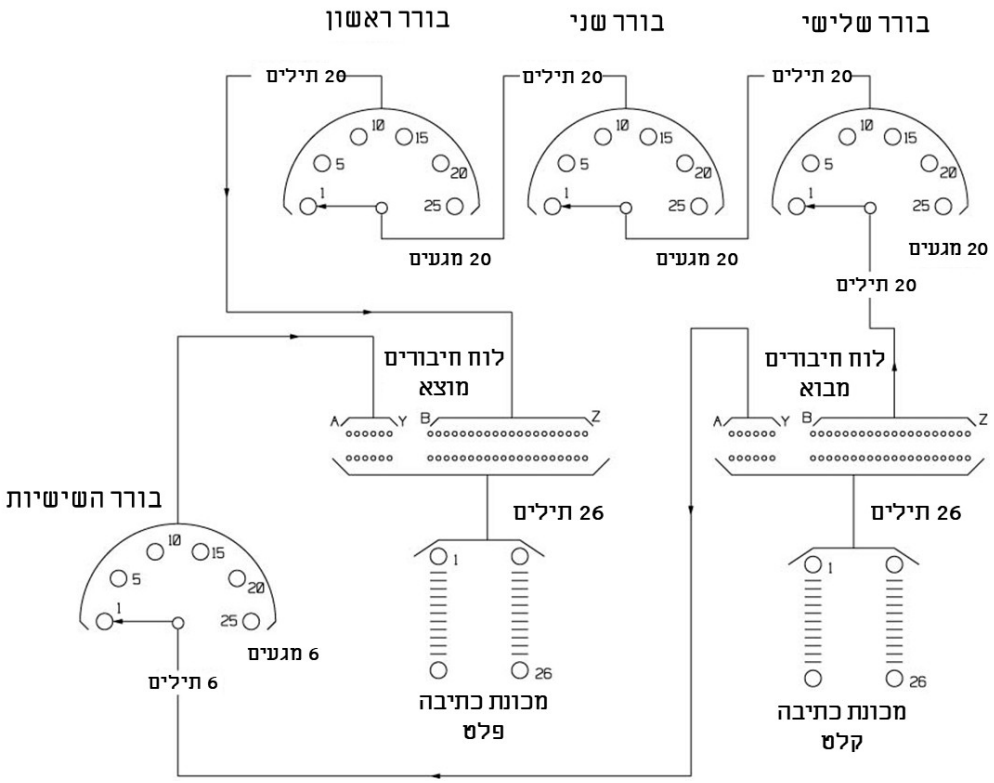
היפנים הצטיידו משנת 1931 במכונת צופן 91, ובשנת 1938 החליפו אותה בהדרגה במכונת צופן 97. מכונות אלה היו מכונות צופן להדפסת תווים אירופאיים, 'הנדסה לאחור' (Reverse Engineering) של מכונת הצפנה פשוטה יחסית תוצרת Hagelin.[36] שם הקוד האמריקאי למכונת צופן 91 היה Red, ולמכונת צופן 97 היה Purple.

הקלט/פלט התבסס על שימוש במכונות כתיבה חשמליות, ומנגנון ההצפנה מומש בצורה מיוחדת: במקום רוטורים מסתובבים, היפנים מימשו את המכונה עם בוררי מבוא (Uni Selectors) טלפוניים מסתובבים. הבוררים התקדמו באמצעות מתקף באלקטרומגנט, והיו להם היו 25 צעדים. בכל צעד היו ששה מגעים. לאחר השלמת 25 צעדים, המתקף הבא באלקטרומגנט קידם את מגעות הבורר לצעד 1.

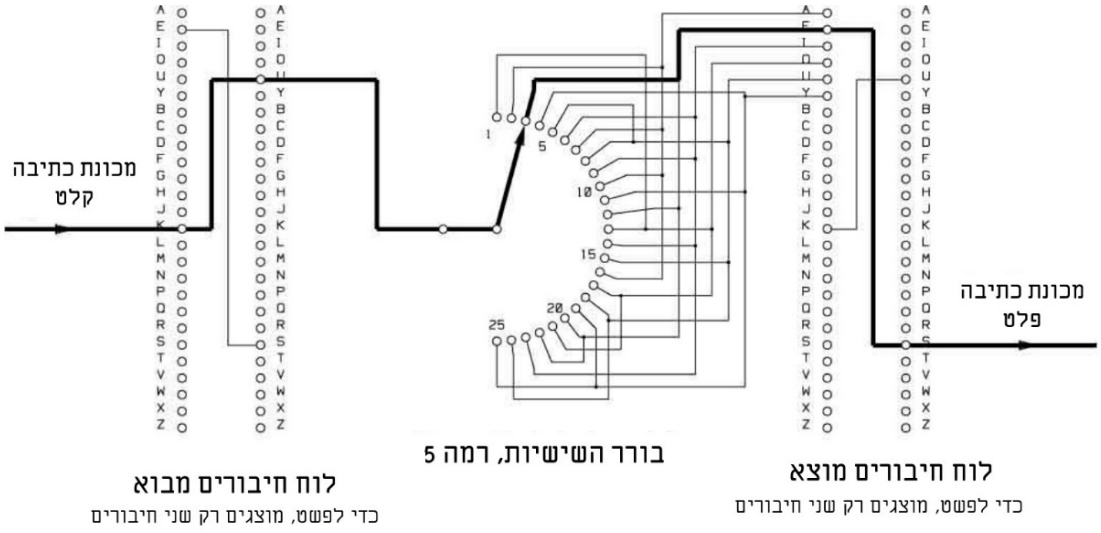
26 אותיות האלף־בית (A עד Z) חולקו לשתי קבוצות, אחת של שש אותיות ושנייה של 20 אותיות. לוח החיבורים במבוא 'חילק' את האותיות לשתי קבוצות. הקבוצה של שש אותיות נותבה לבורר השישיות וביצעה כל צעד תמורה (Permutation) באמצעות בורר השישיות. הקבוצה של עשרים אותיות נותבה לבוררים 1, 2 ו־3, שכל אחד מהם הורכב מארבעה בוררים של 6 מגעים שנעו יחדיו ותויילו בדומה לבורר השישיות, ובכל צעד התבצעה תמורה בין האותיות בהתאם למצב היחסי של שלושת הבוררים.

מכונת הצפנה 91
באדיבות NSA

[36] בוריס הגלין (Boris Hagelin), (1892-1983), היה איש עסקים שבדי שפיתח מכונות הצפנה משנת 1919. המכונות מתוצרתו זכו להצלחה עסקית, בניגוד למכונות של מתחרהו ארתור שרביוס (Arthur Scherbius), ממציא ה'אניגמה'. בין היתר מכר הגלין לארה"ב את הפטנט והזכויות לייצור מכונת ההצפנה הידנית M-209 (מכונת הצפנה טקטית שיועדה להודעות שסיווגן הבטחוני פג לאחר שעות בודדות, ששימשה את כוחות ארה"ב במלחמת העולם השנייה ובמלחמת קוריאה). לאחר מלחמת העולם הוא עבר לשוויץ והקים את חברת Crypto AG, שסיפקה מכונות הצפנה למעל 120 מדינות (כולל איחוד האמירויות הערביות, אירן, ירדן, כווית, לבנון, לוב, מצרים, סוריה, עומן, עירק, ערב הסעודית, קטאר ותורכיה) והתפרסמה בשנת 2015 אחרי שהתברר שה־CIA האמריקאי היה שותף חשאי בחברה משנת 1951, ושמכונות ההצפנה שהחברה מכרה הכילו 'חולשות' שאיפשרו לארה"ב לפענח את התעבורה שעברה בהן. החברה חדלה לפעול בשנת 2018.
Greg Miller, *'The intelligence coup of the century'*, Washington Post, 11 February 2020.
ראו: https://www.washingtonpost.com/graphics/2020/world/national-security/cia-crypto-encryption-machines-espionage/
כתבה זו מציינת כי בריטניה, ישראל, שבדיה ושוויץ היו מודעות למעשיה של החברה או שקיבלו מידע על כך מארה"ב או מגרמניה המערבית.



מרשם עקרוני של מכונות הצפנה יפניות 91/97 [37]



מרשם עקרוני של פעולת 'בורר השישיות', מכונות הצפנה יפניות 91/97 [38]

[37] Freeman, W., Sullivan, G., & Weierud, F., *Purple Revealed: Simulation and Computer-Aided Cryptanalysis of Angooki Taipu B*, Cryptologia, 27(1), 2003, pp. 1–43 (hereinafter: Freeman et al, *A Purple Revealed*).
המאמר זמין ב: http://sysengr.engr.arizona.edu/OLLI/codebreaking/FreemanWithAppendix.pdf

[38] Freeman et al, *Purple Revealed*

צוות בריטי הצליח לפענח את תעבורת מכונת צופן 91 בשנת 1934, וצוות אמריקאי הצליח לעשות זאת בשנת 1935. עם תחילת הפעלת מכונת צופן 97, שעקרון פעולתה היה זהה, היפנים נהגו לשדר אותן ההודעות גם במכונת צופן 91, מה שסייע לפענוח מהיר של מכונת צופן 97.

סיכום

ביטחון המידע בצבאות העולם בתקופת מלחמת העולם השנייה ובתחילת 'המלחמה הקרה' שונה לחלוטין מביטחון המידע של היום. באותה עת התקשורת המסווגת העיקרית הייתה העברת מכתבים באמצעות דואר או רצים, ורק תקשורת דחופה הועברה במברקים, שרובם הוצפנו. בעידן המודרני, ציוד קשר ומערכות מידע נמצאים בשימוש נרחב, צבאות מודרניים חיים, מתנהלים ולוחמים ברשת (מרחב סֶיְבֶ"ר – Cyberspace), ותפקוד צבאות מודרניים מותנה בהגנת מרחב הרשת – שהיא לא רק הצפנת תקשורת, אלא מכלול שלם ומגוון של אמצעים.

הצדדים הלוחמים במלחמת העולם השנייה השתמשו במגוון רחב של אמצעי הצפנה. תעבורה ברמת סיווג בטחוני גבוהה הוצפנה באמצעות מפתח חד־פעמי (OTT – One Time Pad), ידנית או באמצעות מכונות ייעודיות. החלק הארי של התעבורה, שהייתה ברמת סיווג בטחוני נמוכה יותר, הועברה באמצעות מכונות הצפנה אלקטרומגנטיות שייצרו מנגנונים 'אקראיים לכאורה' בטכנולוגיה של רוטורים מסתובבים, הטכנולוגיה המובילה למטרה זו באותה עת.[39]

מאמר זה מציג מספר מכונות הצפנה שהיו מבוססות על הטכנולוגיה של יצור צופן אקראי לכאורה באמצעות מערכת רוטורים מסתובבים, חלק ממגוון מכונות הצפנה שהיו בשימוש במלחמת העולם השנייה. הגם שהמכונות דומות זו לזו, מתיאורן אנו למדים שמומחים ממדינות שונות תפסו אחרת את הסיכונים והחולשות של מערכות אלה, והתמודדו באופן שונה עם הסיכונים. המכונה המתוחכמת ביותר היא מכונת SIGABA.

לא איתרתי הסבר מניח את הדעת לכך שלמרות ההצלחה הבריטית בפענוח תעבורת ה'אניגמה' וה־TUNNY הגרמנית, הבריטים התייחסו ל־TypeX כמכונת הצפנה אמינה ובטוחה, ברמה גבוהה, ולא השקיעו כוח אדם ומאמצים לשפר את ביטחון הקשר של כוחותיהם.

צפנים וטכנולוגיות הצפנה השתכללו במהלך השנים, ואינם דומים לצפנים של מלחמת העולם השנייה, אך חשיבותם נשארה כשהייתה, בטחון הקשר והגנת מרחב הרשת היא נושא חיוני יותר ויותר, וההתלבטות בשאלה עד כמה ניתן לבטוח בצפנים ובמנגנוני הגנת סב"ר נשארה בעינה, במיוחד מול התפתחות טכנולוגיות חדשות, כדוגמת מחשוב קוונטי.

הלקח העיקרי, הנכון גם לימינו, הוא כי בנושא הצפנים חשוב להיות שמרנים וזהירים, ושומר נפשו ישקיע משאבים ואמצעים ראויים בנושא זה, לא יבטח בצופן שבשימושו, ויפעל בדבקות ובהתמדה להעלות את רמת ביטחון הקשר של כוחותינו.

---

[39] הקורא יימצא וודאי עניין בתיאור אמצעי ההצפנה בשנותיו הראשונות של צה"ל. ראו: דניאל רוזן, מרדכי פופר, **כַּסֶּפֶר הֶחָתוּם – ראשית השימוש בכתב־סתרים בצה"ל**, העמותה להנצחת חללי חיל הקשר והתקשוב, כסלו התשס"ב – דצמבר 2021.
המאמר זמין ב: https://www.amutakesher.org.il/_Uploads/dbsAttachedFiles/8(2).pdf