כסלו התשפ״ב
דצמבר 2021

וַתְּהִי לָכֶם חָזוּת הַכֹּל כִּדְבָרֵי הַסֵּפֶר הֶחָתוּם אֲשֶׁר־יִתְּנוּ אֹתוֹ אֶל־יוֹדֵעַ הספר לֵאמֹר קְרָא נָא־זֶה
וְאָמַר לֹא אוּכַל כִּי חָתוּם הוּא: ישעיהו, פרק כט, פסוק יא

כַּסֵּפֶר הֶחָתוּם – ראשית השימוש בכתב־סתרים בצה״ל

דניאל רוזן, מרדכי פופר

מבוא

בשנת 1946 התברר כי הבריטים פענחו מברקים שהוצפנו בכתב־סתרים שהיה בשימוש שירות הקשר של 'ההגנה', וקראו את תוכנם.[1] 'האסון' היה אירוע מכונן בתולדות שירות הקשר וחיל הקשר של צה״ל, והביא למיסוד מערך כתב־סתרים בצה״ל, מימיו הראשונים.

במהלך הפיכת שירות הקשר מארגון חשאי לשירות קשר של צבא הוקם מערך כתב־סתרים. צה״ל השתמש אז בשני סוגים עיקריים של כתב־סתרים: 'תשבץ' לשימוש דרגי השדה, מח״פ (מפתח חד־פעמי – One-time pad) לכל יתר השימושים.

מאמר זה מתאר כתבי־סתרים שהיו בשימוש בצה״ל בשנותיו הראשונות, ואת המערך לייצור כתבי־סתרים ולטיפול בהם.[2]

כתב־סתרים בשיטת 'תשבץ'

כתב־סתרים בשיטת 'תשבץ' מבוסס על שיטה של שינוי סדר האותיות (transposition), שיטה המעניקה ביטחון מוגבל, ולכן התייחסו אליה יותר כדרך לעכב את הבנת התשדורת בידי האויב, מאשר כדרך להבטיח שתוכן התשדורת לא ייוודע לאויב.

כתב־סתרים זה היה בשימוש אלחוטנים (ולא בשימוש צפנים), ביחידות הגמ״ר (הגנה מרחבית) ובדרג הלוחם, ובאמצעותו העבירו מידע בסיווג בטחוני עד 'שמור'.

---

1 דניאל רוזן, **כְּסוּמָא בְּאֲרֻבָּה: הצופן בשירות הקשר של 'ההגנה'**, מפנה האימפריות: סוגיות בחקר היישוב בפרוס המנדט הבריטי, עורך: ניר מן, עלי זית וחרב, כרך י״ט, מודן הוצאה לאור, המרכז לחקר כוח המגן מיסודו של ישראל גלילי, משרד הביטחון – ההוצאה לאור, 2019, עמ׳ 125–152.

2 מילון המונחים הצבאיים של צה״ל מבחין בין **קוד** (״שיטה של הסתרה המבוססת על החלפת מילים (או קבוצות מילים) במילים, באותיות או במספרים לצורכי קיצור או לצורכי סודיות בהעברת תשדורות״) לבין **כתב־סתר** (״שיטה של הצפנה, אשר בה אותיות הא״ב מוחלפות ביניהן או משנות את מקומן, לפי שיטה ומפתח מוסכמים מראש, כפעולה ידנית או באמצעים טכניים״). **הסתרה** היא ״שימוש בקוד או בציוד מיוחד לכך, בהעברת ידיעות, כדי לשמור על הסודיות״. **הצפנה** היא ״שימוש בכתב־סתר לצורך העברת ידיעות בסודיות״. המטה הכללי, עקד כללי 300-1, **מילון מונחים צבאיים**, אג״מ־מה״ד, תש״מ–1980 (להלן: **מילון מונחים צבאיים 1980**). בעניין שימוש בקודים – ראו דניאל רוזן, **סִתְרוֹ כִּגְלוּיוֹ: הסתרת תשדורות טקטיות בצה״ל באמצעות קודים**, העמותה להנצחת חללי חיל הקשר והתקשוב, אלול התשע״ט – ספטמבר 2019.

כתב־סתרים זה החליף שיטות אחרות לשינוי סדר אותיות, שהיו בשימוש בשירות הקשר ובצה״ל, בשנותיו הראשונות.[3]

כתב־סתרים זה, שכונה בשם ׳שיטה 1׳, היה מבוסס על ׳חוברת תשבצים׳ ובה 50 עמודים, בכל עמוד שלושה ׳תשבצים׳ (150 ׳תשבצים׳ בחוברת), ודף חודשי שכלל מפתחות יומיים, אופקיים ואנכיים, 20 ספרות בכל מפתח יומי.

האלחוטן בתחנה המשדרת היה בוחר בתשבץ (שגודלו מתאים לכמות המילים בהודעה שעליו להעביר, כך שיוכל להעביר את ההודעה בתשבץ בודד), רושם את המפתח האופקי והמפתח האנכי, רושם את תוכן ההודעה בתשבץ לפי סדר עולה של המפתח האופקי, כאשר הטקסט נרשם מלמעלה למטה, מעתיק את התוכן המוצפן ב׳חמישיות׳ לטופס מברק לפי סדר עולה של המפתח האנכי (כאשר הטקסט מועתק משמאל לימין),[4] ומשדר את המברק (בדרך כלל: באיתות מורס):[5] חמישיית סרק, חמישיית סימון שסימנה את מספר העמוד והתשבץ בהם השתמש,[6] וחמישיות של ההודעה המוצפנת.

האלחוטן בתחנה הקולטת היה קולט את החמישיות, רושם אותן על טופס מברק, מזהה את התשבץ ב׳חוברת התשבצים׳, מעתיק את החמישיות לתשבץ לפי המפתח האנכי (משמאל לימין), וקורא את התוכן הגלוי לפי המפתח האופקי (מלמעלה למטה).

להמחשה – הודעה גלויה:

מאת: מפח״ט 10 אל גד׳ 3, 4, 5. שמור. כוננות ג׳ בתוקף מ־0500.

תרשם כך, לפי נהלי כתיבת ההודעה הגלויה לצורך הצפנתה:[7]

XדFתוגגוכXוlאeXeאnFצבצkFeדfeXדדfFoאkתתkFסnאאn

**בתוקפFאFnאkאסnאkאkאkאXאkאkאXאkאkאX

תוצפן בתשבץ 3 מדף 43 ב'חוברת התשבצים', כך:

	12	3	4	17	16	8	14	20	1	7	13	19	2	18	5	11	6	9
19					ק	ע			נ		ת							נ
6	כ		F	F								נ		פ				
3	ו	ח	ל				ב	ס	נ		F	ה		ס				ה
11		ת						ק	פ				ק			נ		
1	ל	ק	ד				ת	פ			ד	ק			ה	ו		X
16	ל	פ	ד	נ	פ	F	ו		ח	ר	X	פ			ל	ר	F	ה
10	ו	ס		F		ח		ס	ג	ב				ח	ה		ק	
13			X	ק				X	F							X		

דוגמת הצפנה בשיטה 1 ('תשבץ')

וההודעה המוצפנת, ב'חמישיות', היא:

עקעקע דגXXדד נאתה גאשX וחלבס מהשה כFFמה וFחס טבחק

תאבאא XקXFX נבדמה FוחרX בלרFה קעמתא

כתב־סתרים ידני בשיטת מח"פ

בעקבות ה'אסון' שהתגלה בשנת 1946, לאחר 'השבת השחורה', כאשר התברר כי הבריטים פענחו מברקים שהוצפנו בכתבי־סתרים שהיו בשימוש שירות הקשר של 'ההגנה', וקראו את תוכנם,[8] פעל מפקד השירות, יעקב ינאי (יאן), לגייס מומחים לנושאי צפנים, וכבר בתחילת מלחמת העצמאות אומץ השימוש במח"פ (מפתח חד־פעמי) כשיטת כתב־סתרים עיקרית.

הצפנה בכתב־סתרים בשיטת מח"פ, שכונה בשם 'שיטה 6', היא הצפנה המבוססת על חילופי אותיות (Substitution), המבוססת על טבלת ויז'נר (Vigenère), המוכרת מן המאה ה־15. בצה"ל השתמשו בטבלה בת 25 אותיות, שכללה את כל אותיות האלף־בית העברי (ללא אותיות סופיות) ואת האותיות הלועזיות, F, X ו־Y. אם במברק הופיעה האות V, היא הושארה גלויה.[9]

בהצפנה באמצעות טבלת ויז'נר, מאתרים טור המתחיל באות מפתח בשורה האופקית בראש הטבלה, ומולו שורה המתחילה באות גלויה בטור האנכי הימני. מפגש טור המפתח ושורת הגלוי הוא האות המוצפנת. כך למשל: הצפנת טור המפתח **מ** עם שורת הגלוי **ל** מציגה את האות המוצפנת **ב**. הפענוח נעשה באופן דומה: מפגש טור המפתח **מ** עם שורת הגלוי **ב** מציג את האות המפוענחת **ל**.

---

8 רס"ן שאול בר־לבב (לוינסון) וסא"ל מאיר שפירא, יהודים מדרום אפריקה יוצאי הצבא הבריטי, היו אנשי מפתח בהקמת מערך כתבי־סתרים בצה"ל במלחמת העצמאות. זיגמונט (זיגי) מנדל היה איש מפתח ביישום והנחלת תורת תפעול מערך כתבי־סתרים בצה"ל משנת 1954 עד שלהי שנות ה־70.

9 שירות הקשר השתמש בטבלת ויז'נר דומה, אך המפתח היה פסוק תנ"ך, בית משיר או משפט מספר קריאה (ותדירות החלפת המפתח הייתה נמוכה). רק עם המעבר מפעילות כארגון חשאי לפעילות 'ממוסדת' התאפשר ייצור מפתחות חד־פעמיים, הפצתם לגורמי הצבא השונים ואבטחתם כנדרש.

שימוש בטבלת ויז'נר הוא חיבור מודולו 25 בין המפתח והגלוי. בטבלה העברית, ערכי האלף־בית הם 0 עד 24 ולמעשה מבצעים 'חיסור' מודולו 25, שכן הטבלה כתובה מימין לשמאל (ולא משמאל לימין). להמחשה:

1	**גלוי**	**ג**	**ל**	**ו**	**י**
2	ערך לחישוב	2	11	5	9
3	**מפתח**	**מ**	**פ**	**ת**	**ח**
4	ערך האות העברית	12	16	21	7
5	ערך מתוקן לחישוב	24-12=12	24-16=8	24-21=3	24-7=17
6	חיבור מודולו 25 (שורות 2, 5)	14	19	8	1
7	ערך מתוקן (לקבלת אות עברית)	24-14=10	24-19=5	24-8=16	24-1=23
8	**מוצפן**	**כ**	**ו**	**פ**	**X**

מפתח	א	ב	ג	ד	ה	ו	ז	ח	ט	י	כ	ל	מ	נ	ס	ע	פ	צ	ק	ר	ש	ת	F	X	Y
גלוי א	א	ב	ג	ד	ה	ו	ז	ח	ט	י	כ	ל	מ	נ	ס	ע	פ	צ	ק	ר	ש	ת	F	X	Y
גלוי ב	Y	א	ב	ג	ד	ה	ו	ז	ח	ט	י	כ	ל	מ	נ	ס	ע	פ	צ	ק	ר	ש	ת	F	X
גלוי ג	X	Y	א	ב	ג	ד	ה	ו	ז	ח	ט	י	כ	ל	מ	נ	ס	ע	פ	צ	ק	ר	ש	ת	F
גלוי ד	F	X	Y	א	ב	ג	ד	ה	ו	ז	ח	ט	י	כ	ל	מ	נ	ס	ע	פ	צ	ק	ר	ש	ת
גלוי ה	ת	F	X	Y	א	ב	ג	ד	ה	ו	ז	ח	ט	י	כ	ל	מ	נ	ס	ע	פ	צ	ק	ר	ש
גלוי ו	ש	ת	F	X	Y	א	ב	ג	ד	ה	ו	ז	ח	ט	י	כ	ל	מ	נ	ס	ע	פ	צ	ק	ר
גלוי ז	ר	ש	ת	F	X	Y	א	ב	ג	ד	ה	ו	ז	ח	ט	י	כ	ל	מ	נ	ס	ע	פ	צ	ק
גלוי ח	ק	ר	ש	ת	F	X	Y	א	ב	ג	ד	ה	ו	ז	ח	ט	י	כ	ל	מ	נ	ס	ע	פ	צ
גלוי ט	צ	ק	ר	ש	ת	F	X	Y	א	ב	ג	ד	ה	ו	ז	ח	ט	י	כ	ל	מ	נ	ס	ע	פ
גלוי י	פ	צ	ק	ר	ש	ת	F	X	Y	א	ב	ג	ד	ה	ו	ז	ח	ט	י	כ	ל	מ	נ	ס	ע
גלוי כ	ע	פ	צ	ק	ר	ש	ת	F	X	Y	א	ב	ג	ד	ה	ו	ז	ח	ט	י	כ	ל	מ	נ	ס
גלוי ל	ס	ע	פ	צ	ק	ר	ש	ת	F	X	Y	א	ב	ג	ד	ה	ו	ז	ח	ט	י	כ	ל	מ	נ
גלוי מ	נ	ס	ע	פ	צ	ק	ר	ש	ת	F	X	Y	א	ב	ג	ד	ה	ו	ז	ח	ט	י	כ	ל	מ
גלוי נ	מ	נ	ס	ע	פ	צ	ק	ר	ש	ת	F	X	Y	א	ב	ג	ד	ה	ו	ז	ח	ט	י	כ	ל
גלוי ס	ל	מ	נ	ס	ע	פ	צ	ק	ר	ש	ת	F	X	Y	א	ב	ג	ד	ה	ו	ז	ח	ט	י	כ
גלוי ע	כ	ל	מ	נ	ס	ע	פ	צ	ק	ר	ש	ת	F	X	Y	א	ב	ג	ד	ה	ו	ז	ח	ט	י
גלוי פ	י	כ	ל	מ	נ	ס	ע	פ	צ	ק	ר	ש	ת	F	X	Y	א	ב	ג	ד	ה	ו	ז	ח	ט
גלוי צ	ט	י	כ	ל	מ	נ	ס	ע	פ	צ	ק	ר	ש	ת	F	X	Y	א	ב	ג	ד	ה	ו	ז	ח
גלוי ק	ח	ט	י	כ	ל	מ	נ	ס	ע	פ	צ	ק	ר	ש	ת	F	X	Y	א	ב	ג	ד	ה	ו	ז
גלוי ר	ז	ח	ט	י	כ	ל	מ	נ	ס	ע	פ	צ	ק	ר	ש	ת	F	X	Y	א	ב	ג	ד	ה	ו
גלוי ש	ו	ז	ח	ט	י	כ	ל	מ	נ	ס	ע	פ	צ	ק	ר	ש	ת	F	X	Y	א	ב	ג	ד	ה
גלוי ת	ה	ו	ז	ח	ט	י	כ	ל	מ	נ	ס	ע	פ	צ	ק	ר	ש	ת	F	X	Y	א	ב	ג	ד
גלוי F	ד	ה	ו	ז	ח	ט	י	כ	ל	מ	נ	ס	ע	פ	צ	ק	ר	ש	ת	F	X	Y	א	ב	ג
גלוי X	ג	ד	ה	ו	ז	ח	ט	י	כ	ל	מ	נ	ס	ע	פ	צ	ק	ר	ש	ת	F	X	Y	א	ב
גלוי Y	ב	ג	ד	ה	ו	ז	ח	ט	י	כ	ל	מ	נ	ס	ע	פ	צ	ק	ר	ש	ת	F	X	Y	א

טבלת ויז'נר של 25 אותיות, בשימוש בצה"ל

לשם שימוש בכתב־סתרים בשיטת מח״פ נדרשת אספקה שוטפת של מפתחות כתב־סתרים, שכן השימוש במפתחות הוא חד־פעמי – **משתמשים בהם פעם אחת בלבד**. המפתחות היו בסיווג בטחוני ׳סודי ביותר׳, והושמדו לאחר השימוש. שירות הקשר התארגן לייצור מפתחות, שינועם ליחידות בצורה מאובטחת ובקרה על השימוש בהם ועל השמדתם. מפתחות ל׳עורק׳ בין שתי תחנות הודפסו בשני עותקים עם נייר קופי. מפתחות ל׳רשת׳ של מספר תחנות הודפסו על סטנסיל ושוכפלו במספר העותקים הנדרש.[10] כל עותק היה מסומן וממוספר, ונוהל תחת פיקוח ומעקב מייצורו עד השמדתו.

מפתחות כתבי־סתרים יוצרו בחוברות של 20 דפים, בכל דף היו 20 עד 25 שורות, בכל שורה שש ׳חמישיות׳, כאשר ה׳חמישייה׳ הראשונה בשורה הייתה ׳חמישיית סימון׳, ויתר ה׳חמישיות׳ בשורה היו ׳חמישיות מפתח׳. היו ׳חוברות עורק׳ ו׳חוברות רשת׳, כאשר השוני ביניהן היה ב׳חמישיית סימון׳: ׳חמישיית סימון׳ בחוברת עורק הייתה חמישייה אקראית. ׳חמישיית סימון׳ בחוברת רשת הייתה ׳סדרתית׳, כדי להקל על זיהוי המפתח בעת קליטת הודעה.

דדדדא	**מדקלע**	**קלXקפ**	**בדועת**	**אלגצק**	**רהלYב**
דדדדב	**סוקמל**	**גלרסח**	**הלבFo**	**יכורת**	**בספזג**
דדדדג	**פנהעו**	**סערצד**	**לצאדה**	**יתחכז**	**תכואב**

דוגמת שורות מפתח מח״פ מ׳חוברת רשת׳

להמחשה – הודעה גלויה:

מאת: חטיבה 10, אל: אוגדה 56. גדוד 83 הגיע לצומת מרידית בשעה 2000.

תרשם כך, בחוברת כתב־הסתרים:

					לרYיפ
דדדדא	**מדקלע**	**קלXקפ**	**בדועת**	**אלגצק**	**רהלYב**
	מחטXע	שרFלא	ולXחמ	dXeee	דXeאו
דדדדב	**סוקמל**	**גלרסח**	**הלבFo**	**יכורת**	**בספזג**
	נהשfe	Fהגיע	Fלצוא	תFארי	דיתFפ
דדדדג	**פנהעו**	**סערצד**	**לצאדה**	**יתחכז**	**תכואב**
	שעהFע	שריאא	פסאפס		

וההודעה המוצפנת ב׳חמישיות׳, המתחילה בשתי ׳חמישיות סימון׳, נראית כך:

טהטהט טפתגפ אתכנא Xצבחפ תבחטי וחרפ פגפאת בבXבפ וחצוב חאייכ

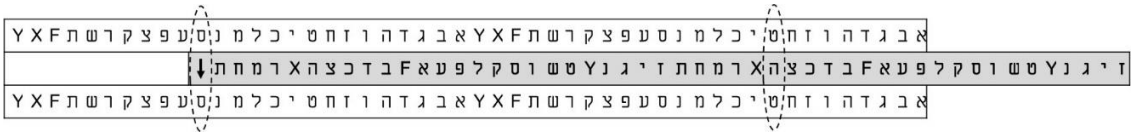
ננקאא Xושיפ תXאקע רתכוד שדאאע

[10] סטנסיל הוא שעוונית דקה עליה הדפיסו במכונת כתיבה ללא סרט דיו. מקשי מכונת הכתיבה נקבו חירורים בשעוונית בצורת האותיות. השעוונית הועברה למכונת שכפול שהייתה מבוססת על גליל דיו עליו הוצמדה השעוונית. סיבוב הגליל הטביע את הדיו על נייר דרך החירורים בשעוונית.

חמישיות הסימון נקבעו כך:

- 'חמישיית הסימון' הראשונה סימנה את הרשת או העורק בהם הוצפן המברק. לרשת בדוגמה נקבעה אות הסימון **ס**, שהפכה לצמד האותיות **טה** בעזרת כלי עזר שכונה בק-105, וחזרו על עצמן 'פעמיים וחצי'.
- 'חמישיית הסימון' השנייה הייתה סימון השורה בה החלה הצפנת ההודעה, כמו שהיא הופיעה בחוברת עורק (שם סימון השורה היה חמישייה אקראית), או כשהיא מוצפנת עם בק-100 מחוברת רשת (שם סימון השורה היה חמישייה סדרתית).

בק-105 היה סרגל מקרטון קשיח עם שלושה מסלולים: במסלול העליון ובמסלול התחתון נרשמו פעמיים כל 25 האותיות; במסלול האמצעי הונחה שורה שנחתכה מגיליון חודשי, בו הייתה שורה לכל יום בחודש. בשורה זו היו 50 אותיות מעורבלות אקראית, ובצידה השמאלי חץ שהצביע כלפי מטה. החץ הצביע על האות המסמנת את הרשת בה הוצפן המברק (בדוגמה: האות **ס**), והצפן בחר אקראית צמד אותיות, אחת מהמסלול העליון והשנייה מתחתיה במסלול האמצעי, כבסיס ל'חמישיית הסימון' הראשונה.



הצפנת חמישיית הסימון הראשונה עם בק-105

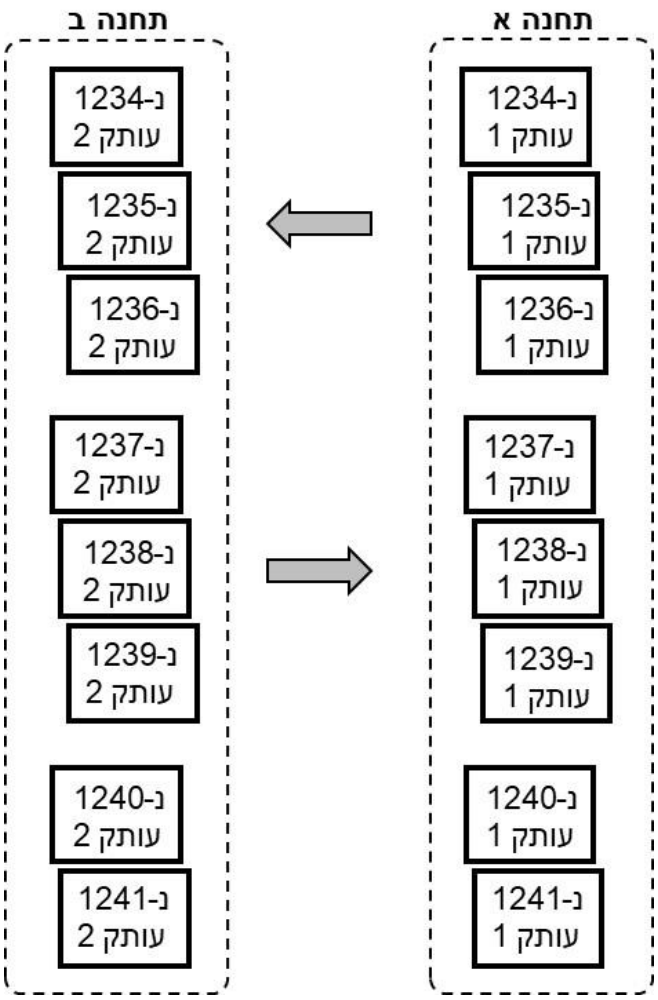
לצורך הפענוח נדרש לזהות את הרשת (או את העורק) של כתב־הסתרים, לזהות את השורה בה החלה הצפנת ההודעה, ואז ניתן היה לרשום את החמישיות המוצפנות בחוברת כתב־הסתרים, ולרשום את ההודעה המפוענחת בטופס מברק.

תהליכי ההצפנה והפענוח היו איטיים, וכדי לזרז את התהליך, הצפנים למדו בעל־פה את 625 הצירופים של טבלת ויז'נר, ולמעשה השתמשו בטבלה רק במקרים של ספק או טעות.

לא חסרו טעויות בפענוח: טעויות אנוש בהצפנה או בפענוח או שיבושים בקליטה. צפנים מיומנים הצליחו להתגבר במהירות על התקלות, ולבקש שידור חוזר של ההודעה רק במקרים מעטים.

ארגון מפתחות מח"פ

ארגון חוברות מפתחות מח"פ היה נושא חשוב כדי להבטיח תעבורה תקינה ולמנוע שיבושים. תחנה קיבלה תמיד את החומר באותו מספר עותק (לדוגמה: תחנה מסוימת הייתה מקבלת תמיד את עותק מס' 2). חוברות מסוימות הוקצו לתעבורה מתחנה **א** לתחנה **ב** ואחרות לתעבורה מתחנה **ב** לתחנה **א**, ותמיד הוכנו ונשמרו חוברות רזרביות. האיור הבא מציג את שיטת הקצאת חוברות המפתח בעורק בין שתי תחנות:

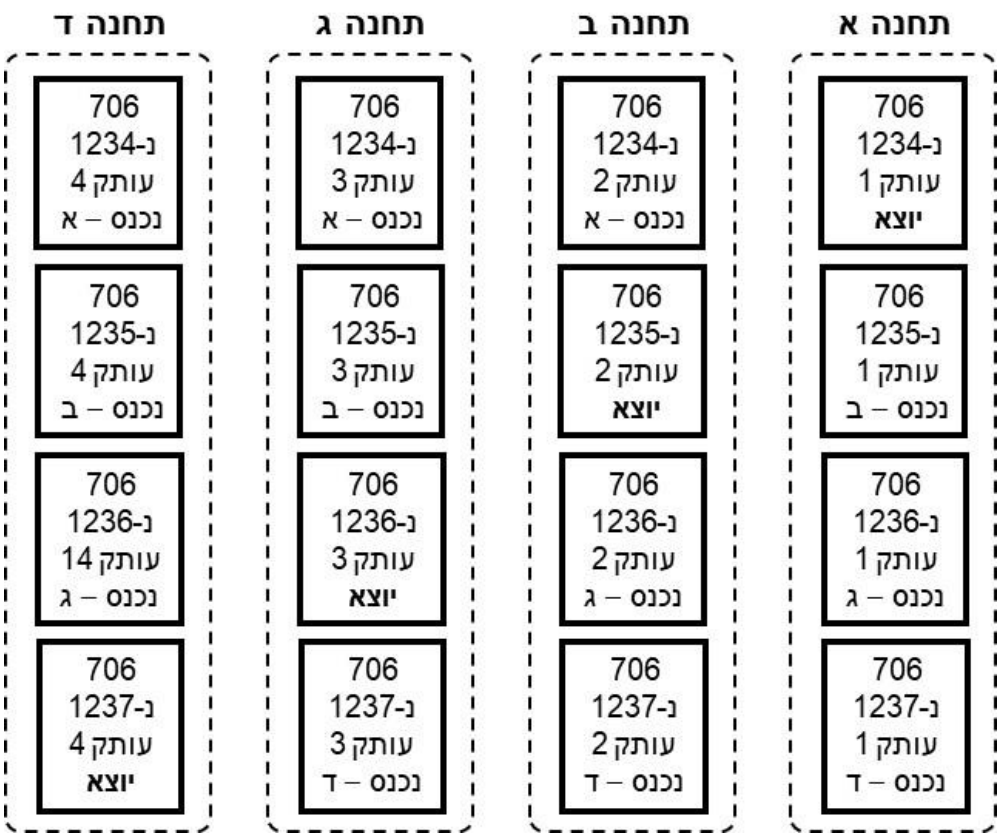


חלוקת חוברות מפתח בעורק מח"פ

הצפנים היו מתחילים להשתמש בחוברת הראשונה בסדרה, וכשהיא 'התמלאה', הם עברו לחוברת הבאה בסדר רץ. כאשר החוברות 'מולאו', עברו לחוברת הרזרבית הראשונה. הצפנים היו מדווחים על כל חוברת ש'התמלאה', ומקבלים 'הוראת הקצבה' לחוברת הבאה ו'הוראת השמדה' לחוברת ש'התמלאה'. כאשר תחנה הייתה מקבלת 'הוראת הקצבה', הצפן היה רושם על החוברת את ייעודה. להמחשה, לפי הדוגמה באיור: עם קבלת 'הוראת הקצבה' לחוברת נ-1240, היו רושמים עליה בתחנה א '**יוצא לב**', ובתחנה ב '**נכנס מא**'.

חלק מהמברקים שהוצפנו במפתח רשת לא היו מיועדים לכל התחנות ברשת, ובחוברות 'נכנסות' נשארו קטעים ריקים (והיו אף מקרים שחוברת שלמה נשארה ריקה). זו הסיבה שחמישית סימון ברשת הייתה חמישייה 'סדרתית' (ולא חמישייה אקראית, כמו בעורק).

ברשת היו מקצים חוברות לתעבורה בין כל אחת מהתחנות ברשת. לדוגמה: ברשת 706, שכללה ארבע תחנות, מציג האיור הבא את שיטת הקצאת חוברות המפתח:



חלוקת חוברות מח"פ ברשת בת ארבע תחנות

כתב־סתרים אלקטרומכני בשיטת מח"פ

כבר ביולי 1949 החל שימוש בטלפרינטרים בצה"ל. טלפרינטר הוא מכונה אלקטרומכנית מורכבת, המאפשרת העברת הודעות מודפסות בטקסט רגיל, בדומה למכונת כתיבה: בתחנה המשדרת מפעיל מקיש אותיות על לוח מקשים במשדר, ומקלט בתחנה הקולטת מדפיס את האותיות הנקלטות על דף נייר או על סרט נייר דביק.

הטלפרינטרים השתמשו בקוד בּוֹד (Baud Code), המבוסס על מילה קבועה בת חמש סיביות. בקוד רק 32 סימנים, וכדי לתמוך בכל מרחב התווים שולב בטלפרינטר מנגנון הסטה ונעילה, שאיפשר מיתוג בין שני מרחבי סימנים, 'אותיות' ו'ספרות' (בדומה למקש היסט (Shift) במקלדת המחשב של היום), עם 26 סימנים בכל מרחב. יישום הקוד בטלפרינטרים בצה"ל כלל אותיות, ספרות, סימני פיסוק ומספר מוגבל של סימונים נוספים. בטלפרינטרים בשימוש צה"ל לא היו אותיות סופיות (בשונה מטלפרינטרים של הדואר האזרחי) ובמקומן היו ארבע אותיות לועזיות (F, V, X, Y).

הטלפרינטרים הראשונים בחיל הקשר היו טפ-2 (דגם T2 תוצרת אוליבטי, איטליה), וערב מלחמת סיני החל שימוש בטפ-3 (דגם LO-15 תוצרת לורנץ, גרמניה), שהדפיסו על גליל נייר רחב (בדרך כלל השתמשו בגליל נייר בו שולב נייר פחם, והדפיסו מברקים בשני עותקים). בטלפרינטרים היה 'מחורר' שייצר סרט נייר מנוקב עם תוכן ההודעה.

בטפ-2 לא היה משדר לסרטי נייר מנוקבים ('משדר אוטומטי', בעגה של אז). כל הטלפרינטרים המתקדמים יותר כללו משדר כזה.

בתחילת שנות ה־60 החל שימוש בטלפרינטר קטן מוקשח ומותאם לעבודה בתנאי שדה, טפ-4 (דגם T68 תוצרת סימנס, גרמניה), שהדפיס על סרט נייר דביק שאותו הדביקו על טופס מברק, ייצר סרט נייר מנוקב וכלל משדר לסרטי נייר מנוקבים.[11]

מס' ההרכב (Combination No.)	ייצוג בינרי (משמאל לימין)	אותיות (Letters)		ספרות (Figures)
		עברית	לועזית	
1	11000	ש	A	-
2	10011	נ	B	?
3	01110	ב	C	:
4	10010	ג	D	לא בשימוש
5	10000	ק	E	3
6	10110	כ	F	!
7	01011	ע	G	לא בשימוש
8	00101	י	H	לא בשימוש
9	01100	X	I	8
10	11010	ח	J	|
11	11110	ל	K	)
12	01001	ת	L	(
13	00111	צ	M	.
14	00110	מ	N	,
15	00011	Y	O	9
16	01101	פ	P	0
17	11101	V	Q	1
18	01010	ר	R	4
19	10100	ד	S	פעמון (Bell)
20	00001	א	T	5
21	11100	ו	U	7
22	01111	ה	V	;
23	11001	F	W	2
24	10111	ס	X	/
25	10101	ט	Y	6
26	10001	ז	Z	"
27	01000	החלף שורה (Line Feed)		
28	00100	רווח (Space)		
29	00010	החזר עגלה (Carriage Return)		
30	11011	ספרות (Figures)		
31	11111	אותיות (Letters)		

קוד בו"ד בשימוש צה"ל

[11] המכשירים הראשונים שסופקו היו בצבע שחור, ולכן כונה המכשיר 'כושי'.

לימוד טלפרינטר טפ-3 בבה"ד 7, 1959
צלם: פוקס. באדיבות ארכיון צה"ל ומערכת הביטחון, אוסף במחנה 1, 2439/84

טלפרינטר טפ-4 בתיבת קשר
משמאל לטלפרינטר התקן להרטבת סרט הנייר הדביק לשם הדבקתו על טופס מברק.
מקור: אוסף העמותה להנצחת חללי חיל הקשר והתקשוב

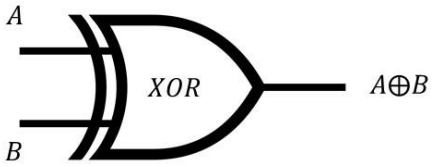
בתחילת שנות ה־50 החל שימוש במכונות הצפנה אלקטרומכניות בשיטה של מח"פ להצפנת תעבורת טלפרינטר. מכשיר ההצפנה האלקטרומכני הראשון, שכונה טג-2022, פעל בשיטה לא מקוונת (Off-line) – טלפרינטר שהיה מחובר למכונת הצפנה הפך הודעה גלויה להודעה מוצפנת על סרט נייר מנוקב, ששודרה בטלפרינטר אחר, או קיבל הודעה מוצפנת על סרט נייר מנוקב, שנקלטה בטלפרינטר אחר, והפך אותה להודעה גלויה.[12] כדי למנוע טעויות אנוש, השתמשו בסרטי נייר

[12] דניאל רוזן, מיכאל נגל, **שבעים שנות חיל הקשר והתקשוב: מערכות, שיטות ואמצעים**, העמותה להנצחת חללי חיל הקשר והתקשוב, יהוד־מונוסון, מהדורה שנייה, התשע"ט – 2018 (להלן: **רוזן ונגל, שבעים שנות חיל הקשר**

אדומים להודעות מסווגות (לפני הצפנה או לאחר פענוח), ובסרטי נייר צהובים להודעות המוצפנות, שאינן מסווגות.

טג-2022 הצפין בשיטה של מח״פ, כאשר גם המפתח היה סרט נייר מנוקב. המכשיר נבנה משני משדרים אוטומטיים, כאשר במשדר אחד הוכנס סרט נייר מנוקב של המפתח ובמשדר השני הוכנס סרט נייר מנוקב של ההודעה (סרט גלוי לצורך הצפנה, סרט מוצפן לצורך פענוח). טלפרינטר שהיה מחובר לטג-2022 ייצר סרט נייר מנוקב מוצפן לצורך שידור לתחנה הנגדית, או שהדפיס את ההודעה המפוענחת.

שיטת ההצפנה הייתה צירוף בינרי בין המפתח להודעה בדרך של ביצוע פעולת XOR בנפרד על כל אחת מחמש הסיביות של קוד בוד – סיבית המפתח מול סיבית ההודעה הגלויה לצרכי הצפנה, מול סיבית ההודעה המוצפנת לצרכי פענוח.



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

מכשיר הצפנה טג-2022
מקור: אוסף העמותה להנצחת חללי חיל הקשר והתקשוב

בשלהי שנות ה־50 הוכנס לשימוש ביחידות השדה מכשיר הצפנה אלקטרומכני, טג-352, שכינויו היה ׳אפרוח׳ (הוא כונה גם ׳שיטה 9׳). מכשיר זה עשה שימוש בטלפרינטר טפ-4 ושני משדרים

והתקשוב), עמ׳ 143–147; המכשירים היו מסוגלים טכנית לפעול גם בשיטה מקוונת (on-line), אך עקב מבנהו הפשוט של המכשיר והעדר מנגנון לטיפול בתקלות (כמו ׳תקיעת׳ סרט המפתח) הוחלט להפעילו רק בשיטה לא־מקוונת.

אוטומטיים (אחד נועד לסרט מפתח, השני נועד להודעה הגלויה להצפנה או להודעה המוצפנת לפענוח) והורכב בארגז עץ כבד, בו הורכבו הטלפרינטר, המשדרים האוטומטיים ויחידת מערכת לוגית ('מוח', בעגה של אז). מכסה הארגז נפתח כשולחן עבודה. טג-352 מימש הצפנת מח"פ על פי טבלת ויז'נר של 25 אותיות, ואפשר היה להצפין/לפענח מול מכשיר טג-352 אחר או מול הצפנה/פענוח ידניים – למכשיר היו שני מצבי עבודה: **ידני**, כאשר המפעיל הקליד מברקים מוצפנים שנקלטו באלחוט מורס, והם פוענחו והודפסו על סרט נייר דביק (שהודבק על טופס מברק), או שהמפעיל הקליד מברקים גלויים והם הוצפנו והודפסו על סרט נייר דביק, כאשר המכונה ייצרה 'רווח' אחרי כל חמש אותיות טקסט מוצפן, כדי שהמברק המוצפן יתאים לשידור חמישיות במורס; **אוטומטי**, כאשר המכשיר מצפין או מפענח מתוך סרטי נייר מנוקבים. המערכת הלוגית במכשיר מומשה באמצעות ממסרי כספית (Mercury Relay), והיה חשוב להעמיד את המכשיר על משטח אופקי (משימה לא פשוטה בתיבת קשר בשדה), כדי שיפעל כהלכה.[13]

הכנסת ציוד הצפנה אלקטרומכני ליחידות השדה הייתה שינוי של ממש ב'תנאי העבודה' של הצפנים: כאשר ההצפנה הייתה ידנית, הצפנים פעלו מאוהלים, עם תאורה בעששיות נפט. המעבר להצפנה אלקטרומכנית חייב להתקין את הציוד בתיבות קשר, עם אספקת חשמל ותאורה חשמלית, שיפור ניכר ב'תנאי העבודה' בשדה.[14]

באוגוסט 1968 הופעלו מכשירי הצפנה אלקטרומכניים טג-1000 ראשונים, שהחליפו בהדרגה את השימוש בטג-2022. טג-1000 פעל אף הוא בשיטה של מח"פ כמו טג-2022, והופעל בעיקר באופן מקוון (On-Line), בו הקשה על מקש בצד המשדר גרמה להצפנה, משלוח האות למקלט בצד השני של העורק ופענוח מיידי של האות והדפסתו, כך שנמנע הצורך להעביר סרט מחדר הכ"ס לחדר הטלפרינטרים, ומהירות העברת המברקים גדלה.

בטג-1000 מומשה מערכת לוגית עם טרנזיסטורים – חידוש טכנולוגי מהותי באותה עת. טג-1000 פעל רק בקווי נקודה־לנקודה, עם 'מפתחות עורק'.

---

13 לראשי צוות הפיתוח (רס"ן אלכס רוזן, סרן צבי ורדיאל וע"צ (לימים אל"ם) זאב מילוא) הוענק פרס בטחון ישראל בשנת 1960. הכוונה המקורית הייתה להדפיס חוברות מח"פ תואמות, כך שתתאפשר הצפנה ידנית ופענוח מכני, או הצפנה מכנית ופענוח ידני, אך רעיון זה לא יושם מעולם.

14 חיל הקשר והתקשוב החל להתקין מזגנים בתיבות קשר רק מתחילת שנות ה־90.

מכשיר הצפנה טג-1000
מקור: אוסף העמותה להנצחת חללי חיל הקשר והתקשוב

ייצור כתבי־סתרים

בשנות צה״ל הראשונות הופקו ונוהלו כתבי־סתרים במדור ביטחון, שקם בפיקודו של שאול בר־לבב (לימים רס״ן), והיה חלק מענף מבצעים במפקדת שירות הקשר (שהפך לחיל הקשר באוקטובר 1948). ביוזמת ישעיהו (אישי) לביא (לימים אל״ם, מפקדו הרביעי של חיל הקשר), הוקם בשנת 1954 ׳מפעל׳ לייצור כתבי־סתרים כיחידה צבאית נפרדת. מפקדה הראשון של היחידה היה ע״צ (עובד צה״ל) זיגמונט (זיגי) מנדל.

היחידה התפתחה להיות ׳מפעל לאומי׳ לייצור, כריכה, בדיקה, סימון, אריזה, הפצה, מעקב והשמדה של מפתחות כתב־סתרים. בשנות ה־50 וה־60 הפעילה היחידה ׳פלוגה ידנית׳, שייצרה מפתחות כתב־הסתרים להצפנה ידנית וקודים שונים שהיו אז בשימוש, ׳פלוגה מכנית׳, שייצרה מפתחות כתב־סתרים להצפנה אלקטרומכנית, ׳פלוגת רישום׳ שעסקה בהפצת מפתחות כתב־סתרים, רישומם ומעקב אחריהם. כן פעלו ביחידה מחלקת מחשב, מחלקת דפוס, מחלקת אפסנאות (שעיסוקה העיקרי היה רכש ואספקה של חומרי הגלם לייצור המפתחות), מחלקה טכנית (לאחזקת המכונות והציוד), מחלקת הנדסת ייצור, קצין תקציבים וקצינת ח״ן. עיקר כוח האדם היו חיילות צפניות, ואזרחיות עובדות צה״ל מילאו את רוב התפקידים הבכירים. ביטחון המידע ביחידה היה קפדני, וכלל מידור בין הפונקציות השונות, כך שכל חייל ומפקד ביחידה הכיר רק את תחום אחריותו, על בסיס ׳הצורך לדעת׳.

מפתחות כתב־סתרים עברו בקרת איכות קפדנית. כך למשל: הצפניות ב׳פלוגה ידנית׳ בדקו כל אות, כל חמישייה, כל שורה וכל דף, כדי לוודא שכל האותיות ברורות ואין שיבושים. כל דף בו נמצא פגם הושמד. מאמץ מיוחד הוקדש כדי להבטיח שמח״פ אכן יהיה אקראי.

הכשרה, אבטחה, תפעול, תחזוקה ולוגיסטיקה

הטיפול בכתב־סתרים היה משימה מרכזית בשירות הקשר ובחיל הקשר. חיילות וחיילים נבחרו בקפידה למקצוע צפן, ועברו הכשרה מקיפה בבסיס ההדרכה של החיל, במדור מיוחד, שהיה מבודד וממודר מיתר הפעילות בבסיס ההדרכה. מאמצים רבים הושקעו בהקניית 'תודעת ביטחון' לצפניות ולצפנים, שדרך תוכן ההודעות שהעבירו היו חשופים לסודות הכמוסים של צה"ל.

פעילות כתב־סתרים ביחידות הצבא נעשתה בחדרים מיוחדים שיועדו לכך, חדרי כ"ס, בהם נשמרו גם מפתחות כתבי־סתרים. חדרי הכ"ס היו חדרים מאובטחים ונעולים, שאויישו 24 שעות ביממה, בכל ימות השנה. לחדרים אלה יכלו להיכנס רק שותפי סוד מעטים: הצפניות והצפנים ששירתו ביחידה ומספר מצומצם של מפקדים בכירים. נוהלה בקרה קפדנית על הפעילות בחדרי הכ"ס ועל מפתחות כתב־סתרים.

בשנות צה"ל הראשונות הייתה הפרדה מוחלטת בין חדרי הכ"ס לבין חדרי האלחוט וחדרי הטלפרינטר, ובין חדר הכ"ס לחדר האלחוט או לחדר הטלפרינטר עברו רק הודעות מוצפנות (הודעות ב'חמישיות' שנקלטו או שיועדו לשידור באיתות מורס; סרטי נייר מנוקבים שנקלטו או יועדו לשידור בטלפרינטר). הדבר השתנה עם השימוש בטג-1000 והמעבר להצפנה מקוונת, שכן הטג-1000 עם הטלפרינטר הצמוד לו הותקנו בחדר הכ"ס.

ההודעות המסווגות הועברו מהמשתמשים לחדר הכ"ס ומחדר הכ"ס למשתמשים כשהם ארוזים במעטפות כפולות, כאשר המעטפה הפנימית חתומה בחותמת שעווה אדומה ייעודית ('גושפנקא', בעגה של אז).

שינוע מפתחות כתב־סתרים מה'מפעל' בו יוצרו למחסני מפתחות כתב־סתרים מרחביים ולחדרי הכ"ס ביחידות נעשה תחת בקרה ואבטחה.

לכל מכשיר הצפנה היה מספר סידורי מזהה, ונוהל רישום ומעקב קפדני אחרי מיקומו. המכשירים שלא היו בשימוש בחדרי כ"ס נשמרו במחסנים מיוחדים, מסווגים ומאובטחים. האפסנאים והטכנאים שטיפלו בציוד עברו בדיקה ביטחונית ייחודית, למדו להכיר את המכשירים והוסמכו לטפל בהם.

סיכום

ה'אסון' של שנת 1946 גרם לבכירי שירות הקשר להיות שמרנים וזהירים, והביא להשקעה מהותית של משאבים ואמצעים בכתבי־סתרים. בשנותיו הראשונות של צה"ל מוסדו השימושים בכתב־סתרים והמערכת התומכת בהפעלתם.

בשנות צה"ל הראשונות, כתבי־סתרים עיקריים היו 'תשבץ' לדרג הלוחם, מח"פ ידני או אלקטרומכני לכל יתר השימושים.

השימוש בכתבי־סתרים טרם הקמת המדינה, בתקופה בה שירות הקשר פעל כארגון חשאי, אופיין במפתחות הצפנה 'קצרים' שהוחלפו בתדירות נמוכה. המעבר למח"פ עם הקמת צה"ל היה שיפור מהותי באיכות וביטחון כתבי־הסתרים. המעבר משימוש בכתבי־סתרים ידניים לשימוש בכתבי־סתרים אלקטרומכניים היה אף הוא מבוסס על מח"פ.

ההכשרה המקצועית של הצפניות והצפנים הייתה יסודית ומעמיקה. הפיקוח והבקרה על ייצור, שינוע, שימוש והשמדה של כתבי־סתרים היו הדוקים ומקיפים.

אירוע ההצטיידות במכונות הצפנה 'אניגמה' (טג-356) ערב מבצע סיני מעלה סימן שאלה – עד כמה היו מומחי חיל הקשר,[15] בשנותיו הראשונות, מודעים לחולשות של מנגנוני כתב־סתרים 'אקראיים לכאורה' בטכנולוגיות האלקטרומכניות של אותה תקופה,[16] ולאפשרות 'שבירתם' ופענוח המידע העובר בהם בידי יריבים?

ביטחון המידע בצה"ל בשנותיו הראשונות שונה לחלוטין מביטחון המידע של צה"ל של היום: בשנות צה"ל הראשונות, התקשורת המסווגת העיקרית הייתה העברת מכתבים באמצעות הדואר הצבאי, ורק תקשורת דחופה הועברה במברקים, שרובם הוצפנו. בעידן המודרני, ציוד קשר ומערכות מידע נמצאים בשימוש נרחב, צה"ל חי ולוחם ברשת (מרחב סֶבֶ"ר – Cyberspace), והגנת מרחב הרשת היא לא רק הצפנת תקשורת, אלא מכלול שלם של אמצעים.

כתבי־סתרים בשימוש צה"ל השתכללו במהלך השנים, ואינם דומים לכתבי־סתרים ששימשו בשנות צה"ל הראשונות, אך חשיבותם נשארה כשהייתה, וההתלבטות בשאלה עד כמה ניתן לבטוח בהם נשארה בעינה.

---

15 המפורסמת בין מכונות ההצפנה האלקטרומכניות בשיטות 'אקראיות לכאורה' שהתעבורה בהם פוענחה בידי יריבים היא מכונת ה'אניגמה' הנאצית, שהופעלה במלחמת העולם השנייה. חיל הקשר הצטייד ב־50 מכונות כאלה לפני מלחמת סיני, הסב אותם לעברית, אך מעולם לא הפעילן. **רוזן ונגל, שבעים שנות חיל הקשר והתקשוב**, עמ' 145־146.

16 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.