WWII Turkish & Allied Archival Cipher Corpus (1939–1945): The 1877 Ottoman Zero-Free 81-Cell Cipher Reborn in the 1939 Republican «YASA» Key

Presidency State Archives of Turkey (BCA, MSB ATASE & Foreign Ministry TDA) 1939–1945 Survey · 1939 «YASA» 81-Cell Zero-Free Homophonic Cipher Key · 1940 RAF Sliding-Strip Weather Cipher & 1942 Alexandria (MTCI) Undeciphered Radio Ciphers

149 Records	81 / 81 Cells	1877 → 1939	92 Groups	10^5 Keys
1939–1945 BETSİS cipher inventory	1939 «YASA» zero-free matrix (11..99)	62-year Ottoman–Republican continuity	1942 Alexandria undeciphered radio ciphers	1940 RAF sliding-strip weather cipher

1. Major Cryptological Discovery: Unbroken Structural Continuity from the 1877 Ottoman 81-Cell Zero-Free Matrix to the 1939 WWII «YASA» Cipher

Our survey of World War II (`1939–1945`) cipher files in the Turkish Republican Archives (`BCA`) revealed an extraordinary continuity in cryptographic engineering: the **`81`-cell zero-free (`11..99 \ *0`) two-digit homophonic cipher architecture** created by the Sublime Porte Cipher Bureau under Sultan Abdülhamid II during the **1877–1878 Russo-Ottoman War** and used through **1884 (Eastern Rumelia)** was preserved intact by the Republic of Turkey's Ministry of the Interior on the eve of World War II in the **26 July 1939 «YASA» Cipher Key (`BCA, 30-10-0-0, 65-435-9`)**—newly declassified on 10 July 2025.

Cryptographic Feature	Ottoman Empire (`1877–1884`) *Registers I–IV, Y.MTV. 1/6–10 & Eastern Rumelia*	Republic of Turkey (`26 July 1939`) *«YASA» Codeword Key (BCA 30-10-0-0, 65-435-9)*
Code Space (`81` Zero-Free Numbers)	The **`81` two-digit numbers in `11..99` containing no `0`** (`10, 20, ..., 90`) were banned because the five-dash Morse zero `-----` caused frequent telegraph errors).	**The exact same `81` zero-free two-digit numbers (`11..99 \ *0`)**: the *Kapamak İçin* decryption table skips every multiple of 10 (`19 → 21`, `29 → 31`, ..., `89 → 91`).
Dual-Homophone Allocation	`29` Ottoman letters × `2` codes = `58` active + `23` blank cells (`Y.MTV. 1/6, 9, 10`); in 1884 Eastern Rumelia, `34 × 2 = 68` active + `13` blank cells.	Following the 1928 Latin Alphabet Reform, the **Turkish Latin alphabet** was slotted into the same `81` cells: `24` letters × `2` homophones (`48` codes) + `8` single-code symbols (`Ç, J, P, S, Q, W, X, Comma`) + `6` word-space nulls (`Fasıla`) = **`62` active + `19` blank cells (`81` total)**.
Hidden Mathematical Law	Dual homophones distributed across decades with reserve blank cells.	**Same-Units-Digit Law:** Both homophones of every 2-code letter share the exact same units digit (`A=12/52`, `B=17/67`, `D=28/78`, `E=19/89`, `O=27/87`, `R=45/95`); the **`6` word-space nulls (`15, 26, 37, 48, 59, 91`)** step along the `+11` main diagonal.
Patching the 1877 Word-Boundary Vulnerability	In `1877–1881` (e.g. `DH.ŞFR. 114/11` Prizren), words were separated by `/` slashes or mixed with plaintext, allowing foreign telegraph clerks to break the key via crib-dragging (confessed in `A.}d. 1060` *Ta'rîfnâme Mi=01*).	Rule 3 of the 1939 «YASA» manual patched this exact vulnerability while retaining the 81-cell engine: 1) `6` homophonic word-space nulls (`Fasılalar`) were inserted between words and as leading/trailing padding, and 2) 2-digit codes were paired into **uniform 4-digit telegraph groups** (`1526 9137 1934 2445...`).

Cryptographic Feature	Ottoman Empire (`1877–1884`) *Registers I–IV, Y.MTV. 1/6–10 & Eastern Rumelia*	Republic of Turkey (`26 July 1939`) *«YASA» Codeword Key (BCA 30-10-0-0, 65-435-9)*
WWII Successor Keys (`1939–1945`)	Registers V & VI (`1879–1883` 5-digit planetary codebooks).	Per `BCA 30-10-0-0, 159-118-20, 24, 25` : **«YASA» (July 1939) → «GÜVEN» (1942–43) → «UFUK» (7 Oct 1943 – 5 Jan 1945) → «ÇELİK» (5 Jan 1945+)** and numbered keys `#7, #8, #9, #10` .

Interactive 1939 «YASA» 81-Cell Zero-Free Cipher Matrix (`11..99 \ *0`) & `1877 ↔ 1939` Comparative Simulator

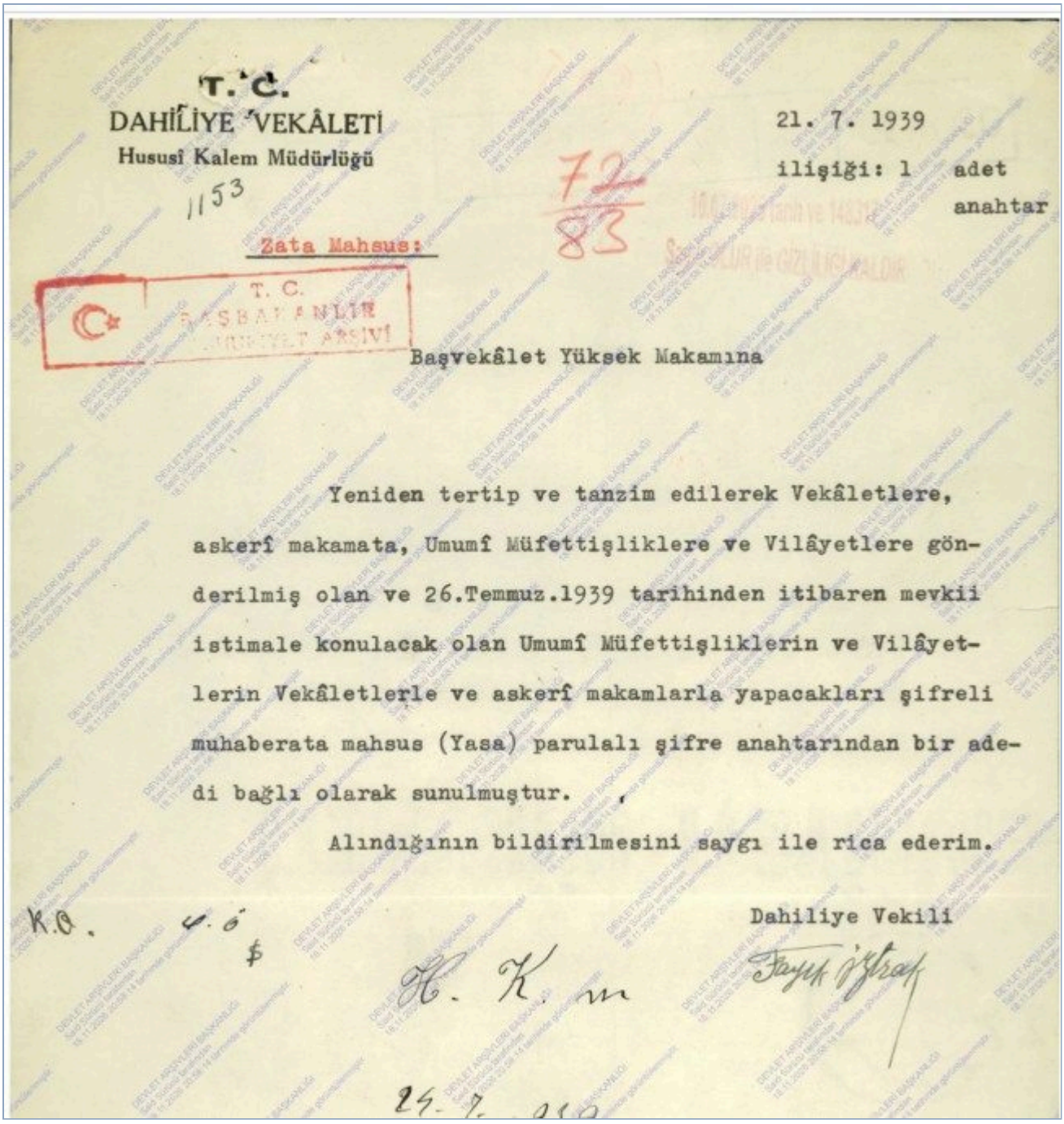
Tens \ Units	·1	·2	·3	·4	·5	·6	·7	·8	·9
1·	11 H	12 A	13 Blank	14 Ç	15 NULL	16 Ş	17 B	18 T	19 E
2·	21 F	22 Blank	23 C	24 İ	25 G	26 NULL	27 O	28 D	29 J
3·	31 L	32 I	33 Blank	34 M	35 K	36 Blank	37 NULL	38 Blank	39 Ö
4·	41 H	42 P	43 Blank	44 N	45 R	46 U	47 Blank	48 NULL	49 Blank
5·	51 L	52 A	53 C	54 Blank	55 Q	56 Blank	57 V	58 Z	59 NULL
6·	61 Blank	62 Blank	63 Ü	64 İ	65 S	66 W	67 B	68 T	69 Ö
7·	71 Blank	72 I	73 Ü	74 Blank	75 G	76 Blank	77 X	78 D	79 Blank
8·	81 F	82 Blank	83 Y	84 N	85 K	86 U	87 O	88 ,	89 E
9·	91 NULL	92 Blank	93 Y	94 M	95 R	96 Ş	97 V	98 Z	99 Blank

2. The «YASA» Cipher Manual & Complete Decipherment of its 18-Group Sample Telegram (21 July 1939)

> **Republic of Turkey, Ministry of the Interior, Private Secretariat — 21 July 1939 (Enclosure: 1 key · Top Secret / Zata Mahsus):**
> "Enclosed is one copy of the newly compiled and arranged cipher key with the codeword (Yasa), which has been dispatched to the Ministries, Military Authorities, Inspectorates-General, and Provincial Governorships and shall enter into force on 26 July 1939 for encrypted correspondence between the Inspectorates-General, Provinces, Ministries, and Military Authorities." — *Minister of the Interior Faik Öztrak*
>
> **«YASA» Operating Instructions (Articles 1–4):**

> “1 — This key is reserved for encrypted correspondence conducted by Provincial Governorships and Inspectorates-General with Ministries and Military Authorities.
> 2 — No copy of this key may be made or carried in one's pocket without the order or permission of the Ministry of the Interior.
> 3 — This key is used in four-digit groups. The two-digit numbers corresponding to the letters to be encrypted are found on the encoding sheet of the key and placed side by side to form four-digit groups. Groups ending with a single two-digit pair are completed into four-digit groups by adding a pause/space number (*fasıla rakamı*). Even if a word ends on a full four-digit group, a space number must mandatory be inserted after every two words.
> **Example:** When the sentence **(Emir alındı ve anlaşıldı — “Order received and understood”)** is encrypted according to these instructions, the following groups are produced:
> `1526 9137 1934 2445 5991 1231 / 7244 7832 5991 5789 3748 5284 / 5112 9672 3128 7237 1526 5948`
> 4 — At the beginning of ciphers locked with this key, the indicator (YA)…”

3. Archival Facsimile Plates («YASA», «GÜVEN», «UFUK», and «ÇELİK» Cipher Keys)



T. C.
DAHİLİYE VEKÂLETİ
Hususî Kalem Müdürlüğü
1153

21. 7. 1939
ilişiği: 1 adet anahtar

72/83

Zata Mahsus:

T. C. BAŞBAKANLIK CUMHURİYET ARŞİVİ

Başvekâlet Yüksek Makamına

Yeniden tertip ve tanzim edilerek Vekâletlere, askerî makamata, Umumî Müfettişliklere ve Vilâyetlere gönderilmiş olan ve 26.Temmuz.1939 tarihinden itibaren mevkii istimale konulacak olan Umumî Müfettişliklerin ve Vilâyetlerin Vekâletlerle ve askerî makamlarla yapacakları şifreli muhaberata mahsus (Yasa) parulalı şifre anahtarından bir adedi bağlı olarak sunulmuştur.

Alındığının bildirilmesini saygı ile rica ederim.

K.O.

Dahiliye Vekili
Faik Öztrak

24. 7. 939

Plate 1 — BCA, 30-10-0-0, 65-435-9, p. 2 (21 July 1939): Cover memorandum signed by Interior Minister Faik Öztrak submitting the «YASA» cipher key to the Prime Ministry prior to its activation on 26 July 1939 (declassified 10 July 2025).

T. C.

Dahiliye Vekâleti

Hususî Kalem Müdürlüğü

872/83

T. C.
BAŞBAKANLIK
CUMHURİYET ARŞİVİ

Yasa

1 — Bu anahtar Vilâyetlerin ve Umumî Müfettişliklerin Vekâletlerle ve Askerî makamlarla yapacakları şifreli muhaberata mahsustur.

2 — Dahiliye Vekâletinin emri veya müsaadesi alınmadıkça bu anahtarın sureti çıkarılamaz ve cepte taşınamaz.

3 — Bu anahtar dörtlü gruplar halinde kullanılır. Şifre edilecek harflerin mukabili olan ikili rakamlar anahtarın kapama levhasından bulunarak yanyana getirilmek suretile dörtlü gruplar haline konulur. İkili olarak biten gruplar fasıla rakamı konulmak suretile dörtlü gruplar haline getirilir. Gruplar dörtlü olarak bitse bile her iki kelimeden sonra mutlaka fasıla rakamı konulmalıdır.

Misal: (Emir alındı ve anlaşıldı) cümlesi bu tarife söre şifre edilince şu gruplar meydane gelir:

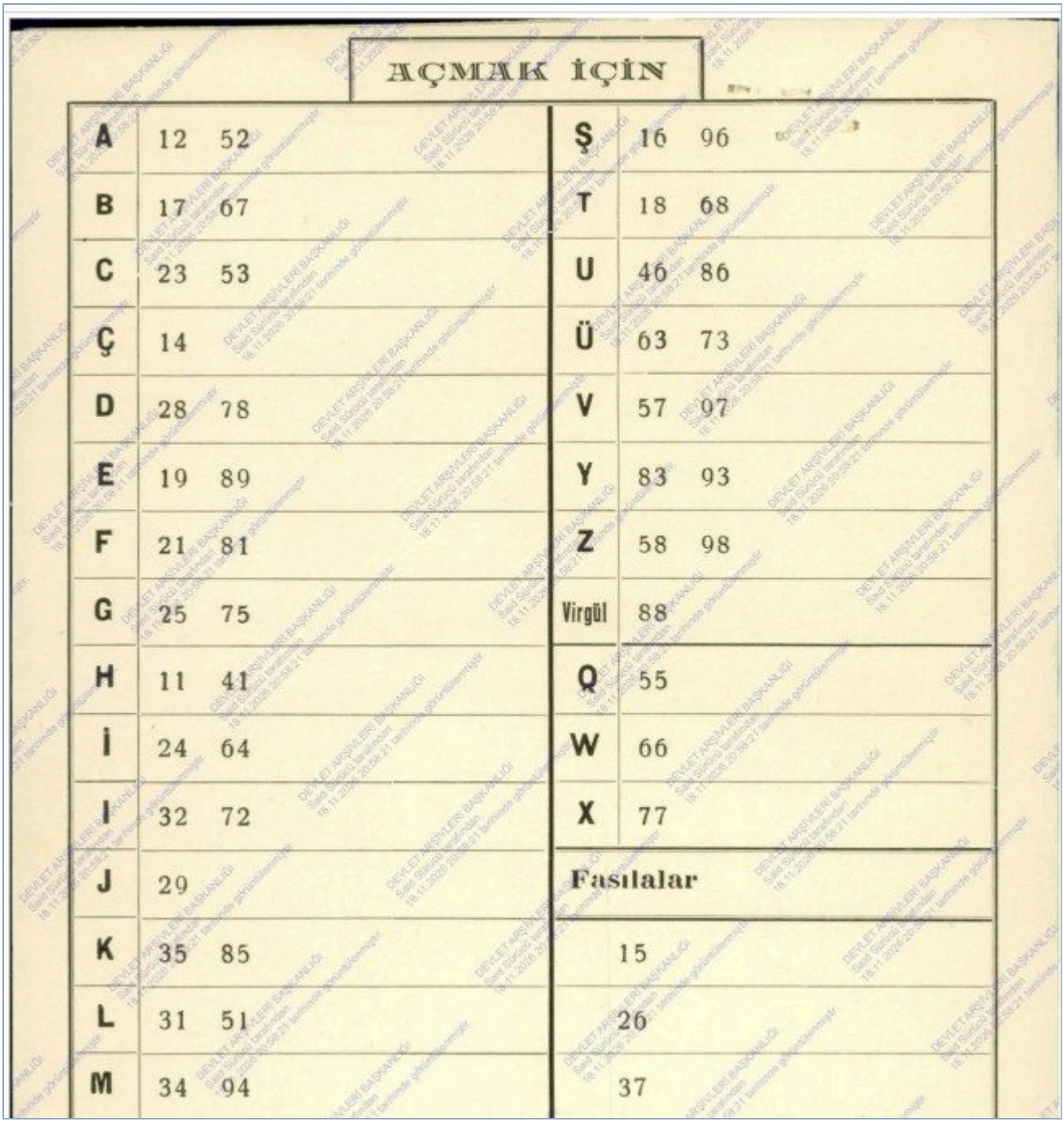
1526 9137 1934 2445 5991 1231

7244 7832 5991 5789 3748 5284

5112 9672 3128 7237 1526 5948

4 — Bu anahtarla kapatılmış olan şifrelerin baş tarafına (YA-

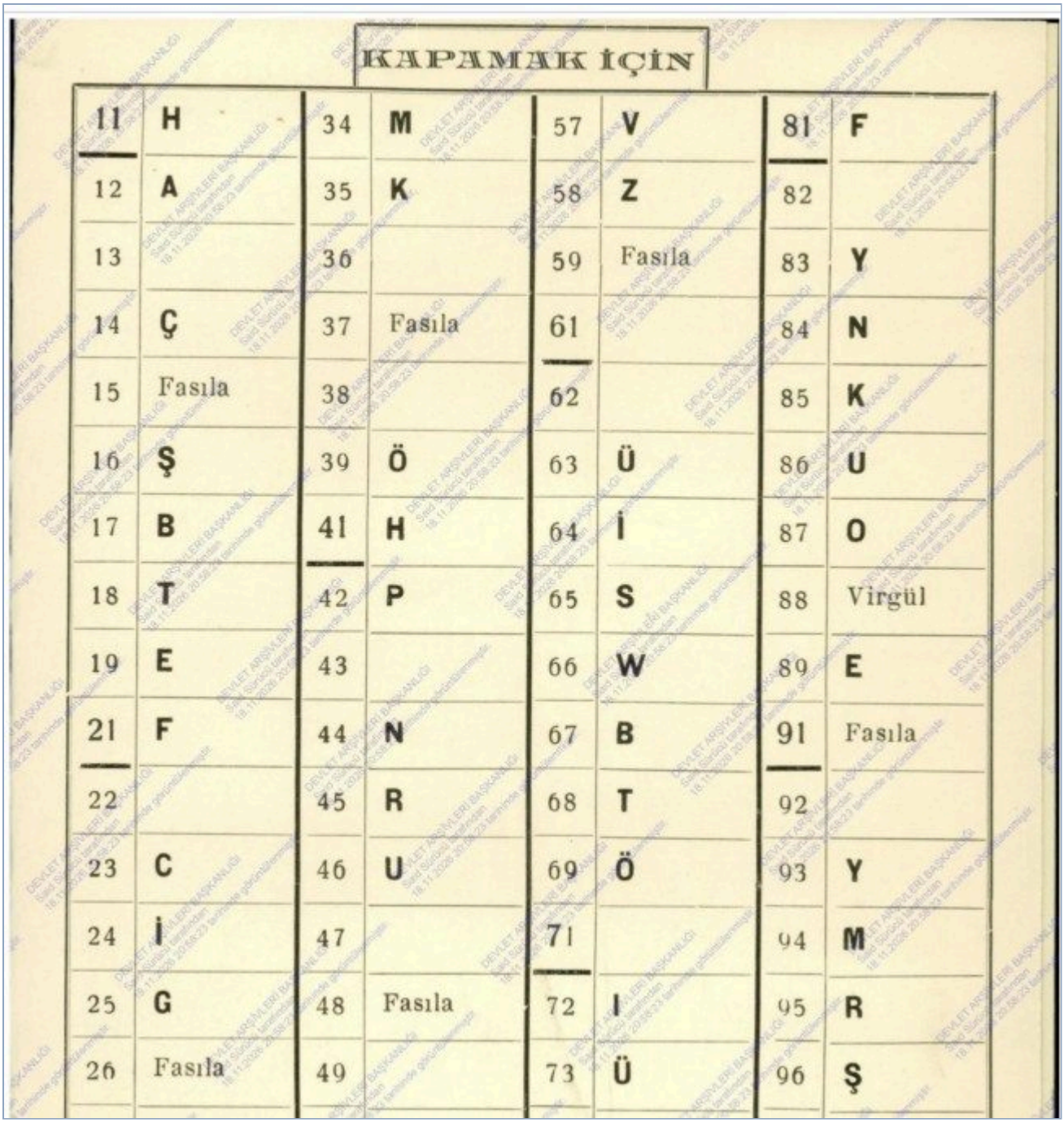
Plate 2 — BCA, 30-10-0-0, 65-435-9, p. 3: Operating instructions explaining the 4-digit grouping and word-space null (*fasıla*) rules, together with the 18-group worked ciphertext example.



AÇMAK İÇİN

A	12	52	Ş	16	96
B	17	67	T	18	68
C	23	53	U	46	86
Ç	14		Ü	63	73
D	28	78	V	57	97
E	19	89	Y	83	93
F	21	81	Z	58	98
G	25	75	Virgül	88	
H	11	41	Q	55	
İ	24	64	W	66	
I	32	72	X	77	
J	29		Fasılalar		
K	35	85	15		
L	31	51	26		
M	34	94	37		

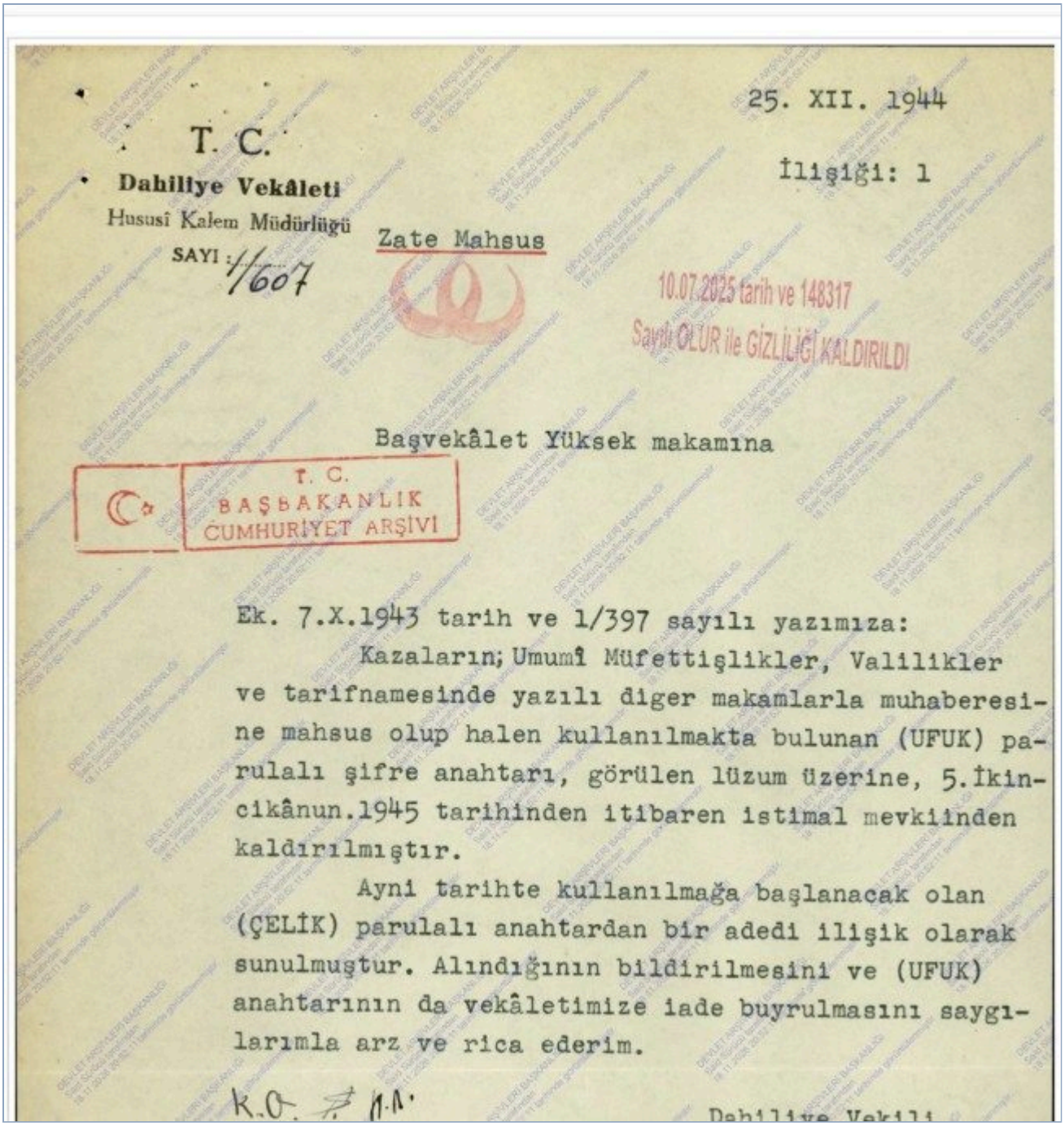
Plate 3 — BCA, 30-10-0-0, 65-435-9, p. 4 (Açmak İçin / Encoding Table): Alphabet table assigning two homophonic zero-free codes per letter under the same-units-digit law (A=12/52, B=17/67, D=28/78, E=19/89…) plus diagonal word-space nulls.



KAPAMAK İÇİN

11	H	34	M	57	V	81	F
12	A	35	K	58	Z	82	
13		36		59	Fasıla	83	Y
14	Ç	37	Fasıla	61		84	N
15	Fasıla	38		62		85	K
16	Ş	39	Ö	63	Ü	86	U
17	B	41	H	64	İ	87	O
18	T	42	P	65	S	88	Virgül
19	E	43		66	W	89	E
21	F	44	N	67	B	91	Fasıla
22		45	R	68	T	92	
23	C	46	U	69	Ö	93	Y
24	İ	47		71		94	M
25	G	48	Fasıla	72	I	95	R
26	Fasıla	49		73	Ü	96	Ş

Plate 4 — BCA, 30-10-0-0, 65-435-9, p. 5 (Kapamak İçin / Decoding Table): Four-column reverse lookup table over the exact 81 zero-free two-digit numbers (`11..99 \ *0`) inherited from the 1877–1884 Ottoman provincial cipher system.



T. C.
Dahiliye Vekâleti
Hususî Kalem Müdürlüğü
SAYI : 1/607

25. XII. 1944

İlişiği: 1

Zate Mahsus

10.07.2025 tarih ve 148317 Sayılı OLUR ile GİZLİLİĞİ KALDIRILDI

T. C. BAŞBAKANLIK CUMHURİYET ARŞİVİ

Başvekâlet Yüksek makamına

Ek. 7.X.1943 tarih ve 1/397 sayılı yazımıza:

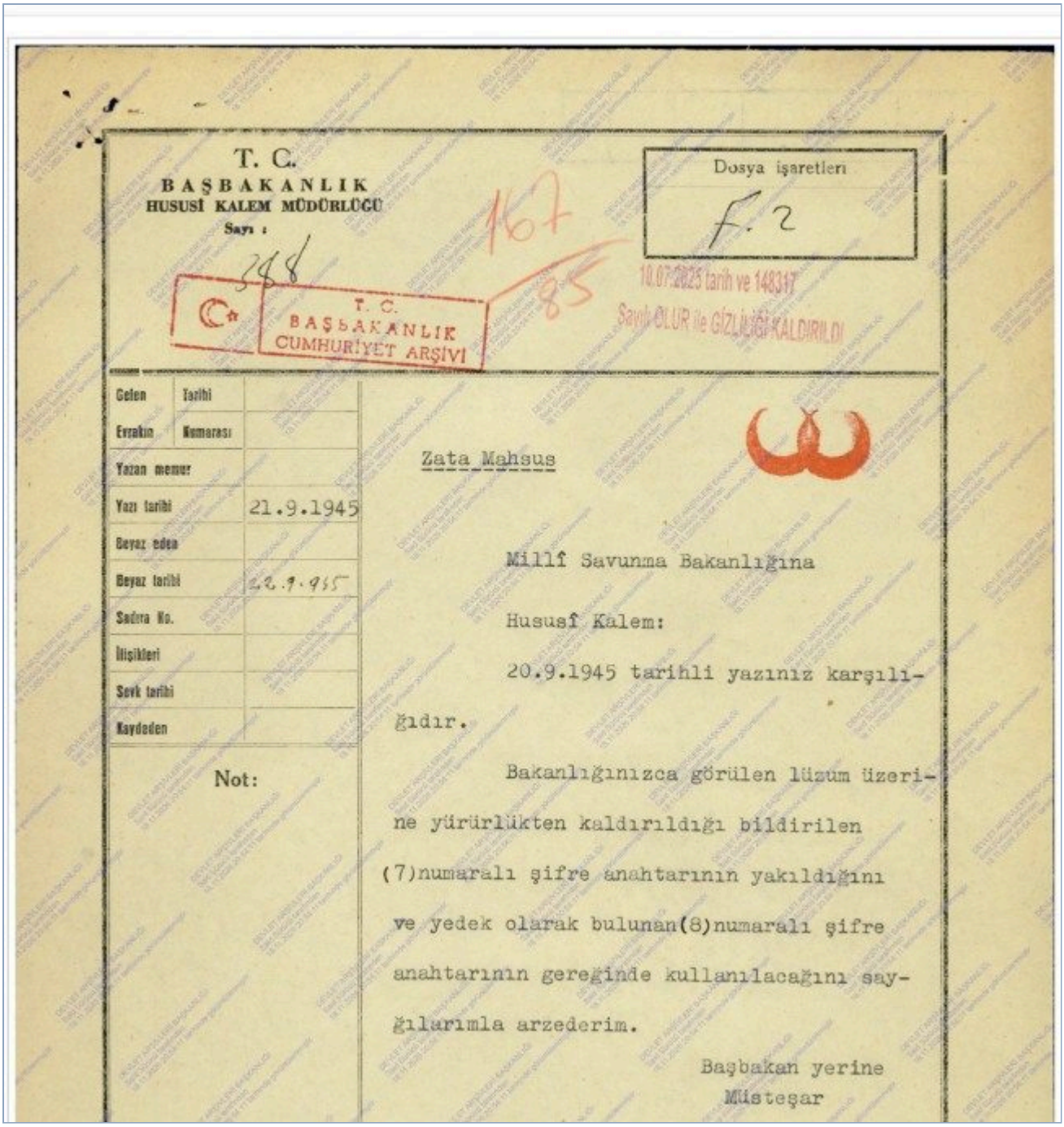
Kazaların; Umumî Müfettişlikler, Valilikler ve tarifnamesinde yazılı diger makamlarla muhaberesine mahsus olup halen kullanılmakta bulunan (UFUK) parulalı şifre anahtarı, görülen lüzum üzerine, 5.İkincikânun.1945 tarihinden itibaren istimal mevkiinden kaldırılmıştır.

Ayni tarihte kullanılmağa başlanacak olan (ÇELİK) parulalı anahtardan bir adedi ilişik olarak sunulmuştur. Alındığının bildirilmesini ve (UFUK) anahtarının da vekâletimize iade buyrulmasını saygılarımla arz ve rica ederim.

K.O.

Dahiliye Vekili

Plate 5 — BCA, 30-10-0-0, 159-118-20, p. 3 (25 December 1944 / 5 January 1945): Secret memorandum retiring the «UFUK» codeword cipher key (active since 7 October 1943) on 5 January 1945 and replacing it with the «ÇELİK» codeword cipher key.



T. C.
BAŞBAKANLIK
HUSUSİ KALEM MÜDÜRLÜĞÜ
Sayı :

Dosya işaretleri
F. 2

167
85

T. C.
BAŞBAKANLIK
CUMHURİYET ARŞİVİ

10.07.2025 tarih ve 148317 Sayılı ÖLUR ile GİZLİLİĞİ KALDIRILDI

Gelen Tarihi	
Evrakın Numarası	
Yazan memur	
Yazı tarihi	21.9.1945
Beyaz eden	
Beyaz tarihi	22.9.945
Sadra No.	
İlişikleri	
Sevk tarihi	
Kaydeden	

Not:

Zata Mahsus

Millî Savunma Bakanlığına

Hususî Kalem:

20.9.1945 tarihli yazınız karşılığıdır.

Bakanlığınızca görülen lüzum üzerine yürürlükten kaldırıldığı bildirilen (7)numaralı şifre anahtarının yakıldığını ve yedek olarak bulunan(8)numaralı şifre anahtarının gereğinde kullanılacağını saygılarımla arzederim.

Başbakan yerine
Müsteşar

Plate 6 — BCA, 30-10-0-0, 159-118-24, p. 2 (22 September 1945): Prime Ministry record certifying the destruction by burning of retired cipher key No. 7 upon activation of key No. 8.

1942 Alexandria (`MTCI`) Undeciphered Radio Cipher Telegrams (No. 142 & No. 145) and the 1939 Berlin (General Mittelberger) Military Cipher

Ministry of National Defense Military History Archive (ATASE) World War II Collection (`110-9-1-14`, Box 2 File 125 & Box 1 File 63)

1. Two Undeciphered Four-Digit Radio Ciphers Received from Alexandria (`MTCI`) by Turkish General Staff Radio (15 April & 11 May 1942)

On the eve of the Battle of Gazala / Tobruk in North Africa, on **15 April 1942** (`03:07`) and **11 May 1942** (`15:05`), the **Turkish General Staff Radio Station (*Genelkurmay Telsizi*)** in Ankara intercepted/received two four-digit encrypted radio dispatches originating from **Alexandria, Egypt (`İskenderiye / MTCI`)**. By direct order of the Chief of the General Staff (Field Marshal Fevzi Çakmak), the 3rd Intelligence Branch forwarded the raw copies undeciphered to the **British Military Attaché** in Ankara.

1.1. Radio Cipher No. 142 (15 April 1942 · 03:07–03:15 · 25 Four-Digit Groups)

```
Origin Station: İskenderiye / MTCI | No: 142 | Sent: 15/4/42 0307 | Received: 15/4/42 031
Stamp: GENELKURMAY TELSİZİ B. 15 NİSAN 1942

27/172360  0419 0926 0774 0230 5648 3055 3363 7221 7901 9521
           3891 4326 3253 8298 6336 1660 8372 3802 8630 2770
           0313 2046 7119 5572 9266/1346 C / 14 .
```

1.2. Radio Cipher No. 145 (11 May 1942 · 15:05–15:12 · 67 Four-Digit Groups)

```
Origin Station: MTCI | No: 145 | Sent: 11/5/942 1505 | Received: 11/5/942 1512
Stamp: GEN. KURMAY TELSİZİ 11-5-1942

3128 2329 6363 8113 9625 9371 8856 9370
7874 2526 4206 2517 0814 0909 4142 7698
2445 6490 0678 0834 2466 9371 3724 8552
6921 2733 0109 7078 4390 6097 1236 6062
0716 9620 8111 2443 4474 9580 0298 0400
8599 7241 8982 3761 0158 3210 0829 9572
8731 4348 9675 0753 1298 7849 5467 1870
1307 3431 6581 4688 0504 4026 5280 3084
3406 5952 2572 = 1228 C / 10
```

2. Cryptanalytic Findings: Protocol Framing, `IC = 0.00927`, and the `d1 == d3` Anomaly

- **Decoded Royal Signals Protocol & Date-Time Groups (`DTG`):** The trailers `/1346 C / 14 .` (No. 142) and `= 1228 C / 10` (No. 145) follow standard British Royal Corps of Signals Date-Time Group syntax: `1346 C / 14` = **14 April 1942, 13:46 hrs, Time Zone `C` (*Charlie* = *GMT+3* Cairo/Ankara time)**; `1228 C / 10` = **10 May 1942, 12:28 hrs, Zone `C` (*GMT+3*)**. In the preamble `27/172360` of No. 142, `27` denotes the total group count (`1` indicator + `25` cipher groups + `1` DTG = `27`), while

`172360` is the 6-digit **superencipherment indicator group** specifying the additive table, page, and starting row/column.

- **Two-Digit Index of Coincidence (`IC = 0.00927`):** Across the `184` two-digit halves (`00..99`) of the `92` four-digit groups, `88` distinct pairs appear (including `00`), yielding `IC = 0.00927` (vs. `0.01000` for uniform randomness). This proves the messages are not unenciphered letter substitutions, but a **British 4-digit military codebook superenciphered with a modulo-10 reciprocating/one-time additive table**.
- **Columnar `9371` Repeat & `d1 == d3` (`22.4%`) Anomaly in No. 145:** In No. 145, the group `9371` repeats twice in Column 6 exactly `16` groups (`2 × 8` rows) apart (Group #6 and Group #22), with `9370` appearing two groups after the first occurrence (Group #8). Furthermore, **`15` of the 67 groups (`22.4%` vs. `10%` random expectation, $p = 0.0018$) share identical 1st and 3rd digits (`d1 == d3` : `2329, 6363, 7874, 2526, 0909, 4142, 0109, 7078, 6062, 0400, 8982, 4348, 3431, 0504, 5952`)** and `21/67` (`31.3%`) satisfy `|BB − AA| <= 9` .

Interactive 1942 Alexandria (`MTCI`) Undeciphered Radio Ciphers Cryptanalysis Lab (`MSB ATASE 110–9–1–14, 2–0–125`)

#1 3128	#2 2329	#3 6363	#4 8113	#5 9625	#6 9371	#7 8856	#8 9370
#9 7874	#10 2526	#11 4206	#12 2517	#13 0814	#14 0909	#15 4142	#16 7698
#17 2445	#18 6490	#19 0678	#20 0834	#21 2466	#22 9371	#23 3724	#24 8552
#25 6921	#26 2733	#27 0109	#28 7078	#29 4390	#30 6097	#31 1236	#32 6062
#33 0716	#34 9620	#35 8111	#36 2443	#37 4474	#38 9580	#39 0298	#40 0400
#41 8599	#42 7241	#43 8982	#44 3761	#45 0158	#46 3210	#47 0829	#48 9572
#49 8731	#50 4348	#51 9675	#52 0753	#53 1298	#54 7849	#55 5467	#56 1870
#57 1307	#58 3431	#59 6581	#60 4688	#61 0504	#62 4026	#63 5280	#64 3084
#65 3406	#66 5952	#67 2572					

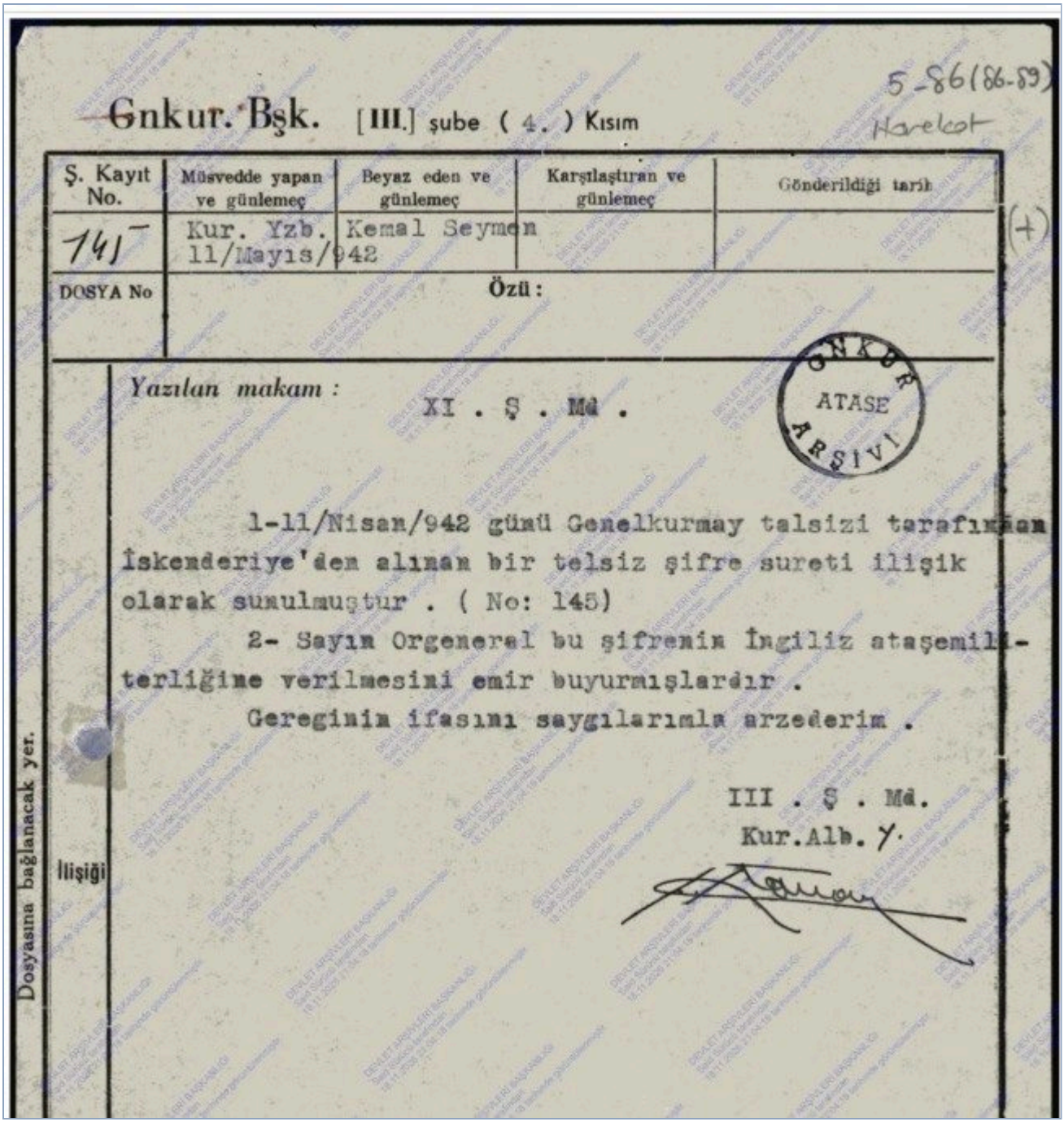
> `Grup Sayısı: 67 | d1 == d3 (Aynı Onluk [AA][BB]): 15/67 (22.4%) | 0xxx Başlangıçlı: 12/67 | 2-Haneli Rastlantı İndeksi (IC): 0.00927`

3. German General Mittelberger's Secret Warning Cipher Sent from Berlin to the Turkish General Staff (6–19 December 1939 · `MSB ATASE 110–9–1–14, 1–0–63`)

> **Republic of Turkey, General Staff Cipher Directorate — No: 8648 (Top Secret · Origin: Berlin · Date: 6–7 Dec 1939 · Deciphered by: Arif Olğaç):**
> "General [Hilmar Ritter von] Mittelberger, who served as a specialist instructor at our War Academy,

> informed Staff Captain Yusuf—who delivered his family travel allowance to him in Berlin—that his long service had bound him morally to Turkey and that he considered it his duty for Turkey's security to communicate the following points:
> [1-] Driving the Turks out of Thrace is a historic aim. Every effort is being exerted toward this goal. The great danger to Turkey will come from Thrace.
> 2- For the security of the Straits and Western Anatolia, holding Thrace is indispensable. To this end:
> A- Thrace must immediately and rapidly be fortified thoroughly with anti-tank obstacles and modern bunkers.
> B- For defense, two armored divisions are required in Thrace.
> C- The most capable commanders must be assigned to Thrace.
> D- The Field Marshal [Fevzi Çakmak] is a supreme commander worthy of deep respect and trust. Division and higher commanders and general staff officers are very good. Regimental and battalion commanders are aged and unable to grasp modern weapons, and must be reformed.
> E- Great importance must be given to factories producing abundant ammunition.
> F- Great attention and importance must be devoted to the air force.
> G- The Caucasus front must not be lost from sight."

4. Archival Facsimile Plates (`MSB ATASE 110-9-1-14`)



Gnkur. Bşk. [III.] şube (4.) Kısım

5-86(86-89)
Harekat

Ş. Kayıt No.	Müsvedde yapan ve günlemeç	Beyaz eden ve günlemeç	Karşılaştıran ve günlemeç	Gönderildiği tarih
141	Kur. Yzb. 11/Mayıs/942	Kemal Seymen		
DOSYA No	Özü:			

Yazılan makam : XI . Ş . Md .

GNKUR ATASE ARŞİVİ

1-11/Nisan/942 günü Genelkurmay talsizi tarafından İskenderiye'den alınan bir telsiz şifre sureti ilişik olarak sunulmuştur . (No: 145)

2- Sayın Orgeneral bu şifrenin İngiliz ataşemiliterliğine verilmesini emir buyurmışlardır .

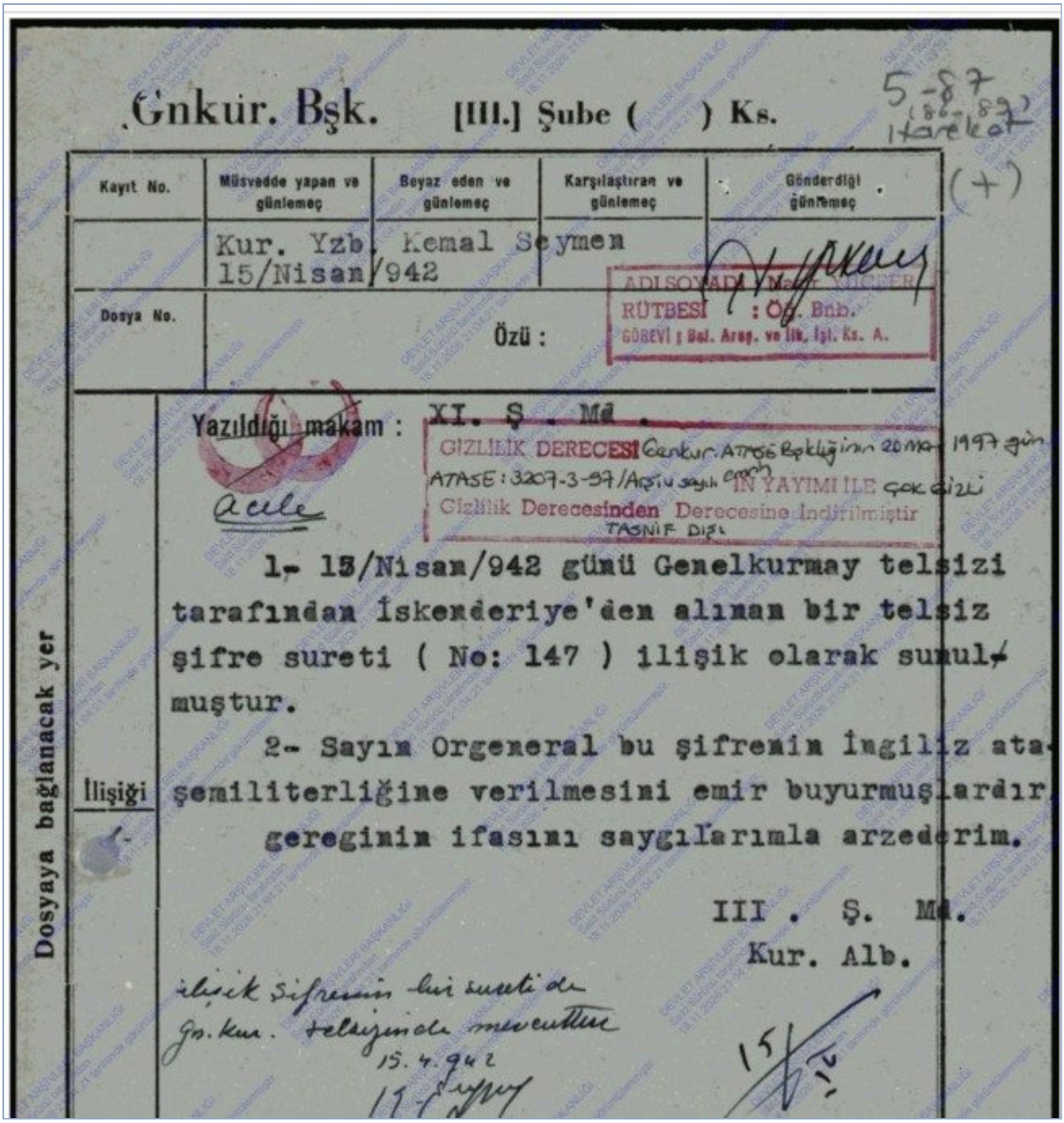
Gereğinin ifasını saygılarımla arzederim .

III . Ş . Md.
Kur.Alb. Y.

İlişiği

Dosyasına bağlanacak yer.

Plate 7 — MSB ATASE, 110-9-1-14, 2-0-125, p. 2 (11 May 1942): General Staff 3rd Branch memorandum transmitting the Alexandria radio cipher intercept (No. 145) to the British Military Attaché by order of the Chief of the General Staff.



Gnkur. Bşk. [III.] Şube ( ) Ks.

5-87 (82-87) Harekat

Kayıt No.	Müsvedde yapan ve günlemeç	Beyaz eden ve günlemeç	Karşılaştıran ve günlemeç	Gönderdiği günlemeç
	Kur. Yzb. Kemal Seymen 15/Nisan/942			

Dosya No.

Özü :

ADI SOYADI [illegible] MÜCEBBER
RÜTBESİ : Ön. Bnb.
GÖREVİ : Bsl. Araş. ve İlk. İşl. Ks. A.

Yazıldığı makam : XI. Ş. Md.

GİZLİLİK DERECESİ Genkur. ATASE Başkanlığının 20 MAY 1997 gün ATASE : 3207-3-97/Arşiv sayılı emriyle IN YAYIMI İLE ÇOK GİZLİ Gizlilik Derecesinden Derecesine İndirilmiştir TASNİF DIŞI

Acele

1- 15/Nisan/942 günü Genelkurmay telsizi tarafından İskenderiye'den alınan bir telsiz şifre sureti (No: 147) ilişik olarak sunulmuştur.

2- Sayın Orgeneral bu şifrenin İngiliz ataşemiliterliğine verilmesini emir buyurmuşlardır, gereğinin ifasını saygılarımla arzederim.

III. Ş. Md.
Kur. Alb.

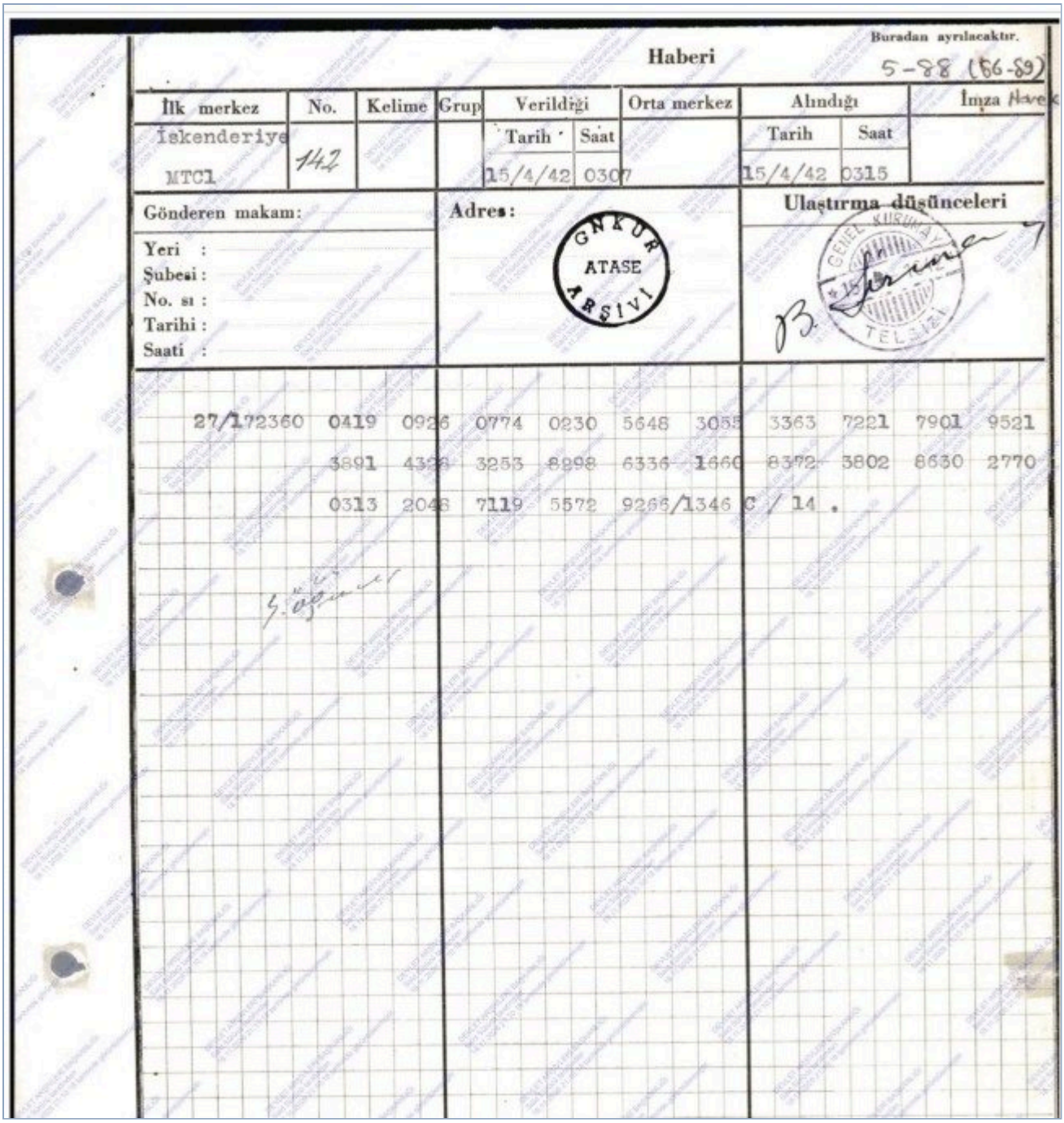
İlişiği
1-

Dosyaya bağlanacak yer

ilişik şifrenin bir sureti de Gn.kur. telsizinde mevcuttur
15.4.942

15/IV

Plate 8 — MSB ATASE, 110-9-1-14, 2-0-125, p. 3 (15 April 1942): First General Staff cover memorandum ordering delivery of the Alexandria radio cipher intercept to the British Military Attaché.



Haberi

Buradan ayrılacaktır.

5-88 (86-89)

İlk merkez	No.	Kelime	Grup	Verildiği Tarih	Verildiği Saat	Orta merkez	Alındığı Tarih	Alındığı Saat	İmza
İskenderiye MTCI	142			15/4/42	0307		15/4/42	0315	

Gönderen makam:

Yeri :
Şubesi :
No. sı :
Tarihi :
Saati :

Adres:

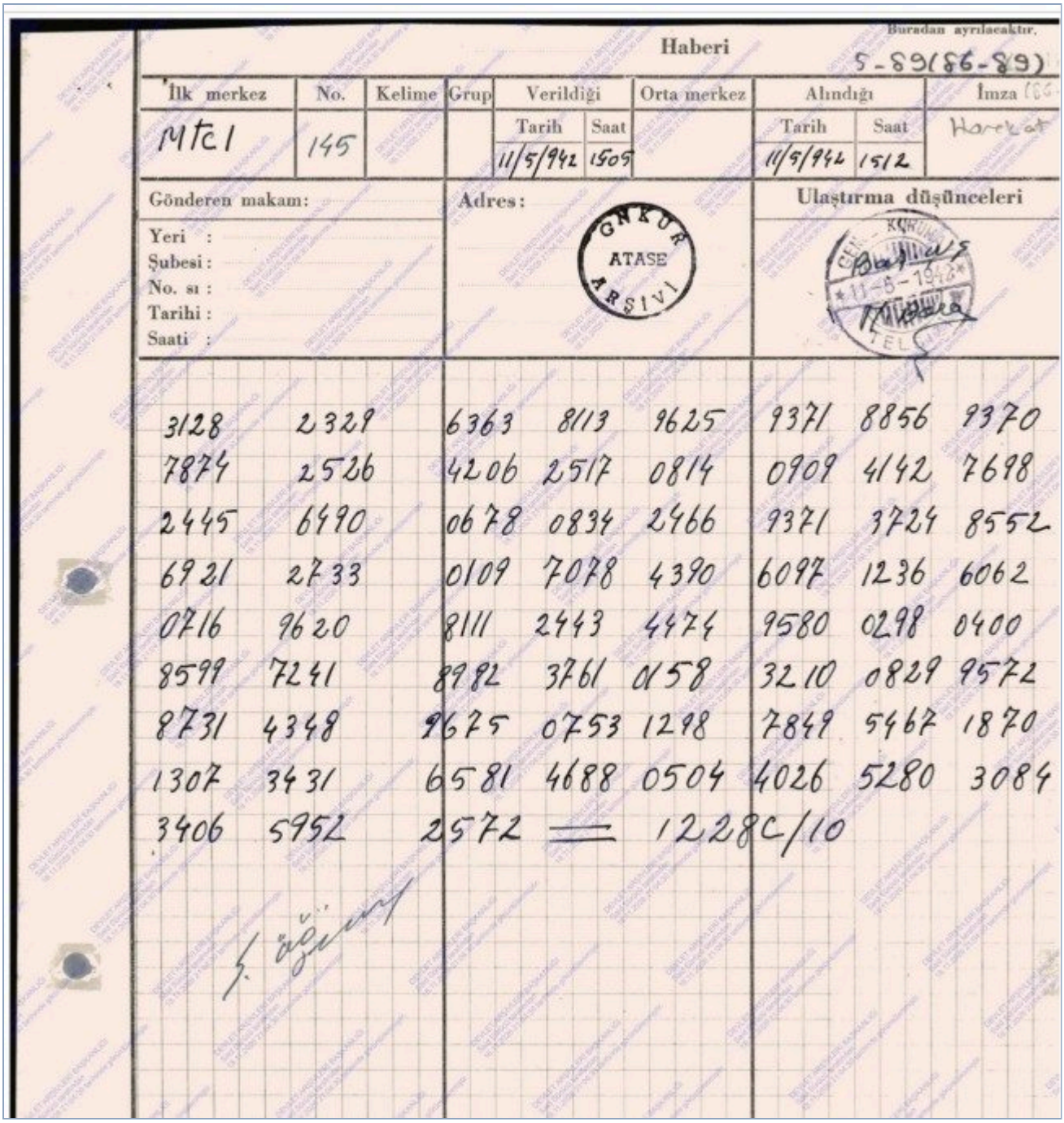
GNKUR ATASE ARŞİVİ

Ulaştırma düşünceleri

GENEL KURMAY TELSİZ

27/172360 0419 0926 0774 0230 5648 3055 3363 7221 7901 9521
3891 4328 3253 8998 6336 1660 8372 3802 8630 2770
0313 2048 7119 5572 9266/1346 C / 14 .

Plate 9 — MSB ATASE, 110-9-1-14, 2-0-125, p. 4 (15 April 1942 · No. 142): Undeciphered 25-group 4-digit radio cipher received from Alexandria / MTCI with indicator header `27/172360` and trailer `9266/1346 C / 14 .`



Haberi

Buradan ayrılacaktır.

5-89(86-89)

İlk merkez	No.	Kelime	Grup	Verildiği Tarih	Verildiği Saat	Orta merkez	Alındığı Tarih	Alındığı Saat	İmza
MTCI	145			11/5/942	1505		11/5/942	1512	Harekat

Gönderen makam:
Yeri :
Şubesi :
No. sı :
Tarihi :
Saati :

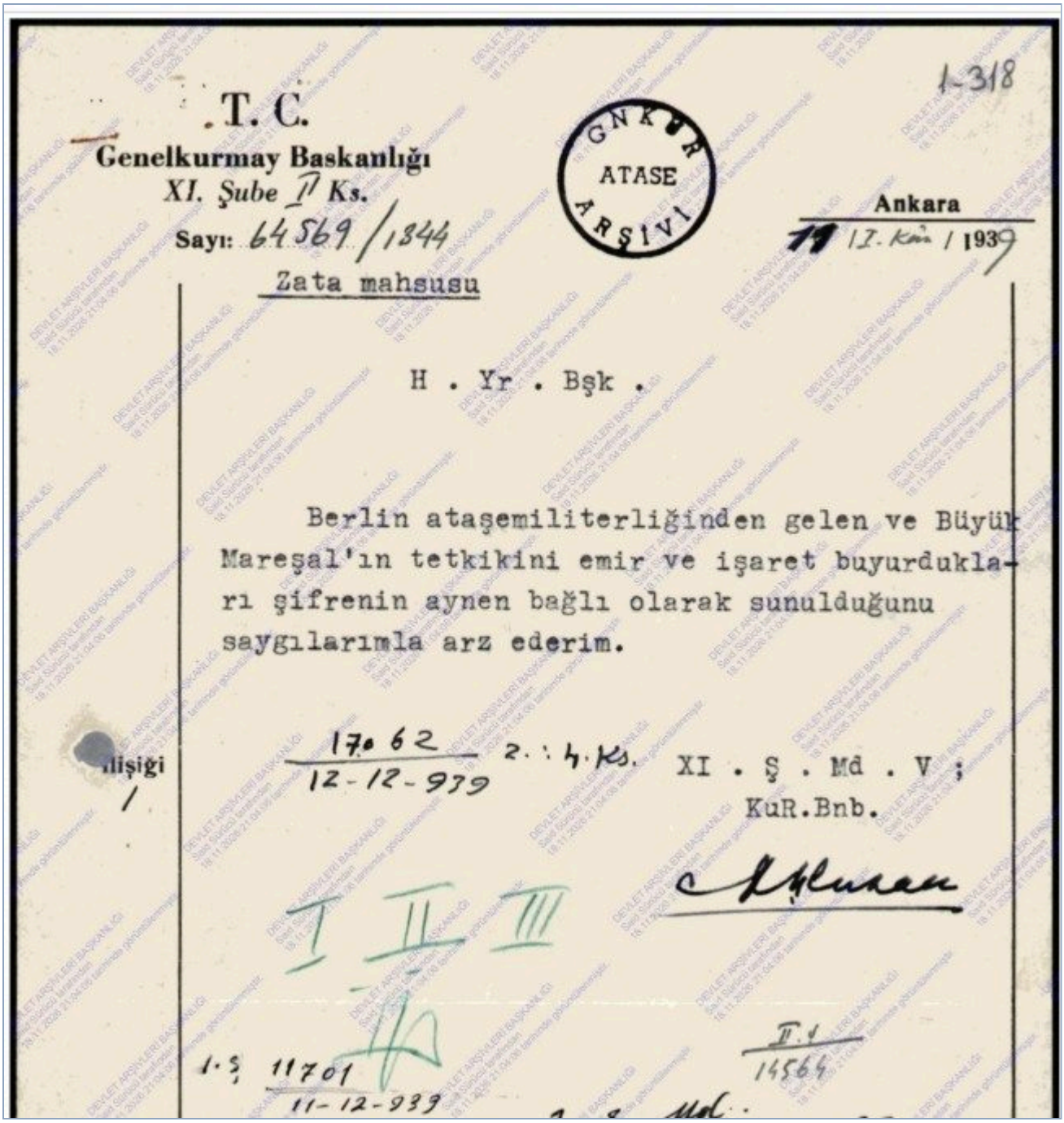
Adres:

GNKUR ATASE ARŞİVİ

Ulaştırma düşünceleri

3128	2329	6363	8113	9625	9371	8856	9370
7874	2526	4206	2517	0814	0909	4142	7698
2445	6490	0678	0834	2466	9371	3724	8552
6921	2733	0109	7078	4390	6097	1236	6062
0716	9620	8111	2443	4474	9580	0298	0400
8599	7241	8982	3761	0158	3210	0829	9572
8731	4348	9675	0753	1298	7849	5467	1870
1307	3431	6581	4688	0504	4026	5280	3084
3406	5952	2572	=	1228C/10			

Plate 10 — MSB ATASE, 110-9-1-14, 2-0-125, p. 5 (11 May 1942 · No. 145): Undeciphered 67-group 4-digit radio cipher received from MTCI ending with Date-Time Group `= 1228 C / 10`.



1-318

T. C.
Genelkurmay Başkanlığı
XI. Şube 1' Ks.
Sayı: 64569 / 1344

GNKUR ATASE ARŞİVİ

Ankara
19 / 12. Kân / 1939

Zata mahsusu

H . Yr . Bşk .

Berlin ataşemiliterliğinden gelen ve Büyük Mareşal'ın tetkikini emir ve işaret buyurdukları şifrenin aynen bağlı olarak sunulduğunu saygılarımla arz ederim.

...lişiği
/

17062 / 12-12-939 2. : 4. Ks.

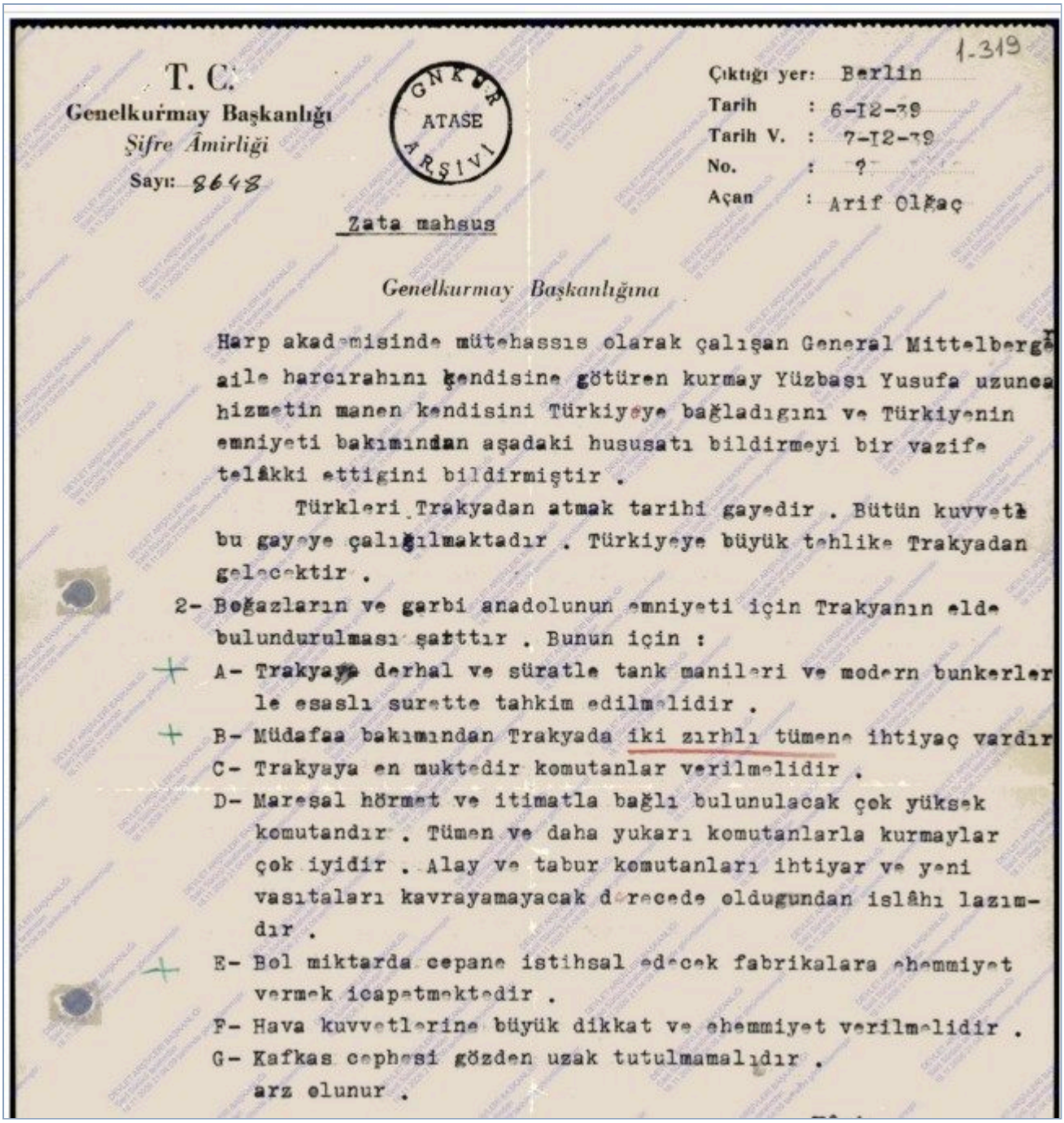
XI . Ş . Md . V ;
KuR.Bnb.

I II III

1.Ş 11701 / 11-12-939

II.1 / 14564

Plate 11 — MSB ATASE, 110-9-1-14, 1-0-63, p. 2 (19 December 1939): General Staff 11th Branch cover letter forwarding the Berlin Military Attaché cipher inspected by Field Marshal Fevzi Çakmak.



T. C.
Genelkurmay Başkanlığı
Şifre Âmirliği
Sayı: 8648

ATASE ARŞİVİ

1-319

Çıktığı yer: Berlin
Tarih : 6-12-39
Tarih V. : 7-12-39
No. : ?
Açan : Arif Olğaç

Zata mahsus

Genelkurmay Başkanlığına

Harp akademisinde mütehassıs olarak çalışan General Mittelberger aile harcırahını kendisine götüren kurmay Yüzbaşı Yusufa uzunca hizmetin manen kendisini Türkiyeye bağladığını ve Türkiyenin emniyeti bakımından aşadaki hususatı bildirmeyi bir vazife telâkki ettigini bildirmiştir .

Türkleri Trakyadan atmak tarihi gayedir . Bütün kuvvetle bu gayeye çalışılmaktadır . Türkiyeye büyük tehlike Trakyadan gelecektir .

2- Boğazların ve garbi anadolunun emniyeti için Trakyanın elde bulundurulması şarttır . Bunun için :

A- Trakyaya derhal ve süratle tank maniler ve modern bunkerler le esaslı surette tahkim edilmelidir .

B- Müdafaa bakımından Trakyada iki zırhlı tümene ihtiyaç vardır

C- Trakyaya en muktedir komutanlar verilmelidir .

D- Maresal hörmet ve itimatla bağlı bulunulacak çok yüksek komutandır . Tümen ve daha yukarı komutanlarla kurmaylar çok iyidir . Alay ve tabur komutanları ihtiyar ve yeni vasıtaları kavrayamayacak derecede olduğundan islâhı lazımdır .

E- Bol miktarda cepane istihsal edecek fabrikalara ehemmiyet vermek icapetmektedir .

F- Hava kuvvetlerine büyük dikkat ve ehemmiyet verilmelidir .

G- Kafkas cephesi gözden uzak tutulmamalıdır .

arz olunur .

Plate 12 — MSB ATASE, 110-9-1-14, 1-0-63, p. 3 (6–7 December 1939): Deciphered Berlin cipher containing German General Hilmar Ritter von Mittelberger's confidential warning regarding the Axis threat to Turkish Thrace.

1940 Turkish Meteorological Service Sliding-Strip («A..J») Synoptic Cipher Machine Shared with the British Royal Air Force (RAF)

Turkish Republican Archives (BCA, 30-10-0-0, 188-289-8 · 16 October – 20 November 1940 · 8-Page Complete Cryptographic File)

1. Historical Context & Mechanical Sliding-Strip Transposition Algorithm

In **October–November 1940**, immediately following Italy's invasion of Greece and the intensification of Eastern Mediterranean air operations, the Turkish Government handed over the **physical sliding-strip synoptic weather cipher key** used by the Directorate-General of State Meteorological Affairs to the British Air Attaché in Ankara so that the **Royal Air Force (RAF)** could decrypt Turkish daily weather broadcasts (Ankara Radio, callsign **TAB** , 3000 m wavelength, broadcast at 08:15 and 14:15 GMT).

> **Republic of Turkey, Prime Ministry Directorate-General of State Meteorological Affairs — 20 November 1940 (To the Air Attaché of the British Embassy, Ankara):**
> "By sliding the red/orange strips, it is possible to permute the positions of the letters of the Synoptic cipher. In this manner, the key of the cipher is generated and simultaneously transmitted by radio. Whenever it is deemed necessary to change the key in preparing the cipher, the arrangement of the table and the structure of the cipher are learned from the letters repeated five times by Ankara Radio (TAB).
> **For example:** If Ankara Radio repeats the letters (**B A B A A**) five times after (TAB), the cipher has been arranged as follows:
> Base Template: G1: İ F N p h | G2: İ W P p Nh | G3: İ W P CL V | G4: T D P CM U | G5: T D a CH W
> BABAA Enciphered Template: **G1: İ F P p h | G2: İ W P p Nh | G3: T W P CL V | G4: T D a CM U | G5: İ D N CH W** "

Interactive 1940 Sliding-Strip («A..J») Synoptic Weather Cipher Machine (BCA 30-10-0-0, 188-289-8)

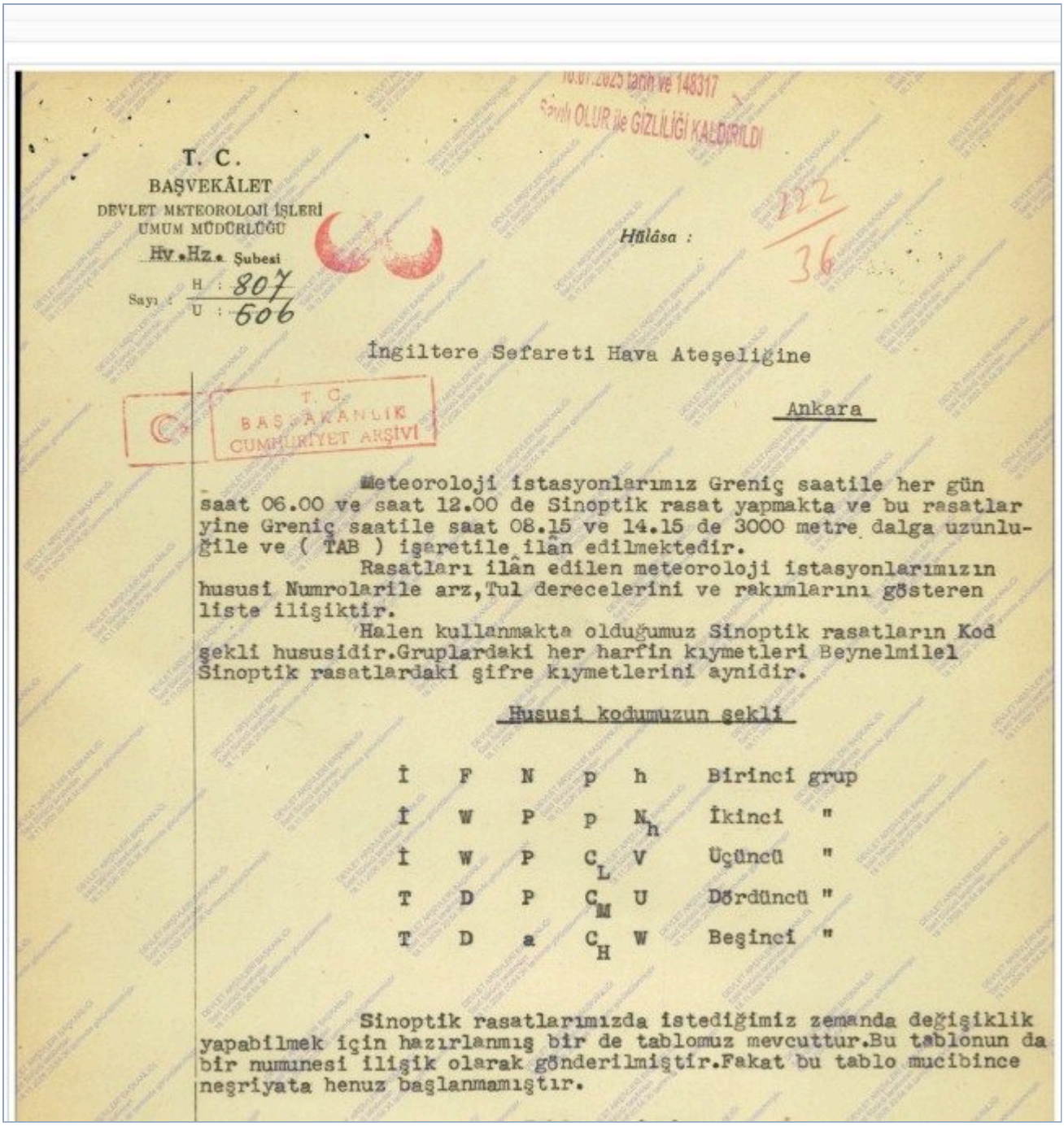


TAB BABAA BABAA BABAA BABAA BABAA ⟹ G1: İ F P p h | G2: T W P p Nh | G3: T W P CL V | G4: İ D a CM U | G5: İ D N CH W

2. Secret Meteorological Station Number Table (`BCA 30-10-0-0, 188-289-8, p. 6`)

Secret Station Code	Station Name	Latitude	Longitude	Altitude
`161`	Edirne	`N 41 40`	`E 26 35`	42 m
`139`	İstanbul	`N 40 58`	`E 28 50`	18 m
`169`	İzmit	`N 40 46`	`E 29 56`	92 m
`198`	Sinop	`N 42 02`	`E 35 10`	25 m
`221`	Trabzon	`N 41 00`	`E 39 44`	97 m
`134`	Çanakkale	`N 40 09`	`E 26 24`	26 m
`118`	Eskişehir	`N 39 47`	`E 30 32`	796 m
`163`	Ankara	`N 39 57`	`E 32 53`	907 m
`158`	Sivas	`N 39 45`	`E 37 02`	1284 m
`156`	Erzurum	`N 39 55`	`E 41 17`	1954 m
`123`	Kayseri	`N 38 44`	`E 35 30`	1059 m
`155`	Malatya	`N 38 21`	`E 38 19`	959 m
`184`	Diyarbakır	`N 37 55`	`E 40 15`	715 m
`199`	Van	`N 38 28`	`E 43 21`	1804 m
`225`	İzmir	`N 38 26`	`E 27 10`	5 m
`195`	Antalya	`N 36 53`	`E 30 44`	43 m
`135`	Konya	`N 37 53`	`E 32 31`	1031 m
`142`	Ulukışla	`N 37 33`	`E 34 30`	1425 m
`215`	Adana	`N 36 59`	`E 35 19`	30 m
`223`	İslahiye	`N 37 03`	`E 36 37`	520 m

3. Archival Facsimile Plates (Physical Sliding-Strip Cipher Device & Manual)



T. C.
BAŞVEKÂLET
DEVLET METEOROLOJİ İŞLERİ
ÜMUM MÜDÜRLÜĞÜ
Hv.Hz.e Şubesi
Sayı : H : 807
U : 606

Hülâsa :

122/36

İngiltere Sefareti Hava Ateşeliğine

Ankara

T.C. BAŞBAKANLIK CUMHURİYET ARŞİVİ

Meteoroloji istasyonlarımız Greniç saatile her gün saat 06.00 ve saat 12.00 de Sinoptik rasat yapmakta ve bu rasatlar yine Greniç saatile saat 08.15 ve 14.15 de 3000 metre dalga uzunluğile ve (TAB) işaretile ilân edilmektedir.

Rasatları ilân edilen meteoroloji istasyonlarımızın hususi Numrolarile arz,Tul derecelerini ve rakımlarını gösteren liste ilişiktir.

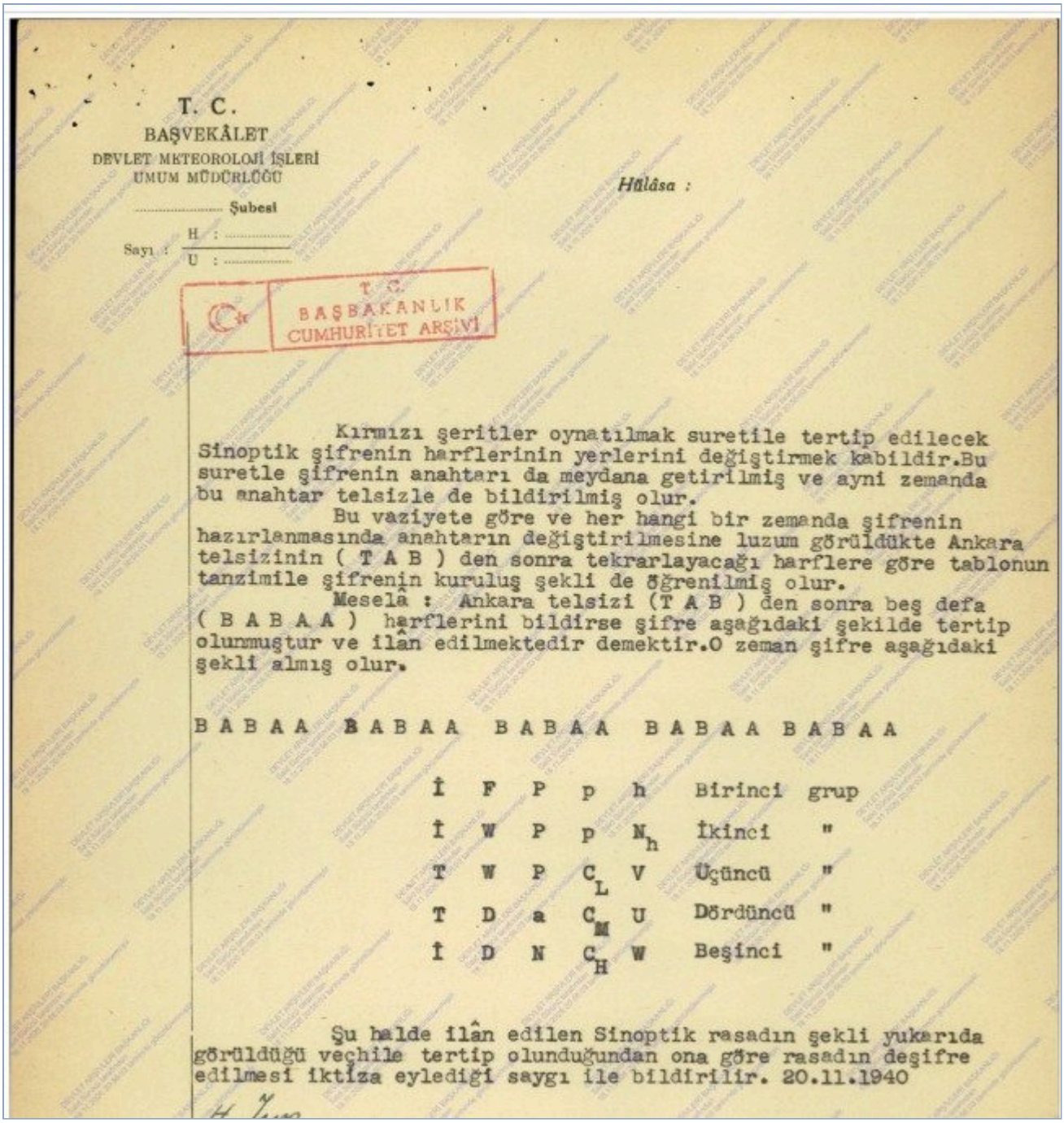
Halen kullanmakta olduğumuz Sinoptik rasatların Kod şekli hususidir.Gruplardaki her harfin kıymetleri Beynelmilel Sinoptik rasatlardaki şifre kıymetlerini aynidir.

Hususi kodumuzun şekli

İ	F	N	p	h	Birinci grup
İ	W	P	p	N_h	İkinci "
İ	W	P	C_L	V	Üçüncü "
T	D	P	C_M	U	Dördüncü "
T	D	a	C_H	W	Beşinci "

Sinoptik rasatlarımızda istediğimiz zemanda değişiklik yapabilmek için hazırlanmış bir de tablomuz mevcuttur.Bu tablonun da bir numunesi ilişik olarak gönderilmiştir.Fakat bu tablo mucibince neşriyata henuz başlanmamıştır.

Plate 13 — BCA, 30-10-0-0, 188-289-8, p. 4 (October 1940): Memorandum to the British Air Attaché in Ankara explaining the Ankara Radio (`TAB`) broadcast schedule and the 5-group custom synoptic code template.



T. C.
BAŞVEKÂLET
DEVLET METEOROLOJİ İŞLERİ
UMUM MÜDÜRLÜĞÜ
..... Şubesi
Sayı : H : .....
U : .....

Hülâsa :

T. C.
BAŞBAKANLIK
CUMHURİYET ARŞİVİ

Kırmızı şeritler oynatılmak suretile tertip edilecek Sinoptik şifrenin harflerinin yerlerini değiştirmek kabildir.Bu suretle şifrenin anahtarı da meydana getirilmiş ve ayni zemanda bu anahtar telsizle de bildirilmiş olur.

Bu vaziyete göre ve her hangi bir zemanda şifrenin hazırlanmasında anahtarın değiştirilmesine luzum görüldükte Ankara telsizinin (T A B) den sonra tekrarlayacağı harflere göre tablonun tanzimile şifrenin kuruluş şekli de öğrenilmiş olur.

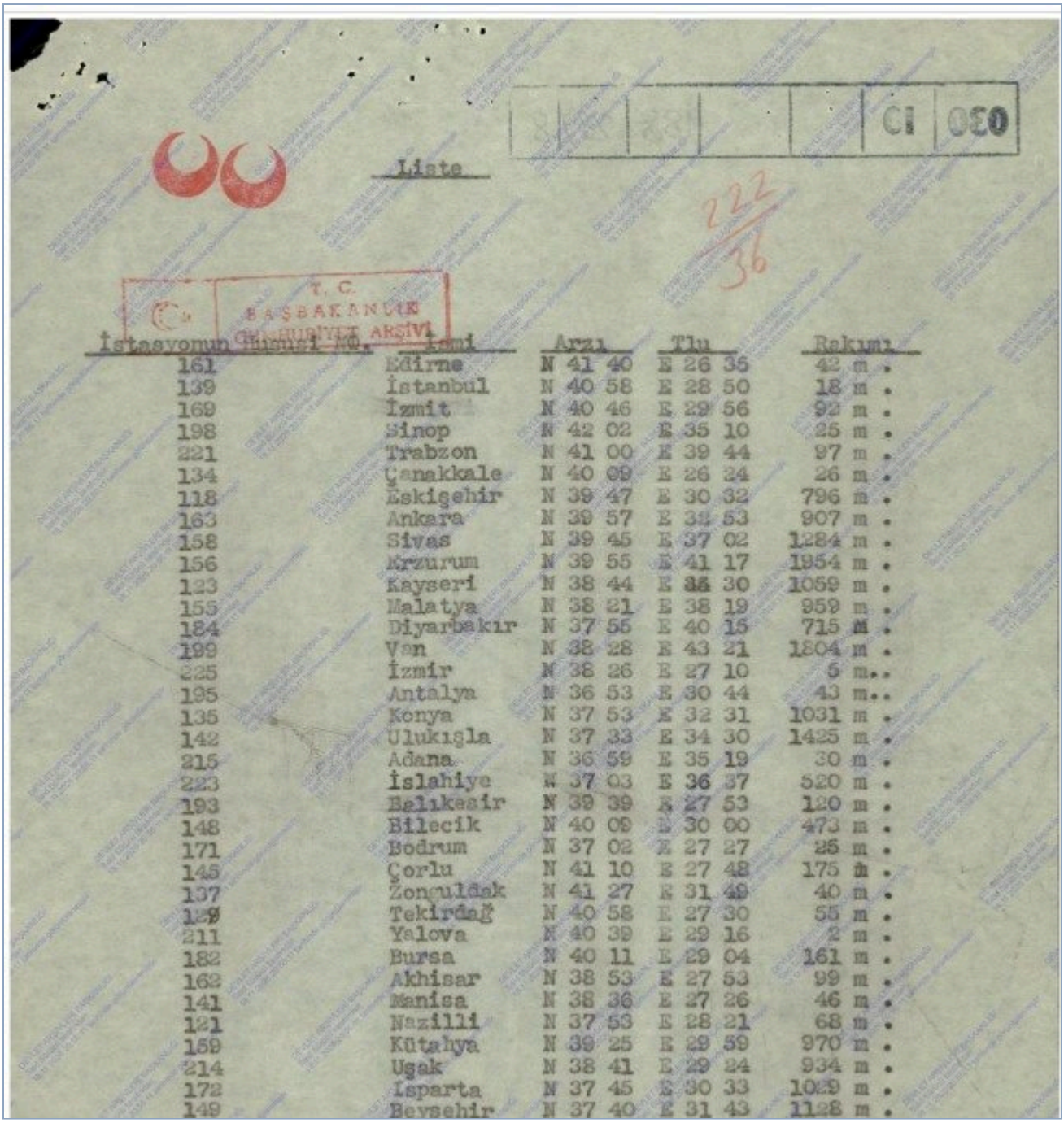
Meselâ : Ankara telsizi (T A B) den sonra beş defa (B A B A A) harflerini bildirse şifre aşağıdaki şekilde tertip olunmuştur ve ilân edilmektedir demektir.O zeman şifre aşağıdaki şekli almış olur.

B A B A A B A B A A B A B A A B A B A A B A B A A

İ	F	P	p	h	Birinci grup
İ	W	P	p	N_h	İkinci "
T	W	P	C_L	V	Üçüncü "
T	D	a	C_M	U	Dördüncü "
İ	D	N	C_H	W	Beşinci "

Şu halde ilân edilen Sinoptik rasadın şekli yukarıda görüldüğü veçhile tertip olunduğundan ona göre rasadın deşifre edilmesi iktiza eylediği saygı ile bildirilir. 20.11.1940

Plate 14 — BCA, 30-10-0-0, 188-289-8, p. 5 (20 November 1940): Worked example demonstrating how sliding the red/orange strips under indicator key `BABAA` permutes the 25 meteorological observation variables.



Liste

222/36

T.C. BAŞBAKANLIK Cumhuriyet Arşivi

İstasyonun Rasmî No.	İsmi	Arzı	Tulu	Rakımı
161	Edirne	N 41 40	E 26 36	42 m.
139	İstanbul	N 40 58	E 28 50	18 m.
169	İzmit	N 40 46	E 29 56	92 m.
198	Sinop	N 42 02	E 35 10	25 m.
221	Trabzon	N 41 00	E 39 44	97 m.
134	Çanakkale	N 40 09	E 26 24	26 m.
118	Eskişehir	N 39 47	E 30 32	796 m.
163	Ankara	N 39 57	E 32 53	907 m.
158	Sivas	N 39 45	E 37 02	1284 m.
156	Erzurum	N 39 55	E 41 17	1954 m.
123	Kayseri	N 38 44	E 35 30	1059 m.
155	Malatya	N 38 21	E 38 19	959 m.
184	Diyarbakır	N 37 55	E 40 15	715 m.
199	Van	N 38 28	E 43 21	1804 m.
225	İzmir	N 38 26	E 27 10	5 m..
195	Antalya	N 36 53	E 30 44	43 m..
135	Konya	N 37 53	E 32 31	1031 m.
142	Ulukışla	N 37 33	E 34 30	1425 m.
215	Adana	N 36 59	E 35 19	30 m.
223	İslahiye	N 37 03	E 36 37	520 m.
193	Balıkesir	N 39 39	E 27 53	120 m.
148	Bilecik	N 40 09	E 30 00	473 m.
171	Bodrum	N 37 02	E 27 27	25 m.
145	Çorlu	N 41 10	E 27 48	175 m.
137	Zonguldak	N 41 27	E 31 49	40 m.
129	Tekirdağ	N 40 58	E 27 30	55 m.
211	Yalova	N 40 39	E 29 16	2 m.
182	Bursa	N 40 11	E 29 04	161 m.
162	Akhisar	N 38 53	E 27 53	99 m.
141	Manisa	N 38 36	E 27 26	46 m.
121	Nazilli	N 37 53	E 28 21	68 m.
159	Kütahya	N 39 25	E 29 59	970 m.
214	Uşak	N 38 41	E 29 24	934 m.
172	Isparta	N 37 45	E 30 33	1029 m.
149	Beyşehir	N 37 40	E 31 43	1128 m.

Plate 15 — BCA, 30-10-0-0, 188-289-8, p. 6: Secret 3-digit station numbers, coordinates, and elevations for 35 Turkish meteorological stations.



Plate 16 — BCA, 30-10-0-0, 188-289-8, p. 7: Reverse face of the cardstock sliding-strip cipher device bearing the official seals of the State Meteorological Directorate.

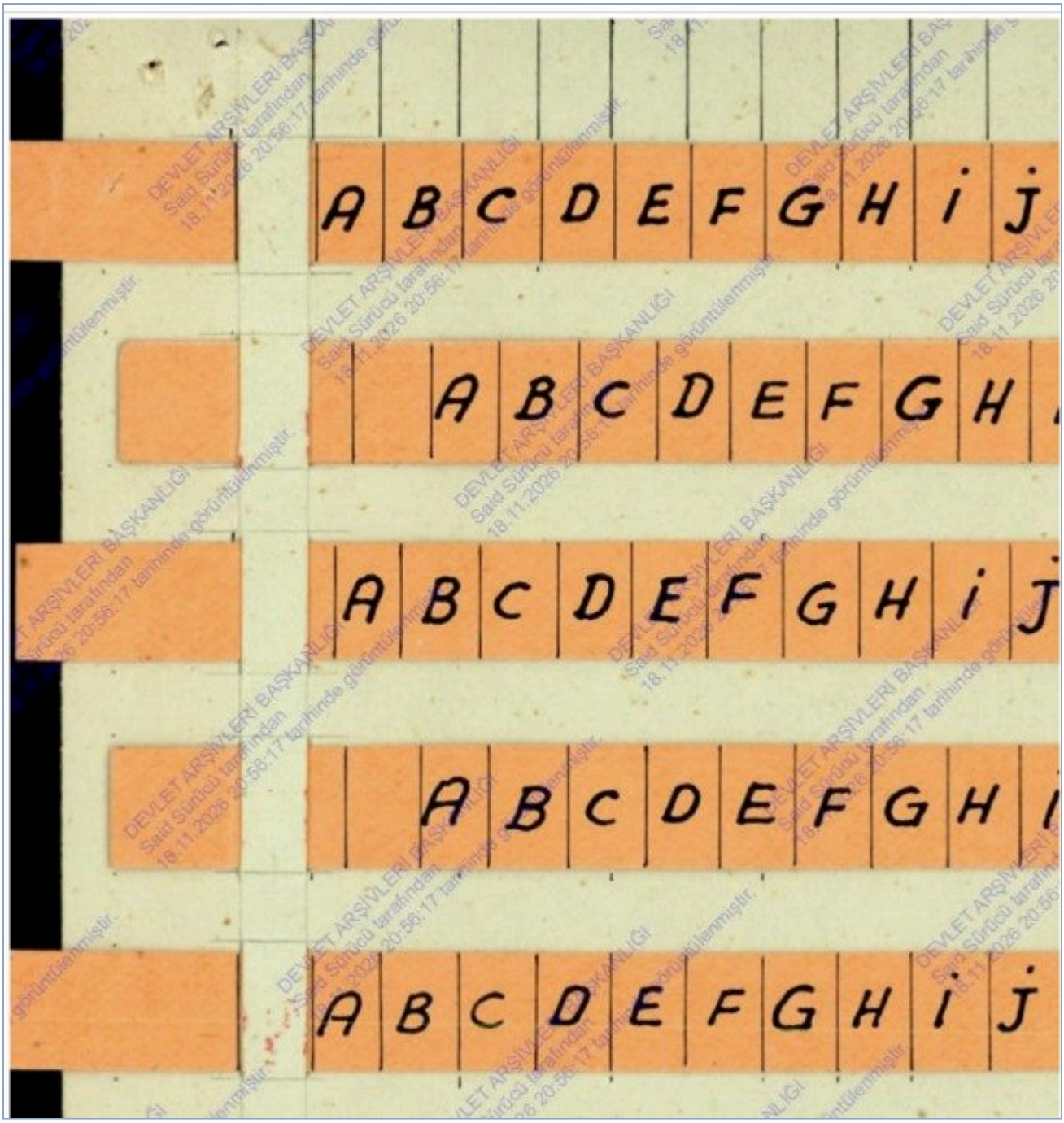


Plate 17 — BCA, 30-10-0-0, 188-289-8, p. 8: Front face of the physical cardstock cipher device with its five movable orange `A B C D E F G H İ J` strips.

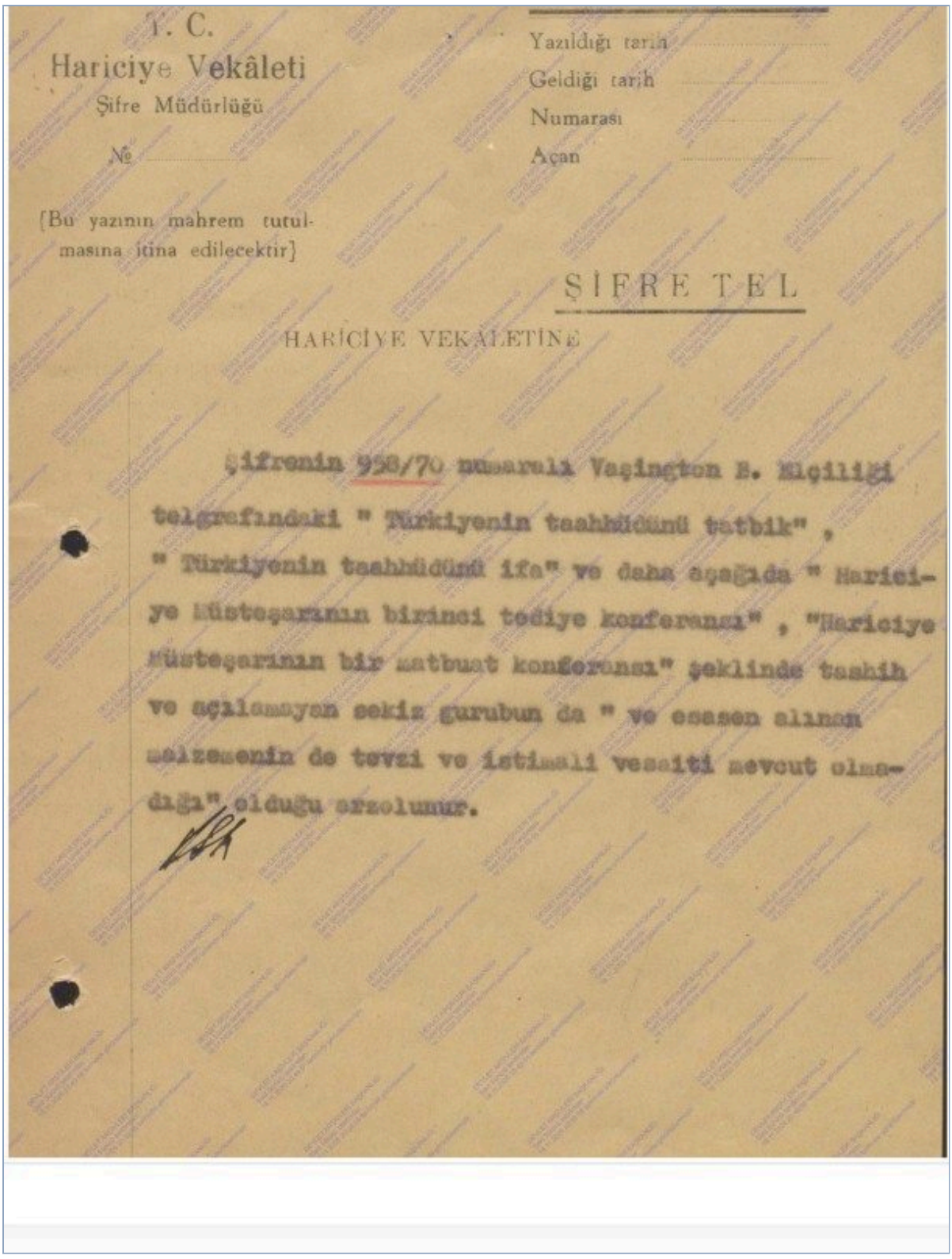
1939–1945 BETSİS World War II Cipher Corpus Inventory (149 Records) & Foreign Ministry / General Staff Documents

Republican Archives (40 Records), Ministry of Foreign Affairs Turkish Diplomatic Archive (79 Records), and MSB Military History Archive / ATASE (30 Records)

1. Distribution of 1939–1945 Cipher Records Across Three Turkish State Archives & Key Files Inspected

#	Archive & Shelfmark	Date	Category / Status	Contents & Cryptological Findings
1	**MSB ATASE** `110-9-1-14, 2-0-125`	15.04 & 11.05.1942	**Undeciphered 4-Digit Radio Ciphers (2 Dispatches)**	Raw 4-digit Alexandria (`MTCI`) radio cipher intercepts No. 142 (25 groups) and No. 145 (67 groups) captured by Turkish General Staff Radio and handed to the British Military Attaché.
2	**BCA** `30-10-0-0, 65-435-9`	21.07.1939	**Complete Cipher Key + Worked Ciphertext**	Interior Ministry «YASA» 81-cell zero-free (`11..99 \ *0`) homophonic cipher key (direct descendant of the 1877 Ottoman key) and 18-group 4-digit sample telegram.
3	**BCA** `30-10-0-0, 188-289-8`	16.10.1940	**Complete Mechanical Cipher Device + Station Codes**	State Meteorological Directorate 5-row sliding-strip (`A..J`) synoptic weather cipher device and `BABAA` radio indicator shared with the British Royal Air Force (RAF).
4	**MSB ATASE** `110-9-1-14, 1-0-63`	06–19.12.1939	Deciphered Military Cipher (`Arif Olğaç`)	Former Turkish War Academy specialist German General Mittelberger's confidential warning from Berlin regarding the Axis threat to Turkish Thrace.
5	**Foreign Ministry TDA** `502-23510-102376-17`	03.03.1944	Foreign Ministry Cipher Directorate Memo	Internal memorandum noting that the **"eight undecipherable groups"** in Washington Embassy telegram No. 29/20 lacked key distribution records.
6	**Foreign Ministry TDA** `571-35231-138611-100`	19.06.1940	Retransmitted Deciphered Telegram	Tehran Embassy cipher bearing the note *"The telegram that could not be opened under wire 201 has been repeated verbatim."*
7	**BCA** `30-10-0-0, 159-118-20`	02.01.1945	Key Replacement / Retirement Memos	Interior Ministry memoranda documenting the succession of codeword keys **«GÜVEN» → «UFUK» (7 Oct 1943) → «ÇELİK» (5 Jan 1945)**.
8	**BCA** `30-10-0-0, 159-118-24 & 25`	22.09 & 28.11.1945	Key Destruction Certificates	Certificates of destruction by burning for retired cipher keys #7 and #8 upon entry into force of keys #9 and #10.
9	**BCA** `30-10-0-0, 46-296-8`	18.10.1940	Field Marshal Fevzi Çakmak Directives	General Staff regulations on priority prefixes (`Tayyare / Harekât / Hayat`) for open and encrypted military telegrams.
10	**BCA** `30-10-0-0, 156-100-7`	29.07.1941	Deciphered Port Authority Telegrams	Deciphered cipher telegrams from the Trabzon Port Authority regarding a Soviet motor vessel landing at Hopa.
11	**Foreign Ministry TDA** `561-36024-142516-24`	13.01.1941	Diplomatic Note Verbale (French)	Hungarian Legation Note Verbale requesting PTT copies of encrypted diplomatic telegrams.
12	**Foreign Ministry TDA** `541-44200-209912-42`	10.04.1941	Deciphered Diplomatic Cipher	Rome Embassy report on Italian wartime censorship of consular cipher communications.

2. Selected Foreign Ministry & General Staff Cipher Plates (`1940–1944`)



T. C.
Hariciye Vekâleti
Şifre Müdürlüğü
№

Yazıldığı tarih
Geldiği tarih
Numarası
Açan

{Bu yazının mahrem tutulmasına itina edilecektir}

ŞİFRE TEL

HARİCİYE VEKÂLETİNE

Şifrenin 930/70 numarala Vaşington E. Elçiliği telgrafındaki " Türkiyenin taahhüdünü tatbik" , " Türkiyenin taahhüdünü ifa" ve daha aşağıda " Hariciye müsteşarının birinci tediye konferansı" , "Hariciye müsteşarının bir matbuat konferansı" şeklinde tashih ve açılamayan sekiz gurubun da " ve esasen alınan malzemenin de tevzi ve istimali vesaiti mevcut olmadığı" olduğu arzolunur.

Plate 18 — Foreign Ministry TDA, 502-23510-102376-17 (3 March 1944): Foreign Ministry Cipher Directorate memorandum reporting that the “eight undecipherable groups” in Washington Embassy telegram No. 29/20 had no key usage record.

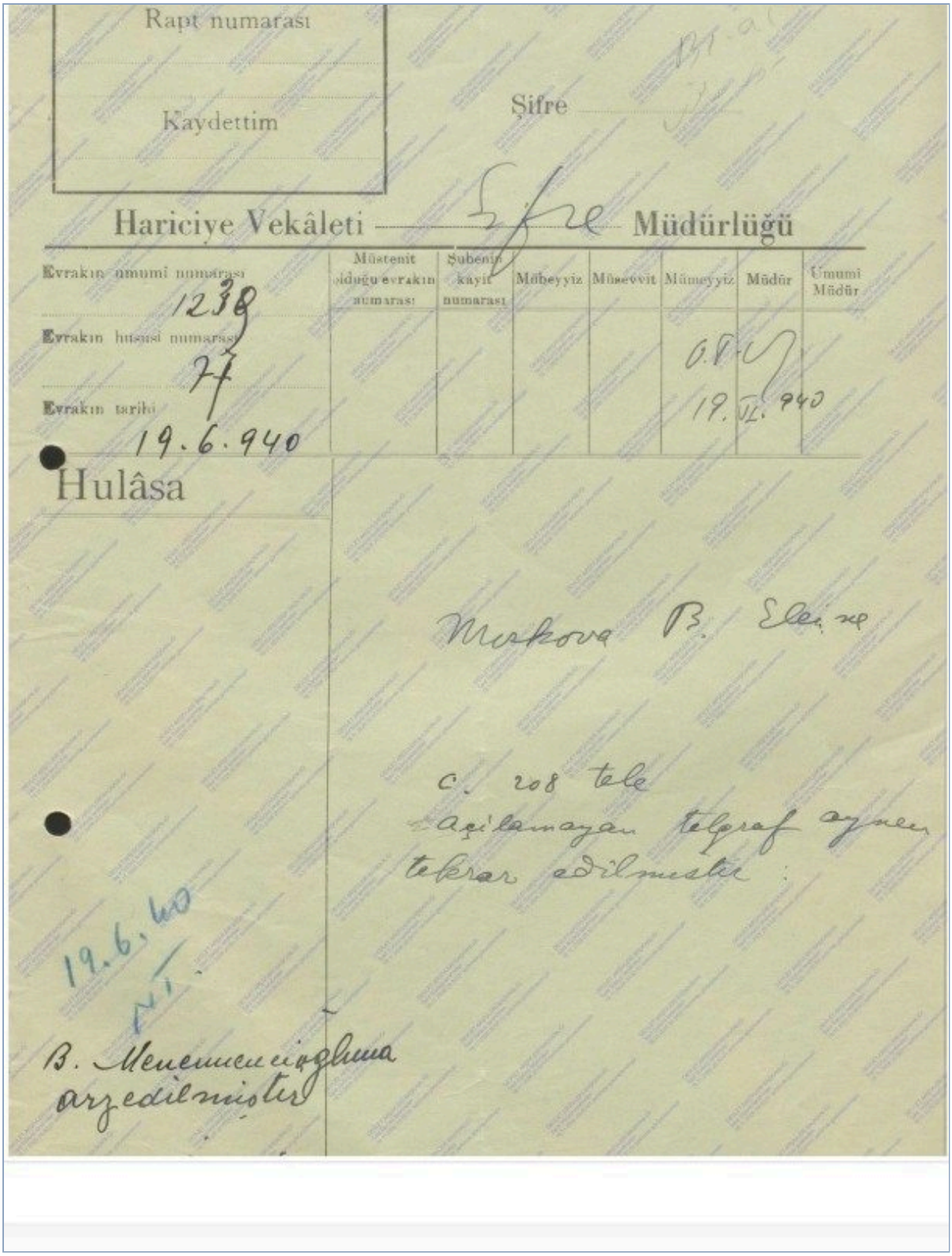
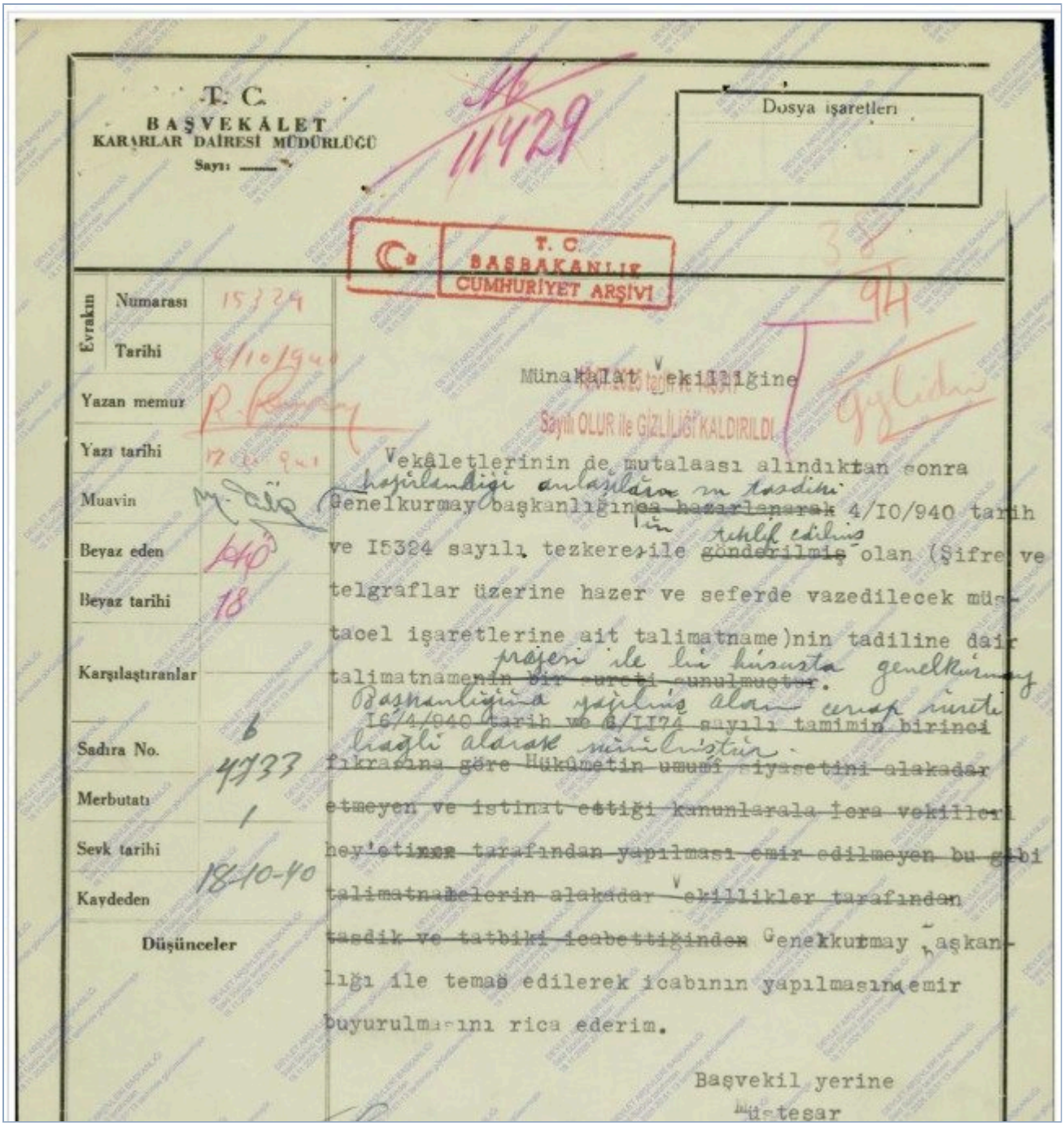


Plate 19 — Foreign Ministry TDA, 571-35231-138611-100 (19 June 1940): Tehran Embassy cipher retransmission noting "the telegram that could not be opened under wire 201 has been repeated verbatim."



T. C.
BAŞVEKÂLET
KARARLAR DAİRESİ MÜDÜRLÜĞÜ
Sayı: ____

Dosya işaretleri

11429

T. C.
BAŞBAKANLIK
CUMHURİYET ARŞİVİ

Evrakın	
Numarası	15324
Tarihi	4/10/940
Yazan memur	R. Ramsay
Yazı tarihi	17 [illegible] 941
Muavin	[illegible]
Beyaz eden	[illegible]
Beyaz tarihi	18
Karşılaştıranlar	
Sadıra No.	4733
Merbutatı	1
Sevk tarihi	
Kaydeden	18-10-40
Düşünceler	

Münakalat Vekilliğine

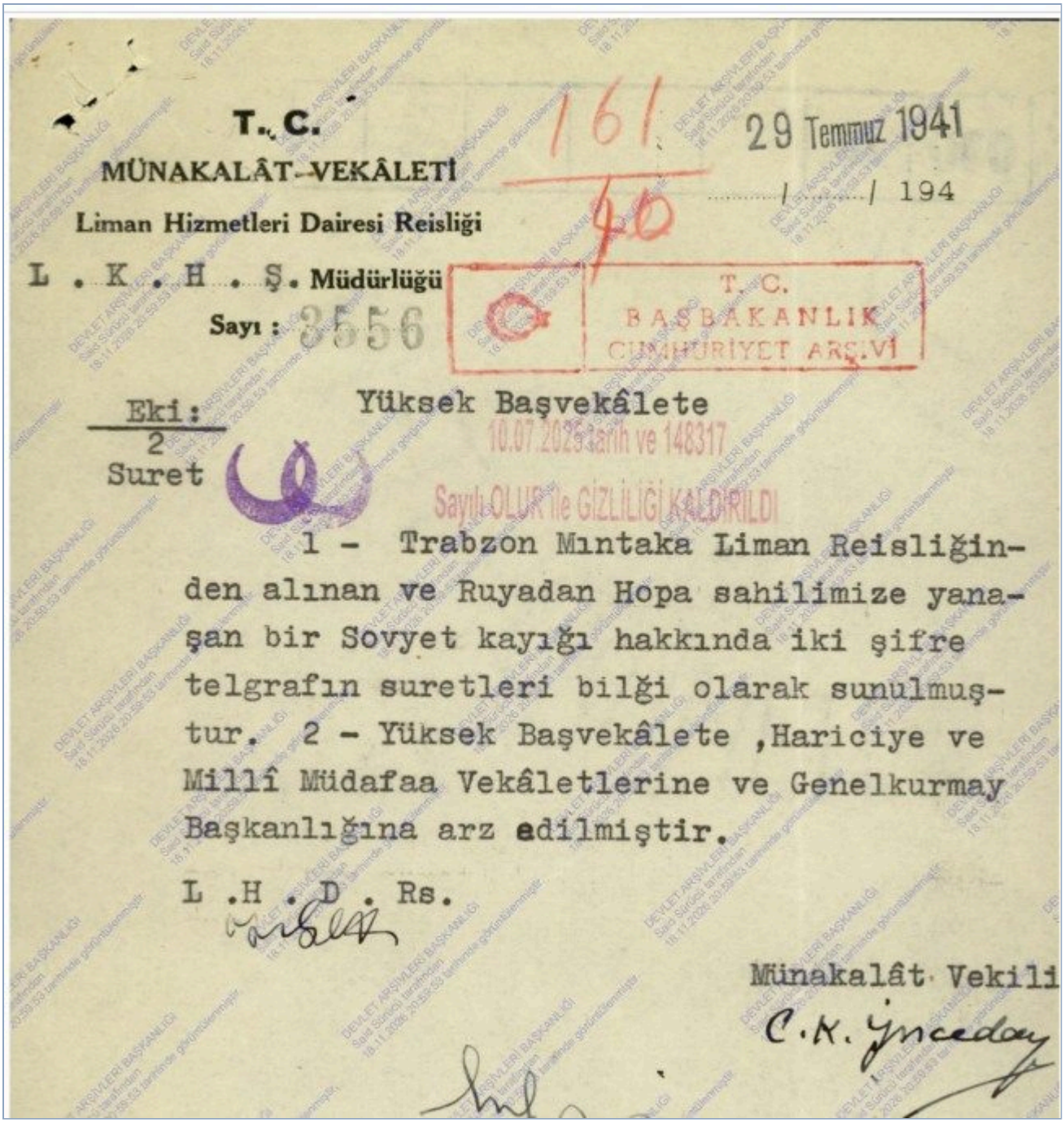
Sayılı OLUR ile GİZLİLİĞİ KALDIRILDI

Vekâletlerinin de mutalaası alındıktan sonra hazırlandığı anlaşılan ~~Genelkurmay başkanlığınca hazırlanarak~~ 4/IO/940 tarih ve I5324 sayılı tezkere ile ~~gönderilmiş~~ teklif edilmiş olan (Şifre ve telgraflar üzerine hazer ve seferde vazedilecek müstacel işaretlerine ait talimatname)nin tadiline dair ~~talimatnamenin bir sureti ekli~~ projesi ile bu hususta genelkurmay Başkanlığına yapılmış olan ~~I6/4/940 tarih ve 4/II74 sayılı tamimin birinci fıkrasına göre Hükûmetin umumî siyasetini alakadar~~ teklifi ekli olarak sunulmuştur.

~~etmeyen ve istinat ettiği kanunlarala icra vekilleri heyetince tarafından yapılması emir edilmeyen bu gibi talimatnamelerin alakadar vekillikler tarafından tasdik ve tatbiki icabettiğinden~~ Genelkurmay Başkanlığı ile temas edilerek icabının yapılmasına emir buyurulmasını rica ederim.

Başvekil yerine
Müsteşar

Plate 20 — BCA, 30-10-0-0, 46-296-8 (18 October 1940): Prime Ministry and General Staff regulations governing open and encrypted military telegrams.



T. C.
MÜNAKALÂT VEKÂLETİ
Liman Hizmetleri Dairesi Reisliği
L . K . H . Ş . Müdürlüğü
Sayı : 3556

161
70

29 Temmuz 1941
...../...../ 194

T. C.
BAŞBAKANLIK
CUMHURİYET ARŞİVİ

Eki:
2
Suret

Yüksek Başvekâlete

10.07.2026 tarih ve 148317
Sayılı OLUR'la GİZLİLİĞİ KALDIRILDI

1 - Trabzon Mıntaka Liman Reisliğinden alınan ve Ruyadan Hopa sahilimize yanaşan bir Sovyet kayığı hakkında iki şifre telgrafın suretleri bilği olarak sunulmuştur. 2 - Yüksek Başvekâlete ,Hariciye ve Millî Müdafaa Vekâletlerine ve Genelkurmay Başkanlığına arz edilmiştir.

L .H . D . Rs.

Münakalât Vekili
C. K. Yücedağ

Plate 21 — BCA, 30-10-0-0, 156-100-7 (29 July 1941): Certified copy of deciphered cipher telegrams from the Trabzon Regional Port Authority regarding a Soviet craft landing at Hopa.