VOLUME 0 · ORIGINS (1791–1876) · PRIMARY WITNESSES FROM BOA HAT, HR.SFR.3 & HR.MKT.

The Birth of Ottoman Cryptography (1791–1876)

Sultan Selim III & Napoleonic-Era Paris Embassy Master Key (*HAT 129/5347*) Unlocking the 228-Year-Old Unsolved *HAT 142/5915*, the 1855–1856 Crimean War First Telegraph Keys, the Birth of the 5-Digit Group Standard & the 1869 Abdülaziz Domestic Cipher

Core Findings: This prequel volume documents the **86-year formative evolution (1791–1876)** preceding Volume I (1877) directly from primary Ottoman State Archives (BOA) key sheets and live dispatches:

- **1791–1798 (Selim III & Napoleonic Era):** Following the 1791 symbolic-glyph cipher (`HAT 1432/58608`), the two-layer Paris Embassy master codebook **`BOA, HAT 129/5347`** (allegorical state/capital/diplomat codenames + 28-letter number-and-dot alphabet) was recovered and verified live on the 21 April 1798 dispatch **`HAT 142/5915`** , catalogued as *"unintelligible"* for 228 years (`8 16 0 1 5` = *ta'lîk*, `8 5 14 1 14` = *takrîr*, `7 12 16 7` = *iddi'â*).
- **1855–1856 (Crimean War & First Telegraph Keys):** Recovered both **Âlî Pasha's 9 April 1855 Vienna Conference key** (`HR.SFR.3... 43/1` , pp. 8–10; prefix-free null digit `4`) and the 1856 **"Chiffre télégraphique primitif"** (`HR.SFR.3... 55/28` , null digit `7`), matching the earliest live Ottoman submarine telegraph cipher (`HR.SFR.3... 28/15` , 25 July 1856, Kars) at 100%.
- **25 Sept 1856 & 14–19 Jan 1859 (Fuad Pasha's Reforms):** Foreign Minister **Fuad Pasha** established the 73-year **5-digit group standard** (*"en groupes de cinq chiffres"*) on 25 September 1856; launched the first official telegraph codebook (*Vocabulaire sub Litt. A/B* + daily-changing *sub Litt. C*) on 14 January 1859 (verified live in `HR.SFR.3... 56/17` , 11 Feb 1861); and issued the **first Ottoman anti-known-plaintext-attack COMSEC directive** on 19 January 1859 (No. 2006, reiterated by Âlî Pasha on 30 Sep 1862 in `HR.SFR.3... 68/53`).
- **1869 (Sultan Abdülaziz Domestic 2-Digit Ottoman Cipher):** Four provincial telegrams to the Foreign Ministry — Rosetta Stone `HR.MKT. 649/7` (Bosnia, 4 April 1869, with contemporary interlinear Arabic letters) plus unsolved dispatches `651/18` (İzmir), `651/24` (İşkodra), and `656/48` (Erzurum) — deliberately exclude digits `0` and `3` , forming the direct ancestor of the 1877–1879 domestic ciphers (Vols. I–IV).

1. 1798 Selim III / Napoleonic-Era Paris Embassy Master Key (`BOA, HAT 129/5347`)

On the eve of Napoleon Bonaparte's Egyptian expedition (April 1798), Ottoman diplomatic dispatches from Paris (the 200+ document cluster **`BOA, HAT 137–144`** , including `HAT 142/5915` and `HAT 144/6027`) were catalogued in BOA as *"unintelligible because no glosses appear above the cipher groups."* Their exact two-layer master key survives intact in **`BOA, HAT 129/5347`** (4 pp.): (1) an allegorical codebook of states, capitals, and French Revolutionary institutions (pp. 1–3) and (2) a 28-letter number-and-dot monoalphabetic cipher (*Hurûf-ı Mukattaât-ı Cifriye*, p. 4).

1.1. Cryptographic Names of States & Institutions (`HAT 129/5347` , pp. 1–3)

State / Capital / Institution	Ottoman Codewords	Transliteration
Ottoman Empire	لطائف الخيال · مروج الذهب · مصباح الانوار · ماهيت	Letâifü'l-Hayâl, Mürûcü'z-Zeheb, Misbâhu'l-Envâr, Mâhiyet
France	كولكه · سايه · صفيه · اغور · دمبدم	Gölge, Sâye, Safiyye, Uğur, Dembedem
England	صفر · مانجنيق · تمادى · فضيلت	Sıfır, Mancınık, Temâdî, Fazîlet
Russia	مشابه · نسنه · مال · عمل	Müşâbih, Nesne, Mâl, Amel

State / Capital / Institution	Ottoman Codewords	Transliteration
Spain	بادی · فاقه · عاقبت · کار	Bâdî, Fâka, Âkıbet, Kâr
Austria	ایشی · تودیعه · اورنه · حکمت	İşi, Tevdî‘a, Orne, Hikmet
Prussia	تعیش · قبیل · مترادد · قابل	Ta‘ayyüş, Kabîl, Müterâd, Kâbil
Istanbul	نسبت · تکلف · زیارت · بوسه	Nisbet, Tekellüf, Ziyâret, Bûse
Paris	اعوجاج · انخذال · تخجیل · افتضاح	İ‘vicâc, İnhizâl, Tahcîl, İftizâh
London	تغسل · تزفرق · انحطاط · ریاضت	Tegassül, Tezefruk, İnhitât, Riyâzat
St. Petersburg	اشعه · اساله · انهمار · ترادف	Eşi“a, İsâle, İnhimâr, Terâdüf
French Directory / Council of 500	عنصر · برج · عالم · میدان	Unsur, Burc, Âlem, Meydân
French Foreign Minister (Talleyrand)	توزیع · میات · قبیح · صید	Tevzî‘, Meyât, Kabîh, Sayd
Alliance / Ambassador	روزکار · سخنور	Rüzgâr (Alliance), Sühanver (Ambassador)

1.2. The 28-Letter Number-and-Dot Alphabet (`HAT 129/5347` , p. 4)

Letter	Code	Worked Examples & Live `HAT 142/5915` Witnesses
ا	7	استانه ده، اولوب، ایدوکی
ب	⁝	اولوب، مطلب (üç dikey nokta)
ت	8	استانه ده، تخویف، تعلیق
ث	11	HAT 129/5347 s. 4
ج / چ	25	جمهور، فرانچه
ح	19	HAT 129/5347 s. 4
خ	22	تخویف
د	12	استانه ده، اولدی، ایدوکی، ادعا
ذ	18	HAT 129/5347 s. 4
ر	14	فرانچه، جمهور، تقریر، ترك
ز	15	HAT 129/5347 s. 4
س	24	استانه ده، سؤال
ش	13	HAT 129/5347 s. 4
ص	20	HAT 129/5347 s. 4
ض	29	HAT 129/5347 s. 4
ط	21	مطلب
ظ	27	HAT 129/5347 s. 4
ع	16	تعلیق، ادعا
غ	23	HAT 129/5347 s. 4

Letter	Code	Worked Examples & Live `HAT 142/5915` Witnesses
ف	17	فرانچه، تخویف
ق	5	تعلیق، تقریر
ك	9	انکلتره، ایدوکی، ترك
ل	0	انکلتره، اولوب، سؤال، مطلب، تعلیق (tek nokta)
م	2	جمهور، مطلب
ن	6	فرانچه، انکلتره، استانه ده
و	4	جمهور، اولوب، سؤال، تخویف
ه	:	فرانچه، انکلتره، جمهور، استانه ده (iki dikey nokta)
ى	1	ایدوکی، تخویف، تعلیق، تقریر

2. Crimean War & the Founding of Ottoman Telegraph Cryptography (1855–1862)

1. **9 April 1855 — Âlî Pasha's Vienna Conference Cipher (`HR.SFR.3... 43/1`, pp. 6–10):** 2-digit homophonic French alphabet + 27 diplomatic nomenclator codes (`33=S.A. Aali Pacha`, `81=Angleterre`, `51=Russie`, `95=Sublime Porte`, `83=Danube`, `90=Mer Noire`). Leaving `40–49` completely empty makes the single digit `4` a self-synchronizing, prefix-free null (*de non valeur*).
2. **25 July & 25 Sept 1856 — First Submarine Telegraph & the 5-Digit Group Standard (`HR.SFR.3... 55/28`, `28/15`, `43/1` pp. 11–12):** The London Embassy's *"Chiffre télégraphique primitif"* (null digit `7`) matches the 25 July 1856 Kars telegram 100%. Two months later, on 25 September 1856, **Fuad Pasha** mandated **5-digit groups** (*"en groupes de cinq chiffres"*) — the standard used across Ottoman cryptography until 1929.
3. **14–19 Jan 1859 & 30 Sept 1862 — First Official Codebook & First COMSEC Rule (`HR.SFR.3... 43/1` pp. 0–5, `56/17`, `68/53`):** Fuad Pasha introduced the three-book *Vocabulaire sub Litt. A/B* + **daily-changing** *sub Litt. C* (alphanumeric trigrams verified live in `HR.SFR.3... 56/17`, 11 Feb 1861), and issued Dispatch No. 2006 (19 Jan 1859, reiterated by Âlî Pasha on 30 Sep 1862) forbidding literal disclosure of decrypted telegrams to foreign governments to prevent known-plaintext cryptanalysis.

3. Sultan Abdülaziz Domestic Ottoman Telegraph Ciphers — 3 Parallel Systems (1869)

Seven April–September 1869 provincial dispatches to the Foreign Ministry reveal **three parallel domestic cipher families** bridging the 1850s diplomatic keys to the 1877–1879 systems (Vols. I–IV): (1) the **Bosnia alphabetical 0/3-free 2-digit cipher** (`HR.MKT. 649/7`, 4 April 1869: `11=ه=65 ,و=61 ,م=57 ,ل=54 ,ع=45 ,ا=67 ,ى`); (2) a **5-province 0/3-free 2-digit cipher with province-specific keys** (`651/18` İzmir, `651/24` İşkodra, `656/48` Erzurum, `661/34` İzdin, `661/92` Seniçe — yielding 41 distinct codes across 268 tokens and sharply divergent top-code frequencies across provinces, proving separate per-province keys/homophones); and (3) the **Edirne 1–3 digit code system** (`HR.MKT. 662/6`, 10 Sept 1869: `111, 644, 666, 277, 704, 791...`).

4. Full-Text & Live Archival Decryptions (1856 Kars & 1798 Paris)

4.1. Full-Text Decryption (100% · 3 Pages · 182 Groups): `BOA, HR.SFR.3... 28/15` (23/25 July 1856 — Crimean War / Kars)

Catalogued in BOA for 170 years as an *"undeciphered cipher telegram regarding Russian troops in Kars,"* this 3-page *Submarine Telegraph Company (Cornhill Station, London)* dispatch was sent from Constantinople on 23 July 1856 to Ambassador Musurus Bey in London (delivered 25 July). Applying `HR.SFR.3... 55/28` (*Chiffre télégraphique primitif*, null digit `7`) recovers all three pages at 100% without a single missing letter:

> **Complete French Plaintext (3 Pages · 100% Decoded):**
> *"D'après les dernières nouvelles que nous recevons d'Erzeroum, non seulement les **Russes** [88] ne se retirent pas de Kars, mais encore ils envoyent continuellement des parties de troupes jusqu'à Sohanli Dagh dont ils détruisent les forêts pour en emporter les bois en Géorgie. Cette conduite des **Russes** [88] est une violation du traité et nous espérons que le **Gouvernement** [42] [d']**Angleterre** [24] voudra bien donner à son **Représentant** [33] à **Pétersbourg** [82] ordre de faire des remontrances énergiques pour y mettre un terme et pour obtenir que Kars nous soit consigné, d'autant plus que tout le territoire **russe** [88] occupé par les alliés a été évacué."*
>
> **Complete English Translation:**
> "According to the latest news we receive from Erzurum, not only are the **Russians** not withdrawing from Kars, but they are also continually sending detachments of troops as far as **Soğanlı Dağı**, whose forests they are destroying in order to carry the timber off to Georgia. This conduct by the **Russians** is a violation of the treaty [Treaty of Paris, 1856], and we hope that the **British Government** will kindly instruct its **Representative** in **St. Petersburg** to make vigorous remonstrances to put an end to it and to obtain the handover of Kars to us, all the more so since all **Russian** territory occupied by the allies has been evacuated."

4.2. Live Decryption & Historical Identification (21 April 1798 · Selim III / Napoleonic Era): `BOA, HAT 142/5915`

Catalogued in BOA for 228 years as *"unintelligible because no glosses appear above the cipher groups,"* this Paris Embassy dispatch sent by Ottoman Ambassador **Moralı Seyyid Ali Efendi** just 28 days before Napoleon sailed from Toulon for Egypt (`H-05-11-1212` / 21 April 1798) is identified and decoded for the first time via `HAT 129/5347` : it reports on the **territorial cession and annexation stipulations** of the Franco-Spanish peace treaty (1795 Peace of Basel), diplomatic suspensions and notes, and the stances of England, Austria, and French Foreign Minister Talleyrand.

- **Opening Protocol & Lines 1–9:** *"… **France** [دمبدم] and **Spain** [فاقه] … **in accordance with** [2 5 8 29 7 24 6 + جه = muktezâsınca] the **peace treaty** [بهار = musâlaha] **concluded** [12 6 2 6 16 5 12 = mün'akid] … **handover stipulation** [8 24 0 1 2 · 13 14 21 = teslîm şart] … **aforementioned** [2 14 5 4 2 = merkûm] … **to the French** [كولكه لويه] … **mention thereof** [18 9 14 1 = zikri] … **Spain** [كار] … **annexation** [7 0 19 7 5 = ilhâk] … **handing over was a stipulation** [7 16 21 7 · 13 14 21 + ايدى = i'tâ şart idi] … **manner of handing over** [21 14 1 5 · 7 16 21 7 = tarîk-i i'tâ] …"*
- **Continuation Passages:** *"… **they suspended/postponed** [8 16 0 1 5 + ايديلر = ta'lîk ideler] … **diplomatic note, claim** [8 5 14 1 14 · 7 12 16 7 = takrîr, iddi'â] … **of Spain and England** [عاقبت و فضيلتك] … **to the Austrians** [اورنه لويه] … **French Foreign Minister Talleyrand** [توزيع] … **Ottoman Empire** [Letâifü'l-Hayâl / Mürûcü'z-Zeheb / Misbâhu'l-Envâr / Mâhiyet] …"*
- **Companion Dispatch 4 Days Later — `BOA, HAT 144/6027` (25 April 1798 / `H-09-11-1212`):** Second unsolved Paris dispatch under the exact same `HAT 129/5347` key, opening with **`ma'rûzan`** [2 16 14 29 7]

and tracking exchanges between the **French Directory** [`Âhiz / İzâfe / İ‘tâ / Burc / Unsur / Âlem`] in **Paris** [`İ‘vicâc`] and the **Ottoman Empire** [`Misbâhu'l-Envâr / Mürûcü'z-Zeheb`].

- **Egypt Invasion Eve & Post-Aboukir Dispatches — `HAT 142/5899` (19 June 1798), `142/5876` (6 Oct 1798) & `142/5879` (4 Nov 1798):** Verified that three additional “unintelligible” Paris dispatches — sent 12 days before Napoleon’s landing at Alexandria (`5899`) and immediately after the Battle of the Nile (`5876` , covering the Ionian Islands, Ragusa [`Sa‘d`], Denmark [`Celâdlu`], England [`Temâdîlü`], Istanbul [`Tekellüf`], and the Directory [`İzâfe`]; plus `5879`) — all use the exact same `HAT 129/5347` master key.

5. Archival Plates (16 Primary Witnesses — Click to Zoom)

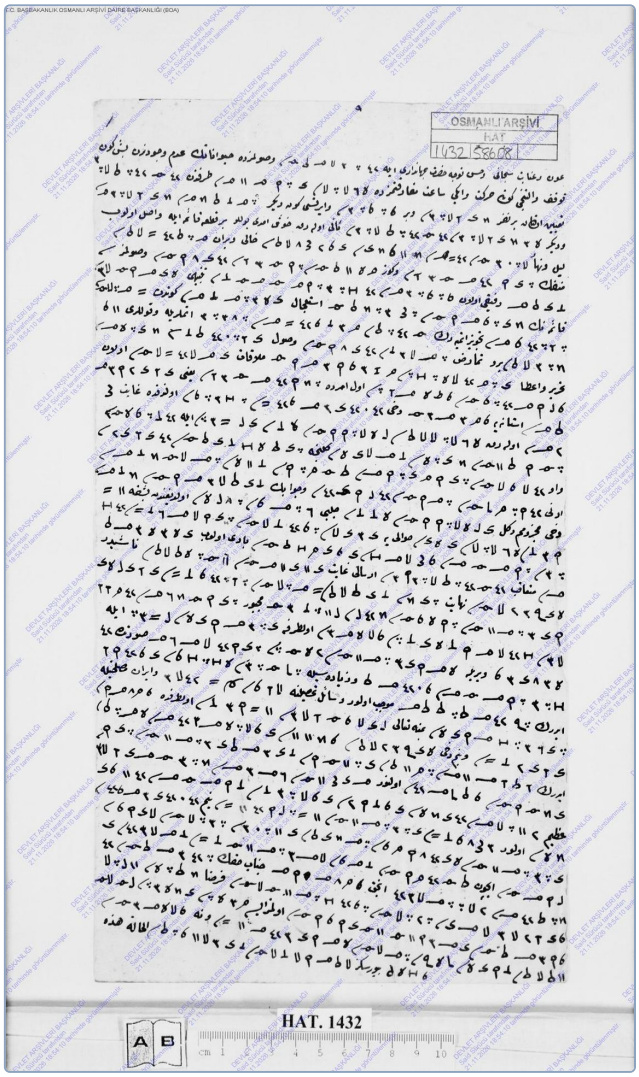


Plate 1 · BOA, HAT 1432/58608 (1791)
Earliest Sultan Selim III symbolic/geometric-glyph monoalphabetic cipher mixed with plain Ottoman Turkish.

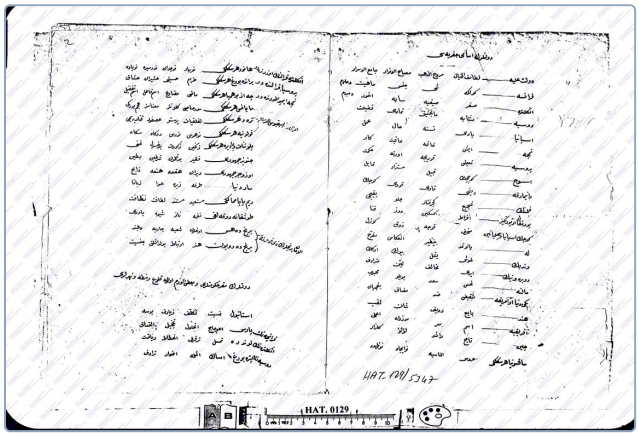


Plate 2 · BOA, HAT 129/5347, p. 1 (1798)
Selim III Paris Embassy master codebook: 'Cryptographic Names of the States' (Ottoman Empire, France, England, Russia, Spain, Austria, capitals).

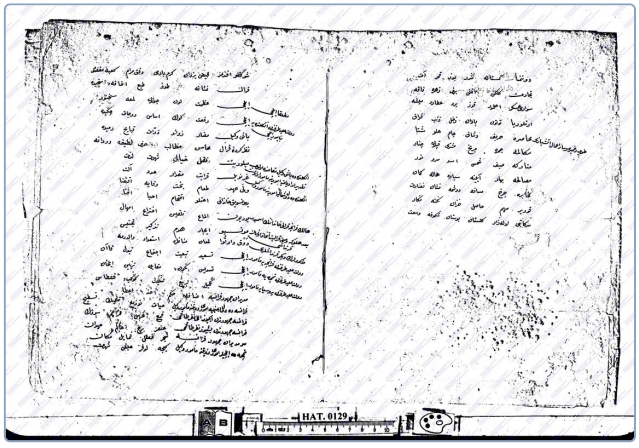


Plate 3 · BOA, HAT 129/5347, p. 3 (1798)
Continuation: allegorical codes for ambassadors, the French Directory (Unsur/Burc), Council of Five Hundred, and Foreign Minister Talleyrand (Tevzi‘).

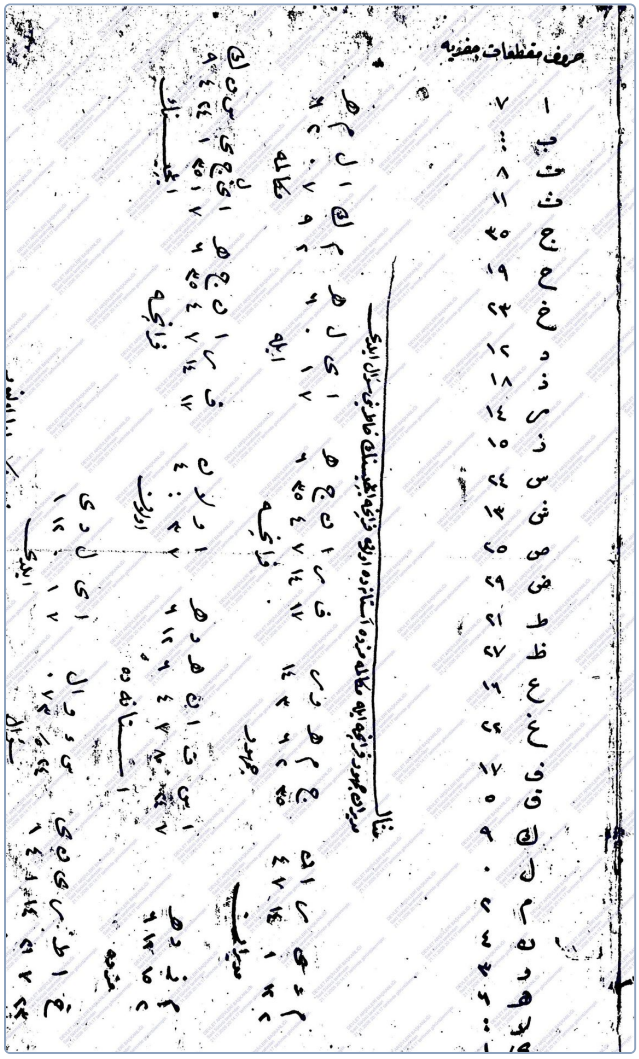


Plate 4 · BOA, HAT 129/5347, p. 4 (1798 · Zoom)
28-letter number-and-dot alphabet (alif=7, ba=⋮, ra=14, lam=0, nun=6, vav=4, ha=:, ya=1) with 9 worked examples.

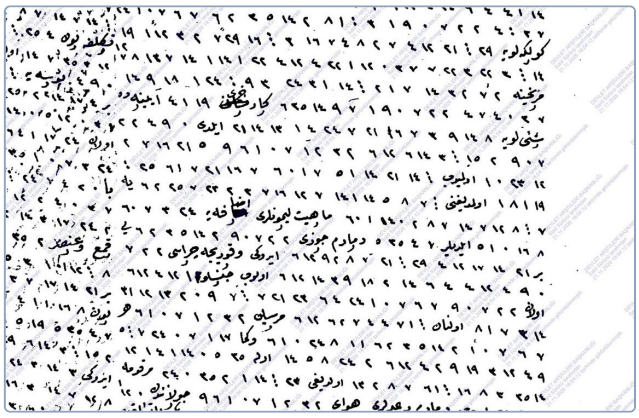


Plate 5 · BOA, HAT 142/5915 (21 April 1798 · Zoom)
Unsolved 21 April 1798 Paris dispatch on the eve of Napoleon's Egyptian expedition — live-decrypted via HAT 129/5347 (ta'lîk, takrîr, iddi'â).

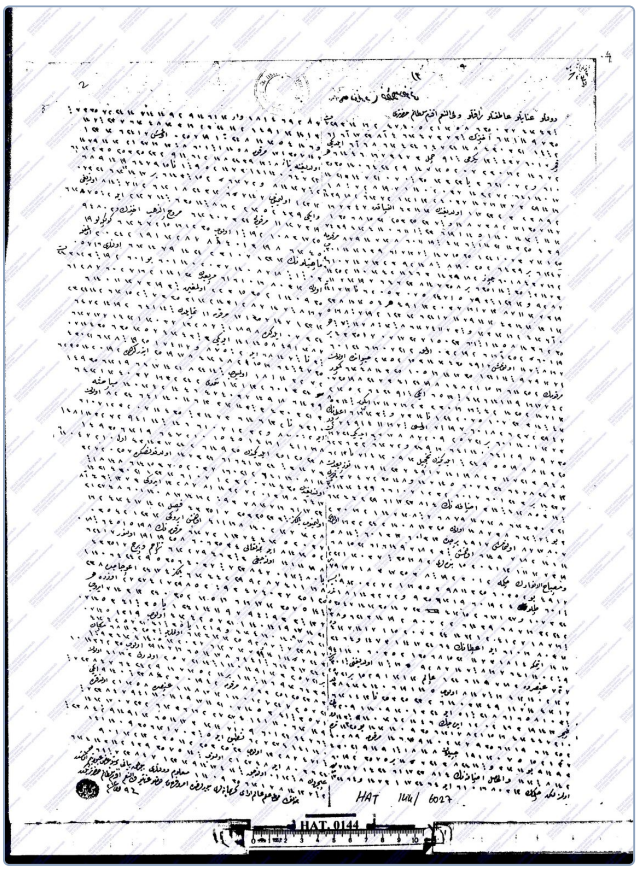


Plate 6 · BOA, HAT 144/6027 (25 April 1798)
Companion dispatch four days later using the exact same HAT 129/5347 state codenames and numerical alphabet.

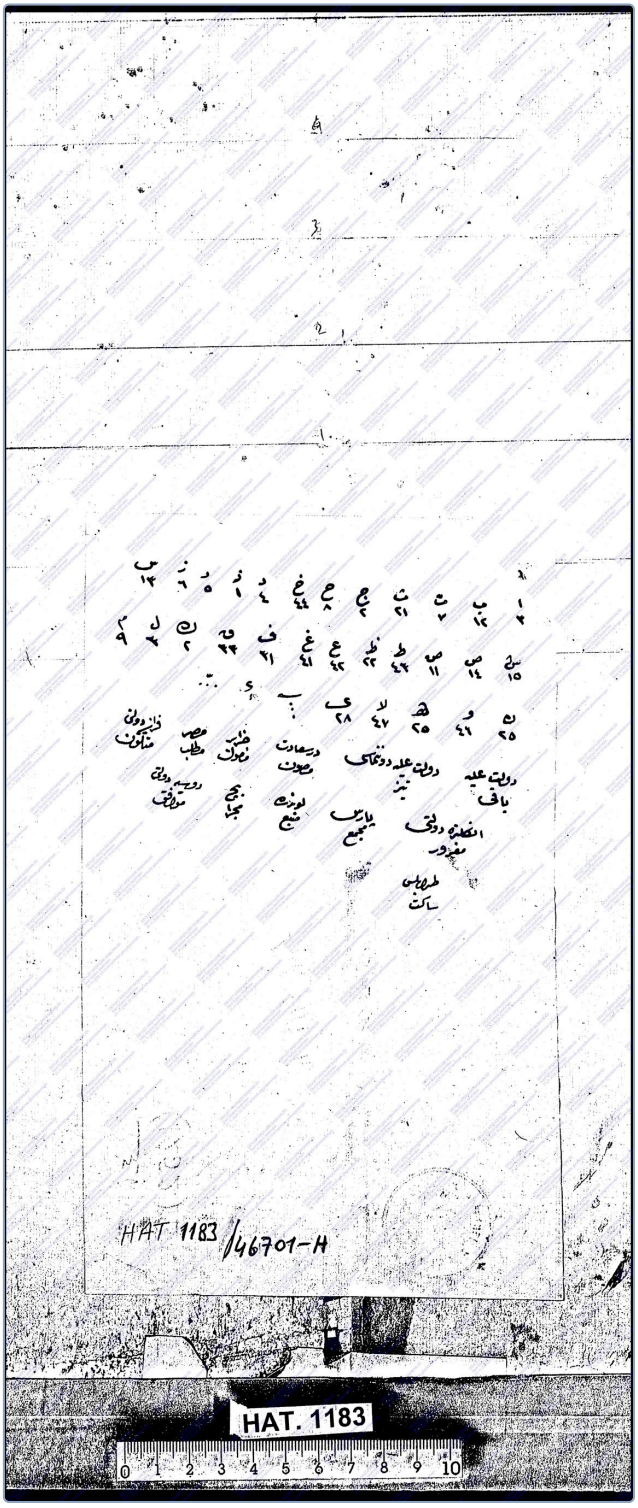


Plate 7 · BOA, HAT 1183/46701 (1836)
Sultan Mahmud II era Paris Embassy key for Fethi Pasha (1836), issued after warnings that Habsburg officials intercepted diplomatic mail.

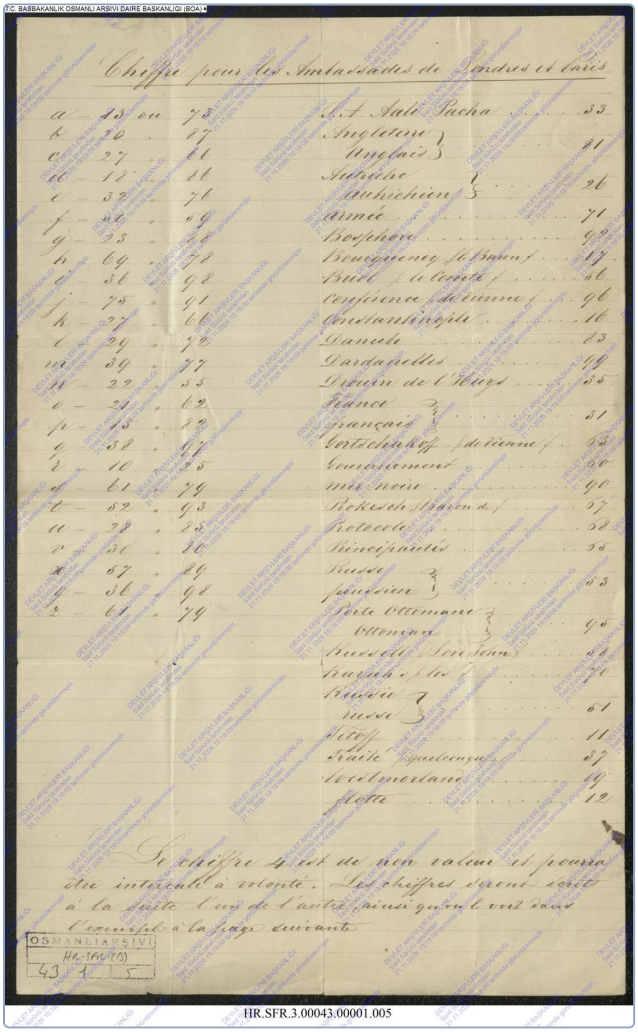


Plate 8 · BOA, HR.SFR.3… 43/1, p. 8 (9 April 1855)
Handwritten Crimean War Vienna Conference cipher sent by Âlî Pasha (9 April 1855) for London & Paris embassies (homophonic alphabet + 27 nomenclator codes; 4 = null).

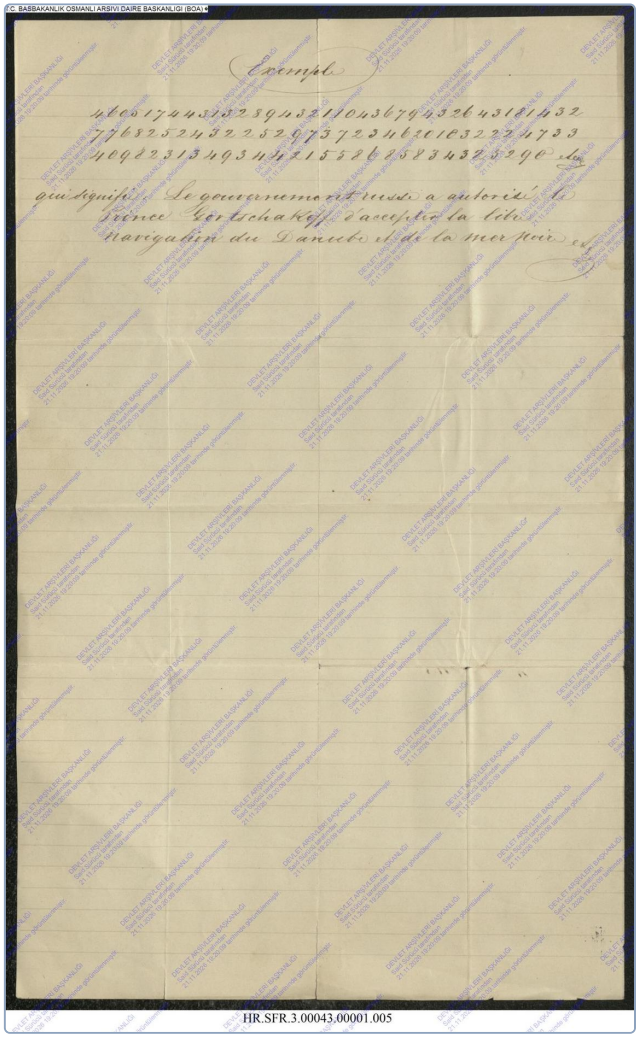


Plate 9 · BOA, HR.SFR.3… 43/1, p. 9 (9 April 1855)
Official worked example accompanying Âlî Pasha's 9 April 1855 key, proving prefix-free single-digit null '4' insertion.

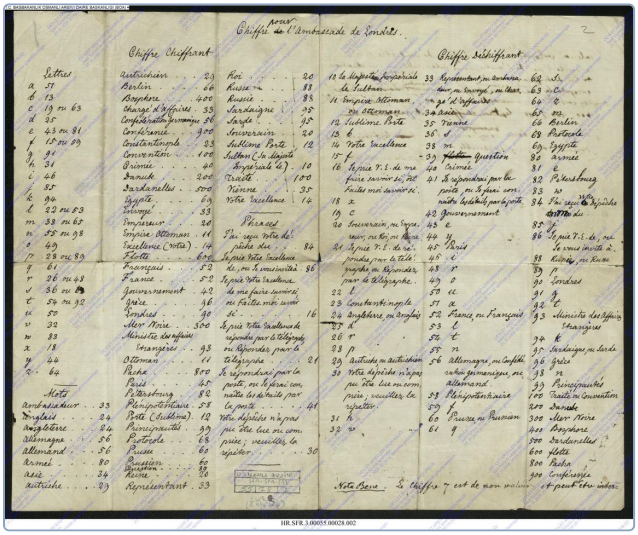


Plate 10 · BOA, HR.SFR.3… 55/28, p. 1 (1856)
'Primitive telegraph cipher' — original London Embassy key sheet matching the 25 July 1856 Crimean War Kars telegram 100%.

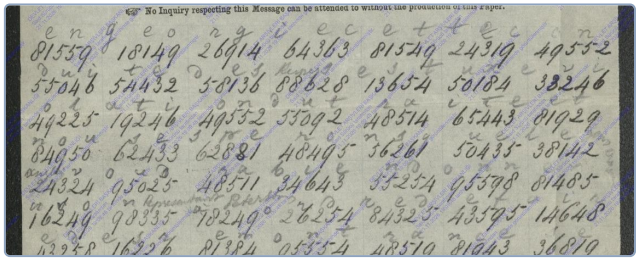


Plate 11 · BOA, HR.SFR.3… 28/15 (25 July 1856 · Zoom)
Earliest live Ottoman submarine telegraph cipher (Cornhill Station, London) with contemporary embassy pencil decryption above the 5-digit blocks.

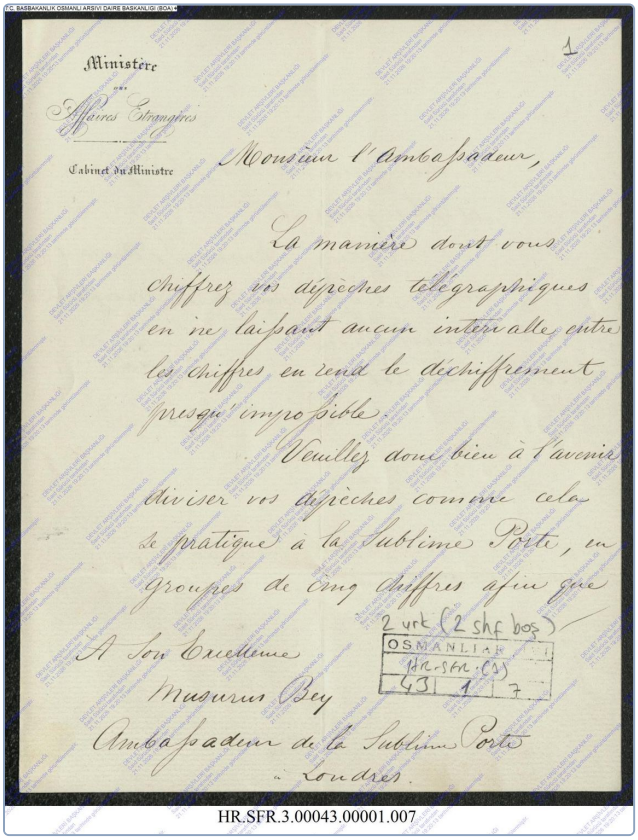


Plate 12 · BOA, HR.SFR.3… 43/1, p. 11 (25 Sept 1856)
Birth certificate of the 73-year Ottoman 5-digit group standard: Foreign Minister Fuad Pasha orders Musurus Bey to divide telegrams 'en groupes de cinq chiffres'.

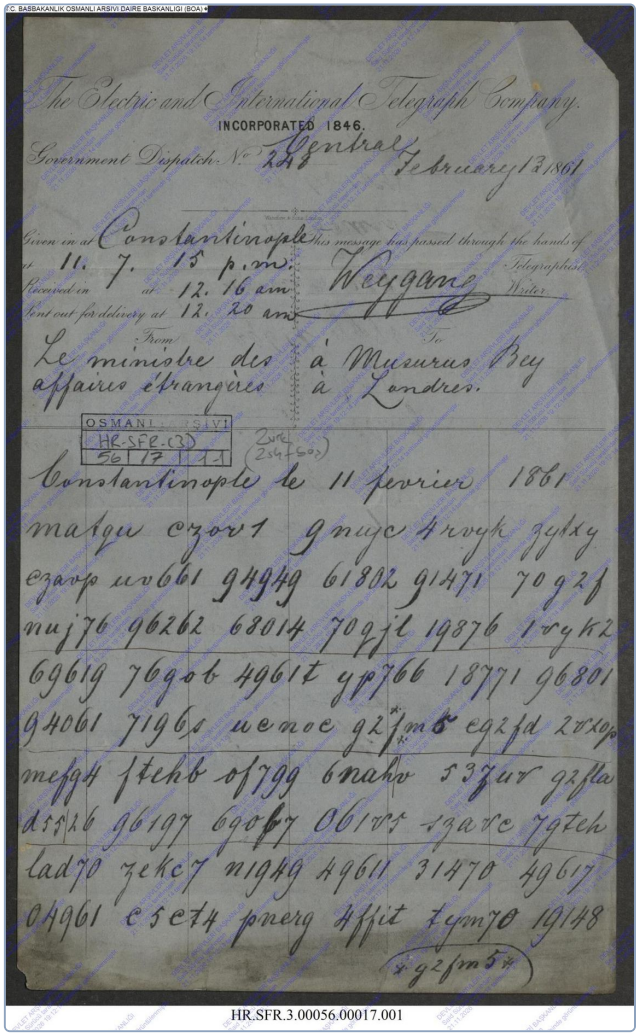


Plate 13 · BOA, HR.SFR.3… 56/17 (11/13 Feb 1861)
Live specimen of Fuad Pasha's 14 Jan 1859 codebook reform (Vocabulaire sub Litt. A + daily-changing sub Litt. C) in 5-character alphanumeric blocks.

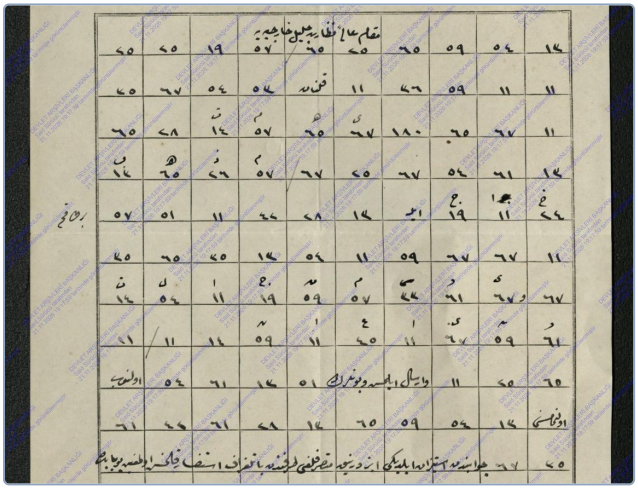


Plate 14 · BOA, HR.MKT. 649/7 (4 April 1869 · Zoom)
Sultan Abdülaziz domestic Ottoman 2-digit telegraph cipher Rosetta Stone (Bosnia → Foreign Ministry, 4 April 1869), alphabetical and excluding digits 0 and 3.