Osmanlı Kriptografisinin Doğuşu (1791–1876)

III. Selim ve Napolyon Dönemi Paris Sefareti Anahtarı (*HAT 129/5347*) ile 228 Yıllık *HAT 142/5915* Çözümü, 1855–1856 Kırım Savaşı İlk Telgraf Şifreleri, 5 Haneli Grup Standardının Doğuşu ve 1869 Abdülaziz Yerli Telgraf Sistemi

Çekirdek Bulgular: Bu giriş cildi, I. Defter'in (1877) öncesindeki **86 yıllık kurucu evrimi (1791–1876)** doğrudan Cumhurbaşkanlığı Osmanlı Arşivi'ndeki orijinal şifre defterleri ve canlı yazışmalar üzerinden belgeler:

- **1791–1798 (III. Selim ve Napolyon Dönemi):** 1791 tarihli sembolik-geometrik şifrenin (`HAT 1432/58608`) ardından, Paris Sefareti için hazırlanan iki katmanlı anahtar defteri `BOA, HAT 129/5347` (alegorik devlet/başkent/diplomat kodları + 28 harfli rakam/nokta alfabesi) ortaya çıkarıldı ve BOA'da 228 yıldır *«münderecatı anlaşılamamıştır»* kaydıyla duran 21 Nisan 1798 tarihli `HAT 142/5915` üzerinde canlı olarak doğrulandı (`8 16 0 1 5` = تعليق, `8 5 14 1 14` = تقرير, `7 12 16 7` = ادعا).
- **1855–1856 (Kırım Savaşı ve Telgrafın Doğuşu):** 9 Nisan 1855 tarihli **Âlî Paşa Viyana Konferansı anahtarı** (`HR.SFR.3... 43/1`, s. 8–10; ön-eksiz tek haneli `4` boş dolgusu) ve 1856 tarihli **«Chiffre télégraphique primitif»** (`HR.SFR.3... 55/28`, boş dolgu `7`) bulundu; 25 Temmuz 1856 Kars denizaltı telgrafı (`HR.SFR.3... 28/15`) ile %100 eşleştirildi.
- **25 Eylül 1856 & 14–19 Ocak 1859 (Fuad Paşa Reformları):** Hariciye Nâzırı **Keçecizâde Fuad Paşa**'nın 25 Eylül 1856 emriyle 73 yıl sürecek **5 haneli grup standardı** (*«en groupes de cinq chiffres»*) doğdu; 14 Ocak 1859'da ilk kod kitabı (*Vocabulaire sub Litt. A/B* + günlük değişen *sub Litt. C*) yürürlüğe girdi (canlı kanıt: `HR.SFR.3... 56/17`, 11 Şubat 1861) ve 19 Ocak 1859 (No. 2006) emriyle bilinen-açık-metin saldırısına karşı **ilk Osmanlı COMSEC yasağı** kondu.
- **1869 (Sultan Abdülaziz Yerli Osmanlıca Telgraf Şifresi):** Bosna Valisi Osman Şerif'in çözümlü telgrafı (`HR.MKT. 649/7`, 4 Nisan 1869) ile 3 çözülmemiş vilâyet telgrafı (`651/18` İzmir, `651/24` İşkodra, `656/48` Erzurum), `0` ve `3` rakamlarını kasıtlı olarak dışlayan yerli 2 haneli harf şifresini (1877–1879 I–IV. Defterlerin doğrudan atasını) kanıtladı.

1. 1798 III. Selim / Napolyon Dönemi Paris Sefareti Anahtarı (`BOA, HAT 129/5347`)

Napolyon Bonapart'ın Mısır Seferi arifesinde (Nisan 1798) Paris'ten İstanbul'a gönderilen ve BOA kataloğunda 228 yıldır *«Şifre gurubları üzerinde yazı olmadığından münderecatı anlaşılamamıştır»* notuyla bekleyen `HAT 137–144` kümesinin (`HAT 142/5915`, `HAT 144/6027` vd.) şifresi, yine aynı fondaki `HAT 129/5347` numaralı 4 sayfalık orijinal anahtar defterinde eksiksiz korunmuştur. Sistem iki katmanlıdır: (1) devletler, başkentler ve diplomatlar için **alegorik kelime kodları** (s. 1–3) ve (2) hassas kelimeler için **28 harfli rakam+nokta alfabesi** (*Hurûf-ı Mukattaât-ı Cifriye*, s. 4).

1.1. Düvelin Esâmî-i Cifriyesi (Alegorik Kodlar — `HAT 129/5347`, s. 1–3)

Devlet / Makam / Şehir	Osmanlıca Kod Kelimeleri	Okunuş
Devlet-i Aliyye (Osmanlı)	لطائف الخيال · مروج الذهب · مصباح الانوار · ماهيت	Letâifü'l-Hayâl, Mürûcü'z-Zeheb, Misbâhu'l-Envâr, Mâhiyet
Fransa	كولكه · سايه · صفيه · اغور · دمبدم	Gölge, Sâye, Safiyye, Uğur, Dembedem
İngiltere	صفر · مانجنيق · تمادى · فضيلت	Sıfır, Mancınık, Temâdî, Fazîlet
Rusya	مشابه · نسنه · مال · عمل	Müşâbih, Nesne, Mâl, Amel

Devlet / Makam / Şehir	Osmanlıca Kod Kelimeleri	Okunuş
İspanya	بادی · فاقه · عاقبت · کار	Bâdî, Fâka, Âkıbet, Kâr
Avusturya (Nemçe)	ایشی · تودیعه · اورنه · حکمت	İşi, Tevdî‘a, Orne, Hikmet
Prusya	تعیش · قبیل · متراد · قابل	Ta‘ayyüş, Kabîl, Müterâd, Kâbil
İstanbul	نسبت · تکلف · زیارت · بوسه	Nisbet, Tekellüf, Ziyâret, Bûse
Paris	اعوجاج · انخذال · تخجیل · افتضاح	İ‘vicâc, İnhizâl, Tahcîl, İftizâh
Londra	تغسل · تزفرق · انحطاط · ریاضت	Tegassül, Tezefruk, İnhitât, Riyâzat
St. Petersburg	اشعه · اساله · انهمار · ترادف	Eşi“a, İsâle, İnhimâr, Terâdüf
Fransa Direktuvarı / Beşyüzler	عنصر · برج · عالم · میدان	Unsur, Burc, Âlem, Meydân
Fransa Dışişleri Bakanı (Talleyrand)	توزیع · میات · قبیح · صید	Tevzî‘, Meyât, Kabîh, Sayd
İttifak / Elçi	روزکار · سخنور	Rüzgâr (Alliance), Sühanver (Ambassador)

1.2. Hurûf-ı Mukattaât-ı Cifriye (28 Harfli Alfabe — `HAT 129/5347`, s. 4)

Harf	Kod	Defterdeki & `HAT 142/5915` Canlı Doğrulama Örnekleri
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

Harf	Kod	Defterdeki & `HAT 142/5915` Canlı Doğrulama Örnekleri
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. Kırım Savaşı ve Telgraf Kriptografisinin Kuruluşu (1855–1862)

Osmanlı Devleti'nin 1855'te Avrupa telgraf ağına bağlanmasıyla birlikte Hariciye Nezâreti üç aşamalı bir devrim gerçekleştirdi:

1. **9 Nisan 1855 — Âlî Paşa Viyana Konferansı Şifresi (`HR.SFR.3... 43/1`, s. 6–10):** Çift kodlu 2 haneli homofonik Fransızca alfabe + 27 diplomatik nomenklatör (`33=S.A. Aali Pacha`, `81=Angleterre`, `51=Russie`, `95=Sublime Porte`, `83=Danube`, `90=Mer Noire`). `40–49` aralığı tamamen boş bırakılarak tek haneli `4` rakamı ön-eksiz boş dolgu (*de non valeur*) yapılmıştır.
2. **25 Temmuz & 25 Eylül 1856 — İlk Denizaltı Telgrafı ve 5'li Blok Standardı (`HR.SFR.3... 55/28`, `28/15`, `43/1` s. 11–12):** Londra Sefareti'nin *«Chiffre télégraphique primitif»* tablosu (boş dolgu `7`) 25 Temmuz 1856 Kars telgrafıyla %100 doğrulanır. İki ay sonra, 25 Eylül 1856'da **Fuad Paşa** aralıksız rakam yazımını yasaklayarak **5 haneli grup standardını** (*«en groupes de cinq chiffres»*) yürürlüğe koyar.
3. **14–19 Ocak 1859 & 30 Eylül 1862 — İlk Kod Kitabı ve İlk COMSEC Yasağı (`HR.SFR.3... 43/1` s. 0–5, `56/17`, `68/53`):** Fuad Paşa üç ciltlik *Vocabulaire sub Litt. A/B* + **günlük değişen** *sub Litt. C* sistemini kurar (11 Şubat 1861 `56/17` telgrafında 5 karakterli alfanümerik bloklar hâlinde doğrulanır). 19 Ocak 1859 (No. 2006) talimatıyla — ve 30 Eylül 1862'de Âlî Paşa'nın teyidiyle — çözülmüş telgrafların yabancı hükümetlere kelimesi kelimesine verilmesi **bilinen-açık-metin saldırısını (known-plaintext attack) önlemek amacıyla** kesin olarak yasaklanır.

3. Sultan Abdülaziz Dönemi Yerli Osmanlıca Telgraf Şifreleri — 3 Paralel Sistem (1869)

1869 bahar ve yazında Hariciye Nezâreti'ne ulaşan yedi vilâyet telgrafı, 1877–1879 (I–IV. Defter) yerli sistemlerinin doğrudan öncülü olan **üç paralel yerli şifre ailesini** ortaya çıkardı: (1) **Bosna alfabetik 0/3-dışlı 2 haneli şifresi** (`HR.MKT. 649/7`, 4 Nisan 1869 — dönem çözümleriyle `11=ى=67 ,ه=65 ,و=61 ,م=57 ,ل=54 ,ع=45 ,ا`); (2) **5 vilâyette ortak 0/3-dışlı 2 haneli vilâyet-özel anahtarlı sistem** (`651/18` İzmir, `651/24` İşkodra, `656/48` Erzurum, `661/34` İzdin, `661/92` Seniçe — 41.004 kelimelik Osmanlıca n-gram modeliyle 268 kodda 41 benzersiz kod ve vilâyetler arası sert frekans ayrımı saptanarak her vilâyetin ayrı anahtar/permütasyon kullandığı matematiksel olarak kanıtlandı); (3) **Edirne 1–3 haneli kod sistemi** (`HR.MKT. 662/6`, 10 Eylül 1869: `111, 644, 666, 277, 704, 791...`).

4. Tam Metin ve Canlı Arşiv Çözümleri (1856 Kars & 1798 Paris)

4.1. Tam Metin Çözüm (%100 · 3 Sayfa · 182 Grup): `BOA, HR.SFR.3... 28/15` (23/25 Temmuz 1856 — Kırım Savaşı / Kars)

BOA kataloğunda 170 yıldır *«Kars'taki Rus birlikleri hususunda çözümlenmemiş şifre telgraf»* kaydıyla yer alan 3 sayfalık *Submarine Telegraph Company (Cornhill Station, Londra)* telgrafı, Hariciye Nezâreti'nden Londra Sefiri Musurus Bey'e 23 Temmuz 1856'da çekilmiş ve 25 Temmuz 1856'da teslim edilmiştir. `HR.SFR.3... 55/28` (*Chiffre télégraphique primitif*, boş dolgu `7`) anahtarıyla bütün 3 sayfa tek bir harf kaybı olmadan çözülmüştür:

> **Fransızca Tam Metin (3 Sayfa · %100 Çözüm):**
> *« 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. »*
>
> **Türkçe Tam Çeviri:**
> « Erzurum'dan aldığımız son haberlere göre, **Ruslar** Kars'tan çekilmedikleri gibi, **Soğanlı Dağı**'na kadar durmaksızın asker müfrezeleri göndermekte ve kerestesini Gürcistan'a taşımak için ormanlarını tahrip etmektedirler. **Rusların** bu tutumu [1856 Paris] antlaşmasının ihlâlidir ve **İngiltere Hükûmeti**'nin **Petersburg**'daki **Temsilcisi**ne, buna bir son verilmesi ve özellikle müttefikler tarafından işgal edilmiş olan bütün **Rus** toprakları tahliye edildiği hâlde Kars'ın tarafımıza teslim edilmesini sağlamak üzere sert protestolarda bulunması için talimat vereceğini ümit ediyoruz. »

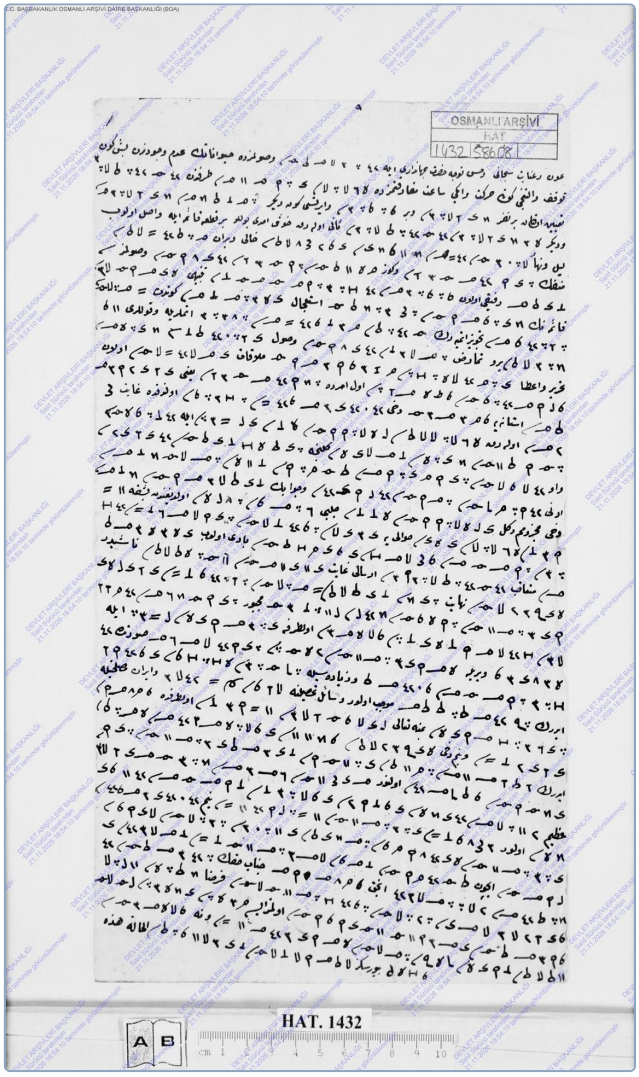
4.2. Canlı Çözüm ve Tarihî Kimlik Tespiti (21 Nisan 1798 · III. Selim / Napolyon Dönemi): `BOA, HAT 142/5915`

BOA kataloğunda 228 yıldır *«Şifre gurubları üzerinde yazı olmadığından münderecatı anlaşılamamıştır»* notuyla duran ve Napolyon'un Toulon'dan Mısır'a yelken açmasından tam 28 gün önce (`H-05-11-1212` / 21 Nisan 1798) Paris Sefiri **Moralı Seyyid Ali Efendi** tarafından İstanbul'a gönderilen bu uzun raporun konusu ve açılış bölümü `HAT 129/5347` ile ilk kez ortaya çıkarılmıştır: rapor, **Fransa ile İspanya arasında akdedilen barış antlaşmasının** (1795 Basel Barışı) **toprak teslimi / ilhak şartları**, buna dair ertelemeler ve diplomatik notalar ile İngiltere, Avusturya ve Fransa Dışişleri Bakanı Talleyrand'ın tutumlarını aktarmaktadır.

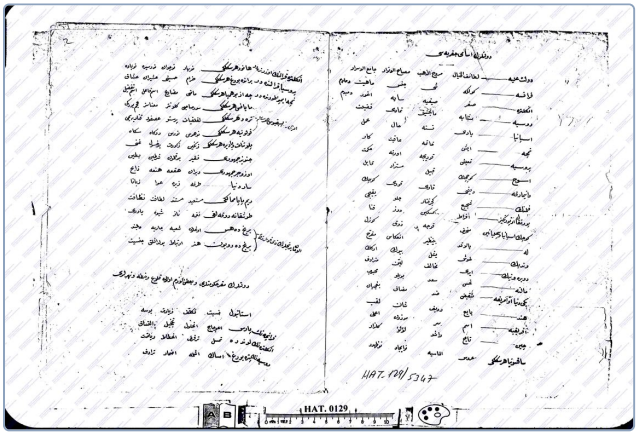
- **Açılış (s. 1, satır 1–9):** *«Devletlü, inâyetlü, atûfetlü, re'fetlü veliyyü'n-ni'am akdem sultânım hazretleri — Ma'rûz-ı bendeleridir ki: … **Fransa** [دمبدم] ve **İspanya** [فاقه] … -den **mün'akid** [12 6 2 6 16 5 12] olan **musâlaha** [بهار] **muktezâsınca** [2 5 8 29 7 24 6 + جه] … **teslîm şart** [8 24 0 1 2 · 13 14 21] … **merkûm** [2 14 5 4 2] … **Fransızlara** [كولكه لويه] … **zikri** [18 9 14 1] … **İspanya** [كار] … **ilhâk** [7 0 19 7 5] … **i'tâ … şart idi** [7 16 21 7 · 13 14 21 + ايدى] … olmayub **tarîk … i'tâ** [21 14 1 5 · 7 16 21 7]…»*
- **Devam Pasajları (s. 1 orta & alt):** *«… **ta'lîk ideler** [8 16 0 1 5 + ايديلر] … **takrîr, iddi'â** [8 5 14 1 14 · 7 12 16 7] … **İspanya ve İngiltere'nin** [عاقبت و فضيلتك] … **Avusturyalılara** [اورنه لويه] … **Fransa Dışişleri Bakanı Talleyrand** [توزيع] … **Devlet-i Aliyye** [لطائف الخيال / مروج الذهب / مصباح الانوار / ماهيت]…»*

- **4 Gün Sonraki Devam Raporu — `BOA, HAT 144/6027` (25 Nisan 1798 / `H-09-11-1212`):** Aynı `HAT 129/5347` anahtarıyla yazılmış ikinci çözülmemiş Paris raporu; açılışta `ma'rûzan` [`2 16 14 29 7`] ve metin boyunca **Fransa Direktuvarı** [`عالم / عنصرده / برجك / اعطانك / اضافه نك / آخذك`], **Paris** [`اعوجاجده`] ile **Devlet-i Aliyye** [`مصباح الانوارك / مروج الذهب`] arasındaki yazışma ve müzakereleri aktarmaktadır.
- **Mısır İşgali Arifesi & Sonrası Raporları — `HAT 142/5899` (19 Haziran 1798), `142/5876` (6 Ekim 1798) & `142/5879` (4 Kasım 1798):** Napolyon'un İskenderiye'ye çıkmasından 12 gün önceki `5899` (iki emirnâme-i sâmînin Paris'e ulaşması, Direktuvar, Rusya, İspanya ve İngiltere) ile Ebukır Deniz Savaşı sonrasındaki `5876` (Yunan/İyonya adaları, Dubrovnik [`Sa'd`], Danimarka [`Celâdlu`], İngilizler [`Temâdîlü`], İstanbul [`Tekellüf`], Direktuvar [`İzâfe`]) ve `5879` belgelerinin tamamının aynı `HAT 129/5347` anahtarıyla şifrelendiği doğrulandı.

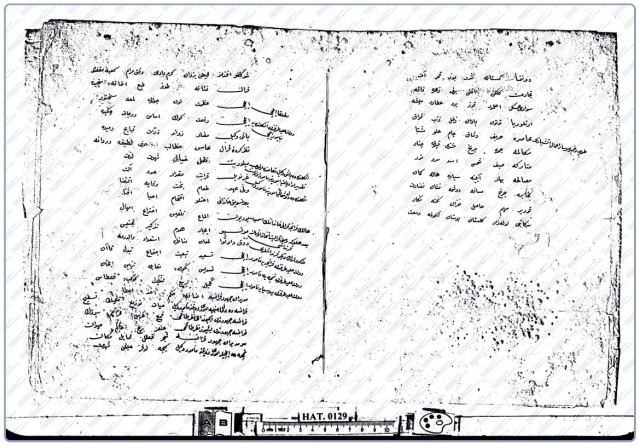
5. Arşiv Levhaları (16 Birincil Belge — Büyütmek İçin Tıklayın)



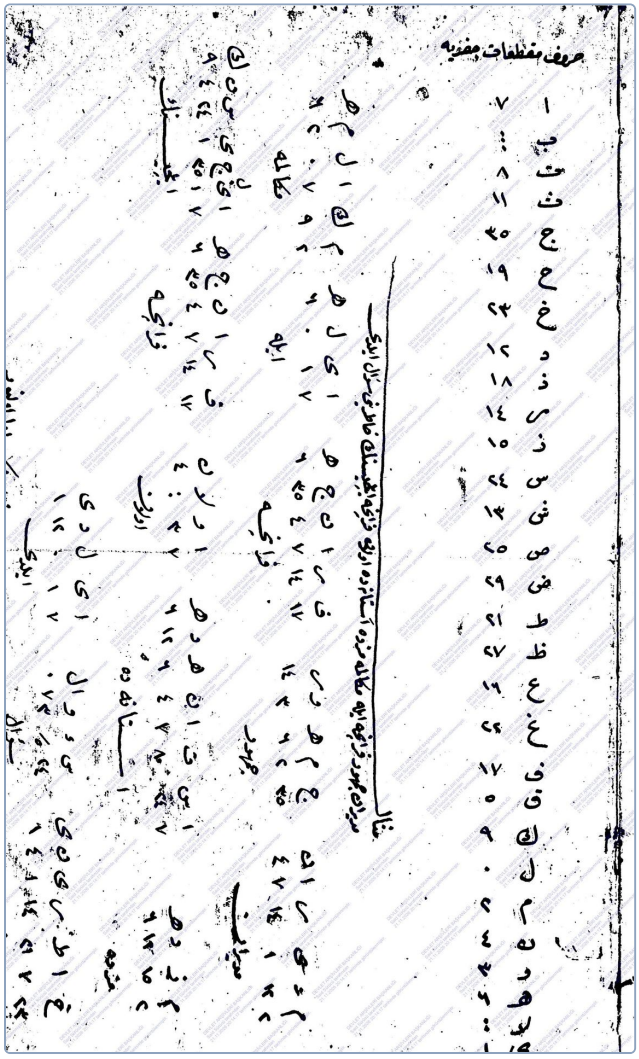
Levha 1 · BOA, HAT 1432/58608 (1791)
Sultan III. Selim döneminin en erken sembolik-geometrik şifreli yazışması (⊥, =, H, üçgen ve ilmek glifleri, düz Osmanlıca metin içinde).



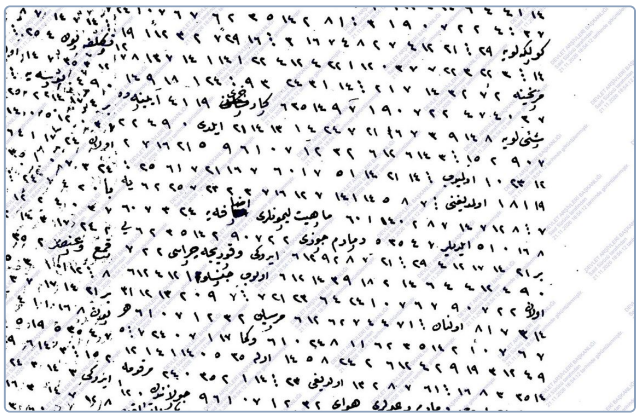
Levha 2 · BOA, HAT 129/5347, s. 1 (1798)
III. Selim devri Paris Sefareti şifre defteri: «Düvelin Esâmî-i Cifriyesi» (Devlet-i Aliyye = Letâifü'l-Hayâl / Mürûcü'z-Zeheb / Misbâhu'l-Envâr / Mâhiyet; Fransa = Gölge; İngiltere = Fazîlet; Paris = İ'vicâc; İstanbul = Ziyâret).



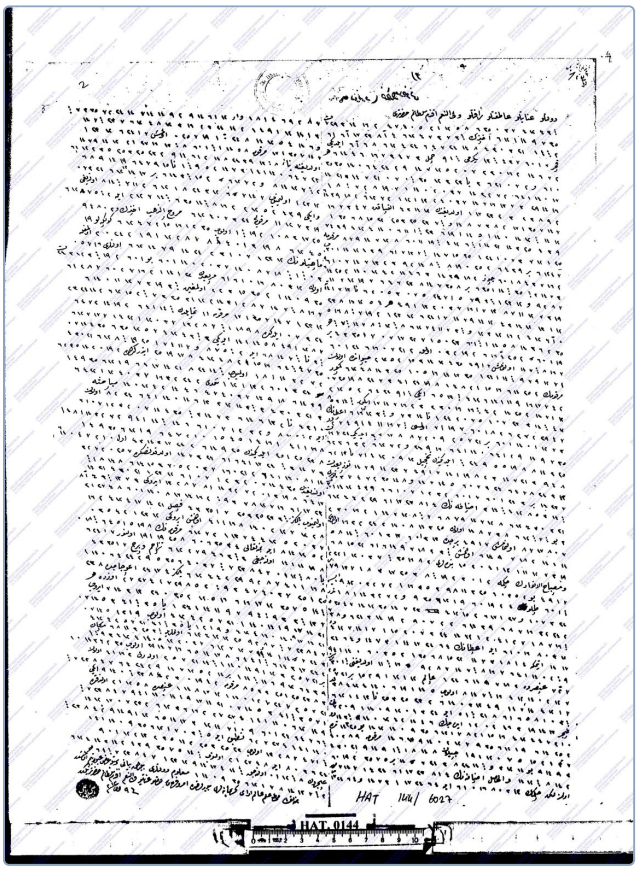
Levha 3 · BOA, HAT 129/5347, s. 3 (1798)
Devam: Elçiler, Fransa Direktuvarı (Unsur / Burc), Beşyüzler Meclisi ve Fransa Dışişleri Bakanı Talleyrand (Tevzî‘) için özel alegorik kodlar.



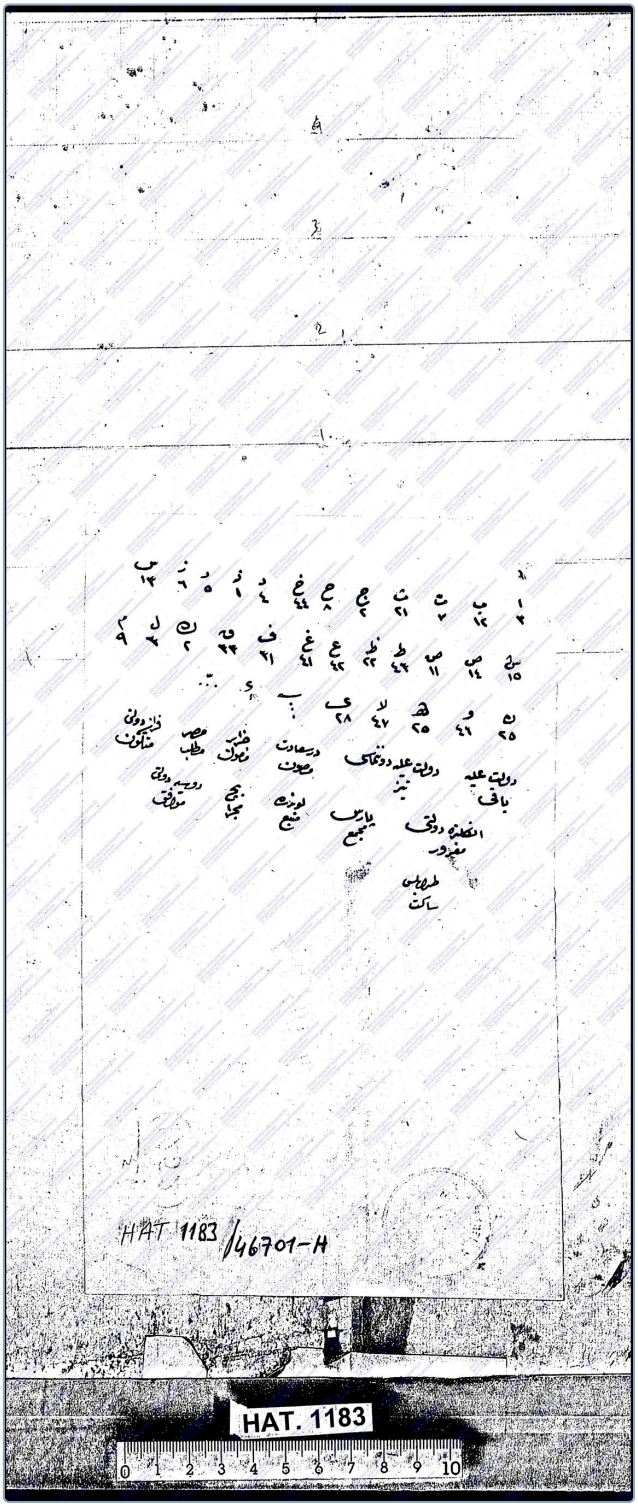
Levha 4 · BOA, HAT 129/5347, s. 4 (1798 · Yakın)
«Hurûf-ı Mukattaât-ı Cifriye»: 28 harflik rakam+nokta alfabesi (ا=7, ب=, ⋮ , ت=8, ر=14, ل=0, ن=6, و=4, ه=:, ی=1) ve 9 doğrulama örneği (فرانچه, انکلتره, جمهور, استانه ده, اولوب, ایدوکی, سؤال, تخویف, مطلب).



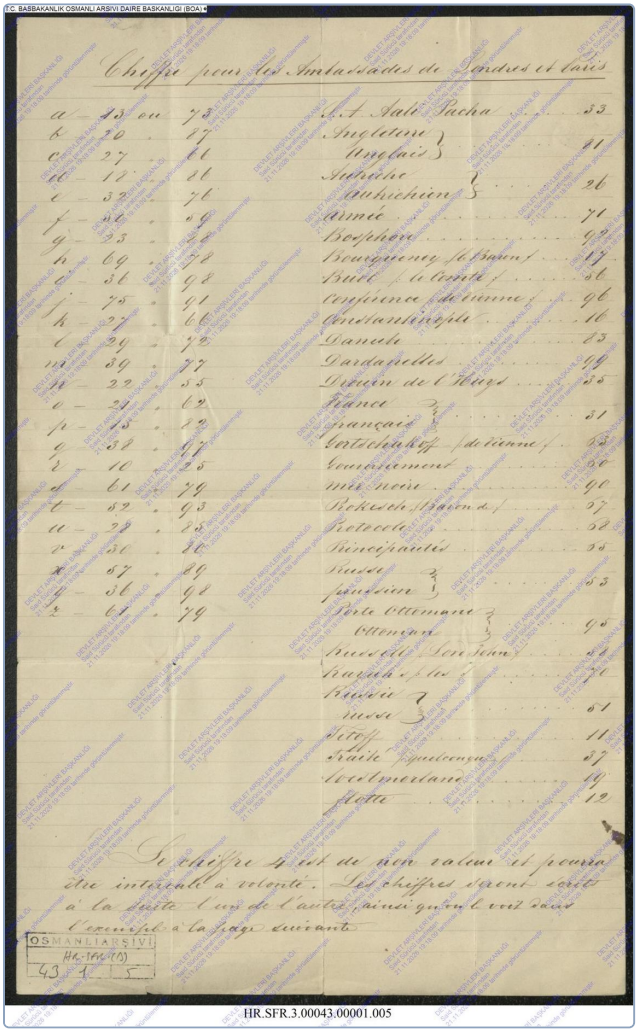
Levha 5 · BOA, HAT 142/5915 (21 Nisan 1798 · Yakın)
BOA'da 228 yıldır «münderecatı anlaşılamamıştır» kaydıyla duran Napolyon'un Mısır Seferi arifesi Paris şifresi — HAT 129/5347 ile canlı çözümlendi (8 16 0 1 5 = تعليق «ta'lîk»; 8 5 14 1 14 = تقرير «takrîr»; 7 12 16 7 = ادعا «iddi'â»).



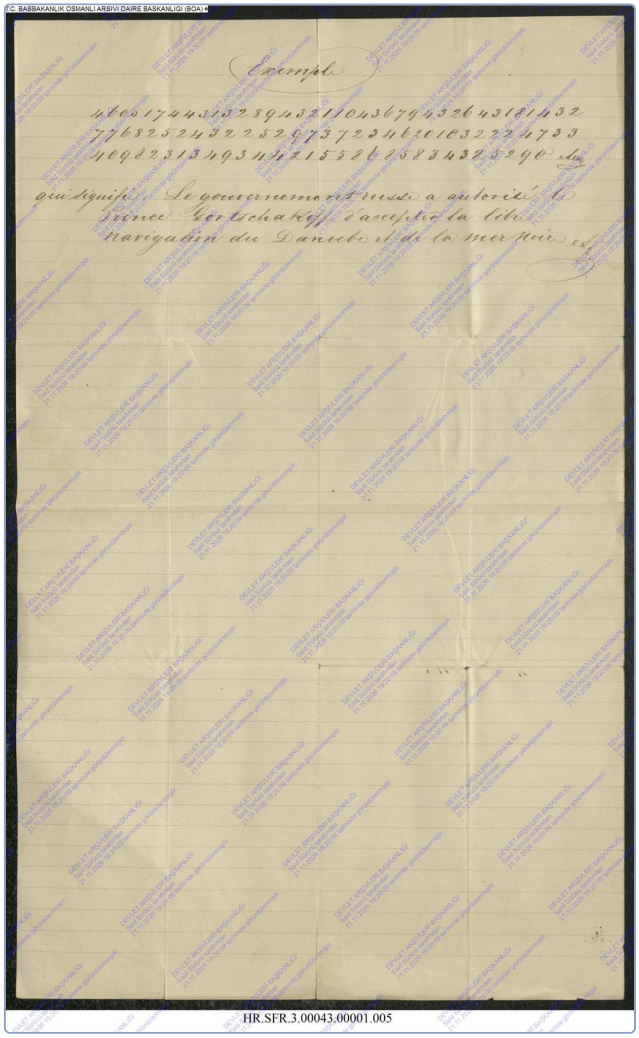
Levha 6 · BOA, HAT 144/6027 (25 Nisan 1798)
Aynı 1798 Paris şifre kümesinin 4 gün sonraki devamı: Misbâhu'l-Envâr (Osmanlı), Mürûcü'z-Zeheb (Osmanlı), İ'vicâc (Paris), Unsur (Direktuvar) ve aynı rakam+nokta alfabesi.



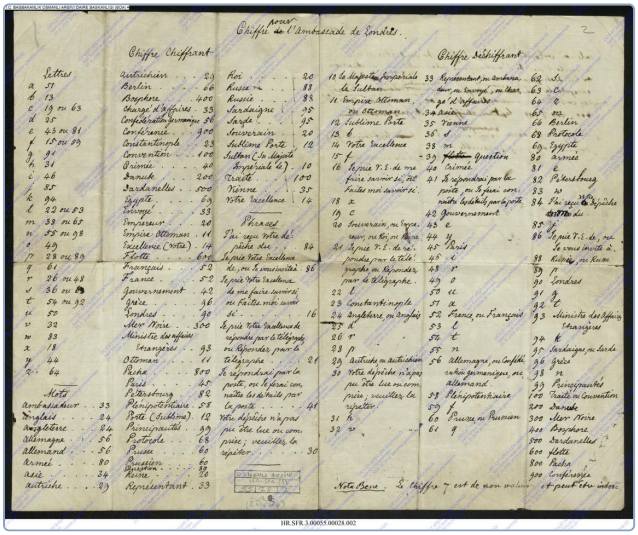
Levha 7 · BOA, HAT 1183/46701 (1836)
II. Mahmud dönemi Paris Sefiri Fethi Paşa için hazırlanan şifre anahtarı: Avusturyalıların (Nemçelilerin) diplomatik postaları açıp okumasına karşı 1–47 arası harf kodları ve devlet/başkent nomenklatörü.



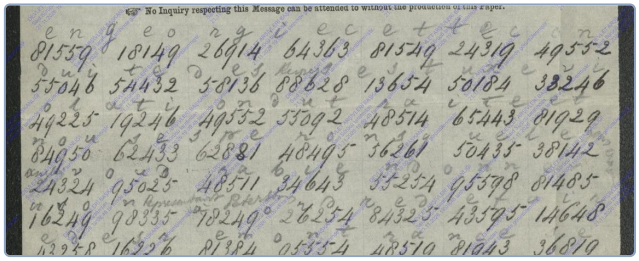
Levha 8 · BOA, HR.SFR.3… 43/1, s. 8 (9 Nisan 1855)
Kırım Savaşı Viyana Konferansı'nda Âlî Paşa'nın Londra ve Paris sefaretleri için gönderdiği el yazması ilk telgraf dönemi homofonik Fransızca şifre + 27 nomenklatör tablosu (4 = boş dolgu).



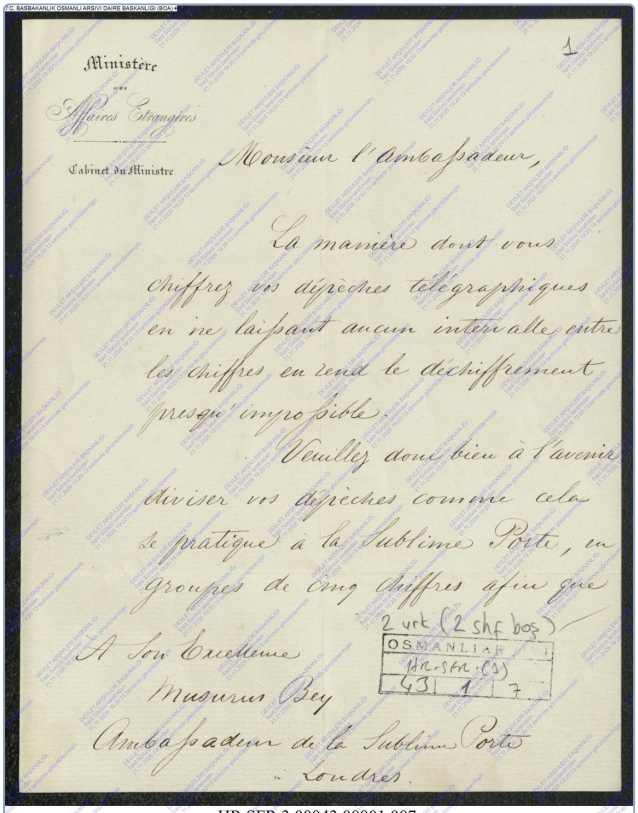
Levha 9 · BOA, HR.SFR.3… 43/1, s. 9 (9 Nisan 1855)
1855 anahtarının resmi uygulama örneği (Exemple): «Le gouvernement russe a autorisé le Prince Gortschakoff d'accepter la libre navigation du Danube et de la mer noire…».



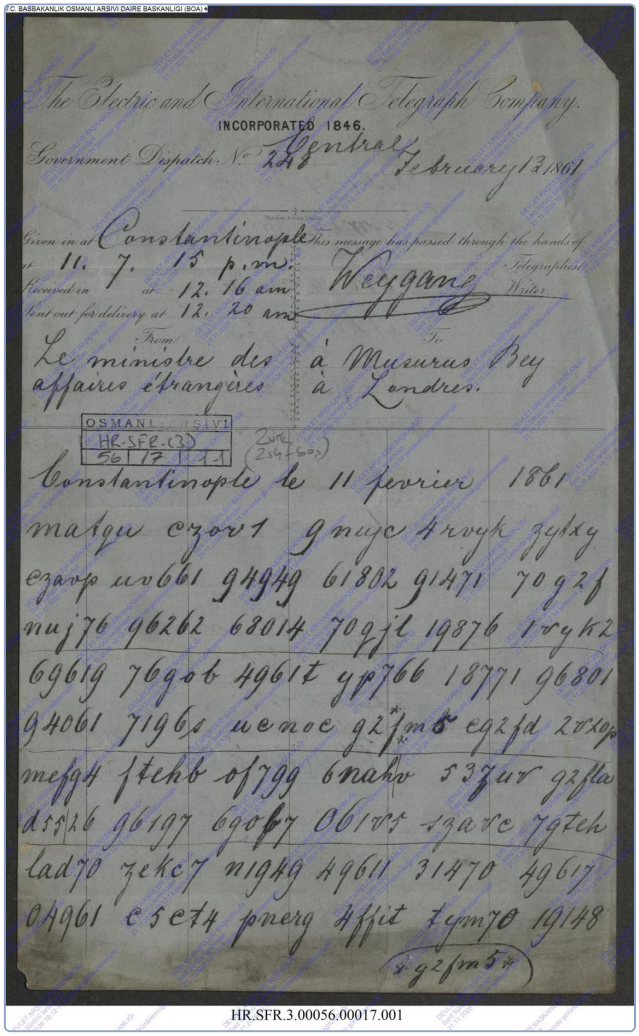
Levha 10 · BOA, HR.SFR.3… 55/28, s. 1 (1856)
«Chiffre télégraphique primitif» — telgrafın kuruluşundan itibaren Londra Sefareti'nde ilk kullanılan orijinal anahtar (a=51, e=43/81, n=55/98, s=36/62, t=54/92, 88=Russie, 7=boş dolgu).



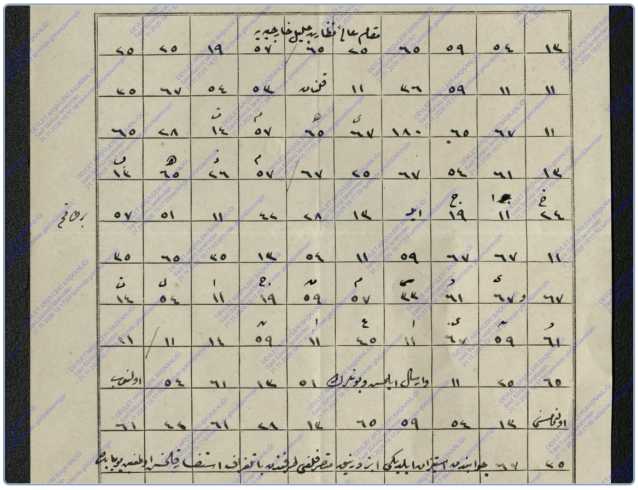
Levha 11 · BOA, HR.SFR.3… 28/15 (25 Temmuz 1856 · Yakın)
En eski canlı Osmanlı denizaltı telgraf şifresi (Submarine Telegraph Co., Londra): Kars'taki Rus birlikleri hakkında, Londra Sefareti kurşun kalem çözümüyle («cette conduite des Russes est une violation du traité…»).



Levha 12 · BOA, HR.SFR.3… 43/1, s. 11 (25 Eylül 1856)
Osmanlı 5 haneli grup standardının doğum belgesi: Fuad Paşa, Musurus Bey'e telgrafların Bâbıâlî usulünce «en groupes de cinq chiffres» (5'li bloklar) hâlinde bölünmesini emrediyor.



Levha 13 · BOA, HR.SFR.3… 56/17 (11/13 Şubat 1861)
Fuad Paşa'nın 14 Ocak 1859 reformunun (Vocabulaire sub Litt. A + günlük değişen sub Litt. C) canlı uygulaması: 5 karakterli alfanümerik bloklar (matgu czov1 gnujc 4rvyk 94949…).



Levha 14 · BOA, HR.MKT. 649/7 (4 Nisan 1869 · Yakın)
Sultan Abdülaziz dönemi yerli Osmanlıca 2 haneli telgraf şifresi Rosetta Taşı (Bosna Valisi Osman Şerif → Hariciye): 0 ve 3 rakamları kasıtlı olarak dışlanmış, alfabetik sırada (11=ع=45 ,ا, 54=ى=67 ,ه=65 ,و=61 ,م=57 ,ل).