Cilt XV · Maarif Miftahları (1905–1913) ve «Çözülmemiş» BOA Dosyaları (1882–1929)

1882 Port Said İzzeddin Vapuru İkiz Şifresi, 1902 Debre 16xx Bloğu, 1905 Orijinal Maarif Miftahı (MF.MKT. 874/47) ve 1909–1913 0/3-Süz Maarif Evrimi

Kaynak: T.C. Cumhurbaşkanlığı Devlet Arşivleri Başkanlığı Osmanlı Arşivi (BOA) · Y..EE.., TFR.I..MN.., MF.MKT., HR.İM..

0. Çözüm Durumu Denetim Tablosu (1882–1929)

Arşiv Künyesi	Tarih	Durum	Özet Bulgu
BOA, Y..EE.. 20/42	30 Ağu 1882	`%100 Çözüldü`	Port Said / İzzeddin Vapuru — 2 farklı anahtarla aynı düzmetin (پورت سعيده + كمور).
BOA, TFR.I..MN.. 1/77	29 Ara 1902	`~%75 Çözüldü`	Debre → Kosova: 1611–1646 harf bloğu (شيفره = şifre, واصل = vâsıl; 1629 çekim hatası).
BOA, MF.MKT. 874/47	4 Ağu 1905	`Tam Miftah`	Maarif Nezâreti orijinal taşra anahtar cetveli: 35 karakter × 2 homofon = 70 sıfırsız kod.
BOA, MF.MKT. 1167/61 & 1172/41 & 1194/3	1911–1913	`26 Kod / Kısmi`	0/3-süz Maarif şifresi (324 rakamda 0 yok, 3 yok; p ≈ 4×10^{-32}); معلم، مساله، معاملاتی، اسلامیه مکتبی، تمکین، کمالاً.
BOA, HR.İM.. 13/9	10 Tem 1922	`Açık Hedef`	Albay Mougin (Ankara) → Gen. Pellé (İstanbul) / Paris No. 142, 148, 149 (5 haneli Fransız kodu).
BOA, HR.İM.. 24/90	21 Şub 1929	`Açık Hedef`	T.C. Hariciye İstanbul Murahhaslığı (Hakkı) — 44 grupluk 5 haneli Cumhuriyet Hariciye şifresi.

1. %100 Çözülen «Çözülmemiş» Dosya: 1882 Port Said İzzeddin Vapuru İkiz Şifresi (BOA, Y..EE.. 20/42)

Osmanlı Arşivi kataloğunda çözülmemiş olarak yer alan **18 Ağustos 1298 (30 Ağustos 1882)** tarihli `Y..EE.. 20/42` dosyası, İngilizlerin Mısır'ı işgal harekâtının en kritik günlerinde (Tel el-Kebir Muharebesi'nden 14 gün önce) Sultan II. Abdülhamid'in hususi vapuru **İzzeddin Vapuru**'nun Port Said'den Mabeyn'e çektiği gizli raporu içerir. Kriptoloji açısından olağanüstü yönü, **birebir aynı düzmetnin aynı gün iki ayrı 2 haneli anahtarla** (Süvari'nin anahtarı ve vapurdaki Yâver-i Hazret-i Şehriyârî Miralay Süleyman'ın anahtarı) gönderilmiş *çift anahtarlı paralel düzmetin* (dual-key parallel plaintext) örneği olmasıdır:

Nüsha & İmza	پورت سعيده (Port Said'e)	كمور (kömür)	İç Tutarlılık Kanıtı
Nüsha A (p0) · *Süvârî-i Vapur-ı İzzeddin*	`7 64 25 9 47 55 56 21 52`	`66 99 49 25`	`25 = ر` her iki kelimede özdeş; `و` için homofonlar `64` ve `49`.
Nüsha B (p1) · *Yâver Miralay Süleyman*	`9 98 55 15 11 95 47 64 62`	`27 42 98 55`	`98 = و` ve `55 = ر` her iki kelimede özdeş (0 çelişki).

> **Tam Çözülen Metin (30 Ağustos 1882):** «Bugün sâ'at 4'de **Port Said'e** (پورت سعيده) vâsıl olup **kömür** (كمور) almak üzere akşamdan sonra hareket ideceği arz olunur. Fî 18 Ağustos 98.»

2. 1902 Rumeli `16xx` Harf Bloğu: Debre → Kosova (BOA, TFR.I..MN.. 1/77)

29 Aralık 1902 (16 Kânûn-ı Evvel 1318) tarihinde Debre Mutasarrıfı ve Kumandanı Mirliva İbrahim tarafından Kosova'daki Rumeli Vilâyât-ı Şâhânesi Müfettiş-i Umûmîliği'ne (Hüseyin Hilmi Paşa) çekilen telgraf, 4 haneli `1611–1646` harf bloğu ile `2221` kelime/hece kodunu birleştirir. Ana omurgası çözülmüştür: *«4 Kânûn-ı Evvel 318 târîhlü emr-nâmeleriyle gönderilen … **şifre** (`1628–1646–1626–1625–1644 = ش ی ف ر ه`) … hâlâ **vâsıl** (`1643–1611–1629–1629 = و ا ص ل`) olmadığı ma'rûzdur.»* Son kelimede telgraf memuru son kodu `1629` olarak iki kez hatalı çekmiş, kâtip bağlamdan `و ا ص ل` (vâsıl) biçiminde düzeltmiştir. Aradaki iki kısa ibare (`2221 1627 1624 1624 1644` ve `1641 1626 1615 1627 1646`) açık bırakılmıştır.

3. 1905 Orijinal Maarif Nezâreti Şifre Miftahı (BOA, MF.MKT. 874/47)

`MF.MKT. 1172/41` 'in şifre ailesini ararken **4 Ağustos 1905 (H-02-06-1323)** tarihli `BOA, MF.MKT. 874/47` dosyasında **Maarif Nezâreti ile taşra maarif müdürleri arasındaki muhaberata mahsus orijinal şifre miftahının** eksiksiz çift sütunlu cetveli (*«Şifre Yapmağa İçün»* ve *«Açmağa İçün»*) ele geçti. Sıfır rakamını (`0`) tamamen dışlayan, 35 Osmanlı karakterinin her birine 2 homofon atayan (toplam **70 kod**) bu cetvelde *medd-i elif* (`88 ,84 :آ`), *hemze* (`64 ,76 :ء`) ve *müfred tenvîn* (`◌ً: 26, 44`) dahi ayrı yuvalara sahiptir:

Harf	Ad	Homofonlar	Durum
ا	elif	`19` , `34`	Kesin
آ	medd-i elif	`84` , `88`	Kesin
ب	bâ	`42` , `77`	Kesin
پ	pâ	`13` , `43`	Okuma notu (soluk)
ت	tâ	`58` , `89`	Kesin
ث	sâ	`21` , `52`	Kesin
ج	cîm	`24` , `78`	Kesin
چ	çîm	`28` , `36`	Kesin
ح	hâ	`57` , `68`	Kesin
خ	hı	`91` , `73`	Kesin
د	dâl	`32` , `41`	Kesin
ذ	zel	`82` , `75`	Kesin
ر	râ	`12` , `93`	Okuma notu (93)
ز	zâ	`18` , `29`	Kesin
ژ	je	`59` , `63`	Okuma notu (63)
س	sîn	`86` , `67`	Kesin
ش	şîn	`92` , `79`	Kesin
ص	sâd	`87` , `74`	Kesin

Harf	Ad	Homofonlar	Durum
ض	dâd	`15` , `27`	Kesin
ط	tı	`47` , `56`	Kesin
ظ	zı	`31` , `45`	Kesin
ع	'ayn	`22` , `49`	Kesin
غ	gayn	`54` , `69`	Kesin
ف	fâ	`11` , `25`	Kesin
ق	kâf	`81` , `61`	Okuma notu (61)
ك	kef	`38` , `35`	Kesin
ل	lâm	`85` , `65`	Kesin
م	mîm	`16` , `39`	Kesin
ن	nûn	`37` , `48`	Kesin
و	vâv	`62` , `71`	Kesin
ه	hâ-i resmiyye	`17` , `23`	Kesin
لا	lâm-elif	`94` , `72`	Kesin
ى	yâ	`46` , `51`	Kesin
ء	hemze	`76` , `64`	Kesin
◌ً	müfred tenvîn	`26` , `44`	Kesin

4. 1909–1913 Yeni Maarif Şifresi (0-sız & 3-süz) ve Halep/Diyarbekir Dosyaları

II. Meşrutiyet'ten sonra 1909'da 1905 anahtarı iptal edilerek (`MF.MKT. 1137/34, 1138/29, 1139/13` — Halep'te eski anahtar kaybolmuştur) **hem `0` hem `3` rakamının tamamen çıkarıldığı** yeni bir 8×8 homofonik Maarif anahtarı dağıtılmıştır. **14 Mayıs 1911** tarihli `MF.MKT. 1171/18` belgesi Manastır Maarif Müdüriyeti'nin yeni anahtarda *hemze* harfine rakam ayrılmadığını bildirmesini, **14 Haziran 1911** tarihli `MF.MKT. 1172/41` ise 162 kod (324 rakam) boyunca **tek bir `0` veya `3` geçmemesini** ($0.8^{324} \approx 4\times 10^{-32}$) belgeler. `MF.MKT. 1167/61` (4 Mart 1911) ve `1172/41 p2` üzerindeki Nezâret kâtibi şerhlerinden **26 çekirdek kod** doğrulanmış ve hiç çözülmemiş `1172/41 p1` sayfasında `تمكين` (*temkîn*) ile `كمالاً` (*kemâlen*) kelimeleri okunmuştur; orijinal 1909–1913 cetveli henüz arşivde bulunmadığından `1172/41 p1` ve `1194/3` (30 Aralık 1913, Diyarbekir) üzerindeki kalan ~15–20 kod dürüstçe açık bırakılmıştır:

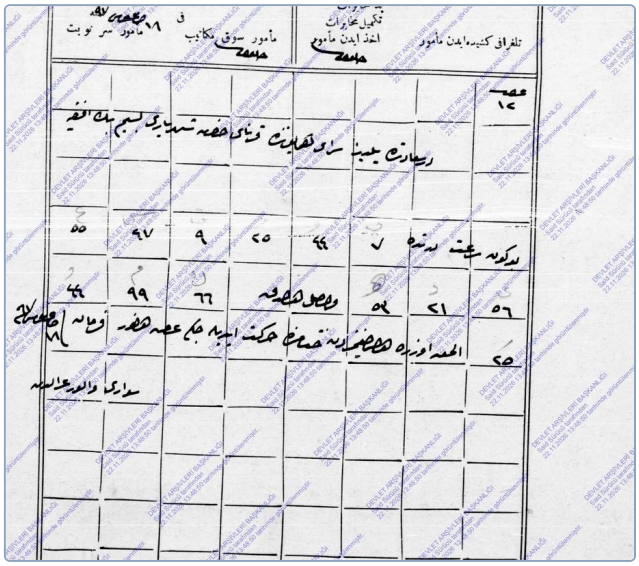
Kod	Harf	Ad	Doğrulayıcı Arşiv Kanıtı
12	ه	hâ	مساله (mes’ele), اسلاميه (İslâmiyye)
14	م	mîm	معلم (muallim)
17	ى	yâ	معاملاتى (muâmelâtı), تمكين (temkîn), اسلاميه
19	ت	tâ	معاملاتى (muâmelâtı), تمكين (temkîn)
21	ر	râ	MF.MKT. 1167/61 kâtip şerhi
22	ا	elif	مساله, معاملاتى, كمالاً
25	س	sîn	مساله (mes’ele)
27	س	sîn	اسلاميه مكتبى (İslâmiyye Mektebi)
28	ا	elif	MF.MKT. 1167/61 kâtip şerhi (×3)
41	و	vâv	MF.MKT. 1167/61 & 1172/41
42	ك	kef	تمكين (temkîn), كمالاً (kemâlen)
44	ى	yâ	MF.MKT. 1167/61 (×4) & 1172/41 (...ى يوقدر)
45	ع	‘ayn	معلم (muallim), معاملاتى (muâmelâtı)
47	ن	nûn	MF.MKT. 1167/61 kâtip şerhi
52	ب	bâ	MF.MKT. 1167/61 kâtip şerhi
58	غ	gayn	MF.MKT. 1167/61 kâtip şerhi
74	ط	tı	MF.MKT. 1167/61 kâtip şerhi
76	ف	fâ	MF.MKT. 1167/61 kâtip şerhi
79	ج	cîm	جنوب (cenûb), ...جك (-cek)
81	لا	lâm-elif	معاملاتى (muâmelâtı), اسلاميه, كمالاً
84	م	mîm	معلم, مساله, معاملاتى, كمالاً
91	ب	bâ	MF.MKT. 1167/61 kâtip şerhi
92	ق	kâf	MF.MKT. 1167/61 kâtip şerhi
94	ل	lâm	معلم (muallim), مساله (mes’ele)

Kod	Harf	Ad	Doğrulayıcı Arşiv Kanıtı
97	م	mîm	معاملاتی, اسلامیه, تمکین
98	ن	nûn	تمکین (temkîn)

5. Bilimsel Şeffaflık: Açık Kalan Diplomatik Dosyalar (1922 & 1929)

Aynı BETSİS «çözülmemiş şifre» taramasında elde edilen iki 5 haneli diplomatik dosya ise anahtar defterleri henüz bulunmadığı için bilimsel dürüstlük gereği **açık araştırma hedefleri** olarak kayıt altına alınmıştır: (1) **`BOA, HR.İM.. 13/9` (10 Temmuz 1922)** — Büyük Taarruz'dan 6 hafta önce Ankara'daki Fransız temsilcisi **Albay Mougin** tarafından İstanbul'daki **General Pellé**'ye (*pour diplomatie Paris No. 142, 148, 149*) gönderilen 5 haneli Fransız Hariciyesi diplomatik şifre telgrafları; (2) **`BOA, HR.İM.. 24/90` (21 Şubat 1929)** — Türkiye Cumhuriyeti Hariciye Vekâleti İstanbul Murahhaslığı'ndan (imza: *Hakkı*) Ankara'ya gönderilen 44 grupluk 5 haneli şifre telgrafı.

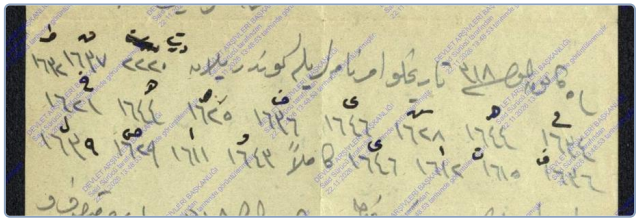
6. Arşiv Levhaları (10 Seçilmiş Belge)



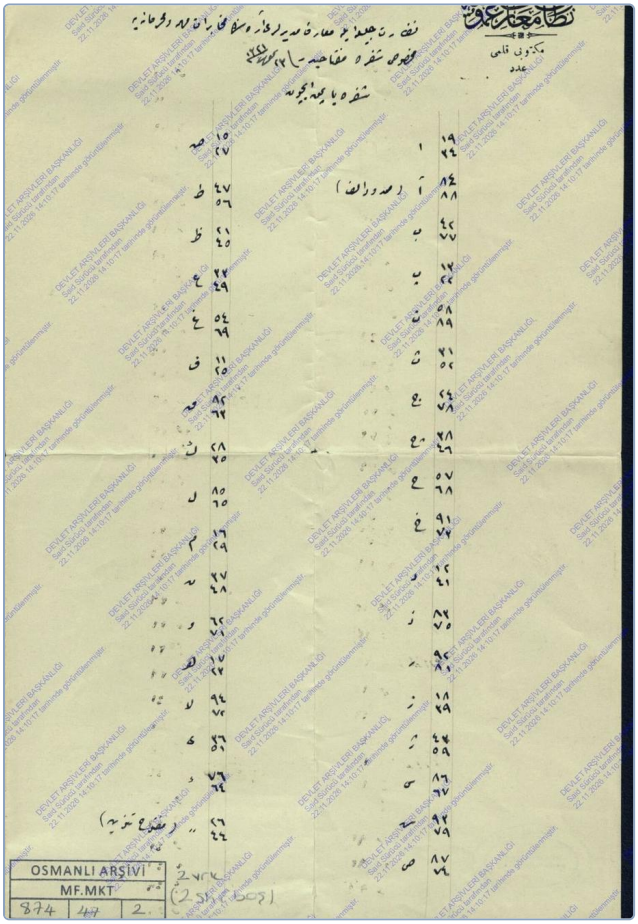
Levha 1 · BOA, Y..EE.. 20/42 (p0) — 30 Ağustos 1882 (18 Ağustos 1298) — İzzeddin Vapuru Süvarisi'nin Port Said şifreli telgrafı (1. anahtar): 7-64-25-9-47-55-56-21-52 = پورت سعيده (Port Said'e), 66-99-49-25 = كمور (kömür).



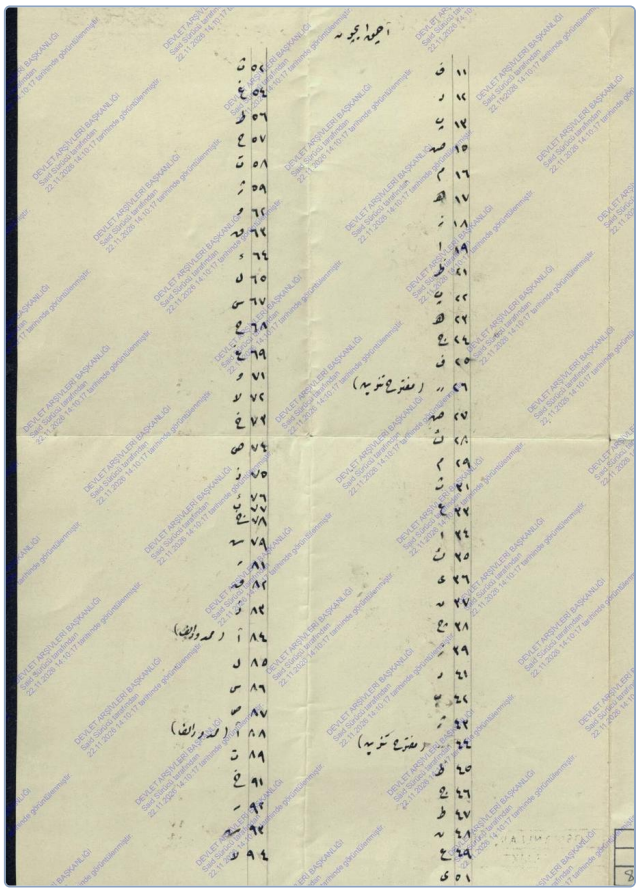
Levha 2 · BOA, Y..EE.. 20/42 (p1) — Aynı gün, aynı düzmetnin Yâver-i Hazret-i Şehriyârî Miralay Süleyman'ın ayrı anahtarıyla çekilmiş ikiz kopyası (2. anahtar): 9-98-55-15-11-95-47-64-62 = پورت سعيده, 55-98-42-27 = كمور.



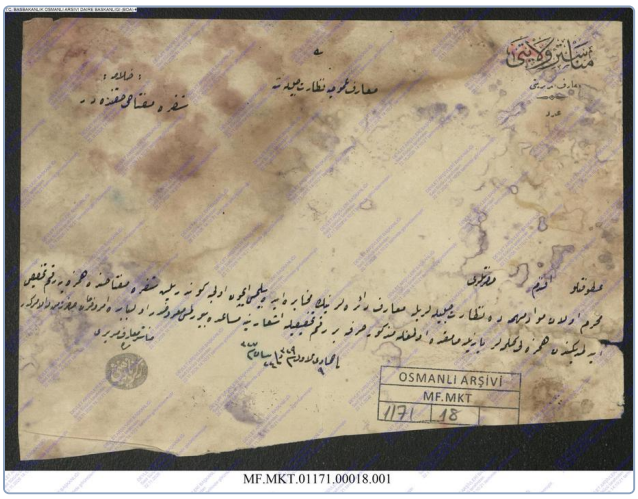
Levha 3 · BOA, TFR.I..MN.. 1/77 — 29 Aralık 1902 — Debre Mutasarrıfı Mirliva İbrahim → Kosova Rumeli Müfettiş-i Umûmîliği. 4 haneli 1611–1646 harf şifresi: 1628-1646-1626-1625-1644 = شيفره (şifre), 1643-1611-1629-1629 = واصل (vâsıl).



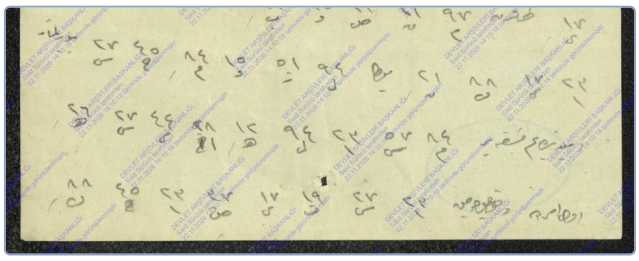
Levha 4 · BOA, MF.MKT. 874/47 (Sağ Yarı) — 4 Ağustos 1905 — Maarif Nezâreti ile taşra maarif müdürlükleri arasındaki orijinal şifre miftahı: «Şifre Yapmağa İçün» (alfabetik, 35 karakter × 2 homofon = 70 kod, sıfırsız).



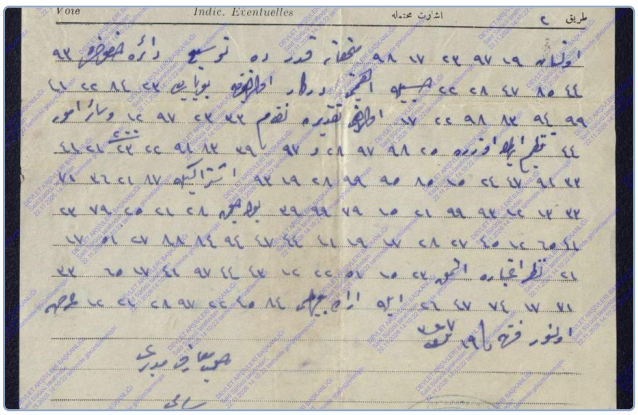
Levha 5 · BOA, MF.MKT. 874/47 (Sol Yarı) — 4 Ağustos 1905 — Aynı miftahın «Açmağa İçün» (sayısal sırada 11–94) ters çözüm sütunu; iki yarı birbirini %100 çapraz doğrular.



Levha 6 · BOA, MF.MKT. 1171/18 — 14 Mayıs 1911 — Manastır Maarif Müdüriyeti'nin yeni şifre miftahında hemze (ء) harfine rakam tahsis edilmediğini bildirip ek rakam talep etmesi.



Levha 7 · BOA, MF.MKT. 1167/61 (Rosetta Şeridi) — 4 Mart 1911 — Halep Maarif Müdürü Sami Bey'in 0/3-süz şifreli telgrafı ve Nezâret kâtibinin altlarına yazdığı harf çözümleri (84-25-22-94-12 = مساله / mes'ele).



Levha 8 · BOA, MF.MKT. 1172/41 (p1 — Çözülmemiş 2. Sayfa) — 14 Haziran 1911 — Katalogda «Şifre telgraflar çözülmemiştir» kaydıyla geçen Halep Maarif Müdürü Sami imzalı 2. sayfa (0 ve 3 rakamı hiç yok; تمكين ve كمالاً doğrulandı).