VAKANÜVİS- Uluslararası Tarih Araştırmaları Dergisi/ International Journal of Historical Researches, Yıl/Vol. 7, Özel Sayı: Dr. Mahmut Kırkpınar'a Armağan (Special Issue: A Tribute to Dr. Mahmut Kırkpınar), ISSN: 2149-9535 / 2636-7777

Araştırma Makalesi/Research Article

19. Yüzyılın İkinci Yarısında Osmanlıda Özel Amaçlı (Göreve Tahsisli) Şifre ve Kodlamalar

Sedat Bingöl*

(ORCID: 0000-0003-2016-2819)

Makale Gönderim Tarihi
18.09.2022

Makale Kabul Tarihi
01.10.2022

Atıf Bilgisi/Reference Information

Chicago: Bingöl, S., "19. Yüzyılın İkinci Yarısında Osmanlıda Özel Amaçlı (Göreve Tahsisli) Şifre ve Kodlamalar", *Vakanüvis-Uluslararası Tarih Araştırmaları Dergisi*, 7/Özel Sayı: Dr. Mahmut Kırkpınar'a Armağan: 1355-1384.

APA: Bingöl, S. (2022). 19. Yüzyılın İkinci Yarısında Osmanlıda Özel Amaçlı (Göreve Tahsisli) Şifre ve Kodlamalar. *Vakanüvis-Uluslararası Tarih Araştırmaları Dergisi*, 7 (Özel Sayı: Dr. Mahmut Kırkpınar'a Armağan), 1355-1384.

Öz

III.Selim döneminde diplomasi anlayışının değişmesine paralel olarak Osmanlı Devleti de diplomatik yazışmalarında kriptografi kullanmaya başlamıştır. Yaklaşık yarım asır boyunca basit seviyeli "Tek Alfabeli (monoalphabetic) Değiştirme (ikame)" şifreleri kullanıldı.

Telgrafın Osmanlıya gelişiyle beraber şifreler azalıp, kodlamalar öne çıktı. Zaman içerisinde geniş kapsamlı Nomanklatörler (isimlendiriciler) oluşturuldu. Gerek Osmanlı harici ve gerek dahili bürokrasisinde Kod-şifrelemede haberleşmesinin temeli oldu. Ancak bu egemen yazışma usulünün dışında, basit düzeyde şifrelemeler özel görevler için yine de kullanılmaya devam etmiştir. Bu çalışmada Osmanlı genel yazışma düzeyinin bir varyantı olarak, göreve tahsisli (özel amaçlı) şifreler ele alınmıştır.

* Doç. Dr., Anadolu Üniversitesi, Edebiyat Fakültesi, Tarih Bölümü, Türkiye, sbingol@anadolu.edu.tr.
Assoc. Prof. Dr., Anadolu University, Faculty of Letters, Department of History, Türkiye.

Anahtar Kelimeler: Kodlar, Şifreler, Tek Alfabe, Kriptografi

Special Purpose (Job Associated) Passwords And Codings In The Ottoman

Abstract

In parallel with the change in the understanding of diplomacy during the reign of Selim III, the Ottoman Empire started to use diplomatic cryptography. For nearly half a century, simple-level "Single Alphabetic (monoalphabetic) Substitution" ciphers have been used. Over time, extensive Nomanculators (namers) have been created. It became the basis of communication in Code-encryption both in Ottoman external and internal bureaucracy. In this study, as a variant of the Ottoman general correspondence level, assigned (special purpose) ciphers are discussed.

Keywords: Codes, Ciphers, Monoalphabet, Cryptography

Giriş

M.Ö. 2000'lere kadar uzanan bir geçmişe sahip olan Kriptografi, yani mesaj açık olmakla beraber bir "mesajın anlamını" saklama çabası Hint, Mezopotamya, Yunan, Roma ve Arap-Müslüman dünyasını da içeren bütün kültürlerde kullanılmıştır.[1] Tarih boyunca sınırlı bir kullanıma sahip olan Kriptografi, 15. yüzyıla gelindiğinde politik alandaki gelişmeler ve Rönesans döneminde sanat ve bilimin gelişimiyle daha geniş ve sürekliliği olan bir kullanım alanı buldu. İtalya'da diplomasinin gelişimi sonucu İtalyan kent devletlerinin birbirlerine büyükelçiler göndermesi, diplomatik haberleşme gereği talimatların gizlenmesi ihtiyacı, Romanın yıkılışı sonrası adeta unutulan (Kriptografi) şifrelemeyi yeniden doğurdu.[2]

Sistemli bir Osmanlı Kriptografisi III. Selim devrinde diplomatik bir alanda doğdu. 29 Ocak 1795'te Londra'ya Yusuf Agah Efendi, Ekim 1796'da Berlin'e Ali Aziz Efendi ve 28 Temmuz 1797'de Paris'e Seyyid Ali Efendi ve Viyana'ya ise İbrahim Afif Efendiler'in Büyükelçi olarak

[1] Sedat Bingöl, "Osmanlı Devleti'nde Kriptografik Uygulamalar ve Kod Defterleri", *Süleyman Demirel Üniv. Fen-Edebiyat Fakültesi Sosyal Bilimler Dergisi*, (2022).

[2] Ioanna Iordanou, *Venedik Gizli Servisi*, çev. Fatih Yücel, Kronik Kitap Yay., İstanbul, 2020, s. 80-84.

atanmalarıyla[3] beraber, Kriptografi'nin kamusal alanda kullanımı başladı.

Osmanlı ikamet elçileri dışında da müzakereler veya antlaşmaları görüşmek için kısa süreli giden, ancak ikamet elçisi olmayan elçilerin de giderek yoğunlaşan şifre ve kod kullandıklarını biliyoruz. 1795-1811 yıllarını içeren ve ilk dönem adını verdiğimiz süreç, Kriptografi'nin emekleme devriydi. Kriptografi'nin bu başlangıç süreci, uygulamadan gelen deneyimlere dayalı olarak gelişmekteydi. Diplomatlara verilen şifre anahtarları, **"**Tek Alfabeli (monoalfabetik) Yerine Koyma (ikame) Şifresi" özelliğine sahipti. Yine şifrelerle birlikte kelime temelli, açık yazılmış sınırlı sayıda da olsa kod kullanılmaktaydı. Herhangi bir anlamı olan veya olmayan "Kod kelime"[4] kullanımları dışında kodların sayısallaştırılması yoluna da gidilmişti.[5]

Ancak Kırım savaşında ve sonrasında Osmanlı Telgraf hatlarının kurulması sonrası yurtdışı temsilciliklerimizle, her harfe karşılık bir sayısal şifre vererek cümlelerin oluşturulması "Tek Alfabeli (mono-alfabetik) Yerine Koyma (ikame) Şifresi" yöntemiyle şifreli telgraf çekmek mümkün değildi. Bu yüzden hariciye bürokrasisi "Tek Alfabeli (mono-alfabetik) Yerine Koyma (ikame) Şifre"lemeyi terk etti. Bunun yerine Homofonik (sesteş) Yerine Koyma Şifresi" anlayışına geçildi. Bu sistem Tek alfabeli sistemden (monoalfabetik) daha yüksek güvenliğe sahip bir sistemdi. Bu sistemde alfabe tek olmakla beraber, numerik karşılıklar (sesler) birden fazlaydı. Şifrelerin arasına rastgele boş sayılar da konularak, güvenliğin daha da artırılması düşünülmüştü. İlave olarak geçmiş şifrelerde de mevcut olan sınırlı sayıdaki kodlamalar eklenmişti.

Öte yandan mesajların numerik şifrelenmesi dışında, kodların sayısallaştırılması yoluna gidildi. Önce Hariciye yazışmalarını Fransızca yaptığı için Fransız alfabesine dayalı "Tek Alfabeli (mono-

[3] E. Kuran, *Avrupa'da Osmanlı İkamet elçiliklerinin Kuruluşu ve İlk Elçilerin Siyasi Faaliyetleri 1793- 1821*, Türk Kültürünü Araştırma Enstitüsü Yayınları, Ankara, 1988, s. 24-25.

[4] Şifre ve kod terimlerinin farklılığı için bkz. Sedat Bingöl, "Serezli (Sirozî) Yusuf Paşa'nın Kriptografisi Hakkında Notlar " *Humanitas*, 2022 (yayın aşamasında)

[5] Sedat Bingöl, "Methods for encryption in early 19th-century Ottoman diplomaticcorrespondence", *Cryptologia* (2021), doi:10.1080/01611194.2021.1919943.

alfabetik)Yerine Koyma (ikame) Şifreler" kullanıldı. Bu yöntem hariciyenin gündelik yazışmaları için kullanıldı. Ancak Büyükelçilerle Hariciye Nazırları arasında çok daha güvenilirliği kanıtlanmış olan bir sisteme geçildi.

6 Temmuz 1856 tarihli Hariciye Nazırı Ali Galip imzasıyla Londra, Paris ve Viyana'daki Türk Elçilerine hitaben gönderilen yazıda, Fransız Alfabesi'ne dayalı "Vigenére Karesi" uygulanarak, "polyalphabetic" çoklu alfabe sistem kullanıldı. Ancak bu yöntem, özellikle gündelik kullanım bakımından kolay olmaması nedeniyle, muhtemelen sürdürülemedi. Hariciye Nezareti zaman içerisinde Kriptografi'de daha da gelişti ve kırılması zor şifreler oluşturularak, sadece kodlardan oluşan bir şifreleme sistemine doğru yönelindi.[6]

Artık "sözleşilmiş harfleri" ifade eden "hurûf-ı ma'hûde" terimi terkedilerek, "Kod" terimi hem harfler düzeyinde hem de kelimeler düzeyinde şifrelemeler için de kullanılmaya başlanmıştı. Nitekim telgraf haberleşmesi için Hariciye'ye ait 1860 tarihli ilk Nomanklatör (isimlendirici) veya ilkel bir "Kod defteri" oluşturulmuştu. Belgenin ön kapağında Fransızca "Chiffre télégraphique primitif" ve ikinci bir başlıkta da Türkçesi "Telgrafın icadından itibaren şifreleme veya deşifre etmede kullanılan yazı" başlığıyla Telgraf haberleşmesinde Kod-Şifreleme'ye vurgu yapılmaktaydı.[7]

Londra Elçiliğimizin bir şifre memuru tarafından hazırlandığı anlaşılan basit bir Nomanklatör ya da bir Kod listesi ortaya çıkmıştı. Oluşan cümle, kelime ve harfler temelindeki 100 civarında Kod-şifre listesi (defteri) zamanla giderek gelişti. Kod Listelerinin geliştirilmesi sonucu 10.000 kelimelik gerek 1871 Paris ve 1877 Londra[8] Nomanklatörleri doğdu.[9]

---

[6] Sedat Bingöl, "The Changes in Ottoman Diplomatic Cryptography and Its Methods During the 19th Century (1811–1877)", *Cryptologia*, (2022), doi: 10.1080/01611194.2022.2092916.

[7] BOA (*Devlet Arşivleri Osmanlı Arşivi*) HR. ŞFR 3. 55-28

[8] Kod defterinin kullanımına dair bilgileri için bkz. Bingöl, "The Changes in Ottoman Diplomatic …"

[9] BOA. HR.SFR.4..._984-1; 984-2

Dahili Haberleşmede Şifre ve Kodlar

Hariciyenin başlattığı şifreli yazışma süreci, zamanla Osmanlı iç yönetim kademelerinde de revaç buldu. Bizim tespit edebildiğimiz kadarıyla Osmanlı bürokrasisinin Kriptolu yazışma uygulamalarının başlangıcı 1816 yılına aittir. 1 Mayıs 1816'da İran'a gönderilen Süleyman Efendi ve Naşid Bey taraflarından "hurûf-ı ma'hûde" ile yazılan bir tahriratta[10] görünen şifre salt sembollerden oluşmaktaydı. [11] Ayrıca 1818'de de Belgrad'a gönderilen Kethüda Kâtibi Esbak Necib Efendi'ye de Sırpların ve Semendire Sancağı'nın durumunu tahkik ederek İstanbul'a bildirme görevi verilmişti. [12]Ona verilen kodlar da 3 basamaklı sayılardan oluşuyordu. [13] Böylece her iki bürokrasi de her harfin- farklı numerik şifre ile gösterildiği şifrelere yöneldiler.

Bilindiği gibi 19. yüzyılda ortaya çıkan merkez-çevre ilişkileri bakımından merkezi devleti güçlendirecek telgraf büyük bir imkan sağlamaktaydı. Nitekim Telgrafın Osmanlıda kullanımıyla beraber, diplomasi bürokrasisinin "tek alfabeli (monoalfabetik) yerine koyma (ikâme) sifre" leri ve numerik kod kullanımı 1855'lerden itibaren başlamıştı.

Bu bağlamda Osmanlı dahili bürokrasisi de yukarda saydığımız gereklilikler çerçevesinde "tek alfabeli (monoalfabetik) yerine koyma

[10] BOA. HAT 1432-58608

[11] Bingöl, "Serezli (Sirozî) Yusuf Paşa'nın…"

[12] Nurbanu Duran, *Sırbistan Emareti Öncesi Belgrad: 1792-1830*, İstanbul Üniversitesi Doktora Tezi, İstanbul 2019, s.156

[13] Bingöl, "Serezli (Sirozî) Yusuf Paşa'nın…"

(ikâme) şifre"ler ve daha sınırlı sayıda da olsa kod kullanımına yönelmiştir. Söz konusu kod kullanımının sınırlı olduğu şifre anahtarlarının (miftâh) zaman içinde geliştiğini görüyoruz. Bu gelişme sürecini belgelerimiz bize açıkça göstermektedir. (15 Ramazan 1294) 23 Eylül 1877 tarihli ve "Bâb- ı âlinin Miftâh-ı Cedidi" başlığını taşıyan küçük çaplı diyebileceğimiz, bir şifre ve kodlardan oluşan defterin (nomenklatör) anahtarı (miftâh) şöyleydi;[14]

ش	س	ز	ر	ذ	د	خ	ح	چ	ث	ت	ب	ا
75	91	87	21	17	43	93	79	61	59	99	95	57
88	98	76	94	38	96	84	18	86	44	72	54	36

ی	لا	ه	و	ن	م	ل	ك	ق	ف	غ	ع	ظ	ط	ض	ص
65	81	51	55	29	35	41	11	49	62	37	45	31	15	13	83
68	92	66	64	42	62	52	24	12	34	22	56	14	16	28	74

Bu "Tek Alfabeli (Monoalfabetik) Yerine Koyma (İkâme) Şifresi" aynı zamanda homofonik (eşsesli) özelliğe de sahipti ve bunun dışında da sınırlı sayıda Kodlara sahipti. -118- Kod'uyla başlayan ve en son 999 Kod'uyla biten numaralandırma ile isimler, sıfatlar vb. için toplam 161 Kod (rakam) kullanılmıştı. Öte yandan bir isim veya ismin sıfat hali ya da ismin çoğulu, aynı Kod (rakam) ile gösterilmişti. Mesela -223-koduyla, "Prusya ve Prusyalı" terimleri karşılanmıştır. Yaklaşık 161 adet Kod rakamıyla, 260 sözcük iletilebilmekteydi.[15]

Bu sürecin hızla gelişerek 19. Yüzyılın son çeyreğinde Hariciye bürokrasinin ulaştığı seviyeyi yakaladığını ve sayısı yüzleri aşan kod defterleri ortaya çıktı.[16] Nitekim bu gelişkin kod defterlerinin en erken örneği olan toplam 66 varak ve 10.000'i aşkın kelimeyi ihtiva eden 1060

[14] BOA. Y.MTV. 1-9

[15] Bingöl, "Osmanlı Devleti'nde Kriptografik…"

[16] BOA'da çeşitli farklı şifreleri içeren "Bâb-ı âli'ye mahsus şifre defteri" veya "Şifre miftâhının tarifname defteri"vb. isimler altında 500'den fazla şifre ve kod defteri bulunmaktadır. Bunlara vilayet merkezleri, Kazalar yazışmaları için kullanılan şifreler veya örneğin "Dahiliye Nezareti" gibi nezaretlerin kullandığı şifrelerini kodlarını gösterir defterler, miftâhlarla binlerce defterlik bir külliyat bulunmaktadır.

nolu miftâh defteri tarafımızca incelenmişti.[17] Osmanlı Arşivi'nde 1060 numara ile kaydedilen ancak orijinalinde ise 21 numaralı görünen bu defterin kullanım yöntemleri, uzun süre kod defterlerinde esas alınmıştır.

Bu defter (Nomanklatör) Başkent ile vilayetler arasında telgraf haberleşmesinde kullanılmıştır. Bu Nomanklatör'ün ya da "Kod ve Miftâh" defterinin giriş kısmında, şifrelerin nasıl üretileceği veya deşifre edileceği tarif edilmektedir. Yine giriş kısmında, bu defterin hazırlanma gerekçesi şu şekilde açıklanmıştır.

> *"(…) Şimdiye kadar isti'mâl edilegelen şifre miftâhları yalnız hurûf-ı hecâdan ve bazen kelimât-ı mahsûsa var ise de onlarda birkaç kelimeden ibâret olduğundan yirmi otuz kelimelik bir telgrafnâme yazmak için birkaç yüz rakam yazmağa mecbûriyet hâsıl oluyor ve uzunca bir telgrafnâmeyi yazmak için birkaç sâat ve halli için dahi bir o kadar vakit zâyi' ediliyor… bazı meraklı telgraf memûrları her gün ellerinden geçmekde olan vukuâta tatbîk ile hall eyledikleri dahi anlaşıldığından şifreli telgrafdan maksûd olan mahremiyetin hükmü kalmayup bu keyfiyyet esrâr-ı devletin şüyû'una sebebiyet vermektedir…"*[18]

Bu tür sakıncaları ortadan kaldırmak için yeni miftâh (Anahtar) düzenlendiği ve mabeyn ile bu miftâhla haberleşilmesine dair irade çıktığı vurgulanmaktaydı.[19]

Temelde "Kodlar" Şems, Kamer, Müşteri, Zuhal, Utarid, Merih, Zühre gökcisimlerinin adını taşıyan 7 gruba ayrılmıştı. Her sayfa başında 2 basamaklı sayılarla numaralandırılan bu gök cisimlerinin bulunduğu sayfadaki kodların her biri 3 basamaklı sayıdan oluşup, "sabah ve akşam " olmak üzere denilerek verilen "Anahtar Kelime" ile oluşan 14 ayrı şifrenin, nasıl kullanılacağı mesajı alana iletilmekteydi.[20]

Defter başlıklarında "Bi'l-umûm vilâyetlerle muhâbereye mahsûs şifre miftâhı (Mektûbî Kalemi)", "Bâb-âlî'ye mahsûs şifre miftâhı", Cebel-i Lübnan Mutasarrıflığı ile gizli muhâberâta mahsûs şifre miftâhı",

---

[17] Bu Nomanklatörün hakkında geniş bilgi ve kullanımına dair örnekler için ayrıntılı bkz. Bingöl, " Osmanlı Devleti'nde Kriptografik…"

[18] BOA. A. d. 1060

[19] BOA. A. d. 1060

[20] Daha detaylı anlatım ve örnek kullanım için bkz. Bingöl, "Osmanlı Devleti'nde Kriptografik…"

"Mekke emiri ile muhabereye mahsûs şifre miftâhı (Mektûbî Kalemi)" gibi isimler taşıyan, genel olarak bütün vilayetlerle ortak haberleşme veya bazen sadece bir vilayete münhasır Kod defterlerinin yüzlercesi ortaya çıkmıştır.[21] Bu Nomanklatörler belli periyodlarda değiştirilerek kullanılmaktaydı.

Özel Amaçlı (Göreve Tahsisli) Şifre Anahtarları

Bu genel esasa dayalı vilayetlerle, şifreli muhabere süreci imparatorluğun sonuna kadar sürmekle beraber zaman zaman "özel amaçlı" ya da belirli görevler için tahsis edilen "göreve tahsisli" diyebileceğimiz şifreler oluşturulmuştu. Bu görevler sona erdiğinde şifre anahtarının işlevi kalmamaktaydı. Buna dair bazı örnekler vermekte fayda var.

İlk örneğimiz, 1894'te Bitlis vilayeti Muş Sancağına bağlı Sason'da (Talori) ortaya çıkan, isyanla ilgilidir. 1894' te programlı ve büyük bir Ermeni isyanı düzenlenmiştir.[22] Tıpkı isyancıların istediği gibi İngiltere, Rusya ve Fransa konuya karışmış ve isyan bölgesine bir inceleme heyeti gönderilmesi için Osmanlı yönetimine baskı yapacaklardı. Osmanlı yönetimi de bölgeye giderek Sason İsyanı'nı ve olayları araştıracak bir komisyonun yani bir "Tahkik Heyeti"nin [23] kurulmasını kabul etmek zorunda kalmıştı.

Tahkik Heyetinin çalışmaları sırasında heyetin Osmanlı üyeleri, Mabeyn Başkitâbeti ile sürekli yazışmaktaydı. Her yeni durum ve her

[21]Bazı örnekler için bkz. BOA. A. d 1520, 1186, 1187, 1190, 1190, 1200, 1194, 1201, 1202, 1061, 1071, 1072, 1074, 1084, 1112, 1128, 1129, 1131, 1181,1158, 1178, 1153, 1173, 1154 vb.

[22] Nurettin Gülmez, "Tahkik Heyeti Raporlarına Göre 1894 Sason İsyanı", *Belleten*, (2006), c. 70, sayı 258, s.695, 698.

[23] Tahkik Heyeti şu üyelerden meydana gelmişti.
"Başkan : Şefik Bey (Temyiz Mahkemesi Dilekçe Dairesi Başkanı)
Üye : Ömer Bey (Emniyet Sandığı Müdürü)
Üye : Celâlettin Bey (İstinaf-ı Crınha Dairesi Başkanı)
Üye : Mirliva Tevfik Paşa
Üye : Mecid Efendi (Dahiliye Nezâreti memuru)
Üye : Shipley (İngiliz Konsolosu)
Üye : Prjevalsky (Rus Konsolosu)
Üye : Vilbert (Fransız Konsolosu)" Gülmez, *a.g.m*., s. 699- 701.

gelişme hakkında Yıldız Sarayı'na bilgi vermişler ve oradan talimatlar almışlardır.[24] 24 Ocak 1895'te göreve başlayan Tahkik Heyeti yaklaşık altı ay süren görevleri sırasında yüz sekiz toplantı yapmış ve yüz doksanın üzerinde tanık dinlemiştir.[25] Heyet başkentle haberleşirken, bölge vilayet ve sancaklarına verilen genel haberleşmeye dair şifre miftâhlarından farklı özel bir miftâh kullanacaktır. Altı ay boyunca Mabeynden verilen özel bir miftâh veya göreve tahsisli diyebileceğimiz, bu miftâhta 200 kelimelik kod dizisi kullanılmıştır. [26] Bu göreve tahsisli şifre anahtarı, her harf için 2 basamaklı sayılardan oluşan 3'lü bir homofon (eşsesli) yapıya sahipti.

Tahkik Heyeti Miftahı

ح	چ	ج	ث	ت	پ	ب	ا
138	139	141	142	143	144	145	146
175	176	177	178	179	181	182	183
214	213	195	194	193	192	191	189

ش	س	ژ	ز	ر	ذ	د	خ
135	134	133	132	131	129	128	137
153	154	155	156	157	172	173	174
223	222	221	219	218	217	216	215

ق	ف	غ	ع	ظ	ط	ض	ص
113	112	111	117	118	119	121	136
169	171	158	147	148	149	151	--
211	212	229	228	227	226	225	224

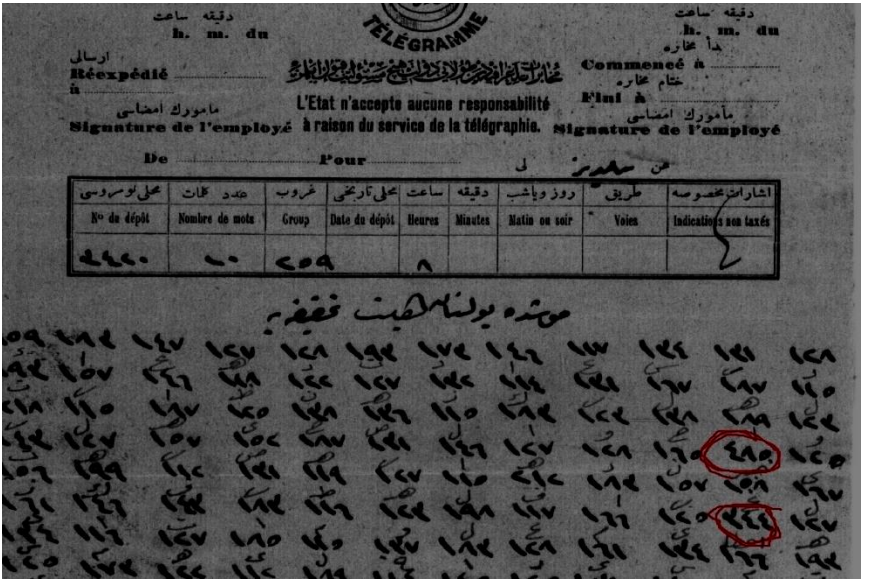
ء	ى	لا	ه	و	ن	م	ل	ك
124	125	126	127	123	122	116	115	114
159	161	162	163	164	165	166	167	168
184	185	186	187	188	196	197	198	199

[24] Gülmez, *a.g.m.*, s.705-706.

[25] Gülmez, *a.g.m.*, s.733.

[26] BOA. Y..EE. 171-43; Bkz. *EK-1*

Öte yandan 200 kelime ve cümle grubu 3 basamaklı sayılarla Kodlanmıştı. Örneğin "haber" kelimesi için 485 kodu kullanılırken, "ita" kelimesi için 344 kodu kullanılmıştı.



BOA. Y. EE. 176-109 [27]

Şifreler ve Kodların 3'er basamaklı oluşu güvenliği artırıcı bir unsurdu. Bir kriptoanalist için veya telgraf görevlilerinin deşifre yönündeki çabalarını önleyici nitelikte, 3 basamaklı bir sayının Harf değeri mi? Kod değeri mi? olduğunu anlamalarını önlüyordu. Öte yandan bir telgrafta herhangi bir harfin 3 kombinasyonu da kullanılabilmekteydi. Böylece kırılması güç bir şifreleme oluşturulmuştu.

Göreve tahsisli veya özel amaçlı ikinci şifre örneğimiz ise Teftiş-i Askeri Komisyon-ı Âlisi Reis-i Sanî Müşir İsmail Hakkı Paşa'ya aittir. (11 Safer 304) 9 Kasım 1886'da Bağdad ve Musul vilayetlerinde aşiretlerin yarattıkları eşkıyalık hareketlerine karşı alınacak önlemler için Mabeyn dairesinde bir komisyon kurulup, müzakere edilmişti. Bölgeye Müşir

[27]Anılan dönemde gerek Tahkik Heyeti'nden Yıldız Sarayı'na gerekse Yıldız'dan heyete bu miftâh ile pek çok yazı gönderilmiştir. Bazı şifreli örnekler için bkz. BOA. Y. EE. 171-43;163-20;176-139;176-81;176-79;176-80; 176-75;176-76; 176- 77 176-145; 176-146.

İsmail Hakkı Paşa'nın gönderilmesi ve kendisine bir talimat verilmesine dair padişah iradesi çıkmıştı. İsmail Paşa kendi riyasetinde bir Divan-ı Harp kurarak ilgilileri yargılayacaktı. Aşiretler arasında anlaşma ve asayişi sağlamak konusunda da yetkilendirilmişti.[28] 31 Ocak 1887' de bölgeye gitmek üzere olan İsmail Paşa'ya haberleşme için bir şifre miftâhı da verilmişti.[29] Verilen şifre anahtarı temelde "tek alfabeli (monoalfabetik) yerine koyma (ikâme) şifresi" ydi.

ح	ج	ث	ت	ب	ا	
85	18	15	34	41	66	
94	61	28	38	46	83	
ش	س	ز	ر	ذ	د	خ
77	54	19	63	45	13	25
69	65	24	72	11	14	26
ق	ف	غ	ع	ظ	ط	ض	ص
21	31	39	75	44	22	91	99
68	32	56	33	51	23	93	88
ى	لا	ه	و	ن	م	ل	ك
81	55	17	16	12	68	78	58
73	86	96	47	29	98	87	63

BOA. DH.ŞFR. 132-148[30]

Homofonik (eşsesli) bir şifre anahtarının yanında, bu kısa Nomanklatör listesi "478 kodu Rusya- Rusyalı, 118- asayiş, 129-esliha" vb. karşılığı olan 150 kod içeren basit bir kodlama idi. Kodların 3

[28] BOA. Y.A.RES 35-14; Y.A.RES 35-10

[29] BOA. DH.ŞFR. 132-148

[30] Bkz. EK-2

basamaklı, harflerin ise 2 basamaklı sayılardan oluşması ilk bakışta ayırt edilmeleri dolayısıyla bir güvenlik zafiyetini ortaya koymaktadır.

Osmanlı arşivinde yaptığımız araştırmada İsmail Paşa'nın bu görevi sırasındaki gelen-giden şifreli telgraflarına[31] ne yazık ki ulaşamadık. Ancak İsmail Paşa'nın bu görevi yani Musul Meselesi devam ederken aynı anda bir başka şifre kullandığını tespit ettik. Asker olması hasebiyle İsmail Paşa'nın, Serasker Ali Saib Paşa ile Kod'ları ve harfleri 3 basamaklı sayılardan oluşan yeni bir miftâh kullanmaktaydı. Bu da özel amaçlı şifre-kod miftâhıydı. Çünkü harici ve dahili haberleşme sistemi bir Nomanklatöre bağlı olarak 5 basamaklı olan Osmanlı haberleşme-genel şifreleme- sistemi dışında bir miftâhtı.[32]

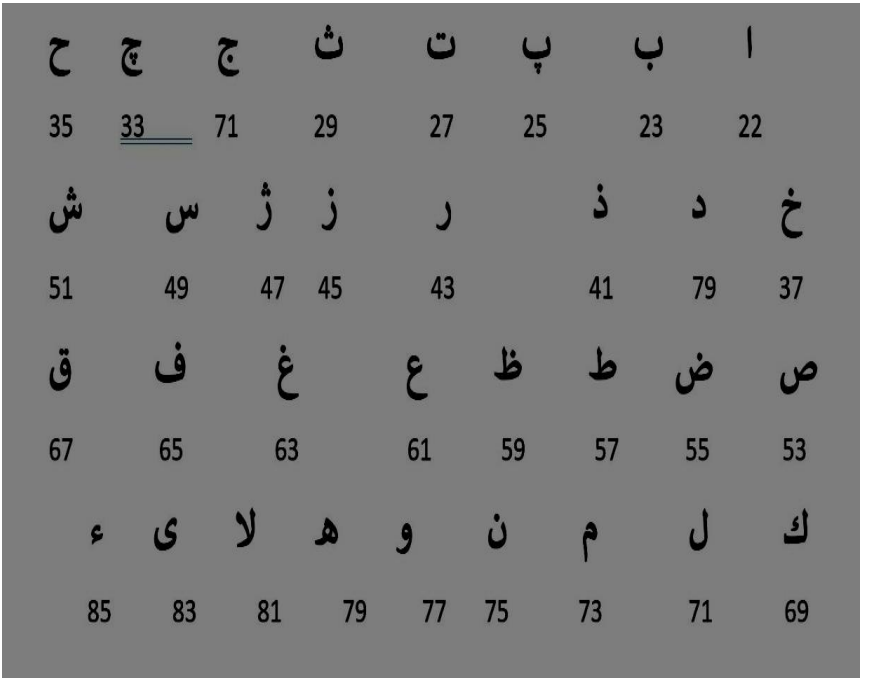
Son örneğimiz ise II. Abdülhamit döneminde ABD'den Mecidiye Kruvazörü satın alınması ile ilgilidir. Amerika'da yapımı 1904'te tamamlanan Mecidiye Kruvazörü, Kaptan Ransford D. Bucknam tarafından, 1904 Nisan'ında Rauf (Orbay) Bey'e Midilli'de teslim edildi. Akabinde İstanbul'a da gelen ve yapılan iş teklifi üzerine Kaptan Bucknam İstanbul'da kaldı.[33] Kaptan Bucknam Mabeyn Başkitabet dairesinde Yarbay(kaimmakam) rütbesi ile işe başladı. Yarbay Bucknam ailesini getirmek için Amerika'ya dönme izni istediği sırada, Sultan II. Abdülhamit ondan İngiltere'ye de uğramasını orada yeni askeri gemiler hakkında bilgi edinmesini ve özellikle "tahte'l bahr" denizaltılar hakkında araştırma yapmasını istedi. Bucknam'a kapaklı bir dosya içinde özel bir şifre anahtarı vererek, Bucknam'ın toplayacağı bilgileri Osmanlı elçilik ve konsolosluklarından şifreli olarak Mâbeyn-i Hümayun Başkitabetine göndermesini talep etti.[34] Aşağıda miftâhını veriyoruz.

[31] Sadaretle yürütülen haberleşmelere dair açık yani şifre içermeyenler için bazıları için bkz. BOA. Y.A.HUS. 201-27; 202-21; 202-49; 199- 78

[32] Bkz. EK-3

[33] Özcan Mert, "Osmanlı Bahriye Mirlivası *Bucknam* Paşa"**,** *Tarih Boyunca Dünyada ve Türklerde* Denizcilik Semineri Bildirileri 17-18 Mayıs 2004, İstanbul, 2005, s. 87.

[34] Ender Kuntsal, *Osmanlı Bahriyesinde Bir Amerikalı Bucknam Paşa* , T. İş bankası Yay., 2017, s. 125-126.



Bu miftâhla beraber Yarbay Bucknam'a görevine uygun silah alımı, araştırma gibi görevine uygun "17- zırhlı, 19 torpido, 21 torpil, 24 gambot " gibi deniz savaş araç terimlerinden oluşan 29 Kod verilmişti.[35]

[35] BOA. Y, EE. d. 318 Bkz. Ek-4

Sonuç

III. Selim döneminde ilkin Osmanlı diplomasisinin 1797'den itibaren Kriptografi'yi kullandığını ve 816 yılından itibaren ise Osmanlı dahili bürokrasisi de kriptografik yazışma yöntemlerini kullanmaya başladığını görüyoruz. Hem dahili hem de harici bürokrasisi, esas olarak "monolfabetik ikame şifrelerine" dayanıyordu. İlk günlerden itibaren, şifre anahtarlarındaki harfler sayısallaştırıldı. Bu şifreleme anahtarlarının yanında "kelime" tabanlı "Kodlar" kullanılsa da sayıları çok sınırlıydı. Telgrafın Osmanlı Devleti'ne 1855' te girişiyle beraber durum değişti ve "monolfabetik ikame şifreler" varlığını devam ettirseler de Kod'lar ağırlık kazandı. Zamanla Kod Listelerinin geliştirilmesi sonucu neredeyse 10 binlik kelime -Kod haznesine ulaşan Nomanklatörler hem dahili hem de harici bürokrasimiz tarafından imparatorluğun sonuna kadar kullanıldı. Ancak arşivlerimizde tespit ettiğimiz üzere, sınırlı sayıda da olsa salt "monolfabetik ikame şifrelerine" dayanan, görece daha az kompleks şifre ve kod kullanımının özellikle belirli bir işe, göreve tahsisli olarak devam ettiğini, görevler bittiğinde bu miftâhların iptal edildiğini görüyoruz.

Osmanlı Devleti sürekliliği olan telgraf haberleşmeleri için belli bir sistemi olan ve güvenlik derecesi de yüksek geniş hacimli Kodlardan oluşan Nomanklatörler oluşturmuştu. Ancak birkaç aylığına ve sadece belirli bir göreve tahsisli kullanımlar için 10.000 kelimeyi aşan Nomanklatör ya da Kod listeleri hazırlamak pratik değildi. Bunun yerine temelde daha basit ve güvenliği derecesi düşükte olsa, geniş Kod defterleri yerine, monoalfabetik ikame şifreleri kullanmayı daha pratik bulmuştur. Şifreli yazı bolluğu içindeki arşivlerimizde yer alan şifreli yazışmalar incelenirken, araştırmacılar bu hususu göz önünde bulundurmalıdırlar.

Kaynakça

Arşiv Kaynakları

T.C. Cumhurbaşkanlığı Devlet Arşivleri Başkanlığı Osmanlı Arşivi (BOA)

BOA. DH.ŞFR. 132-148

BOA. HAT 1432-58608

BOA. HR. ŞFR 3. 55-28

BOA. HR.SFR.4..._984-1; 984-2

BOA. Y.MTV. 1-9

BOA. A. d. 1060 ; A. d. 1520, 1186, 1187, 1190, 1190, 1200, 1194, 1201, 1202, 106, 1071,1072, 1074, 1084,1112, 1128,1129,1131, 1181,1158,1178, 1153,1173 1154 vb.

BOA. Y. EE. 171-43;163-20;176-139;176-81;176-79;176-80; 176-75;176-76; 176- 77 176-145; 176-146.

BOA. Y, EE. d. 318

BOA. Y.A.HUS. 201-27; 202-21; 202-49; 199-78

BOA. Y.A.RES 35-14; Y.A.RES 35-10

Kitap ve Makaleler

Bingöl, Sedat, "Osmanlı Devleti'nde Kriptografik Uygulamalar ve Kod Defterleri", *Süleyman Demirel Üniv. Fen-Edebiyat Fakültesi Sosyal Bilimler Dergisi*, (2022)

Bingöl, Sedat, "Serezli (Sirozî) Yusuf Paşa'nın Kriptografisi Hakkında Notlar " *Humanitas*, (2022), (yayın aşamasında).

Bingöl, Sedat, "Methods for encryption in early 19th-century Ottoman diplomatic correspondence"*Cryptologia*, (2021), doi:10.1080/01611194.2021.

1919943

Bingöl, Sedat, "The changes in Ottoman diplomatic cryptography and its methods during the 19th century (1811–1877)", *Cryptologia*, (2022), doi: 10.1080/01611194.2022.2092916

Gülmez, Nurettin "Tahkik Heyeti Raporlarına Göre 1894 Sason İsyanı", *Belleten*, c. 70, sayı 258, (2006), s.695-742.

Kuntsal, Ender, *Osmanlı Bahriyesinde Bir Amerikalı Bucknam Paşa*, T. İş Bankası Yay., 2017

Mert, Özcan "Osmanlı Bahriye Mirlivası *Bucknam* Paşa", *Tarih Boyunca Dünyada ve Türklerde Denizcilik Semineri Bildirileri (17-18 Mayıs 2004)*, İstanbul, (2005), s.85-100.

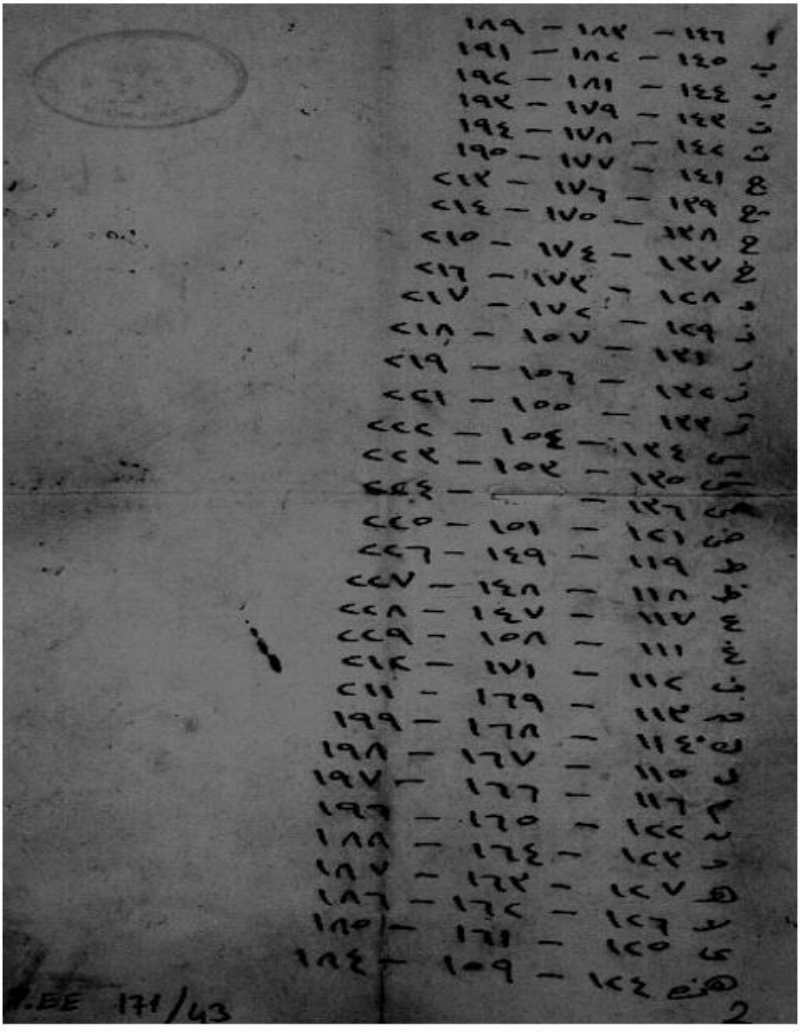
Iordanou, Ioanna, *Venedik Gizli Servisi*, çev. Fatih Yücel, Kronik Kitap Yay., İstanbul 2020.

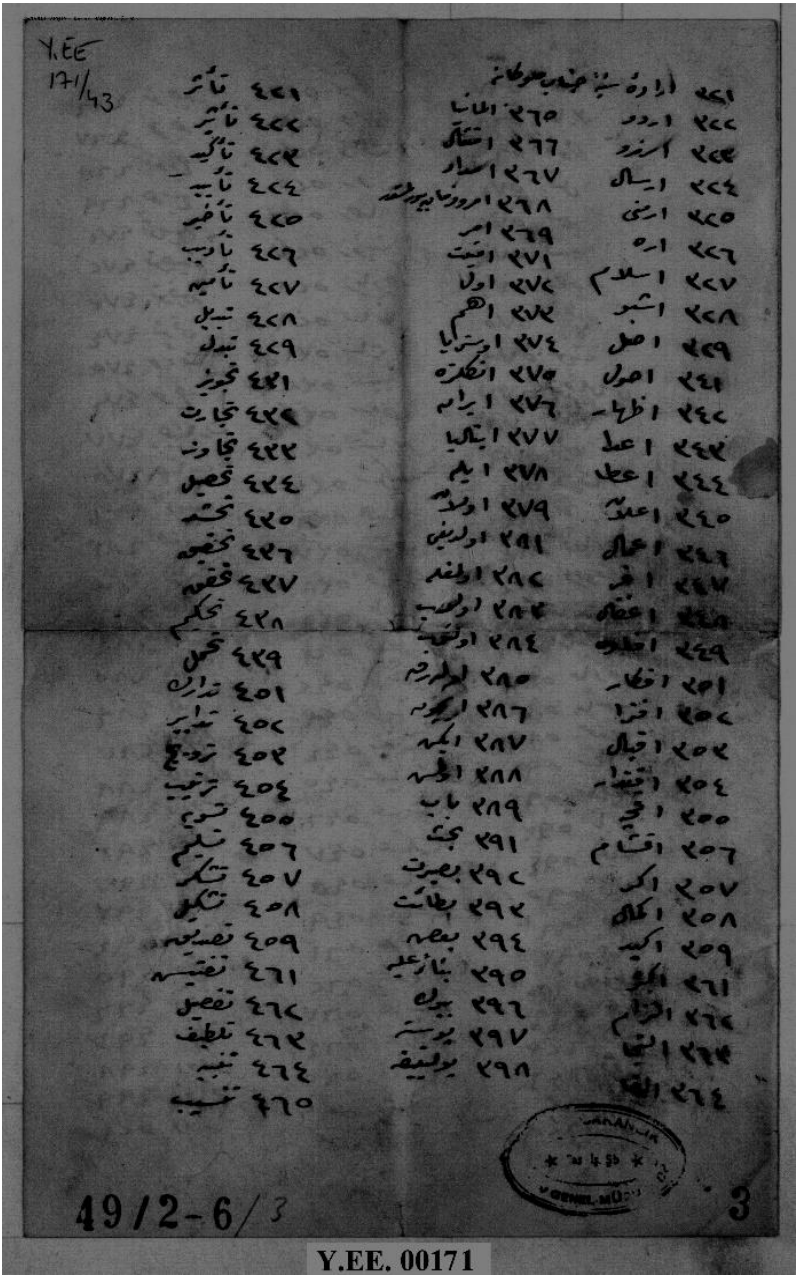
Kuran, E., *Avrupa'da Osmanlı İkamet elçiliklerinin Kuruluşu ve İlk Elçilerin Siyasi Faaliyetleri 1793- 1821*, Türk Kültürünü Araştırma Enstitüsü Yayınları, Ankara 1988.

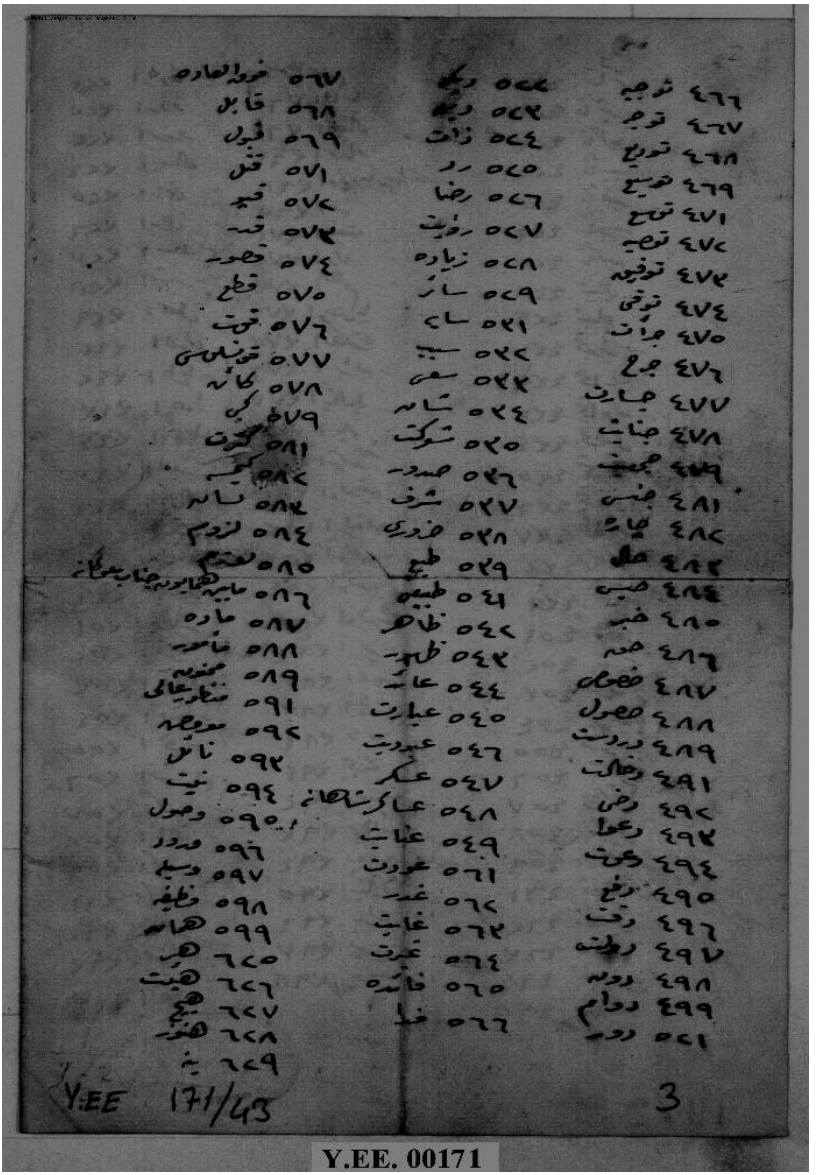
Nurbanu Duran, *Sırbistan Emareti Öncesi Belgrad: 1792-1830*, İstanbul Üniversitesi Doktora Tezi, İstanbul 2019.

EKLER

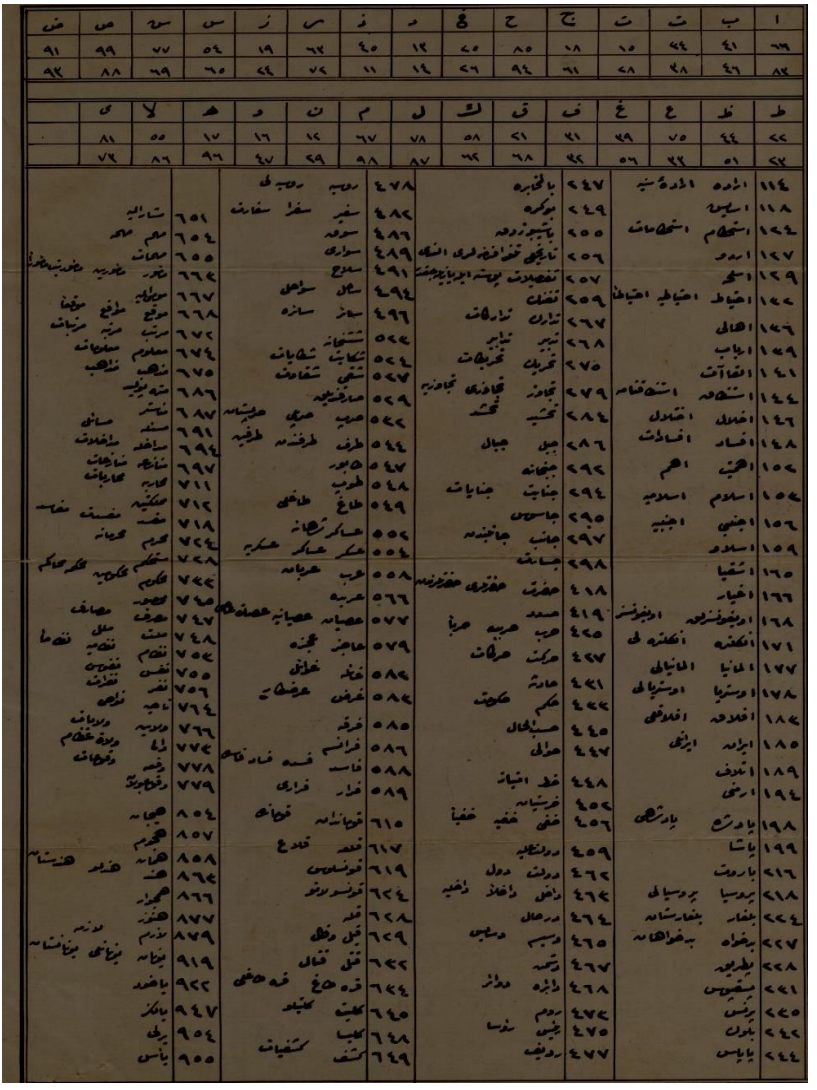
Ek-1. BOA. Y. EE. 171-43

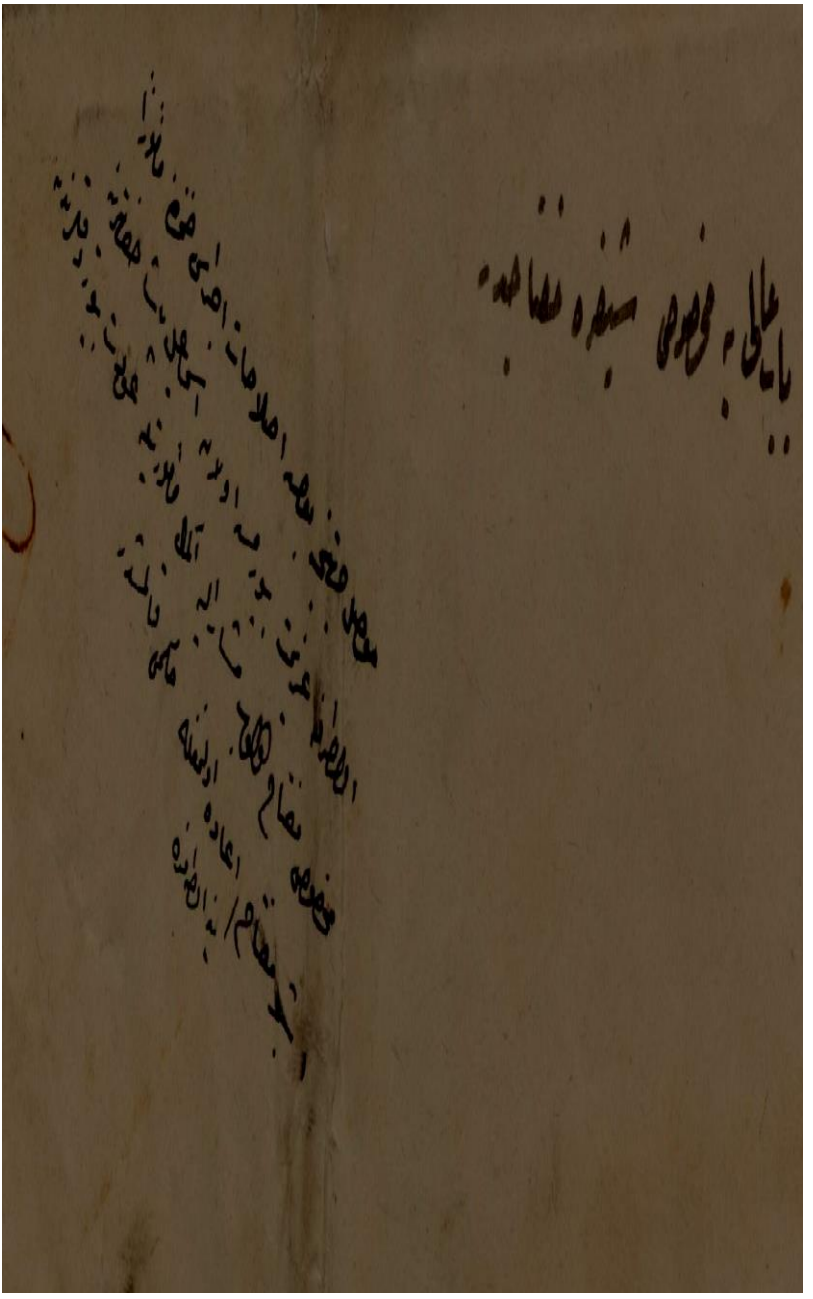




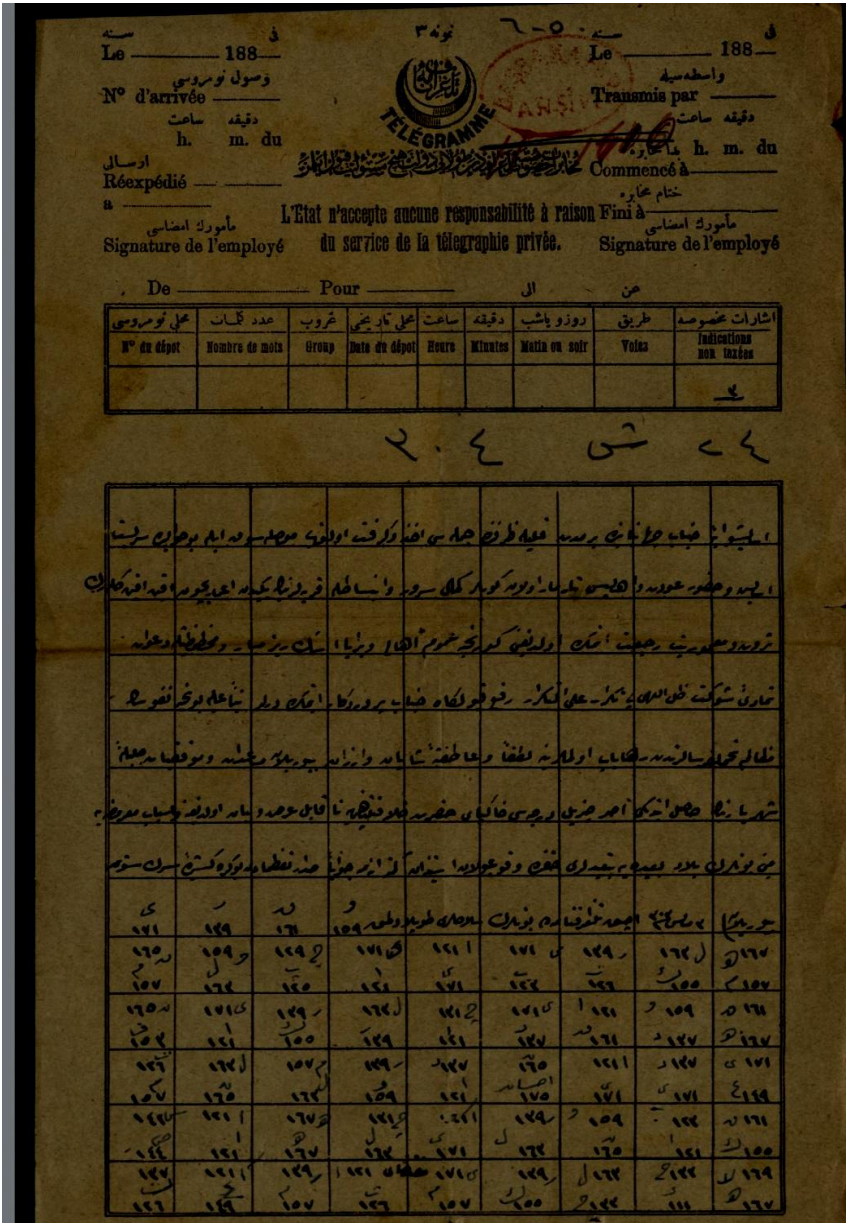


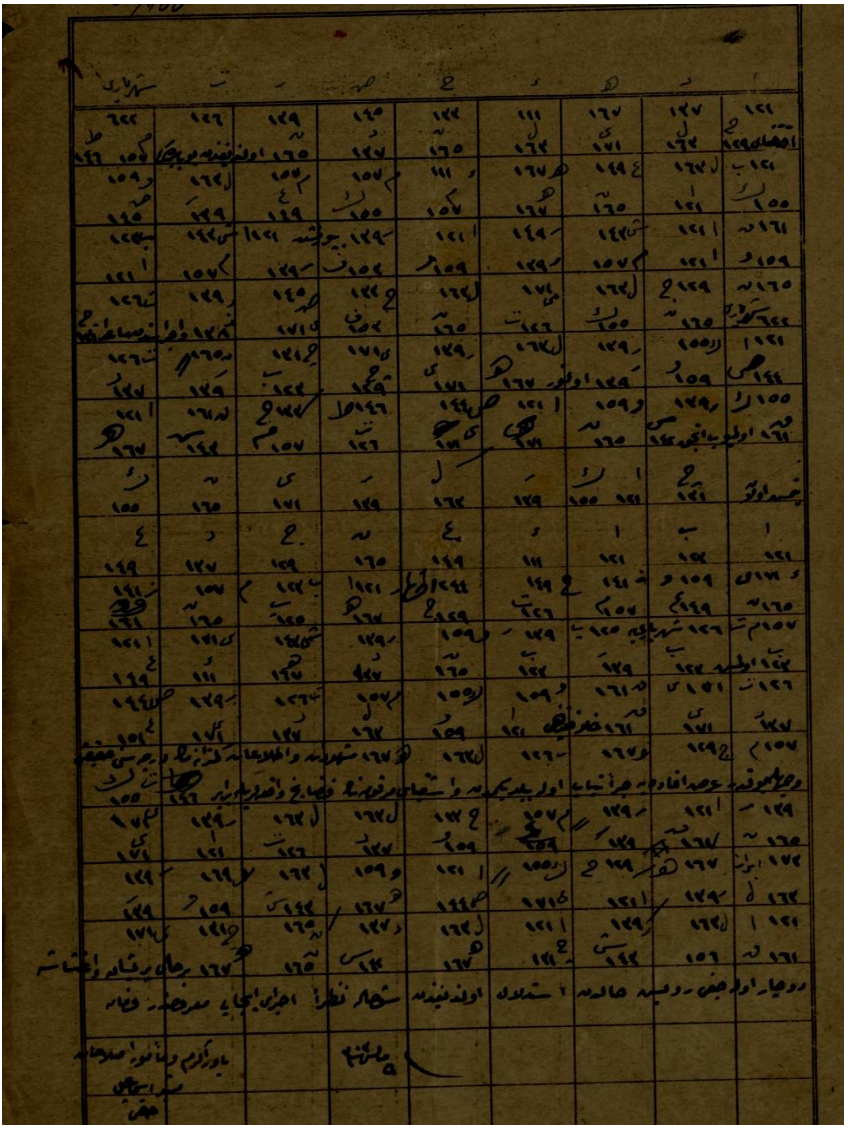
Ek- 2. BOA. DH.ŞFR. 132- 148



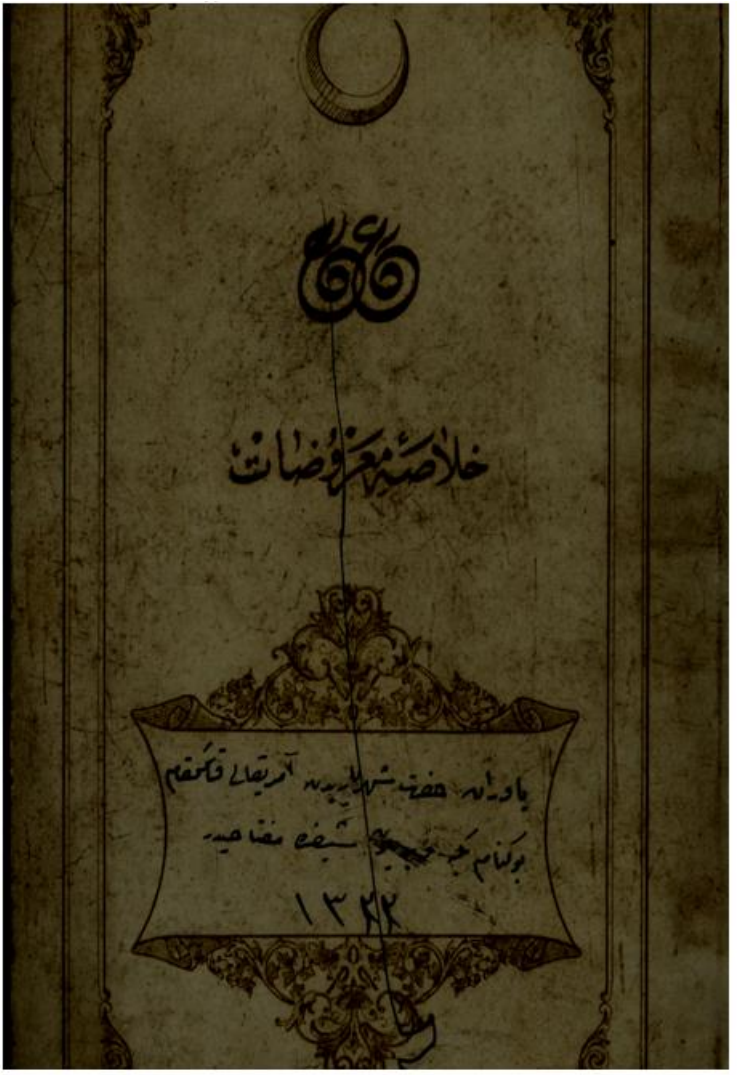


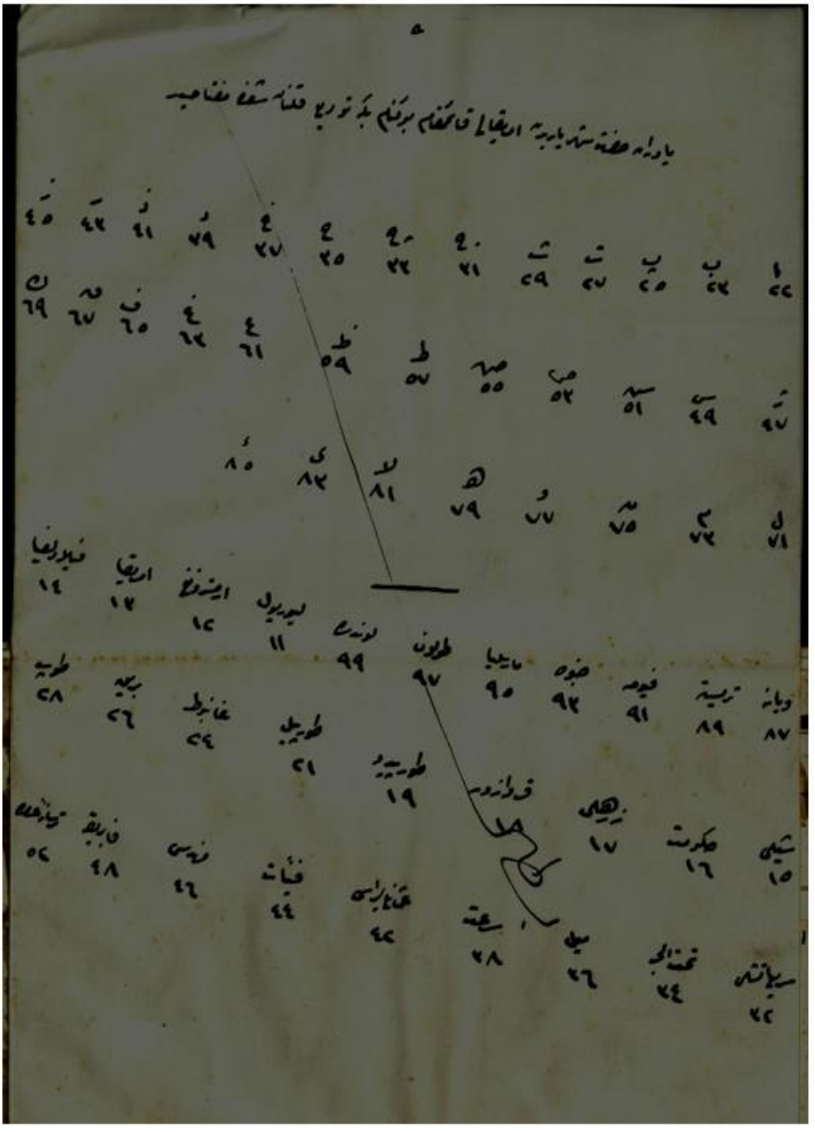
Ek-3. BOA.Y.PRK.ASK. 39-100





Ek- 4. BOA. Y, EE. d. 318





Extended Abstract

Cryptography, which has a history dating back to 2000 BC, is an effort to hide the meaning of the message in a clear message. The first examples were seen in the Indian, Mesopotamian, Greek, Roman and Arab-Muslim worlds. Although the cryptography, which had a limited use throughout history, found a wider and more continuous use from the beginnins of the 15th century. Since so many different developments have been realized in politics and in the fields of art and science in parallel with the birth of Renaissance. As a result of the development of diplomacy in Italy, the Italian city-states firstly began to send represantatives to each other and the inevitable necessity of hiding the instructions due to diplomatic communication, gave birth to the encryption (Cryptography), which was almost forgotten since the collapse of the Roman Empire.

A Systematic Ottoman Cryptography was executed in diplomacy during the reign of Selim III. With the appointment of Yusuf Agah Efendi to London on January 29th, 1795, Ali Aziz Efendi to Berlin on October 1796, and Seyyid Ali Efendi to Paris on July 28th, 1797, and İbrahim Afif Efendi to Vienna as Ambassadors, Cryptography was started to use. For nearly half a century, simple-level "One Alphabet (one alphabetic) Substitution (substitution)" ciphers were used. With the arrival of the telegraph to the Ottoman Empire, the codes increased and the codes came to the fore. Over time, extensive Nomanculators (namers) have been created. It became the basis of communication Code-encryption in both the Ottoman external and internal bureaucracy. But outside of this dominant correspondence method, simple encryptions still continued to be used for special tasks.

In the Crimean War and after the establishment of the Ottoman Telegraph lines, it was not possible to send encrypted telegrams with the "Single Alphabet (mono-alphabetic) Substitution (substitution) Code" method.

That's why the diplomatic bureaucracy abandoned "One Alphabet (mono-alphabetic) Substitution (substitution) Cipher". Instead, the concept of "Homophonic (sound) Substitution Code" was adopted. This system was had a higher security than the other one (i.e. Single-

alphabet system monoalphabetic). In this system, although the alphabet was single, the numerical equivalents (sounds) were more than one. It was intended to increase the security even more by placing random blank numbers between the passwords. In addition, a limited number of encodings, which were also available in past passwords, were added.

On the other hand, besides the numerical encryption of the messages, the codes were also digitized. Firstly, "Single Alphabet (mono-alphabetic) Substitution (Substitution) Passwords" based on the French alphabet were used, since Foreign Affairs correspondence was made in French. This method was used for the daily correspondence of the foreign ministry. However, between the Ambassadors and the Ministers of Foreign Affairs, a much more reliable system was adopted. In terms of center-periphery relations that emerged in the 19th century, the telegraph provided a great opportunity to strengthen the central state. With the use of the telegraph in the Ottoman Empire, the use of "single-alphabet (monoalphabetic) substitution (substitution) ciphers" and numeric codes by the diplomatic bureaucracy began in 1855.

This "One Alphabet (Monoalphabetic) Substitution Code" also had a homophonic feature. Apart from that, it had a limited number of Codes. Nouns, adjectives, etc., with numbering starting with Code -118- and ending with Code 999 last. A total of 161 codes (digits) were used for a noun or the adjective form of the noun or the plural of the noun were shown with the same Code (number). For example, with the code -223, the terms "Prussian and Prussian" are met. With approximately 161 Code numbers, 260 words could be transmitted. This process developed rapidly and in 1877 we see that the foreign bureaucracy reached the level it had reached. Especially in the last quarter of the 19th century, more than a hundred code books emerged. We examined the Miftâh book no. 1060, which is the earliest example of these advanced code books, containing a total of 66 leaves and more than 10,000 words.

Although the encrypted communication process lasted until the end of the empire with these general-based provinces, from time to time passwords that we can call "special purpose" or "task-dedicated" allocated for certain tasks were created. When these tasks are over, the encryption key is no longer functional. Encryption, which is also used

extensively in internal affairs, has also been used very effectively by the Investigation Committees, which were established to investigate the problems experienced in many parts of the country. During the work of the Investigation Committees, the Ottoman members of the delegation were in constant correspondence with the Mabeyn Başkitabeti. They informed Yıldız about every new situation and every development and received instructions from there. For example, an the Investigation Committee, which started its duty on January 24th, 1895, held one hundred and eight meetings and listened to over one hundred and ninety witnesses during its duties that lasted for about six months. While communicating with the capital, the Ottoman members of the delegation will use a special key (miftâh) different from the codekey used for the general communication given to the provinces and sanjaks of the region.

The Investigation Committee was used this key, which 200-words code sequence we can call a special key (miftâh) or assigned codes for six months. The cipher key dedicated to this task had a 3-digit homophone structure consisting of 2-digit numbers for each letter. The 3-digit passwords and codes were a security-enhancing element. The letter value of a 3-digit number for a cryptoanalyst or to prevent telegraph officials from deciphering it? Code value? prevented them from realizing it. Besides, 200 words and sentence groups were coded with 3-digit numbers. For example, while the code 485 was used for the word "news", the code 344 was used for the word "itâ". On the other hand, 3 combinations of any letter could be used in a telegram. Thus, an unbreakable encryption was created.

It is possible to encounter many examples in the Ottoman Archives in order to explain the assigned or special purpose encryption methods. It would be appropriate to mention a few examples among these. Our first example belongs to the vice-president of Military Investigation Commission Müşir İsmail Hakkı Pasha. (11 Safer 1304) On 9th November 1886, a commission was established and negotiated in the Mabeyn department for the measures to be taken against the banditry movements created by the tribes in the provinces of Baghdad and Mosul. The sultan's had send Müşir İsmail Hakkı Pasha to the regions and given him one instruction. İsmail Pasha would set up a Divan-ı Harp

under his own leadership and judge those concerned. He was also authorized to ensure agreement and order among the tribes. On January 31, 1887, İsmail Pasha, who was about to go to the region, was given a code-cipher for communication. The given cipher key was basically a "monoalphabetic substitution cipher"

The last example that can be given in this regard is II. It is about the purchase of the Mecidiye Cruiser from the USA during the reign of Abdulhamid. The Mecidiye Cruiser, whose construction was completed in America in 1904, was delivered by Captain Ransford D. Bucknam to Rauf (Orbay) Bey in Midilli in April 1904. Afterwards, Captain Bucknam stayed in Istanbul upon the job offer that came to Istanbul. Captain Bucknam Mabeyn started to work in the Office of the Epistle, with the rank of Lieutenant Colonel. While Lieutenant Colonel Bucknam was asking permission to return to America to bring his family, Sultan II. Abdulhamid asked him to stop by England, learn about new military ships there, and do research on "taht-el bahir" submarines. He gave Bucknam a private encryption key in a clamshell file. He asked him to send the information he collected from the Ottoman embassies and consulates in the countries they visited, in encrypted form, to the Mabeyn.

As a result, the Ottoman Empire, which started to use Cryptography at first during the reign of Selim IIIrd, that is, from 1797, and since 1816, the Ottoman internal bureaucracy also started to use cryptographic correspondence methods. Its bureaucracy, both internal and foreign, relied mainly on "monolphabetic substitution ciphers". From the earliest days, the letters in the cipher keys were digitized.

Although "word"-based "Codes" were used alongside these encryption keys, their number was very limited. The situation changed with the entry of the telegraph into the Ottoman Empire in 1855. Although "monolphabetic substitution ciphers" continued to exist, Codes gained weight. As a result of the development of Code Lists over time, Nomanculators, which reached a code repository of almost 10 thousand words, were used by both our internal and foreign bureaucracy until the end of the empire. However, we have determined that continues the use of relatively less complex passwords and codes

based on "monolphabetic substitution ciphers". Specifically these keys had canceled when the tasks are completed.

This study briefly emphasizes the general features of Ottoman Cryptography, the transition from simple ciphers to the Code system with Telegram. Despite the extensive use of codes based on Nomanclators, this study mainly concenrates upon the occasional use of classical single-alphabet substitution ciphers in singular events until the ends of the Ottoman Empire.