ISSN: 2645-8837
HUMANITAS - Uluslararası Sosyal Bilimler Dergisi
HUMANITAS – International Journal of Social Sciences
2022, *10*(20), 67-92

Serezli (Sirozî) Yusuf Paşa'nın Kriptografisi Hakkında Notlar

Sedat BİNGÖL[1]

Öz

Bu makalemizde Matematik biliminin çalışma alanlarından olan Kriptoloji'ye ait iki yönelim olan Kriptoanaliz ve Kriptografi hakkında temel bazı kavramlar tanıtılıp, Avrupa ve Osmanlı Kriptografisinin kısa bir başlangıç tarihi verilecektir. Bu çerçevede Osmanlı Kriptografi'sinin başlangıcı olan III. Selim dönemi diplomatik kriptografisinin temel özellikleri ele alınıp değerlendirilmiştir. Daha sonra ise Serezli (Sirozi) Yusuf Paşa'nın bazı tarihsel olaylardaki rolünden söz edilecektir. Bu rollere bağlı olarak, Osmanlı idari yapısı içerisinde esinlendiği Kriptografik yöntemlerin kaynağı ve ortaya koyduğu şifre anahtarlarının (Miftah), algoritmaları incelenecektir. Serezli (Sirozi) Yusuf Paşa'nın Ruslara esir düşmesi sonrası ise özellikle Osmanlı Kriptografi'sine getirdiği Kesirli kodlar dışında ve yine oluşturduğu 2 farklı Anahtar (Miftah) incelenerek, Serezli (Sirozi) Yusuf Paşa'nın Kriptografi tarihimizdeki yenilikleri ve yeri değerlendirilecektir.

Anahtar Sözcükler

Kriptografi

Varna

tarihsel şifreler

tarihsel kodlar

Makale Hakkında

Geliş Tarihi: 14.06.2022

Kabul Tarihi: 12.08.2022

Doi:
10.20304/humanitas.1130938

Notes On The Cryptography Of Sirozî Yusuf Pasha

Abstract

In this article, some basic concepts about Cryptoanalysis and Cryptography, which are two orientations of Cryptology, one of the study areas of Mathematics, will be introduced and a brief start date of European and Ottoman Cryptography will be given. The beginning of the Ottoman Cryptography of Selim the IIIrd period are discussed and evaluated. Then, the role of Serezli (Sirozi) Yusuf Pasha in some historical events will be mentioned. Depending on these roles, the source of the cryptographic methods inspired by the Ottoman administrative structure and the algorithms of the cipher keys (Miftah) that he revealed will be examined. After Serezli (Sirozi) Yusuf Pasha was captured by the Russians, apart from the Fractional codes he brought to the Ottoman Cryptography, and the 2 different Keys (Miftah) he created, the innovations and place of Serezli (Sirozi) Yusuf Pasha in our cryptography history will be evaluated.

Keywords

Cryptography

Varna

historical ciphers

historical codes

About Article

Received: 14.06.2022

Accepted: 12.08.2022

Doi:
10.20304/humanitas.1130938

[1] Doç. Dr., Anadolu Üniversitesi, Edebiyat Fakültesi, Tarih Bölümü, Eskişehir/Türkiye, sbingol@anadolu.edu.tr, ORCID: 0000-0003-2016-2819

Giriş

Bir tarihçi olarak bir bilim alanının (Kriptoloji) kavramsal çerçevesini çizmek ve tarihle bağıntısı çerçevesinde sınırımızı belirlemek zorunlu bir durumdur. Bu bakımdan Kriptoloji içerisinde yer alan Kriptografi üzerinde duracağız. Öncelikle "şifre" ve "kod" terimleri arasındaki benzeşmeleri veya farklılıkları kısaca tespit etmeğe çalışacağız.

Kod (code), anlamlı bir öğenin (kelime, cümle veya ifade gibi) başka bir şeye (genellikle daha kısa bir semboller grubuna) eşlenmesidir [1](Akdeniz ve Yarman, 2000, s. 9; Kodlama nedir?, t.b.). Kısaca bu *bilgileri kodlamadır*. Örneğin, ''*elma*'' kelimesinin *78* veya *?+* sembollerinin yazıldığı bir kodlama yaratabiliriz. Genellikle kodlar zaman kazanma yöntemleridir. Gizlilik amacı taşımayabilirler. Uluslararası Mors (Alfabesi) Kod'u buna dair en bilinen örneklerdendir (Akleylek, Akyıldız ve Çimen, 2011, s. 6). Bir kod kitabı, cetveli veya listesi bu eşleşmelerin listesini gösterir. Kodlama yapılan şeyler için bir kod kitabı, cetveli veya listesine ihtiyaç vardır. Ancak Kriptografi alanında ise *Kod* kavramıyla *Şifre* kavramı arasındaki ilişki ise şu şekildedir. "Günümüzde kodların yerini şifreler alarak Kod kelimesinin kullanımı azalmış, sözcüklerin değil, harflerin yerlerini değiştirerek daha temel düzeyde işlev gören "şifre" alternatif bir kod'dur" (Akleylek, Akyıldız ve Çimen, 2011, s. 7). Bir başka deyişle şifreler de bir kodlamadır. R. F. Churchhouse, Kodlar belirli bir şifreleme sistemidir, ancak tüm şifreleme sistemleri kod değildir Kodlar ve şifreler arasındaki farkın biraz bulanık olduğu ve Julius Caesar Şifresi'nin tek sayfalık bir kod kitabı kabul etmek mümkündür, demektedir (Churchhouse, 2002, s. 5).

Ancak her kodlama bir şifreleme, yani gizleme amacı gütmez. "Teknik olarak Kod, sözcükler düzeyinde yerine koyma, şifre harf düzeyinde yerine koyma olarak tanımlanır" (Singh, 2004, s. 46). Nitekim ticari kolaylık, zaman kazanma, hız vb. faktörlere bağlı kodlamalar dışında, bilginin güvenliği veya istenmeyen kişilerce öğrenilmemesi söz konusuysa bu kodlamalar artık *şifreleme kodlamaları*dır. Şifre kavramı üzerinde durmadan önce üzerinde durmamız gereken diğer bir diğer kavram Kriptolojidir. Günümüzde Elektronik, Optik, Bilgisayar bilimleri gibi birçok disiplin için kullanan ve Matematiğin

[1] Kod, iletişimde harf, sözcük ya da sözcük grubu gibi bir bilgi birimi yerine buna eşdeğer bir başka bilgi birimini koymak amacıyla tanımlanan belirli ve değişmeyen kural olarak tanımlanır. Ancak kriptografi söz konusu olduğunda bu tanımdaki "…belirli ve değişmeyen kural…" ifadesi geçerli olduğunu söyleyemeyiz. Diğer yandan günümüz de *Kod* veya *Kodlama* terimi yukarda zikrettiğimiz anlam dışında, diğer adıyla programlamadır. Kelime anlamıyla belirli şartlara ve düzene göre yapılması öngörülen işlemlerin bütünü anlamına gelir. Programlama bilgisayara ya da elektronik devre ve mekanik sistemlerden oluşan düzeneklere bir işlemi yaptırmak için yazılan komutlar dizisinin bütünü veya bir kısmı olarak tanımlanır.

özelleşmiş bir alt bilim dalı olarak kabul edilmektedir (Akay, Obaid ve Sabonchi, 2016, s. 100). Kriptolojinin iki temel alt dalı Kriptografi ve Kriptoanalizdir.

Kriptografi; Bilgi güvenliği kavramlarını sağlamak için çalışan matematiksel yöntemler bütünüdür. Yani gönderdiğiniz bir bilginin istemediğiniz kişilerce okunmaması için kullanılan şifreleme (Encryption) tekniklerinin tümüdür.

Kriptoanaliz; Kriptografi ile şifrelenmiş dosyaların ve verilerin şifresi analiz ederek şifreyi çözmeye dayanır (Kriptografi, Sezar Şifresi ve Stenografi, t.b.).

Şifreler ise bir anlam ifade etmezler. Bunun yerine, algoritma[2] olarak bilinen, tek veya bir grup harf üzerine uygulanan araçlardır (Algoritma, t.b.). Kriptografik şifreleme teknikleri klasik ve modern olmak üzere ikiye ayrılır. Klasik şifreleme teknikleri, geçmişi yüzyıllar öncesine uzanan, kalem kâğıt veya basit aletler kullanılarak tasarlanan şifrelemelerin tekniğidir (Kındap, 2015). Bu çalışmamızda bilgi alanımız (Tarih) çerçevesinde Klasik Kriptografi'nin Osmanlı Devleti içinde kullanımına dair, Serezli (Sirozi) Yusuf Paşa'nın Kriptografisini ele alacağız.

Kısa Kriptografi Tarihi

M.Ö. 1900'de Nil Nehri üzerindeki Menet Khufu kasabasında bir kâtip, soylu Khnumhotep II'nin mezarının ana odasındaki kayaya, sıradan olanların yerine bazı sıra dışı hiyeroglif sembolleri yazmıştı. Yazıt kriptografinin temel unsurlarından biri olan yazının kasıtlı bir dönüşümü göstermekteydi. Bunu yaptığı bilinen en eski metindir (Kahn, 1973, s. 64-65). Uzun insanlık tarihi içerisinde pek çok uygarlık, yazıyı veya bilgiyi saklama (şifreleme) konusunda farklı yöntemler kullandı. Bir mesajı saklayarak sağlanan haberleşme Yunanca, *saklı yazı* anlamına gelen *Steganografi*' dir [3] (Lunde 2013, s. 76-77). Herodot'un çağından sonraki iki bin yıl boyunca Steganografi'nin birçok biçimi kullanılmıştır. Çinliler mesajlarını yazdıkları ipeği iyice ufaltıp top yaparak balmumuyla kaplayarak, ulağa yutturup gönderirken, 16 yüzyılda İtalyan Giovanni Porta, alüminyum ve sirke karışımı ile elde ettiği mürekkeple mesajını haşlanmış bir yumurta kabuğuna yazmakta ve mürekkep pişmiş yumurta yüzeyine geçmekteydi. Böylece yazı gizlenmekteydi (Singh, 2004, s. 17-18; Lunde, 2013, s. 64).

Bu ve benzeri yöntemler yüzyıllarca kullanılmışsa da Steganografi'nin zayıf yönü habercilerin yakalanması halinde mesajların ortaya çıkmasıydı. Bu yüzden Steganografi'nin

[2] Algoritma, iyi tanımlanmış kuralların ve işlemlerin adım adım uygulanmasıyla bir sorunun giderilmesi veya sonuca en hızlı biçimde ulaşılması işlemi.

[3] Filmlere de konu olan Da Vinci'nin not defterlerinde tuttuğu kayıtlar, gerçekte şifreli değildir. Da Vinci Steganografi yöntemini kullanmıştır. Da Vinci notları, bir aynaya tutulduğunda okunabilen "ters yazılar" dı.

gelişimine bağlı olarak, mesajı saklamak yerine "mesajın anlamını" saklama çabası *Kriptografi*'nin doğuşunu sağladı (Singh, 2004, s. 19). Kriptografi doğumu sonrasında iki kola veya yönteme doğru evrildi.

(Konum) Sıra Değiştirme Şifrelemesi

YARIN SEN BÜTÜN ORDUYU TOPLA VE DÖNÜŞE GEÇ [4] (Singh, 2004, s. 20-21).

Mesajını *Sıra Değiştirme* yöntemiyle şifrelemek istediğimizde mesajdaki harfler yeniden sıralanır ve bir anagram[5]oluşturulur (Lunde, 2013, s. 66). Harf sayısı artıkça olası düzenlemelerin sayısında da olağanüstü artış olur. Bu yüzden harflerin sıralanma şekli gönderici ve alıcı arasında önceden anlaşılmış bir sistem (algoritma) doğrultusunda, yani bir şifreleme yöntemine göre yapılır. Örneğimizde *Atlama-ekleme*'li sıra değiştirme yöntemi kullanılmıştır (Singh, 2004, s. 20). Şifreleme metodu;

Y	**R**	**N**	**E**	**B**	**T**	**N**	**R**	**U**	**U**	**O**	**L**	**V**	**D**	**N**	**Ş**	**G**	**Ç**
A	**I**	**S**	**N**	**Ü**	**Ü**	**O**	**D**	**Y**	**T**	**P**	**A**	**E**	**Ö**	**Ü**	**E**	**E**	

Şekil 1.

İki gruba ayrılan mesaj aşağıdaki gibi alttaki mesaj üsttekine eklenmiştir.

Şifrelenmiş mesaj; YRNEBTNRUUOLVDNŞGÇ **AISNÜÜODYTPAEÖÜEE**

Şekil 2.

Alıcı işlemi tersten uygulayarak şifreli mesajı çözerdi. Bir başka *Sıra Değiştirme* şifrelemesi örnekleri varsa da (Çeşmeci, 2009, s. 22) konumuz bakımından üzerinde durmayacağız.

Yerine Koyma (İkame) Şifrelemesi

Tarihi süreç içerisinde *Yerine Koyma* şifrelemesi, MÖ. 205-123'te *Polybius Karesi* şifrelemesi ile karşımıza çıkmaktadır. Yunan Matematikçisi Polybius'un dama tahtası 5X'lik bir matristen oluşuyordu. Alfabe sırasıyla matrise yazılır ve her harfi belirleyen iki rakam vardır. İlk rakam harfin satırını, ikinci rakam bulunduğu sütunu ifade eder. Türkçeye uyarlanmış hali için 5X6'lık matris kullanılan bir örnek üzerinde gösterirsek;

[4] Bu mesaj 35 harflik olup, hepsi birbirinden farklı 50 Oktilyon (27 sıfır ilave) sıralama oluşturulabilir.

[5] Anagram; aynı harflerle yazılan ama harfleri yer değiştirince ayrı anlama gelen sözcük; örneğin rakı sözcüğünün harfleri yer değiştirince ortaya çıkan ırak/karı/arık sözcükleri birer anagramdır.

	1	2	3	4	5	6
1	A	B	C	Ç	D	E
2	F	G	Ğ	H	I	İ
3	J	K	L	M	N	O
4	Ö	P	R	S	Ş	T
5	U	Ü	V	Y	Z	

Polybius Karesi

Şekil 3.

Görüleceği üzere örneğin, D harfi için 15, K harfi için 32 kullanılarak şifreleme yapılır. Örneğin göndereceğimiz mesaj *Tarih Yazmak* olsun, şifrelememiz şu şekilde gelişir. 46, 11,43, 26, 24, 54, 11,55, 34, 11, 32 şeklinde şifrelenir (Akleylek, Akyıldız ve Çimen, 2011, s. 20-21).

Modern Kriptograflar, Polybius'un *dama tahtası*'nın, çok değerli özelliklerini buldular. Polybius'un dama tahtası bu nedenle çok sayıda şifreleme sisteminin temeli olarak çok yaygın bir şekilde kullanılmaktadır. Uygulamada -askeri ve diplomasi alanlarında -bu şifrelemeyi ilk kullanan kişinin *Julius Sezar* olduğu düşünülmektedir (Churchhouse, 2002, s. 2-3; Kahn, 1973, s. 72). Eski Roma yazarlarından olan Suetonius, Sezar'ın arkadaşlarına yolladığı mesajlarında alfabe harflerini "a" yerine, sonraki üçüncü basamaktaki D, B yerine E vb. harflerini kaydırarak kullandığını kaydeder. Bugünün, standart diziden oluşan herhangi bir şifre alfabesi Sezar'ınki gibidir:

	a b c d e f g h ı j k l m n o p q r s t u v w x y z
Şifre	D E F G H I J K L M N O P Q R S T U V W X Y Z A B C

Şekil 4.

"D" harfi dışında bir harfle başlasa bile bu tür kaydırmalara Sezar alfabesi denmektedir (Kahn, 1973, s. 73). Sezar şifresi basit bir *Tek Alfabeli Yerine Koyma* şifresidir. *Sezar Şifrelemesi* diye anılan ve alfabedeki her bir harfin belli sayıda ileriye kaydırılmasına yani ötelenmesine dayanan bir şifreleme metodu uzun yıllar kullanıldı (Akleylek, Akyıldız ve Çimen, 2011, s. 24-25). Yüzyıllarca süren *Tek Alfabeli (mono-alfabetik) Yerine Koyma (ikame) Şifresi* yazışmalarda güvenliği sağladıysa da önce Arap dünyasında sonrada Avrupa'da gelişen *Frekans Analizi* ve Kriptoanalizin gelişimi zaman içerisinde bu şifrenin güvenliğini yok etti.

Roma İmparatorluğu'nun çöküşüyle beraber Avrupa'da neredeyse bin yıl yerinde sayan Kriptografi, 15. yüzyıla gelindiğinde canlanmaya başladı. Politik alandaki gelişmeler ve Rönesans döneminde sanat ve bilimin gelişimi, Kriptografi'ye etki yaptı. İtalya'da diplomasinin gelişimi sonucu İtalyan kent devletlerinin birbirlerine büyükelçiler

göndermesine yol açtı. Diplomatik haberleşme önem kazanırken talimatların gizlenmesi ihtiyacı, şifrelemeyi doğurdu. Büyükelçilere şifre kâtipleri (sekreterleri) verilmeye başladı (Singh, 2004, s. 43).

Avrupa'da modern Kriptografinin gelişimi aynı zamanda Kriptoanalizi de geliştirmeye başladı. 1506'da Venedik'e şifre sekreteri olarak atanan, El-Halil veya el-Kindi'nin frekans analizini kullanan, Giovanni Soro idi (Kahn,1973, s. 79; Singh, 2004, s. 44). 1460 yılında Floransalı Leon Batista Alberti'nin, şifrelemede iki ya da daha fazla alfabe kullanılmasına (polialfabetik) yönelik girişimini, Alman Rahip Johannes Trithemius ve İtalyan Giovanni Battista Bellaso geliştirdilerse de daha ileri aşamaya taşıyan Fransız diplomat Blaise de Vigenére'ydi (Kahn, 1973, s. 91-92; Lunde, 2013, s. 73).

Avrupa uluslarında kriptoloji gelişirken, Osmanlı Türklerinin özellikle 18. yüzyıla kadar öncelikle Kriptografiye ve dolayısıyla Kriptolojiye ilgisi oldukça sınırlıdır. Osmanlı Devleti'nin kuruluşundan itibaren halk kültürü ve edebiyatında, (*remizi, rümûzi, lugazlı*) kısaca "bilmece"li diyebileceğimiz şifre veya şifreye benzer alfabe ve sayıların kullanıldığı, araştırmacılarca tespit edilmiştir. Amil Çelebioğlu, bu tür yazı veya şifreleri sınıflamaya çalışmıştır. (Çelebioğlu, 1988, s. 19-20) Türk Edebiyatı'nda ise "Tarih Düşürme" Chronogram, önemle üzerinde durulan bir sanat geleneği olarak dikkat çeker (Karabey, 2011, s. 80-82). Ebced Sisteminden faydalanılarak, ağaca benzemesi nedeniyle de "ağaç biçimli yazı" anlamına gelen (Çelebioğlu, 1988, s. 24-25) "Hatt-ı Şecerî" ile şifreli yazılar yazılmıştır. Türkçe, Arapça ve Farsça el yazması eserlerdeki kayıtlardan görüldüğü kadarıyla, İslam dünyasının hemen her yerinde çeşitli amaçlarla "Hatt-ı Şecerî" kullanılmıştır. Türklerde şifrelemeler konusunda ilk akademik çalışmayı yapan M.J.A Decourdemanche, Hatt-ı Şecerî'yi verdiği dört farklı türdeki şifreli yazıdan biri olarak tanıtır (Decourdemanche, 1899, s. 261-264).

Nihayet 19. yüzyıl başında bir ansiklopedi yazarı olan Mehmed Hafid Efendi de şifrelemenin bazı türlerini bize vermektedir (Hafîd, 2018, s. 441-465). Ancak Osmanlı Devleti'nin resmi işlemlerinde ne bu türde ne de başka bir tarzda şifreleme biçimine 18. yüzyıla kadar rastlanılmaz. Hatta bu tür girişimlerinde hoş karşılanmadığını da söyleyebiliriz.

Osmanlı Devleti'nin Şifrelemeye Bakışı

Osmanlılar diplomasi alanında yabancı elçiliklerin şifre kullanmasını 15.yüzyılın sonuna kadar şüpheli teşebbüsler olarak değerlendirmiştir (Bingöl ve Pınar, 2021, s. 1-19). Ancak bu tür girişimleri, 16. yüzyılın ortalarından itibaren diplomasinin zorunlu bir gereği olarak görmeğe başlamıştır. Devletlerarası ilişkiler bakımından, sonraki yüzyıllar içinde

zorunluluk temelinde gelişen uygulamalar, Osmanlı Devleti açısından da kabul edilebilir olmuştur. Nitekim Osmanlı Devleti'nde şifreleme ve kodlamalar resmi işlemlerde sık olmasa da 18. yüzyılın başlarından itibaren görülmeğe başlamıştır. Bu konuda ilk ve belki de tek örneğimiz, Hayrullah Örs'ün yayınlamış olduğu iki belgede görülmektedir. H. Örs, *Frekans Analizi* yöntemiyle bu şifreleri çözmüş, Türkçe olanın deşifresini ve her iki belgenin şifre anahtarlarını (miftah) vermiştir. 18. yüzyıla ait belgenin içeriğine bakıldığında, vergi tahsildarlarının (haraç-güzâr) yolsuzluklarına dair bir rapordu (Örs, 1964, s. 84-87).

18. yüzyıl sonlarına doğru kamusal alanda şifre kullanımına dair başka emareler (COA, HAT 986-41774; 125 – 5171) varsa da asıl ve yoğun kullanımı 19. yüzyıl başlarında diplomasi alanında oldu. 19. Yüzyıl başına kadar, Osmanlı Diplomasisinin en karakteristik özelliği mütekabiliyet ilkesine dayanmamasıdır. Osmanlı Devleti, Avrupa devletlerinin ikamet elçilerini yüzyıllarca kabul etmesine rağmen, kendisi XVIII. yüzyılın sonuna kadar Avrupa başkentlerine ikamet elçileri göndermemişti. Osmanlı Devleti yeni bir yüzyıla girerken eski anlayışını terk ederek, III. Selim devrinde Avrupa'nın önemli başkentlerine ikamet elçileri gönderdi. Bu girişimin ilk günlerinden itibaren diplomaside şifre kullanımı başlamıştır. Şifre kullanımlarına *Kod*'larında eşlik ettiği görülmektedir.

19. Yüzyıl Osmanlı Diplomasisinin Şifreleri ve Kodları

III. selim devrinde diplomatik bürokrasisinin gelişimiyle birlikte resmi alanda Osmanlı Kriptografisi doğmuştu. 29 Ocak 1795'te Londra'ya Yusuf Agâh 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 Büyükelçi statüsünde atandılar (Kuran, 1988, s. 24-25). 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 (Bingöl, 2021). 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 (mono-alfabetik) Yerine Koyma (ikame) Şifresi" özelliğine sahipti. Yine şifrelerle birlikte kelime temelli, açık yazılmış kodlar da kullanılmıştı. Herhangi bir anlamı olan veya olmayan "Kod kelime" kullanımları dışında[6] (Bingöl, 2021) kodların sayısallaştırılması yoluna da gidilmişti. Ocak 1795'te Londra'ya Yusuf Agâh Efendi atanmasıyla başlayan süreç, çeşitli siyasal olaylar çerçevesinde büyükelçilerin geri çağrılması ve en nihayet, son Paris

[6] Örneğin, Paris elçimiz Abdurrahim Muhib Efendi, Fransa için "*şeytan, melun", İsveç için "Eşek" kodlarını kullanıyordu.*

Büyükelçisi Abdurrahim Muhib Efendi'nin 21 Ağustos 1811'te dönmesiyle sona erdi (Bingöl, 2021).

Böylece III. Selim devrinde başlayan Avrupa başkentlerine ikamet elçisi atama usulünden vazgeçilmiş oluyordu. Londra, Berlin, Viyana elçiliklerine zaten daha önceki yıllarda yeni atama yapılmayarak, dış temsilcilikler maslahatgüzarlara bırakılmıştı (Kılıç, 2019, s. 257; Dönmez, 2006, s. 28-32). Bu maslahatgüzarlar da merkezle yazışmalarında "Tek Alfabeli Yerine Koyma (ikâme)" şifrelemeleri ve kelime temelli kodlamalara devam ettiler (COA. HAT 1347-52652-E; 1347-52652-Ç; 252-14356; 237-13179; 1348-52711).

Ancak 1806-1812 Osmanlı-Rus Savaşı'nın ardından 31 Ekim 1811'de başlayan görüşmeler için Mehmed Said Galip Efendi gönderilmişti (Düzcü, 2016, s. 183; Köprülü, 1996, s. 330). Bükreş Antlaşması'nın imzasıyla sonuçlanan görüşmeler için Galip Efendi'ye verilen şifre anahtarı yine tek alfabeli (mono-alfabetik) "Yerine koyma (ikame) şifresi" verilmişti. Kodlar ise kelime temelli olmayıp, ilk kez 3 basamaklı sayılar şekline dönüşmüştü. Örneğin, 444- Kotozof, Rus General, 655- Rusya Baş Delegesi, 888- Fransa'yı ifade ediyordu.

Daha sonra Kodların sayısallaştırılmasının bir başka örneğine 8 yıl sonra İran'a elçi olarak gönderilen Süleyman Hadi Efendi'ye doğrudan kendisine verilmiş olan 14 Mart 1819 tarihli Miftahda (Anahtar) rastlıyoruz. Bazı kodlarına baktığımızda, 222-İran Şahı 888-Devlet- Aliyye, 111- İran Devleti'ni ifade ediyordu. Süleyman Efendi'ye verilen anahtara baktığımızda, yine her Osmanlı harfinin karşılığında bir ya da iki basamaklı sayı verilmişti. Kodlar ise üç basamaklı yine idi (COA. HAT 800-37061).

Osmanlı Dâhili Yazışmalarında Kriptografi

Hariciyenin başlattığı şifreli yazışma, zamanla Osmanlı iç yönetim kademelerinde de revaç bulmuştu. Bizim tespit edebildiğimiz kadarıyla Osmanlı bürokrasisinin Kriptolu yazışma uygulamalarının başlangıcı 1816 yılına aittir. 1 Mayıs 1816'da İran'a memur Süleyman Efendi ve Naşid Bey taraflarından "hurûf-ı ma'hûde" ile yazılan bir tahrirat[7] (COA. HAT 1432-58608) görünen şifre salt sembollerden oluşmaktaydı. Ancak bu tarihin yapılacak araştırmalarla, geriye çekilebilme ihtimali bulunmaktadır. Sadece semboller üzerinden şifreleme yapılmıştır. Ancak makalemizin kapsamı dışında bir konu olması nedeniyle üzerinde durmayacağız.

[7] Bitirdiğimiz 19. yüzyılın tamamını kapsayacak olan ve "Osmanlı Kriptografisi" başlığını vermeyi düşündüğümüz, yayın hazırlıklarını sürdürdüğümüz çalışmada ayrıntılı bilgi bulunacaktır.

1818'de de Belgrad'a gönderilen Kethüda Kâtibi Esbak Necib Efendi'ye Sırpların ve Semendire Sancağı'nın durumunu tahkik ederek İstanbul'a bildirme görevi verilmişti (Doğan, 2019, s. 31; Duran, 2019, s. 156). Ona verilen kodlar da 3 basamaklı sayılardan oluşuyordu. Örneğin, 615- Sırp Milleti, 113, Belgrad'ı ifade ediyordu (HAT 1145-45509 A;1206-47293-Ç; 400-21033-A; 400-21033-B; 1206-47293-F). Osmanlı Kriptografisi giderek daha güvenilir bir aşamaya geçmekteydi. Aynı şekilde Yusuf Paşa'nın da bu erken dönemde bir şifreli yazısına rastlamaktayız.

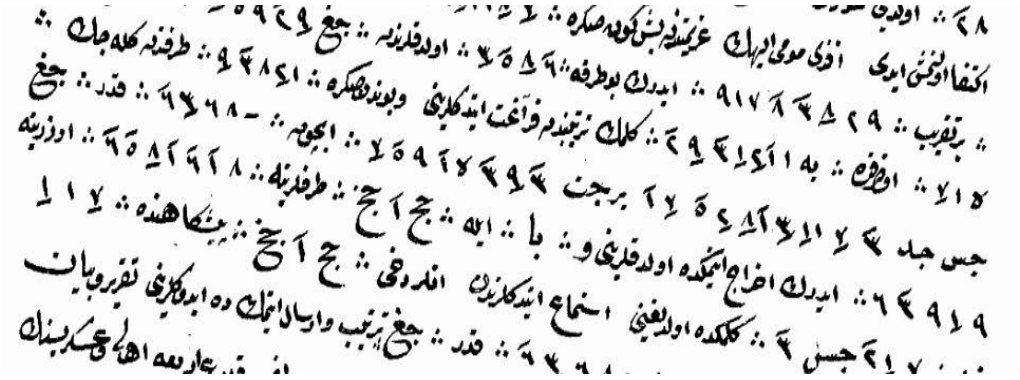
Sirozî Yusuf Paşa'nın Şifresi

Osmanlı devleti 19 yüzyıla girerken güçlü merkezkaç kuvvetler bulunmaktaydı. Bunlar arasında Sirozi İsmail Bey'de[8] önemli bir Âyan ailesi kurmuştu (İnal, 1969, s. 969). Sirozi İsmail Bey'in oğullarından Yusuf Muhlis Paşa makalemizin konusunu oluşturmaktadır. Babası İsmail Bey'in vefatı üzerine (Evasıt Recep 1228) 1813 yılı temmuz ayı ortalarında Siroz Âyanlığı'na tayin oldu (Serezli, 2012, s. 4-6).

Rusya desteğiyle, bağımsız bir Yunan devleti kurmak amacıyla Aleksander İpsilantis (Ypsilantis) Şubat 1821'de Prut üzerinden Eflak ve Boğdan'a girip bir isyan başlattı. Osmanlı ordusunun bölgeye girmesiyle isyan bastırıldı. Ancak sonrasında İstanbul'da Rum Patriği V. Grigorios ile pek çok metropolit ve cemaat önde gelenlerinin idam edilişi vb. nedenlerle isyan tekrar canlandı. Mora yarımadası, Ege adaları, Tesalya ve Selanik bölgesinde hızla yayıldı (Aydın, 2018, s. 304). Dağılan isyancılar isyanı Mora Yarımadası'na yaydılar. Rumlar, 6 Nisan 1821'de Kalavrita Kalesi'nde isyanı resmen ilan ettiler. İsyanın liderliğine Aleksander İpsilanti'nin kardeşi Dimitrios getirildi (Örenç, 2011, s. 9-10). Kısa sürede isyan Mora'nın her yerine yayılmasıyla Selanik'e kadar olan bölgede etkisini göstermişti. Eğriboz'da ayaklanmış ve Sirozi Yusuf Paşa Eğriboz Muhafızı olarak atanmıştı. Balyabadra Kalesi isyancılarca kuşatılınca, Yusuf Paşa buraya ulaşarak, kuşatmayı kaldırdı. Buranın muhafızlığı kendisine verildi (Bayrak, 2019, s. 72-73). Bu arada isyan bütün adalara yayılmıştı.

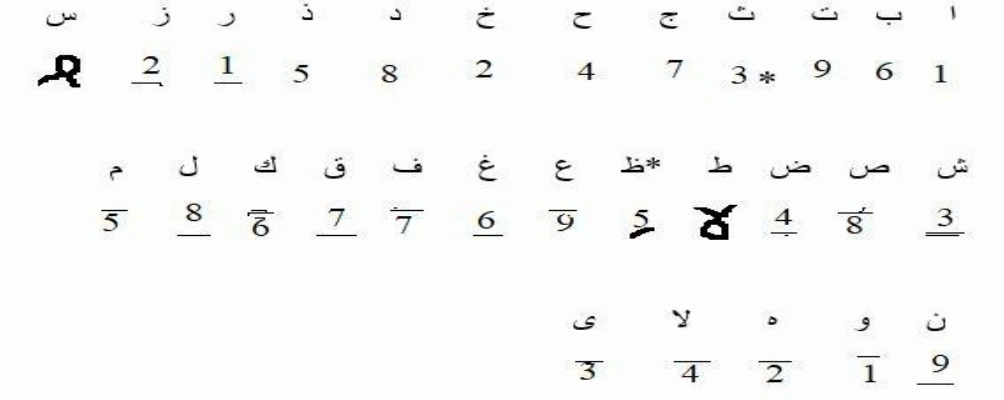
İsyan sürerken Sirozi (Serezli) Yusuf Paşa merkezle doğal olarak bilgi paylaşımı yapmaktaydı. Ancak mesajları şifreliydi. Şifreli kullanımına dair bir örnek yazısını verelim.

[8] 1808 Sened-i İttifak'ın imzalanmasıydı İstanbul'a davet edilip de gelenler ve 1808 Sened-i İttifak'a imza atanlar arasında Sirozi İsmail Bey'de vardır.



Şekil 5. (COA. Hat 934-40441 -a)

Mesajlarında şifre kullandığını gördüğümüz Sirozi Yusuf (Muhlis) Paşa'ya ait Mart-Nisan 1823 tarihli 3 adet şifreli yazı için ve ayrıca bu tahriratların deşifresi için bakınız (COA. HAT 934-40441 -A; 934-40441- B; 934-40441-C; HAT 934-40441). Sirozi Yusuf (Muhlis) Paşanın kullandığı şifre miftahı (Anahtar) ise şöyledir.



Şekil 6. Yusuf Paşa Miftahı (Anahtarı)[9]

Kelimeler arasına ⁘ bir anlamı olmayan ayırıcı işareti konmuştur. Kriptolu metine ayrıca "به Badra, عج Zahire, خ Kaptan Paşa hazretleri, با Donanma-yı Hümayun" vb. kodlar da yerleştirilmişti. Öte yandan kodlar konusunda Yusuf Paşa teknik bir yenilik getirmişti. Anlamlı veya anlamsız kelime öbekleri yerine, yukarda örneklerini verdiğimiz, sadece harflerden oluşan çoğu zaman hiçbir anlam ifade etmeyen harf öbekleriyle kodlama yapmayı düşünmüştü. Diğer yandan "Tek Alfabeli Yerine Koyma (ikâme)" şifresi kullanmakla beraber, şifrelemeye de yine bir yenilik getirmişti. Muhtemelen orijinali "Hatt-ı Kemsıla" olan bir şifre alfabeden esinlenmişti. Bu tarzı kendi şifresine uygulamıştı. *Hattı Kemsıla* adı verilen bu tarzı kısaca anlatırsak;

[9] Miftahta * işaretiyle gösterilen harflerin sıklık derecesi az olup, şifreli ve açık metinde gösterilmemiş olup tarafımızdan tahminen konmuşlardır.

Hatt-ı Şeceri'de yer alan 8 anahtar kelime grubu gibi *Hattı Kemsıla* 'da bu kez grup sayısı 7 olarak belirlenmişti.

Şekil 7. (Hafîd, s.465)

Burada "1- abcd 2- hvzh 3- tykl 4- mns' 5- fskr 6- ştsh 7- zdzg" şeklinde gruplandırılan kelimelerle, farklı bir düzen kullanılmıştır[10](Çelebioğlu,1988, s. 29; Egüz, 2010, s. 309). Her gurup 4 harften oluşurken her grupta 1. harflerin üzerinde fetha **(´)**, 2. harflerin üzerinde ötre **(ُ)**, 3. harflerin altında esre **(ِ)** 4. Harflerin üzerinde cezm **(ْ)** işaretleri bulunmaktadır. Bundan sonra şifrelenecek ibare mesela "dünya" kelimesi olsun, Osmanlıca yazılışı دنیا olup,

Yukardaki gruplamalara göre, د harfi 1. grupta olup harekesi cezm (ْ) dir. Birinci gruptaki harf o zaman دْ'dır. Bu örneğe göre, sırayla yazdığımızda Osmanlıca görünüm şöyle olur;

Şekil 8.

Yine Osmanlıca sayılarla ifade edersek,

Şekil 9.

şeklinde kriptolanmaktadır. Doğal olarak işlem tersine çevrildiğinde ise deşifre olmaktadır. Anlaşılan edebi kimliği ve kendisine ait bir Divân'a da sahip bir kişi olarak hem Âşirefendizâde Mehmed Hafîd'in eserini hem de Priştineli Begzâde Nûrî Divanı'nı görmüş ve ilham almıştı.

Bu miftahı kullanan Sirozi (Serezli) Yusuf Paşa daha sonra 1818 [1233 H.]'de memuren Yanya'da bulunduğu esnada vezirlikle Ağrıboz muhafızlığına, daha sonra Saruhan, Haleb eyaleti valiliklerine tayin kılındı. Az müddet sonra Karaburun ve İğne Ada

[10] Esra Egüz bu şifrelemeyi incelediği Priştineli Begzâde Nûrî Divanı'ndaki kayda göre "Hatt-ı Rumuz" olarak niteler. Ancak hem Âşirefendizâde Mehmed Hafîd'in eserinde hem de Amil Çelebioğlu'nun gösterdiği "Hatt-ı Kemsıla" ismini kullanmayı tercih ediyoruz.

muhafızlığına atandı (İnal, 1969, s. 969; Süreyya, 1996, s. 1694). 1827'de Halep Valiliği'ne atandıysa da kısa süre sonra azledildi (Lûtfî, 1999, s. 194).

Sirozî Yusuf Paşa'nın Esareti ve Şifreleri

Yusuf Paşa Nisan 1828 'de başlayan Osmanlı-Rus Savaşı sırasında Varna Muhafızlığı'na atandı. Rus muhasarasına karşı denizden Kaptan-ı Derya (Darendeli) İzzet Paşa'da gönderilmişti (Lütfi, 1999, s. 335). Ancak Varna'ya destek kuvvetleri gelemediği için 13 Ekim 1828 de düştü (Lütfi, 1999, s. 348). Sirozi Yusuf (Muhlis) Paşa Rusların esiri olarak, 23 Ekim 1828'de Odesa'ya götürüldü. Ancak Sirozi Yusuf (Muhlis) Paşa hain sıfatıyla damgalanarak malına, mülküne el konulmuştu[11] (COA. HAT 1015-42494; Varol, 2021, s. 148-164). Üstelik bu hain damgalamasının birinci derecede müsebbibi olan Darendeli İzzet Mehmed Paşa (14 Rebiyülahir 1244) 24 Ekim 1828'de Sadaret makamına geçmişti (Lütfi, 1999, s. 352).

İşin bu kısmı bir yana Sirozi Yusuf (Muhlis) Paşa, esareti sırasında (13 Cemâziyelevvel 1244) 21 Kasım 1828 tarihli bir mektup serisini ailesinin üyeleri ve güvendiği adamlardan olan Baruthane Nazırı Necip Efendi gibi kişilere göndermişti. Mektuplarında çektiği hasret, mali zorluklar veya bazı eşyaların satılıp kendine gönderilmesi gibi hususlar yer almaktaydı (Varol, 2021, s. 166-168).

Ancak bu mektuplar arasında, yine esaretteki Yusuf Paşa'nın (13 Cemâziyelevvel 1244) 21 Kasım 1828 tarihli olanı dikkat çekicidir. Sadrazamın İstanbul dışında cephede olmasına binaen, Sadaret Kaimmakamına hitaben yazılmış olan mektupta,

> "…farîza-i zimmet ubudiyetim olan hal-i acziyetimin dahi elden gelen sadâkatin icrâsında kusûr etmemek i'tikâd sahihinde olduğuma binâen hasbelkader esir olduğum halde mersuman Amiral ve Graf ve Ransof ve sâirleriyle görüşülüp onlar bizim imparatorumuz Devlet-i Aliyye ile mübâyeneti istemezdi… Ancak tarafeynde kıtal ile sefk-i dimâ'olmaması için Devlet-i Aliyye tarafından musâlahaya rağbet olunsa imparator dahi muhâdeneye râzı olur idi deyu ifâde ettiklerinde… imparatorun merâmı Ulah ve Boğdan usûlü üzere fakat Mora'nın serbestliğidir… deyü ifâde ediyorlar. Şimdiki halde Rusyalu'nun umûr-ı harbiyede nizâm ve kuvvet-i kemâlde ve bâ-husûs bahar mevsimi için tedârikât-ı külliyesi evvelkiden birkaç kat ziyâde…"

dedikten sonra Yusuf Paşa nihayet,

[11] M. Varol, Varna'nın düşmesinde Sirozi Yusuf (Muhlis) Paşa'nın rolü konusunda ileri sürülen görüşleri, sıkı kaynak eleştirileriyle çürütüp, Sirozi Yusuf (Muhlis) Paşa'ya atfedilen "hain" damgasının haksızlığı ortaya konmuştur. Ayrıca (13 Cemâziyelevvel 1244) 21 Kasım 1828 tarihli Sadaret Kaimimakamı'na hitaben tahriratında Varna'nın düşüşünü anlatarak, savunmasını yapmıştır. Bu savunma incelendiğinde haksız bir ithama maruz kaldığı görülecektir.

> "…Devlet-i Aliyye tarafından musâlahaya rağbet buyrulduğu takdirde onların dahi musâlahaya meylleri olduğu mersûmların sohbetlerinden fehm olunmağın bu husûs-ı muvafık idâre-i aliyye olur ise eğerçe böyle madde-i cesimede kulunuz bulunmamış olduğumdan kavuşturacağım maslahat değil ise de elimden geldiği kadar bazı sohbetlerini ederek meramları anlaşılmak için bervech-i hafî kulunuza bir ta'limnâme gönderilse ve irâe olunmak için gayri mültezim sûret ve ibâ-i cevâb ile birkaç satır emirnâme irsâl buyrulsa iktizâsına say ve gayret edeceğim…" (COA. HAT 1015-42494-A).

Bir arabuluculuk teklifi ya da Rusların barış görüşmeleri öncesi düşüncelerini öğrenmek gibi bir role soyunmak istemekteydi. Bunun için kendine bir talimat verilmesini teklif ediyordu. Bu arada yine aynı tarihli, yani (13 Cemâziyelevvel 1244) 21 Kasım 1828 tarih ve Yusuf Paşa imzalı iki mektup ise Siroz'a yollamıştır. (11 Cemaziyelahir 1244) 19 Aralık 1828'de Siroz'a Viyana postası yoluyla ulaşan ve yeni Siroz Ayanı Karaosmanzade Yakup Ağa tarafından güya ele geçirilen Yusuf Paşa'nın mektupları, derhal İstanbul'a gönderilmişti. Mektupların birisi Siroz'da Yusuf Paşa'nın dayısı Abdurrahman Ağa'ya, bir diğeri Biraderi Abdi Bey'e hitaben yazılmışlardı. Yukarda zikrettiğimiz Baruthane Nazırı Necip Efendi'ye ya da Sadaret Kaimmakamlığı'na yani doğrudan İstanbul'a yazmak yerine Siroz'a yazması ilginçtir. Çünkü bu mektuplarda Yusuf Paşa'nın hazırladığı anlaşılan iki adet şifre miftahı ve geniş kapsamlı kodlar dizisi bulunmaktaydı.

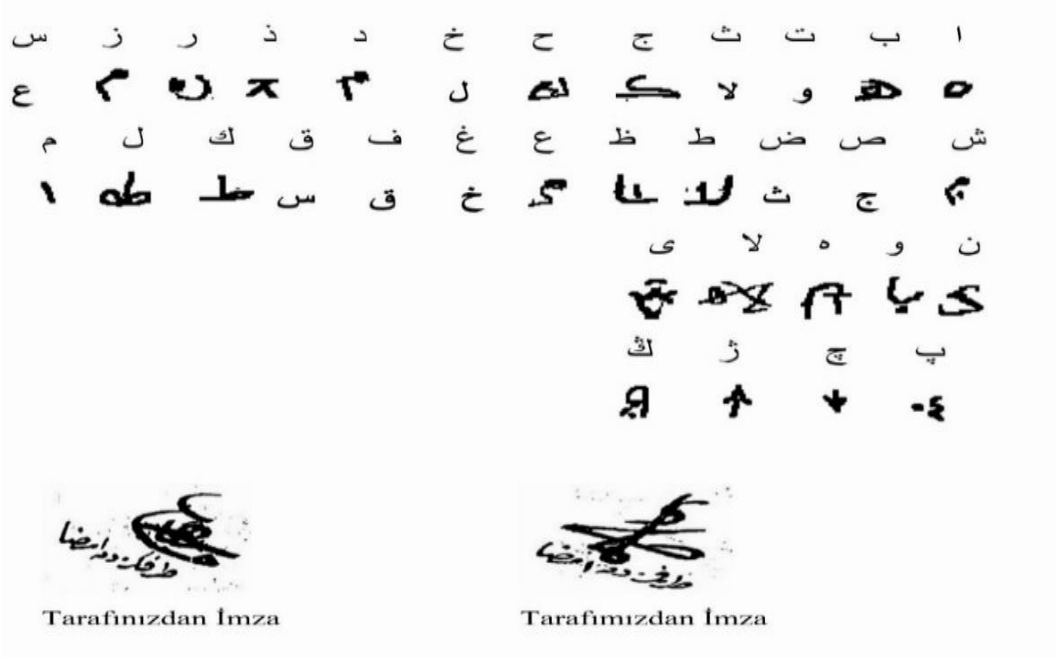
Dayısı Abdurrahman Ağa'ya, bir diğeri Biraderi Abdi Bey'e hitaben yazılan mektuplar içerik bakımından, devlete mahsur oluşturabilecek ya da onun dönüşünü muhtemelen engellemek isteyen Siroz Ayanı Karaosmanzade Yakup Ağa'nın ileri sürdüğü gibi aile fertleri vb. beraber bir tehdit oluşturma özelliğine sahip değildi.

O zaman bu derece kapsamlı bir şifre ve kodlamaya neden ihtiyaç duymuştu? Anlaşılan yukarda mektubunda bahsettiği Rus generallerle ya da yetkililerle görüşmeleri sonrasında Yusuf Paşa, muhtemelen onların bilgisi dâhilinde bir arabuluculuk teklifini yaparken, aynı zamanda onlardan habersiz Beç'e (Viyana'ya) bir şekilde bu iki mektubu göndermişti. Söz konusu iki adet şifre miftahı ve kodları içeren mektupları, muhtemelen Ruslardan gizli olarak ve dikkat çekmemesi için Dersaadet yetkililerine doğrudan göndermek yerine, Viyana'dan Siroz'a postalattırmıştı. Geriye kalan İstanbul'a ulaştırılması işini Siroz Ayanı Karaosmanzade Yakup Ağa'nın bizzat yapacağını düşünmüş ve haklı çıkmıştır. Böylece kendisine İstanbul'dan talimat vb. gönderilmesi için gereken şifre ve kod anahtarını vermiş olmaktaydı.

Bu görüşümüzün altında yatan neden Dayısı, biraderi ya da diğer aile üyelerine ve kendi adamlarına yazmış olduğu mektupların konusu, genellikle para meseleleri veya aile

üyelerinin hal ve gidişatını ya da kendisinin durumunu anlatmaktan ibaretti. Neticede aile ilişkileri, para vb. konularda yazacağı ve alacağı mektupların şifreli olmasına gerek yoktu. Ancak bu derece geniş kapsamlı 2 anahtar hazırlanması kendisinin tasarlayıp aday olduğu görevle ilgili olması gerekir.

Nitekim arabuluculuk teklifini yineleyen benzer bir mektubu da 1 ay sonra (19 C. 1244) 27 Aralık 1828'de bu kez Reisülküttab'a hitaben yazmıştır. Neredeyse benzer ifadelerle aynı talebini yinelemiştir (COA. HAT 1070-43777-A; Varol, 2021, s.171). Bu anahtarlar ve kod listelerini vererek meramımızı daha net anlatabiliriz.



Şekil 10. (Dayısı Abdurrahman Ağa'ya) Yusuf Paşa Şifre Miftahı

Şifre anahtarına baktığımızda, temelde tek alfabeli (mono-alfabetik) bir "Yerine koyma (ikame) şifresi" olmakla beraber, anahtarın yarısını semboller oluşturmaktaydı.[12] Yusuf Paşa'nın kriptografik alanda yine farklı bir yaklaşım gösterdiğini görüyoruz. Bunun dışında gelişmiş bir Kod Sistemi kullanmaktaydı. Önce numerik kodlar kullanmıştı. Ancak bu numerik kodlar, yukarda örneklerini verdiğimiz 3 basamaklı numerik kodlar değildi. Yusuf Paşa Kesirli sayılar yoluyla kodlama yapmaktaydı. Kodları ise şöyleydi;

> "Şer-i şerif (Hüma), Şeriat-ı Mutahhara (Sa), Kanun (<u>☰</u>), Âdet (Â), Padişah (1/10), Devlet-i Aliyye (1/9), Sadaret-i uzmâ (1/8) Sadrazam (1/7), Şeyhülislam (1/6), Mehmed Ali Paşa (1/5),

[12] Yukarda zikrettiğimiz, 1 Mayıs 1816'da İran'a memur Süleyman Efendi ve Naşid Bey'ler kullandığı gibi salt sembollerden oluşan bir şifre anahtarı yerine, Yusuf Paşa şifre anahtarının yarısını sembollerden kurmuştu. Ancak hemen belirtelim ki, Süleyman Efendi ve Naşid Bey'in sembolleri ile Yusuf Paşa'nın kod sembolleri birbirlerinden farklıdır.

İslambol Kaymakamı Paşa (1/4), Rikâb-ı Hümayun Kaymakamı Paşa (1/3) Hüsrev Paşa (1/2), Asakir-i Mansure Seraskeri (1/1), Ordu-yu Hümayun Seraskeri (2/10), Tuna Sevahili Seraskeri (2/9) Erzurum Canibi Seraskeri (2/8), Rikâb-ı Hümayun Seraskeri (2/7), Vidin Kolu Seraskeri (2/6), Rumeli Seraskeri (2/5) Mora Seraskeri (2/4), Serasker (2/3), Asakir-i Mansure Seraskeri (2/2), Vezir (2/1), Vüzerat (3/10) El-hac İbrahim Paşa (3/9), Said Paşa (3/8), Halil Paşa (3/7), Reşid Paşa (3/6), Galib Paşa (3/5) Rauf Paşa (3/4), İmamüddin Paşa (3/3), Sengelli İbrahim Paşa (3/2), Aliş Paşa (3/1), Celal Paşa (4/10) İsmed Paşa (4/9), Derviş Paşa (4/8), Köse Mehmed Paşa (4/7), Hacı Mustafa Paşa (4/6), Palaslı İsmail Paşa (4/5) Kapudan Paşa (4/4), Sadr-ı Esbak Silahdar Ali Paşa (4/3), Salih Paşa (4/2), İşkodralı Mustafa Paşa (4/1), Namık Ali Paşa (5/10)

Kavanozzade Hüseyin Paşa (5/9), Hafız Ali Paşa (5/8), Kara Süleyman Paşa (5/8), Der Girit, İzmirli Hasan Paşa (5/6) Kethüda-yı Sadr-ı Ali (5/5), Reis Efendi (5/4), Defterdar Efendi (5/3), Çavuşbaşı (5/2) Tersane Emini (5/1), Darbhane Emini (6/10), Mukataat Nazırı (6/9), Asakir-i Mansure Nazırı (6/8) Hüsnü Bey (6/7), Pertev Efendi (6/6), Ata Efendi (6/5), Hekimbaşı Efendi (6/4), Tabib Efendi (6/3) Silahdar-ı Şehriyari (6/2), Sır Kâtibi Efendi (6/1), Baş Çukadar Bekir Ağa (7/10), Hazine-i Hümayun Kethüdası Emin Ağa (7/9) Darüssaade Ağası (7/8), Hazinedar Ağa (7/7), Büyük Mirahur Ağa (7/6), Küçük Mirahur Ağa (7/5), Bostancıbaşı (7/4) Hünkâr Kapıcılar Kethüdası (7/2), Paşa (7/1), Mir-i Miran (8/10), Bey (8/9), Efendi (8/8), Ağa (8/7), Adam (8/6) Kethüda (8/5), Hazinedar (8/4), Divan Kâtibi (8/3), Silahdar (8/2), İç Çukadar (8/1), Mühürdar (9/10) Kaftan Ağası (9/9), Kapıcılar Kethüdası (9/8), Divan (9/7), Katib (9/7), Yazıcı (9/5), Tatar (9/4) Hatt-ı Hümayun (9/3), Ferman (9/2), Buyruldu (9/1), Kaime (9/0), Mektub (0/10), Tezkire (0/9), Kağıd (0/8) Menzil (0/7), Posta (0/6), Süvari (0/5), Piyade (0/4), Asakir-i Mansur (0/3), Ulufeli Asker (0/2) Nefir-i Amm Askeri (0/1), Yeniçeri (1/0), Muharebe (2/0), Musaleha (3/0), Meclis-i Şura (4/0), Meşveret (5/0), Mukaleme (6/0), Müzakere (7/0), Murahhas (8/0), Elçi (9/0), Evvel (10/0), Ahir (11/10), Sani (20/20), Muhabere (30/30), Mekatibe (40/40) Rical-i Devlet (50/50), Ulema (60/60), Mütesellim (70/70), Duyure (80/80), Ayan (90/90), Menab (10/20), Azl (10/30), Nasb (10/40) Tevcih (10/50), Tevcihat (10/60), Nef'i (10/70), İdam (10/80), Müsadere (10/90), Zabt (21/21), Aman (20/30), Vali (20/40)

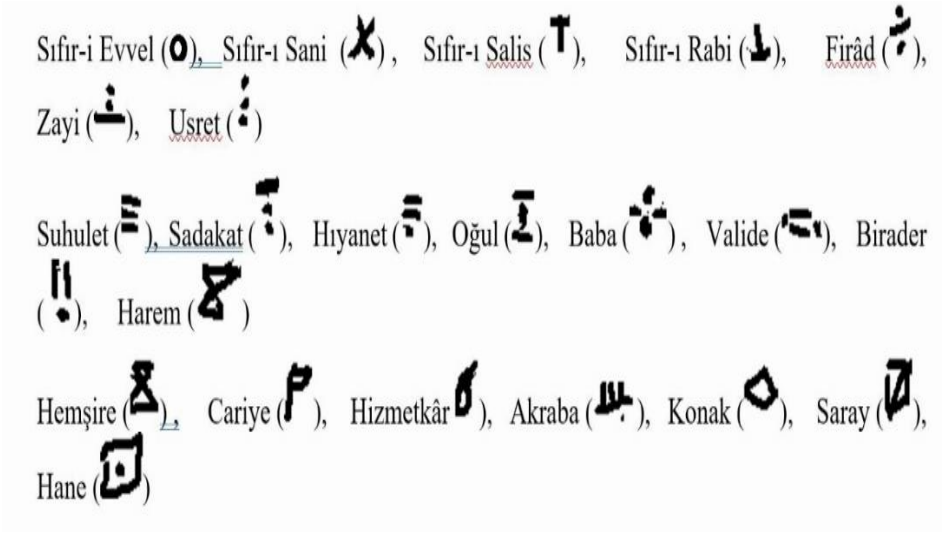
Vilayet (20/50), Eyalet (20/60), Sancak (20/70), Kaza (20/80), Kasaba (20/90), Köy (30/10), Çiftlik (30/20), Malikane (30/30), İslambol (30/50), Edirne (30/60), Selanik (30/70), Yenişehir (30/80), Mora (30/90), Badre (40/10), Kastel (40/20), Modon (40/30) Koron (41/41), Yanya (40/50), Preveze (40/60), Narda (40/70), İşkodra (40/80), Mısır (40/90), İskenderiye (50/10), Şam (50/20) Haleb (50/60), İzmir (50/70), Kütahya (50/80), Gelibolu (50/90), Siroz (60/10), Vidin (60/20), Şumnu (60/30), Ruscuk (60/40) Silistre (60/50), Varna (61/61), Asyolu (61/70), İneata (60/80), Aydos (60/90), Mesuri (70/10), Derviş Büvan (70/20) Köprü Köyü (70/30),

Cenke (70/40), Kazgan (70/50), Çalık Kavak (70/60), Şıpka (71/71), Cenkine Derbendi (70/80), Hamioğlu Pazarcığı (70/90) Kavarna (80/10), Balçık (80/20), Tolçı (80/30), İsakçı (80/40), Babadağı (80/50), Hocabey (80/60), Kırım (80/70) Petreburg (80/80), Beç (80/90), Belgrad (90/10), Eflak (90/20), Boğdan (90/30), Rumeli (90/40), Anadolu (90/50) Erzurum Canibi (90/60), Bahr-i Sefid (90/70), Bahr-i Siyah (90/80), Bahr-i Sefid Boğazı (91/91), Bahri Siyah Boğazı (110/110) Nehr-i Tuna (11/11), Neh-i Kamçı (12/12), Donanma-yı Hümayun (13/13), Donanma (14/14), Üç Anbarlı (15/15), Kaynak (16/16), Fırkateyn (17/17) Berik (18/18), Galib (19/19), Mağlub (210/210), Mansur (11/22), Makhur (24), Sağ (24), Hasta (25), Mecruh (26)

Vefat (27/27), Halas (28/28), Esir (29/29), Habs (310/310), Necat (32/32), Selamet (322/322), Sabık (33/33), Lasık (34/34) Sadık (35/35), Hain (36/36), Sahih (38/38), Kizb (39/39), Hilaf (410/410), Muhalif (42/42), Fesad (43/43), İhtilal (44/44) Asayiş (45/45), İstirahat (46/46), Haber (47/47), Havadis (48/48), Makv (49/49), Nemçe (51/51), İngiliz (52/52), Fransız (53/53)

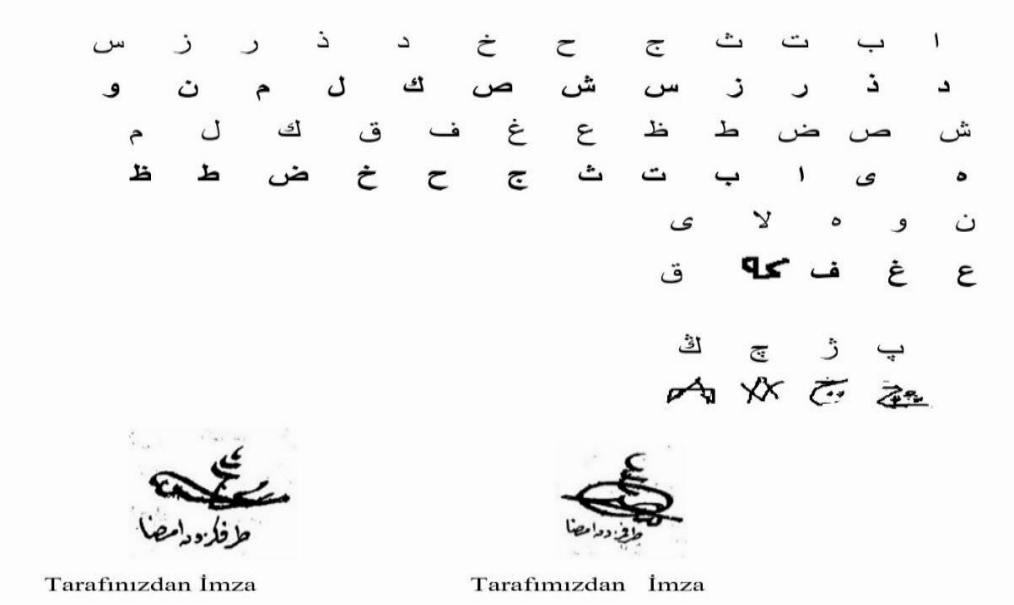
Amerika (54/54), Sardinye (56/56), Rum Gavurları (57/57), Tercüman (58/58), Gizli (59/59), Aşikâr (61/61), Taife (62/62), Daire (63/63) Arnavud (64/64), Türk (65/65), Sirkat (66/66), Hatta (67/67), Mevcud (68/68), Akçe (69/69), Altun (710/710), Yolcuye (72/72) Tebdil (74/74), Tahvil (74/74), Nefl (75/75), Hareket (76/76), Azimet (77/77), İkamet (78/78), Tertib (79/79), Tedarik (810/810) Nefer (82/82), Hazr (83/83), Tarik (84/84), Cesed (86/86), At (87/87), Bargir (88/88), Araba(89/89), Muhtemat (910/910) Top (92/92), Tüfenk (93/93), Kılıç (94/94), Kale (95/95), Tabya (96/96), Meters (97/97), Kara (98/98), Deniz (990/990) Gece (1/90), Gündüz (1/80), Sene (1/70), Ay (1/60), Gün (1/50), Saat (1/40), Vakit (1/30), Eyyam (1/20) Mevsim (1/10), Kış (2/20), Yaz (2/30), Bahar (2/40), Güz (2/50), Pazar (2/60), Pazartesi (2/70), Salı (2/80) Çarşamba (2/90), Perşembe (2/81), Cuma (2/91), Cumartesi (2/100), 1 (7), 2 (8), 3 (9), 4 (2), 5 (4), 6 (3), 7 (5), 8 (6), 9 (1) "

Daha sonra ise kesirli sayılara ilave olarak, sembol kodlamalar gösterilmişti.



Şekil 11. (COA. Hat 1016-42511-a)

Şayet bu miftahla ve kodlarla bir yazı kaleme alınırsa, ortaya görünümü karmakarışık ve çözülmesi oldukça zor kriptografik bir belge oluşmaktaydı. 2. mektubu ise Yusuf Paşa Biraderi Abdi Bey'e göndermişti. Burada da bir başka şifre miftahı gösterilmişti.



Şekil 12. (Biraderi Abdi Bey'e) Yusuf Paşa Şifre Miftahı

Bu miftahı incelediğimizde Yusuf Paşa'nın Kriptografi konusunda oldukça geniş bilgiye sahip olduğunu görüyoruz ve Osmanlıların belki de en önemli Kriptografi olduğunu düşünmekteyiz. Bunu şöylece Şifre Miftahını inceleyerek açıklayalım.

Düz Alfabe; ا ب ت ث ج ح خ د ذ ر ز س ش ص ض ط ظ ع غ ف ق ك ل م ن و ه لا ى

Şekil 13.

Düz alfabenin İlk 7 harfini oluşturan 1. grup, د harfiyle başlayıp ص ile biten, sekiz harf kaydırılarak (ötelenmiş) şifrelenmişti.

Şekil 14.

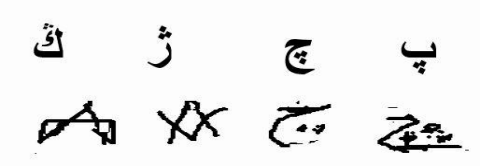
Düz alfabenin ikinci 7 harfli grubu ve 8. harf د ise düz kaydırma yapılsaydı ذ şifrelenmesi gerekirken, "Sıra Değiştirme" de uygulanarak, düz alfabenin 15. harfi ك **ile** başlatılarak د harfi şifrelenmiş, ikinci grubun son harfi olan ص harfi ise ى ile şifrelenmiştir.

Şekil 15.

Düz alfabenin üçüncü 7 harfli grubu 15. harf olan ض düz alfabenin başına dönerek 1. harf ا harfiyle başlayarak, üçüncü 7 harfli grubun son harfi olan ق ise düz alfabenin 7. harfi olan خ ile şifrelenmiştir.

Şekil 16.

Düz alfabenin sonuncu ve dördüncü grubu 8 harfli kabul edilmiş ve aradaki (lamelif) لا bir sembolle gösterilmiştir. Bunun dışında düz alfabemizin geriye kalan ve ك ile başlayan kısmı ise ك harfi ض ile şifrelenirken, son harf olan ى ise ق harfiyle şifrelenmiştir. Temel Arap Alfabesi bu şekilde şifrelenirken, Osmanlı Alfabesini oluşturan diğer unsurlar sembollerle şifrelenmiştir. Şöyle ki;



Şekil 17.

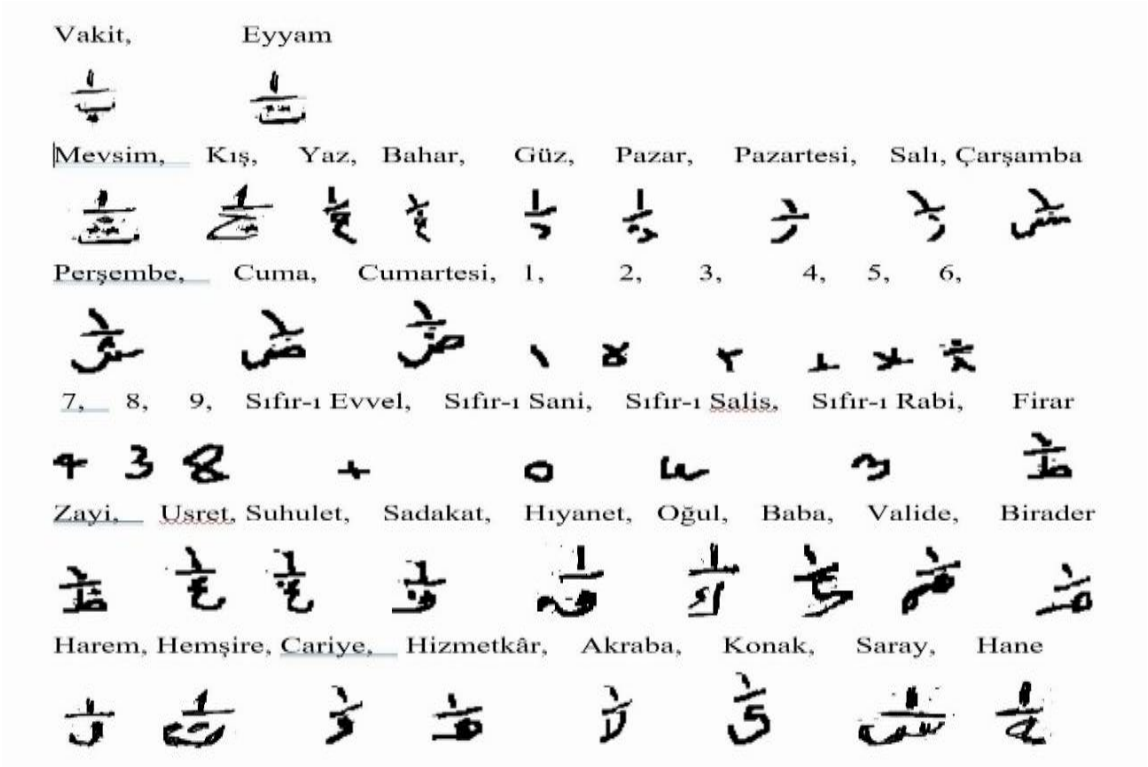
Yusuf Paşa'nın anahtarını incelediğimizde yukarda izah ettiğimiz Sezar şifresi denilen basit bir "Tek Alfabeli Yerine Koyma" şifresini yöntemini uygulamıştı. "Sezar Şifrelemesi" alfabedeki her bir harfin belli sayıda ileriye kaydırılmasına (ötelenmesine) dayanmaktaydı. Ancak bu kaydırılması (öteleme) işlemini aynı zamanda "Sıra Değiştirme" yöntemi ile kullanarak çözümü zor bir anagram oluşturmuştu. Bu onun döneminde gerek hariciyemizin ve gerekse dâhili haberleşmede genel olarak kullanılan basit düzeydeki "Tek Alfabeli Yerine Koyma (ikâme)" şifrelerinden farklılaşmıştı. Çözümlenmesi çok daha zordu. Yusuf Paşa ilave tedbirler de almıştı ve bu mektupta da birçok kod[13] verilmişti ve bunların bir kısmı numerikti (Varol, 2021, s. 276-278). Sayın M. Varol'un, bir Osmanlı Paşa'sının zihniyet dünyasını göstermesi ve bu kodlara dair kıymetli değerlendirmeleri için bakınız (Varol, 2021, s. 170-171). Bunlar şöylecedir.

> "Şer-i şerif (Asr), Şeriat-ı Mutahhara (At), Kanun (Nu), Âdet (Lâ), Padişah (10/9), Devlet-i Aliyye (10/8), Sadaret-i Uzma (10/7) Sadrazam (10/6), Şeyhülislam (10/5), Mehmed Ali Paşa (10/4),İslambol Kaymakamı Paşa (10/3), Rikâb-ı Hümayun Kaymakamı Paşa (10/2) Hüsrev Paşa (10/1), Asakir-i Mansure Seraskeri (10/0), Ordu-yu Hümayun Seraskeri (20/9), Tuna Sevahili Seraskeri (20/8) Erzurum Canibi Seraskeri (20/7), Rikâb-ı Hümayun Seraskeri (20/6),Vidin Kolu Seraskeri (20/5), Rumeli Seraskeri (20/4) Mora Seraskeri (20/3), Serasker (20/2), Asakir-i Mansure Seraskeri (20/1), Vezir (20/0), Vüzerat (30/9) El-hac İbrahim Paşa (30/8), Hüseyin Paşa (30/7), Halil Paşa (30/6), Reşid Paşa (30/5), Galib Paşa (30/4) Rauf Paşa (30/3), Ömer Melyon Paşa (30/2), Senegalli İbrahim Paşa (30/1), Aliş Paşa (30/0), Celal Paşa (40/9) Esad Paşa (40/8), Derviş Paşa (40/7), Köse Mehmed Paşa (40/6), Hacı Mustafa Paşa (40/5), Palaslı İsmail Paşa (40/4) Kapudan Paşa (40/3), Sadr-ı Esbak Silahdar Ali Paşa (40/2), Salih Paşa (40/1), İşkodralı Mustafa Paşa (40/0), Namık Ali Paşa (50/9), Kavanozzade Hüseyin Paşa (50/8), Hafız Ali Paşa (50/7), Kara Süleyman Paşa Der Girit (50/6) İzmirli Hasan Paşa (50/5), Kethüda-yı Sadr-ı Ali (50/4), Reis Efendi (50/3), Defterdar Efendi (50/2), Çavuşbaşı (50/1) Tersane Emini (50/0), Darbhane Emini (60/9), Mukataat Nazırı (60/8), Asakir-i Mansure Nazırı (60/7) Hüsnü Bey (60/6), Pertev Efendi (60/5), Ata Efendi (60/4), Hekimbaşı Efendi (60/3), Necib Efendi (60/2) Silahdar-ı Şehriyari (60/1), Sır Kâtibi Efendi (60/0), Başçukadar Bekir Ağa (70/9), Hazine-i Hümayun Kethüdası Emin Ağa (70/8) Darüssaade Ağası (70/7), Hazinedar Ağa (70/6), Büyük Mirahur Ağa (70/5), Küçük Mirahur Ağa (70/4), Bostancıbaşı (70/3) Hünkâr Kapıcılar Kethüdası (70/2), Paşa (70/1), Mir-i Miran (70/0), Bey (80/9), Efendi (80/8), Ağa (80/7), Âdem (80/6) Kethüda (80/5), Hazinedar (80/4),

[13] Sayın M. Varol, Miftah yani şifre anahtarını vermeksizin Abdi Bey'e gönderilen mektuptaki Kodları "Şifre Anahtarı" başlığıyla vermiştir. Kriptografi hakkında muhtemelen az ilgisi nedeniyle, hatalı olarak "Şifre anahtarı" şeklinde vermiştir. Yine "Ekler" bölümünde gösterim zorluğundan olsa gerek, bazı sayıların karşılığı olan sembol kodlamalarını verememiştir.

Divan Kâtibi (80/3), Silahdar (80/2), İç çukadar (80/1), Mühürdar 80/0) Kaftan Ağası (90/9), Kapıcılar Kethüdası (90/8), Divan (90/7), Kâtib (90/6), Yazıcı (90/5), Tatar (90/4) Hatt-ı Hümayun (90/2), Ferman (90/1), Buyruldu (90/0), Kaime (1/1), Mektub (1/2), Tezkire (1/3, Kağıd (1/4) Menzil (1/5), Posta (1/6), Süvari (1/7), Piyade (1/8), Asakir-i Mansure (1/9), Ulufeli Asker (1/10) Nefîr-i âmm askeri (1/11), Yeniçeri (1/12), Muharebe (1/13), Musalaha (1/14), Meclis-i Şura (1/15), Meşveret (1/16), Mukaleme (1/17), Müzakere (1/18), Murahhas (1/19), Elçi (1/20), Evvel (1/21), Ahir (1/22), Sani (1/23), Muhabere (1/24), Mekatibe (1/25) Rical-i Devlet (1/26), Ulema (1/27), Mütesellim (1/28),Voyvoda (1/29), A'yân(1/30), Mansıb (1/31), Azl (1/32) Nasb (1/33), Tevcih (1/34), Tevcihat (1/35), Nefy (1/36), İdam (1/37), Müsadere (1/38), Zabt (1/39), İhsan (1/40) Vali (1/41), Vilayet (1/42), Eyalet (1/43), Sancak (1/44), Kaza (1/45), Kasaba (1/46), Köy (1/47), Çiftlik (1/48), Malikane (1/49), İslambol (1/50), Edirne (1/51), Selanik (1/52), Yenişehir (1/53), Mora (1/54), Badra (1/55), Kestel (1/56), Matuf (1/57) Koron(1/58), Yanya (1/59), Preveze (1/60), Narda (1/61), İşkodra (1/62), Mısır (1/63), İskenderiye (1/64), Şam (1/65) Haleb (1/66), İzmir (1/67), Kütahya (1/68), Gelibolu (1/69), Siroz (1/70), Vidin (1/71), Şumnu (1/72), Ruscuk (1/73) Silistre (1/74), Varna (1/75), Ahyolu (1/76), İneada (1/77), Aydos (1/78), Misivri (1/79), Derviş Yovan (1/80) Köprü Köyü (1/81), Cenke (1/82), Kazgan (1/83), Çalık Kavak (1/84), Şıbka (1/85), Cengane Derbendi (1/86), Hacıoğlu Pazarcığı (1/87) Kavarna (1/88), Balçık (1/89), Tolçı (1/90), İsakçı (1/91), Babadağı (1/92), Hocabey (1/93), Kırım (1/94) Petesburg (1/95), Beç (1/96), Belgrad (1/97), Eflak (1/98), Boğdan (1/99), Rumeli (100), Anadolu (99/1) Erzurum Canibi (98/1), Bahr-i Sefid (97/1), Bahr-i Siyah (96/1), Bahr-i Sefid Boğazı (95/1), Bahr-i Siyah Boğazı (94/1) Nehr-i Tuna (93/1), Nehri-i Kamçı (92/1), Donanma-i Hümayun (91/1), Donanma (90/1), Üç Anbarlı (89/2), Kaynak(88/2), Fırkateyn (87/2) Brik (86/2), Galib (85/2), Mağlub (84/2), Mansur (83/2), Makhur (82/2), Sağ (81/2), Hasta (80/2), Mecruh (79/3) Vefat (78/3), Halas (77/3), Esir (76/3), Habs (75/3), Necat (74/3), Selamet (73/3), Sabık (72/3), Lahık (71/3) Sadık (70/3), Hain (69/4), Sahih (68/4), Kizb (67/4), Hilaf (66/4), Muhalif (65/4), Fesad (64/4), İhtilal (63/4) Asayiş (62/4), İstirahat (61/4), Haber (60/4), Havadis (59/5), Moskov (58/5), Nemçe (57/5), İngiliz (56/5), Fransız (55/5) Amerika (54/5), Sardunya (53/5), Rum Gavurları (52/5), Tercüman (51/5), Gizli (50/5), Aşikâr (49/6), Taife (48/6), Daire (47/6) Arnavud (46/6), Türk (45/6), Sirkat (44/6), Hafi (43/6), Mevcud (42/6), Akçe (41/6), Altun (40/6), Poliçe (39/7) Tebdil (38/7), Tahvil (37/7), Nakl (36/7), Hareket (35/7), Azimet (34/7), İkamet (33/7), Tertib (32/7), Tedarik (31/7) Sefer (30/7), Hazer (29/8), Tarik (28/8), Cisr (27/8), At (26/8), Bargir (25/8), Araba(24/8), Muhimmat (23/8) Top (22/8), Tüfenk (21/8), Kılıç (21/8), Kale (20/8), Tabya (19/9), Metris (18/9), Kara (17/9), Deniz (16/9) Gece (15/9), Gündüz (14/9), Sene (13/9), Ay (12/9), Gün (11/9), Saat (110/9)"

Bir kısım kelime için üretilen kodlar ise harf görünümlü sembollerdi.



Şekil 18. (COA. Hat-1016-42511- b)

Son olarak Yusuf Paşa tüm bu tedbirlere ilaveten gerek kendisinin gerektiğinde istediğini kullanacağı 2 ve gerekse talimatlarını beklediği makamdan gelecek şifreli yazıların güvenliğini artırmaya yönelik 2 olmak üzere, toplamda 4 adet imza oluşturmuştu. Görünen o ki kendini Varna Vakasında lekeleyen "hain" ithamını kaldırmak için çabalamaktadır. Ancak temsilci veya arabulucu çabaları muhtemelen sonuçsuz kalmıştır. Nitekim Tarihçi A. Lütfi'de bu çabasının sonuç vermediğini kaydeder (Lütfi, 1999, s. 351). Öte yandan bizde Osmanlı Arşivi'nde yaptığımız araştırmada gelen ve giden yazışmalarda bu miftahlar ve kodlarla kriptolanmış belgeye tesadüf edilmemiştir.

14 Eylül 1829'da imzalanan Osmanlı-Rus Antlaşması için Osmanlı delegeleri 28 Ağustos'ta Edirne'ye gittiler. Görüşmeler sırasında irtibat için Mehmed Sadık ile Anadolu Kazaskeri Abdülkadir Efendilere verilen şifre anahtarı numerik olup, Yusuf Paşa'nın Miftahlarıyla da bir ilgisi bulunmadığını da kaydedelim (COA. HAT 1047-43235;1050-43272-D).

Sonuç

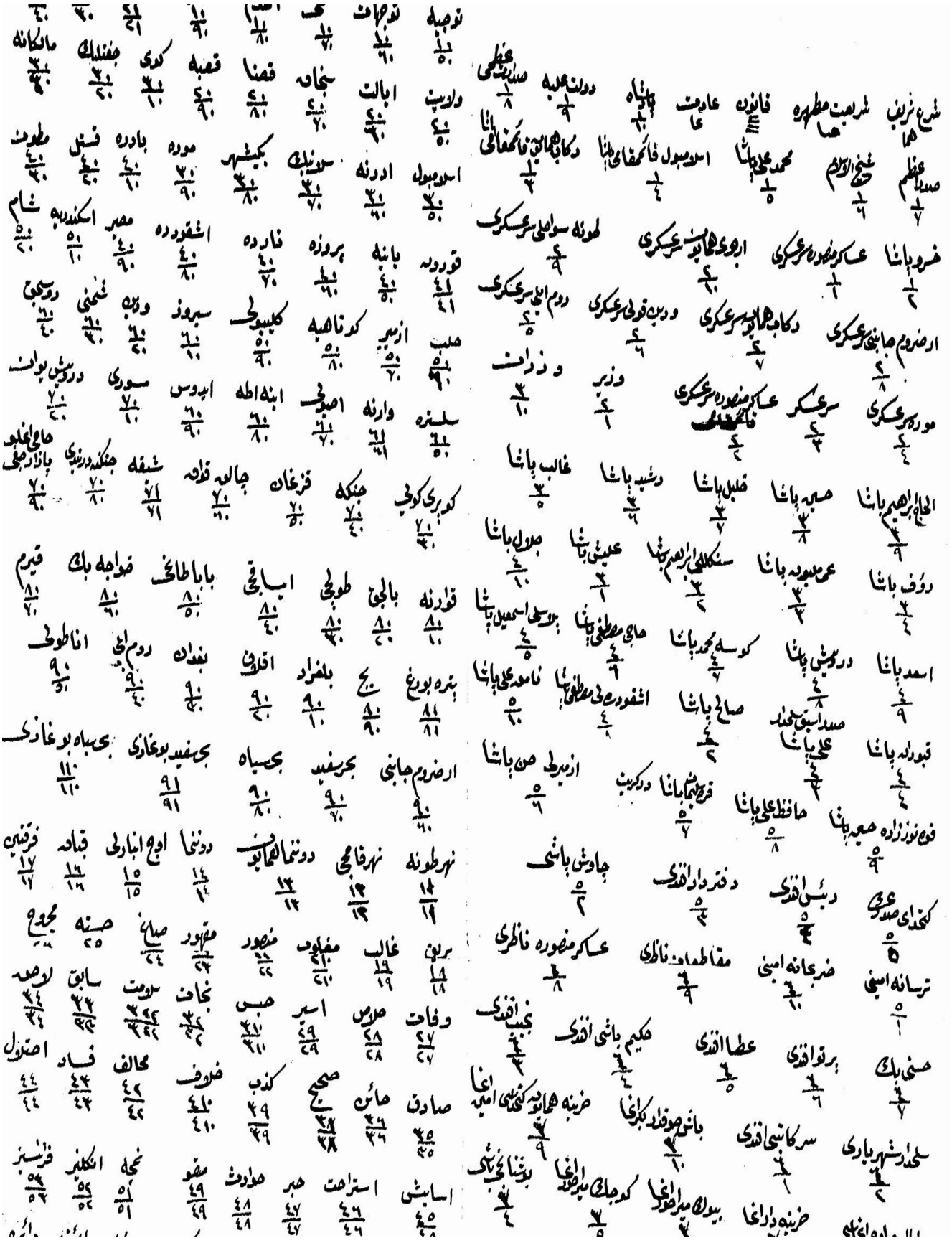
Osmanlı Devleti halk kültürü ve edebiyatında Kriptografi'nin semboller veya mecazi anlatımlar bakımından varlığından her zaman için söz edilebilirse de yönetim alanında 18.yüzyıla kadar herhangi bir girişim görülmez. III. Selimle döneminde Kriptografik

girişimler, Osmanlı Devleti'nin diplomasi alanındaki anlayış değişikliğinin getirdiği bir zorunluluk olarak karşımıza çıkar.

Kriptografi'nin başlangıç süreci, uygulamadan gelen deneyimlere dayalı olarak gelişmekteydi. Diplomatlara verilen şifre anahtarları, tek alfabeli (mono-alfabetik) bir "Yerine koyma (ikame) sifre" leriydi. Avrupa'nın bu alandaki gelişmeler ya da bir başka deyişle, kriptoanaliz ve polialfabetik konularındaki adımların izlenmediği anlaşılmaktadır. Yine sayısal şifrelerle birlikte kelime temelli, açık yazımlı kodların kullanımı, sonradan kodların da sayısallaştırılmasına dönüşmüşse de bu yavaş gelişme süreci bile 1811'den kesintiye uğramıştı. Diplomatik alanda Kriptograf'nin yeniden gelişebilme sürecinin başlayabilmesi için Osmanlı ikamet elçiliklerinin yeniden açılacağı 1830'lar sonrası beklenecektir.

Ancak iç bürokraside ise tespit edebildiğimiz kadarıyla 1815'lerden itibaren başlayan Kriptolu yazışmalar içeresinde dikkati çeken Sirozi Yusuf (Muhlis) Paşa'dır. Şifre algoritması üretme (Miftah) ve kodlamalar noktasında, kendinden önceki ve diyebiliriz ki kendisinden sonraki şifre hazırlayan kişilerden, ayrışarak seçkin bir şahsiyet olarak karşımıza çıkar. Kriptografi alanındaki kesirli sayılar, ya da Sezar şifresi vb. uygulamaları ile Türk Kriptoloji Tarihi'nde önemli bir yer tutmaktadır.

Ek



(COA. HAT 1016-42511-A)

Kaynakça

Akdeniz, R. (2000). Konuşma kodlama için yeni bir yaklaşım. *Trakya Üniversitesi Fen Bilimleri Dergisi*, *1*(1), 9-17.

Akleylek, S., Akyıldız, E. ve Çimen, C. (2011). *Şifrelerin matematiği: Kriptografi* (5. baskı). Ankara: ODTÜ Yayıncılık.

Algoritma. (t.b.). *Türk Dil Kurumu güncel Türkçe sözlük* içinde. http://sozluk.gov.tr/

Âşirefendizâde, M, Hafîd. (2018). *Ed-dürerü'l-müntehabati'l- mensure fi ıslahai'l-galatati'l-meşhure*. (Y. Yılmaz, Çev.). Ankara: Türk Dil Kurumu Yayınları. (Orijinal çalışma tarihi 1804).

Aydın, H. V. (2018). 1821 Yunan isyanı sırasında Selanik sancağı ve isyana karşı alınan önlemler. *Tarih İncelemeleri Dergisi*, *33*(2), 303-334.

Bayrak, M. (1999) *1821 Mora isyanı ve Yunanistan'ın bağımsızlığı* (Yayınlanmamış doktora tezi). Anadolu Üniversitesi, Eskişehir.

Bingöl, S. ve Pınar, H. (2021). Diplomatic immunity and encrypted diplomatic correspondence in the Ottoman Empire. *Tarih İncelemeleri Dergisi*, *36*(1), 1-19

Bingöl, S. (2021, 20 Mayıs). Methods for encryption in early 19th-century Ottoman diplomatic correspondence. *Cryptologia,* https://doi.org/10.1080/01611194.2021.1919943

Churchhouse, R. F. (2002). *Codes and ciphers; Julius Caesar, the Enigma, and the internet* New York: Cambridge University Press.

Cumhurbaşkanlığı Osmanlı Arşivleri (COA). HAT 800-37061; 1047-43235; 1050-43272-D; 1347-52652-E; 1347-52652-Ç; 252-14356; 237-13179; 1348-52711.; 1015-42494; 934-40441;1015-42494-A; 1070-43777-A; 1016-42511-A; 934-40441-A;934-40441-B; 934-40441 C; 986-41774; 125-5171;1145-45509 A;1206-47293-Ç; 400-21033-A; 400-21033-B; 1206-47293-F; 1145-45509 A;1206-47293-Ç; 400-21033-A; 400-21033-B; 1206-47293-F; 1432-58608; 1016-42511-B.

Çelebioğlu, A. (1988). Kültür ve edebiyatımızda şifre alfabeleri. *Tarih boyunca paleografya ve diplomatik semineri bildirileri* içinde (s. 19-33). İstanbul: İstanbul Üniversitesi Yayınevi.

Çeşmeci, M.Ü. (2009). Kriptoloji tarihi. *Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü Dergisi*, *1*(1), 22-30.

Decourdemanche, J. M. A. (1899). Note quatre systémes turcs de notation numérique secréte. *Journal Asiatique*, (14), 258-27.

Doğan, M. (2019). *Mehmet Emin Rauf Paşa (1780-1860)* (Yayınlanmamış doktora tezi). Hacettepe Üniversitesi, Ankara.

Dönmez, A. (2006). *Karşılıklı diplomasiye geçiş sürecinde Osmanlı daimî elçiliklerinin Avrupa'da yeniden tesisi 1832–1841* (Yayınlanmamış yüksek lisans tezi). Selçuk Üniversitesi, Konya.

Duran, N. (2019). *Sırbistan emareti öncesi Belgrad:1792-1830* (Yayınlanmamış doktora tezi). İstanbul Üniversitesi, İstanbul.

Düzcü, L. (2016). Tuna sınırını yeni baştan düzenlemek/tahdîd-i hudûd: Osmanlı'nın Rusya ile imtihanı (1812-1818). *İzzet Baysal Üniversitesi Sosyal Bilimler Enstitüsü Dergisi*, *16*(3), 181-210.

Egüz, E. (2010). Priştineli Begzâde Nûrî divanı ve divan'daki şifreli yazılar. *Selçuk Üniversitesi Türkiyat Araştırmaları Dergisi*, (27), 297-311.

İnal, İ. M. K. (1969). *Son Osmanlı şairleri c. II*. İstanbul: Millî Eğitim Bakanlığı Yayınları.

Kahn, D. (1973). *The codebreakers: The story of secret writing*. New York: The Macmillan Company.

Karabey, T. (2011). Tarih düşürme. *İslâm ansiklopedisi* içinde (Cilt 40, s. 80-82). İstanbul: Türkiye Diyanet Vakfı Yayınları

Kılıç, M. (2019). İlk ikamet elçilerinin halefleri Rum maslahatgüzarlar (1800-1821). *Ankara Üniversitesi Tarih Araştırmaları Dergis*i, *38*(65), 251-278.

Kındap, N. (2015, 12 Kasım). Kriptografi'de şifreleme teknikleri. https://www.linkedin.com/pulse/kriptografide %C5%9Fifreleme-teknikleri-nihal kindap.

Kodlama nedir? (t.b.). *Dersimiz Kodlama.* http://www.kodlamadersi.com/kodlama-nedir-cocuklar-icin-onemi.html

Köprülü, O. F. (1996). Galib Paşa, Mehmed Said. *İslam ansiklopedisi* içinde (Cilt 13, s. 329-331). İstanbul: Türkiye Diyanet Vakfı Yayınları.

Kriptografi, Sezar Şifresi ve Stenografi (t.b.). https://gurelahmet.com/kriptografisezar-%c5%9fifresi-ve-stenografi/

Kuran, E. (1988). *Avrupa'da Osmanlı ikamet elçiliklerinin kuruluşu ve ilk elçilerin siyasi faaliyetleri 1793-1821*. Ankara: Türk Kültürünü Araştırma Enstitüsü Yayınları.

Lunde, P. (2013). *Şifreler kitabı* (5. baskı). (D, Akın, Çev.). İstanbul: NTV Yayınları.

Lûtfî, A. (1999). *Vak'anüvîs Ahmed Lûtfî Efendi tarihi*. (Y. Demirel ve T. Erdoğan, Çev.). İstanbul: Tarih Vakfı-Yapı Kredi Yayınları. (Orijinal çalışma basım tarihi 1873).

Obaid, Z., Sabonchi, A. ve Akay, B. (2016). Klasik kriptoloji yöntemlerinin karşılaştırılması. *Engineering Sciences, 11*(4), 100-108.

Örenç, A. F. (2011). Yunanistan'ın bağımsızlığı sürecinde yok edilen Mora Türkleri. *Uluslararası Suçlar ve Tarih*, *11*(12), 5-32.

Örs, H. (1964). Topkapı Sarayı arşivinde bulunan şifreli iki vesika. *Belleten*, *28*(109), 85-92.

Serezli, M.E. (2012). *Memleket hatıraları c. II.* Ankara: Türk Tarih Kurumu Yayınları.

Singh, S. (2004). *Kod kitabı*. (C, Hamitoğulları ve E. Y. Sınır, Çev.). İstanbul: Klan Yayınları.

Süreyya, M. (1996). *Sicill-i osmani*, (N. Akbayar, Çev.). İstanbul: Tarih Vakfı Yurt Yayınları. (Orijinal çalışma basım tarihi 1893-1897).

Varol, M. (2021). *Beş nesil beş devir Sirozîler*. İstanbul: Timaş Akademi Yayınları.