https://dergipark.org.tr/tr/pub/igdirsosbilder

Iğdır Üniversitesi Sosyal Bilimler Dergisi

E-ISSN: 2147-6152

Yıl 14, Sayı 40, Ekim 2025

[Araştırma Makalesi] **Atıf/Citation**: Çil, S. (2025). "Caesar Şifrelemesinin Tarihsel ve Kriptografik Analizi", *Iğdır Üniversitesi Sosyal Bilimler Dergisi*. (40): s. 385-395. **Gönderim Tarihi**: 21.03.2025 **Kabul ve Yayın Tarihi**: 01.10.2025-15.10.2025 **DOI**: 10.54600/igdirsosbilder.1662852

Yazar/Author

Sait ÇİL*

Makale Adı/Article Name

Caesar Şifrelemesinin Tarihsel ve Kriptografik Analizi

Historical and Cryptographic Analysis of the Caesar Cipher

ÖZ

Antik çağlarda iletişim güvenliği için güvenli yollar, ulaklar için dinlenme noktaları ve posta teşkilatı gibi unsurlar gerekli olmuştur. Ancak tüm bu unsurların varlığı dahi çoğu zaman iletişim güvenliğini sağlamaya yetmemiştir. Dolayısıyla, iletişim güvenliği sorununu çözmek amacıyla antik çağlardan itibaren kriptografi kullanılan başlıca yöntemlerden biri olmuştur. Özellikle devletlerarası ilişkiler, askeri stratejiler ve diplomatik yazışmalar gibi kritik alanlarda bilgi güvenliğinin sağlanması hayati bir önem taşımıştır. Bu durum ise dönemin siyasi ve askeri liderlerini daha sofistike yöntemler geliştirmeye yöneltmiştir. Kriptografinin erken dönem örneklerinden biri sayılan ve Caesar'ın adıyla özdeşleşen ikame (yerine koyma) şifresi, literatürde Caesar şifrelemesi olarak bilinmektedir. Bu yöntemde, orijinal metin yerine şifreli bir metin konulmuş ve böylece asıl içerik gizli tutulmuştur. Caesar şifrelemesi, modern güvenli iletişim yöntemlerinin evriminde önemli bir kilometre taşı olarak kabul edilmekte ve aynı zamanda kriptografi literatüründe tarihsel bir dönüm noktasını temsil etmektedir. Bu çalışmada, antik edebi kaynaklar ve araştırma eserleri ışığında Caesar şifrelemesinin tarihsel gerçekliği incelenmiş, ayrıca bu yöntemin gelişimi ve modern kriptografi üzerindeki etkileri ele alınmıştır.

Anahtar Kelimeler: Kriptografi, Caesar şifrelemesi, Antik Roma, İletişim güvenliği.

ABSTRACT

In ancient times, secure roads, resting points for messengers and postal organisations were necessary to ensure the security of communication. However, the existence of all these elements alone has often been insuficient to ensure communication security. Therefore, cryptography has been one of the primary methods used since ancient times to solve the problem of communication security. Ensuring information security has been of vital importance, particularly in critical areas such as international relations, military strategies, and diplomatic correspondence. This situation has led the political and military leaders of the period to develop more sophisticated methods. The substitution cipher, regarded as one of the earliest examples of cryptography and associated with Caesar's name, is known in the literature as the Caesar cipher. In this method, an encrypted text is be placed in place of the original text, thus keeping the actual content hidden. The Caesar cipher is regarded as an important milestone in the evolution of modern secure communication methods and also represents a historical turning point in cryptography literature. In this study, the historical authenticity of Caesar ciphering has been examined in light of ancient literary sources and research works, and moreover, the development of this method and its effects on modern cryptography have also been discussed.

Keywords: Cryptography, Caesar cipher, Ancient Rome, Communication security.

* Arş. Gör., Bartın Üniversitesi, Edebiyat Fakültesi, Tarih Bölümü, scil@bartin.edu.tr,

Extended Abstract

The Caesar cipher is a simple substitution cipher based on the principle of shifting the letters of the alphabet by a fixed number of positions. In its most common form, the letters are shifted three positions to the right. For example, the letter A is replaced with D, and B is replaced with E (See Table 3). This method allows the encrypted text to be deciphered by shifting the letters the same number of positions in the opposite direction. Due to its ease of implementation and practicality under the communication conditions of the time, the Caesar cipher became widely used. This study aims to discuss the historical authenticity of Caesar cipher on the one hand, and on the other hand, examine the impact of this method on the discipline of cryptography and its reflections in subsequent periods.

During the historical analysis, the authenticity of the Caesar cipher was questioned in light of ancient sources, and whether this method was truly used by Gaius Iulius Caesar was critically discussed. A qualitative research method was adopted; primarily, Caesar's works *Bellum Gallicum* and *Bellum Civile* were examined to identify direct evidence of the use of encryption. In addition, the writings of ancient authors such as Suetonius, Cassius Dio, and Aulus Gellius, along with modern research literature, were analyzed. Various narratives in the sources suggest that Caesar wrote secret messages and used encryption when necessary. Particularly, examples of encryption used to prevent messages from falling into enemy hands during the Gallic Wars indicate that this method might have been applied in practice. Furthermore, the fact that later Roman leaders, such as Augustus, adopted similar encryption techniques shows that the Caesar cipher became a lasting element of communication security culture in Rome.

One of the main reasons for the lasting influence of the Caesar cipher is its simplicity and practical applicability compared to other ancient cryptographic techniques. Unlike more complex and error-prone methods such as Polybius' square or the use of fire signals requiring precise coordination, the Caesar cipher offered a straightforward and efficient approach to secure communication. Its ease of use, especially in military contexts where rapid and reliable message transmission was crucial, contributed to its widespread adoption. This operational advantage may explain why the Caesar cipher, despite its simplicity, has endured through centuries and inspired various modern encryption models. The ability to adapt its fundamental logic into new forms has ensured its continued relevance not only in historical studies but also in the conceptual foundations of contemporary cryptography. This foundational simplicity not only ensured its effectiveness in antiquity but also laid the groundwork for its influence on encryption practices in subsequent historical periods. The historical continuity of the Caesar cipher is not limited to antiquity; it also influenced encryption techniques developed in Europe from the Middle Ages onward. Innovative methods such as the Vigenère cipher and the cipher disk developed by Leon Battista Alberti have been regarded as advanced versions of substitution cipher systems like the Caesar cipher. During the world wars, the growing need for secure communication led to the resurgence of classical methods, including variations of the Caesar cipher. This historical trajectory demonstrates that the Caesar cipher has had a long-term impact in both theoretical and practical domains.

In the second stage of the study, during the cryptographic analysis, evaluations were made based on the works of modern cryptographers. Within this scope, cryptographic methods developed after the Caesar cipher were examined, and it was emphasized how this ancient technique inspired more complex cryptographic systems in the following centuries. Indeed, methods such as ROT13, FCC, and FP-cipher are derived from the fundamental structure of the Caesar cipher, and the development of these techniques demonstrates how the flexible nature of the Caesar cipher contributed to the evolution of modern security systems. Therefore, the Caesar cipher is not only a historical phenomenon but also regarded as a conceptual foundation in the field of cryptography. Today, it is frequently used as an introductory tool for those seeking to understand the basic principles of encryption. However, despite its historical importance, the Caesar cipher is considered highly vulnerable by modern standards, offering only a limited number of key variations and being easily deciphered through brute-force techniques.

Although doubts had persisted about the historical authenticity of the Caesar cipher in previous scholarship, the evidence presented here suggests that the technique was in all likelihood historically real. In our opinion, accounts of the capture of messengers, Caesar's own references to secret letters and reports in his works, and the fact that his adopted son, Augustus, adopted a similar encryption method, can be considered strong evidence that he used this technique and may even have invented it. In this context, the validity of the method in question has been debated within the study, and based on data obtained from ancient sources and research works, a strong conclusion has been reached that the Caesar cipher was indeed applied in its historical context. Thus, in line with the study's objective, the controversial issue of historical reality has been clarified with concrete evidence, and it has been concluded that the uncertainties regarding Caesar's cipher have been significantly resolved. The Caesar cipher, which largely clarifies uncertainties regarding

historical accuracy, is significant not only as an early example of cryptography but also as a concrete reflection of the need for secure communication in the ancient world.

Giriş

İletişim güvenliği modern döneme özgü bir çalışma alanı olmayıp, antik çağlardan itibaren birçok uygarlık gizli mesajları şifrelemek için çeşitli yöntemlere başvurmuştur (Diepenbroek, 2021a). Kriptografi, mesajların amaçlanan alıcı dışında herkes tarafından anlaşılamaz hâle getirilmesi için gizli kodlarla şifrelenmesi ve çözümlenmesi uygulamasıdır. Şifreleme pratiği, mesajların yetkisiz kişilere karşı korunmasını sağlamak üzere içeriklerinin dönüştürülmesine dayanan temel bir teknik olup (Singh, 2003: 2), en erken örnekleri antik döneme kadar dayanmaktadır. Antik çağlarda bir uygarlık belli bir gelişim gösterdikten sonra okuryazarlık oranının artmasıyla birlikte kriptografi örnekleri belirmeye başlamıştır. Sosyal yaşamın içerisinde mahremiyetin talep edilmesi her zaman insani ihtiyaçlardan biri olmuştur. Bu ihtiyaç kaçınılmaz olarak kriptografinin kullanımına yol açmıştır (Kahn, 1996: 73). Tarih, kriptografi kullanımına dair oldukça zengin örnekler sunmaktadır. En çarpıcı örneklerden biri, ulakların tıraş edilmiş kafalarına mesajın dövme olarak işlenmiş ve ardından saçların uzamasının beklenmiş olmasıdır (Andress, 2014: 70-71).

Eski Yunan şifreleme yöntemlerine dair kaynaklarımızdan birisi MÖ 2. yüzyılda yaşamış olan tarihçi Polybios'tur. Polybios'un aktardığı üzere, Yunan yazar Aineias Taktikos MÖ 4. Yüzyılda geliştirdiği haberleşme sistemiyle ateş sinyalleri kullanarak önceden belirlenmiş mesajları iletmeye çalışmıştır Polyb. X.43-44) Bu yöntem, su saatleri ve meşaleler kullanarak ateşle işaretleşmeye yönelik zahmetli bir uğraş gerektirmiştir. Dolayısıyla hem zahmeti hem de hata payı yüksek olduğu için kullanım alanı sınırlı kalmıştır (Diepenbroek, 2019: 64). Polybios'un tanıttığı şifreleme yöntemlerinden bir diğeri, modern kriptograflar tarafından "Polybios Karesi" olarak bilinmektedir (Bkz. Tablo 1 ve 2). Polybios bu şifrelemeyi kendisinin mükemmelleştirdiğini söylemiştir. Bu yöntemde alfabe her biri beş harften oluşan beş bölüme ayrılmıştır (Polyb. X.45). Alfabenin beş satır ve beş sütuna ayrılması sonucunda 25 harfin sadece beş sayıya karşılık geldiği bir şifreleme yöntemi ortaya çıkmıştır. (Reinke, 1962: 115; Kahn, 1996: 76-77; 82-83; Dieponbroek, 2019: 68-69). Bir harfin sayı karşılığını belirlemek için, satırdaki rakam birinci, sütundaki rakam ise ikinci sayıyı oluşturmaktadır (Macit vd., 2019: 236). Polybios karesi kullanarak şifrelenen örnek bir cümle:

"DESTEK BİRLİK YOLDA" = 14 15 43 44 25 – 12 24 42 31 24 25 – 54 34 31 14 11

Tablo 1: Yunan harflerinden oluşan bir Polybios karesi.

	1	**2**	**3**	**4**	**5**
1	Α	Β	Γ	Δ	Ε
2	Ζ	Η	Θ	Ι	Κ
3	Λ	Μ	Ν	Ξ	Ο
4	Π	Ρ	Σ	Τ	Υ
5	Φ	Χ	Ψ	Ω	

Tablo 2: Modern Latin harflerinden oluşan bir Polybios karesi.

	1	**2**	**3**	**4**	**5**
1	A	B	C	D	E
2	F	G	H	I/J	K
3	L	M	N	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z

Eski Yunanlar tarafından kullanılan diğer bir şifreleme yöntemi, *skytale* yani sarmal şifreleme olmuştur. Bu yöntemde, ahşap ya da metal bir çubuk etrafına şerit halinde sarılan deri veya parşömen üzerine yazılmış mesajlar, yalnızca aynı çapta bir çubuğa sarıldığında okunabilmiştir. Bu sistem, askerî ve diplomatik haberleşmede gizliliği sağlamak amacıyla kullanılmıştır (Bruen ve Forcinito, 2011: 20; Diepenbroke, 2021b: 45-46). Antikçağda uygulanan şifreleme yöntemleri, bunlarla sınırlı kalmamış hem işlev hem de kullanım bağlamı bakımından çeşitlilik göstermiştir. Örneğin, Yunanca belgelerde görülen izopsefik sisteme dayalı yöntem, bir harfin kendisinden daha yüksek basamaktaki izopsefik farkı temsil eden başka bir harfle değiştirilmesine dayanmakta ve çoğu zaman gizlilikten ziyade okuyucunun dikkatini çekmek amacıyla kullanılmaktaydı. Buna karşın, Londra ve Leiden'de korunan bir büyü papirüsünde tespit edilen özel sembollerle oluşturulmuş kod, ilaç yapımında kullanılan maddelerin adlarını gizlemek üzere geliştirilmiş gerçek bir şifreleme sistemi olarak kullanılmıştır. Son olarak, Medinet Madi'de ele geçen ve MS 2. yüzyıla tarihlenen ostrakonlarda, Yunanca kelimeler ile özel isimlerin sayılar aracılığıyla yazıldığı bir başka sistem saptanmıştır. Bu sistem, kimi zaman astrolojik bağlamlarla ilişkilendirilmiş, kimi zamansa katiplerin özel bilgileri gizleme arzusu veya basit yazınsal alıştırmalarla bağlantılı olduğu ileri sürülmüştür (Menchetti, 2005: 237-240).

Eski Yunanlar ve diğer uygarlıkların geliştirmiş olduğu şifreleme teknikleri, Romalıların da ilgisini çekmiştir. Yunan etkisiyle geliştirilmiş bu tekniklere özellikle askerî ve diplomatik iletişim açısından önem atfetmiş olmalarının en iyi örneğini, bu makalenin konusunu oluşturan Caesar şifrelemesi teşkil etmiştir. Caesar şifrelemesinin incelenmesi bu bakımdan önem arz etmiştir. Antik Roma'da güvenli haberleşme pratiklerinin anlaşılması ve kriptografi tarihindeki yerinin belirlenmesi açısından iyi bir örnek teşkil eden Caesar şifrelemesi, modern kriptografi çalışmalarını da etkilemiştir. Nitekim antik dünyada iletişim güvenliğinin sağlanması, devletler için olduğu kadar ordular ve diplomatik temsilciler için de kritik bir mesele olmuştur. Güvenli yollar, ulaklar için dinlenme noktaları ve posta teşkilatı gibi unsurlar iletişim ağını desteklemiş olsa da bilgi güvenliği esasen içeriğin korunmasına bağlı kalmıştır. Bu bağlamda Caesar şifrelemesi tarihsel olarak öne çıkan erken örneklerden biri olmakla birlikte, söz konusu şifrelemenin gerçekliği ve uygulanma biçimleri belirsizliğini korumuştur. Fikrimizce bu belirsizliğin günümüzde yeniden incelenmesi, hem tarihsel bir sorunsalın açıklığa kavuşturulması hem de kriptografi alanındaki evrimsel sürecin anlaşılması açısından önem arz etmektedir. Bu çalışma, bir yandan Caesar şifrelemesinin tarihsel gerçekliğini tartışmaya açmış, diğer yandan bu yöntemin kriptografi disiplinine olan etkilerini ve sonraki dönemlere yansımalarını ele almayı amaçlamıştır.

1. Gaius Iulius Caesar ve Şifrelemesi

Bu makalenin konusunu oluşturan şifrelemenin isim babası olan Gaius Iulius Caesar (MÖ 100-44), Roma Cumhuriyeti'nin en önemli siyasi ve askeri liderlerinden biridir. Genç yaşta siyasete atılan Caesar, MÖ 60'ta Pompeius ve Crassus ile Birinci Triumvirliği kurarak Roma siyasetinde güç kazanmıştır. MÖ 58-50 arasında yaptığı Galya Savaşları'nı yürüterek Roma topraklarını genişletmiş ve büyük bir askeri deha olarak ün elde etmiştir. Caesar, *"De Bello Gallico"* (Galya Savaşları) başlığıyla kitaplaştırmış olduğu bu savaşları MÖ 49'da sonlandırmış ve aynı yıl Rubicon Nehri'ni geçerek bir iç savaş başlatmış, kısa sürede Roma'nın mutlak hâkimi olmuştur. Ayrıca, başlatmış olduğu iç savaşı anlatan *"Bellum Civile"* başlıklı bir eser daha kaleme almıştır (*OCD*, 1999: 780-782). MÖ 44'te senatörler tarafından öldürülene kadar diktatör olarak Roma'yı yönetmiştir (Plut. *Caes*. 57). Marcus Lepidus'un evinde nasıl bir ölüm istediklerine dair yaptıkları konuşmada ani ve beklenmedik bir ölüm arzuladığını söyleyen Caesar'ın ölümü istediği gibi olmuştur (Suet. *Iul*. 77). Nitekim, senatörler tarafından beklemediği bir anda birçok yerinden bıçaklanarak öldürülmüştür (Suet. *Iul*. 72; Plut. *Caes*. 66). Caesar hırslı birisi olduğu kadar aynı zamanda cömert ve halkın sevgisini kazanmaya odaklı bir lider olmuştur. Düzenlediği oyunlar ve yaptığı yardımlar bu yanını kanıtlamaktadır (Suet. *Iul*. 38-39). Karizmatik bir lider olarak halkın sevdiği bir figür olan Caesar, herkesi mutlu etmeye çalışmıştır (Plut. *Caes*. 58). Ölümü sonrasında halk onun katillerine büyük öfke beslemiştir (Plut. *Caes*. 68). Öte yandan, Caesar'ın MÖ 49 yılındaki askerî darbesiyle başlamış olan İç Savaş ve sonrasındaki siyasi eylemleri, cumhuriyet

rejimini zayıflatmıştır. Daha sonra Caesar'ın uğramış olduğu suikast, Roma'yı derinden etkilemiş ve cumhuriyetin sonu ile imparatorluk döneminin başlangıç sürecini tetiklemiştir (Kaya, 2017: 822).

Eskiçağın klasik kriptografi örneklerinden biri olan Caesar şifrelemesi, Iulius Caesar tarafından kullanılmış veya geliştirilmiş olduğu iddia edilmiştir. Reinke'ye göre Caesar, bu yöntemi gerçekten kendisi geliştirmiş olsa bile, bunu Yunanlılardan bağımsız olarak yapmıştır (Reinke, 1962: 115). Bu yöntemde alfabedeki harflerin belirli sayıda kaydırılması sonucunda şifreli bir metin ortaya çıkmaktadır. Şifreli metnin şifresi, aynı sayıda harfin ters yöne kaydırılması sonucunda çözülebilmektedir (Andress, 2014: 71). Bu tür şifreleme yöntemi ikame şifresi veya yerine koyma şifrelemesi olarak bilinmektedir. Caesar şifrelemesinde alfabenin ilk harfi olan A, üç sıra kaydırılarak D harfiyle eşleştirilmiş ve aynı düzen tüm harfler için uygulanmaya devam etmiştir (Bkz. Tablo 3). Suetonius'un aktardığına göre Caesar bu yöntemi kullanmış ve şifreleme yöntemini bilmeyenler için anlamsız yazılar ortaya çıkarmıştır (Suet. *Iul.* 56). Bu yöntemin basitliği ve uygulama kolaylığı sebebiyle farklı versiyonlar zamanla ortaya çıkmıştır. Buna rağmen bu tür ikame şifrelerin hepsi Caesar şifrelemesi olarak adlandırılmaktadır (Singh, 2003; 2). Bu yüzden Iulius Caesar, kriptolojiye adını kalıcı olarak yazdırmıştır (Kahn, 1996; 73). Caesar şifrelemesi, teknik açıdan basitliği nedeniyle kriptografi tarihinde yüksek bir matematiksel derinlik sunmamış olsa da antik dünyada şifreli iletişime dair en görünür ve etkili örneklerden biri olmuştur. Bu durum, yöntemin kendisinden ziyade tarihsel bağlamının ve onunla özdeşleşmiş lider figürünün, kriptoloji literatüründe kalıcı bir simge hâline gelmesine imkân tanımıştır. Polybios karesindeki örnek cümlenin Caesar şifrelemesine göre şifrelenmiş hali:

"DESTEK BİRLİK YOLDA" = GHVWHN ELUOLN BROGD

Tablo 3: Caesar şifrelemesinin Latin alfabesindeki karşılığı.

Alfabe	A	B	C	D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T	V	X	Y	Z
Şifre	D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T	V	X	Y	Z	A	B	C

2. Caesar Şifrelemesinin Tarihsel Gerçekliği

Modern kriptoloji literatüründe Caesar şifrelemesinin mucidi olarak Iulius Caesar kabul edilmiş olsa da, ona atfedilen gizli mesajların hiçbiri günümüze ulaşmamış ve Caesar'ın kaleme almış olduğu *Bellum Gallicum* ile *Bellum Civile* adlı eserlerinde de bu şifrelemeden açıkça söz edilmemiştir. Bu nedenle, bu yöntemin Caesar tarafından kullanılmış olduğuna dair iddialar Aulus Gellius, Cassius Dio ve Suetonius gibi antik yazarlar tarafından aktarılmıştır. Cassius Dio, Caesar'ın birine gizli bir mesaj göndereceği zaman bu şifreleme yöntemini kullandığından bahsetmiştir (Dio Cass. 40.9). Suetonius, Caesar'ın generali Quintus Cicero'ya[1] ve yakınlarına özel konular hakkında yazdığı mektuplar olduğunu söyler ve önemli meseleleden bahsedecekse şifreleme kullandığını aktarmıştır (Suet. *Iul*. 56). Nitekim Caesar, Galya Savaşı eserinde Quintus Cicero'nun Galyalılar tarafından kuşatıldığında ona yardım göndereceğini bildirmek için bir mektup yazdığından bahsetmiştir. Caesar, eserinde mektubun kuşatma altındaki Quintus Cicero'ya ulaşamaması halinde Galyalıların anlamaması için Yunanca harflerle yazıldığını belirtmiş (Caes. *BG* 5.48), Cassius Dio ise bu mektubun Yunanca kaleme alındığını ve şifreleme yönteminin kullanıldığını aktarmıştır (Dio. Cass. 40.9). Harris'e (1991: 182, dn. 39) göre Caesar'ın bu hareketinin sebebi, Galyalıların Yunanca bilmediğini varsaymasıdır. Fikrimizce, Caesar'ın mesajını şifrelemek için sadece Yunanca yazılmış bir mektupla yetinecek olması, yetersiz bir yorumu gibi görünmektedir. Çünkü Caesar Galyalılardan bazılarının Yunan dilini ve yazısını bildiğinden haberdardı (Caes. *BG* 6.14). Nitekim, bu görüşü destekleyen bir anlatım Diepenbroke tarafından kaleme alınmıştır. Diepenbroke, Caesar'ın, Galya Savaşı eserinde bahsettiği gibi aslen Latince yazılmış bir mesajı Yunan karakterlerine ya da harflerine çevirdiğini varsaymıştır. Dolayısıyla, Caesar'ın Cicero'ya yazdığı gizli mektup büyük olasılıkla Yunanca

[1] Quintus Cicero, Roma'nın ünlü hatip ve siyasetçisi olan Marcus Tullius Cicero'nun küçük kardeşidir (*OCD,* 1999: 1564).

yazılmış ve daha sonra Yunanca bir ikame şifresiyle şifrelenmiş bir mektuptu. Diepenbroke, bu anlatıyı Caesar'ın kendi şifresinin sahada kullanıldığına dair üstü kapalı bir açıklama olarak kabul edilebileceğini savunmuştur (Diepenbroke, 2021a). Diepenbroek'in tezini destekleyen bazı örnekler antik kaynaklarda da görülmektedir. Caesar, Galya Savaşı'nda Galyalıların zaman zaman ulaklarını yakaladığını (Caes. *BG* 5.45) ve Quintus Cicero'nun kendisine gönderdiği en az bir mektubun ele geçirildiğini aktarmıştır (Caes. *BG* 5.39). Dolayısıyla bu anlatımlar Caesar şifrelemesinin kullanılmış olabileceği gerçeğini güçlendirmektedir.

Aulus Gellius, Caesar'ın yokluğunda işlerini yürüten Gaius Oppius ve Cornelius Balbus'a hitaben yazdığı şifrelenmiş mektuplardan bahsetmiştir (Gell. 17.9). Suetonius, şifrelemenin Caesar'dan sonra kullandığına dair bilgiler vermiş ve Caesar'ın soyundan gelen ve Roma'nın ilk imparatoru olan Augustus'un bu şifreleme yöntemini kullandığını söylemiştir. Fakat Augustus bu yöntemi kendine göre değiştirerek farklı bir ikame şifreleme tekniğini benimsemiştir. Yazmak istediği harf yerine kendisinden sonra gelen harfi kullanmıştır. Örneğin, A yerine B, B yerine C harfini yazılmış, Z harfi ise AA ile şifrelenmiştir (Suet. *Aug*. 88.). Tüm bu örnekler, Caesar'ın bir şifreleme yöntemi kullanmış olduğuna dair görüşü güçlendirmektedir. Bu anlatılar, Caesar'ın yalnızca haberleşme pratiklerinde gizlilik arayışına işaret etmekle kalmayıp, aynı zamanda antikçağda kriptografinin pratik bir ihtiyaç olarak benimsendiğini göstermesi bakımından da önem taşımaktadır.

Reinke, Caesar'ın üç harf kaydırmaya dayalı ikame şifrelemesinin yanı sıra başka yöntemler de kullanmış olabileceğini iddia etmiştir (Reinke, 1962: 114). Caesar'ın kendi şifreleme yöntemini gerçekten kullanıp kullanmadığı gibi, başka yöntemler veya farklı ikame şifrelemelerden yararlanıp yararlanmadığı da kesin değildir. Buna rağmen Caesar şifrelemesi, basitliği ve farklı versiyonlarının bulunması sayesinde varlığını günümüze kadar koruyabilmiştir. Bu yöntem, kriptografi alanındaki çalışmaları etkilemekle kalmamış, aynı zamanda kriptografların öğrendikleri ilk tekniklerden biri hâline gelmiştir. Günümüzde ise basit bir aramayla Caesar şifrelemesini uygulamaya imkân veren çok sayıda internet sitesine ulaşılabilmektedir.

Sonuç olarak Caesar'ın bu şifreleme yöntemini gerçekten kullanıp kullanmadığını, kaç adet gizli mektup bulunduğunu ve bunların kimlere gönderildiğini ortaya koyabilecek şifreli mesaj örnekleri günümüze ulaşmamış olmakla birlikte, onun kendi eserlerinde çok sayıda gizli mesaj ve raporun varlığına dair dolaylı kanıtlar bulunabilmektedir. Suetonius, Cassius Dio ve Aulus Gellius gibi yazarların da şifreleme ve gizli mesajlara dair yaptıkları atıflar, Caesar'ın gerekli durumlarda şifreli mesajlar yazmış olabileceği yönündeki argümanı güçlendirmektedir. Bununla birlikte, Caesar'ın kendi eserlerinde ulakların ve mesajların düşmanlar tarafından ele geçirilmiş olduğundan söz etmesi ve Augustus'un benzer bir şifreleme yöntemini kullanmış olması gibi kanıtlar göz önünde bulundurulduğunda, onun bu tekniği hem bulmuş hem de uygulamış olabileceği güçlü bir olasılık olarak öne çıkmaktadır. Dolayısıyla ulaşılan bulgular neticesinde, Caesar şifrelemesinin tarihsel gerçekliği etrafında süregelen tartışmaların belirli kanıtlarla desteklenebileceği gösterilmiş ve yöntemin antikçağda gerçekten kullanılmış olabileceğine dair kayda değer bir çıkarım ortaya konulmuştur.

3. Caesar Şifrelemesinin Modern Kriptografiye Etkisi

Kriptografiye dair çalışmalar günümüze kadar hız kesmeden sürdürülmüştür. 1464 yılında Leon Battista Alberti tarafından icat edilen şifreleme diski (Kelly, 2025), Caesar şifrelemesi örneğinde görülen antik dönem kriptografi çalışmalarının sürdürülmüş olduğunun bir kanıtıdır. Alberti'nin iç içe geçmiş iki diskten oluşan tasarımı, tek alfabeli şifreleme yöntemlerinden çok alfabeli şifrelemelere geçişin ilk örneğini teşkil etmiştir (Babaoğlu, 2009: 26). Bir diğer erken dönem örneği Vigenère şifrelemesidir. 1553 yılında İtalyan kriptograf Giovan Battista Bellaso tarafından ortaya konan bu yöntem, çok alfabeli bir ikame şifrelemesidir. Bu yöntemde Caesar şifrelemesinin basit yapısından farklı olarak, her harf için farklı bir kaydırma değeri kullanılmaktadır. Bu özellik, şifreli metnin analizini ve çözümünü güçleştirmiştir. Bir anahtar kelime aracılığıyla harfleri farklı karşılıklarla değiştiren bu sistem, 1586 yılında benzer bir yöntem geliştiren Fransız kriptograf Blaise de Vigenère'e atfedilmiş ve yüzyıllar boyunca onun adıyla

anılmıştır (Bruen ve Forcinito, 2011: 21; Simmons, 2025). Vigenère'in ardından, telgrafın icadına kadar kriptoloji alanında önemli bir ilerleme yaşanmamıştır. Telgrafın kullanılmaya başlanmasıyla birlikte, gizli mesajların posta görevlileri tarafından açılıp okunması veya telgraf hatlarının dinlenmesi gibi riskler ortaya çıkmıştır. Bu durum hem yeni şifreleme sistemlerinin geliştirilmesini hem de bu sistemlerin kriptanalizine yönelik çalışmaların yoğunlaşmasını beraberinde getirmiştir (Babaoğlu, 2009: 26-27).

İletişim güvenliğinin sağlanması için devam eden güncel çalışmalar, eski şifreleme tekniklerden esinlenilerek güncellenmiş ve 20. yüzyılda da sürdürülmüştür. Bu yüzyılda hem insan hem de makinelerin kullanıldığı bu çalışmalarda, esin kaynağı olarak başvrulan eskiçağ şifreleme tekniklerinden biri Polybios Karesi olmuştur. Nitekim I. Dünya Savaşı'nda Alman ordusu tarafından kullanılan ADFGX ve ADFGVX şifreleme sistemlerinin temelini bu teknik oluşturmuştur (Diepenbroek, 2019: 69-71). Sonraki Dünya Savaşı'nın (II. Dünya Savaşı) yaşandığı dönem iletişim güvenliğinin belki de en çok arandığı dönem olmuştur. Bu süreçte savaşan tüm taraflar, farklı şifreleme teknikleri geliştirmeye yönelmişlerdir. Taraflardan biri olan Sovyetler, basit bir Caesar şifrelemesi kullanmışlardır (Kahn, 1996: 350). Almanlar ise bu ihtiyaçlarını karşılamak için bir adım öteye geçerek özel bir şifreleme makinesi geliştirmiştir (Bruen ve Forcinito, 2011: 22). Arthur Scherbius tarafından icat edilen Enigma adlı bu makine ordu birimleri, hava ve deniz kuvvetleri ve tren istasyonları gibi kurumlarda gizli mesajlaşma için kullanılmıştır (Singh, 2003: 4). Yaklaşık 10 kg ağırlığında olan ve görünüm olarak daktiloya benzeyen Enigma, rotorlu ve elektromekanik bir şifreleme cihazıydı (Kara, 2009: 29). Bu cihazın şifresinin çözülmesi ise savaşın seyrini belirleyici şekilde değiştirmiştir.

II. Dünya Savaşı'nın ardından kriptografi, bir bilim dalı olarak sistematik bir gelişim sürecine girmiştir. Claude Shannon'ın 1949 tarihli "Gizli Sistemlerin Haberleşme Teorisi" makalesi, modern simetrik şifreleme sistemlerinin temelini atmıştır. 1970'lerde IBM mühendisleri tarafından geliştirilen LUCIFER algoritması, bu ilkeler doğrultusunda tasarlanmış ve yapılan değişikliklerin ardından DES (Data Encryption Standard) adıyla 1976'da ABD'nin resmi şifreleme standardı haline gelmiştir. 1976'da Diffie ve Hellman, açık anahtarlı kriptografi kavramını tanıtarak kriptoloji tarihinde bir dönüm noktası yaratmıştır. Bu gelişmeleri takiben RSA algoritması geliştirilmiş ve güvenliği büyük sayıların çarpanlara ayrılması problemine dayandırmıştır. 1980'lerin sonlarında ise eliptik eğri kriptografisi gündeme gelmiş, başlangıçta şüpheyle karşılansa da zamanla güvenilirliği kanıtlanmıştır. 1990'larda DES'in güvenliği zayıflmış, özellikle diferansiyel kriptanaliz (Biham ve Shamir) ve doğrusal kriptoanaliz (Matsui) saldırıları sonucunda ciddi güvenlik açıkları ortaya çıkmıştır. Bu gelişmelerinden ardından AES (Advanced Encryption Standard), 2001 yılında yeni şifreleme standardı olarak kabul edilmiş ve günümüzde en yaygın kullanılan algoritmalardan biri haline gelmiştir (Kara, 2009: 33).

Daha yakın bir tarihte Caesar şifrelemesinin farklı bir versiyonunun kullanıldığına dair dikkat çekici bir haber yayımlanmıştır. 2006 yılında yürütülen bir soruşturmada, emniyet gücü tarafından aranan Bernardo Provenzano isimli bir kişi, Caesar şifrelemesinin bir versiyonunu kullanmıştır. Provenzano'nun mesajlarını şifrelemek için ikame şifrelme yöntemini kullandığı ortaya çıkmıştır. Provenzano, harfler yerine sayılar kullanmış, A için 4, B için 5 olmak üzere alfabenin geri kalanını da aynı sistemle sayısal karşılıklarıyla kodlamıştır. Günümüzde basit görülebilecek bu yöntem sebebiyle gizli mesajlarının şifresi çözülmüş ve sonucunda mafya lideri Provenzano yakalanmıştır (Leyden, 2006). Caesar şifrelemesinin, günümüzde dahi kullanılıyor olması, bu yöntemin kalıcı etkisinin açık bir kanıtıdır.

Yukarıdaki haberin de gösterdiği üzere günümüzde, dijitalleşmenin ve yapay zekâ teknolojilerinin hızla gelişmesiyle birlikte, bireyler ve kurumlar iletişim güvenliği konusunda daha karmaşık ve sofistike çözümlere ihtiyaç duymaktadır. Bu güvenlik ihtiyacı, özellikle veri gizliliğinin korunması, kimlik doğrulamanın sağlanması ve bilgi bütünlüğünün güvence altına alınması gibi temel unsurlara dayanmaktadır. Bu doğrultuda, sanal güvenliği sağlamak amacıyla yazılım uzmanları çeşitli kriptografi teknikleri geliştirmekte ve yeni güvenlik önlemleri uygulamaya devam etmektedir. Kriptografi ve bilgisayar alanındaki gelişmeler Caesar şifrelemesini de etkilemiştir. Bu yöntemle gizlenmiş mesajlar, hackerlar tarafından kullanılan

"kaba kuvvet saldırısı" (Brute-force attack) yani bir şifre veya kombinasyonu tahmin etme yöntemiyle çözülebilmektedir (Aydoğan vd, 2016a: 46). Nitekim, Caesar şifrelemesi düz bir metinde kullanıldığında sadece 25 farklı şifrelemeye izin vermektedir. Bu nedenle mesajı deşifre etmek için kaba kuvvet yöntemi kullanılabilmekte ve 25 olası kaydırmanın tümü denendikten sonra anlamlı olan metin seçilebilmektedir (Raikar, 2025). Bu bağlamda Caesar şifrelemesinin daha yeni bir versiyonu olan ROT13 geliştirilmiştir. Bu yöntemde, temel Latin alfabesi 26 harften oluştuğu için bu sayının yarısı denk gelen 13 harfin kaydırılmasıyla basit bir şifreleme sağlanmaktadır (Bruce, 1996: 11). ROT13 zayıf bir şifreleme olarak kabul edildiği için günümüzde tercih edilmemektedir (Swenson, 2008: 5). Ancak ROT13'ün kullanımına yönelik yardımcı programlar, Linux ve UNIX gibi işletim sistemlerinin temel araç setinde yer almaktadır (Andress, 2014: 71).

2016 yılında, klasik Caesar şifrelemesinin temel mantığına dayanan ve daha karmaşık bir yapı sunan Fragmented Caesar Cipher (FCC; Parçalı Caesar Şifrelemesi) isimli yeni bir şifreleme yönteminin tanıtan bir çalışma yayımlanmıştır. Söz konusu çalışmada, şifrelemede parçalanmış alfabe kullanılması sayesinde klasik Caesar şifreleme yöntemine kıyasla daha fazla olasılık elde edilmiştir. Çalışmanın içeriğinde yeni yöntemin matematiksel modeliyle birlikte bilgisayar uygulamalarıyla desteklenen bir şifreleme algoritması sunulmuştur. FCC yönteminde, alfabe rastgele parçalara ayrılmakta ve her parçadaki harfler belirli sayıda kaydırılarak şifrelenmektedir. Bu yöntem, klasik Caesar şifrelemesine kıyasla daha yüksek güvenlik sağlamaktadır. Zira farklı fragmanlar için ayrı kaydırma anahtarları kullanılmaktadır. Yapılan çalışmada, FCC yönteminin matematiksel modeli oluşturulmuş, algoritması geliştirilmiş ve bilgisayar programlarıyla desteklenmiştir. Ayrıca yöntemin işleyişini göstermek için örnekler sunulmuştur. FCC yöntemi, klasik şifrelemenin basitliğini korurken, parçalara ayrılması ve her parçanın farklı bir sayıda harfin kaydırılması sayesinde kaba kuvvet saldırılarına karşı daha dirençli bir yapı sunmaktadır. Çalışmada ayrıca FCC yönteminin şifreleme ve çözme süreçlerine ilişkin detaylı algoritmalar ve C# programlama dili ile geliştirilmiş kod örnekleri paylaşılmıştır. Bu yöntem, modern kriptografi uygulamalarında klasik yöntemlerin nasıl geliştirilebileceğine dair yeni bir perspektif ortaya koymaktadır (Aydoğan vd., 2016a: 46-57). Bu yapı, klasik Caesar şifrelemesine göre daha fazla olasılık sunmakta ve çözülmesi daha zor bir şifreleme yöntemi meydana getirmektedir. Aynı araştırma ekibi tarafından yürütülen diğer bir çalışmada, Vigenère şifresinin bir genellemesi olan Fragmented Polyalphabetic Cipher (FP-şifreleme; Parçalı Polialfabetik şifreleme) yöntemi yayımlanmıştır. FP şifrelemesi, yukarıda değinilen FCC yöntemine dayanmaktadır. Bu yöntemde düz metin, FCC kullanılarak elde edilen çoklu şifreleme alfabeleri aracılığıyla şifrelenmektedir. Çalışmada ayrıca matematiksel bir modelleme geliştirilmiş ve yöntemin uygulandığı bir bilgisayar programı hazırlanmıştır (Aydoğan vd., 2016b: 58-72). Bu yöntemlerin geliştirilmesi, klasik şifreleme tekniklerinin modern güvenlik gereksinimlerine nasıl uyarlanabileceğini göstermesi açısından önem arz etmektedir. FCC ve FP şifrelemeleri, geleneksel algoritmaların zayıflıklarını gidererek daha karmaşık ve güvenilir sistemlere doğru bir evrimin mümkün olduğunu ortaya koymaktadır. Güncel çalışmaların da gösterdiği üzere Caesar şifrelemesi, modern kriptografi üzerinde etkisini sürdürmeye devam etmektedir.

Sonuç

Antik çağlarda şifreleme ihtiyacı, artan okuryazarlık, askerî gereklilikler ve diplomatik ilişkilerin güvence altına alınması gibi nedenlerle ortaya çıkmış ve farklı uygarlıklarca çeşitli yöntemlerle karşılanmıştır. Ateş sinyalleri ve skytale gibi erken teknikler zahmetli ve sınırlı kullanımlarıyla dikkat çekerken, Polybios Karesi daha sistematik bir yaklaşım sunmuş, izopsefik yöntemler ve büyü papirüslerindeki özel semboller ise gizlilik veya simgesel işlevler üstlenmiştir. Mısır'daki Medinet Madi ostrakonlarında görülen sayısal kodlamalar da bu çeşitliliğin bir başka örneğini teşkil etmiştir. Şifreleme alanında yaşanan bu gelişmeler, Romalılar tarafından da benimsenmiş ve özellikle askeri ve diplomatik bağlamda önem kazanmıştır. Bu çerçevede Caesar şifrelemesi, hem antik dünyanın güvenli haberleşme arayışlarını yansıtan hem de kriptografi tarihine yön veren sembolik bir örnek olarak öne çıkmıştır.

Antik çağın diğer uygarlıklarında olduğu gibi Roma'da da iletişim güvenliği, özellikle askeri ve diplomatik alanlarda temel bir gereklilik haline gelmiştir. Bu bağlamda, Suetonius, Cassius Dio ve Aulus Gellius gibi antik yazarların aktardığı bilgilerden haberdar olduğumuz Iulius Caesar'ın şifreleme tekniği, muhtemelen bu ihtiyaca cevap vermek üzere geliştirilmiştir. Bu çalışmaya kadar Caesar şifrelemesinin tarihsel gerçekliği konusunda şüpheler bulunsa da, burada ortaya konan gerekçeler göz önünde bulundurulduğunda bu tekniğin tarihsel gerçekliği kuvvetle muhtemeldir. Burada sunulan kanıtlar, Caesar şifrelemesinin uygulanmış olmasının tarihsel açıdan güçlü bir olasılık olduğunu göstermiştir. Fikrimizce, ulakların yakalanmasına dair anlatımlar, Caesar'ın kendi eserlerinde bahsettiği gizli mektuplar ve raporlar ile evlatlığı Augustus'un benzer bir şifreleme yöntemini benimsemiş olması, onun bu tekniği kullanmış ve hatta icat etmiş olabileceği hususunda elle tutulur güçlü kanıtlar olarak değerlendirilebilir. Bu bağlamda, çalışma içerisinde söz konusu yöntemin gerçekliği tartışmaya açılmış ve antik kaynaklar ile araştırma eserlerden elde edilen veriler ışığında Caesar şifrelemesinin tarihsel bağlamda uygulanmış olduğuna dair güçlü bir kanaate ulaşılmıştır. Böylece çalışmanın amacı doğrultusunda, tartışmalı olan tarihsel gerçeklik meselesi somut kanıtlarla açıklığa kavuşturulmuş ve Caesar şifrelemesine ilişkin belirsizliklerin önemli ölçüde giderildiği sonucuna varılmıştır. Tarihsel gerçekliği konusundaki belirsizliklerin büyük ölçüde aydınlatıldığı Caesar şifrelemesi, yalnızca kriptografinin erken bir örneği olarak değil, aynı zamanda antik dünyada iletişim güvenliğine yönelik ihtiyaçların somut bir yansıması olarak da önem taşımaktadır.

Caesar şifrelemesinin basit yapısı, dönemin iletişim ihtiyaçlarına pratik çözümler sunmuş ve güvenli haberleşmenin erken dönem örneklerinden birini oluşturmuştur. Bu teknik, Caesar'ın stratejik yazışmalarda bilgi gizliliğini nasıl temin ettiğini ve düşmanların mesajları çözmesini hangi yöntemlerle zorlaştırdığını ortaya koyan dikkate değer bir uygulamadır. Şifre, yalnızca belirli kişilerin anlayabileceği şekilde düzenlenerek yazılı iletişimde gizlilik sağlamıştır. Ancak basit yapısı nedeniyle Caesar şifrelemesi zamanla güvenilirliğini yitirmiş ve modern kriptografi yöntemleri karşısında etkisiz bir hâle gelmiştir. Buna rağmen bu basit yöntem, kriptografinin temellerini atmış ve sonraki şifreleme tekniklerine ilham kaynağı olmuştur. Nitekim Vigenère şifresi, ROT13 ve Fragmented Caesar Cipher (FCC) gibi daha gelişmiş sistemlerin geliştirilmesine zemin hazırlamış olması, bu etkinin açık bir göstergesidir.

Modern kriptografi alanında Caesar şifrelemesi, temel bir referans noktası olarak kabul edilmektedir. Basit bir ikame şifresi olmasına rağmen, ROT13 gibi varyasyonları sayesinde dijital çağda da varlığını sürdürmektedir. Ayrıca, Fragmented Caesar Cipher (FCC) ve Fragmented Polyalphabetic Cipher (FP-cipher) gibi daha karmaşık yapılar bu teknik temel alınarak geliştirilmiştir. Bu yeni yöntemler, önceki versiyonlara kıyasla şifrelemenin kırılmasına karşın daha dirençli hale getirilmiştir. Caesar şifrelemesine dayalı yeni yöntemlerin geliştirilmesi, klasik şifreleme tekniklerinin modern güvenlik gereksinimlerine nasıl uyarlanabileceğini ortaya koyması bakımından önem taşımaktadır. Bu durum, Caesar şifrelemesinin yalnızca tarihsel unsur olmadığını, aynı zamanda modern şifreleme tekniklerinin kavramsal temelini oluşturan bir yapı taşı olduğunu göstermektedir. Dolayısıyla, kriptografi alanındaki gelişmeler sürerken Caesar şifrelemesi gibi tarihsel yöntemlerin yeniden değerlendirilmesi, çalışmada örnekleri verilen yeni yöntemlerin de ortaya koyduğu üzere, modern araştırmalara yeni fikirler kazandırabilmektedir. Sonuç olarak, Caesar şifrelemesi gibi erken dönem yöntemler, güvenli haberleşmenin tarihsel gelişim sürecini anlamak açısından kritik bir rol oynamaktadır. Nitekim Caesar şifrelemesi, yalnızca Antik Roma'da güvenli iletişimin sağlanmasında değil, aynı zamanda kriptografinin tarihsel gelişiminde de önemli bir yer edinmiştir. Bu şifreleme tekniği, kriptografinin evriminde ilk adımların atılmasını sağlamış ve daha karmaşık sistemlerin temellerinine zemin hazırlamıştır. Basitliğine rağmen, kriptografinin temel ilkelerini öğrenmek isteyenler için bir model sunmakta ve kriptografi tarihinde zamanlar ötesi bir köprü işlevi görmektedir. Bu bağlamda, Caesar şifrelemesi sadece tarihsel bir olgu değil, aynı zamanda modern şifreleme sistemlerinin gelişimini anlamak için önemli bir referans noktasıdır.

Bu çalışma, Caesar şifrelemesinin tarihsel gerçekliğine ilişkin belirsizlikleri tartışmaya açarak, hem antik kaynaklardan hem de modern araştırmalardan elde edilen veriler ışığında söz konusu

yöntemin kriptografi tarihinde taşıdığı yeri ortaya koymuştur. Böylece, çalışmanın başında belirtilen amaç yerine getirilmiş ve Caesar şifrelemesinin yalnızca Antik Roma bağlamında değil, modern kriptografinin kavramsal temelleri açısından da anlamlı bir örnek sunduğu sonucuna ulaşılmıştır. Gelecek araştırmalarda, benzer erken dönem şifreleme pratiklerinin karşılaştırmalı analizlerle incelenmesi ve özellikle farklı uygarlıkların geliştirdiği tekniklerin birbirleriyle etkileşimlerinin araştırılması, kriptografi tarihine dair daha bütüncül bir perspektif geliştirilmesine katkı sağlayacaktır.

Kaynakça

Antik Edebi Kaynaklar

Cassius Dio, *Historiae Romanae* = Dio Cassius (1914). *Roman History, Volume III: Books 36-40*, (Translated by Earnest Cary, Herbert B. Foster), Loeb, Cambridge: Harvard University Press.

Aulus Gellius, *Noctes Atticae* = Gellius (1927). *Attic Nights, Volume III: Books 14-20*, (Translated by J. C. Rolfe), Loeb, Cambridge: Harvard University Press.

Caesar, *Bellum Civile* = *Commentarii - De Bello Civili* = Caesar (2016). *Civil War*, (Edited and translated by Cynthia Damon), Loeb, Cambridge: Harvard University Press. = Caesar (2018). *Notlar - İç Savaş Üzerine*, (Çev.: S. Özgüler), Ankara: Doğu Batı Yayınları.

Caesar, *Bellum Gallicum* = *Commentarii de Bello Gallico* = Caesar (1917). *The Gallic War*, (Translated by H. J. Edwards), Loeb, Cambridge: Harvard University Press. = Caesar (2019). *Notlar – Galya Savaşı Üzerine*, (Çev.: S. Özgüler), Ankara: Doğu Batı Yayınları.

Plutarkhos, *Bioi Paralleloi* = Plutarch (1919). *Lives, Volume VII: Demosthenes and Cicero. Alexander and Caesar*, (Translated by Bernadotte Perrin), Loeb, Cambridge: Harvard University Press. = Plutarkhos (2018). *Paralel Hayatlar - İskender-Sezar*, (Çev.: İ. Çokona), İstanbul: İş Bankası Kültür Yayınları.

Polybios, *Historiai* = Polybius (2011). *The Histories, Volume IV: Books 9-15*, (Translated by W. R. Paton), Loeb, Cambridge: Harvard University Press.

Suetonius, *De Vitis Duodecim Caesarum* = Suetonius (1914). *Lives of the Caesars, Volume I: Julius. Augustus. Tiberius. Gaius Caligula*, (Translated by J. C. Rolfe), Loeb, Cambridge: Harvard University Press. = Suetonius (2019). *On İki Caesar'ın Yaşamı*, (Çev.: Gül Özaktürk, Ü. Fafo Telatar), Ankara: Doğu Batı Yayınları.

Modern Kaynaklar

Andress, J. (2014). "Cryptography", *The Basics of Information Security (Second Edition)*, Editor Jason Andress, s. 69-88.

Aydoğan, Y., Çağman, N. ve Şimşek, İ. (2016)a. "Fragmented Caesar Cipher", *Journal of New Theory*, 14, s. 46-57.

Aydoğan, Y., Çağman, N. ve Şimşek, İ. (2016)b. "Fragmented Polyalphabetic Cipher", *Journal of New Theory*, 14, s. 58-72.

Babaoğlu, A. (2009). "Kriptolojinin Geçmişi. Bir Şifreleme Algoritması Kullanmadan Önce Son Kullanma Tarihine Bakın!", *Bilim ve Teknik*, 500, s. 24-27.

Bruce, S. (1996). *Applied Cryptography*, New Jersey: John Wiley & Sons.

Bruen, A., A. ve Forcinito, M., A. (2011). *Cryptography, Information Theory, and Error-Correction: A Handbook for the 21st Century*, New Jersey: John Wiley & Sons.

Diepenbroek, M. (2019). "From Fire Signals to ADFGX: A Case Study in the Adaptation of Ancient Methods of Secret Communication", *KLEOS – The Amsterdam Bulletin of Ancient Studies and Archaeology*, 2, s. 63-76.

Diepenbroek, M. (2021)a. "Ancient Cybersecurity II: Cracking the Caesar Cipher" *Antigone*. https://antigonejournal.com/2021/09/cracking-caesar-cipher/ adresinden 05.02.2025 tarihinde alınmıştır.

Diepenbroek, M. (2021)b. "The Spartan scytale", *Ancient Warfare*, 14(3), s. 45-47.

Harris, W., V. (1991). *Ancient Literacy*, Cambridge, London: Harvard University Press.

Menchetti, A. (2005). Words In Cipher In The Ostraka From Medinet Madi. *Egitto e Vicino Oriente*, 28, s. 237-243.

Kahn, D. (1996). *The CodeBreakers*. *The Story of Secret Writing*, New York: The Macmillan Co.

Kara, O. (2009). "II. Dünya Savaşı'ndan Günümüze Kriptoloji: Enigma'dan AES'E Şifreleme", *Bilim ve Teknik*, 500, s. 28-33.

Kaya, M., A. (2017). "Roma Cumhuriyeti'nin İÖ 80'li Yılları: Siyaset, Darbeler ve İç Savaş", *Uluslararası Darbe Sempozyumu*, cilt 2, 26-28 Mayıs 2017, Aydın, Türkiye, s. 807-828.

Kelly-Gadol, J. (2025). "Leon Battista Alberti". *Encyclopedia Britannica*. https://www.britannica.com/biography/Leon-Battista-Alberti adresinden 10.02.2025 tarihinde alınmıştır.

Leyden, J. (2006). "Mafia Boss Undone By Clumsy Crypto", *The Register*, 16 Nisan 2006.

Macit, H., B., Koyun, A. ve Yüksel, M., E. (2019). "Embedding Data Crypted With Extended Shifting Polybius Square Supporting Turkish Character Set", *BEÜ Fen Bilimleri Dergisi*, 8(1), s. 234-242.

Raikar, S., P. (2025). "Caesar cipher." *Encyclopedia Britannica*. https://www.britannica.com/topic/Caesar-cipher adresinden 03.02.2025 tarihinde alınmıştır.

Reinke, E., C. (1962). "Classical Cryptography." *The Classical Journal*, 58(3), s. 113–21.

Simmons, G., J. (2025). "Vigenère cipher", *Encyclopedia Britannica*. https://www.britannica.com/topic/Vigenere-cipher adresinden 08.02.2025 tarihinde alınmıştır.

Singh, S. (2003). "The History of Cryptography: How the History of Codebreaking Can Be Used in the Mathemathics Classroom with Resources on a New CD-ROM", *Mathematics in School*, 32(1), s. 2-6.

Swenson, C. (2008). *Modern Cryptanalysis: Techniques for Advanced Code Breaking*, New Jersey: John Wiley & Sons.

The Oxford Classical Dictionary, *OCD* (1999). S. Hornblower ve A. Spawforth (ed.). Oxford: Oxford University Press.

Çatışma beyanı

Makalenin yazarı, bu çalışma ile ilgili taraf olabilecek herhangi bir kişi ya da finansal kuruluş ile ilişkisi bulunmadığını dolayısıyla herhangi bir çıkar çatışmasının olmadığını beyan eder.

Destek ve teşekkür

Çalışmada herhangi bir kurum ya da kuruluştan destek alınmamıştır.