Proje Ana Alanı

Matematik

Proje Tematik Alanı

Büyük Veri: Hazır Algoritma Uygulamaları

FAKTÖRİYEL TABANLI DÖNGÜSEL SİMETRİK ŞİFRELEME

Özet

Gelişen teknolojiler ve her geçen gün artan veri kullanımı nedeniyle verilerin güvenliğini sağlamak açısından sürekli yenilenen veya yenilenmesi gereken yöntemlerin geliştirilmesi gerekmektedir. Elektronik belgelerin oluşturulması ve kullanılması sırasında karşı karşıya kalınan başlıca tehditler kullanılan sistemlerdeki açık ve zayıflıklar, belgenin yetkisiz kişilerce görülmesi ve belgenin yetkisiz kişilerce değiştirilmesi olarak sıralanabilir. Bilgi güvenliğini sağlamak için kullanılan önemli yöntemlerden biri olan **şifreleme,** genel olarak bir mesajın, o mesajı çözmek için bir anahtara sahip olan kişi veya kişiler haricinde ulaşılmasını engelleyen matematiksel işlem olarak tanımlanabilir.

Bu projemizde, aktarılan verilerin şifrelenmesi için faktöriyel tabanlı ve AES (Advanced Encryption Standard; Gelişmiş Şifreleme Standardı) şifreleme tekniği ışığında bir matematiksel yöntem geliştirmeye çalıştık. Taban aritmetiği sisteminin çalışma prensibinden faydalanarak işleyen "!" tabanı basamak değerleri faktöriyel ile hesaplanan $(\cdots)_!$ sayıları ile çalışan bir sistem olarak geliştirilmiştir. Yaptığımız literatür taramalarında birçok şifreleme tekniğinde taban aritmetiğinden faydalanıldığını görmemiz geliştirdiğimiz faktöriyel tabanını şifreleme alanında kullanabileceğimiz konusunda bize yön verdi.

Bu şifreleme tekniğinde (k, n) anahtar sistemi ile çalışan faktöriyel tabanlı bir dönüşüm sistemi ile n adet döngüsel işlem sonucunda ulaşılan şifrelenmiş sayısal metin elde edilmektedir. AES şifreleme sisteminde olduğu gibi döngü sayısı oluşan şifrelenmiş sayısal metnin tekrar şifrelenmesi sonucu tekrarsız bir sayısal şifrelenmiş metin oluşturmaktadır. AES şifreleme tekniğindeki gibi şifrelenmiş metinde her bloktaki her değerin birbirine ve anahtardaki değerlere bağlı olması ve döngüsel tasarımı tekniğimizi AES yöntemi gibi güvenli yapmaktadır.

Anahtar kelimeler: Faktöriyel Tabanı, Sınırsız Varyasyon, Tekrarsız Şifreleme, AES Şifreleme, Aktarılan Veri, Döngüsel Şifreleme

İÇİNDEKİLER

AMAÇ

Bu projede genel amacımız faktöriyel tabanı adını verdiğimiz ve raporda da faktöriyel tabanı adını kullanacağımız özel bir taban sistemi ile sınırsız varyasyona sahip döngüsel bir simetrik şifreleme yöntemi üretmek ve bu yöntem yardımıyla aktarılan verileri şifrelemek ve şifrelenmiş metinleri çözmektir. Bu şifreleme tekniğinde açık olarak paylaşılan anahtar (k, n) ile karakter dizininin başlangıç sayısı ve şifreleme için yapılacak döngü sayısı belirlenmektedir. Şifrelenmiş metinde her bloktaki her değerin birbirine ve anahtardaki değerlere bağlı olması ve döngüsel tasarım ile oluşturduğumuz şifreleme tekniğinin bireysel kullanıcılar için düşük maliyetli sistemlerde uygulanabilecek güvenli bir yöntem olması amaçlanmıştır.

GİRİŞ

Şifreleme, veri güvenliğinin temel yapı taşıdır. Büyük şirketler için bilgi güvenliği ne kadar önemli ise bireysel kullanıcılar için de o kadar önemli hale gelmiştir. Bu bilgiler, ödeme verilerinden kişisel bilgilere kadar büyük bir yelpazeden oluşmaktadır. Bu nedenle tüm kullanıcılar için aktarılan verilerde veri güvenliği ve bu işlem için şifreleme yöntemleri ön plana çıkmaktadır. Bilinen şifreleme algoritmaları için hem şifreleme hem de çözme aşamalarını hızlandırmak amacıyla yüksek maliyetli yatırımlar gerekmektedir.

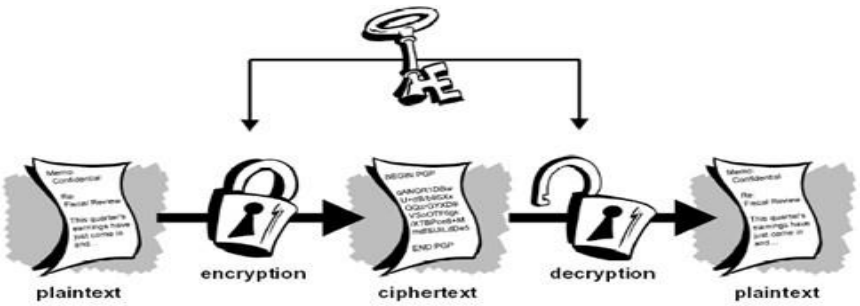
Şifreleme, herkes tarafından okunabilen düz metinleri şifreli metin olarak bilinen anlaşılmaz metinlere dönüştürmektir. Bu yöntem aktarılan verinin rastgele bir görünüme dönüştürülmesi olarak ifade edilebilir. Şifrelemede, gönderen ve alıcı tarafından kabul edilen bir dizi matematiksel değer, yani bir şifreleme anahtarı kullanılır. Alıcı, verilerin şifresini çözmek için bu anahtarı kullanır, böylece veriler tekrar okunabilir düz metne dönüştürülebilir.

EN YAYGIN ŞİFRELEME TEKNİKLERİ

Günümüzde, bilişim teknolojilerinin gelişmesiyle birlikte haberleşme ve bilgi güvenliğinin sağlanması için şifrelemenin önemi giderek artmaktadır. Özellikle internet teknolojisinin gelişmesiyle birlikte veri güvenliğinin sağlanması için birçok şifreleme algoritmaları kullanılmaktadır. (Beşkirli, A. Vd , 2019)

En yaygın olarak bilinen iki şifreleme yöntemi simetrik ve asimetrik şifreleme olarak ifade edilebilir. Bu isimler, şifreleme ve şifre çözme için aynı anahtarın kullanılıp kullanılmadığını ifade etmek için kullanılır. Bu teknikleri şu şekilde özetleyebiliriz:

- **Simetrik Şifreleme Anahtarları:** Bu, özel anahtar şifrelemesi olarak da bilinir. Şifreleme için kullanılan anahtar, şifre çözmek için kullanılan anahtar ile aynıdır. Bu, bireysel kullanıcılar ve kapalı sistemler için en iyi sonucu sağlar. Aksi takdirde, anahtarın alıcıya gönderilmesi gerekir. Bu durum, anahtarın bilgisayar korsanları gibi üçüncü taraflarca ele geçirilme riskini artırır. Bu yöntem asimetrik yönteme göre daha hızlıdır.



- **Asimetrik Şifreleme Anahtarları:** Bu yöntemde, matematiksel olarak birbirine bağlanan iki farklı anahtar (genel ve özel) kullanılır. Anahtarlar, birbiriyle eşleştirilmiş ancak birbirinin aynı olmayan büyük sayılardır, bu nedenle asimetrik terimi kullanılır. Özel anahtar, sahip tarafından gizli tutulur ve genel anahtar ya yetkili alıcılar arasında paylaşılır ya da herkese açık olarak sunulur.

AKTARILAN VERİLERDE ŞİFRELEME

Bilgiler elektronik ortamda özel ağlarda veya internet üzerindeki cihazlar arasında yer değiştirdiğinde, aktarılan veriler olarak kabul edilmektedir. Aktarım yöntemi ile ilgili zayıflıklar ve güvenlik açıkları nedeniyle veriler daha fazla risk altındadır. Aktarım sırasında verilerin özel tekniklerle tümüyle –uçtan uca– şifreleme adı verilen yöntemle şifrelenmesi, verilerin ele geçirilmesi durumunda dahi gizliliğinin korunmasını sağlayacaktır.

Bu konuda yaptığımız araştırmalarda özellikle şifrenin kırılması üzerine yapılan çalışmalar dikkatimizi çekmiştir. El- Kindi'nin "Şifreli Mesajların Kırılması Hakkında" isimli eseri, diğer kültürlerde bu işlerle uğraşan insanları yeni şifreleme metotları bulmak için motive etmiş ve modern şifrelemenin temellerini atmıştır. Buradan da anlaşılacağı gibi şifreleme yöntemi geliştirilirken birçok ölçüt dikkate alınmalıdır.

Simon Singh, 1999 yılında yayınladığı Kod Kitabı'nda, El-Kindî'yi ilk şifre kırma metodunun kâşifi olarak göstermiştir. Singh kitabında "Bir toplumda kripto analizin doğabilmesi için üç farklı alanda yüksek standartların yakalanması şarttır: Dilbilim, istatistik

ve matematik. Bu şartların oluştuğu bir dönemde yaşayan Kindî, bu üç alanda ve daha nice alanlarda uzmanlaşmıştır." ifadesine yer vermiştir. (Simon Singh, 1999)

Bu projede, aktarılan verinin çalınmasını önlemek ve kötü amaçlarla kullanmak isteyen kişiler tarafından okunmasını engellemek amacıyla yenilikçi ve etkili olduğunu düşündüğümüz bir yol üretilmeye çalışılmıştır. Projede verilerin şifrelenmesi için simetrik şifreleme anahtarı yöntemi kullanılmıştır.

Şifreleme algoritmalarının performans ölçütlerinin başlıca olanları kırılabilme süresinin uzunluğu, şifreleme ve çözme işlemlerine harcanan zaman ile şifreleme ve çözme işlemlerinin maliyetidir.

Simetrik şifreleme anahtarlarının bireysel kullanıcılar ve kapalı sistemler için en iyi sonucu sağlayacağı düşünüldüğünde veri güvenliğinin sağlanması için yenilikçi matematiksel algoritmalardan yararlanarak sınırsız varyasyona sahip döngüsel bir şifreleme türü geliştirmek projenin en temel amacı niteliğindedir. Bu amaç özellikle bireysel kullanıcılara düşük maliyetli şifreleme olanakları sunmaktır. Gelişen teknolojiler sebebiyle uzaktan çalışma yönteminin gittikçe artması veri güvenliğine ayrılan maliyetlerin de artmasına sebep olmuştur. IBM'in yaptığı bir araştırmaya göre "Uzaktan çalışmanın bir faktör olarak belirtildiği ihlallerde ortalama maliyet, uzaktan çalışmanın faktör olarak belirtilmediklerine kıyasla 1,07 milyon ABD Doları daha yüksektir."

Veri güvenliğini sağlamak için geliştirilen birçok yöntem vardır. AES elektronik verinin şifrelenmesi için sunulan bir standarttır. Amerikan hükûmeti tarafından kabul edilen AES, uluslararası alanda da defacto şifreleme (kripto) standardı olarak kullanılmaktadır. DES'in (Data Encryption Standard - Veri Şifreleme Standardı) yerini almıştır. AES ile tanımlanan şifreleme algoritması, hem şifreleme hem de şifreli metni çözmede kullanılan anahtarların birbiriyle ilişkili olduğu, simetrik-anahtarlı bir algoritmadır. AES için şifreleme ve şifre çözme anahtarları aynıdır.

Bu projede AES benzeri bir şifreleme yöntemi ile şifreleme ve şifre çözme işlemi için aynı anahtar kullanılmaktadır.

YÖNTEM

Bilgisayar sistemleri ile ilgilenen birçok kişi taban aritmetiği ifadesi ile sıklıkla karşılaşmaktadır. Günümüzde bilgisayarlarda yalnız 1 ve 0 sayılarının kullanımı ile yazılar yazılmakta, oyunlar kodlanmakta, yazılımlar oluşturulabilmektedir. Hatta işlemciler ve transistörler de bu sistemle çalışmakta 1 sayısı enerjinin olduğunu, 0 sayısı ise enerjinin

olmadığını belirtmektedir.

Taban aritmetiğinin tarihi sürecine bakıldığında Araplar 10'luk sistem ile ortaya çıktığında Avrupalılar bunu kullanışlı bulmuş ve kullanmaya başlamış, Aztekler 20'lik sayma düzeni kullanırken Babiller 60'lık sayma düzeni kullanmışlardır. Başka medeniyetlerin de 12'lik sayma düzeni kullandığı görülmektedir. Hatta bu sistemler günümüzde de hala etkisini göstermektedir. 24 saat, 12 ay, 60 dakika, 60 saniye, 180 derece, bir düzine 12 adet gibi kullanımların bu sayma sistemlerinin etkileri olduğu ifade edilebilir.

Projenin temelini oluşturan faktöriyel tabanı, bilinenlerden farklı bir taban aritmetiği sistemi oluşturmayı hedeflemektedir.

Faktöriyel tabanlı döngüsel simetrik şifreleme yöntemini açıklayabilmek için

I. Faktöriyel Tabanı adı verilen taban aritmetiği sistemini oluşturacağız.
II. Verileri verilen anahtar yardımıyla sayısal metinlere çevireceğiz.
III. Sayısal metinleri bloklar halinde faktöriyel tabanlı sayılara çevirip şifrelenmiş sayısal metni elde edeceğiz.
IV. Anahtar değerde verilen döngü sayısı kadar bu işlemi tekrarlayacağız.

Bunun için öncelikle faktöriyel tabanını açıklayalım.

I. FAKTÖRİYEL TABANI

Günümüzde hesaplamalarda yaygın olarak 10 tabanı kullanılmaktadır. 10 tabanında kullanılan rakam kümesi {0, 1, 2, 3, 4, 5, 6, 7, 8, 9} olup her rakam kullanıldığı basamağa bağlı olarak bir basamak değerine sahiptir.

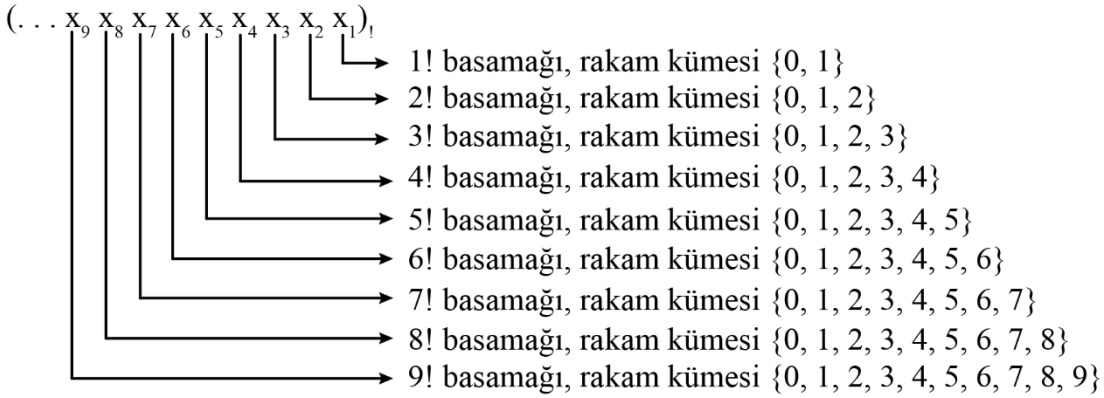
Örneğin; 10 tabanında $\left(\underset{10^2}{a}\ \underset{10^1}{b}\ \underset{10^0}{c}\right)_{10} = a.10^2 + b.10^1 + c.10^0$ olarak ifade edilmektedir.

2 tabanında ise kullanılan rakam kümesi {0, 1} olup her rakam kullanıldığı basamağa bağlı olarak bir basamak değerine sahiptir.

Örneğin; 2 tabanında $\left(\underset{2^2}{a}\ \underset{2^1}{b}\ \underset{2^0}{c}\right)_{2} = a.2^2 + b.2^1 + c.2^0$ olarak ifade edilmektedir.

Faktöriyel tabanı adını verdiğimiz taban aritmetiği sisteminde sayıları yazmak için bilinen taban aritmetiğinden farklı olarak her bir basamakta kullanılabilecek rakam kümeleri değişmektedir. "!" tabanında her bir basamak değeri n! olarak belirlenmiş olmuş n! basamağında kullanılabilecek rakamlar {0, 1, 2, … , n} olarak ifade edilebilir.

Bu sistemi aşağıdaki şema ile gösterebiliriz:



Buna göre bu sayı … $x_9.9! + x_8.8! + x_7.7! + x_6.6! + x_5.5! + x_4.4! + x_3.3! + x_2.2! + x_1.1!$ olarak 10'luk sisteme çevrilebilmektedir. Aslında bu işleme 10! ve daha fazlası ile devam edilebilmektedir. Fakat bu durumda kullanılacak rakam kümesinde 10 sayısı da yer alacağı için tıpkı 16'lık sistemdeki gibi A = 10 eşitliğinden yararlanılarak rakamları temsilen harfler kullanılması gerekecektir.

Çalışmamızda bu sistemi 10! sayına kadar olan basamaklar için kullanarak şifreleme ve taban dönüşümlerinde sadece 10'luk sistemde kullanılan rakam kümesi kullanılmıştır. Bunun için 10.10! sayısından küçük bloklar faktöriyel tabanına çevrilecektir.

Basamak değerlerinde 0! kullanılmamasının temel sebebi bu basamakta 0 dışında bir rakam kullanılamayacak olmasıdır. Aynı zamanda n! basamağında en fazla n rakamının kullanılmasının nedeni de (n + 1).n! işleminin sonucunun 1.(n + 1)! olmasından ötürü bir sonraki basamağa yazılacak olmasıdır.

10'luk Sistemden Faktöriyel Tabanına Dönüştürme

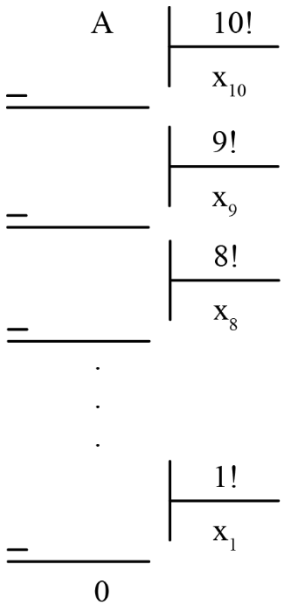
Bu işlemde kullanılacak en büyük faktöriyel değeri 10! olduğundan aşağıdaki tablo değerlerinden faydalanılacaktır.

1! = 1
2! = 2
3! = 6
4! = 24
5! = 120
6! = 720
7! = 5040
8! = 40320
9! = 362880

10! = 3628800 olduğundan 10.10! = 36288000 sayısından küçük sayılar için dönüşüm yapılacaktır.

10'luk sistemde verilen sayı değeri için gerekli bölme işlemleri yapılarak sayı faktöriyel tabanında yazılacaktır. Bu işlem yapılırken verilen bir A sayısının içerisinde kaç tane 10! sayısı olduğu belirlendikten sonra kalan sayı bulunur, ardından kalan sayının içerisinde kaç tane 9! sayısı olduğu belirlendikten sonra kalan sayı bulunur, ardından kalan sayının içerisinde kaç tane 8! sayısı olduğu belirlendikten sonra kalan sayı bulunur, … , ardından kalan sayının içerisinde kaç tane 1! sayısı olduğu belirlenir. A pozitif tam sayısı için en son kalan değer her zaman 0 olacaktır.

Bu işlem aşağıdaki gibi görselleştirilebilir.



$(x_{10}\, x_9\, x_8\, x_7\, x_6\, x_5\, x_4\, x_3\, x_2\, x_1)_!$ elde edilir.

Örneğin; 425 sayısını faktöriyel tabanına çevirmek istediğimizde

- 425 sayısının içerisinde 5! = 120 sayısından **3** tane vardır. Burada kalan 425 – 360 = 65 tir.
- 65 sayısının içerisinden 4! = 24 sayısından **2** tane vardır. Burada kalan 65 – 48 = 17 dir.
- 17 sayısının içerisinde 3! = 6 sayısından **2** tane vardır. Burada kalan 17 – 12 = 5 tir.
- 5 sayısının içerisinde 2! = 2 sayısından **2** tane vardır. Burada kalan 5 – 4 = 1 dir.
- 1 sayısının içerisinde 1! = 1 sayısından **1** tane vardır ve son olarak kalan 0 elde edilecektir.

O halde 425 sayısı "!" tabanında $(32221)_!$ olarak elde edilmiş olacaktır.

Faktöriyel Tabanından 10'luk Sisteme Dönüştürme

Faktöriyel tabanında verilen bir sayı 10'luk sisteme çevrilirken her bir basamaktaki rakam o basamağın basamak değeri olan faktöriyel ifadesi ile çarpılarak elde edilen sonuçlar toplanır.

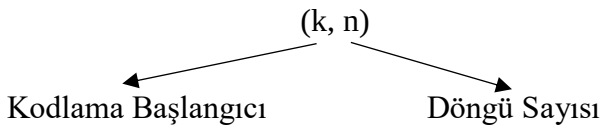
Örneğin; $(32221)_! = 3.5! + 2.4! + 2.3! + 2.2! + 1.1!$

$= 3.120 + 2.24 + 2.6 + 2.2 + 1.1$

$= 360 + 48 + 12 + 4 + 1 = 425$ elde edilecektir.

II. VERİLERİ SAYISAL METNE ÇEVİRME

Projede şifreleme işlemi için kullanılacak anahtar (k, n) şeklinde iki değişkenden oluşmaktadır. Burada k kodlama başlangıcı ve n döngü sayısı olarak belirlenmektedir.



Proje çalışması sırasında karakter listesini kodlamak için k değeri A harfi ile eşleştirilerek belirlenen harf listesinin sayısal karşılıkları elde edilecektir. Değişen bir k değeri sayesinde her şifreleme işleminde her A harfinin karşılığı olarak elde edilen sayısal değer değiştirilmiş olacaktır.

A	B	C	Ç	D	E	F	G	Ğ	H	I	İ	J	K	…
k	k+1	k+2	k+3	k+4	k+5	k+6	k+7	k+8	k+9	k+10	k+11	k+12	k+13	…

Bu sisteme göre, bir metnin k değişkenine bağlı olan sayısal karşılığı, yukarıdaki tablo yardımıyla karakter bazında belirlenir. Projemizde k değeri olarak 3 basamaklı sayılar kullanılmıştır. Fakat şifreleme tekniği bakımından bunun belli bir sınırı yoktur. Aşağıda "Tübitak" kelimesinin farklı k değerleri için elde edilen sayı dizisi aşağıdaki tabloda verilmiştir.

Metin	k değeri	Sayısal Metin
Tübitak	100	124155131141153130143
Tübitak	151	175206182192204181194
Tübitak	303	327358334344356333346
Tübitak	259	283314290300312289302
Tübitak	442	466497473483495472485
Tübitak	189	213244220230242219232
Tübitak	378	402433409419431408421

Projede kullanılan anahtar yapısından ötürü her harfin sayısal karşılığı her defasında değişmekte olup verilen metne karşılık bir sayısal metin bu anahtara göre her defasında farklı bir sayı dizisi olarak elde edilmektedir.

III. SAYISAL METNİ FAKTÖRİYEL TABANINA ÇEVİREREK ŞİFRELENMİŞ SAYISAL METNİ ELDE ETMEK

Projede verilen anahtardaki k değişkeni kullanılarak verilen metin sayısal metne çevrildikten sonra şifreleme işlemi için bu sayısal metin bloklar halinde faktöriyel tabanına çevrilecektir.

Tüm pozitif tam sayılar faktöriyel tabanında yazılabileceği halde bu proje için sadece 10'luk sistemdeki rakamları kullanmak adına belli basamaktaki sayıları faktöriyel tabanına çevirmeye karar verdik. Buna göre bu sistemde yazabileceğimiz en büyük faktöriyel tabanlı sayı $(9987654321)_!$ olacaktır.

Bu durumda bu sayının 10'luk sistemdeki karşılığı

$$9.10! + 9.9! + 8.8! + 7.7! + 6.6! + 5.5! + 4.4! + 3.3! + 2.2! + 1.1!$$

$$= 36287999 < 10.10! = 36288000$$

olduğundan elde edilen sayısal metin 7 basamaklı bölümlere ayrılarak her 7 basamaklı bölümün 10 basamaklı faktöriyel sayılara çevrilmesi garanti altına alınmış olacaktır.

Aşağıda verilen metinlere göre girilen k anahtarı için elde edilen faktöriyel tabanlı şifrelenmiş sayısal metinlere örnekler verilmiştir.

Metin	k Değeri	Sayısal Metin(SM) / Faktöriyel Tabanlı Şifreli Sayısal Metin(ŞM)
Tübitak	124	SM:148179155165177154167
		ŞM:0406001101151634431119633201 01
Tübitak	328	SM:3523833593693813583 71
		ŞM:0963111111163164212003653333 01
Tübitak	491	SM:5155465225325445215 34
		ŞM:1416621001061703021012410521 00

Dönüştürme işlemi sırasında değişen k değerleri için sadece 1 kez şifreleme işlemi uygulanmış ve tablodaki değerler elde edilmiştir.

Bu işlemler sırasında sayısal metin 7 basamaklı bloklara ayrılırken eğer sayısal metnin basamak sayısı 7'nin katı değilse sayısal metnin sonuna dönüştürme aşamasında 0 rakamları basamak sayısı 7'nin katı oluncaya kadar eklenmektedir. Böylelikle hem bloklara ayırma işlemi hem de oluşan şifreli sayısal metin bir standart dönüşüme ulaştırılmış olacaktır. Bunun sonucunda elde edilen şifrelenmiş metin 10'un katı olan bloklardan oluşmaktadır.

IV. DÖNGÜ SAYISI İLE ŞİFRELENMİŞ METNİ TEKRAR ŞİFRELEMEK

Projede kullandığımız anahtar (k, n) şeklinde iki değişkenden oluşmakta olup bu değişkenlerden ilki kodlama başlangıcı olarak harflerin sayısal karşılıklarını belirlemekte, ikincisi ise şifreleme işleminin kaç kez tekrar edeceğini yani döngü sayısını belirlemektedir. Şifreleme işlemi her sayısal metne uygulandığında sayısal metin 7 basamaklı bloklara ayrılarak her blok faktöriyel tabanına çevrilmektedir. Bu çevirme işleminde her bir 7 basamaklı blok 10 basamaklı faktöriyel tabanına çevrilmektedir. Bu işlem şifrelenmiş sayısal metne döngü sayısı kadar uygulanacaktır.

Bazı anahtar değerleri için elde edilen şifreli metinlere örnekler aşağıdaki tabloda verilmiştir.

Metin	Anahtar (k, n)	Şifreli Sayısal Metin
Tübitak	(135, 1)	0433554021182100401022440303 00
	(135, 2)	011600430000520103110007640320066411410100000000 00
	(135, 3)	00270032000823142020002431110000171031210546100001 03775240200000000000000000000
	(135, 4)	00052300110544652211038153000000601342110000012011 00756241111262443110027561422011054200000000000000 00000000000000000000

Bilgisayar yardımıyla yapılan bir şifreleme örneği ve anahtar aşağıda verilmiştir.

Metin	Anahtar (k, n)
Bu şifreleme tekniğinde (k, n) anahtar sistemi ile çalışan faktöriyel tabanlı bir dönüşüm sistemi ile n adet döngüsel işlem sonucunda ulaşılan şifrelenmiş sayısal metin elde edilmektedir. AES şifreleme sisteminde olduğu gibi döngü sayısı oluşan şifrelenmiş sayısal metnin tekrar şifrelenmesi sonucu tekrarsız bir sayısal şifrelenmiş metin oluşturmaktadır.	(267, 5)

000220411006044430101762132200113044000000001422110332032221196532220000
000020003516441111501223300007423032005704400000004402201196561032102663522
222003775240200000022201030102430103322110000881052200000444111006065011210
105526540200000420000030214331108551331211420303310002210222011055412201240
405433010000213301087265032016745102000732302011030214312112166431202044134
340200016630021091051130117860340200000000000026650101116726303100385542201
010025401010118321322014143242110047643111060445311000834333000376644221082
825230100115333330007466403200266314020003165401006422240210001420001115333
331100027540310022352300103022333101682201220083024311002712021000081603221
055710000100054331200004113300182562220005260120200874631311088320122015
706523200026202011145552122109112212200013224211061044400101611423210541622
220060433132002730033002486431220000104021003576203110110141100001321202
100514500010382123110020121130005465410010110000000157350311100006231101
133303120183131410003042222100906642021148542031000640431200024001321011
352201009826322110270111101141015131119630203100022100120002560311003041531
100064613311000165122000062233011243413001002502331006342113111985344210
028761222009066430101215014211007365221000476021101432213300022150220105
445503210544543110010033020000101310001105421221137415220000050323210023552
211167235122004016331200023611200091250332009204431110050231311007545420
006306331110223212321026632031003855131100270654020054601001109126343001
523200010032325430106064521001762010310010242122008471312001213130310005203
312005705211201372020011155113421100000042200002121310195451000003214230
010823140000087504201007315333010305021200010752000000050042200005414021
112545111105545333000172150121060633421106323420100907123110000050031008231
403101217303300001254130011254501012016542321008333202008726243010913051
220165703031105716241000326210310204054122100132310010326043211182145402
003162533100570441000083153000025661340210546400220005602031000836141000282
303000085303221005706103110055601110087301320015215503110364640011054465
122014555213111251400310028301300100476230011537043111001264032005445431
100000000001065520001000000101201211252000205041012000101300010851023110113
330330000074112320002600101103101412211220653110000000000008551331100100
204021001335122106044543110435613300000453001005705543100853303110015703020
100010323200827250110063305122000332513110332150000005010000000056401210
330143020167644311014661200010266331120140620022115416120200035530020082
330400103305000000315123121082540002003822401200030602201000045211008553043
212064604210027514131000275421001262633110017153002000474431100376251220
074040012000260102101107533110011200201002740442200825131220000214110101653
300010606411101041601000001360233000003342100117723421004423300100281531
000091264022116810240200354001220032610132014060512200007632200027042001
011075422002034143110000001330005470021000847031221010020000005465400000
082755122000043031100272033001145340312100243012200001342221003001230010
0

430402000021411000025654300171410201106561222100270050010003012320119525131200270344220000200410011512423200005032021002601411111512333000056601220002355320011274413111274534211032123331008530201210073641220014401411005726322010940653111125114421102663022010933004020207200311000130002100851024101141161330000000041100606414310091651000004653142110266633001137015010008275522100307442020112532320006402231100314550201030220000100275442100437344020030365201114573513202364523000003561020003320302101245404020007363410103301313111646500000000001421003040223001106012320005220402002746422010910512320115153031003143243000047443310064021311008322500000547520211121524012109725123210273611301003000332019252231100160203121082321421104215133002265210001026703000008811521010164020001000523001000514421001413614211048625232003300313110700250000174241331100014520110936530310054760201100125341011153221210030461220002241111200572431221140634000002055341000575103320143604410018236320100267633310118110131015251200000027542010004753320009630020101732303001000154012014534031210077621101003530031100000133111153352201000005111008750023001481544020167333300100012503211127603201198505201003046320100000003121210604031100745141000572514110148542012009105431110571123321112533221107200133000325424211030214311114416240210073643311057244000000814503100401633120026664010005706013200121214021026742221000754531101650604020000000001008730232000823140000020701312003036323210355620111112745110003311220110853020010097042031000003032000270343020152314201007321441010302621220112545021107004031200267603200060645002020876300010450442220057044410008533031100000010310054633421003101323102074153120000565021106063242100632243110025561032008726430111135430310166323312000261202000266252200113401311100051542110326041101003224201000655420200025611311146151421016630100010550151001065441220118054040200274610020066324221055313000001163001200546541001110202000003144131210302432320063235031009706422010266411200000001221063223000000542010000572454100088331421024874112200000101200083125032100814503100034250011112545331117640203100001134220087303330104114331200277133120026632002113723032201287113110000041110008510311200107241220000500430005726121010332312010116023020100000000000091063330114576400100273554111002754121012664312200230030310002405210111014312202010500201000034112011774010012060212020030255430000275410101734253111024503110102663430000660531220000430402002673232011181222011096654122100370120101105541300146025031100861421000051654301057314122000506122110570521120121711430011415323210003650321115533111016723333000235144021026651412005704401200737514221027112410000061012200163553111000530222100514443111442023110057134001008746230211786200120233053202102702132011127320101110402110102666132000851152111071421031103721331200872623210007604122102811203210025101311110753311017705223200006313310063433311016723522000660653301060435230103064242102413204220054462410105505313010551413000030024411006303511010686542010000002221006044202001211003300242713012103033111100030123201124131220100336113000077450220141015201000706513010302314111148201110121042240200266502110055054102006864022010001342021060633302114562501210074010020027031400114301041000825443110030260111111811042110686302321003440111011532123201963151221008050331108746230211676204020057330311002662512201127603301003424312000202341100906520000000000000001

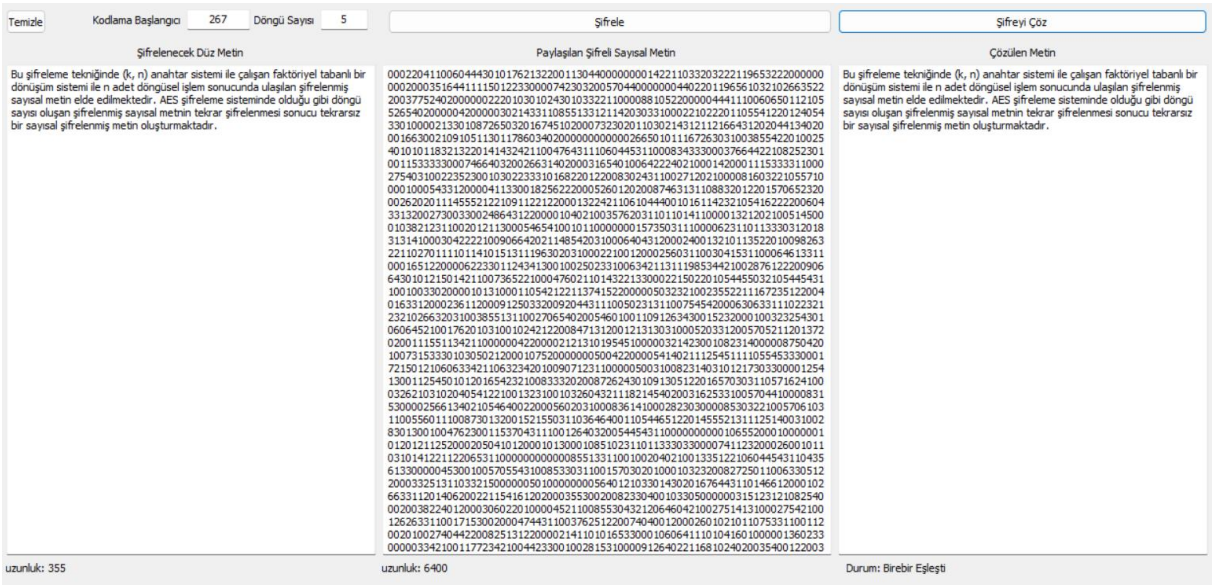
ŞİFRELİ SAYISAL METNİ ESKİ HALİNE ÇEVİRME

Şifreli sayısal metin (k, n) anahtarına göre şifrelenmiş olduğundan eski hale çevirme işlemi de yine bu anahtara göre yapılacaktır. Şifreleme işlemi sırasında n değerine göre kaç kez döngü uygulanmış ise yine aynı miktarda döngü çevirme işleminde uygulanarak şifrelenmiş metnin sayısal değerine ulaşılmış olacaktır.

Şifreleme işlemi sırasında sayısal metin 7 basamaklı bloklara bölünmüş ve her 7 basamaklı blok 10 basamaklı bloklar şeklinde faktöriyel tabanına çevrilmiştir. Buna göre ters işlem uygulanarak bu sefer şifrelenmiş metin 10 basamaklı bloklara ayrılır ve her 10 basamaklı bloktan oluşan faktöriyel tabanlı sayı 10 tabanına çevrilecektir. Bu işlem anahtardaki n değeri kadar tekrarlanarak sayısal metne ulaşılmış olacaktır.

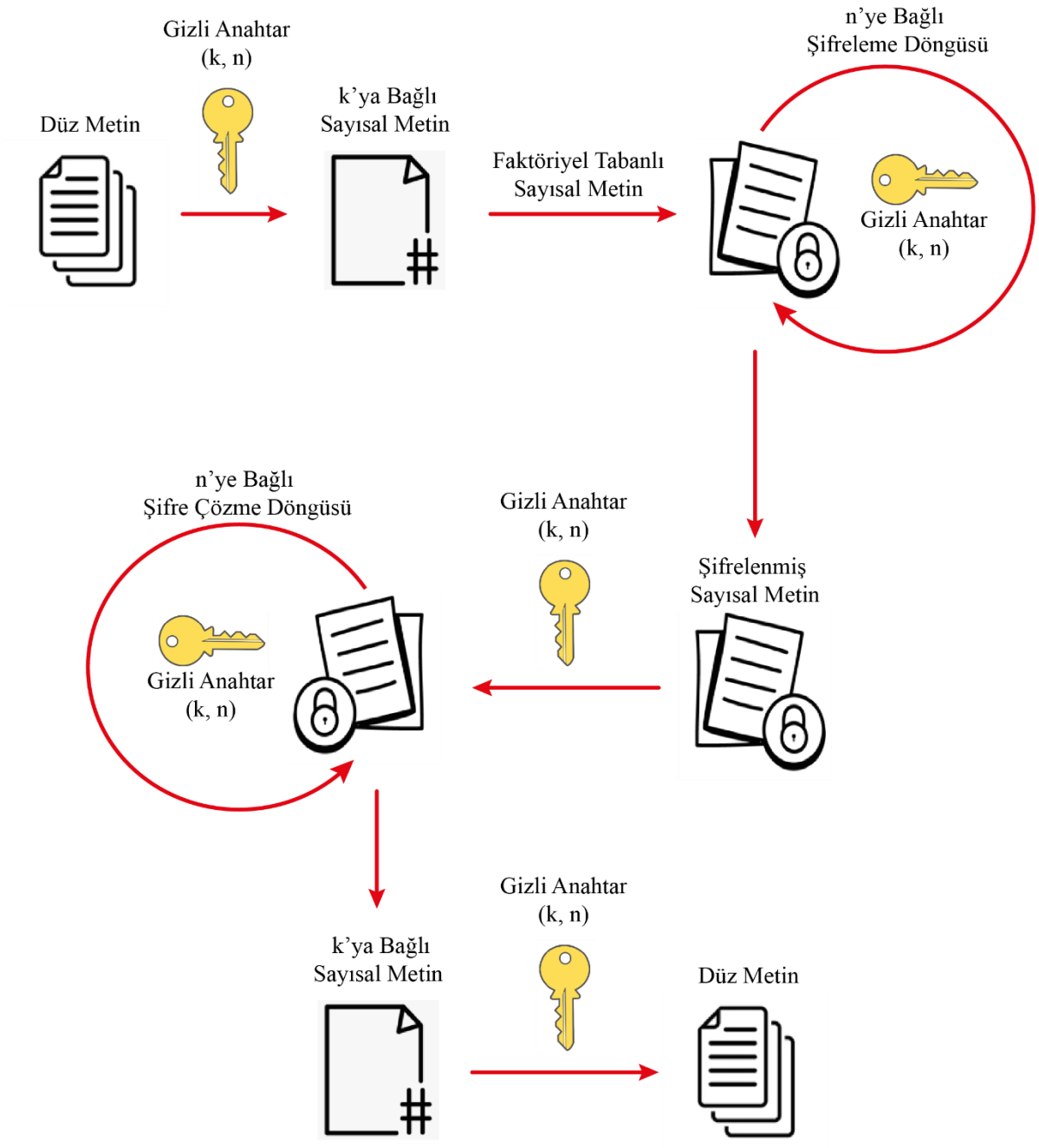
Sayısal metin oluşturulurken k sayısı ile harf dizisinin sayısal kodları eşleştirildiği için bu işlem tersten uygulanarak sayısal metin şifrelenen metne dönüştürülmüş olacaktır.

Aşağıda bilgisayar yardımıyla yapılan şifreleme ve çözme ekranı gösterilmiştir.



Bu şifreleme ekranına göre 355 karakterden oluşan bir metin k = 267 değeri için sayısal metne çevrildikten sonra n = 5 değeri için 5 kez şifrelenmiş ve 6400 basamaktan oluşan tekrarsız bir şifrelenmiş sayısal metin elde edilmiştir. Bu şifreli sayısal metne şifre çözme işlemi uygulandığında ilk metin ile çözülen metin arasında birebir eşleşme sağlanmıştır.

Bu projede anlatılan şifreleme ve şifre çözme basamakları aşağıdaki şema ile bir bütün halinde gösterilmiştir.



SONUÇ VE TARTIŞMA

Bilgi sistemleri ve veri kullanımındaki sonsuz artış, bilgi güvenliğinde tehlikenin doğuşunu tetiklemiştir. Son yayınlanan raporlara göre askeri kuvvetler ve e-ticaret web siteleri dışında sıradan kullanıcılar da sistemlerini ve belgelerini korumak için şifreleme teknikleri kullanmaya başlanmışlardır. Alınan tedbirlere rağmen çeşitli gizleme tekniklerini kullanarak hazırlanan akıllı saldırılar mevcut korunma yöntemlerini atlatarak hedef sistemdeki parola ve kullanıcı adlarını ve hatta aktarılan verileri ele geçirebilmektedir.

Bu projede temel amacımız bilinen tekniklerin dışında bir matematiksel yöntem yardımıyla bireysel kullanıcılara maliyeti düşük ve saldırılardan daha iyi korunan bir şifreleme tekniği sunmaktır. Bu tekniği uygularken geliştirdiğimiz bir bilgisayar programı şifreleme için seçilen (k, n) anahtarı için basit matematiksel işlemler ile hızlı bir şekilde şifreleme işlemi yapabilmektedir. Birçok şifreleme yönteminde kullanılan fonksiyonlar ve fonksiyon döngüleri ile şifreleme işlemi gerçekleştirilebilmesi için donanım olarak güçlü bilgisayarlar ve yüksek kapasiteli işlemciler gerekmektedir. Oysa bu projede kullandığımız yöntem hesap makinesi ile dahi hızlıca gerçekleştirilebilecek kadar küçük donanıma ve basit işlemciye sahip bilgisayarların dahi yapabileceği ölçüde bir matematiksel işlemdir. Bu durum bireysel kullanıcılar için düşük maliyetli şifreleme yöntemlerinin geliştirilebileceğini bizlere göstermektedir.

Projede kullandığımız şifreleme işleminde anahtar olarak belirlenen (k, n) değeri için sınırsız sayıda alternatif olması şifre kırma işlemleri açısından sınırsız sayıda deneme gerektiği anlamına gelmektedir. Bilindiği üzere AES algoritması için 2^{200} işlem gerektiren bir saldırı algoritmanın kırılması olarak kabul edilirken 2^{200} mertebesindeki bir işlem, şu an için, evrenin yaşından daha uzun bir süre gerektirmektedir. Projemizde AES benzeri bir yapı ve 3DES benzeri döngüler ile sınırsız anahtara sahip bir şifreleme oluşturmaya çalıştık.

Şifre algoritması geliştirmek için çalışan her araştırmacının dikkate alması gereken önemli notalardan biri de şifre kırma algoritmalarının kullandığı yöntem ve tekniklerdir. Bu bağlamda özellikle şifre kırma algoritmaları, frekans analizi ve bilinen şifreleme yöntemlerinde ters işlem yaparak oluşturulan şifreli metni incelediği için şifre yapısında bu algoritmaları geride bırakacak bir düzenleme yapılması gerekmektedir. Bu projede geliştirdiğimiz şifre yapısında sınırsız anahtara sahip bir şifreleme yöntemi ve döngüsel yaklaşım düşük maliyetli yenilikçi bir algoritma yapısı ortaya koymaktadır.

ÖNERİLER

Şifre ve parolalar dijital dünyada siber saldırıların odağında olmakta ve kırılan tek bir şifre ile tüm güvenlik sistemleri atlatılarak veriler ele geçirilebilmektedir. Şifreli verilere veya bilgi sistemlerine ulaşmak saldırganlar kadar sıradan insanlarında ilgisini çekmekte ve bu durum şifre kırmak için her geçen gün yeni yöntemler geliştirilmesine sebep olmaktadır. Şifre kırma işlemi için geliştirilen bu yeni yöntemlere karşı şifreleme için de yeni yöntemler geliştirilmesi zorunlu bir ihtiyaçtır.

Projemizde ulaşmaya çalıştığımız temel hedef sınırsız varyasyona sahip bir anahtar yapısı ile şifre bloğu üretmenin yanında tüm yöntemlerden farklı olarak faktöriyel tabanı olarak tanımladığımız yenilikçi bir işlemle sayısal şifrelenmiş metin elde ederek şifre kırma işlemlerini daha da zorlaştırmaktır. Projemizin bu tür şifreleme teknikleri geliştirmek isteyen araştırmacılara yol göstermesi açısından bu yöntem bir örnek teşkil edecektir. Temel bir matematiksel fonksiyon olan taban aritmetiğinin ve şifrelemeyi güçlendirmek için tekrarlanan fonksiyon döngülerinin şifreleme için uygun yöntemler olduğunu göstermeye çalıştığımız bu araştırmamız şifreleme için yeni yöntemler geliştirmeye çalışan araştırmalara yol gösterecektir.

KAYNAKÇA

Simon, S. "*The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography*", 1999

Beşkirli, A., Özdemir, D., & Beşkirli, M. (2019). *"Şifreleme Yöntemleri ve RSA Algoritması Üzerine Bir İnceleme"*. Avrupa Bilim ve Teknoloji Dergisi, 284-291.

Kara, İ. (2019). *"Kaba Kuvvet Saldırı Tespiti ve Teknik Analizi."* Sakarya University Journal of Computer and Information Sciences, 2(2): 61-69.

Kaya, Ö. F., Öztürk, E. (2017). *"Veri ve Ağ Güvenliği İçin Uygulama ve Analiz Çalışmaları."* Istanbul Ticaret Universitesi Fen Bilimleri Dergisi, 16(31): 85-102.

İnternet: 3DES Algoritması, https://bidb.itu.edu.tr/seyir-defteri/blog/2013/09/08/3des-algoritmas%C4%B1, Son Erişim Tarihi: 15.01.2023

İnternet: Ev ve İşletmeler İçin Kaspersky Siber Güvenlik Çözümleri, Kaspersky, https://www.kaspersky.com.tr/ , Son Erişim Tarihi: 15.01.2023

İnternet: Bir Veri İhlalinin Maliyeti Raporu 2021 - Türkiye | IBM, https://www.ibm.com/tr-tr/security/data-breach, Son Erişim Tarihi: 15.01.2023

İnternet: AES, https://tr.wikipedia.org/wiki/AES, Son Erişim Tarihi: 15.01.2023

İnan A., Nergiz M., Saygın Y., "*Öğrenci Verilerinin Korunması: Fatih Projesi Işığında Teknik Değerlendirme*", Bilişim Teknolojileri Dergisi, 10(1), 67-77, 2017.

Çalık E., Erdem H. A., Aydın M. A.: "*Bulut Bilişim Güvenliği için Homomorfik Şifreleme*", 19. İnternet Konferansı, Yaşar Üniversitesi, İzmir, 249-253, 27-29 Kasım 2014.

Özbilgin F., Durmuş F., Karagöl S., "*Yazılı metni şifreleyip LSB yöntemi ile gizleme*", Düzce Üniversitesi Bilim ve Teknoloji Dergisi, 2018

Aksakallı I. K., "*Bulut Bilişimde Güvenlik Zaafiyetleri, Tehditler ve Bu Tehditlere Yönelik Güvenlik Önerilerinin İncelenmesi*", Uluslararası Bilgi Güvenliği Mühendisliği Dergisi, 5(1), 18-19, 2019.

Knuth, D. E. (1973), "*Volume 3: Sorting and Searching, The Art of Computer Programming*", Addison-Wesley, p. 12, ISBN 0-201-89685-0

Cantor, G. (1869), "*Zeitschrift für Mathematik und Physik"*, vol. 14.

Knuth, D. E. (1997), "*Volume 2: Seminumerical Algorithms*", The Art of Computer Programming (3rd ed.), Addison-Wesley, p. 192, ISBN 0-201-89684-2.

McCaffrey, James (2003), Using Permutations in .NET for Improved Systems Security, Microsoft Developer Network.

Mantaci, Roberto; Rakotondrajao, Fanja (2001), "*A permutation representation that knows what "Eulerian" means*" (PDF), Discrete Mathematics and Theoretical Computer Science, 4: 101–108

Arndt, Jörg (2010). Matters Computational: Ideas, Algorithms, Source Code. pp. 232–238.