

**Proje Adı:**Pi'releme

**Proje Konusu:** Siber Güvenlik

**Proje Türü:** Tübitak Projesi

**Proje Alanı:** Kodlama ve Matematik

**Proje Amacı:** Bu projedeki temel amaç pi sayısının asla kendini tekrar etmeyişinden faydalanarak pi sayısının belli bir basamak sayısını Monte Carlo metodu ile hesaplamak ve bu hesaplama sonucu elde edilen küsurat bölümünü kullanarak her alanda kullanılabilecek bir güvenlik, kolaylık, hafiflik ve güvenilirliğe sahip bir algoritma oluşturmak ve bu algoritmayı kullanarak güçlü bir şifreleme metodu oluşturmak ve bu sayede yerli, güvenilir bir kriptolama metodu oluşturmaktır. Daha sonra oluşturulan bu kriptolama metodunu Uluslar arası kullanılabilir bir hale getirmektir.

**Projede Kullanılacak Yöntem ve Gereçler:** Literatür taraması kapsamında konu ile alakalı kitaplar, makaleler, tezler taranacaktır. Ardından Monte Carlo metodu kare içindeki bir daireye düşen rastgele noktaların karenin tamamına düşeni ile oranlanacak ve sonuç olarak elde edilen pi sayısının (en yaklaşık değeri) hesaplanacak ve bu sayının küsurat deneni kısmındaki rastgele seçilen aralıklar kullanılarak bir algoritma oluşturulacaktır. Bu metot ise temelini Pi sayısının kendini tekrerrür etmeden sonsuza kadar ilerlemesi sonucu oluşur. Bu işlemi kısaca özetleyecek olursak; Pi sayısındaki kendini hiç tekrar etmeyen küsurat bölümü, şifreleme algoritmasına göre belirlenen basamak aralıklarındaki rakamlar kadar ileri bir karakter ile değiştirilip bu karakterlerin belirlendiği aralıktaki -yerine harfleri gelecek- olan rakamların toplamının karşılığı olan karakterin; şifrelenecek olan içeriğin uzunluğuna göre yine algoritma tarafından yeri belirlenerek yerleştirilmesi ile dosyamız kriptolu hale geliyor. Bu esnada JavaScript programlama dili ve Başta Proccesing.js, Velocity.js kütüphaneleri olmak üzere Grafik, Matematik ve Fizik tabanlı Javascript kütüphaneleri kullanılacaktır. Ayrıca işletim sistemi olarak alpha(yapım) aşamasında iken windows işletim sisteminde, beta(test ve düzeltme) aşamalarında kense linux ve android işletim sistemlerinde çalıştırılacak ve bu işletim sistemleriyle uyumlu hale getirilecektir. Daha sonra ise kullanılan işletim sistemlerinin sahip olduğu kernel ve güvenlik açıkları göz önünde bulunduracak, tespit edilen açıkların programa olan veya olabilecek potansiyel tehditleri giderilmeye çalışılacaktır. Başlangıç olarak demo amaçlı, toplam iki parçadan oluşan bir şifreleme ve deşifreleme programları kullanılacaktır

**Proje Özeti:** Günümüzde iletişim kurmak; çevremizdeki birçok internet kullanan araç sayesinde oldukça kolay ancak bu iletişim ne kadar güvenli? Bu projedeki temel amaç; hem yerli, hem de Askeri alandan günlük kullanıma kadar yayılabilecek bir hafiflikte olan ve bir o kadar da güvenli olacak bir kriptolama metodu oluşturmaktır. Bu metot ise temelini Pi sayısının kendini tekrerrür etmeden sonsuza kadar ilerlemesi sonucu oluşur. Bu işlemi kısaca özetleyecek olursak; Pi sayısındaki kendini hiç tekrar etmeyen küsurat bölümü, şifreleme algoritmasına göre belirlenen basamak aralıklarındaki rakamlar kadar ileri bir karakter ile değiştirilip bu karakterlerin belirlendiği aralıktaki -yerine harfleri gelecek- olan rakamların toplamının karşılığı olan karakterin; şifrelenecek olan içeriğin uzunluğuna göre yine algoritma tarafından yeri belirlenerek yerleştirilmesi ile dosyamız kriptolu hale geliyor. Şifreleyici ve şifre çözücü olmak üzere iki parçadan oluşan yöntemde şifre oluşturunun ve çözücünün mantığı kullanıldığı cihaza göre değiştirilip, bu mantık ise yalnızca ana bilgisayar tarafından çözümlenebilir olmaktadır. Ve yine Şifreleyici + deşifreleyici parçaların kendileri de aynı algoritma ile şifrelenmektedir.

**Anahtar Kelimeler:** pi sayısı, algoritma, rakam, kriptolama, şifre, deşifre

### İş-Zaman Tablosu

İşin Tanımı									
	Mayıs	Haziran	Temmuz	Ağustos	Eylül	Eki m	Kası m	Aralık	Ocak
<b>Literatür Taraması</b>	X	X	X	X	X	X	X	X	X
Pi sayısının Yaklaşık değerinin hesaplanması						X	X	X	
Algoritmanın oluşturulup, test edilmesi ve uygulanması			X	X	X	X	X	X	
<b>Proje Raporu Yazımı</b>						X	X	X	X