**Proje Adı:** Pi'releme

**Proje Konusu:** Siber Güvenlik

**Proje Türü:** Tübitak Projesi

**Proje Alanı:** Kodlama ve Matematik

**Proje Amacı:** Şifreleme genel anlamıyla bir mesajın, o mesajı çözmek için (decrypt) bir anahtara sahip olan kişi veya kişiler haricinde okunmasını engelleyen matematiksel işleme verilen isimdir. İnsanlar, tarih boyunca yalnızca istedikleri kişinin okumasını umdukları mesajları şifreleme yöntemini kullanarak göndermişlerdir.(1) Günümüzde ise bu şifreleme işlemini bizim yerimize yapabilen bilgisayarlara sahibiz. Bugün gizli mesajlaşmanın da ötesine giden dijital şifreleme teknolojisi, mesajların yazarını doğrulamak gibi özel amaçlar için de kullanılabiliyor. Doğru kullanıldığında kırılması neredeyse imkânsız olan şifreleme teknolojisi, elimizdeki bilgileri kötü aktörlerden, devletlerden ve servis sağlayıcılarından korumamız için günümüzde sahip olduğumuz en önemli araçlardan biri.

Şifrelemedeki genel sorun ise şifreleme anahtarlarının sunucu bazlı olmalarıdır. Bu, verilerin belli bir sunucudan geçmesini ve yine gönderenin bu veri gönderdiği servisin sunucusuna güvenmekten başka çaresinin olmadığı anlamına gelmektedir. Bu sebeple projedeki temel amaçlardan biri de bir sunucu gereksinimini kaldırmak ve şifreleme anahtarını verinin içinde gizleyerek göndermeyi sağlamaktır.

Bu projenin amacı Deşifre anahtarı kendi içinde olan ve mesaj özelliklerine göre konumlanan rastgele –mesaj aynı olsa dahi- bir anahtarla çalışan şifreleme metodu üretmektir. Bu metot pi sayısının kendini asla tekerrür etmeyişinden faydalanan, her alanda kullanılabilecek bir güvenlik, kolaylık ve hafifliğe sahip güvenilir bir şifreleme algoritması oluşturmak ve bu algoritmayı kullanarak güçlü bir şifreleme metodu oluşturmaktır.

Sonuç olarak; bu metodun önce metin türü verilerde daha sonra ise her türlü(resim, video, mp3 vs…) veride kullanımı ve yine oluşturulan metodun hem uluslarası hem de daha güvenilir olması planlanmaktadır.

**Projede Kullanılacak Yöntem ve Gereçler:** Literatür taraması kapsamında konu ile alakalı kitaplar, makaleler, tezler taranacaktır.

Projede söz konusu olan programımızın içerisinde kullanılacak olan c#(sharp) dilinin getirdiği ağırlıktan dolayı en uyumlu olduğu ve en hızlı derleyen işletim sistemi olan Windows platformu tercih edilecektir.

C# (si şarp şeklinde telaffuz edilir), Microsoft'un geliştirmiş olduğu yeni nesil programlama dilidir. Yine Microsoft tarafından geliştirilmiş DOTNET Teknolojisi için geliştirilmiş dillerden biridir. Microsoft tarafından geliştirilmiş olsa da ECMA ve ISO standartları altına alınmıştır.

Windows’ta uygulama geliştirebilmek için Visual Studio, MonoDevelop vb. gibi bir geliştirme aracına ihtiyaç duyulmaktadır. Projede Visual Studio 2017 Community Edition kullanılacaktır.

Visual Studio; Microsoft tarafından 1997 yılında “Boston” kod adı ile yayımlanmıştır. Visual Studio’nun yayımlanan son sürümü 15,9’dur ve 11 Kasım 2018 tarihinde yayımlanmıştır.

Projenin Yapımı, üç temel aşamada planlanmıştır. İlk aşama pi sayısı kullanılarak projenin şifreleme algoritmasının tasarlanması ve bir Windows Forms App’e(Windows Formlar Uygulaması) uyarlanmasıdır. İkinci aşama İki bölümden oluşacak Windows Forms App’in birinci bölümü olan encryptor(şifreleyici) kısmının oluşturulmasıdır. Bu bölüme projede “Pi’Releyici” adı atanmıştır. Üçüncü aşama ise Windows Forms App’in ikinci bölümü olan decryptor(şifre çözücü) kısmının oluşturulmasıdır Bu bölüme de tüm işlemleri tersinden yapacak şekilde tasarlanan ve bu anlama gelmekte olan “DePi’releyici adı atanmıştır. Son olarak bu iki formdan oluşan uygulama; Pi’releyici ve DePi’releyici olmak üzere iki farklı uygulamaya bölünecektir.

**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 temelini Pi sayısının kendini tekrar etmeden sonsuza kadar ilerlemesi sonucu oluşur. İşlemi kısaca özetleyecek olursak; Pi sayısındaki tekrarlanmayan küsurat bölümü, (şifreleme algoritmasına göre belirlenen basamak aralıklarındaki rakamlar kadar) ileri bir karakter ile değiştirilir karakterlerin belirlendiği aralıktaki -yerine harfleri gelecek- rakamların toplamının karşılığı olan karakterler; şifrelenecek olan içeriğin uzunluğuna göre yine algoritma tarafından yeri belirlenerek yerleştirilmesi ile veriler kriptolu hale gelir. Şifreleyici ve şifre çözücü olmak üzere iki parçadan oluşan sistemde şifre oluşturucunun ve çözücünün mantığı kullanıldığı cihaza göre değiştirilir ve sadece ana bilgisayar tarafından çözümlenebilir olmaktadır. Ayrıca Şifreleyici + deşifreleyici parçaları da aynı algoritma ile şifrelenmektedir. Şifreleyici cihaz da deşifreleyici cihazda birbirinden ayrı çalışır.

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

**İş-Zaman Tablosu**

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **İşin Tanımı** |  |  | | | | | | | | |  |
|  | Mayıs | | Haziran | Temmuz | Ağustos | Eylül | Ekim | Kasım | Aralık | Ocak | |
| **Literatür Taraması** | X | | X | X | X | X | X | X | X | X | |
| **Pi’Releyici** |  | |  | X | X | X | X | X |  | X | |
| **DePi’releyici** |  | |  |  |  | X | X | X | X | X | |
| **Proje Raporu Yazımı** |  | |  |  |  |  | X | X | X | X | |