

PROJE TÜRÜ

İnceleme

PROJE ALANI

Yapay Zeka

ÖZET

Asal sayılara kriptolojide nasıl kullanıldığını inceleyeceğiz. Gizli mesaj yollamak isteyen mesajı ile birlikte iki büyük asal sayının çarpımını da yollar. Şifreyi çözmek için, şifre ile birlikte yollanan sayıyı bölen o iki asal bilmek gerekir ki bu da dışarıdan birisi için hemen hemen olanaksızdır. Kriptolojide asal sayıların nasıl kullanıldığını göreceğiz

YÖNTEM

Asal olmayan bir sayı farklı bir şekilde yazılabilir ama asal olan bir sayı başka bir şekilde gösterilemez. Öklid den beri Asal sayıların sonlu olmadığı ispatlamaya çalışılmıştır. Asal sayılarla ilgili olarak Eratosten (M.Ö. 300) kendi adıyla anılan (erato kalburu)bir sayı bulma yöntemi geliştirmiştir. Fermat asalları Mersenne sayıları ve aritmetiğin temel Teoremi den yararlanarak Asal sayıların sırlarını araştırdık. Hipotez: Asal sayıların kriptoloji ve elektronikte kullanılır. İşlemler ; Eratosthenes kalburu 1'den 1000'e kadar olan sayıların içinde asal sayıları bulmak için 50x20 lik bir tablo yapıp sayıları yerleştireceğiz. Daha sonra 2 dışında 2'nin katı olan sayıları işaretleyip asal olmadıklarını belirleyeceğiz. İşaretlenmemiş sayılardan sırasıyla 3'ün, 5'in katlarını işaretleyeceğiz. Bu şekilde devam ettirildiğinde geriye asal sayılar kalacaktır. Geriye kalan bu asal sayılar arasındaki ilişkilerini inceleyeceğiz.

BEKLENEN SONUÇLAR

Bu projemiz de Asal sayıların ne olduğunu, Asal sayıların sonsuz olup olmadıklarını, asal sayılar arasındaki ilişkilerin ne olduğunu ve bir sayının asal olup olmadığını çözümleneceğiz. Asal sayılarla ilgili bilgiler toplandıktan sonra Asal sayıların günümüzde günlük yaşamda, teknolojik alanda, Siber alanda, askeri güvenlik alanlarında ve buna benzer daha başka hangi alanlarda kullanıldıklarını gözlemlemeye çalışacağız. Ortaya çıkan bulgulara göre Asal sayıların çarpanlarına ayrılması güç olduğundan, askeri sistemlerde, hatta internet sayfalarının gizli şifrelerinin düzenlenmesinde kullanılır. Çok büyük sayıların asal olup olmadıkları çok kolay bir şekilde anlaşılabilir. Bu da bize gizlilik sağlamak için rahat bir kullanım alanı sunar.



DANIŐMAN ÖĐRETMENLER

Emrah Kőse

GÖREVLİ ÖĞRENCİLER

Elif Naz Sallan, Esra Zenginler

