YENİ BİR ŞİFRELEME ALGORİTMASI

Celil GÜNDOĞMUŞ, Muhammet Umut DEDE, Hilay SÖNMEZ

Danışman: Yrd. Doç. Dr. Fidan NURİYEVA

ÖZET

Bu projede , konumsal sayı sistemini baz alarak konumsal olmayan bir sayı sistemi önerilmiş ve bu sayı sistemine dayanarak ikilik sistemde verilmiş verilerin yine de ikilik sistemde tekrar kodlanması gösterilerek yeni bir şifreleme algoritması önerilmiştir.[1]

I. GİRİŞ

Bugünün bilgisayarlarında veri 0'lar ve 1'ler şeklinde kodlanmaktadır. 0 ve 1'lerin desenleri sayısal değerleri, alfabedeki karakterleri, sesleri vb. göstermektedir. Bilgisayarlar bütün işlemleri 0 ve 1'ler üzerinde Boolean işlemleri yaparak gerçekleştirmektedir.
Bilgisayarlarda 0 ve 1'lerin desenlerinin gösterimini basitleştirmek, onlar üzerinde işlemleri kolaylaştırmak için farklı (sekizlik, onaltılık, vb.) gösterimler kullanılır ve bunun için de uygun sayı sistemlerinden yararlanılır.

Bu çalışmada önce bilinen sayı sistemlerine değinilmiş, sonra ise ikilik sayı sistemini temel alan yeni bir sayı sistemi önerilmiştir. Bu sayı sistemi kullanılarak ikilik sistemde verilmiş verilerin tekrar ikilik sistemde kodlanması için yeni bir yöntem önerilmiştir. Önerilen yöntem veri şifreleme ve veri sıkıştırma işlemleri için kullanılabilir.

II. SAYI SİSTEMLERİ

Sayı sistemleri genelde konumsal (pozisyonel) ve konumsal olmayan (pozisyonel olmayan sistemler) olmakla iki gruba ayrılır.

A. Konumsal olmayan sayı sistemleri: Konumsal olmayan sayı sistemlerine en yaygın örnek sıfır ve basamak kavramı olmayan Roma rakamları günümüzde çe¸sitli amaçlar için kullanılmaktadır.
B. Konumsal sayı sistemleri: Bu sistemde her sembölün konumu ve şekli önem taşımaktadır. Konumsal sistemlerde genellikle tüm sayı sistemleri aynı ilkeye göre oluşturulmaktadır: sayı sisteminin tabanı olan *p* sayısı belirlenir ve her hangi *N* sayısı bu sayının üslerinin
(0; *p* - 1) arasında değişen a_i katsayılarıyla (basamak) çarpımıyla elde edilir:

$$N = a_k p^k + a_{k-1} p^{k-1} + \cdots + a_2 p^2 + a_1 p^1 + a_0$$

III. YENİ SAYI SİSTEMLERİ

Aşağıda önerilen N^k sistemi (*k* = 1, 2, 3, …) taban olarak konumsal sayı sistemini (ikilik sayı sistemi) kullanılmasına rağmen genel olarak konumsal olmayan sayı sistemidir.
Bu sistemde de sıfır değeri yoktur.
Tabanda ise farklı basamaklı ikilik sayılar kullanılabilir, burada "*k*" tabanı göstermektedir.
İkilik sistemde bir basamaklı sayılar iki tanedir: 0 ve 1.
Burada "0", "1+" anlamına gelmektedir.
Örneğin:
$(1)^1_N = (1)_{10}$
$(0)^1_N = (1+)_{10}$
$(01)^1_N = 1+1 = 2_{10}$
$(00)^1_N = 1+1 = (2+)_{10}$

Bu kural ile bir basamaklı tabanla sonsuzluğa kadar devam edebileriz.
İkilik sistemde iki basamak ile dört sayı gösterilebilir:
$(00)_2 = 0_{10}$ $(01)_2 = 1_{10}$ $(10)_2 = 2_{10}$ $(11)_2 = 3_{10}$

Bu sayılar kullanılarak N^2 sisteminde sonsuza kadar sayılar gösterilebilir:
$(01)^2_N = 1_{10}$ $(0001)^2_N = 3+1 = 4_{10}$ $(0001)^2_N = 3+1 = 4_{10}$

$(10)^2_N = 2_{10}$ $(0010)^2_N = 3+2 = 5_{10}$ $(000001)^2_N = 6+1 = 7_{10}$

$(11)^2_N = 3_{10}$ $(0011)^2_N = 3+3 = 6_{10}$ $(000010)^2_N = 6+2 = 8_{10}$

$(00)^2_N = (3+)_{10}$ $(0000)^2_N = 3+3+ = (6+)_{10}$ $(000011)^2_N = 6+3 = 9_{10}$

Böylece N^k sistemindeki sayılar için aşağıdaki genel formülü yazabiliriz.

$$(\underbrace{\underbrace{0\ldots0}_{k}\ \underbrace{0\ldots0}_{k}\ \ldots\ \underbrace{0\ldots0}_{k}\ \underbrace{a_{k-1}\ldots a_0}_{k}}_{m/k})^k_N = (\frac{m}{k}-1).(2^k-1) + (a_{k-1}2^{k-1} + a_{k-2}2^{k-2} + \ldots + a_1.2 + a_0),\ m : \text{tüm bitlerin sayısı}$$

IV. YENİ ŞİFRELEME YÖNTEMİ

Önerilen şifreleme yöntemi "0" ve "1" lerden oluşan dizinin yukarıda anlatılan sayı sistemini kullanarak tekrar kodlanmasına dayanmaktadır. Bu yönteme göre tekrar kodlama için ilk önce verilmiş dizinin ilk elemanı yazılır ve sonra bu elemanın ardışıklık sayısı yazılır ve bu kural ile dizinin sonuna kadar devam ettirilir.
Örneğin, varsayalım ki, "0" ve "1" lerden oluşan aşağıdaki dizi verilmiştir ve 2 basamaklı N^2 sistemini kullanalım.

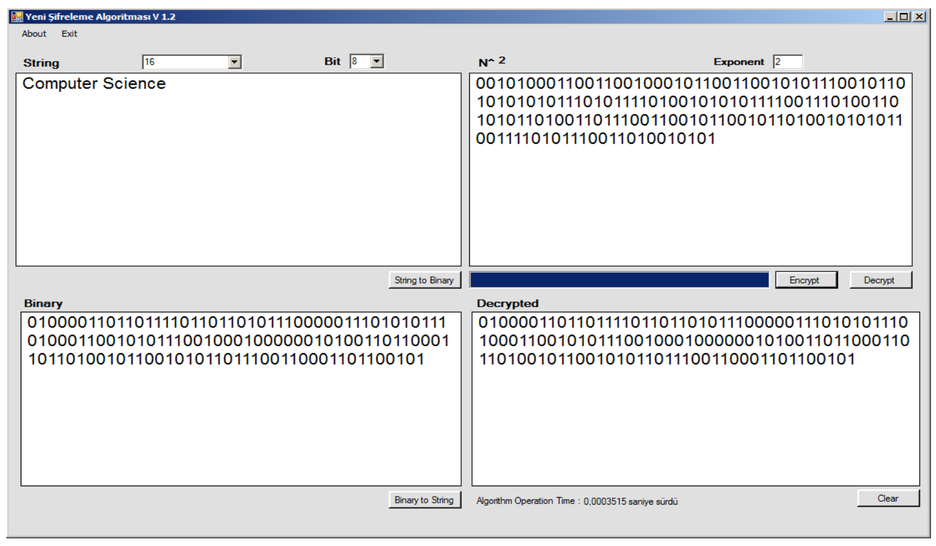
$$\underbrace{000}_{3}\underbrace{111}_{3}\underbrace{00}_{2}\underbrace{1}_{1}\underbrace{0000}_{4}\underbrace{11}_{2}\underbrace{00000}_{5}\underbrace{111111}_{6}$$

Bu dizini önerilen yöntemle tekrar kodlayalım. İlk eleman "0" olduğu için yeni kodda ilk önce "0" ve sonra burada ardışık "0"ların sayısı 3 oldu˘gu için 11 yazılacak ve böyle devam ederek bütün dizini kodlayalım.

$$0\ \underbrace{11}_{3}\ \underbrace{11}_{3}\ \underbrace{10}_{2}\ \underbrace{01}_{1}\ \underbrace{0001}_{4}\ \underbrace{10}_{2}\ \underbrace{0010}_{5}\ \underbrace{0011}_{6}$$

Önerilen Şifreleme yöntemi "0" ve "1" lerden oluşan dizinin bir kaç defa farklı tabanlı yeni önerilmiş sayı sistemlerini kullanarak yukarıda anlatılan şekilde tekrar kodlanmasına dayanmaktadır.
Bütün dizini kodlamamız bittiğinde "000111001000011000000111111" dizisinin şifrelenmiş hali "011111001000110001000011" elde etmiş oluruz.
Sonra bu alınmış dizini başka bir sistemde, örneğin N^5 sisteminde tekrar kodlayarak yeni bir dizi, daha sonra bu dizini de diğer bir sistemde, örneğin N^3 sisteminde kodlayarak öncekinden farklı bir dizi alırız ve bu şekilde devam ederek 0 ve 1 lerden oluşan yeni diziler alacağız.
En sonda aldığımız dizi şifrelenmiş metin olacak. Metnin şifresini çözmek için işlemleri tersinden yapmalıyız.

V.UYGULAMA VE SONUÇ



Bu çalışma ile önerilen yeni bir sayı sistemini kullanılınarak, yeni bir kodlama algoritması geliştirilmiştir. Bu geliştirilen yöntemi kullanarak yeni şifreleme algoritması önerilmiştir.
Bu algoritma simetrik bir algoritmadır. RSA açık anahtarlı sistemi ile birlikte kullandıldığında Hibrid bir sistem önerilmiş olur.
İlerleyen dönemde algoritmanın belirlenen açıkları kapatılarak güvenli hale getirilmesi üzerine çalışmalar yapılması planlanmaktadır.

KAYNAKÇA

1. Çimen, C., Akleylek, S., Akyıldız, E., (2007), Şifrelerin Matematiği Kriptografi, ODTÜ – Ankara.
2. Nuriyev, U., Nuriyeva, F., Sadık T., (2016), On a New Number System, Proceedings of the International Conference on Computer Science and Engineering (UBMK 2016), Namık Kemal University, Tekirdağ, Turkey, October 20-23, 2016, pp. 825-827.
3. Schneier, B., (1996), Applied Crpytography – Protocols, Algorithms and Source Code in C, Wiley-India.
4. WEB_1. (2016). https://csrc.nist.gov/