Tiny Encryption Algorithm (TEA)

Ad: Yunus Emre

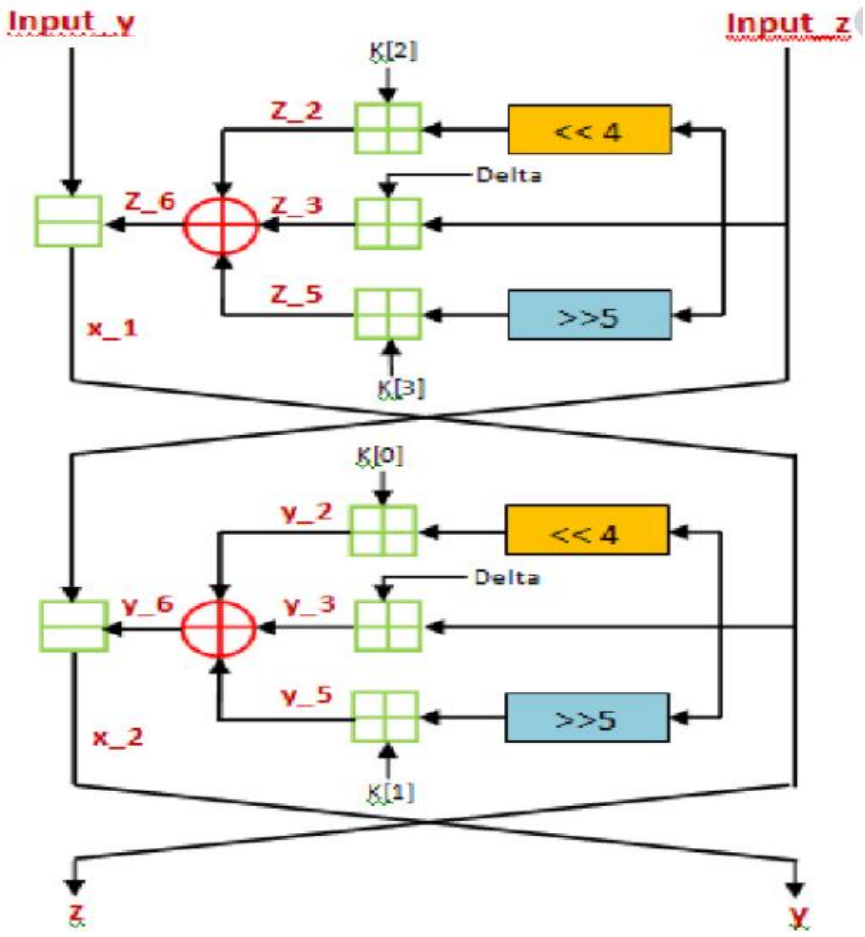
Soyad: Tosun

Numara: G171210013

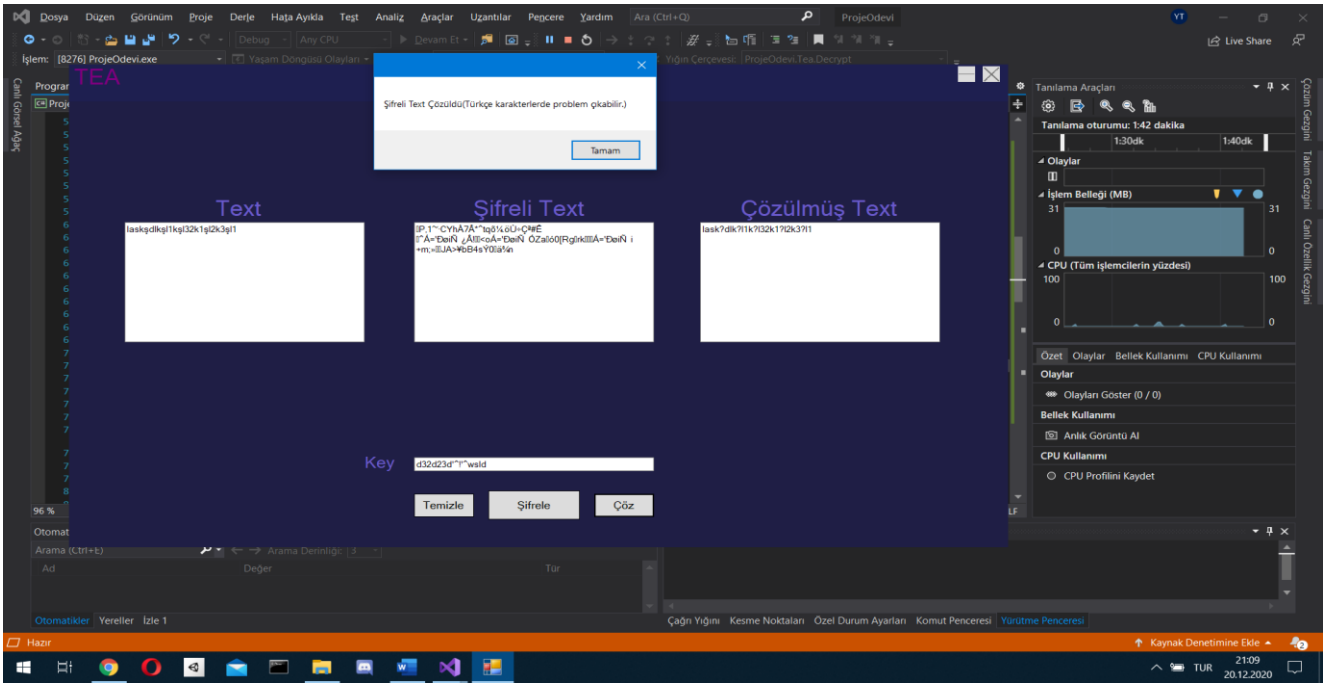
TEA:

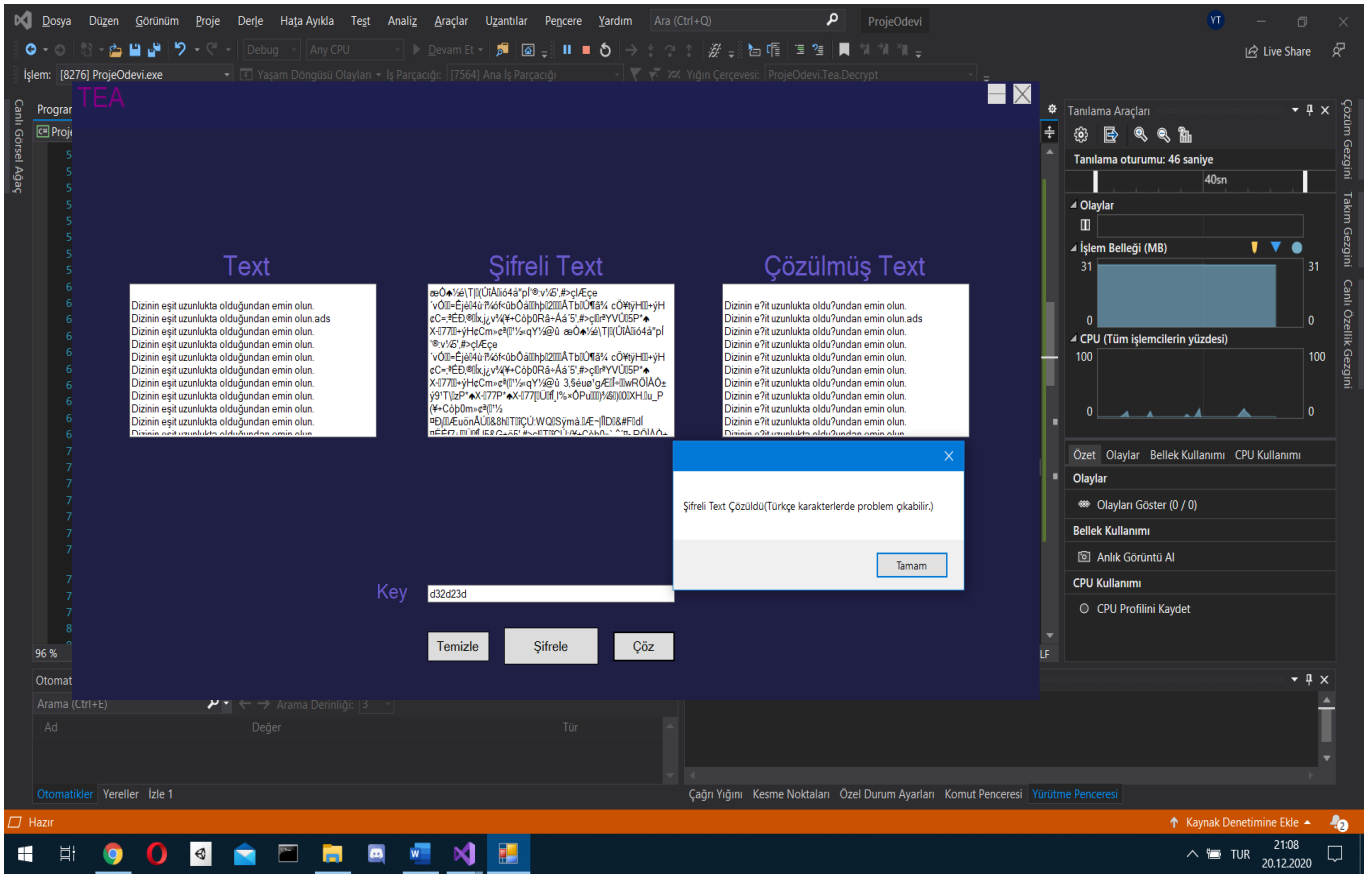
TEA, var olan en hızlı şifreleme algoritmalarından biridir.
Kod boyutunun kısıtlı yer kaplamasından dolayı gömülü sistemlerde kullanımı oldukça popülerdir.
Minimum hafıza ile maksimum hız elde edilmeye çalışılır.
64 bitlik bloklar kullanır. Bu 64 veri bloğunu 128 bitlik anahtar ile şifreler.
128 bitlik K anahtarı 32 bitlik bloklara bölünür.
Değişebilmesine rağmen 64 adet Fietsel Turu -- 32 döngü tavsiye edilmektedir.
2 Fiestel turu = 1 döngü) Terminolojide 2'li yani çift tura Cycle = Döngü denmektedir.
TEA, Shannonun ve güvenli bir blok şifreleme için gerekli olan karıştırma(confusion) ve yayılma (diffusion) özelliklerini sağlayan önemli bir şifreleme yöntemidir.
Karıştırma(confusion) şifreli metin ve açık metin arasındaki ilişkiyi gizlemeyi amaçlarken, yayılma(diffusion) açık metindeki izlerin şifreli metinde sezilmemesini sağlamak için kullanılır.
Bu algoritma bu işlemleri yapmak için mantıksal operatörleri kullanır. (And,XOR,Shift...)

TEA Diyagramı:



Uygulama Çıktıları:





Not:
Bu şifreleme algoritmasında şifrelenmiş veri 8 baytın katı olmalıdır.

8 baytın katı olmadığı durum: