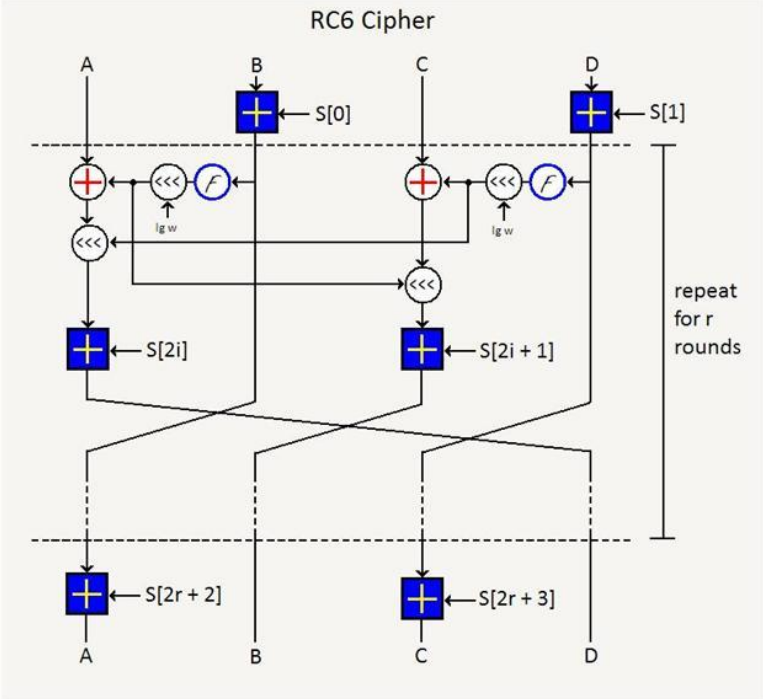
RC6 ŞİFRELEME ALGORİTMASI

Ron Rivest, Matt Robshaw, Ray Sidney ve Yiqun Lisa Yin tarafından 1998 yılında RC5 şifrelemesinin bir uzantısı olarak geliştirilen AES yarışmasının finalisti olan bir kriptoloji yöntemidir. Anahtar boyutu 128, 192 veya 256 bit olabilir. Blok boyutu 128 bit kadardır. Yapısal olarak basit, hızlı ve günümüzde halen güvenli olarak düşünülmektedir.



RC6 Güvenlik Analizi

Kuvvetli analiz en etkin bilinen ataklar temeline dayanmaktadır.

- Lineer kriptoanaliz
- Diferansiyel kriptoanaliz

Anahtar Genişletme'nin Güvenliği

Anahtar genişletme prosedürü RC5 ile aynı şekildedir. Henüz bilinen bir zayıflık içermemektedir.
Bilinen zayıf anahtar içermemektedir
Bilinen ilişkili anahtar saldırısı içermemektedir
Çevrim anahtarları işlenmiş anahtarın rassal bir fonksiyonu gibi görünmektedir.
Anahtar genişletme tamamı ile tek yönlüdür. Çevrim anahtarlarından işlenmiş anahtarın sonucuna ulaşılması oldukça zordur.

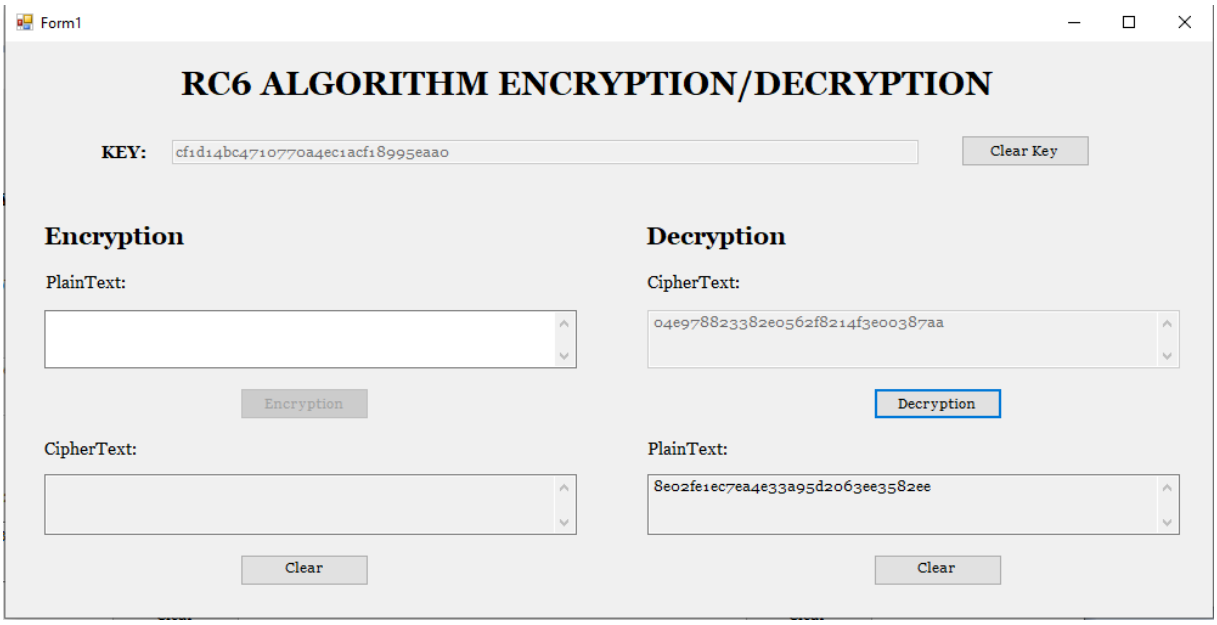
Sonuç

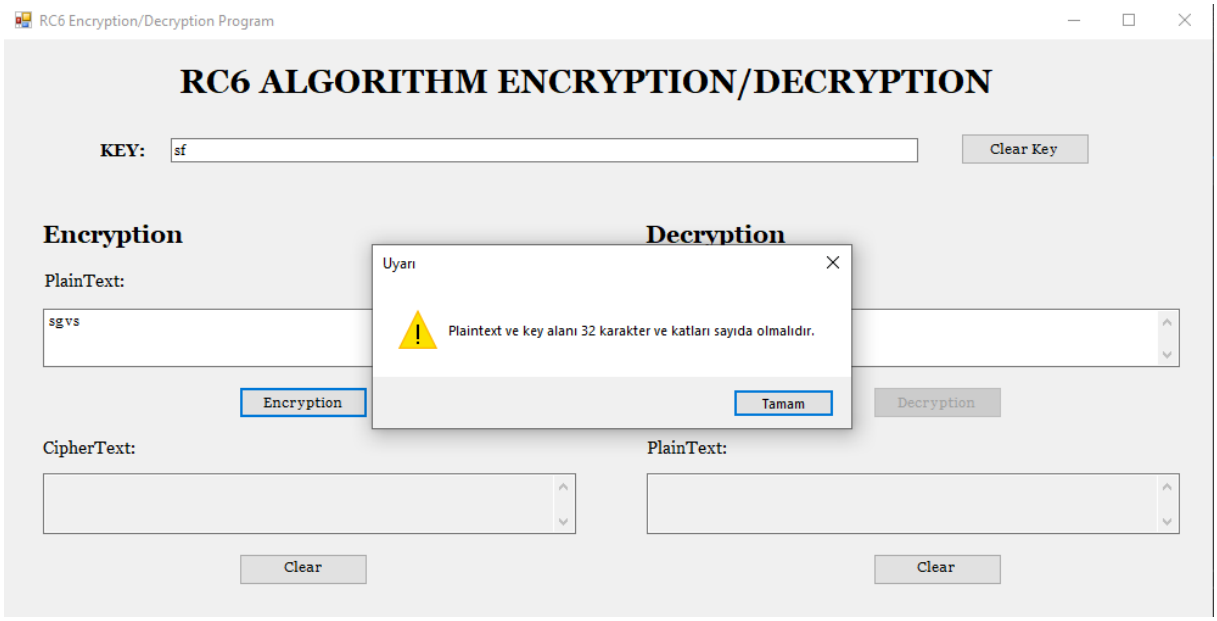
RC6, AES gereksinimlerinden daha fazlasını kapsar.RC6, kolay, hızlı ve güvenlidir.
Kuvvetli şifreler üretmek için oldukça basit bir yapı içermektedir.

PROGRAMIN TANITIMI

C# diliyle yazılmış, dışarıdan alınan key, plaintext ve ciphertext değerlerine göre gerekli işlemleri yapan, kullanıcıya girdiği text verisine uygulanan encryption ve decryption işlemlerinin sonuçlarını döndüren bir programdır.

Proje Ekran Çıktıları


Form1
RC6 ALGORITHM ENCRYPTION/DECRYPTION
KEY:
cf1d14bc4710770a4ec1acf18995eaa0
Clear Key
Encryption
PlainText:
Encryption
CipherText:
Clear
Decryption
CipherText:
04e97882382e0562f8214f3e00387aa
Decryption
PlainText:
8e02fe1ec7ea4e33a95d2063ee3582ee
Clear


RC6 Encryption/Decryption Program
RC6 ALGORITHM ENCRYPTION/DECRYPTION
KEY:
sf
Clear Key
Encryption
PlainText:
sgvs
Encryption
CipherText:
Clear
Uyarı
Plaintext ve key alanı 32 karakter ve katları sayıda olmalıdır.
Tamam
Decryption
PlainText:
Clear