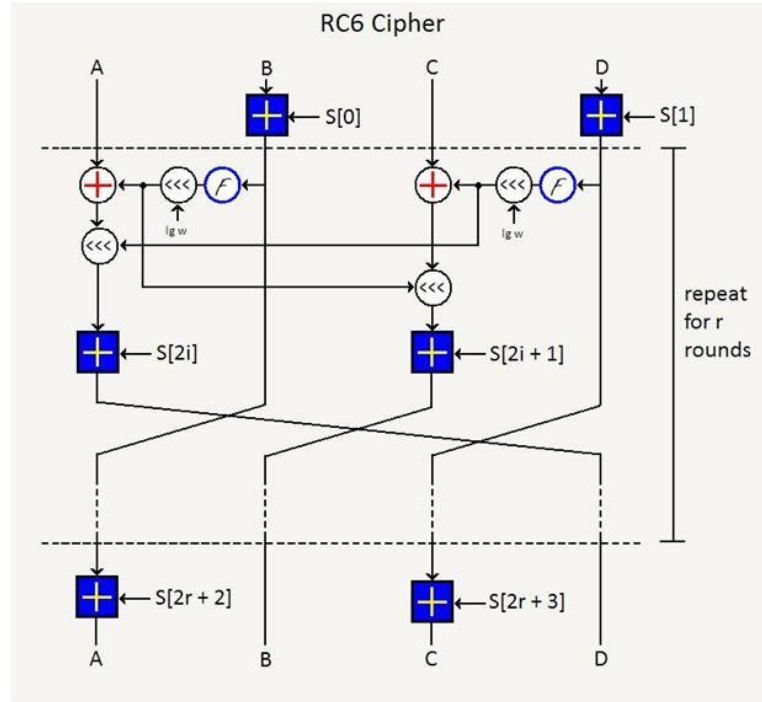


RC6 ŞİFRELEME ALGORİTMASI

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 kriptanaliz
- Diferansiyel kriptanaliz

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

The screenshot shows a Windows application window titled "Form1" with the title bar containing standard minimize, maximize, and close buttons. The main content area has a light gray background and is titled "RC6 ALGORITHM ENCRYPTION/DECRYPTION" in bold black text. Below the title, there is a "KEY:" label followed by an empty text input field and a "Clear Key" button. The interface is divided into two columns: "Encryption" on the left and "Decryption" on the right. Each column has a "PlainText:" label above an empty text input field with a vertical scrollbar. Below each input field is a button labeled "Encryption" and "Decryption" respectively. At the bottom of each column is a "CipherText:" label above another empty text input field with a vertical scrollbar, followed by a "Clear" button.

This screenshot shows the same application window after an encryption operation. The "KEY:" field now contains the hexadecimal string "cf1d14bc4710770a4ec1acf18995eaa0". In the "Encryption" column, the "PlainText:" field contains "8e02fe1ec7ea4e33a95d2063ee3582ee", the "Encryption" button is highlighted with a blue border, and the "CipherText:" field contains "04e978823382e0562f8214f3e00387aa". The "Decryption" column remains empty, with its "CipherText:" field empty and its "PlainText:" field also empty. All other elements, including the "Clear Key" and "Clear" buttons, are present and unchanged.

Form1

RC6 ALGORITHM ENCRYPTION/DECRYPTION

KEY:

Encryption

PlainText:

CipherText:

Decryption

CipherText:

PlainText:

RC6 Encryption/Decryption Program

RC6 ALGORITHM ENCRYPTION/DECRYPTION

KEY:

Encryption

PlainText:

CipherText:

Decryption

PlainText:

Uyarı

! Plaintext ve key alanı 32 karakter ve katları sayıda olmalıdır.