SİMETRİK KRIPTO ALGORİTMALARININ .NET PLATFORMUNDA GERÇEKLENMESİ VE PERFORMANS ANALİZLERİ

Ali Sağat¹ ve Murat Aydos²

¹ Ar. Gör. Pamukkale Üniversitesi Bilgisayar Mühendisliği Bölümü
Morfoloji Binası Kınıklı Kampüsü, 20017 DENİZLİ
asagat@pamukkale.edu.tr

² Yrd. Doç. Dr., Pamukkale Üniversitesi Bilgisayar Mühendisliği Bölümü
Morfoloji Binası Kınıklı Kampüsü, 20017 DENİZLİ
maydos@pamukkale.edu.tr

Anahtar Kelimeler: Güvenlik, Kripto, .Net
Oturum Konusu: Güncel Bilgisayar Bilimleri, Yazılım Donanım

1. GİRİŞ


Bilgisayarların ve özellikle internetin kullanılamaya başlanmasıyla sahisal ortamındaki bilgilerin güvenliği ve bilgisayar uygulamalarında kriptografya kullanımı da gündeme gelmiş; bu amaçla değişik kriptografik metotları içeren kriptografik algoritmalar geliştirilmştir. Basit Sezar Şifrelemesinden, günümüz modern açık anahtarlı şifreleme tekniklerine gelindiğinde, özellikle sahisal teknolojinin gelişmesiyle, geçmişte geliştirilen algoritmaların gizliliğine dayanan sistemlerin yerini, güçlü algoritmalar ve matematiksel metotlara dayanan sistemler almıştır.

Bu çalışmaların hedefi, ana amacımız olan bir kripto kütüphanesi için gerekli olan kodların ilk kısmını oluşturmak. Algoritma olarak, modern kripto sistemlerin temelini teşkil eden ve hala kullanım alanlarına sahip olan simetrik kripto algoritmalarından DES, 3DES, RC4, RC5, ve RC6 algoritmalarını ele aldık.¹²

2. SİMETRİK KRIPTO ALGORİTMALAR

Simetrik kriptodaki gönderici ve alıcı taraflar arasında aynı bir tek anahtar kullanır. Algoritma, bu gizli anahtarın sadece iki taraf tarafından bilindiği temeli üzerinde şifreleme ve çözme amacı ile çalışır. Gönderilecek metin bu anahtarla gönderici tarafından şifrelenir ve yine bu anahtarla alıcı tarafından şifreli metin açılır ve güvenli iletişim sağlanmış olur. Saldırıya şifreli metne sahip olabilir ama gizli anahtara sahip olmalıdır asıl metni elde edemez.

\[ C = E_K(P) \]
\[ P = D_K(C) \]
Şekil 1. Simetrik Kripto

Simetrik kripto algoritmaları veriye iki farklı şekilde işler: Ağız veya blok şifreleme. Veri, ağız şifrelemede binary XOR operatörü kullanılarak bit bit veya byte byte şifrelenir. Blok şifrelemede ise veri, bloklar halinde (mesela 64 bitlik), belirli sayıda çevrilmelerde, alt anahtarlar alt metinlerle şifreleme fonksiyonuna sokularak şifrelenir.\(^{1,2}\)

2.1. DES ve 3DES

DES, en iyi bilinen simetrik kripto blok şifreleme algoritmasıdır. 56 bit (parity bitleriyle 64 bit) anahtar, 64 bit blok uzunluğudur. 16 çevrim sayısına sahiptir. Deşifreleme, alt anahtarların ters sırada kullanılmasıyla \((K_{16};K_{15};\ldots;\ldots;K_{1})\) aynı algoritma ile sağlanır.\(^{1,2,3,4,5}\)

3DES, 168 (56x3) bit anahtar, 64 bit blok uzunluğunu ve DES ile aynı şifreleme algoritmasını kullanır. 168 bitlik anahtar 56 bitlik iki ya da üç anahtar kullanılarak elde edilir. İki anahtarı; \(C = E_{K_3}[D_{K_2}[E_{K_1}[P]]]\) ve üç anahtarı; \(C = E_{K_3}[D_{K_2}[E_{K_1}[P]]]\).\(^{2,3}\)

2.2. RC4

En geniş şekilde kullanılan ağız şifreleme tekniğidir. Anahtar uzunluğu 1-256 byte \((8\,\text{-}2048\text{ bit})\)'tır. 1 byte uzunluğundaki akan metinleri, 1 byte uzunluğundaki alt anahtarlara XOR'layarak şifreleme yapılır. Deşifreleme, aynı algoritma ve anahtar kullanılarak gerçekleştirilir.\(^{2,6}\)

2.3. RC5 ve RC6

RC5, blok şifreleme algoritmaları olup değişken blok uzunluğuna (blok uzunluğu = 2 word) \(w = 16, 32, 64\) bit; değişken çevrim sayısına \(r = 0, 1, \ldots, 255\) ve değişken anahtar uzunluğuna \(b = 0, 1, \ldots, 255\) byte sahiptir. RC5-w/r/b şeklinde gösterilir.\(^{1,2,3,4,5}\)

RC6, RC5 gibi parametrik bir algoritmadır, RC6-w/r/b olarak tanımlanır. Anahtar düzenleme algoritmaları RC5 ile aynıdır fakat anahtar sayısı fazladır.\(^{1,2,3,4,5}\)

3. NET PLATFORM VE C#


Net framework yapısı kolay, güvenli ve genişleyebilir bir yapıda internet uygulamaları, mobil web uygulamaları ve web servisleri için yazılım geliştirmeyi sağlar. .Net CLR her
donanım üzerinde çalışabilen kodlar geliştirilebilmeyi, minimum kaynak kullanımını, ayarlanabilir performansı ve aygıt, işlemci ve işletim sistemi bağımsızlığını sağlar.


4. SONUÇ


![Simetrik Kripto Algoritmaları Performans Karşılaştırması](image)

5. Fast Implementations of AES Candidates, Kazumaro, 3rd AES Candidate Conference, NY, 2000