SİMETRİK KRİPTO ALGORİTMALARININ .NET PLATFORMUNDA GERÇEKLENMESİ VE PERFORMANS ANALİZLERİ

Ali Sağat[1] ve Murat Aydos[2]

[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

Kişisel bilgisayarlar ve İnternet, bilgi dünyasını yeniden şekillendirmiş ve sayısal ortamı, günümüz insanının ayrılmaz bir parçası haline getirmiştir. Adım attığı hemen her yerde bir sayısal ortamla karşılaşmakta; e-Ticaret, e-Bankacılık, e-Devlet, e-Eğitim, e-Seçim gibi kavramlar ve uygulamalar, hemen her gün modern insanın hayatına bir parça daha girmektedir. Bireysel güvenliğine binlerce yıldır yatırım yapan insanoğlunun, modern dünyanın vazgeçilmezlerinden olan sayısal ortama güvenlik yaklaşımları geliştirmesi yadsınmaz bir gerçektir.

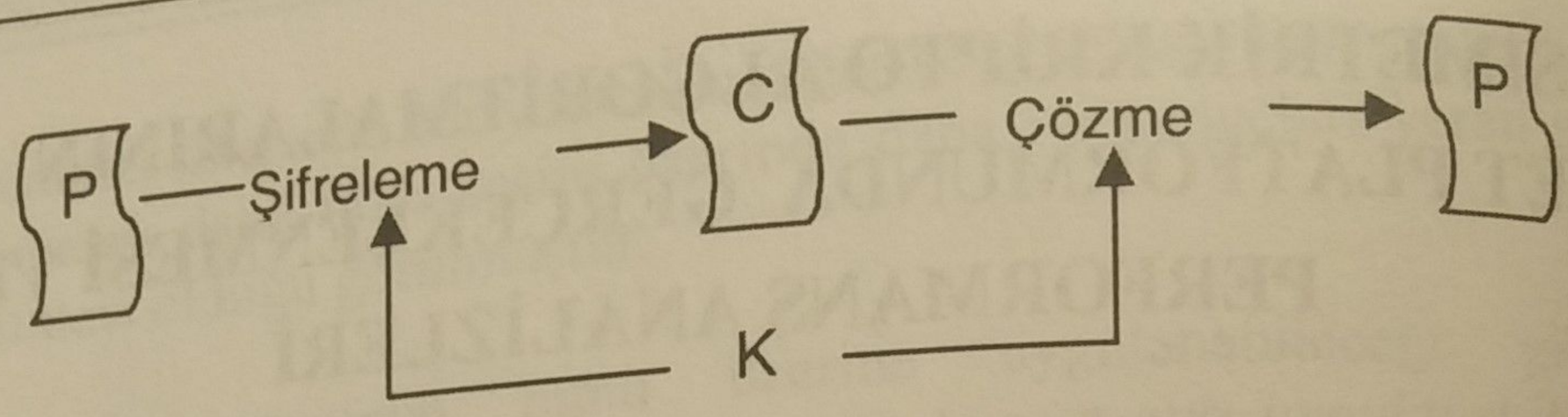
Bilgisayarların ve özellikle internetin kullanılmaya başlanmasıyla sayısal ortamdaki bilgilerin güvenliği ve bilgisayar uygulamalarında kriptografi kullanımı da gündeme gelmiş; bu amaçla değişik kriptografik metotları içeren kriptografik algoritmalar geliştirilmiştir. Basit Sezar Şifrelemesinden, günümüz modern açık anahtarlı şifreleme tekniklerine gelindiğinde, özellikle sayısal teknolojinin gelişmesiyle, geçmişte geliştirilen algoritmanın gizliliğine dayanan sistemlerin yerini, güçlü algoritmalara ve matematiksel metotlara dayanan sistemler almıştır.

Bu çalışmamızın hedefi, ana amacımız olan bir kripto kütüphanesi için gerekli olan kodların ilk kısmını oluşturmak. Algoritma olarak, modern kripto sistemlerinin temelini teşkil eden ve hala kullanım alanlarına sahip olan simetrik kripto algoritmalarından DES, 3DES, RC4, RC5, ve RC6 algoritmalarını ele aldık.[1,2]

2. SİMETRİK KRİPTO ALGORİTMALARI

Simetrik kriptoda gönderici ve alıcı taraflarda aynı bir tek anahtar kullanır. Algoritma, bu gizli anahtarın sadece bu iki taraf tarafından bilindiği temeli üzerinde şifreleme ve çözme amaçlı çalışır. Gönderilecek metin bu anahtarla gönderici tarafından şifrelenir ve yine bu anahtarla alıcı tarafından şifreli metin açılır ve güvenli iletişim sağlanmış olur. Saldırgan şifreli metne sahip olabilir ama gizli anahtara sahip olmadıkça asıl metni elde edemez.

$$C = E_K(P) \qquad P = D_K(C)$$



Şekil 1. Simetrik Kripto

Simetrik kripto algoritmaları veriyi iki farklı şekilde işler: Akış veya blok şifreleme. Veri, akış şifrelemede binary XOR operatörü kullanılarak bit bit veya byte byte şifrelenir. Blok şifrelemede ise veri, bloklar halinde (mesela 64 bitlik), belirli sayıda çevrimlerde, 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 ($K_{16};K_{15};:::;K_1$), 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 anahtarlı; $C = E_{K1}[D_{K2}[E_{K1}[P]]]$ ve üç anahtarlı; $C = E_{K3}[D_{K2}[E_{K1}[P]]]$. [2,3,4]

2.2. RC4

En geniş şekilde kullanılan akış şifreleme tekniğidir. Anahtar uzunluğu 1-256 byte (8-2048 bit)'tır. 1 byte uzunluğundaki akan metinleri, 1 byte uzunluğundaki alt anahtarlarla XOR'layarak şifreleme yapılır. Deşifreleme, aynı algoritma ve anahtar kullanılarak gerçekleştirilir.[2,6]

2.3. RC5 ve RC6

RC5, blok şifreleme algoritması olup değişken blok uzunluğuna (blok uzunluğu = 2 word) w = 16, 32, 64 bit; değişken çevrim sayısına r = 0,1, . . . , 255 ve değişken anahtar uzunluğuna b = 0,1, . . . , 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 algoritması RC5 ile aynıdır fakat anahtar sayısı fazladır. [1,2,3,4,5]

3. NET PLATFORMU VE C#

Microsoft .NET, insan, bilgi , sistem ve araçları birleştiren; WEB servislerini baz alarak yüksek düzeyde yazılım entegrasyonu sağlayan bir yazılım teknolojisidir. .Net bileşenleri; Web servisleri, istemciler, sunucular ve geliştirme araçları olup Microsoft Visual Studio .NET ve Microsoft .NET Framework'ün yazılım geliştiriciler için, bir çok modern programlama dilini de kapsayan, komple bir çözüm sunması çalışmamızda bu platformu seçmemizdeki en önemli etkendir.

Net framework yapısı kolay, güvenli ve genişleyebilir bir yapıda internet uygulamaları, mobil web uygulamaları ve web servisleri için yazılım geliştirmeyi sağlar. .Net CLR her

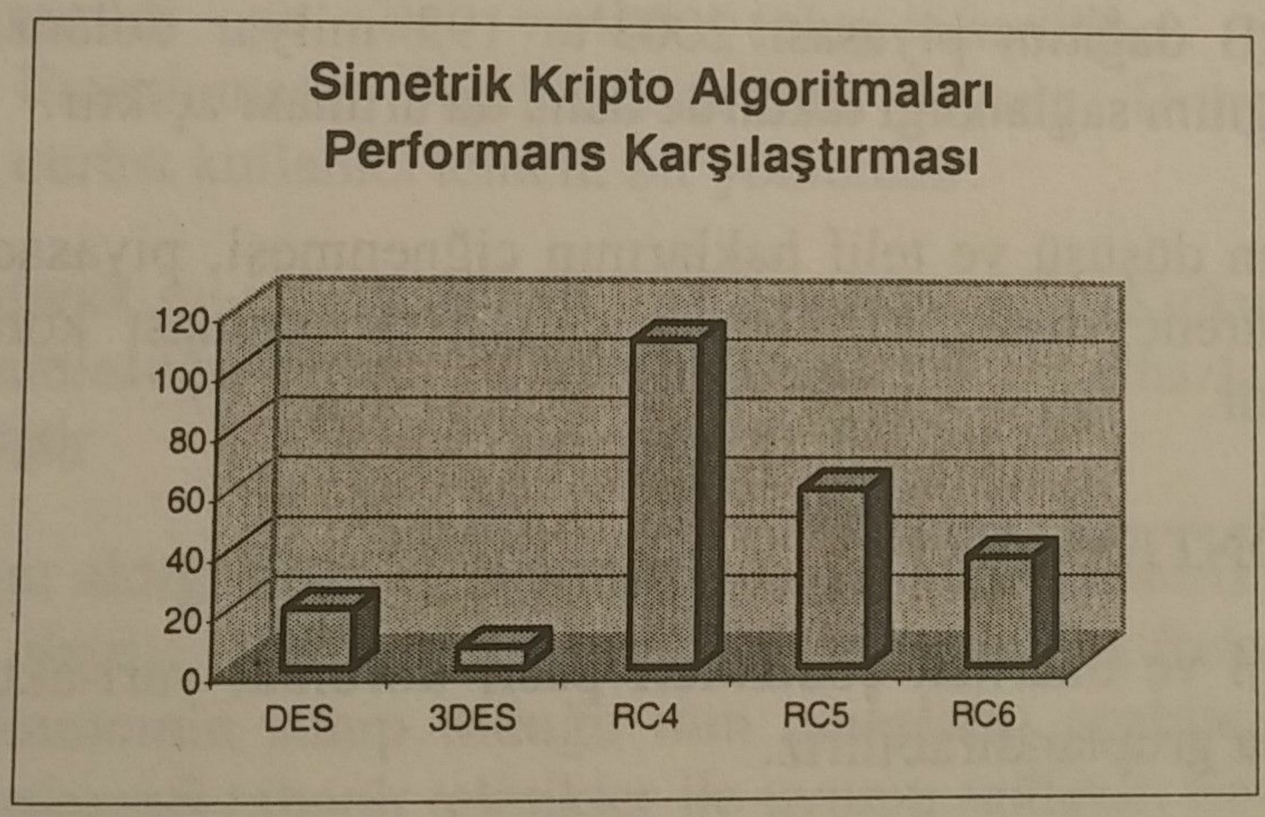
donanım üzerinde çalışabilen kodlar geliştirilebilmeyi, minimum kaynak kullanımını, ayarlanabilir performansı ve aygıt, işlemci ve işletim sistemi bağımsızlığını sağlar.

C#, C ve C++'dan türetilmiş, basit ve modern bir nesneye dayalı programlama dilidir. C ve C++ programcılarının kolaylıkla adapte olabileceği bir dildir. C# geliştirebilmek için C ve C++'ın gücünü ve Visual Basic'in basitliğini önermektedir.

4. SONUÇ

Bu çalışma ile, modern kripto sistemlerinin temelini teşkil eden ve hala kullanım alanlarına sahip olan simetrik kripto algoritmalarından DES, 3DES, RC4, RC5, ve RC6 algoritmaları baz alınıp gerçeklenerek, uzun vadede oluşturulacak olan açık anahtarlı kripto algoritmalarını da içerecek olan bir kripto kütüphanesinin ilk adımı tamamlanmış oldu. Yukarıda açıkladığımız simetrik kripto algoritmaları C# programlama dili kullanılarak .Net platformunda gerçeklendi; kodlandı. Kodların kriptografik standartlara uygunluğu ve test vektörleri kullanılarak programların doğrulukları test edildi. Son olarak da .Net platformunda C# programlama diliyle oluşturulan kodların zamanlamaları ölçülerek performanslarını incelendi. Kodların anlaşılırlığı öncelikli bir kriter olarak ele alınırken performanstan taviz vermemeye çalışıldı. Performans parametreleri olarak çalışma hızı ve hafıza kullanımı temel alındı. Çalışma hızlarında da anahtar düzenleme hızı ve şifreleme hızı ayrı ayrı ele alındı. [1,2,3,5,7]

Kodlar Microsoft Development Environment 2003 ve .Net Framework 1.1 ortamında Microsoft Visual C# .Net kullanılarak; Intel Pentium M 1.6 GHz işlemcili, 512 MB Ram olan bir makine üzerinde yazıldı ve derlendi.



1. Applied Cryptography, Schneier B.,John Wiley & Sons, New York,1996

2. Cryptography and Network Security, Stallings W., Prentice Hall, New Jersey, 2003

3. NIST National Institute of Standards and Technology's web site, http://www.nist.gov/

4. Crypto++™ Library 5.1, http://www.eskimo.com/~weidai/cryptlib.html

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

6. Efficient Implementation of Large Stream Cipher Systems, Palash, CACR Univ.of Waterloo, 2001

7. Evaluating Cryptosystems, Paul Kocher, San Francisco, 2002.