International Journal of Innovative Research in Education

Volume 04, Issue 3, (2017) 148-154

www.ijire.eu

Performance analysis of AES, DES, and RSA Algorithms for computer science education

Bilgisayar mühendisliği eğitiminde AES, DES, ve RSA ve SEA algoritmalarının performans analizi

Abdülkadir Tepecik*, Bilgisayar Mühendisliği bölümü, Mühendislik Fakültesi, Yalova Üniversitesi, 77200, Yalova, Türkiye

Abidin Doğan, Bilgisayar mühendisliği bölümü, Mühendislik Fakültesi, Yalova Üniversitesi, 77200, Yalova, Türkiye

Melike Sardoğan, Bilgisayar mühendisliği bölümü, Mühendislik Fakültesi, Yalova Üniversitesi, 77200, Yalova, Türkiye

Müfit Çetin, Bilgisayar mühendisliği bölümü, Mühendislik Fakültesi, Yalova Üniversitesi, 77200, Yalova, Türkiye

Suggested Citation:

Tepecik , A., Doğan, A., Sardoğan, M., & Cetin, M. (2017). Comparative examination of rsa and SEA algorithms for computer engineering education. *International Journal of Innovative Research in Education. 4*(3),148-154.

Gönderim 24 Mayıs 2017; Düzeltme 30 Temmuz 2017; Kabul edilen 20 Eylül 2017.

Seçim ve hakem süreci sorumlusu Assoc. Prof. Dr. Zehra Ozcinar Atatürk Öğretmen Akademisi, Kıbrıs.

Abstract

Nowadays, due to the position of technology, the need for cyber security has increased considerably. The most personal information of people is easily accessible on the internet. Information such as banking information, personal information, state secrets, military secrets need to be protected. Many encryption algorithms have been developed to protect people's personal information and state secrets. In this article, comparison of RSA, AES, DES, algorithms is done.. These comparisons were made considering the speed of the algorithms.

Keywords: DES, RSA , SEA , algorithm analysis, performance evaluation, big o.

*ADDRESS FOR CORRESPONDENCE: **Abdülkadir Tepecik,** Bilgisayar Mühendisliği bölümü, Mühendislik Fakültesi, Yalova Üniversitesi, 77200, Yalova, Türkiye

E-mail adres: atepecik@yalova.edu.t

Özet

Günümüzde teknolojinin geldiği konum sebebiyle siber güvenliğe ihtiyaç oldukça artmış bulunmaktadır. İnsanların en kişisel bilgilerine internet üzerinden kolayca ulaşılabilmektedir. Banka bilgileri, özlük bilgileri, devlet sırları, askeri sırlar gibi bilgilerin korunmaya ihtiyacı vardır. İnsanların kişisel bilgilerini ve devlet sırlarını koruma altına almak için bir çok şifreleme algoritması geliştirilmiştir. Bu makalede şifreleme algoritmalarından RSA, AES, DES, algotirmalarının karşılaştırılması yapılmıştır. Bu karşılaştırmalar algoritmaların hızları göz önünde bulundurularak yapılmıştır.

Anahtar Kelimeler: DES, RSA , SEA , algoritma analizi, performans hesaplama, büyük-o.

1. Giriş

Teknolojinin gelişmesi ve internet kullanımının artması sebebiyle günümüzde siber güvenliğe çok fazla ihtiyaç duyulmaktadır. Kara, hava ve denizden sonra yeni savaş alanının siber dünya olması beklenmektedir. Bu yüzden devletler ve kişiler kendilerini koruma altına almak zorundadırlar.

Siber alanda güvenliği sağlayabilmek için kriptoloji bilimi geliştirilmiştir. Kriptoloji, iki bölüme ayrılır:Kriptografi ve kriptoanaliz (Yerlikaya, 2006). Kriptografi şifreleme ile ilgilenir, kriptoanaliz ise şifre çözme ile. Bu makalede kriptografi algoritmalarından RSA, AES ve DES incelenmiş ve karşılaştırılmış bulunmaktadır.

1978'de, Ron Rivest, Adi Shamir, and Leonard Adleman, daha güvensiz bir algoritma olan NBS'nin yerine geçmesi için bir kriptografik algoritma tanıttılar (Milanov, 2009). RSA, güvenliği tam sayıları çarpanları ayırmanın zorluğuna dayanan bir tür açık anahtarlı şifreleme yöntemidir. RSA'da iki büyük asal sayının çarpımı olan bir sayı üretilir ve seçilen diğer bir değerle birlikte ortak anahtar oluşturulur. Seçilen asal çarpanlar ise saklanır. Ortak anahtarı kullanan biri herhangi bir mesajı şifreleyebilir, ama günümüzdeki yöntemlerle eğer ortak anahtar yeterince büyükse ancak asal çarpanları bilen kişi mesajı çözebilir. RSA şifrelemeyi kırmanın çarpanlara ayırma problemini kırmak kadar zor olup olmadığı hala kesinleşmemiş bir problemdir (Wikipedia-RSA, 2016).

The Data Encryption Standard(DES), 1974'te IBM'deki bir grup tarafından geliştirilmiştir ve 1977 bir standard olarak kabul edilmiştir (Coppersmith, 1994). Dünyada en yaygın olarak kullanılan şifreleme algoritmalarından birisidir (Dalkilic, 2008). DES algoritması blok şifreleme mantığına göre çalışır. Veriler bir anahtar yardımıyla bloklar halinde şifrelenir. Anahtar ne kadar uzunsa şifreyi çözmekte o kadar zor olacaktır (Sahin, 2015). Şifrelenecek olan açık metni parçalara bölerek her parçayı birbirinden bağımsız olarak şifreler ve şifrelenmiş metni açmak içinde aynı işlemi bloklar üzerinde yapar. Bu blokların uzunluğu 64 bittir. DES algoritması aynı zamanda 64 bit uzunluğunda bir anahtar alır. Bu anahtarın geçerli olan uzunluğu 56 bittir çünkü 8 bit parity bitidir.

1997'de, National Institute of Standards and Technology(NIST), DES algoritması artık yeterince güvenlik sağlamadığı ve 3DES algoritmasıda çok yavaş olduğu için bu algoritmaların yerine geçecek bir algoritma bulmak amacıyla bir yarışma düzenledi. Yarışmayı Vincent Rijmen ve Joan Daemen tarafından oluşturulan ve kendilerinin isimlendirdiği Rijndael algoritması kazandı. Ancak bu ismi telaffuz etmesi zor olduğu için algoritmanın ismi Advanced Encryption Standard(AES) olarak kullanılmaya başlandı (Selent, 2010). AES algoritmasının 128, 192 ve 256 bitlik versiyonları mevcuttur(Dalmisli, 2008). Bu algoritmalar anahtar uzunluklarına göre AES-128, AES-192 ve AES-256 olarak isimlendirilir (Singh,2013). 2006 yılı itibariyle en çok kullanılan algoritmalardan biridir (Dalkilic, 2008).

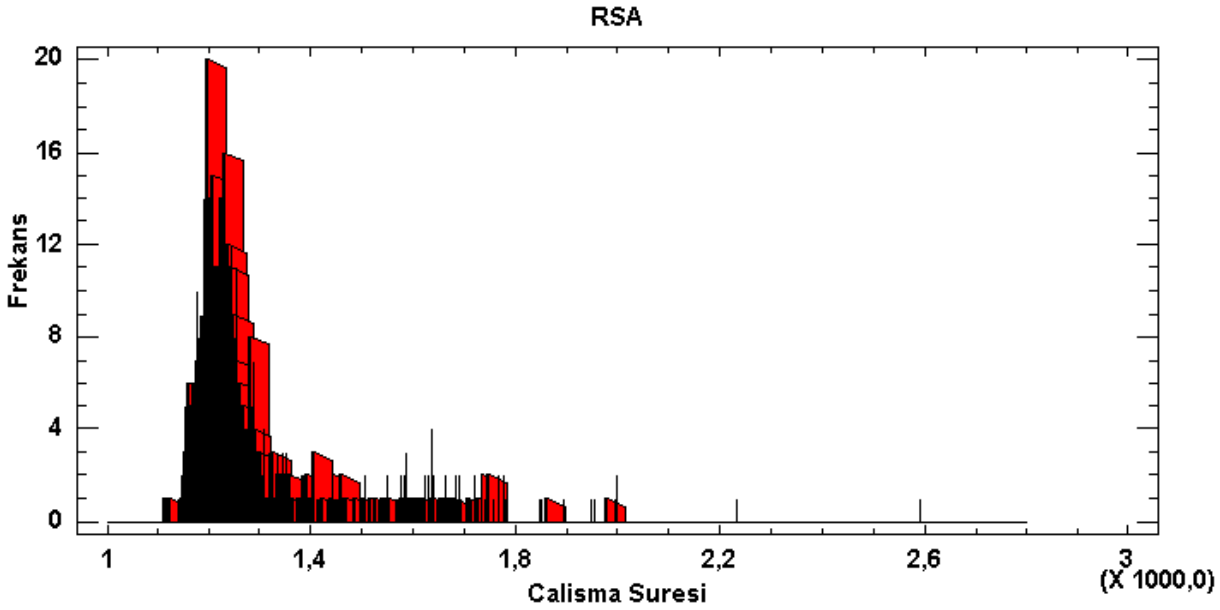
2. Algoritmaların Analizleri

RSA, DES ve AES algoritmaları, ortamın kararlı(stabil) olması için tek çekirdekli bir işlemciye sahip sanal makine kurularak karşılaştırılmıştır. Bu makineye kurulan NetBeans programı üzerinden algoritmalar gerçeklenmiştir ve hızları analiz edilmiştir.

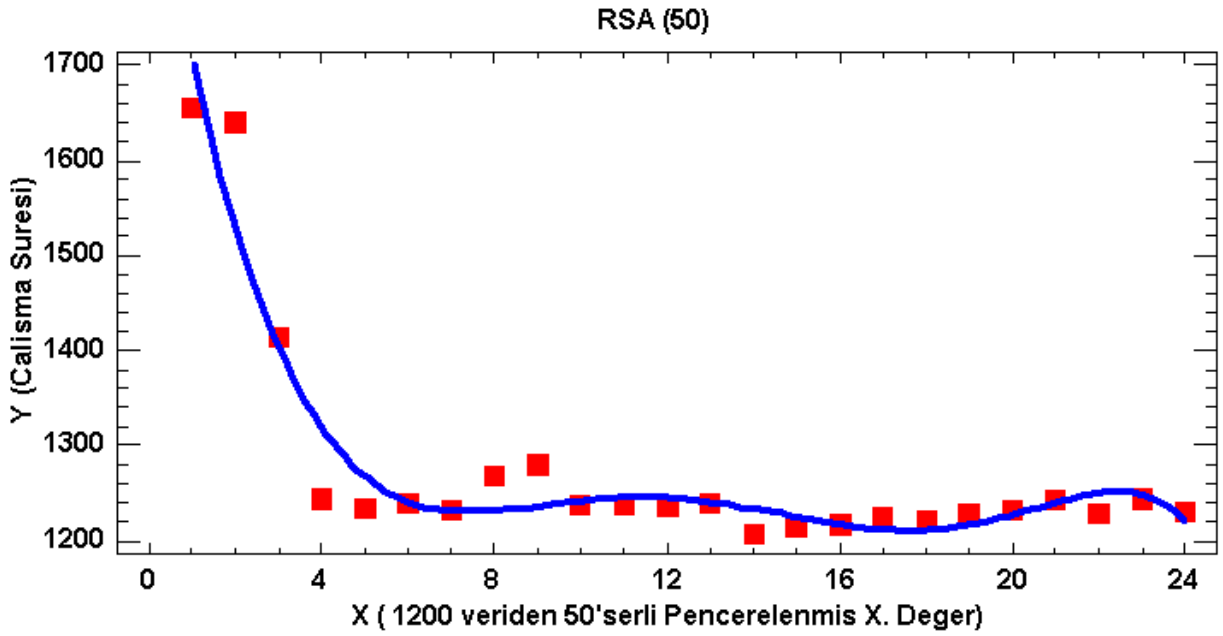
Üç algoritmada da aynı metin şifrelenmek için kullanılmıştır. Her algoritma için metin 1200 kez gerçeklenmiş ve veri setleri çıkarılmıştır. Bu veri setleri üzerinde regresyon analizi yapılarak sonuçları karşılaştırılmıştır.

2.1. RSA 'nın Analizi

RSA 1200lük veri setine 10luk, 20lik, 30luk, 40lık ve 50lik pencerelemeler uygulanmıştır. Elde edilen değerler kümesinin grafiğine uygun regresyon analizleri yapılmıştır. Çıkan en yüksek değerin grafiği, fonksiyonu ve sonucu aşağıda bulunmaktadır. En yüksek değer 50lik pencerelemede 6. dereceden polinomyal regresyon ile sağlanmıştır. Şekil 1'de 1200 verili RSA'nın grafiği gösterilmiştir. Şekil 2'de RSA'nın 50lik pencerelenmiş grafiği regresyon modeli ile gösterilmiştir. RSA'nın ortalama hızı 1277'dir.



Figür 1.RSA bütün veri

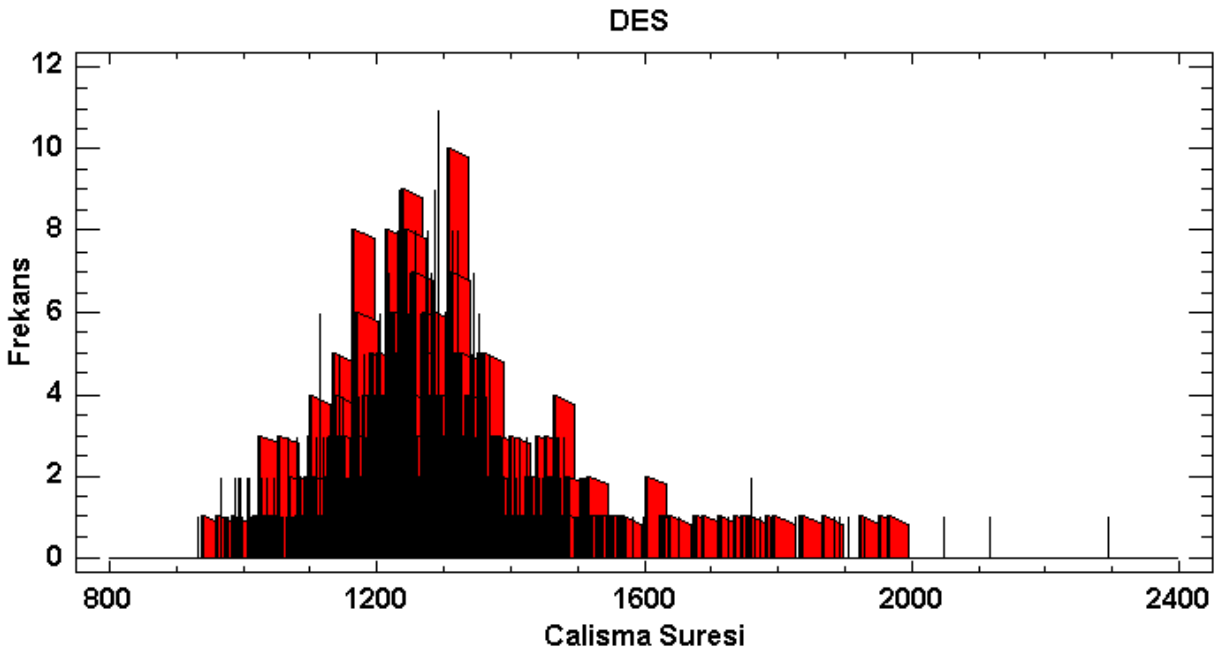


Figür 2.RSA 50

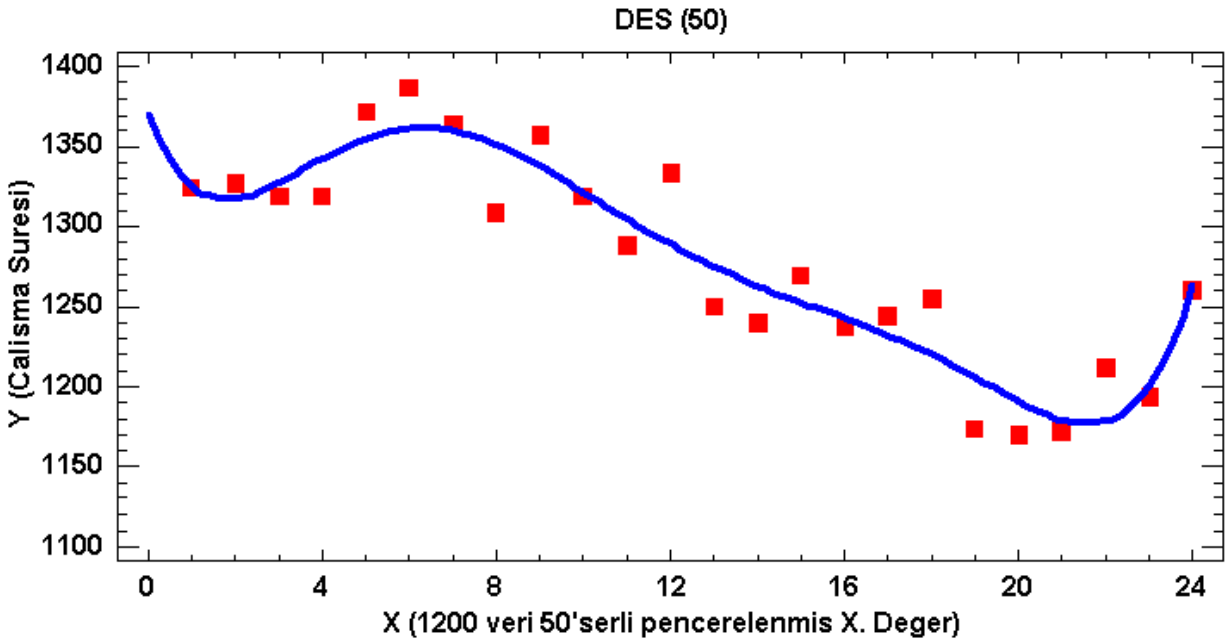
Regresyon modeli y = -0.0001x6 + 0.0055x5 – 0.0668x4 – 1.1477x3 + 33.676x2 - 270,4x + 1947.1 olup korelasyon katsayısı ise R^2 = 0.9193 dir.

2.2. DES 'in Analizi

DES 1200lük veri setine 10luk,20lik,30luk,40lık ve 50lik pencerelemeler uygulanmıştır. Elde edilen değerler kümesinin grafiğine uygun regresyon analizleri yapılmıştır. Çıkan en yüksek değerin grafiği, fonksiyonu ve sonucu aşağıda bulunmaktadır. En yüksek değer 50lik pencerelemede 6.dereceden polynomial regresyon ile sağlanmıştır. Şekil 3'de 1200 verili DES'in grafiği gösterilmiştir. Şekil 4'de DES'in 50lik pencerelenmiş grafiği regresyon modeli ile gösterilmiştir. DES'in ortalama hızı 1279'dir.



Figür 3. DES bütün veri

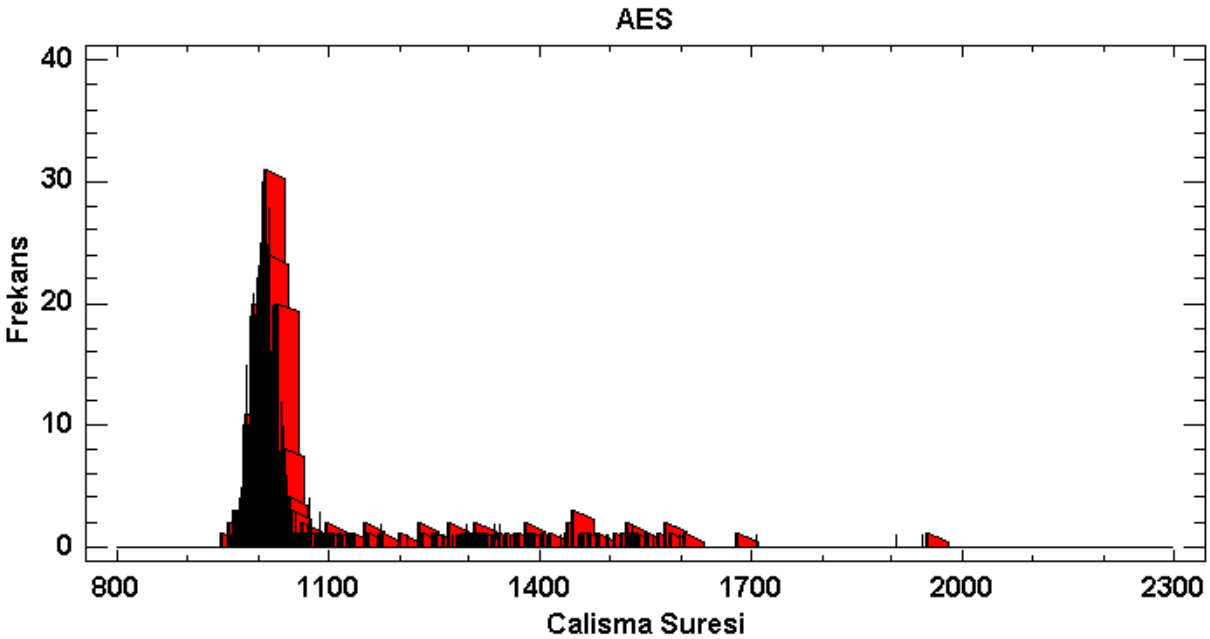


Figür 4. DES 50

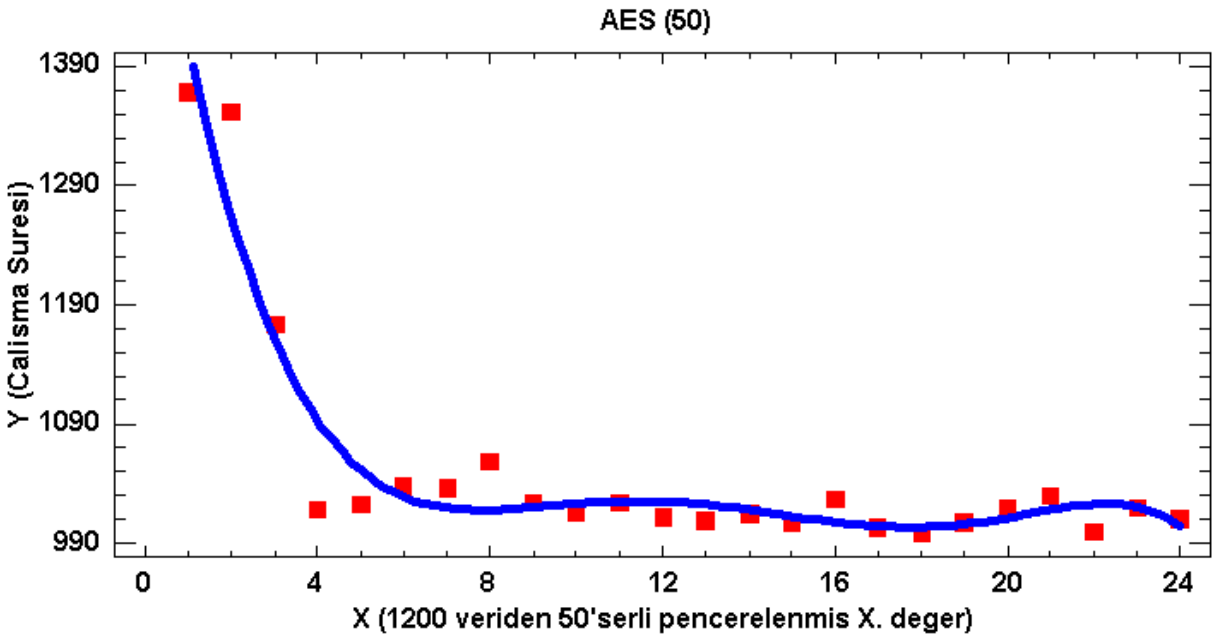
Regresyon modeli $y = 0.0002x^6 - 0.0141x^5 + 0.3947x^4 - 5.2297x^3 + 31.696x^2 - 71.931x + 1370.5$ olup korelasyon katsayısı $R^2 = 0.8826$ dir.

2.3. AES 'in Analizi

AES 1200lük veri setine 10luk,20lik,30luk,40lık ve 50lik pencerelemeler uygulanmıştır. Elde edilen değerler kümesinin grafiğine uygun regresyon analizleri yapılmıştır. Çıkan en yüksek değerin grafiği, fonksiyonu ve sonucu aşağıda bulunmaktadır. En yüksek değer 50'lik pencerelemede 6.dereceden polynomial regresyon ile sağlanmıştır. Şekil 5'de 1200 verili AES'in grafiği gösterilmiştir. Şekil 6'da AES'in 50lik pencerelenmiş grafiği regresyon modeli ile gösterilmiştir. AES'in ortalama hızı 1053'dir.



Figür 5. AES bütün veri



Figür 6. AES 50

Regresyon modeli $y = -0.00005x^6 + 0.0015x^5 + 0.0216x^4 - 1.8349x^3 + 32.27x^2 - 230.93x + 1611.1$ olup, korelasyon katsayısı $R^2 = 0.9151$ dir. Model $O(n^6)$ mertebesindedir.

Tablo-1. Algoritmaların karşılaştırılması

Algoritma	Model	R^2 Kor. Kat.	Big O
RSA	$y = -0.0001x^6 + 0.0055x^5 - 0.0668x^4 - 1.1477x^3 + 33.676x^2 - 270,4x + 1947.1$	0.9193	$O(n^6)$
DES	$y = 0.0002x^6 - 0.0141x^5 + 0.3947x^4 - 5.2297x^3 + 31.696x^2 - 71.931x + 1370.5$	0.8826	$O(n^6)$
AES	$y = -0.00005x^6 + 0.0015x^5 + 0.0216x^4 - 1.8349x^3 + 32.27x^2 - 230.93x + 1611.1$	0.9151	$O(n^6)$

3. Sonuç

RSA, DES ve AES için 1200 veriden oluşan veri setleri oluşturulmuştur ve bunlar karşılaştırılmıştır. Her veri setinin ayrı ayrı ortalaması bulunmuş ve regresyon analizleri yapılmıştır. Lineer, üstel, eksponansiyel, logaritmik, polinomyal vb regresyonlar denenmiş, bunların içinden üçüne de en uygun olan 6.dereceden polinomyal regresyon olmuştur.

Veri setleri algoritmaların hızları baz alınarak oluşturulmuştur. Bu veri setlerinin her algoritma için ayrı ayrı ortalaması hesaplanmıştır. RSA'nın ortalaması 1277, DES'in ortalaması 1279 ve AES'in ortalaması 1053 olarak ölçülmüştür. Buradan çıkan sonuçlara göre AES'in daha hızlı bir şekilde çalıştığı görülmüştür.

Her algoritma için regresyon analizleri karşılaştırıldığında RSA için %91.93, DES için %88.26 ve AES için %91.51 sonuçları ortaya çıkmıştır. Aralarındaki fark çok küçük olsa da RSA regresyonda AES'ten daha iyi bir sonuç ortaya çıkarmıştır.

Çıkan sonuçlar bu verilerle birbirlerine yakın olacağından bu çalışmalar bu algoritmaların çalışma süreleri testlerinde yardımcı olarak kullanılabilir. Her algoritma için çıkan regresyon denklemleri kullanılarak algoritmanın hızı hakkında bilgi edinilebilir. Yukarıda elde edilen sonuçlar ileride yapılacak olan araştırmada yardımcı kaynak olabilir.

Kaynakça

Coppersmith, D. (1994). The Data Encryption Standard (DES) and its strength against attacks. *IBM journal of research and development*, *38*(3), 243-250.

Dalkiliç, G., & Yildizoğlu, G. (2008). *Tek Anahtarlı Yeni Bir Şifreleme Algoritması Daha.*

Dalmıslı, K. V., & Ors, B. (2008). *Gelismis Sifreleme Standardının-AES-FPGA Uzerinde Gerçeklenmesi.*

Milanov, E. (2009). *The RSA algorithm*. RSA Laboratories.

Şahin, F. (2015). *Modern Blok* Şifreleme Algoritmaları.

Selent, D. (2010). *Advanced Encryption Standard*

Singh, G. (2013). A study of encryption algorithms (RSA, DES, 3DES and AES) for information security. *International Journal of Computer Applications*, *67*(19).

Wikipedia, R.S.A (2016) , Retrieved from http://www.midwestleague.com/indivpitching.html

Yerlikaya, T., Buluş, E., & Buluş, N. (2006). Kripto algoritmalarinin gelişimi ve önemi. *Akademik Bilişim Konferansları*.