International Journal of Innovative Research in Education

Volume 04, Issue 3, (2017) 135-141

www.ijire.eu

Comparative examination of rsa and SEA algorithms for computer engineering education

Bilgisayar mühendisliği eğitiminde RSA ve SEA algoritmalarının performansının karşılaştırmalı incelenmesi

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),135-141.

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

In this era of rapid technological development, critical prescriptive documents and personality information have begun to be stored in digital media. Increasing the importance of stored information has led to the development of security procedures for them and has led to the emergence of new encryption algorithms. We compare the RSA algorithm with the SEA (Scalable Encrytion Algorithm) algorithm, which is used in recently emerging and mostly embedded systems.

Keywords: 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.tr

Özet

Teknolojinin hızla geliştiği bu dönemde kritik öneme sahip belgeler ve kişilik bilgileri dijital ortamlarda saklanmaya başlanmıştır. Saklanan bilgilerin öneminin artması onlar için uygulanan güvenlik prosedürlerinin de gelişmesine yol açmış ve yeni şifreleme algoritmalarının türemesine sebep olmuştur.Bu makalede yakın dönemde ortaya çıkan ve çoğunlukla gömülü sistemlerde kullanılan SEA (Sclable Encrytion Algoritm) algoritması ile RSA algoritması karşılaştırılmıştır.

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

1. Giriş

SEA, mantıksal AND, OR ve XOR gibi basit işlemler kullanarak çalışan düşük maliyetli bir şifreleme algoritmasıdır. Bu özelliği sayesinde sınırlı komut seti olan işlemcilerde oldukça işe yarar.

SEA, metinde, anahtarda ve işlemcide parametrik bir yapıya sahiptir. Bu esnek yapısı sayesinde farklı boyuttaki metinler, anahtarlar ve kelimeler üzerinde işlem yapabilmektedir. Değişken döngü sayısı ve aşağıda tanımlanan parametrelerle birlikte Feistel yapısına dayalıdır(Standaert , 2006).

n: şifresiz metin boyutu, anahtar boyutu

b: işlemci(ya da kelime) boyutu

$n_b = \overline{2b}$: her Feistel dalı için kelime sayısı

n_r : blok şifreleme döngü sayısı

Tek sınırlaması n, 6b'nin katları şeklinde olmalıdır. Güvenliği sağlamak için gerekli minimum döngü sayısı $\frac{3n}{4} + 2.\left(n_b + \lfloor {}^{b}/_{2} \rfloor\right)$ şeklinde olmalıdır. Ayrıca gerekli minimum kelime sayısı ise $b \geq 8$ olmalıdır(Bayimis, 2008).

SEA, lineer ve diferansiyel ataklara karşı güvenlik sağlar. Bu algoritmanın başka bir avantajı ise oldukça basit olmasıdır.

RSA algoritması, Ron Rivest, Adi Shamir ve Leonard Adleman tarafından geliştirilmiştir. Adını bu kişilerin soyadlarının ilk harflerinden almıştır(Milanov, 2009).

RSA, açık anahtarlı bir şifreleme yöntemidir. Tam sayıları çarpanlarına ayırmanın algoritmik zorluğuna dayanan bir tür şifreleme algoritması olduğu için güvenilirdir. Hem şifreleme hem de elektronik imza atma olanağı sağlar.

Bu algoritmada biri gizli (Private Key) diğeri açık (Public Key) olmak üzere iki anahtar kullanılır. Sistemin hem güvenilir hem de hızlı olması için kullanılacak anahtar boyutunun büyüklüğü önemlidir.

RSA'da gizli anahtarın paylaşılması gerekmediği için saklanması da gerekmez. Bu da sistemi depolama yükünden kurtarır. Ancak büyük sayılarla işlem yapan bir algoritma olduğu için yavaştır. Band genişliğini fazlaca tüketir ve sistemi yavaşlatır. Bu uygulamada RSA'nın anahtar boyutunun 4096 bitten başlayarak 512 bite kadar çekilmesiyle işlem yükünü hafifletip işleyişinin hızlandırılması sağlanmıştır.

RSA algoritması anahtar üretimi, şifreleme ve şifre çözme olmak üzere 3 adımdan oluşur(Wikipedia, 2016).

2. Algoritmaların Sınanması

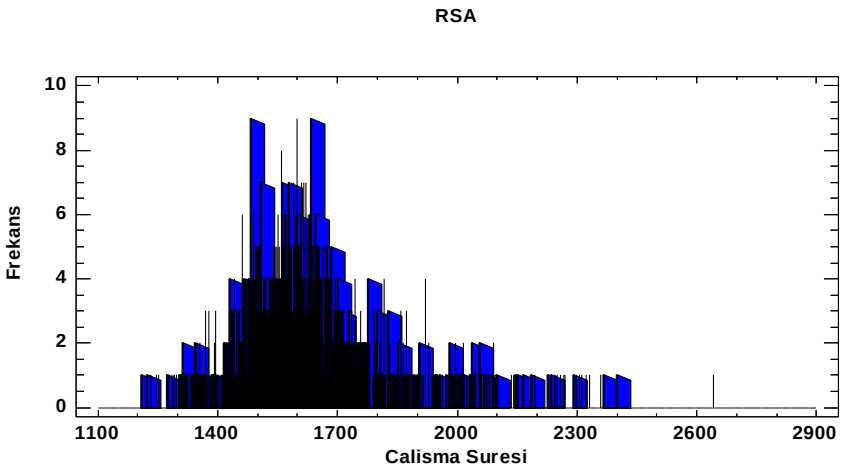
Aynı düz metin kullanılarak İki algoritma ile şifreleme işlemi yapılmıştır. Bu yapılırken RSA 'nın 512 bit uzunluklu anahtarı kullanılmıştır. Çalışma süreleri ölçülerek kaydedilmiştir. Bu ölçümlerden veri setleri oluşturulmuştur.

Ölçümler yapılırken ortamın kararlı (stabil) olması, çalışma sürelerine etki edecek arka plan çalışmalarının minimize edilmesi için tek çekirdekli bir işlemciye sahip sanal makine kurulmuştur. Bu makineye yüklenen netbeans programı vasıtasıyla algoritmalar gerçeklenmiştir.

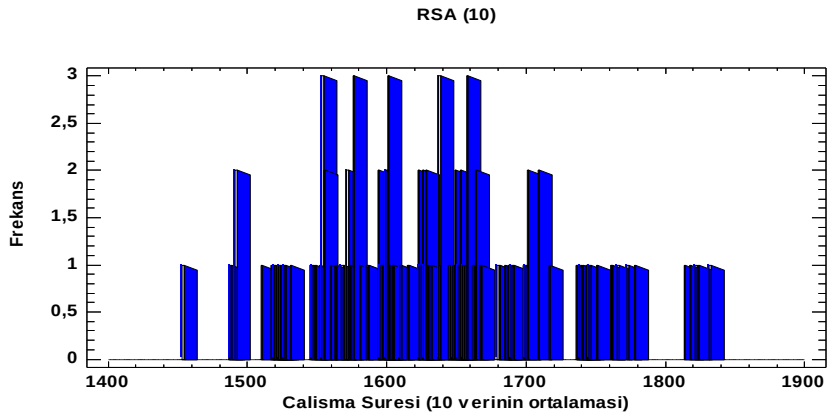
İlk olarak 30 veriden oluşan veri setleri sınamanın kalitesini artırmak adına zamanla artırılmış 100 'erli , 120 'şerli ve son olarak 1200 'erli veriler içerir hale getirilmiştir.

3. Veri setleri için Regresyon Analizi Regression

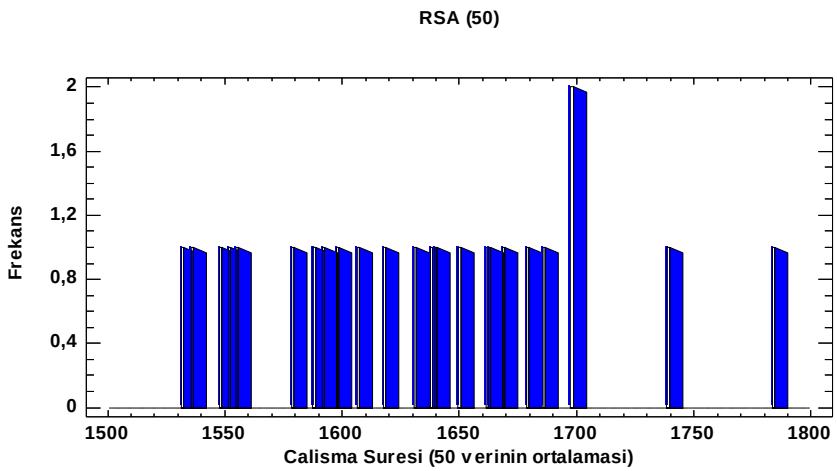
Veri setlerinin analizine başlamadan önce veriler farklı boyutlarda pencereleyerek, bunlara en uygun modelleri elde etmeye çalışıldı. Bu sebeple verilerimizi 10, 50, 100 'lü pencerelere ayırarak bar grafiklerini incelendi. Bunların yanında verilerin tamamını içeren veri setinin grafiğini de eklendi.



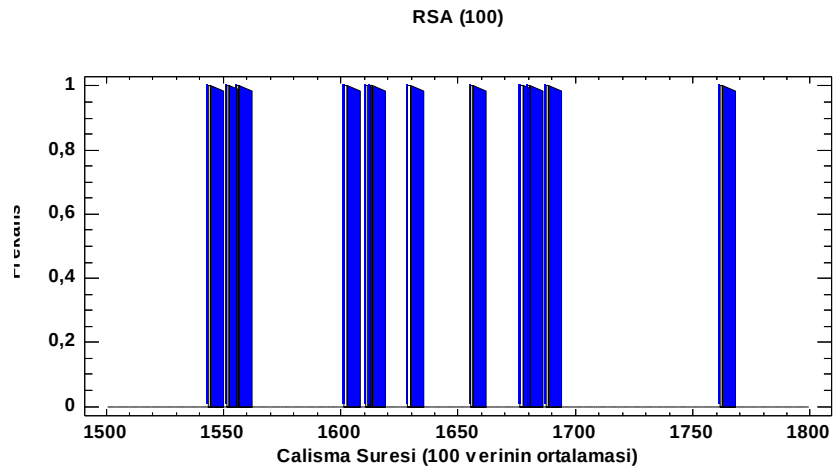
Figür 1. RSA tüm veri



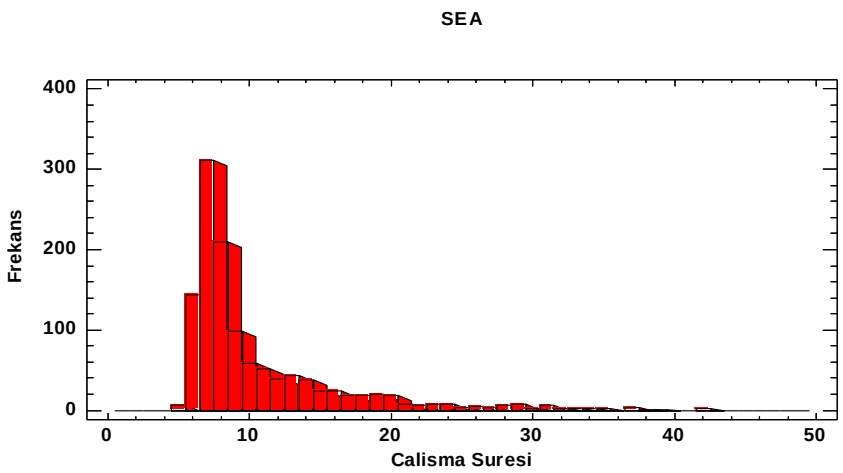
Figür 2. RSA -10 lu gruplar



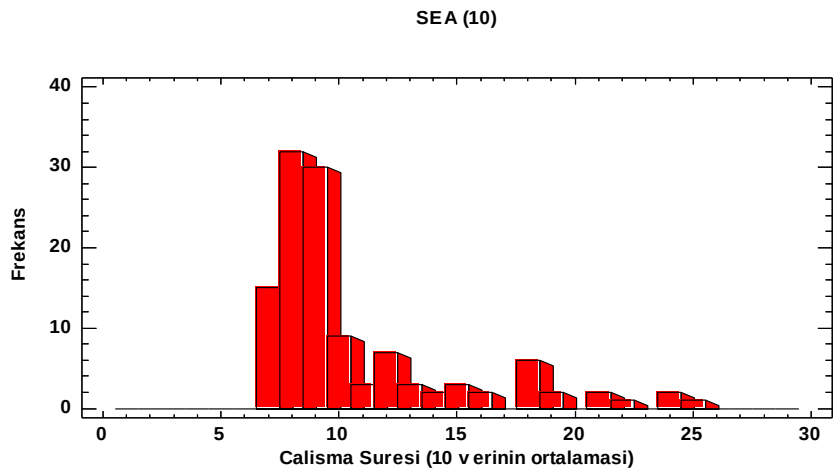
Figür 3. RSA -50 li gruplar



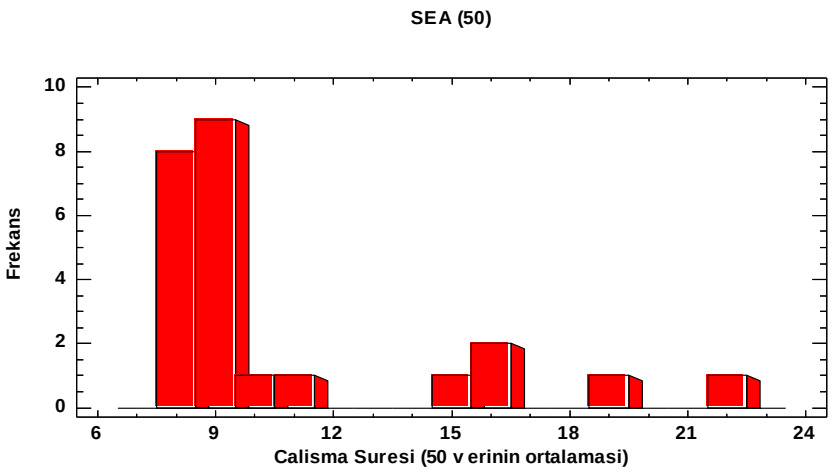
Figür 4. RSA -100 lü gruplar



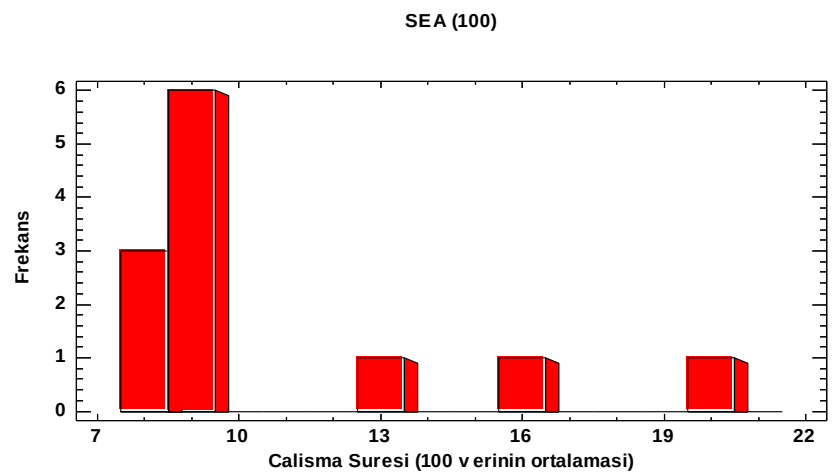
Figür 5. SEA –tüm ver



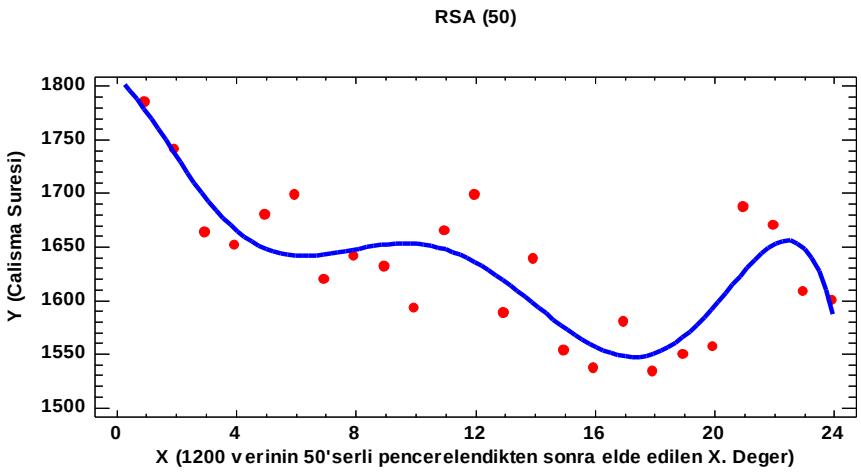
Figür 6. SEA -10 lu gruplar



Figür 7. SEA -50 li gruplar

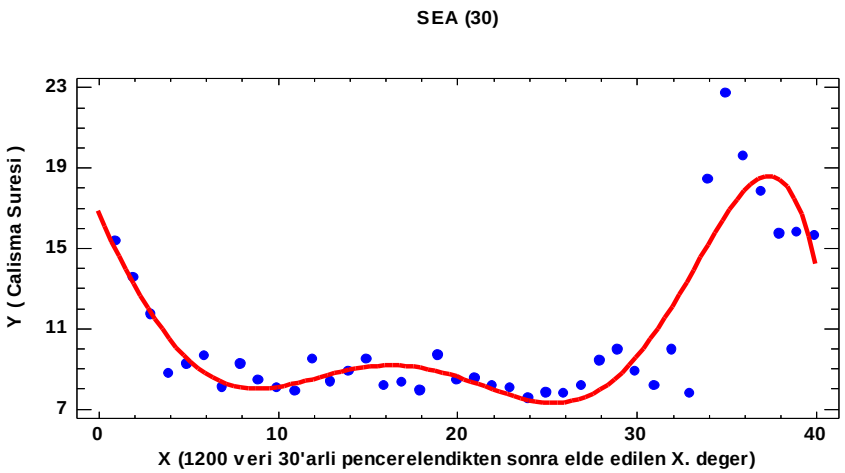


Figür 8. SEA -100 lı gruplar



Figür 9. RSA-Big O için regresyon modeli

Regresyon denklemi $y = -0.0003x^6 + 0.0184x^5 – 0.4415x^4 + 4.5347x^3 – 16.622x^2 – 17.519x + 1806.7$ olup korelasyon katsayısı ise $R^2 = 0.7276$ dır.



Figür 10. SEA-Big O için regresyon modeli

Regresyon denklemi $y = -0.000007x^6 -0.000005x^5 – 0.0018x^4 + 0.0222x^3 + 0.0106x^2 – 1.8845x + 16.789$ olup korelasyon katsayısı ise $R^2 = 0.7898$ dir.

4. Sonuç

Bu çalışmada elde edilen veriler ve yapılan incelemeler neticesinde SEA algoritmasının ve RSA algoritmasının ortalama çalışma süreleri hesaplanmıştır. Bu verilere göre analiz yapılarak polinominal denklemleri oluşturulmuştur.

SEA algoritmasının ortalama çalışma süresi 10.5358 milisaniye olarak tespit edilmiştir. Algoritmanın varyansı 33.6151 olarak hesaplanmıştır.

RSA algoritmasının ortalama çalışma süresi 1630.9 milisaniye olarak tespit edilmiştir. Algoritmanın varyansı 31949 olarak hesaplanmıştır.

Tüm bu çalışmalar sonucunda bu algoritmaların bundan sonraki çalışma süresi testleri yukarıda belirtmiş olduğumuz grafikler ve denklemlerle tahmin edilebilir veya ölçüm yapılması halinde bunlarla paralellik gösterecektir.

References

Bayimiş, C., & Çakiroğlu, M. (2008). SEA şifreleme algoritması kullanarak güvenli kablosuz algılayıcı ağ haberleşmesinin gerçekleştirilmesi. In *Proceeding of 3rd international information security and cryptology conference held at Ankara, Türkiye*.

Milanov, E. (2009). The RSA Algorithm. https://tr.wikipedia.org/wiki/RSA adresinden erişilmiştir.

Standaert, F. X., Piret, G., Gershenfeld, N., & Quisquater, J. J. (2006, April). SEA: A scalable encryption algorithm for small embedded applications. In *International Conference on Smart Card Research and Advanced Applications* (pp. 222-236). Springer, Berlin, Heidelberg.

Wikipedia, RSA, (2016). http://www.midwestleague.com/indivpitching.html adresinden erişilmiştir.