Fırat Üniversitesi Müh. Bil. Dergisi
35(2), 891-900, 2023

Araştırma Makalesi
https://doi.org/10.35234/fumbd.1296228

Simetrik ve Asimetrik Şifreleme Algoritmalarının Performans Karşılaştırılması

Alev KAYA[1*], İbrahim TÜRKOĞLU[2]
[1,2] Yazılım Mühendisliği Bölümü, Teknoloji Fakültesi, Fırat Üniversitesi, Elazığ, Türkiye
[*1] alev.kaya@firat.edu.tr, [2] iturkoglu@firat.edu.tr

(Geliş/Received: 12/05/2023; Kabul/Accepted: 28/08/2023)

Öz: İnternet tabanlı teknolojilerin her geçen gün artması, dünyadaki veri oluşumunu da sürekli artırmakta ve veri büyüklüğü genişledikçe kullanıcılar için bilginin güvenliği ve gizliliği risk taşımaktadır. Güvenli olmayan bir iletişim kanalı üzerinden veriler iletildiğinde tehlikeli durumların minimuma indirgenmesi veya tamamen önlenmesi için önerilen yöntemlerden biri kriptografik algoritmalardır. Temeli matematiksel ifadelere dayanan tekniklerin ve uygulamalarının birleşimini içeren tüm şifreleme algoritmaları; verilerin kullanılabilirliğini, gizliliğini ve bütünlüğünü korumayı amaçlamaktadır. Ancak başarımları; seçilen dosya türü, boyutu, karmaşıklığı, anahtar yapısı ve kullanılan bilgisayar platformu(yazılım ve donanım) gibi çeşitli faktörlere göre değişmektedir. Bu faktörler temelinde, üç farklı simetrik(AES, Blowfish, Cast-128) ve asimetrik(ECDH, El-Gamal, RSA) şifreleme algoritması kullanılarak bir uygulama yapılmıştır. *"The Da Vinci Code"* adlı içerikten üretilen 100 KB, 1, 5 ve 100 MB arasında değişen 4 adet çeşitli metinsel dosya boyutlarının karmaşıklığı; *UTF-8* tablo yapısındaki birleşimleridir. Anahtar(gizli ve açık) sistemi; *32 karakterden(256 bit)* oluşan mimaridir ve uygulama platformu; yazılım için, *Windows, Python VS Code,* donanım için, *Intel I7-CPU, 16 GB RAM, 4 GB-GPU* kullanılmıştır. Literatürde kabul edilen performans kriterleri; şifreleme ve şifre-çözmedeki hızı (s), bellek (MB) ve CPU (%) kullanım oranları temel alınarak başarımları değerlendirilmiştir. Böylece, simetrik ve asimetrik şifreleme algoritmalarının başarımları aynı veri setleri üzerinde karşılaştırılmıştır. Simetrik şifreleme algoritmalarının başarım sonuçlarının daha iyi olduğu gözlemlenmiştir.

Anahtar kelimeler: Bilgi güvenliği, simetrik kriptografi, asimetrik kriptografi, performans analizi.

Performance Comparison of Symmetric and Asymmetric Encryption Algorithms

Abstract: The increasing use of Internet-based technologies is constantly increasing the formation of data in the world, and as the size of data expands, the security and privacy of information for users carries risks. When data is transmitted over an unsecured communication channel, one of the recommended methods for minimizing or completely preventing dangerous situations are cryptographic algorithms. All encryption algorithms, the basis of which includes the combination of techniques and their application based on mathematical expressions; aims to protect the availability, confidentiality and integrity of data. However, their achievements; The file type chosen varies according to various factors such as size, complexity, key structure and the computer platform (software and hardware) used. On the basis of these factors, an application was made using three different symmetric (AES, Blowfish, Cast-128) and asymmetric (ECDH, El-Gamal, RSA) encryption algorithms. the complexity of the 4 various textual file sizes ranging from 100 KB, 1, 5 and 100 MB generated from the content called "The Da Vinci Code"; UTF-8 are combinations in a table structure. Key (hidden and public) system; It is the architecture consisting of 32 characters (256 bits) and the application platform; For software, Windows, Python VS Code, for hardware, Intel I7-CPU, 16 GB RAM, 4 GB-GPU are used. Performance criteria accepted in the literature; performance in encryption and decryption was evaluated based on speed (s), memory (MB), and CPU (%) utilization rates. Thus, the performances of symmetric and asymmetric encryption algorithms are compared on the same data sets. It has been observed that symmetric encryption algorithms have better performance results.

Key words: Information security, symmetric cryptography, asymmetric cryptography, performance analysis.

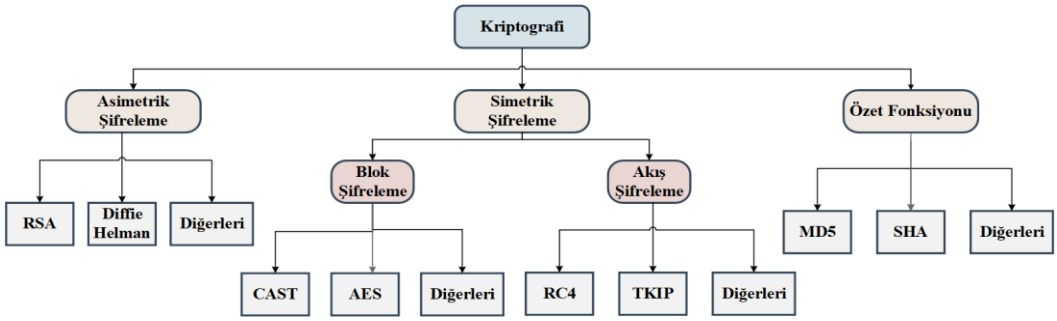
1. Giriş

Günümüzde internet tabanlı teknolojilerin her geçen gün artması, veri hacmini de artırmakta ve veri büyüklüğü genişledikçe dijital ortamdaki bilgilerin kullanıcıları için güvenliği ve gizliliği risk taşımaktadır [1]. Güvenli olmayan bir iletişim kanalı üzerinden veriler iletildiğinde tehlikeli durumların minimuma indirgenmesi veya tamamen kaldırılması için önerilen yöntemlerden biri de bilgi güvenliğinin alt dalı olan kriptografik algoritmalardır. Kriptoloji, iletişim sağlanması planlanan taraflar arasında paylaşılacak dosya türlerinin belirli bir sisteme göre şifrelenmesi (kriptografi) ve bu mesajların güvenlikli bir ortamda iletilmesi ve iletilmiş mesajın bozulmadan orijinal haline şifre çözme ile geri (kriptoanaliz) getirilmesidir. Temeli matematiksel ifadelere dayanan tekniklerin ve uygulamalarının birleşimi olan ve Şekil 1' de "kriptolojinin kategorik sınıflandırması"

* Sorumlu yazar: alev.kaya@firat.edu.tr .Yazarların ORCID Numarası: [1] 0000-0002-3544-5267, [2] 0000-0003-4938-4167

100/2000 YÖK Doktora Bursiyeri

başlığı ile görselleştirilen kriptografik algoritmaların tümü; verilerin kullanılabilirliğini, gizliliğini ve bütünlüğünü korumayı amaçlamaktadır**.** Ancak başarımları; seçilen dosya türü (örneğin; metin, video, sinyal, görüntü vb.), boyutu (örneğin; KB, MB, GB, …), karmaşıklığı (örneğin; karakter yapısı, multi özelikler vb.), anahtar yapısı (örneğin; anahtarlı, anahtarsız, hibrit) ve kullanılan bilgisayar platformu (örneğin; Python, Java vb. yazılım ve ram gibi vb. donanım) gibi çeşitli faktörlere göre değişim göstermektedir [2]. Bu faktörler temelinde, simetrik olarak Gelişmiş Şifreleme Standardı (Advanced Encryption Standard: AES), Blowfish, Cast-128 ve asimetrik olarak Eliptik Eğri Diffie-Hellman (Elliptic-Curve Diffie–Hellman: ECDH), El-Gamal, Rivest–Shamir–Adleman (RSA) adlı altı farklı şifreleme algoritması kullanılarak bir uygulama yapılmıştır. Çalışmada gerçek bir veri seti olan *"The Da Vinci Code"* adlı içerikten 100 KB, 1, 5 ve 100 MB arasında üretilen dört adet metinsel dosya boyutlarının karmaşıklığı; 8-bitlik bir Unicode dönüşümlü (Unicode Transformation Format- 8: UTF-8) tablo yapısındaki birleşimleridir. Anahtar (gizli ve açık) sistemi; 32 karakterden (256 bit) oluşan mimaridir ve uygulama platformu; yazılım için; *Windows, Python VS Code,* donanım için, *Intel I7-CPU, 16 GB RAM, 4 GB-GPU* hafızadır. Literatürde kabul edilen performans kriterleri; şifreleme ve şifre-çözmedeki hızı (s), bellek (MB) ve CPU (%) kullanım oranları temel alınarak başarımları değerlendirilmiştir.



Şekil 1. Kriptolojinin kategorik sınıflandırması

Çalışmanın geri kalanı aşağıdaki şekilde düzenlenmiştir. İkinci bölümde ilgili çalışmalar başlığı altında; literatürdeki son beş yılı içeren benzer veya yakın çalışmalar incelenmiş, çalışmaların performans sonuçları, çalışmalarda kullanılan farklı veri setleri ve yöntemleri hakkında bilgiler verilmiştir. Üçüncü bölümde materyal ve metot başlığı altında; çalışmada kullanılan veri seti, şifreleme algoritmaları ve performans kriterleri hakkında bilgiler verilmiş görsel içeriklerle zenginleştirilmiştir. Uygulama sonuçları dördüncü bölümde Tablo 1 ile verilmiş ve benzer çalışmalarla kıyasın yapıldığı tartışma ve sonuç başlığı altındaki son bölümünde (beşinci bölüm) çalışmanın avantaj ve dezavantajları vurgulanmış ve ileriye dönük çalışmalar tartışılmış ve ikinci bölümdeki çalışmalar ile sonuçlar karşılaştırılmalı incelenmiştir. Çalışmanın öne çıkan özellikleri şu şekilde ifade edilebilir;

- Gerçek bir veri kümesi olan *"The Da Vinci Code"* adlı metinsel içerikten üretilen farklı boyutlardaki (100 KB, 1,5 ve 100 MB) yapay veri setlerinin şifrelenmesi,
- Uygulama için seçilen simetrik ve asimetrik algoritmaların, literatürde metinsel dosya türü için kabul edilen performans kriterleri; şifreleme ve şifre-çözmedeki hızı (s), bellek (MB) ve CPU (%) kullanım oranları temel alınarak başarımlarının değerlendirilmesi,
- Türkçe literatüre, son beş yılı kapsayan benzer çalışmaların özeti niteliğinde güncel ve genel bir kaynak araştırması ve uygulamasının sunulması.

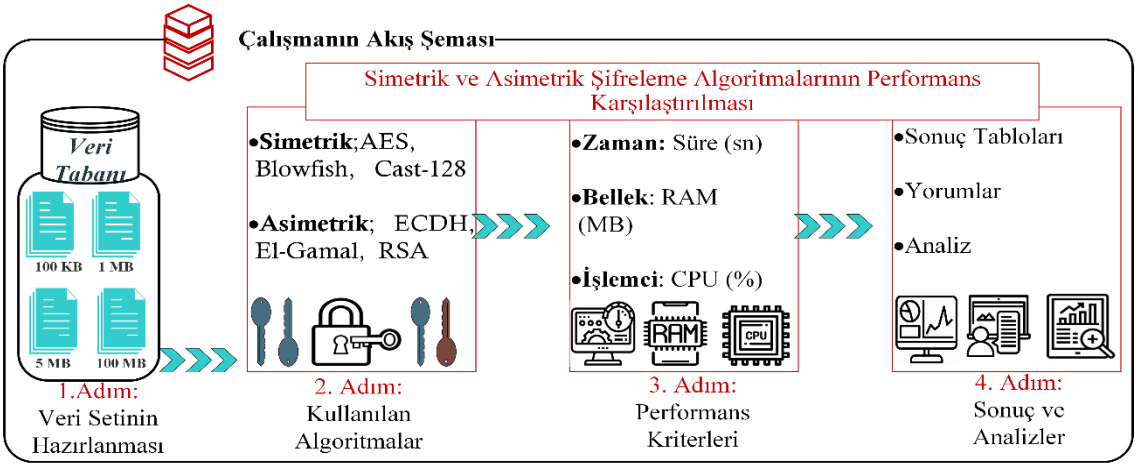
2. İlgili Çalışmalar

Farklı boyutlardaki metinsel veri türü üzerinde10 farklı simetrik şifreleme algoritmalarının uygulandığı çalışmada [3], performans kriterleri olarak süre, CPU, RAM ölçülmüştür. Şifreleme ve şifre çözme sonuçlarında; Blowfish, Salsa20, 3DES, Cast, AES ve DES algoritmalarının daha iyi sonuçlar verdiği gözlemlenmiştir. Farklı boyutlardaki metinsel veri türü üzerinde3 farklı asimetrik şifreleme algoritmalarının uygulandığı bir başka çalışmada [4] ise performans kriterleri olarak süre, CPU, RAM ölçülmüştür. Şifreleme ve şifre çözme sonuçlarında; ECDH, El-Gamal ve RSA sıralaması çıkmıştır. 3 farklı simetrik ve asimetrik şifreleme algoritmalarının (AES, DES, RSA) metinsel veri türü üzerinde değerlendirildiği uygulamada [5], performans kriterleri olarak hız, süre, verim, çığ etkisi dikkate alınmıştır. Çıkan sonuçta AES algoritmasının en verimli olduğu bulunmuştur. AES ve RSA algoritmalarının süre, anahtar uzunluğu ve şifre uzunluğu kriterlerine göre metinsel veri türünde yapılan karşılaştırmalı çalışmada [6], AES' nin iki şifreleme tekniği arasından daha iyi olduğu ve

özellikle mobil uygulamaların geliştirilmesinde güvenlik önlemi için iyi bir algoritma olarak önerisi verilmiştir. AES, DES ve RSA algoritmalarının metinsel veri türü üzerinde, hesaplama süresi, bellek kullanımı ve çıkış baytı kriterlerine göre kıyaslandığı bir diğer çalışma [7] yapılmıştır. Sonuçlara göre, DES algoritmasının en az şifreleme süresi tükettiğini ve AES algoritmasının en az bellek kullanımına sahip olduğunu, AES ve DES algoritması durumunda ise şifreleme süresi farkının küçük olduğunu gösterdiği söylenmiştir. Ayrıca RSA, en uzun şifreleme süresini tükettiği ve belleği çok yüksek kullandığını ancak çıkış baytı en az olduğu sonuçlarına varılmıştır. Süre, CPU, RAM kriterlerine göre kıyaslanan çalışmada [8] ise asimetrik ve simetrik anahtar algoritmalarının zayıflıklarını ve güçleri açıklanmıştır. RC5 ve RC4 güvenliği sorgulanması gerektiği ve ayrıca RC4, RC5'ten daha hızlı olduğu verilmiştir. Bu şifreleme algoritmaları AES, 256 bitlik anahtar boyutlarına izin vererek ve gelecekteki saldırılara karşı koruma sağlayarak tüm algoritmalardan daha güvenli, verimli ve hızlıdır sonucun varılmıştır. RSA' nın en iyi asimetrik anahtar algoritması olduğuna ancak şifre çözme sürecinde büyük tamsayılar için şifreleme ve çarpanlarına ayırma sorunu için daha fazla zaman harcamasına değinilmiştir. Metinsel veri türünde yapılan bir diğer çalışma [9], simetrik ve asimetrik şifreleme algoritmalarının kıyasını; güvenlik, anahtar boyutu, karmaşıklık, süreye göre yapmıştır. Bu çalışmaya göre şifreleme, zaman, hız ve esneklik açısından AES, BlowFish, RC4, E-DES ve TDES en hızlı algoritmalardır. AES' in şifreleme hızı, kod çözme karmaşıklığı, anahtar uzunluğu, güvenlik ve esneklik açısından en güvenilir algoritma olduğu sonucuna varılmıştır. Hibrit, geliştirme, döngü sayısı, anahtar uzunluğu, blok boyutu, bulunan saldırılar, güvenlik düzeyi, olası anahtarlar, tüm olası anahtarları kontrol etmek için gereken süre gibi kriterlerin temel alındığı uygulama [10]; metinsel veri türünde simetrik, asimetrik ve hibrit anahtarlı algoritmalardan oluşmaktadır. AES-ECC' nin zaman ve mekân karmaşıklığını azalttığı ve DSA-RSA hibrit algoritmasının daha iyi performans ve verime sahip olduğu sonucuna varılmıştır.

3. Materyal ve Yöntem

Tasarımı güvenlik ve verimlilik üzerine inşa edilen kriptografik algoritmalar; farklı platformlarda kullanılabilir yapısı, bellek hacmi tasarrufu ve optimal maliyet sunan kolay uygulaması gibi vb. özellikleri içermektedir. Bu özellikler temelinde, kripto sisteme ulaşmaya çalışan üçüncü (kriptanalizler) şahıslardan kaynaklı zorluklar, yüzde yüz güvenli bir kriptografik algoritma geliştirmeyi de oldukça zorlamaktadır. İletişimde uygun, doğru ve yüksek güvenlik düzeyi sağlayan algoritmaların seçilmesine ek bir gereksinim vardır [11]. Yapılan çalışma kapsamında; kriptografik anahtarlı sistemlere dayanan asimetrik ve simetrik şifreleme algoritmalarıyla uygulamalar yapılmış ve farklı boyutlardaki metinsel veri türü üzerinde performans analizleri karşılaştırılmıştır. Çalışmanın akış şeması Şekil 2' te görselleştirilerek ve alt bölümlerde takiben açıklanarak aktarılmıştır.



Şekil 2. Çalışmanın akış şeması

3.1. Veri setinin hazırlanması

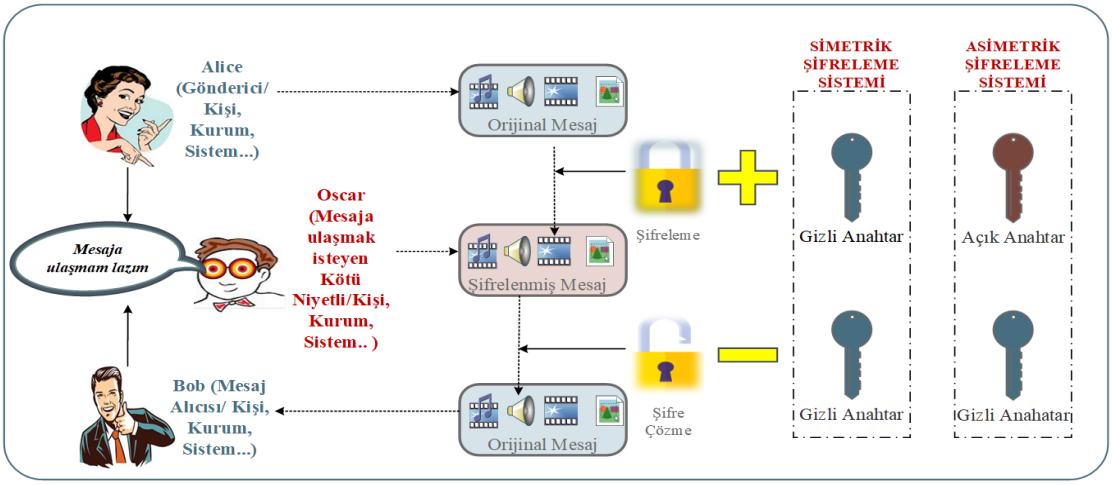
Bu çalışmada; *"The Da Vinci Code"* adlı içerikten [12] dört farklı boyutta yapay olarak üretilen veri setleri kullanılmaktadır. Orijinal ve yapay üretilen veri formu metinsel türdür. Yapay veri setlerinin boyutları; 100 KB, 1 MB, 5 MB ve 100 MB arasında değişmektedir.

3.2. Kullanılan Şifreleme Algoritmaları

Herhangi bir modern şifreleme sistemi kısa açıklamasıyla[13] aşağıdaki bileşenlerden ve algoritmalardan oluşur.

- *Gönderici- Alıcı:* Mesaj iletişiminde bilgiyi gönderen ve alan taraflar.
- *Kanal:* Mesaj iletiminin yapıldığı ortam (internet, telefon, …).
- *Orijinal (Düz) Form:* Şifreli forma dönüştürülecek veri türünün orijinal hali.
- *Şifreli Form:* Ham veri türünün işlenmiş (şifreleme) hali.
- *Şifreleme:* Herhangi bir mesajın orijinal halini değiştirmek için yapılan gizleme işlemi.
- *Şifre Çözme:* Şifrelenerek gizlenmiş veriyi tekrar eski orijinal haline bozulmadan geri döndürme işlemi.
- *Anahtar:* Orijinal veri türünün şifreli forma dönüştürülmesinde ve tekrar orijinal hale çevrilmesinde yararlanılan karakter dizisi yani şifreleme ve şifre çözme sürecinin (anahtarlı sistemlerde) ana aracı.
- *Anahtar Arama Algoritması:* Her türlü olası kombinasyonu denerek anahtara ulaşılmaya çalışılan süreç.
- *Açık (Genel) Anahtar:* Asimetrik şifrelemede herkes tarafından erişilebilen ve sadece şifreleme sürecinde kullanılan ayrıca şifre çözme sürecinde de özel anahtara yardımcı olan anahtar tipi.
- *Gizli (Özel) Anahtar:* Asimetrik şifreleme algoritmasında kullanılan ve sadece sahibi tarafından bilinen ve paylaşılmayan anahtar türü.
- *Şifre Kırma:* Şifrelemede kullanılan yapıyı öğrenmek için yapılan teşebbüs.
- *Saldırgan:* Mesaj iletişiminde ilgili tarafların arasında olmayan yapılar (kişi, kurum, sistem, …).
- *Saldırı:* Şifrelenmiş sistemin yapısını(şifresini) kırmak için yapılan uygulama.
- *Kriptanalist:* Şifrelenmiş mesajı çözen kişi.
- *Kerckhoffs Prensibi:* Auguste Kerckhoffs [14] tarafından ortaya atılan prensibe göre; tasarlanması gereken kriptolojik sistemlerin güvenlik riski yalnızca anahtar sisteminin gizlilik riskine bağımlıdır. Şifrenmiş yapının anahtar haricinde her detayı bilinse dahi şifre çözme işlemi başarısızlıkla sonuçlanacaktır.
- *Shannon Prensibi:* Cloude Shannon [15] tarafından ortaya atılan prensibe göre; şifreleme sisteminin güçlülüğünden bahsetmek için karıştırma ve yayılma özellikleri olmalıdır. Karıştırma özelliği, şifrelenmiş form ile anahtar arasındaki ilişkinin istatistiksel tekniklerle tespiti yapılmamalıdır. Yayılma özelliği; orijinal formun bir karakterinde gerçekleştirilecek değişimle şifrelenmiş formdaki birden fazla karakteri etkilemesinin sonucuyla oluşan yapıdır. Buradaki amaç; şifrelemede ve şifre çözme sürecinde anahtar yapısının istatistiksel tekniklerle belirlenmemesi için yapılan gizlemedir.

Yukarıda açıklamalara dayanarak güvenli bir kripto sistemin tasarımı için geliştirilen şifreleme algoritmaları Şekil 3 ile gösterildiği gibi anahtar yapısına göre; simetrik ve asimetrik şifreleme sistemleri olarak sınıflandırılmıştır.



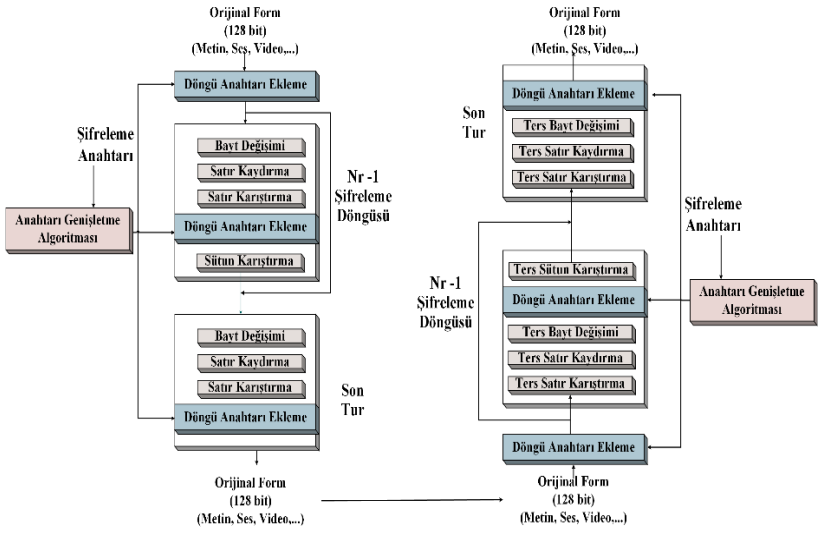
Şekil 3. Simetrik ve asimetrik şifreleme sistemleri

3.2.1. Kullanılan simetrik şifreleme algoritmaları

Bu çalışmada kullanılan simetrik anahtarlı şifreleme algoritmaları; AES, Blowfish ve Cast-128' tir. Simetrik anahtarlı sistemler şifreleme ve şifre çözme sürecinde aynı anahtar (gizli) kullanılır ve bu anahtar gizli tutulmalıdır. Ayrıca anahtarların aynı olmasından dolayı asimetrik yapılara göre sık sık anahtar değişikliği gerekebilir. Gönderici taraf alıcı tarafın gizli anahtarı hakkında tamamen bilgi sahibidir. Asimetrik şifrelenmeye göre kırılma durumları daha az dirençlidir. Gizlilik kriteri hariç bütünlük- kimlik doğrulama- inkâr edilememe kriterlerini sağlamamaktadır. Taraflar arasında bilinen tek bir anahtar yapısı olduğu için şifre çözme süreci asimetrik yapıya göre daha düşüktür (hızlıdır) ve buda önemli avantajlardan biridir. Şifrelenebilecek veri miktarı asimetrik yapılara göre daha yüksektir. İşlemciyi ve diğer kaynakları asimetriklere göre daha az tüketir. Tüm güvenlik, anahtara ve anahtar uzunluğuna bağlıdır. Asimetrik yapılara göre daha uzun anahtar dizinine sahip olabilir. Güvenli bir şekilde anahtarın iletilmesi ve kapasite sınırı dezavantajıdır. Donanım ile uyumludur. Modern şifreleme sistemlerinin temelini oluşturmaktadır [16-19].

3.2.1.1. AES

1997 yılında Ulusal Standartlar ve Teknoloji Enstitüsü (National Institute of Standards and Technology: NIST), yüksek güvenlik ve verimlilik gibi öncelikli ihtiyaçları karşılayan yeni bir şifreleme algoritması AES'i duyurmuştur. Mevcutta bulunan Veri Şifreleme Standardı (Data Encryption Standart: DES) ve Üçlü DES (Triple DES; TDES) algoritmalarının yerini almaya (uzunluk değişkenli tuşlar, daha hızlı oluşu) çalışan AES; 128(10 tur), 192(12 tur) ve 256(14) bit anahtar uzunluklarıyla esnek bir yapıda tasarlanmıştır. Çok büyük blok boyutlarına sahip olduğundan daha fazla işlem için güç ve kaynak harcaması, bu basit matematiksel yapının dezavantajıdır [20,21]. AES kriptografik süreci Şekil 4 ile görselleştirilmiştir. AES kriptografik mimarisi; bayt değişimi, satır kaydırma, sütun karıştırma ve döngü anahtarının eklenmesi olarak dört aşamalı döngüsel bir sürecin tekrarıdır. Her bir adım sırasını bozmadan işlemleri gerçekleştirir yalnızca sütunları karıştırma son döngüde işleme katılmaz. Şifre çözme süreci ise bu adımların tam teri olarak uygulanır. Süreç; 128 bit =16 bayt uzunluğunda sadece veri girişlerinin (ve çıkışlarının), 4 ×4(satır × sütun) matrisler aracılığıyla, her bölmesi bir bayt= 8 bit ve her satırı 4 baytlık =32 bitlik bir kelime olacak şekilde toplamda 16 bölümlü bir yapıyla başlar.

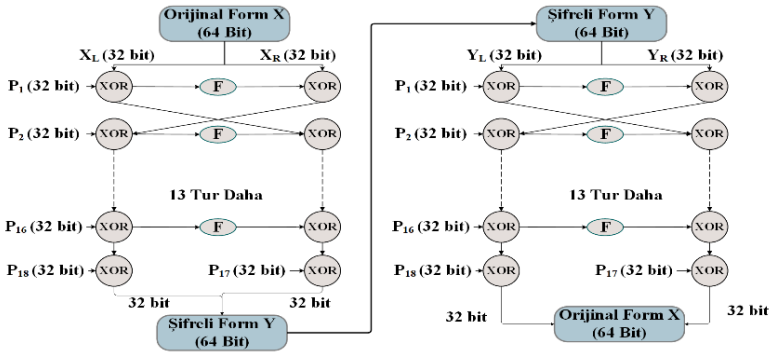


Şekil 4. AES kriptografik süreci

3.2.1.2. Blowfish

Anahtar uzunluğu (32- 448 bit arasında değişen) esnek ve DES' ten daha hızlı yapısıyla Blowfish algoritması, 64 bitlik bloklara mesajları bölerek kodlama yapmaktadır. Ayrıca bu 64 bitlik bloklar, anahtar ve veri genişletmeye bölünerek çalıştırılır. Kendine özgü diğer avantajlar (karmaşık tuş programı, verimlilik, yüksek hız ve bağımsız S kutuları gibi) sayesinde Blowfish en hızlı algoritmalardan biri konumundadır. Güvenlik riski taşıyan durumlarda

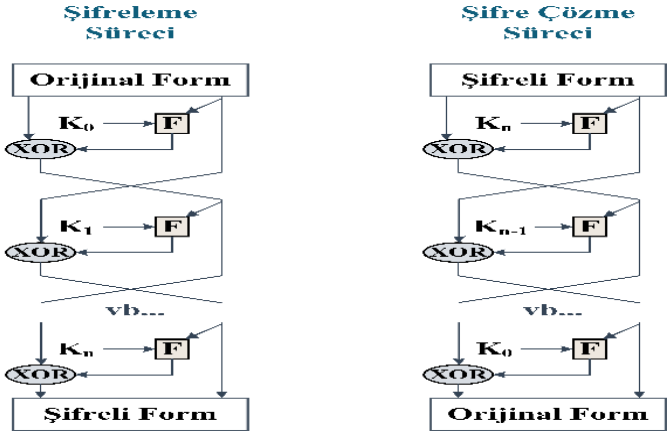
anahtarın aktarılmasındaki hassasiyet, zaman faktöründeki tüketim hacmi gibi vb. durumlar algoritmanın dezavantajlarıdır [20,21]. Blowfish kriptografik süreci Şekil 5 ile görselleştirilmiştir.



Şekil 5. Blowfish kriptografik süreci

3.2.1.3. Cast-128

Anahtar uzunluğu 8 bit artışla 40- 128 bit aralığında değişen Cast-128, 64 bitlik düz metin şablonunu 64 bitlik kodlanmış forma dönüştürürken 16 döngülük yapısıyla çalışmaktadır [22]. Cast-128 kriptografik süreci Şekil 6 ile görselleştirilmiştir.



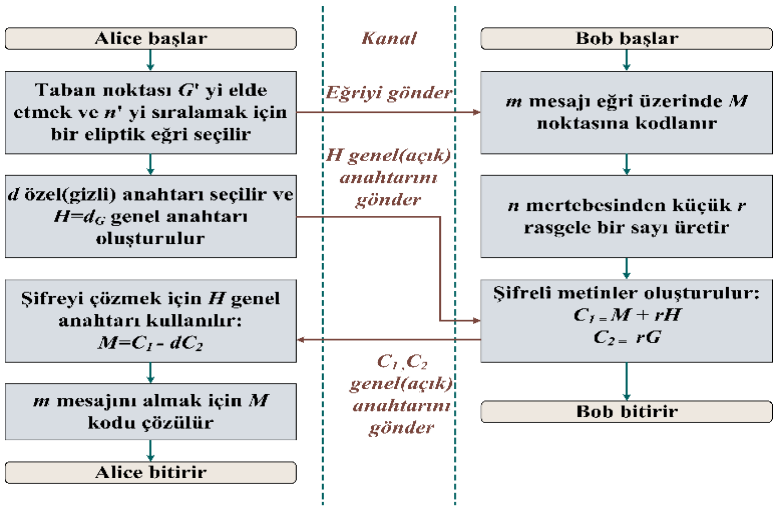
Şekil 6. Cast-128 kriptografik süreci

3.2.2. Kullanılan asimetrik şifreleme algoritmaları

Bu çalışmada kullanılan asimetrik anahtarlı şifreleme algoritmaları; ECDH, El- Gamal ve RSA' dır. Asimetrik anahtarlı sistemler, şifreleme ve şifre çözme sürecinde farklı anahtarlar (gizli ve açık) kullanılır. Şifreleme için kullanılan anahtar herkes tarafından bilinebilir fakat şifre çözmede kullanılan gizli anahtar sadece alıcı tarafından bilinmelidir. Simetrik yapılar kadar sık anahtar değişimine gerek duymaz çünkü şifrelemede kullanılan açık anahtar şifreli formu çözememektedir. Gönderici taraf alıcı tarafın gizli anahtarını bilemez ama açık anahtarı hakkında tamamen bilgi sahibidir. Simetrik şifrelenmeye göre daha zor kırılırlar. Gizlilik- bütünlük- kimlik doğrulama- inkâr edilememe kriterlerini sağlamaktadır. Taraflar arasında bilinmeyen tek bir anahtar(gizli) yapısı olduğu için şifre çözme süreci simetrik yapıya göre daha yüksektir (yavaştır) ve buda önemli dezavantajlardan biridir. Dosya türünün boyutuna göre üssel olarak artış göstermektedir. Ayrıca veri güvenliğini sağlamada çözülmesi zor matematiksel hesaplamalar yani büyük asal sayılar üzerine kurulu olduğundan işlemciyi ve diğer kaynakları daha fazla tüketir. Anahtar uzunluğu, simetrik yapılara göre daha kısa anahtar dizinine sahiptir. Güvenlik, anahtar uzunluğuna bağlıdır ve iki farklı anahtar yapısı olduğu için simetriklere göre daha güvenliklidir. Çok büyük sayılar ile işlem yapılmasından dolayı donanımsal yapıların entegresi zordur. Şifrelenebilecek veri miktarı simetrik yapılara göre daha düşüktür. Elektronik imzaların ortaya çıkmasının temelini oluşturmaktadır[16-19].

3.2.2.1. ECDH

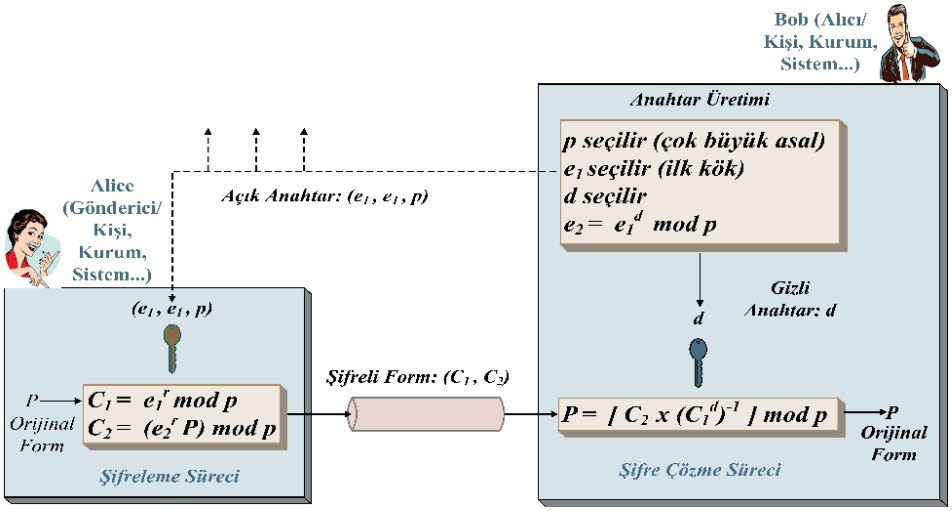
ECDH kriptografik süreci Şekil 7 ile görselleştirilmiştir. Görselde iletişim kanalı incelendiğinde; eğrinin bilgileri, ortak kullanılan anahtarı ve şifreli metni yansıttığı görülmektedir. Yani üçüncü şahıslar (kötü niyetli kişi, kurum vb.) özel anahtar erişimine sahip olmadan bu yapıya müdahalede bulunamazlar. Asimetrik şifreleme sistemlerinin avantajlarından biri olan ek güvenlikli hali, bu yansımanın karşılığıdır [22].



Şekil 7. ECDH kriptografik süreci

3.2.2.2. El- Gamal

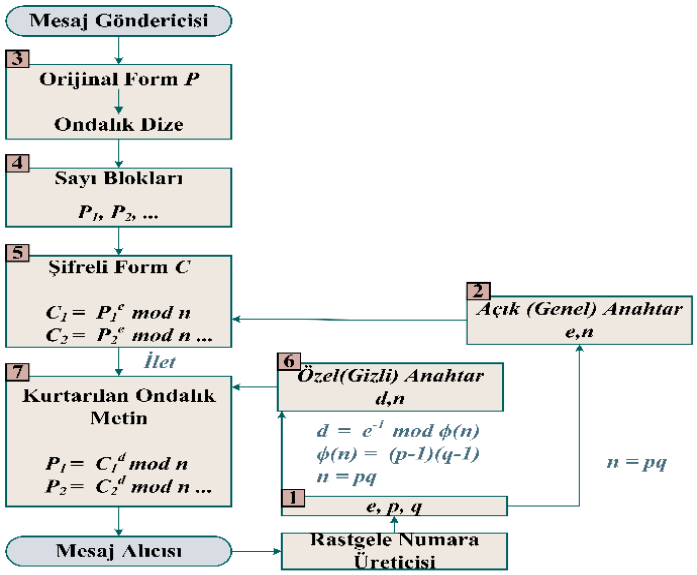
Asimetrik kripto sistemlerinden biri olan ve temeli Diffie – Hellman (DH) anahtar değişimine dayanan El Gamal algoritması; Taher Elgamal [23] tarafından önerilmiştir. Ayrık logaritma problemleri önerisi, imzalama yapısı ve şifreleme algoritmasından oluşan şablonuyla çoğu kriptografik yöntemlerin esinlenilen durumunda konumlanmıştır [24,25]. RSA asimetrik şifreleme algoritması gibi tekniklerden ayrılan yönü; güvenlik sağlamada El- Gamal' da büyük bir asal modülün ayrık logaritmalarının hesabına dayanmasıdır. RSA' da güvenlik; büyük tamsayılardan oluşan çarpanların bulunma zorluk derecesidir. El- Gamal'ın diğer bir üstünlüğü; kullanılacak mesajın her şifreli yapısında farklı bir forma dönüştürülmesidir yani sabit olamayan dinamik yapısı vardır [26-29]. Şekil 8 ile El- Gamal kriptografik süreci tasvir edilmiştir.



Şekil 8. El- Gamal kriptografik süreci

3.2.2.3. RSA

1977'de Ron Rivest, Adi Shamir ve Leonard Adleman'ın soyadlarının baş harflerinden ismini alan RSA algoritması; gizli tutulan iki büyük asal sayıyla birlikte bir yardımcı değerin birleşimi sonucu açık anahtar oluşturulur. İletilmek istenilen bilgi paylaşılan ortak anahtar ile herkes tarafından şifrelenebilir ama sadece gizli olan asal sayılara ulaşılmadıkça şifre çözme olamaz [30-32]. RSA' nın güvenliği kullanılan asal sayılarının çarpımlarındaki sonucunun çarpanlara ayrılmasının zorluğuyla eşdeğerdir yani anahtar boyutu ne kadar büyükse bu algoritmanın kırılması da o kadar güvenlidir. 2048 ve daha büyük bit uzunluğundaki anahtar boyutları yeterli güvenlikte kabul edilir (1024 bit uzunluğundaki anahtar boyutlu sistemlerin yakın gelecekte kırılacağı düşünülmekte [33]. Şekil 9 ile RSA kriptografik süreci verilmektedir.



Şekil 9. RSA kriptografik süreci

3.3. Kriptografik algoritmalarının başarım metrikleri

Kullanılan veri türü kapsamında değişkenlik gösteren kriptogafik bir sürecin başarım kriterleri, metinsel veri türünde aşağıdaki metriklere göre kıyaslanabilir [19]

- Şifrelenmiş veriye erişim için saldırı süresinin uzunluğu (sn),
- Şifreleme ve şifre çözme aşamalarında toplam harcanan zaman(sn),
- Şifreleme ve şifre çözme aşamalarında toplam ihtiyaç duyulan bellek miktarı(),
- Kurulacak sistem ile kullanılan algoritmanın uyumu.

4. Uygulama Sonuçları

Çalışmaya ait şifreleme ve şifre çözme performans sonuçları Tablo 1 ile bu bölümde verilmektedir. Ancak başarımları; seçilen dosya türü (örneğin; metin, video, sinyal, görüntü vb.), boyutu(örneğin; KB, MB, GB, …), karmaşıklığı(örneğin; karakter yapısı, multi özelikler vb.), anahtar yapısı(örneğin; anahtarlı, anahtarsız, hibrit) ve kullanılan bilgisayar platformu (örneğin; python, java vb. yazılım ve ram gibi vb. donanım) gibi çeşitli faktörlere göre değişim göstermektedir. Bu faktörler temelinde çalışmada, kullanılan bilgisayarın donanım özellikleri;

- *İşlemci (CPU)*: *11th Gen Intel(R) Core(TM) @2.70GHz*
- *Bellek (RAM)*: *16,0 GB, Intel I7-CPU, 16 GB RAM, 4 GB-GPU*
- *İşletim Sistemi: Windows 11 Pro 64-bit.*

Kullanılan bilgisayar yazılımı özellikleri; *Python 3.9.13, Vs Code 1.78.0.*

Tablo 1: Şifreleme ve şifre çözme performans sonuçları

BOYUT	ALGORİTMA	CPU		RAM		SÜRE		TOPLAM	
		Şifreleme	Çözme	Şifreleme	Çözme	Şifreleme	Çözme	Şifreleme	Çözme
100 KB	AES	4.2	3.5	3	3	0.12	0.5	7.32	**7**
	Blowfish	3.99	7	2	6	0.08	0.03	**6.07**	13.03
	Cast-128	4	4.2	4	1	0.07	0.003	8.07	**5.203**
	ECDH	2.95	2.4	2	1	0.071	0.002	**5.021**	**3.402**
	El-Gamal	3.3	4.7	4	6	0.045	0.035	7.345	10.735
	RSA	3.4	3.2	2	3	1.8	1.2	**7.2**	7.4
1 MB	AES	5.4	5.5	4	6	0.14	0.7	**9.54**	**12.2**
	Blowfish	3.55	5.9	9	10	0.09	0.01	**12.64**	15.91
	Cast-128	6	8.3	10	3	0.11	0.1	16.11	**11.4**
	ECDH	4.65	4.8	8	9	0.087	0.007	**12.737**	**13.807**
	El-Gamal	5.125	5.65	23	66	0.346	0.253	28.471	71.903
	RSA	-	-	-	-	-	-	-	-
5 MB	AES	6.5	6.8	11	12	0.26	0.12	**17.76**	**18.92**
	Blowfish	5.6	5.9	10	21	0.17	0.08	**15.77**	26.98
	Cast-128	7.1	8.5	25	5	0.24	0.12	32.34	**13.62**
	ECDH	6.36	7.36	8	7	0.144	0.023	**14.504**	**14.383**
	El-Gamal	6.1	9.52	25	352	1.95	1.74	33.05	363.26
	RSA	-	-	-	-	-	-	-	-
100 MB	AES	7.47	9.47	128	381	2.1	1.1	**137.57**	**391.57**
	Blowfish	8.52	10.63	84	396	2.39	1.98	**94.91**	**408.61**
	Cast-128	7.25	9.68	34	371	3.42	1.64	**44.67**	**382.32**
	ECDH	7.683	8.12	178	403	1.71	0.54	187.393	411.66
	El-Gamal	9.07	6.36	3447	5162	72.96	50.76	3529.03	5219.12
	RSA	-	-	-	-	-	-	-	-

5. Tartışma ve Sonuç

Bu çalışmada, gerçek ve tam bir veri seti olan *"The Da Vinci Code"* adlı içerik üzerinde, simetrik ve asimetrik şifrelemeye ait uygulama yapılmıştır. Veri seti üzerinden; 100 KB, 1, 5 ve 100 MB arasında değişen dört adet çeşitli metinsel dosya boyutları yapay olarak üretilmiştir. Yapay olarak üretilen bu dört farklı veri seti; üç farklı simetrik ve asimetrik şifreleme algoritması (AES, Blowfish, Cast-128, ECDH, El-Gamal ve RSA) ile performans analizi yapılmıştır. Şifreleme algoritmalarının metinsel dosya türleri için literatürde kabul edilen performans kriterleri; şifreleme ve şifre çözmedeki hızı (sn), bellek (MB) ve CPU(%) kullanım oranları temel alınarak başarımları değerlendirilmiştir. Çıkan sonuçlar incelendiğinde;

- 100 KB ölçekli bir veri seti ile **şifrelemede**; ECDH, Blowish, RSA ve **şifre çözmede**; ECDH, Cast-128, AES,
- 1 MB ölçekli bir veri seti ile **şifrelemede**; AES, Blowfish, ECDH, ve **şifre çözmede**; Cast-128, AES, ECDH,
- 5 MB ölçekli bir veri seti ile **şifrelemede**; ECDH, Blowfish, AES ve **şifre çözmede**; Cast-128, ECDH, AES,
- 100 MB ölçekli bir veri seti ile **şifrelemede**; Cast-128, Blowfish, AES ve **şifre çözmede**; Cast-128, AES,

Blowfish, algoritmalarının ilk üç sırada daha optimal sonuçlar ürettiği görülmüştür. Girişlere göre farklı algoritmaların performansının da farklı olduğu ve ikinci bölümde verilen literatürle neredeyse benzer veya yakın sonuçlar verdiği gözlemlenmiştir. RSA algoritmasının, anahtar yapısından kaynaklı kısıtlama gereği 100 kb dan sonraki boyutlandırmalarda kıyaslanmaya dâhil edilmediği ve en uzun şifreleme süresini tükettiği ayrıca belleği çok yüksek kullandığı, sonuçlarla teyit edilmiştir. Bu çalışmadaki ana hedef; farklı boyutlardaki veri setlerinin güvenliğini sağlamak için simetrik ve asimetrik anahtarlı algoritmaların performans sonuçlarını kapsayacak şekilde, literatüre son yıllara ait güncel bir uygulama sunmaktır. Simetrik algoritmaların yüksek boyutlu verilerde daha iyi çıkması, veriler arasındaki bağımlılıkların daha az olmasından asimetrik algoritmalara göre daha yüksek hızda süreci tamamlamaktadır. Taraflar arasında bilinen tek bir anahtar yapısı olduğu için şifre çözme süreci asimetrik yapıya göre daha düşüktür (hızlıdır) ve buda önemli avantajlardan biridir. Ayrıca donanım ile esneklik süreci ve özellikle 2000 yıllardan itibaren donanım platformlarındaki hızlı gelişmeler nedeniyle, başarım arttırma çalışmaları daha çok simetrik kripto sistemler üzerinden yapılmaktadır. İlerideki çalışmalar, simetrik şifrelemede; gizli anahtarın güvenlik sorunu ve asimetrik şifrelemede; hız ve bellek sorunlarının giderilmesine yönelik hibrit veya yeni nesil olarak adlandırılan kripto sistemlerin tasarımları olabilmektedir.

Teşekkür

Bu çalışma, Fırat Üniversitesi Bilimsel Araştırma Projeleri Koordinasyon Birimi (FÜBAP) tarafından ADEP.22.06 numaralı proje ile desteklenmiştir.

Kaynaklar

[1] Şatir E, Kendirli O. A symmetric dna encryption process with a biotechnical hardware. Journal of King Saud University – Science 2022; 34(3): 1-10.

[2] Alenezi MN, Alabdulrazzaq H & Mohammad NQ. Symmetric encryption algorithms: review and evaluation study. International Journal of Communication Networks and Information Security 2020; 12(2): 256-272.

[3] Kaya A, Türkoğlu İ. Evaluation of symmetric cryptography algorithms in terms of performance analysis. Cukurova 10th Internatıonal Scıentıfic Researches Conference; 2-4 April 2023; Adana-Türkiye. pp. 4048-462.

[4] Kaya A, Türkoğlu İ. Evaluation of asymmetric cryptography algorithms in terms of performance analysis. 4. International Cappadocia Scientific Research Congress; 16-17 April 2023; Nevşehir- Türkiye. pp. 1056-1070.

[5] Sood R, Kaur H. A literature review on rsa, des and aes encryption algorithms. In Vikram Dhiman & Pooja Dhand (eds.), Emerging Trends in Engineering and Management 2023; 57–63.

[6] Olutola A, Olumuyiwa M. Comparative analysis of encryption algorithms. European Journal of Tech. 2023;7(1): 1 -9.

[7] Luo Z, Shen K, Hu R, Yang Y & Deng R. Optimization of aes-128 encryption algorithm for security layer in zig bee networking of internet of things. Computational Intelligence and Neuroscience 2022; 1-11.

[8] Thirupalu U, Reddy EK. Performance analysis of cryptographic algorithms in the information security. International Journal of Engineering Research & Technology (IJERT) 2019; 8(2):63-69.

[9] Abood OG, Guirguis SK. A survey on cryptography algorithms. International Journal of Scientific and Research Publications 2018; 8(7): 410–415.

[10] Dixit P, Gupta AK, Trivedi MC, Yadav VK. Traditional and hybrid encryption techniques: a survey. In Networking Communication and Data Knowledge Engineering 2018; 4: 239–248.

[11] Mushtaq MF, Jamel S, Disina AH, Pindar ZA, Shakir NSA, Deris MM. A survey on the cryptographic encryption algorithms. (IJACSA) International Journal of Advanced Computer Science and Applications 2017; 8(11): 333-344.

[12] Brown D. The Da Vinci Code. ABD; Random House, 2003.

[13] Basu S, Karuppiah M, Nasipuri M, Halder AK, Radhakrishnan N. Bio-inspired cryptosystem with dna cryptography and neural networks. Journal Of Systems Architecture 2019; 94: 27-31.

[14] Kerckhoffs A. La cryptographie militaire. Journal Des Sciences Militaires 1883; 9: 5–38.

[15] Shannon CE. Communication theory of secrecy system. Bell Syst. Tech. J. 1949; 28: 656–715.

[16] Indrasena RM, Siva KAP, Subba RK. A secured cryptographic system based on dna and a hybrid key generation approach. Biosystems 2020; 197: 1-10.

[17] Rahman G, Wen CC. Omega network pseudorandom key generation based on dna cryptography. Applied Sciences 2022; 12(16): 1-19.

[18] Erişim Tarihi:10.07.2023, https://www.ssl2buy.com/wiki/symmetric-vs-asymmetric-encryption-what-are-differences

[19] Kodaz H, Botsalı FM. Simetrik ve asimetrik şifreleme algoritmalarının karşılaştırılması. Selçuk-Teknik Dergisi 2010; 9(1): 10-23.

[20] Panhwar MA, Khuhro SA, Panhwar G, Ali K. Saca: a study of symmetric and asymmetric cryptographic algorithms. IJCSNS International Journal of Computer Science and Network Security 2019; 19(1): 48-55.

[21] Al-Shabi MA. A survey on symmetric and asymmetric cryptography algorithms in information security. International Journal of Scientific and Research Publications 2019; 9(3): 576-589.

[22] Krishnamurthy GN, Ramaswamy V. Encryption quality analysis and security evaluation of cast-128 algorithm and its modified version using digital images. International Journal of Network Security & Its Applications 2009; 1(1):28-33.

[23] Li J, Luo Y, Wang E, Gao W. Design and implementation of real-time image acquisition chip based on triple-hybrid encryption system. Electronics 2022; 11(18): 1-29.

[24] ElGamal T. A public-key cryptosystem and a signature scheme based on discrete logarithms. IEEE Transactions on Information Theory 1985; 31 (4): 469-472.

[25] Erişim Tarihi:17.04.2023, https://en.wikipedia.org/wiki/ElGamal_encryption

[26] Erişim Tarihi:10.04.2023, https://www.educba.com/elgamal-encryption/

[27] Imran OA, Yousif SF, Hameed LS, Al-Din Abed WN, Hammid AT. Implementation of el-gamal algorithm for speech signals encryption and decryption. Procedia Computer Science 2020; 167: 1028–1037.

[28] Rani S, Kaur H. Technical review on symmetric and asymmetric cryptography algorithms. International Journal of Advanced Research in Computer Science 2017; 8(4): 182-186.

[29] Erişim Tarihi:10.04.2023, https://www.ques10.com/p/33937/el-gamal-cryptography-algorithm/

[30] Rivest R, Shamir A, Adleman L. A method for obtaining digital signatures and public-key cryptosystems. Communications of the ACM 1978; 21 (2): 120–126.

[31] Erişim Tarihi:10.04.2023, https://en.wikipedia.org/wiki/RSA_(cryptosystem)

[32] Erişim Tarihi:18.04.2023, https://www.geeksforgeeks.org/rsa-algorithm-cryptography/

[33] Al-Juaid N, Gutub A. Combining rsa and audio steganography on personal computers for enhancing security. SN Appl. Sci. 2019; 1(830): 1-11.