WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

A Comparative Analysis of AES and DES: Security, Efficiency, and Applications

Mr. Aayush Agarwal[1], Arun Saini[2]

Student, Computer Science Engineering
Arya College of Engineering and IT, Jaipur, Rajasthan
(Affiliated to Rajasthan Technical University)

ABSTRACT—

This paper discusses two pivotal symmetric key encryption algorithms in cryptography: the Advanced Encryption Standard (AES) and the Data Encryption Standard (DES). With an analysis of their security mechanisms, efficiency, and application domains, it is the goal of this study to enhance the reader's understanding of these encryption algorithms- their strengths and weaknesses. AES with its advanced design has become the current standard of the industry replacing DES, though both these algorithms hold historical and practical significance in securing digital communications. This paper notes their comparative performance and denotes some situations where one is favored over the other.

I. INTRODUCTION

Safeguarding the sensitive information against the unauthorised access is becoming a major challenge in today's digitisation. The Data Encryption Standard (DES) and Advanced Encryption Standard (AES) are encryption algorithms commonly used to implement secure communication over the networks. The widely accepted encryption standard originated in the 1970s. Its vulnerabilities, mainly linked to short key length, have exposed the fairly standard DES to brute-force attacks, which led to its gradual disuse. In an effort to address these maladies, AES was established in the late 1990s and is now considered the gold standard in encryption. AES is considered more secure, scalable, and performant than DES because of its sturdy design. This case presents a comprehensive comparative analysis of these two algorithms, discussing their structural differences, performance metrics, and application scenarios, so that the equivalent strengths and weaknesses of these competitive algorithms may be established.

II. Encryption Algorithms: DES and AES

Data Encryption Standard (DES)

i. Introduction & Historical Context: Developed in the 1970s by IBM, and officially standardized in 1977 by NIST, DES remained the leading encryption standard for over twenty years. DES employs a key size of 56 bits and a Feistel network structure that encrypts the data in 16 rounds. It was meant to deliver hopefully sufficient security, but even then, its short length became clearly evident as a weakness.
ii. Issues of Security: The primary shortcoming of DES is that it uses a relatively short 56-bit key, easily revealed by brute-force attacks. Breakthroughs in analyzing cryptographic systems, further intensified by differential cryptanalysis, exposed the disease of the algorithm. Thus, DES ceased to be acceptable in modern applications where high levels of data are expected to be protected.
iii. Applications and Legacy Use: DES may now be an outdated encryption standard, but it still exists in legacy environments of low security need where computational power is scant. It was employed in the early versions of SSL/TLS and ATM systems, and it is still used for some legacy encryption applications.

Advanced Encryption Standard (AES)

i. Introduction and Standardization: Established in 2001, the Advanced Encryption Standard (AES) was selected after an extensive and rigorous public competition organized by the National Institute of Standards and Technology (NIST) to replace the Data Encryption Standard (DES). AES supports key lengths of 128, 192, or 256 bits by providing a complete and robust security configuration in comparison to the weak DES. The design permits byte substitution, a row shifting process, column mixing, and key mixing, among others; this significantly enhances security through the spread of these transformations across several rounds.
ii. Security Features: The longer the keys and the advanced cryptographic design AES has introduce it has made most difficult the chances of brute-force analysis and any types of cryptanalytic attack. This enlarging of the key size, from 56 bits (in DES) to 128, 192, or 256 bits-also manages to significantly

increase the examination number combinations which could be subjected to hacking attempts-the bigger it gets, the more inefficient AES attacks become against it.

iii. Scalability and Efficiency: In terms of scalability and efficiency, AES runs faster and is therefore more scalable as compared to DES. Its design guarantees speed when encrypting and decrypting so it can fit into several applications; from secure communications and financial transactions through to cloud storage and government communications.

iv. Adoption and Current Relevance: The adoption of AES as a universal standard is essentially one of its main strengths in the world of security: highly secure and efficient. It fits neatly into various standards, such as SSL/TLS, IPsec, and PGP-and it is the encryption algorithm most commonly requested by users requiring security and speed.

III. Security Comparison

DES Security

i. Vulnerabilities: The small key size of the DES (56 bits) makes brute-force attacks particularly feasible. Attackers may use this method to systematically test all possible keys into decrypting the data. Several forms of cryptanalysis, such as differential and linear, reveal that these attacks are potentially effective against the security of DES because of its small keyspace. To a large extent, those are the reasons for the transition toward AES, which has been suggested as a more secure standard. The weak security of DES basically has rendered it obsolete in high-security situations like banking and governmental communications; the risk for breaches is simply too high. Hence, for new applications, DES is no longer valid for ensuring confidentiality and integrity of any data.

ii. Impact of Advancing Cryptographic Attacks: By now, the 56-bit key length is not of secure enough construction against modern threats due to the advancements in cryptographic techniques and their tooling alongside the exponential increase in computational power. As current capabilities for exhaustive key searches are made within reach of lower server costs, DES fell short in the backers of hyped forms of attacks. Pairwise advances in cryptographic attacks have led to the adoption and establishment of more advanced standards for encryption in AES, while the future of strong encryption awaits, which can deal with advanced cryptogamic attacks. Thus, DES is no longer suitable for far-reaching applications calling for stronger data encryption.

AES Security

i. Advantages: Because of longer key sizes (128, 192, and 256 bits), AES has other security advantages. In his work, these key sizes yield a massive key space, aggravating brute-force attacks. A type of structural design with a series of application rounds based on four transformations: byte substitution, row shifting, column mixing, and key mixing provides an integral defense to common forms of cryptographic assaults like a differential and linear cryptanalysis. The layered approach applied makes it an obstacle for AES to resist any evolving threats. AES is one such algorithm that can effectively handle the information of the modern cyber world.

ii. Modern Application Suitability: AES is known for its high speed and security. Thus, AES suits a variety of uses. The factoring scalability and security features have made it an ideal choice for secure online transactions, government communications, cloud computing services, embedded devices, etc. With SSL/TLS and IPsec standards having AES integrated into them, its place as a standards implementation is well established. AES has seen the rapid penetration into the market, indicating its performance in protecting the sensitive data in a digitalized, interconnected world, which itself has high stakes when it comes to breaches.

IV. Efficiency Comparison

DES Efficiency

i. Processing Speed: At first, DES was efficient in performing its encryption and decryption operations with a balance of speed and security, enough for usual requirements. However, DES serves inadequate requirements for modern data environments in terms of scalability, given its limited key sizes and processing time. A single block size and 16 rounds of processing result in slower encryption and decryption times than concatenated modes, rendering it ineffectual for high-speed applications or our current client's data-intensive applications, such as virtual cloud storage and real-time data encryption in streaming services. The modest processing and speed characteristics of DES make its use inappropriate in contexts where the delivery of rapid power is pivotal.

ii. Computation Reluctance: Less computation is required to run DES, which, once again, was a strong advantage when the technology was very new, as hardware capabilities then were far less than they are now. The compromise is a level of security that is weakened by the shortage of a key; in actuality, only 56 bits are available at that time to secure the document being transmitted. In shrouding sensitive data under attack from modern cryptographers, this key size poses an achievement limitation. In addition, the limited capabilities serve to render DES less suitable for any environments where security is absolutely critical, including those such as financial or government. As a result, it becomes less relevant and obsolete for any future application requiring fruitful protection of any data in transit.

AES Efficiency

i. Processing speed: AES has an edge over DES as it processes data faster with such large key sizes. It can maintain speed with increased data volume. It can process data much faster than DES, making it a suitable choice for modern applications that require a quick encryption and decryption process such as online banking transactions, cloud computing, and streaming services. Its scalability ensures that AES handles various data sizes without compromising speed and security. This is what makes AES a more suitable choice for high-media environments.

ii. Justifiable Computational Requirement: While AES demands a large amount of such an imposed computational time, the edge goes back to security and efficiency because AES security is largely validated. With larger key sizes, 128, 192, and 256 bits, and multiple transformation rounds, the processing requirement is seen to be greater than DES. Nevertheless, this increased computational effort is necessary to handle the larger key space and the more complex workings of encryption. The ability to handle data while offering strong security makes AES an effective alternative to speed and security today.

V. Applications and Use Cases

A. DES Applications

i. Legacy Systems: DES was popular as a standard encryption algorithm in its time and was integrated into many systems, such as early versions of the SSL/TLS protocols, ATMs, and smart cards. Nevertheless, due to different factors, such as compatibility with legacy systems, DES is still used on legacy systems, EVEN though it's giving way to stronger algorithms. Because DES was traditionally accepted by a larger percentage of companies, it continued to be used in legacy systems where the protection of high-risk data was not a primary issue, for instance, for the compatibility and cost reasons.

ii. Transition to AES: Cryptographic flaws in DES were unveiled over the years forcing the development of AES, which sought to fill the selected standard for encryption. The passing over from DES to AES emphasizes the changing needs of modern cryptography, which is bent on satisfying the demands for strong protection against difficult attacks. This also serves to provide strong data protection to modern applications in compliance with current standards for security.

B. AES Applications

i. AES is one of the prominent usages in a variety of applications as it perfectly balances speed, security, and versatility. Secure communication, online banking, digital rights management, and cloud computing services are some examples. It was further exemplified in its practicality with several major protocols such as SSL/TLS, IPsec, and PGP, which lay testimony to its robustness in thickly guarding sensitive data in transport and storage. This flexibility makes AES a necessary component of modern encryption practices.

ii. Some implementations of AES may entail secure data storage solutions, secure boot mechanisms for firmware protection, and mobile device encryption protocols. Its being able to provide high levels of security while managing great amounts of data in an efficient manner counts a lot for modern cryptographic practices. The overwhelming use of AES in these areas further qualifies as a mark of significance in preserving their value of digital assets across industries.

VI Performance Evaluation and Practical Considerations

Performance Metrics

i. Speed and Throughput: AES is considerably quicker than DES and throughputs more data than DES, especially when larger data files are encrypted. Having rounds of changes has made AES robust, enabling a swift means of encrypting and decrypting texts quickly. This efficiency is crucial for present times with demands such as online banking, cloud computing, and real-time communications, where the efficient processing of data is crucial. Thus, AES is practically superior to DES in implementing applications since it executes data-rich tasks with minimum latency.
ii. Latency and Overhead: Though AES permits somewhat higher latency owing to the numerous rounds that would be needed for larger key sizes (e.g. 256 bits), it outperforms all productivity metrics with high efficiency. This is especially important in contexts that require secure and quick data encryption. Diaclystor suggested the AES algorithm is still able to offer an acceptable performance level across various applications, while not adversely affecting the total utilization of computational resources.
iii. Computational Resources: AES is more computationally heavy than DES because it requires more complex rounds of transformation and its key size is larger. Still, this choice is worth it because of higher security and enhanced performance. AES performs larger amounts of data more easily without a considerable slowdown whatsoever; this makes it preferred for high-security environments, such as military establishments, financial networks, and large enterprises.
Why do large companies like ING, Paypal, ADP, and Spotify keep using Docker? Why is Docker adoption growing that fast? Let’s cover the top advantages of docker to better understand it.

Practical Scenarios

i. Resource-Constrained Environments: DES may be limited to those environments with minimal computational resources; e.g. though it does see use in older embedded systems or legacy hardware that cannot support AES. In most cases, however, the AES is preferred-even in constrained environments-because such situations offer scalability, higher security, and consistency in performance. Its adaptability to different hardware and software environments ensures that it remains effective in protecting the data in a resource-constrained setup.
ii. Selecting the Right Algorithm: The choice between AES and DES should be dictated by the needs of the application, including the sensitivity of the data, availability of computational resources, and performance needs. DES could still work in lower-security contexts or with legacy systems, AES's security, efficiency, and ability to scale, therefore, render it as the technology of choice for new systems and applications concerned about guarding data. AES hence becomes the long-term protection solution for the sensitive data.

Conclusion

AES is much more secure and efficient than DES, which has already become obsolete for modern applications. Due to DES's key-length limitations and relatively rudimentary design mechanisms, it has become inadequate in addressing present-day data encryption requirements. On the other hand, AES has become the de facto industry standard in encryption practices: a cryptographic design with larger key sizes and a more sophisticated architecture which also allows for better scalability and serves critical roles with robust security mechanism and efficiency in protecting sensitive data in different areas.
AES is highly recommended for high-security and high-performance applications, while DES could still find use in legacy systems, which aren't suited for new implementations due to secure vulnerabilities. Migration to AES is of paramount importance for ensuring solid and trustworthy data protection in the digital world because security requirements are always changing.
For the most part, no new encryption standards are supposed to be formed right away. It has its stance concerning AES as a ground; specific matters toward the development need to take off. New algorisms must be crafted with heightened security and performance capabilities to counteract unlocking computing power and novel cryptographic threats. This would be indispensable to retain the integrity of digital assignments in a more interconnected world.

The comparative analysis of AES and DES accentuates that the encryption algorithm chosen for encryption should suit modern-day security needs and operational exigencies. The wide acceptance of AES and the demonstration of its ongoing efficacy and operational capability underscore its continuing relevance and trustworthiness that cement its position as a core feature of modern cryptographic practice.

REFERENCES

[1] Daemen. J. & Rijmen. V. (Year 2002).The Design of Rijndael- AES - The Advanced Encryption Standard, Springer-Verlag. 1-238.
URL-[https://cs.ru.nl/~joan/papers/JDA_VRI_Rijndael_2002.pdf]

[2] National Institute of Standards and Technology (Year 2001). Announcing the Advanced Encryption Standard (AES) (197).
1-51.
URL-[https://nvlpubs.nist.gov/nistpubs/fips/nist.fips.197.pdf]

[3] National Institute of Standards and Technology (Year 1999). Data Encryption Standard (DES) (46-3).
1-23.
URL-[https://csrc.nist.gov/files/pubs/fips/46-3/final/docs/fips46-3.pdf]

[4] Katz, J., & Lindell, Y. (2020). Introduction to Modern Cryptography (3rd Edition). CRC Press.
Pages: 97–145.
DOI: 10.1201/9780429347004