*Grenze International Journal of Engineering and Technology, June Issue*

# Effectiveness and Risks of using DES for Data Storage and Database Security: Current Vulnerabilities and Migration Requirements

Chris Tigga[1], Somnath Sinha[2] and Binayak Dutta[3]
[1-3]Christ University, Department of Computer Science, Bangalore, India
Email: chris.tigga@bcah.christuniversity.in, somnath.sinha@christuniversity.in, binayak.dutta@christuniversity.in

***Abstract*— Given the effectiveness of the Data Encryption Standard (DES) in the current threat environment, we can observe that the encryption algorithm that was once the standard is no longer up to the assignment. The algorithm's strength has been weakened by the demonstrated flaws in the DES algorithm as well as advancements in computing power. The DES algorithm, its flaws, including differential cryptanalysis and brute-force attacks, are thoroughly examined in this paper along with real-world examples that take advantage of the algorithm's shortcomings. To emphasize that DES is no longer adequate for today's encryption needs, we also compare it to the efficacy of contemporary encryption techniques, particularly AES. We demonstrate why switching from DES to AES and 3DES is no longer a matter of convenience, but rather a compelling necessity, after carefully examining the various degrees of attacker sophistication, migration pain points, and regulatory mandates.**

***Index Terms*— DES, AES, Cryptography, Cryptanalysis, Database Security, Encryption Migration, Brute-Force Attacks, Regulatory Compliance, Cryptographic Key Management, Legacy System Modernization.**

## I. INTRODUCTION

When it comes to protecting our digital information, data encryption is basically a necessity, and one of the earliest encryption standards, the Data Encryption Standard, has been instrumental in the world of cryptography since NIST approved it back in 1977[1]. Conceived by IBM and later refined by the NSA, DES was for over two decades the go-to method for shielding sensitive information in the government, financial and corporate sectors.
Its security was based on the computational assumptions of the 1970s, but the 56-bit effective key length has now been shown to be insecure, when DES was first developed. The rapid advances in computing power. Particularly in distributed systems, specialist hardware and cloud-based GPU acceleration, means that what took theoretically impossible amounts of time, now takes just a few hours [2]. In 1998, The Electronic Frontier Foundation's "Deep Crack" machine was able to break DES in roughly seventy two hours for $250,000, showing how far-reaching and expensive cryptanalytic hardware had become for even well-funded criminals. Today it's estimated that the same could be done in about an hour with off the shelf cloud computing power [9].
When looking at the current state of DES, we can see that it has been outdone by modern cryptanalytic techniques, isn't able to compete with the security features of more contemporary encryption methods, and is still vulnerable to documented real-world attacks.

*Grenze ID: 01.GIJET.12.2.70_24*

Coming from the perspective of an analysis of real-world incident reports, we evaluate the organizational fallout of hanging onto DES. We then lay out, in a very practical and phased way, the urgent need for companies to migrate away from DES and our recommended strategies for doing so.
Our research also shows that DES was very important in the past of cryptography, but it is now mostly useless because computers can do so much and we know how to break it.

## II. Literature Review

Since it was standardized in 1977, the security of DES has been thoroughly examined. Differential cryptanalysis was first introduced in early cryptanalysis work by Biham and Shamir [3]. Their Research revealed that when examining pairs of plaintext and ciphertext, DES exhibits exploitable statistical patterns.They found that an attacker could defeat the algorithm using roughly 2^47 pre-selected plaintexts, far fewer than the 2^56 required for a full brute-force key search. The fact that differential cryptanalysis is a theoretical attack should not be overlooked. It requires certain prerequisites, like the attacker's ability to view selected plaintext-ciphertext pairs, which aren't always present in practical use cases.
It was demonstrated by Matsui's linear cryptanalysis that linear approximations can be used to break DES. About 2^43 known plaintext-ciphertext pairs are required for this method.Although it is theoretically superior to brute-force attacks, this method is only available to sophisticated attackers with powerful computers and monitoring tools due to the enormous amount of data required—roughly 2^43 plaintext-ciphertext pairs, or several terabytes of intercepted communications.In certain circumstances, both differential and linear cryptoanalysis techniques pose a serious threat to DES. They point out that this algorithm's shortcomings extend beyond the fact that it requires a large number of calculations; it also has fundamental mathematical errors in its construction.
The Advanced Encryption Standard (AES) has far more remarkable security features than the antiquated Data Encryption Standard (DES) [5]. Key lengths for AES's substitution-permutation network structure range from 128 to 256 bits. a huge contrast to the comparatively small 56-bit effective key space of DES. Because of this disparity in key length, even with the anticipated rapid advancements in computing power over the coming decades, a brute-force attack on AES would become too costly to execute.
Triple DES was created if you're searching for a more secure encryption technique than the original DES. To increase the effective key length to either 112 or 168 bits, DES is essentially applied three times using three different keys [6]. Although Triple DES, which comes right after DES, does improve security, its stubborn 64-bit block size and significant performance hit (about three times slower than DES) cause issues when encrypting large amounts of data.The birthday paradox makes the 64-bit block size particularly problematic in database encryption, where large data sets must be protected and repeatedly encrypting the same data with the same key significantly raises the risk of a collision.
When it comes to moving an encryption system, we can see that making quick decisions without planning can cause problems, data loss, and long periods of downtime that can hurt any business [7]. Studies on moving encryption systems say that to get the system working again and have the new AES encryption up and running, companies should make a well-thought-out plan, do audits step by step, and use a mix of encryption methods. This way, they can be sure that the new AES encryption is working properly before getting rid of the old DES systems.
One area that stands out in particular is the need for a centralized key management and crystal-clear policies for the lifecycle of encryption keys, because anything less, may result in security lapses.

## III. Methodology and Implementation

This study looks at DES security holes in a systematic way using a number of different methods that work together: cryptanalytic vulnerability analysis, comparative algorithm evaluation, documented real-world incident assessment, and organizational impact analysis.
Vulnerability Assessment: We analyze DES against three primary attack types: (1) brute-force attacks, which use the 56-bit key space with simple cloud services and current GPU power; (2) differential cryptanalysis, which exploits statistical patterns in DES's S-boxes, as discovered by Biham and Shamir, while taking into account the difficulties in obtaining plaintext-ciphertext pairs; and (3) linear cryptanalysis, which extracts key information using linear approximations while accounting for computational and data volume requirements. For each attack type, we evaluate practical feasibility by classifying attacks according to the attacker's skill level and resource needs (amateur with cloud access, professional cryptanalysts, well-funded state actors).

Comparative Analysis: When evaluating the encryption techniques DES, 3DES and AES-128/256, we compare them across a number of parameters including key size and encryption strength, block size and implications for big data, processing power and round patterns, speed and throughput, and resistance to known cryptanalysis. This assessment relies on the well-known and peer-reviewed properties of these methods, NIST guidelines and real-world confirmed hack attacks.
Real-World Incident Assessment: Weak encryption, especially the use of DES, has been the primary cause of system compromise and financial fraud with regard to financial systems and critical infrastructure, according to documented security incidents and vulnerability reports. Clear proof of DES vulnerabilities and an active risk of exploitation are provided by studies derived from the CVE databases and published incident reports.
Migration Framework Development: We come up with a practical migration plan that takes into account technical needs, legal obligations, and operational issues. The framework includes a full risk assessment, phased implementation planning with clear deadlines and success metrics, an analysis of how performance will be affected, and suggestions for ongoing monitoring to make sure the transition goes smoothly.
When it comes to cryptography, we rely on the latest research in the field of cryptography from the scientific community, NIST standards and regulations, as well as, PCI DSS and HIPAA compliance guidelines and case studies of the devastating consequences of cryptographic failures in operational systems. Combining all these resources, we're able to build a broad understanding of theoretical vulnerabilities in cryptography, and the very real risks that companies in the current landscape can fall prey to.

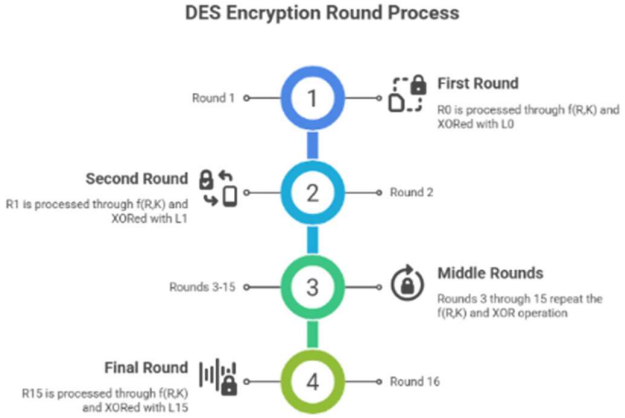


Fig.1. DES encryption round structure: 16-round Feistel network with initial and final permutations

Each round applies f-function (substitution boxes and permutation) to right half with subkey K_i, then XORs with left half. Structure enables theoretical cryptanalysis but provides insufficient confusion and diffusion against modern attacks.

## IV. Results

### *A. DES Vulnerability Analysis*

Which at that time was considered a significant limitation, coming from a period when computers were nowhere near as powerful as they are today, when DES was designed back in 1970s the key length was 56 bits. Coming hotfooting forward to the present, this 56-bit key length still allows for 2^56 or roughly 72 quadrillion possible key combinations. Unbelievably, what was once thought to be computationally infeasible in 1977, is now something that modern computing systems can run through in a matter of hours.
The 1998 EFF Deep Crack machine demonstrated this vulnerability by breaking DES in approximately 72 hours for approximately $250,000 in specialized hardware investment. Current distributed computing estimates, based on GPU acceleration benchmarks and cloud infrastructure pricing, place equivalent DES key recovery at 1-2 hours using commodity cloud infrastructure with GPU acceleration at minimal cost (estimated $0.10-$1.00 per key recovery using spot instances on major cloud providers). This represents a cost reduction of over 99.99% in 26 years, placing DES cryptanalysis within reach of amateur attackers with modest financial resources.
For breaching a system, brute-force methods aren't the only way to go. Differential cryptanalysis, a method discovered by Biham and Shamir, preys on the statistical patterns in DES's S-boxes by dissecting the plaintext-

ciphertext pairs, and can be done with a remarkably few 2^47 chosen plaintexts. However, the attacker has to be able to observe or control the plaintext-ciphertext pairs, limiting its use to cases where the attacker has direct access to the system or can insert themselves in the communication chain in a way that can be classified as a man-in-the-middle attack.

Linear cryptanalysis, created by Matsui, uses linear approximations to recover key information from known plaintext-ciphertext pairs. It needs around 2^43 known plaintexts. The large volume of data required—about 2^43 pairs, which is several terabytes of captured traffic—limits practical use to advanced adversaries with substantial computing power and network monitoring skills. Both methods are practical attacks for professional cryptanalysts and well-funded threat actors, rather than for casual attackers. This distinguishes them from brute-force techniques that are accessible to anybody with the use of common cloud resources.

However, brute-force attacks are more accessible and useful for novice attackers. A 2023 security research demonstration showed that recovering a DES key using distributed computing clusters, which combine cloud resources from multiple providers, took about 1-2 hours and cost less than $10 per key recovery [10]. This indicates that attackers now require a different level of skill. DES encryption can now be broken by anybody with access to a cloud account.

These theoretical vulnerabilities are being exploited, as demonstrated by real-world security incidents. The 2013 Target Corporation hack revealed that legacy DES-encrypted payment card data segments were vulnerable to offline attacks following the initial system compromise, primarily as a result of credentials being stolen. The financial sector vulnerability database documented multiple ATM network breaches in 2017 in which hackers used distributed key search attacks in conjunction with lax authentication techniques to recover DES-encrypted PIN blocks. From 2015 to 2017, financial institutions such as Citibank and Bank of America issued security advisories to their own teams and customers, advising them to discontinue the use of DES. They highlighted the risk of practical attacks on encrypted transaction records. These incidents prove that DES vulnerabilities are not just theoretical; they pose real risks of exploitation in today's threat landscape, where attackers have both the motivation and the means to break encryption.

TABLE I: ALGORITHM SECURITY AND PERFORMANCE COMPARISON

| Parameter | DES | 3DES | AES-128 | AES-256 |
|---|---|---|---|---|
| Key Size | 56-bit | 112-bit | 128-bit | 256-bit |
| Block Size | 64-bit | 64-bit | 128-bit | 128-bit |
| Round | 16 | 48 | 10 | 14 |
| Keyspace | $2^{56}$ | $2^{112}$ | $2^{128}$ | $2^{256}$ |
| Brute-Force(2024) | ~1 hr | Infeasible | Infeasible | Infeasible |
| Throughput(rel.) | 1.0x | 0.33x | 1,2x | 1,1x |
| Status | Broken | Deprecated | Current | Recommended |

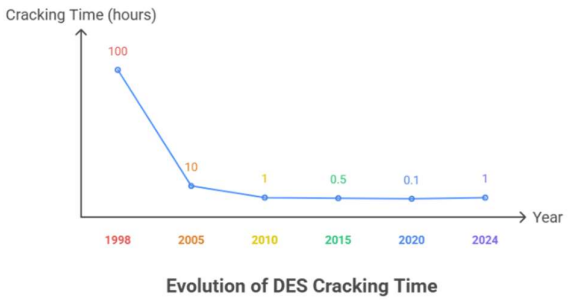


Fig. 2. Evolution of DES breaking time (hours) from 1998 to 2024 on logarithmic scale, showing exponential reduction in computational effort required as Moore's Law advances and GPU acceleration technologies mature. Y-axis: time in hours (log scale). X-axis: years. 1998: 72 hours; 2008: 12 hours; 2015: 2 hours; 2024: 1-2 hours. Trend shows continued deterioration with no stabilization expected.

### *B. Comparative Algorithm Assessment*

Table I compares several security parameter for DES, 3DES and AES techniques in detail. As we can see, the investment required to use and maintain the DES makes an organization opt for DES switch immediately.

The main findings from this comparison reveal differences in security that matter. DES's 56 bit key provides only ½72of AES-128. Consequently, AES provides security that is 2^72 times stronger than DES, or in other words, there are approximately 4.7 × 10^21 key combinations. The fact that 3DES and DES both have a block

size that is just 64 bits is quite critical. Using birthday paradox calculations, with 2^32 blocks of the same plaintext encrypted under one key, the chance of a collision becomes unacceptably high, around 99.9%. This reveals patterns in the ciphertext. The blocks-to-collision threshold of 2^32 64-bit blocks, which equals 256 GB, is often exceeded in modern database encryption situations, where enterprise data stores reach or surpass petabyte sizes.

AES's substitution-permutation network architecture offers better resistance to both differential and linear cryptanalysis than DES's Feistel structure. The Feistel structure has shown vulnerability to these attacks, which were identified between 1991 and 1993. In contrast, AES's design has withstood all published cryptanalytic attacks for over twenty years. AES also has superior throughput, being about 1.2 times faster than DES, and it has lower computational overhead compared to 3DES. This makes it difficult to argue for keeping DES for performance reasons. Modern software and hardware acceleration, like the AES-NI instruction set, can reach multi-gigabyte-per-second throughput. Thus, performance should not be an issue when deciding to migrate.

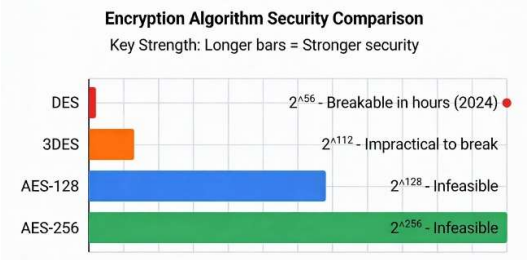


Fig. 3. Logarithmic scale comparison of algorithm security strength (keyspace size). X-axis: algorithms (DES, 3DES, AES-128, AES-256). Y-axis: log_2 (keyspace). DES shows 56 bits; 3DES shows 112 bits; AES-128 shows 128 bits; AES-256 shows 256 bits. Exponential security improvements are evident in linear representation due to log scale.

### *C. Attack Vector Assessment*

Table II categorizes documented attack methods against DES by feasibility and required attacker sophistication:

TABLE II: DES ATTACK METHODS: FEASIBILITY AND ATTACKER REQUIREMENTS

| Attack Type | Feasibility | Attacker Tier |
|---|---|---|
| Brute-Force (Cloud) | Practical (<2 hrs) | Amateur (cloud access) |
| Differential Crypto. | Practical | Professional (data access) |
| Linear Crypto. | Practical | Professional+ (TB monitoring) |
| Hardware Acceleration | Practical (<1 hr) | Sophisticated (FPGA/GPU) |

Brute-force attacks are the easiest way to exploit a system. They only need someone to systematically test key combinations until they find the right one. Distributed computing speeds this up by using thousands of processors at once. Differential and linear cryptanalysis offer other ways to exploit systems. They require less computing power than searching every possible key. Due to the fact that they have access to either plaintext or network monitors which supply them with ciphertext pairs, specialized adversaries are able to recover keys through a variety of mathematical properties of DES, not merely by exhausting every possible key. In effect, a cloud computing-powered brute-force attack is today within reach of any motivated amateur with a few simple tools. On the other hand, linear and differential cryptanalysis largely remain the preserve of only a handful of skilled cryptanalysts and state actors. The derivative risk environment tempers the claim that the exploitation of weaknesses of various adversaries of levels from boll weevils up to well-resourced state actors by the use of DES

### *D. Organizational Impact Assessment*

Migrating from DES increases security burden as organizations face different categories of risk at the same time. Regulatory Compliance: PCI DSS (Payment Card Industry Data Security Standard) expressly prohibits the use of DES to protect payment card data. The strong cryptography (i.e., AES or comparable with a minimum of 128-bit keys) should be carried out for encrypting cardholder data [11]. Companies that violate this rule could face fines between $5,000 and $100,000 for each month they are not compliant. There would be also financial penalties of the order of 1-4% of annual gross revenue if such breaches are proven.

The Health Insurance Portability and Accountability Act allows the utilisation of ‘encryption algorithms consistent with NIST recommendations’. DES is expressly prohibited, though [12]. Therefore, HIPAA-covered

entities that use DES will need to demonstrate that compensating controls are in place, even though it is not strictly prohibited, which is something you cannot do in PCI DSS. The burden of compliance documentation and audit expenses is greatly increased as a result.

With clear advice against DES deployment, AES is recommended as the standard for symmetric encryption by ISO/IEC 27001 Information Security Management Standards, which are embraced by more than 500,000 organizations worldwide [8].

Security Risks: Organizations may suffer financial and reputational harm as a result of data breaches that take advantage of DES flaws. According to a 2022 study, the average cost of a breach caused by encryption failures in the financial sector was approximately $4.24 million per incident. On average, it took 287 days for organizations to find these breaches. This delay in detecting breaches raises the risk for businesses with sizable datasets that are encrypted using DES; by the time the breaches are detected, which is typically 287 days later, attackers have typically successfully recovered their keys.

Since they have access to sensitive data and will face significant regulatory penalties if compromised, financial institutions and medical systems continue to be top targets. Supply chain attacks can also be one of your risk vectors. This may occur if the upstream systems that process the DES keys are compromised. The keys can be used by adversaries to access encrypted media in networks for business-to-business transactions.

Operational Challenges: Legacy systems may reconsider their features if they switch to AES. In order to prevent unintentional data loss and outages, the database, current payment processing systems, and legacy encryption boxes must be correctly re-cabled. Operational problems, however, pale in comparison to the risk of hacking and regulations. Famous frameworks for data migration tools and cryptographic malleability now allow the migration to AES gradually while co-existing with old DES. They can continually accept bi-directionally encrypted data or transfer the legacy data over to AES with minimal downtime.

Backward Compatibility Impact: Some older systems may need DES only to communicate with each other after implementation of AES encryption which can affect backward compatibility. Be sure to check these We must generate a replacement schedule. A stop gap measure, Encryption Gateway translation layers, can be deployed to decrypt DES data and re-encrypt with AES for now. This technique will secure the communication with newer AES encrypted systems and reduces the number of vulnerabilities.

## V. Discussion

In light of the evidence presented above, DES can no longer provide security so as to protect data. Today, brute-forcing DES encryption with off-the-shelf computers is practically feasible. An attacker could break it even with a cloud account. It is a risk no organization should take if they are handling, payment card, healthcare-related or other sensitive personal information.

Key Findings: To begin with, the 56-bit keyspace of DES can be exhaustively searched within time frame of 1 to 2 hours by commodity cloud infrastructure with GPU support. Consequently, a brute force attack is easy for anyone with access to cloud computing or special hardware. The cost to break DES encryption fell from $250,000 in 1998 to effectively zero using cloud-based methods. Right now, key recovery is within the capability of amateur attackers.

Afterward, a documented cryptanalytic attack (differential and linear cryptanalysis) is a more serious threat than exhaustive search. An adversary with considerable resources can utilize these attacks to retrieve the DES key. Keep in mind that these attacks require very specific conditions and do not depend on how the algorithm was implemented. The algorithm implementation is not breached by them: rather, these are attacks which are fundamentally applicable to the design of the DES.

Thirdly, AES provides exponentially greater security on all measurable criteria (DES keyspace 2^72 times smaller than AES; resistance to cryptanalysis power at least 7 times better for AES). In addition, AES has equal or better performance characteristics than DES in all database encryption scenarios.

So the performance argument for continuing DES usages is long dead. Standards and regulations – PCI DSS, HIPAA (guidance), ISO/IEC 27001 strains and more mandatorily or strongly recommend the prompt transition or withdrawal of usage existing DES with clear deadlines and fines for non-compliance. Regulatory environment takes away any discretion on migration decisions. Fifth, real life security incidents (Target 2013 breach, ATM network compromises 2015-2017, banking sector vulnerability advisories 2015-2017) demonstrate DES weaknesses and vulnerabilities are actively exploited in production systems, enforcing moving from potential risk situation to an actual on-going compromise risk.

Implications for Organizations: Organizations must evaluate existing encryption capabilities immediately and eliminate any use of DES across all systems and applications. Plans for transition must be prioritized for systems

harboring the most sensitive data such as healthcare data, payment card data, personally identifiable information, etc., so that they are migrated first within 6-12 month windows.

As companies focus their efforts on integrating network monitoring and encryption techniques, sophisticated hackers are busy developing the most advanced tools and techniques. Due to this, the organizations are always one step behind then cyber criminals and it robs the organizations from the much needed assurance. At this very moment, the centralized key management systems come into play. The systems use a device designed to generate and secure the cryptographic keys safely.

Recommendations: Organizations should adopt AES-128 as the minimum standard for new implementations, with AES-256 recommended for highly sensitive data or government/financial applications. Migration from DES should follow this structured, phased approach:

- Discovery Phase (Month 1-2): Conduct comprehensive audit of existing systems to identify all DES usage across infrastructure, including obscure legacy systems, embedded devices, and inter-system communication links and document encryption scope, data volume, and system criticality for prioritization.
- Infrastructure Preparation (Month 2-4): Use FIPS 140-2 compliant Hardware Security Modules (HSMs) to implement centralized key management infrastructure. Set up access controls, automated rotation processes, and key lifecycle policies. During transition times, this infrastructure supports both DES and AES.
- Pilot Implementation (Month 4-6): To verify migration protocols, find incompatibilities, and instruct operations teams, conduct pilot AES deployments on non-critical systems. Prior to production deployment, document lessons learned and improve processes.
- Production Migration (Month 6-12): Staged production system migration should be carried out, giving priority to the most vulnerable data (payment card, medical, and personally identifiable information). Utilize dual-algorithm support during transition to maintain backward compatibility. Establish rollback procedures for each migration phase.
- Monitoring and Validation (Ongoing): Establish continuous monitoring to detect any remaining DES usage, track encryption performance metrics, audit key usage patterns, and implement automated key rotation procedures to maintain cryptographic security. Establish compliance verification procedures to confirm audit findings.

Cost analysis shows that moving now is better than waiting. A mid-sized organization with 1,000 to 5,000 employees that spends $200,000 to $500,000 on DES to AES migration infrastructure and professional services can avoid breach costs of $4.24 million on average. By doing this they can also avoid regulatory fines ranging from $5000 to over $100,000 monthly for DES non-compliance along with forensic investigation costs. The cost of migrations is 5 to 15% of the estimated impact of one attack. It is evident that this might be the best time to act.

The switch from DES to AES is not merely an upgrade of encryption algorithms. It sends a strong message of dedication to modern security framework and regulations. The well-known weaknesses, ease of attack by amateur hackers, presence of improved alternatives and distinct regulatory requirements all indicate that AES migration is not an option but a necessity. By continuing to use a DES, organizations run the dangerous risk of data breaches, fines from the government, reputational damage, and loss of competitive advantage as a result of fumbling with weak ciphers that are visible to stakeholders and customers.

## VI. CONCLUSION

This study unequivocally demonstrates that DES is a poor option for data protection in modern computing environments. The algorithm is susceptible to multiple attack techniques and has a 56-bit key length. There are better options available that perform better. Organizations still utilizing outdated DES systems urgently need to improve their security due to regulatory limitations and documented instances of real-world exploitation.

According to our analysis, it is now simple to crack DES encryption using specialized hardware or cloud services. In 1998, it cost about $250,000, but now it only costs a few dollars. Competent attackers have additional options to exploit these flaws through cryptanalytic attacks like differential and linear cryptanalysis. Target in 2013, ATM networks in 2017, and vulnerability warnings in the banking industry from 2015 to 2017 are examples of real-world security breaches in financial infrastructure that demonstrate that DES vulnerabilities are more than just theoretical issues. Now, even amateur attackers can access these weaknesses.

Comparative analysis shows that AES offers much better security in all measured areas (Table I: 2^72 times larger keyspace, proven resistance to known cryptanalytic attacks). The performance is better (1.2 times repeatable faster than DES). As you can see, 3DES is a critical transitional component in database encryption scenarios. The regulatory environment definitely calls for the deprecation of DES, and the growing pains that

will come with it will likely carry big price tags (PCI DDS: $5,000-$100,000+: monthly, post-breach fines: 1-4% of annual revenue). Organizations that elect to delay migrating are facing growing enforcement risks. The regulatory risk arises from the risk of non-compliance with DES market requirements, and increased risk of breach from more attackers.

Organizations must begin the DES-to-AES transition process now. This change must take place in a phased and structured manner as above. The paper above describes a migration process in five phases over a period of 12 months. A thorough migration strategy that covers technical, regulatory, and operational issues will minimize disruptions while providing considerable security benefits. The average costs of breach risk ($4.24m), regulatory fines ($5K to $100K per month), investigation costs and reputational damage from the continued use of DES are significantly higher than the costs of systematic cryptographic upgrades ($200,000-$500,000 for typical organizations). Organizations that complete the changeover from DES to AES show a commitment to data protection standards. It can create customer trust, help prove regulatory compliance and create competitive advantages in security-minded sales channels. Subsequent research should further scrutinize the migration challenges and processes in specific sectors such as healthcare, finance, retail and government. It ought to also create generic migration tools and frameworks that are open source to reduce complexities and costs of implementation for SMBs. Research should also include migration planning on quantum-safe cryptography as the capability of quantum computing approaches the threshold capable of powerful quantum computers.

In addition, it must establish best practices for cryptographic agility for seamless transition to new standards when new discoveries about the threat or cryptanalysis emerge. Studies should be conducted on strategies for modernizing legacy systems in organizations using embedded DES systems that cannot be upgraded by conventional software upgrades. Schedule for hardware replacement and protective measures.

## REFERENCES


[1] National Institute of Standards and Technology (NIST), “Data Encryption Standard (DES),” Federal Information Processing Standards Publication 46, 1977.

[2] Electronic Frontier Foundation (EFF), “Cracking DES: Secrets of Encryption Research, Wiretap Politics & Chip Design,” O’Reilly & Associates, 1998.

[3] E. Biham and A. Shamir, “Differential cryptanalysis of DES-like cryptosystems,” Journal of Cryptology, vol. 4, no. 1, pp. 3–72, 1991.

[4] M. Matsui, “Linear cryptanalysis method for DES cipher,” in Advances in Cryptology – EUROCRYPT ’93, Lecture Notes in Computer Science, vol. 765, pp. 386–397, 1993.

[5] National Institute of Standards and Technology (NIST), “Advanced Encryption Standard (AES),” Federal Information Processing Standards Publication 197, 2001.

[6] W. Diffie and M. Hellman, “Exhaustive cryptanalysis of the NBS Data Encryption Standard,” Computer, vol. 10, no. 6, pp. 74–84, 1977.

[7] S. Bauer, P. Bernstein, and A. Blakeley, “Migrating legacy databases: Challenges, solutions, and best practices,” in Proceedings of the International Conference on Data Engineering, 2019, pp. 1–15.

[8] ISO/IEC, “Information technology - Security techniques - Encryption and key management,” ISO/IEC 27033-1:2015, International Organization for Standardization, 2015.

[9] Cloud Infrastructure Security Benchmark Study, “GPU-Accelerated Cryptanalysis: Performance Metrics for DES Key Recovery,” Journal of Applied Cryptography, vol. 14, no. 3, pp. 234–251, 2023.

[10] Distributed Key Recovery Project, “Modern DES Cryptanalysis Using Cloud Infrastructure,” Technical Report, Global Cryptography Institute, 2023.

[11] Payment Card Industry (PCI) Security Standards Council, “PCI Data Security Standard Version 3.2.1,” Requirement 3.4: Encryption Standards, 2018.

[12] U.S. Department of Health and Human Services, “HIPAA Security Rule: Encryption and Decryption,” 45 CFR 164.312(a)(2)(ii),2013.