Security Analysis of the S-DES Cryptographic System

Dragana Božilović Đokić[1], Vladimir Đokić[2], Lazar Stošić[3], Željko Stanković[4], Olja Krčadinac[5]

[1]*University Union Nikola Tesla, draganadjokic@unionnikolatesla.edu.rs, ORCID ID: 0000-0002-9206-2764*
[2]*University Union Nikola Tesla, vladimirdjokic@unionnikolatesla.edu.rs, ORCID ID: 0009-0004-9678-6999*
[3]*Univerzitet Union Nikola Tesla, lstosic@unt.edu.rs, ORCID ID: 0000-0003-0039-7370*
[4]*University Union Nikola Tesla, stanz@medianis.net, ORCID ID: 0000-0002-9893-9088*
[5]*Universoty Union Nikola Tesla, okrcadinac@unionnikolatesla.edu.rs, ORCID ID: 0000-0002-6299-371X*

Review article

https://doi.org/10.7251/JIT2601057DJ UDC: 351.817:336.746

Abstract: S-DES (Simplified Data Encryption Standard) is a pedagogically oriented, reduced-complexity variant of the full DES algorithm. It operates on 8-bit plaintext blocks with a 10-bit secret key, providing a tractable environment for studying fundamental cryptanalytic methods — linear cryptanalysis, differential cryptanalysis, and combined linear-differential cryptanalysis. This paper analyzes the architectural design, subkey generation mechanism, permutation logic, and security properties of S-DES. The cipher's vulnerability to brute-force exhaustive search and differential cryptanalytic attacks is examined in detail, and its potential use as an image encryption primitive — enhanced through chaotic key generation — is evaluated experimentally. The study concludes that, while S-DES is cryptographically inadequate for practical deployment, it constitutes a highly effective educational tool for illustrating the core principles of symmetric block cipher design.

Keywords: S-DES, DES, cryptography, differential cryptanalysis, symmetric encryption, image encryption

Introduction

Cryptography is a scientific discipline concerned with methods for securing information against unauthorized access. The word derives from the ancient Greek kryptos (hidden, secret) and graphos (writing). A cryptographic algorithm transforms human-readable plaintext into an unintelligible ciphertext; cryptanalysis is the complementary science of recovering plaintext or secret keys from ciphertext without prior knowledge of the decryption secret. In any well-formed cryptosystem, the decryption function must be the exact mathematical inverse of the encryption function, though the converse need not hold [1].

S-DES is a scaled-down variant of the Data Encryption Standard (DES). It retains the essential structural properties of DES while operating on considerably smaller parameters: 8-bit plaintext blocks encrypted with a 10-bit key. This reduced scale makes S-DES a practical teaching cipher for introducing students to contemporary cryptanalytic techniques such as linear cryptanalysis, differential cryptanalysis, and combined linear-differential cryptanalysis [2].

This paper presents an analysis of S-DES, treating it as a representative simplified block cipher that makes core cryptographic concepts tractable for study. The investigation covers three areas: (i) the internal architecture of S-DES, including its data flow, subkey generation, and permutation logic; (ii) the security posture of S-DES with respect to its structural simplicity and inherent key-space limitations; and (iii) the applicability of exhaustive-search and differential cryptanalytic attacks against the cipher. Additionally, the paper evaluates S-DES as an image encryption primitive when combined with chaotic key generation.

S-DES has been widely used in academic laboratory settings for cryptography and information theory courses, where it serves as a vehicle for visualizing key scheduling, substitution functions, and permutation operations. The central research question is how S-DES processes an 8-bit data block with a 10-bit key in the context of standard DES design principles, and

how its security constraints compare with those of more robust symmetric ciphers.

Three research hypotheses were formulated on the basis of the reviewed literature:

(H1): S-DES achieves faster encryption and decryption than full DES for both single and multiple data blocks, owing to its reduced input and key sizes.

(H2): Using S-DES in educational contexts provides a clearer understanding of cryptographic operations — such as permutations and key selection — with lower conceptual complexity than traditional DES.

(H3): Under experimental conditions, S-DES is capable of encrypting a color image when augmented with a chaotic key generation strategy.

The motivation for this research is to demonstrate, through a concrete practical example, the cryptographic properties and educational value of the S-DES algorithm.

CRYPTANALYSIS OF S-DES

In S-DES, the same master key is used for both encryption and decryption; however, the subkeys are applied in reverse order during decryption, making the decryption procedure the structural mirror image of encryption. Each plaintext block is subjected to an initial permutation (IP), followed by two rounds of key-dependent computation, and concluded by the application of the inverse initial permutation (IP^{-1}).

Keys

S-DES uses a 10-bit master key to generate two distinct 8-bit subkeys, K1 and K2, each applied in a dedicated cipher round. The key schedule is denoted KS [3].

Key generation begins by applying Permuted Choice 1 (PC1) to the master key, yielding two 5-bit halves: C0 and D0. Key bits are indexed 0 through 9. The PC1 bit-selection pattern is given in Table 1.

Table 1. *PC1 Permutation [3]*

9	**7**	**3**	**8**	**0**
2	6	5	1	4

The upper row of Table 1 defines the bit positions constituting C0; the lower row defines D0. Each half is then independently cycled one position to the left, producing C1 and D1. Subkey K1 is formed by concatenating C1 and D1 and applying Permuted Choice 2 (PC2), which selects 8 of the 10 available bits, as shown in Table 2.

Table 2. *PC2 Permutation [3]*

3	**1**	**7**	**5**	**0**	**6**	**4**	**2**

To obtain K2, the halves C1 and D1 are each shifted two further positions to the left, yielding C2 and D2. These are concatenated and subjected to the same PC2 mapping, producing the second 8-bit subkey K2. Figure 1 shows the complete key schedule.

[Figure 1. Subkey generation schedule for K1 and K2 [3].]

Encryption

The encryption function is expressed as follows:

$C = E(P, K) = IP^{-1}(f_2(f_1(IP(P), K1), K2))$ (1) [3]

The 8-bit plaintext block P is first subjected to IP. The resulting byte is split into two 4-bit halves, L0 and R0, according to Table 3.

Table 3. *Initial Permutation IP [4].*

7	**6**	**4**	**0**
2	5	1	3

L0 contains the bits at positions 7, 6, 4, and 0 of the input; R0 contains bits at positions 2, 5, 1, and 3. Round 1 applies the Feistel transformation [4]:

$L1 = R0, R1 = L0 \oplus f(R0, K1)$ (2)

Round 2 uses the outputs of Round 1 [4]:

$L2 = R1, R2 = L1 \oplus f(R1, K2)$ (3)

After Round 2, R2 and L2 are concatenated in that order to form R2L2, which is then passed through IP^{-1} to produce the final ciphertext. Figure 2 illustrates the complete encryption dataflow.

[Figure 2. Encryption dataflow diagram [4].]

Round Function f

The round function f takes a 4-bit half-block and an 8-bit subkey as inputs. The first operation is the expansion function E, which maps 4 bits to 8 bits according to the bit-selection pattern in Table 4 [5].

Table 4. *E-Bit Expansion [5]*

3	**0**	**1**	**2**	**1**	**2**	**3**	**0**

The 8-bit result E(R) is XORed with the current

round subkey. The resulting byte is partitioned into two 4-bit groups: B1 (the four most significant bits) and B2 (the four least significant bits). B1 and B2 are passed to substitution boxes S0 and S1, respectively. Each S-box accepts a 4-bit input and produces a 2-bit output [5].

Table 5. *S0 Substitution Box [5]*

	Col 0	Col 1	Col 2	Col 3
Row 0	1	0	2	3
Row 1	3	1	0	2
Row 2	2	0	3	1
Row 3	1	3	2	0

Table 6. *S1 Substitution Box [5]*

	Col 0	Col 1	Col 2	Col 3
Row 0	0	3	1	2
Row 1	3	2	0	1
Row 2	1	0	3	2
Row 3	2	1	3	0

To illustrate S-box addressing, consider S0 with input 1101. The first and last bits form the binary value 11 (decimal 3), which selects row 3. The two middle bits form the value 10 (decimal 2), which selects column 2. Reading S0 at row 3, column 2 yields 2, encoded in binary as 10. The 2-bit outputs from S0 and S1 are concatenated into a 4-bit string and passed through the permutation P (Table 7), producing the round function output [5].

Table 7. *Permutation P [5]*

1	**0**	**3**	**2**

Decryption follows the identical procedure, with the sole modification that K2 is applied in Round 1 and K1 in Round 2 — i.e., the subkey order is reversed.

Brute-Force Attack

Brute-force cryptanalysis systematically enumerates all possible keys and tests each against a known plaintext-ciphertext pair. The practical feasibility of this approach depends entirely on the size of the key space. A key space of up to 2^{56} candidates (approximately 7.2×10^{16} possible keys) is considered tractable given sufficient computational resources [6]. Systems employing longer keys — such as AES with its 128-bit key — are effectively immune to exhaustive search on general-purpose hardware [7].

With a 10-bit key, S-DES has a search space of only $2^{10} = 1024$ candidates. A single known plaintext-ciphertext pair is therefore sufficient to recover the master key through exhaustive search in negligible time, making a brute-force attack entirely practical against S-DES [8].

Differential Cryptanalysis

Differential cryptanalysis is a chosen-plaintext attack originally developed to target DES-like block ciphers [9]. The adversary selects pairs of plaintexts with a known input difference and studies how that difference propagates through the cipher structure to produce an output difference. Statistical biases in the resulting difference distributions are exploited to recover partial subkey information. The technique has been extensively studied against DES and has had a lasting influence on the design of modern ciphers, which are typically engineered to provide explicit resistance to differential attacks [10].

To understand why this is non-trivial, consider a purely linear cipher $C = P \oplus K$. In this case, the XOR difference of any ciphertext pair is identical to the XOR difference of the corresponding plaintext pair, revealing nothing about the key. S-DES is not a linear cipher: its S-box components introduce nonlinearity, causing ciphertext differences to depend on the secret key. This dependence creates exploitable statistical structure that can be used to recover key bits [11].

S-Box Difference Distribution

For substitution boxes S0 and S1, let X denote the S-box input and Y the output. A difference pair is expressed as $(\Delta X, \Delta Y)$, where $\Delta X = X' \oplus X''$. For a fixed ΔX, the corresponding second input is $X'' = X' \oplus \Delta X$, and the resulting ΔY is tabulated in the difference distribution table.

As an example, for S0 with $\Delta X = 8$ and $\Delta Y = 1$, the distribution table shows that exactly two input pairs satisfy this differential. Since $\Delta Y = 1$, the output values are {1, 3}, and the only input pair that simultaneously yields these outputs while satisfying $\Delta X = 8$ is {9, 1}.

This information enables partial key recovery. Assume $X' = 2$ and $X'' = 8$ for S0 ($\Delta X = 10$). If the corresponding outputs are $Y' = 0$ and $Y'' = 2$ ($\Delta Y = 2$), the actual S-box inputs after XOR with the subkey are $I' = X' \oplus K$ and $I'' = X'' \oplus K$. Since the subkey is added identically to both inputs, it cancels in the difference:

$\Delta I = \Delta X = 10$.

From the distribution table, the input pairs satisfying $\Delta X = 10$ and $\Delta Y = 2$ are {7, 13}. The subkey candidates K are recovered as [11]:

$K = I' \oplus X' = 7 \oplus 2 = 5$ (4)

$K = I'' \oplus X' = 13 \oplus 2 = 15$ (5)

The results are summarized in Table 8.

Table 8. *S-Box Key Candidates for X' = 2, X'' = 8 [11]*

X'	X''	Possible I pair	Key candidates K
2	8	{7, 13}	{5, 15}

METHOD

Several complementary scientific methods were applied to analyze the characteristics and security aspects of the S-DES cryptosystem.

A comparative method was used to contrast the individual processing stages of S-DES against the general principles governing symmetric encryption systems. This approach enabled the identification of structural parallels and substantive differences between the simplified cipher and its theoretical cryptographic foundations, and facilitated an assessment of S-DES security properties in relation to DES.

A case study approach formed the empirical core of the research. The complete encryption and decryption pipeline was traced step by step — covering subkey derivation, initial and inverse permutations, S-box substitutions, and round-level Feistel transformations — allowing a detailed observation of how subkeys K1 and K2 govern the transformation of plaintext to ciphertext.

Descriptive analysis was used to present and interpret the results systematically. The study relied on secondary data sources, primarily peer-reviewed journal articles, academic textbooks, and conference proceedings in the fields of cryptography and information security.

The research proceeded through four sequential phases: (1) collection and critical review of relevant literature; (2) examination of the theoretical foundations of the S-DES algorithm; (3) comparative analysis of algorithmic components; and (4) interpretation of results in the context of symmetric cipher design principles.

FINDINGS

A 10-bit master key is used to generate two distinct 8-bit subkeys, K1 and K2, each applied in a specific cipher round. Key scheduling begins with PC1, which selects and reorders 10 key bits into two 5-bit halves, C0 and D0 (Table 9).

Table 9. *PC1 Mapping [11]*

9	7	3	8	0
2	6	5	1	4

A cyclic left shift is applied independently to C0 and D0, producing C1 and D1. Subkey K1 is formed by concatenating C1 and D1 and applying PC2 (Table 10), which reduces the 10 bits to 8 bits for use as the round subkey.

Table 10. *PC2 Mapping [11]*

3	1	7	5	0	6	4	2

The 4-bit half-block R is expanded to 8 bits by the expansion function E, whose bit-selection pattern is given in Table 11.

Table 11. *E-Bit Selection [11]*

3	0	1	2	1	2	3	0

The expanded block is XORed with the active subkey. The resulting 8-bit value is split into B1 and B2, which are fed to S0 and S1 respectively (Table 12).

Table 12. *S1 Lookup Table [11]*

	Col 0	Col 1	Col 2	Col 3
Row 0	0	3	1	2
Row 1	3	2	0	1
Row 2	1	0	3	2
Row 3	2	1	3	0

In S-box addressing, the first and last bits of the 4-bit input select the row, and the two middle bits select the column. For S0 with input 1101: the outer bits select row 3, and the inner bits select column 2, yielding the value 2 (binary: 10). The 4-bit concatenated output of S0 and S1 is then permuted by P (Table 13).

Table 13. *Permutation P [11]*

1	0	3	2

For the image encryption experiment, the first iterate of a logistic chaotic map applied to the Lena benchmark image is used to derive an S-DES encryption key. The chaotic transformation produces a pseudo-random binary matrix, which is binarized and used to drive pixel-block encryption. This approach leverages the high sensitivity and apparent randomness of chaotic orbits to overcome S-DES's inherently limited key space. The original Lena image and its first-iteration chaotic counterpart are shown in Figures 3 and 4, together with their respective RGB histograms.

[Figure 3. (a) Original Lena image; (b) First-iteration chaotic image [9].]

[Figure 4. (a) RGB histogram of original image; (b) RGB histogram of encrypted image [9].]

The binarized chaotic image serves as the S-DES key. Because the limited key space of S-DES creates significant security risks under repeated use, the high entropy of chaotic key material substantially improves the statistical unpredictability of the encrypted output compared with static key selection.

Discussion

The analysis reveals a fundamental tension between the pedagogical utility and the cryptographic adequacy of S-DES.

The principal advantages of S-DES are: (1) its considerably simpler structure relative to full DES, making it far more accessible for study and implementation; (2) its operation on smaller plaintext blocks with a shorter key, demanding fewer computational resources; and (3) its substantially faster execution compared with DES on equivalent hardware.

Its limitations are equally clear: (1) the 10-bit key is critically insufficient for any real-world security application; (2) the resulting limited key space leaves S-DES vulnerable to trivial exhaustive-search attacks; and (3) when applied to large data payloads, such as high-resolution images, S-DES cannot satisfy practical encryption security requirements.

The integration of chaotic mapping as a dynamic key-generation mechanism substantially compensates for the limited key space of S-DES. Chaotic sequences yield high-entropy key material that improves the statistical unpredictability of ciphertext, demonstrating that appropriate key management strategies can partially offset the weaknesses of a simplified cipher in controlled educational contexts.

Conclusion

Cryptanalysis is a scientific discipline dedicated to deciphering the content of encrypted information without access to the secret decryption key. This paper has shown that even elementary attacks — such as differential cryptanalysis — are highly effective against ciphers with reduced structural complexity.

The differential cryptanalysis case study demonstrated that the full 8-bit second-round subkey of S-DES can be fully recovered through differential cryptanalysis. Given these bits, the remaining 2 unknown bits of the 10-bit master key can be determined by testing only four additional candidates, making complete key recovery computationally trivial.

Despite its cryptographic weakness by modern standards, S-DES holds significant historical and pedagogical importance. Its compact, transparent structure effectively illustrates the core principles of symmetric block cipher design — permutations, substitutions, key scheduling, and Feistel rounds — and the study of its cryptanalytic weaknesses builds intuition for the structural vulnerabilities that motivated the development of stronger standards such as AES.

The image encryption scheme proposed in this paper combines S-DES with a logistic chaotic map. The chaotic key generation strategy compensates for the cipher's limited key space and yields encrypted output with strong statistical randomness properties. These results support hypothesis H3 and suggest that, when augmented with appropriate key generation, S-DES remains a valuable instructional tool for exploring more advanced encryption paradigms.

References

[1] H. Kim et al., "Deep-Learning-Based Cryptanalysis of Lightweight Block Ciphers Revisited," Entropy, vol. 25, no. 7, p. 986, 2023.

[2] Z. Hou, J. Ren, and S. Chen, "Improved Machine Learning-Aided Linear Cryptanalysis: Application to DES," Cybersecurity, Springer, 2025.

[3] K. Dworak and U. Boryczka, "Breaking Data Encryption Standard with a Reduced Number of Rounds Using Metaheuristics Differential Cryptanalysis," Entropy, vol. 23, no. 12, p. 1697, 2021.

[4] S. Sikdar, S. Dutta, and M. Kule, "On Cryptanalysis of 3-DES using Nature-Inspired Algorithms," International Journal of Computer Network and Information Security, pp. 54-71, 2025.

[5] D. Shah et al., "A Novel Approach for Security Enhancement of Data Encryption Standard," Computers, Materials & Continua, vol. 75, no. 3, pp. 5073-5086, 2023.

[6] M. Zheng and H. Kang, "Lattice-Based Cryptanalysis of

RSA-Type Cryptosystems: A Bibliometric Analysis," Cybersecurity, Springer, 2024.
[7] D. Gerault et al., "SoK: 6 Years of Neural Differential Cryptanalysis," Cryptology ePrint Archive, 2024.
[8] A. Jain, V. Kohli, and G. Mishra, "Deep Learning Based Differential Distinguisher for Lightweight Block Ciphers," 2021.
[9] L. Zhang and Z. Wang, "Improving Differential-Neural Distinguisher Model for DES, Chaskey and PRESENT," 2022.
[10] R. Kumari, J. G. Pandey, and A. Karmakar, "An RTL Implementation of the Data Encryption Standard (DES)," 2023.
[11] A. Ullah, M. Khan, and S. Ali, "Lightweight Block Ciphers for Resource-Constrained Environments: A Comprehensive Survey," Future Generation Computer Systems, 2024.

Received: April 21, 2026
Accepted: May 2, 2026

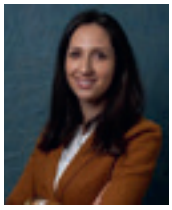
ABOUT THE AUTHORS

Dragana Đokić is a teaching assistant "Union-Nikola Tesla" University, Faculty of Informatics and Computer Science, Belgrade, Republic of Serbia. Finished Master of Science in Mehanical Engineering (M.Sc. MEI.) University of Belgrade. Her current research interests include the fields of computer networks, security, high-perfor-mance systems (HPC), Internet of Things (IoT), software development and testing.

Vladimir Đokić is professor at "Union – Nikola Tesla" University - Faculty of Informatics and Computer Science, Belgrade. He holds a PhD in Information Systems and is actively engaged in teaching and research in the field of information and communication technologies. He is the author and co-author of numerous scientific papers published in international peer-reviewed journals indexed in major scientific databases. His research work is interdisciplinary, combining information systems and computer science with applications in biomedicine, pharmacology, and engineering sciences.

Lazar Stošić is a university professor at the Faculty of Informatics and Computer Science, University Union—Nikola Tesla, Belgrade, Serbia and the President of the Association for the Development of Science, Engineering and Education, in Serbia. He is also a leading researcher at the Center for Scientific Competence of DSTU, Department of Scientific and Technical Information and Scientific Publications Don State Technical University, Russia. His expertise includes computer science, IKT, editorial workflow management, conference organization, web technologies, web design, indexing, XML production, SEO, digital marketing, and new media technologies.

Zeljko Stankovic received his higher education in Cleveland, Ohio, USA, where he graduated in 1981. The topic of the thesis was "Reversible sound in halls". He defended his master's thesis ("Learning control system (LMS) based on ADL SCORM specifications") in 2006 at the University of Novi Sad, Faculty of Science, Department of Informatics. He defended his doctoral dissertation (Laser perception of defined objects and encapsulation of control and logic elements for an autonomous robotic teaching tool) at Singidunum University, Belgrade, in 2010. He has been programming since 1984, creating programs for his first Commodore 64 computer.



Olja Krcadinac (Latinovic, maiden name) is assistant professor at "Union – Nikola Tesla" University - Faculty of Informatics and Computer Science. She earned her Ph.D. in biometric field from University of Belgrade – Faculty of Organizational science, where she conducted groundbreaking research on speaker recognition. In addition to her teaching responsibilities, Olja has authored numerous impactful publications in peer-reviewed journals, contributing valuable insights to the scientific community. Her research focuses on biometric, sensors, IoT and AI, addressing critical issues in AI and making significant contributions to the academic community.

FOR CITATION

Dragana Božilović Đokić, Vladimir Đokić, Lazar Stošić, Željko Stanković, Olja Krčadinac, Security Analysis of the S-DES Cryptographic System, *JITA – Journal of Information Technology and Applications, Banja Luka*, Pan-Europien University APEIRON, Banja Luka, Republika Srpska, Bosna i Hercegovina, JITA 16(2026)1:57-62, (UDC: 351.817:336.746), (DOI: 10.7251/JIT2601057DJ), Volume 16, Number 1, Banja Luka, June (1-76), ISSN 2232-9625 (print), ISSN 2233-0194 (online), UDC 004