ISSN 3083-7502

UDC 004.056.55:004.421.2

Sahun Andrii
PhD, Associated Professor of the Department of Computer Systems, Networks and Cybersecurity, National University of Life and Environmental Sciences of Ukraine
ORCID: https://orcid.org/0000-0002-5151-9203
E-mail: a.sagun@nubip.edu.ua

Panasko Olena
PhD, Associated Professor of the Department of Telecommunication and Robotics Systems and Cybersecurity,
Cherkasy State Technological University
ORCID: https://orcid.org/0000-0002-0510-7742
E-mail: lena.pa@ukr.net

TRENDS IN INCREASING THE CRYPTO-STRENGTH OF SYMMETRIC BLOCK CIVERS IN THE CONTEXT OF THE MODERN CRYPTOSYSTEMS DEVELOPMENT

Abstract. *The article examines the combination of analytical and applied approaches to improving symmetric block ciphers in light of current trends in the development of cryptographic systems. The study analyzes the current SOG-IS standards and recommendations that define the basic directions of symmetric algorithm evolution, such as the transition from outdated Feistel-based schemes to optimized structures (AES, lightweight block ciphers for IoT). Using a modified version of the Simple-DES (S-DES) cipher, the paper proposes a method for enhancing cryptographic strength without changing the key or block length. The main improvements involve an enhanced design of S-boxes and their dynamic selection based on a key graph. The results of the comparative analysis demonstrate a significant increase in resistance to brute-force and differential cryptanalysis compared to the standard S-DES, while maintaining low computational complexity. The conducted research confirms the relevance of using educational and experimental models such as S-DES to explore modern methods for improving the security of symmetric ciphers, which is of practical importance for prototyping and lightweight implementations in Internet of Things systems.*
Keywords: *Symmetric Encryption, Block Ciphers, Feistel Network, S-DES, S-Boxes, Cryptographic Strength, AES, Lightweight Ciphers, IoT, SOG-IS.*

Introduction. Symmetric block cryptosystems are a fundamental component of modern information protection methods that ensure data confidentiality and integrity in both networked and autonomous environments. The rapid development of asymmetric algorithms has had little effect on the evolution of symmetric ciphers, since symmetric encryption remains crucial due to its combination of high performance, implementation simplicity, and low computational cost.

Recently, there has been a growing interest in lightweight block ciphers designed for Internet of Things (IoT) and mobile systems, as well as in improving the components of block algorithms—namely, S-boxes, key generation mechanisms, and round functions. However, the study of trends in the evolution of well-known and thoroughly analyzed symmetric cryptosystems, particularly those based on classical Feistel networks, remains relevant. For this reason, in many studies, the S-DES cipher is considered primarily as an educational symmetric block cryptosystem with research potential.

Literature Review. The principles of constructing symmetric block ciphers, particularly Feistel networks, are presented in the classical works of W. Stallings [1] and B. Schneier [2-4]. A generalization of approaches to the development of modern cryptographic algorithms is provided in the works of AES standard developers – J. Daemen and V. Rijmen [5].

The current trends in the evolution of block ciphers, described in [6-13], indicate a gradual transition from complex and cumbersome algorithms to energy-efficient and secure implementations, such as those used in the PRESENT, GIFT, and SPECK ciphers, among others.

As shown in several studies [2, 8-10], the modernization of a basic Feistel-based cipher solely through an increased number of rounds leads to a noticeable improvement in cryptographic strength. At the same time, enhancing resistance by increasing key length results in significant complications

ISSN 3083-7502

in cryptographic transformations and increases the computational load. Therefore, in practice, the only feasible way to improve the cryptographic strength when modifying the S-DES cipher is by refining the design of its S-boxes. Some possible improvements are described in [14, 15]. Although for 4-bit S-boxes used in the S-DES cipher there are no ideal variants with perfect cryptographic properties, it is possible to select tables with similar properties among 4→4 or 6→4 mappings, or even use S-boxes from the DES cipher.

Ukrainian studies [10, 11] and national standards [16, 17] emphasize the importance of adapting international cryptographic solutions to national security requirements and educational applications.

Among many works devoted to an in-depth analysis of modern trends in symmetric cryptosystem development, sources [7-10] deserves particular attention. It explores the prospects for improving S-boxes, key-schedule methods, and integrating post-quantum principles into classical symmetric encryption structures.

A review of block cipher development reveals the dominance of AES (Advanced Encryption Standard). Numerous sources note that AES is currently the most widely used block cipher, particularly in the context of NIST certification [18]. In most cases, practical data protection mechanisms are implemented using AES-based systems, which firmly establishes it as the "standard block cipher." However, there is also a growing interest in lightweight block ciphers.

Recent research (2025) covering 58 lightweight block ciphers – spanning the period between 2018 and 2025 — highlights this trend [6, 7, 11, 12]. The emergence of lightweight block ciphers suitable for microcontroller implementations is directly linked to the rapid growth of the IoT market (52 such ciphers introduced in the current year) [7, 11].

Thus, while major computer systems primarily rely on AES-based cryptosystems, the increasing demand for specialized encryption solutions in resource- or energy-constrained environments drives the development of new lightweight block ciphers. Numerous studies note that algorithms such as DES or 3-DES are recommended exclusively as "legacy" solutions rather than viable options for new computer systems.

The recommendations of the European organization SOG-IS (Senior Officers Group – Information Systems Security Mutual Recognition Agreement, Crypto Working Group) describe current and legacy symmetric algorithms for data protection and specify their permitted usage periods. For instance, the 3-DES algorithm with two effective keys (effective key length ≈112 bits) is officially considered obsolete and permitted for practical use only until 2024, after which its use is discouraged due to insufficient cryptographic strength. The 3-DES algorithm with three independent keys (effective key length ≈168 bits) is permitted only until 2027.

According to the SOG-IS Crypto Working Group documents (2023, v1.3), AES is recognized as the only symmetric cipher recommended for new applications in Europe. The 3-DES cipher may be allowed only for compatibility with existing systems but should be gradually phased out of use [19].

Objectively, there is a lack of comprehensive statistical data on the practical use of most existing symmetric block ciphers; however, some sources provide sufficient information to assess the overall trends in this field [1, 9, 10].

Purpose. The main point of research is to develop and substantiate an integrated approach to enhancing the cryptographic strength of symmetric block ciphers, which combines the modification of internal structural components of the cipher, the use of multilevel encryption schemes, and the application of modern methods for assessing resistance to differential and linear cryptanalysis, taking into account current trends and the potential for the development of cryptographic systems.

Results and Discussion. In the context of modern trends, the focus is not merely on the choice of the encryption algorithm itself but on its implementation and the optimization of security.

The dynamics of the development trends of symmetric block ciphers from 2001 to 2025, shown in Figure 1, demonstrate a steady increase in the number of various AES system implementations and an intensive growth in the number of new "lightweight" block ciphers within the IoT segment.

ISSN 3083-7502

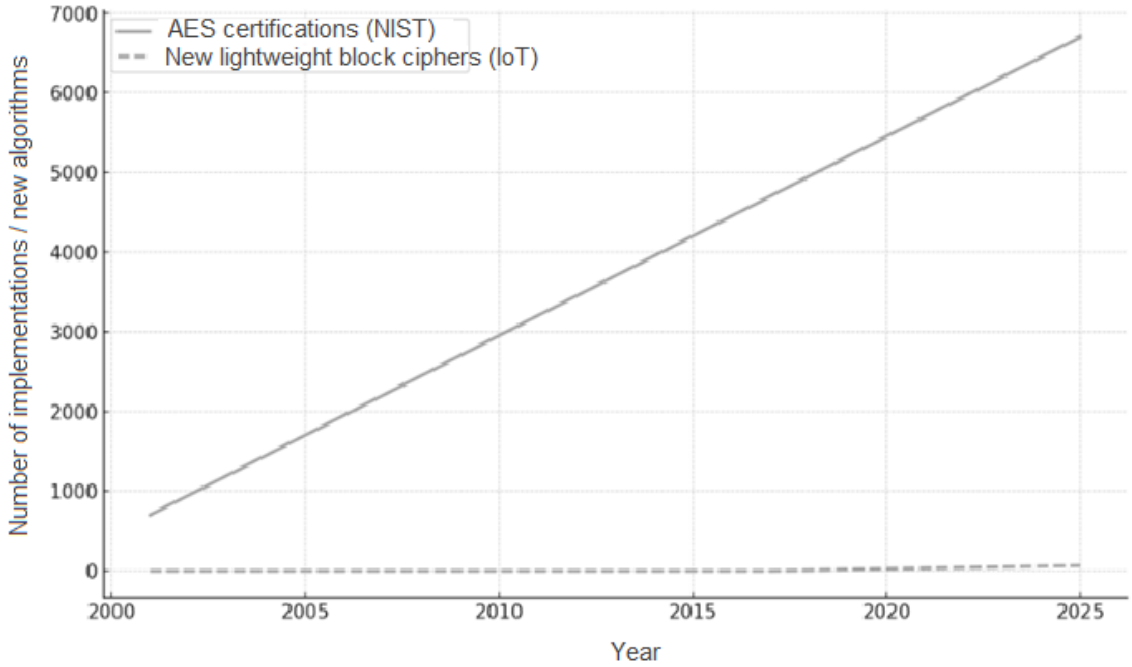

Figure 1 – Dynamics of the symmetric block ciphers developmene from 2001 to 2025

Existing statistics and assessments of the use of symmetric block ciphers for the period from 2018 to 2025 show that NIST certifications of symmetric block cipher variants indicate a continuous increase in various implementations of the AES cipher (over the reviewed period, the number of implementations has grown more than 7,000 times compared to 2001) [7, 8, 10]. In the IoT segment, according to research data for 2025, 58 new "lightweight" block ciphers have emerged during the period from 2018 to 2025.

To enhance the encryption quality of the Feistel-based block cipher Simple-DES (S-DES), a specific set of S-boxes was generated (a pool derived from the PRESENT cipher S-box), and a modified version of S-DES was implemented. The modified cipher uses 12 rounds (R = 12), incorporating an improved key-schedule transformation and dynamic S-box selection. It was compared to the original S-DES (2 rounds) using two metrics:

- average avalanche effect — the mean number of ciphertext bits that change when a single plaintext bit is inverted (averaged over 500 cases). In the original S-DES, this value was approximately 3.94 bits, while in the modified S-DES (R = 12) it increased to about 3.99 bits;
- maximum differential probability (DDT probability) — the worst-case value from the differential distribution table of the S-boxes. For the original S-DES (S_0/S_1 mapped as a 4→2 equivalent), this probability was approximately 0.75, whereas for the modified PRESENT-based S-DES it decreased to about 0.44;
- both variants were compared according to the criterion of resistance to differential cryptanalysis (Fig. 2).

As shown in Figure 2, the implemented modification significantly reduced the maximum differential probability of the S-boxes, which directly complicates differential cryptanalysis. Moreover, the avalanche effect in the original cipher was already very close to the ideal (~4 bits out of 8), and the modification slightly improved this parameter.

Despite the unchanged key space (10 bits), the proposed enhancement has effectively increased the cipher's resistance to analytical attacks, particularly differential and linear cryptanalysis. During testing of the developed S-DES cipher modification, it was also found, that even a very significant modification is unable to somehow increase the theoretical cryptographic strength of this cipher. This can be attributed to the fact that both of its variants (S-DES with two rounds of iterations and with 12 rounds of crypto transformation iterations) use a similar length of the common key – 10 bits. That's

ISSN 3083-7502

why the estimate of the complexity of the full enumeration for both variants of the cipher is the same and is the number of: $log_{10}(2^{10}) = 10 * log_{10}(2) \approx 3{,}0103$.

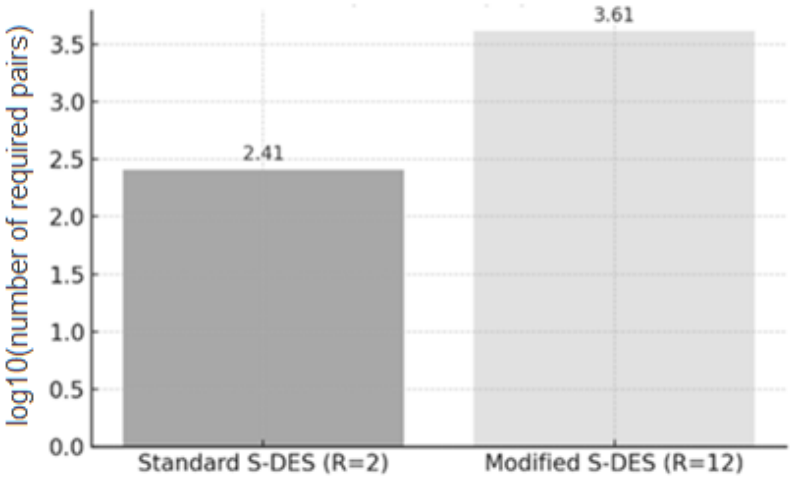

Figure 2 – Indicator of equivalent resistance against differential cryptanalysis (logarithmic scale)

At the same time, the equivalent resistance against differential cryptanalysis for the modified version of the cipher has improved significantly, which can be seen in the graph (Figure 3).

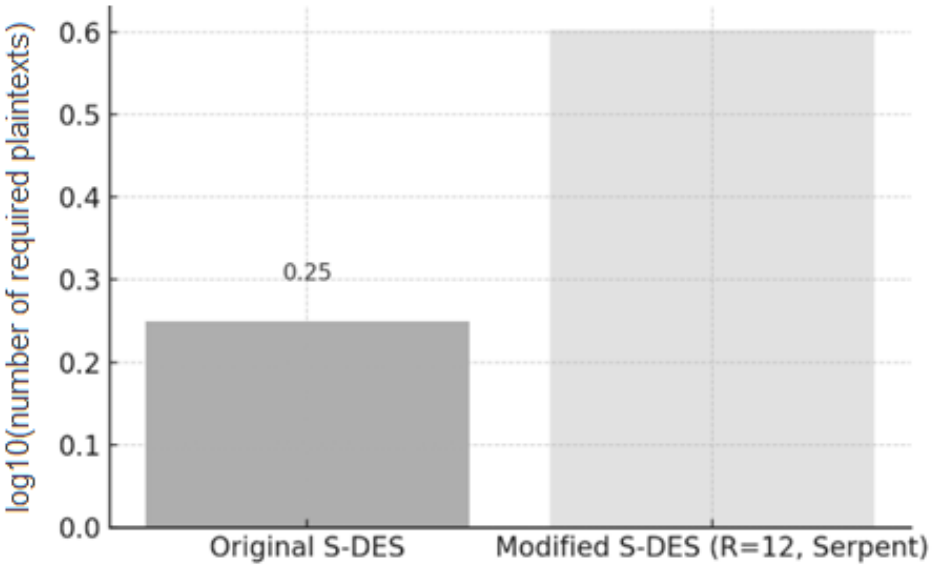

Figure 3 – Comparison of resistance to linear cryptanalysis for the modified and unmodified version of the S-DES cipher (logarithmic scale)

It is known that the standard S-DES cipher with the number of encryption rounds R=2 requires approximately $10^{2,4} \approx 251{,}84$ pairs of plaintext and ciphertext for key computation. While the modified S-DES cipher with the number of rounds R=12, in one of its modifications, the PRESENT-based S-box pool modification, requires already $10^{3,6} \approx 3981$ pairs, i.e., approximately 16 times more.

The obtained data indicate a real increase in the cryptoresistance of the cipher to known types of cryptanalysis, achieved only by optimizing the structure of S-boxes and increasing the number of rounds. Moreover, such changes in the design of the S-DES cipher were not accompanied by a change in the length of the key.

ISSN 3083-7502

Conclusions. Improving the design of S-boxes is the most effective way to improve S-DES stability without increasing the key size or block size. Using a pool of S-boxes based on proven schemes (example, Serpent cipher, PRESENT, etc.) allows to significantly reduce the number of linear and differential dependencies in the output sequences. To complicate the construction of analytical attacks, it is effective to use dynamic selection of S-boxes, which depends on the current round key (key-dependent S-box selection).

It is expected that increasing the number of rounds of the S-DES training cipher from 2 to 12 in the modified version of this cipher performs an avalanche effect and allows to ensure a more uniform distribution (dispersion) of the ciphertext bits. Although legacy algorithms like DES or 3-DES are increasingly used in new systems, their role is still important because it allows for the exploration of the design of S-boxes, which are part of modern encryption algorithms.

As can be seen from the conducted research, improving the quality of the design of S-boxes of symmetric block ciphers, even without increasing the key length, allows in practice to increase their resistance to differential cryptanalysis by approximately 16 times, and to linear cryptanalysis by approximately 2–3 times, which is confirmed by Linear Approximation Table type cryptanalysis.

As a result of the analysis of modern trends in the development of symmetric cryptographic systems, it should be noted that the AES cipher today remains the main practical cipher for use in large information and communication systems.

Prospects for improvment. Given the current trend towards smaller systems with limited resources, as well as the development of Internet of Things or Smart Home technologies, the current trend is to use lightweight block ciphers. Today, the key parameters in choosing a block cipher are not only the algorithm itself, but also its implementation (hardware/software), resistance to side-channel attacks, and adaptability to new threats (such as post-quantum ones). This indicates that one of the directions for improving symmetric block ciphers may involve changes to the key space and enhancements to the design of S- and P-boxes. Increasing the key space of such a “lightweight” IoT cipher can significantly improve its practical cryptographic strength. A similar effect can be achieved by refining the structure of the round functions.

References

1. Stallings, W. (2014). Cryptography and network security: Principles and practice (6th ed.). Pearson Education. URL: https://www.uoitc.edu.iq/images/documents/informatics-institute/Competitive_exam/Cryptography_and_Network_Security.pdf.
2. Schneier, B., Kelsey, J., Whiting, D., Wagner, D., & Hall, C. (1998). On the Twofish key schedule. In Selected Areas in Cryptography (pp. 27–42). Springer. https://doi.org/10.1007/3-540-48892-8_3.
3. Schneier, B. (1998). Cryptographic design vulnerabilities. Computer, 31(9), 29–33. https://doi.org/10.1109/2.708447.
4. Blaze, M., & Schneier, B. (1995). The MacGuffin block cipher algorithm. In B. Preneel (Ed.), Fast Software Encryption: FSE '94 (pp. 97–110). Springer. https://doi.org/10.1007/3-540-60590-8_8.
5. Daemen, J., & Rijmen, V. (2020). The design of Rijndael: The Advanced Encryption Standard (AES) (2nd ed.). Springer. https://doi.org/10.1007/978-3-662-60769-5.
6. Banik, S., Bogdanov, A., Isobe, T., Shibutani, K., Hiwatari, H., Akishita, T., & Mori, K. (2015). Midori: A block cipher for low energy. In Advances in Cryptology – ASIACRYPT 2015 (pp. 411–436). Springer. https://doi.org/10.1007/978-3-662-48800-3_17.
7. Al-Nofaie, S. M., Sharaf, S., & Molla, R. (2025). Design trends and comparative analysis of lightweight block ciphers for IoTs. Applied Sciences, 15(14), 7740. https://doi.org/10.3390/app15147740.
8. Knudsen, L. R. (1994). Block ciphers: Analysis, design and applications (DAIMI Report Series No. 23/485). University of Aarhus. https://doi.org/10.7146/dpb.v23i485.6978.
9. Luzhetskyi, V. A., & Ostapenko, A. V. (2013). Analiz alhorytmiv symetrychnoho blokovoho shyfruvannia [Analysis of symmetric block cipher algorithms]. ITKI, 25(3).

ISSN 3083-7502

10. Kuznetsov, O. O., Oliinykov, R. V., Horbenko, Yu. I., Pushkarov, A. I., Dyrda, O. V., & Horbenko, I. D. (2014). Obgruntuvannia vymoh, pobuduvannia ta analiz perspektyvnykh symetrychnykh kryptoperetvoren na osnovi blochnykh shyfriv [Substantiation of requirements, construction and analysis of перспективних symmetric cryptographic transformations based on block ciphers]. Visnyk Natsionalnoho universytetu "Lvivska politekhnika", 124–141.https://science.lpnu.ua/sites/default/files/journal-paper/2017/nov/6634/21-124-141.pdf.
11. Hryshchuk, R., & Hryshchuk, O. (2025). Otsiniuvannia kryptostiikosti kryptosystemy Fredholma: metodolohiia ta analiz rezultativ [Evaluation of the cryptographic strength of the Fredholm cryptosystem: Methodology and analysis of results]. Kiberbezpeka: osvita, nauka, tekhnika, 1(29), 748–761. https://doi.org/10.28925/2663-4023.2025.29.935.
12. Jiang, X., Lakhno, V., Sahun, A., & Mamchenko, S. (2024). Development of a symmetric cryptographic differential distinguisher based on deep learning. Cybersecurity: Education, Science, Technique, 2(26), 123–139. https://doi.org/10.28925/2663-4023.2024.26.674.
13. Gargiulo, J. (2002, July 25). S-Box modifications and their effect in DES-like encryption systems (GSEC v1.4, Option 1). GIAC. https://www.giac.org/paper/gsec/2048/s-box-modifications-effect-des-like-encryption-systems/103534.
14. Shawky, N., Ahmed, I., & Ibrahim, A. (2023). S-box modification for the block cipher algorithms. Przegląd Elektrotechniczny, 99(4), 47–50. https://doi.org/10.15199/48.2023.04.48.
15. Ministerstvo ekonomichnoho rozvytku i torhivli Ukrainy. (2009). DSTU GOST 28147:2009. Systema obrobky informatsii. Zakhyst kryptohrafichnyi. Alhorytm kryptohrafichnoho peretvorennia (GOST 28147-89). Kyiv: DP «UkrNDNTs». https://online.budstandart.com/ua/catalog/doc-page.html?id_doc=55943.
16. Ministerstvo ekonomichnoho rozvytku i torhivli Ukrainy. (2014). DSTU 7624:2014. Informatsiini tekhnolohii. Kryptohrafichnyi zakhyst informatsii. Alhorytm symetrychnoho blokovoho peretvorennia. Kyiv: DP «UkrNDNTs», 2014. https://online.budstandart.com/ua/catalog/doc-page?id_doc=65314.
17. National Institute of Standards and Technology. (2001). Advanced Encryption Standard (AES) (NIST FIPS 197). U.S. Department of Commerce. https://doi.org/10.6028/NIST.FIPS.197. https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=901427 (Accessed December 4, 2025).
18. SOG-IS Crypto Working Group. (2023). SOGIS agreed cryptographic mechanisms (Version 1.3). SOG-IS. https://www.sogis.eu/documents/cc/crypto/SOGIS-Agreed-Cryptographic-Mechanisms-1.3.pdf.

Сагун Андрій Вікторович
кандидат технічних наук, доцент, доцент кафедри комп'ютерних систем, мереж та кібербезпеки,
Національний університет біоресурсів і природокористування України
ORCID: https://orcid.org/0000-0002-5151-9203
E-mail: a.sagun@nubip.edu.ua

Панаско Олена Миколаївна
кандидат технічних наук, доцент, доцент кафедри робототехнічних і телекомунікаційних систем та кібербезпеки,
Черкаський державний технологічний університет, м. Черкаси
ORCID: https://orcid.org/0000-0002-0510-7742
E-mail: lena.pa@ukr.net

ТЕНДЕНЦІЇ ПІДВИЩЕННЯ КРИПТОГРАФІЧНОЇ МІЦНОСТІ СИМЕТРИЧНИХ БЛОКОВИХ ШИФРІВ У КОНТЕКСТІ СУЧАСНОГО РОЗВИТКУ КРИПТОСИСТЕМ

***Анотація**. У статті розглядається поєднання аналітичних та прикладних підходів до вдосконалення симетричних блокових шифрів у світлі сучасних тенденцій розвитку криптографічних систем. У дослідженні аналізуються сучасні стандарти та рекомендації SOG-IS, що визначають основні напрямки еволюції*

ISSN 3083-7502

симетричних алгоритмів, такі як перехід від застарілих схем на основі алгоритму Файстеля до оптимізованих структур (AES, полегшені блокові шифри для Інтернету речей). Використовуючи модифіковану версію шифру Simple-DES (S-DES), у статті пропонується метод підвищення криптографічної стійкості без зміни довжини ключа або блоку. Основні вдосконалення полягають у вдосконаленій конструкції S-боксів та їх динамічному виборі на основі графа ключів. Результати порівняльного аналізу демонструють значне підвищення стійкості до брут-форс-аналізу та диференціального криптоаналізу порівняно зі стандартним S-DES, зберігаючи при цьому низьку обчислювальну складність. Проведене дослідження підтверджує актуальність використання навчальних та експериментальних моделей, таких як S-DES, для вивчення сучасних методів підвищення безпеки симетричних шифрів, що має практичне значення для прототипування та легких реалізацій у системах Інтернету речей.

***Ключові слова**: симетричне шифрування, блокові шифри, мережа Файстеля, S-DES, S-бокси, криптографічна стійкість, AES, полегшені шифри, Інтернет речей, SOG-IS.*