Journal scientific and applied research, vol. 26, 2024
International Journal

ISSN 1314-6289 (Print)
ISSN 2815-4622 (Online)

Original Contribution

IMPLEMENTATION OF THE SYMMETRIC CRYPTOGRAPHIC ALGORITHMS RC2 AND TRIPLE DES IN ECB MODE USING CRYPTOGRAPHIC SOFTWARE PROGRAM CRYPTOOL

Petar Kr. Boyanov

COMMUNICATION AND COMPUTER TECHNOLOGIES, FACULTY OF TECHNICAL SCIENCES, KONSTANTIN PRESLAVSKY UNIVERSITY OF SHUMEN, SHUMEN 9712, 115, UNIVERSITETSKA STR., E-MAIL: petar.boyanov@shu.bg

ABSTRACT: *This paper presents an in-depth analysis of symmetric key cryptographic algorithms, focusing on RC2 and Triple DES (ECB) as implemented in CrypTool. It is widely used educational software that demonstrates various cryptographic algorithms and methods. This paper aims to provide a foundational understanding of CrypTool, explain the functionalities of RC2 and Triple DES in Electronic Codebook (ECB) mode and evaluate their performance and security.*

KEY WORDS: *Algorithms, Cryptology, CrypTool, Decryption, Encryption, Hex, Integrity, Crack, Method, Privacy, Security, RC2, Triple DES.*

1. Introduction

The Symmetric encryption algorithms, which use a single shared key for both encryption and decryption, are integral to secure data transfer. RC2 and Triple DES [3,21,24,26,31] are widely used symmetric key algorithms, each with unique properties, use cases, and vulnerabilities.

The primary aim of this scientific paper is to analyze and compare the RC2 and Triple DES (ECB) algorithms using CrypTool, an open-source educational tool [1,6,7,9,11,15,18,19,20,22] for cryptographic analysis. This paper aims to provide insights into their operational principles, security features, and practical applications, as well as to explore their effectiveness within the CrypTool software environment [1,3,4,9,11,15,19,20,25,39].

CrypTool is a free of charge software environment that serves as an educational platform for cryptography [23,24,26,27,32,33,36,43,44]. It offers various modules for classical and modern cryptography, allowing users to experiment with encryption, decryption, key management, and several cryptographic cyber-attacks. It supports several cryptographic algorithms,

including both symmetric and asymmetric key algorithms [21,24,26,30,33, 35,42].

The RC2 algorithm operates on 64-bit data blocks with a variable key size ranging from 8 to 128 bits, typically using a 64-bit key in practical applications.

In CrypTool, the RC2 algorithm can be executed with various key sizes, providing flexibility in terms of encryption strength. The software allows users to input a plaintext, select a key size, and visualize the plaintext transformed into ciphertext via a series of encryption rounds [5,6,7,8,9,22,23,37,38,39,43].

Typically, 3DES uses either two or three unique 56-bit keys (resulting in a 112-bit or 168-bit [3,21,24,26,31] effective key length, respectively). In the Electronic Codebook (ECB) mode, each 64-bit data block is encrypted independently. While this approach allows parallel processing and is simple to implement, it has limitations and issues with the same plaintext blocks that will produce same ciphertext blocks [1,2,3,4,5,6,27,30,31,32,33,34,35,36].

In CrypTool, 3DES (ECB) [3,21,24,26,31] mode can be applied to plaintext data, with users specifying the number of keys (2 or 3) and observing the block-by-block encryption process.

The program CrypTool [23,24,26,27,32,33,36,43,44] also visualizes the differences between ECB mode and other block cipher modes, such as CBC (Cipher Block Chaining), highlighting ECB’s susceptibility to certain types of cyber-attacks [4,5,6,7,35,38].

The conducted experiments in this scientific paper that aim to encrypt and decrypt important and confidential information without the host's permission is considered as a crime and, if proven, is punishable to the full extent of the law of the respective country [4,5,11,12,21,23,24,34,42]. Everything illustrated and explained in this scientific paper is for research work and educational purposes and the author is not responsible in cases of abuse.

2. Related work

These scientific works [1,3,4,5,6,8,15,20,30,33,35,36,42,43] collectively explore various aspects of implementation symmetric cryptographic [7,9,11,18,19,21,22,23,24,38] algorithms RC2 and Triple DES for encrypt and decrypt concealed plaintext [25,26,27,31,32,35,37,39,44].

The Information encryption is also used in application of electronic platforms [28], various types of instrumental equipment for cyberattack prevention [17], specific models for accessing information resources in a secure environment and other technologies [16], net model of command and control system [13], building data center system for defense and security [12], designing and implementation of software-defined systems [14], information exchange management in multimodule multi-position security systems [10], applications of Artificial Intelligence in e-Learning [29], information systems for crisis prevention [34], performance analysis of a mobile computer equipped with solid

state disk [41], modeling and calculation of passive audio crossovers [40] and designing of stream ciphers based on random feedback shift registers [2].

3. Experiment

CrypTool [1,6,7,9,11,15,18,19,20,22] is ideal for simulating cryptographic techniques and evaluating algorithmic strengths and weaknesses. In this scientific study, it is used the software program CrypTool version 1.4.40 in order to implement RC2 and Triple DES in ECB mode, observing their encryption-decryption processes and evaluating their performance [33,34,36,42,43,44].

RC2 was widely adopted in early internet communications, particularly in Microsoft applications and email encryption protocols. However, its usage has declined due to advances in cryptanalysis and the development of stronger encryption algorithms [1,3,9,23,24,25,31,30,37,44].

Triple DES [3,21,24,26,31] was widely used in financial and government institutions, particularly for legacy systems. However, due to its slower performance and security limitations, it is gradually being replaced by more secure algorithms such as AES [1,3,11,25,31,30,34,35,37,38,43].

The scientific experiments in this paper in a specialized computer network laboratory in the Faculty of Technical Sciences of the Konstantin Preslavsky University of Shumen are made. The used operating system is Windows 10 Pro x64 version 22H2, OS build: 19045.4355 [4,5].

When the program starts, the following dialog box appears shown in fig. 1.

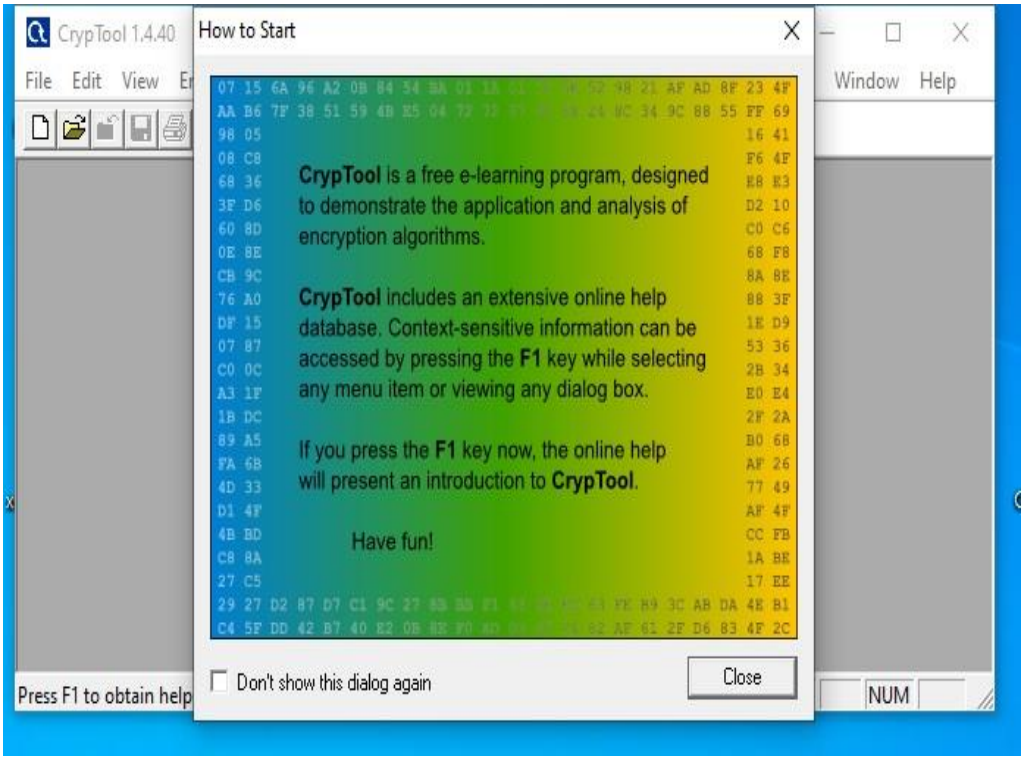

Fig. 1. The started program CrypTool

The next task a text file is to be created. It contains the following text: “This is the first test made by Petar Boyanov!!!” (shown in fig. 2). Scientific research will begin with the implementation of the symmetric key cryptographic algorithms RC2.

The next step involves encrypting the plaintext with RC2 algorithm. This is shown in fig. 3. Then, the length of the key is chosen to be 8 bits with key - “AF” and the button “Encrypt” is selected. This is presented in fig. 4. After that, the encryption process is instantaneous and the encrypted message in Fig. 5 is shown.

Finally, the encrypted plaintext with name “encrypted_text_1” and file extension “.hex” is saved. The software editor Notepad++ for opening the encrypted file is used. All these steps in fig. 6 are illustrated.

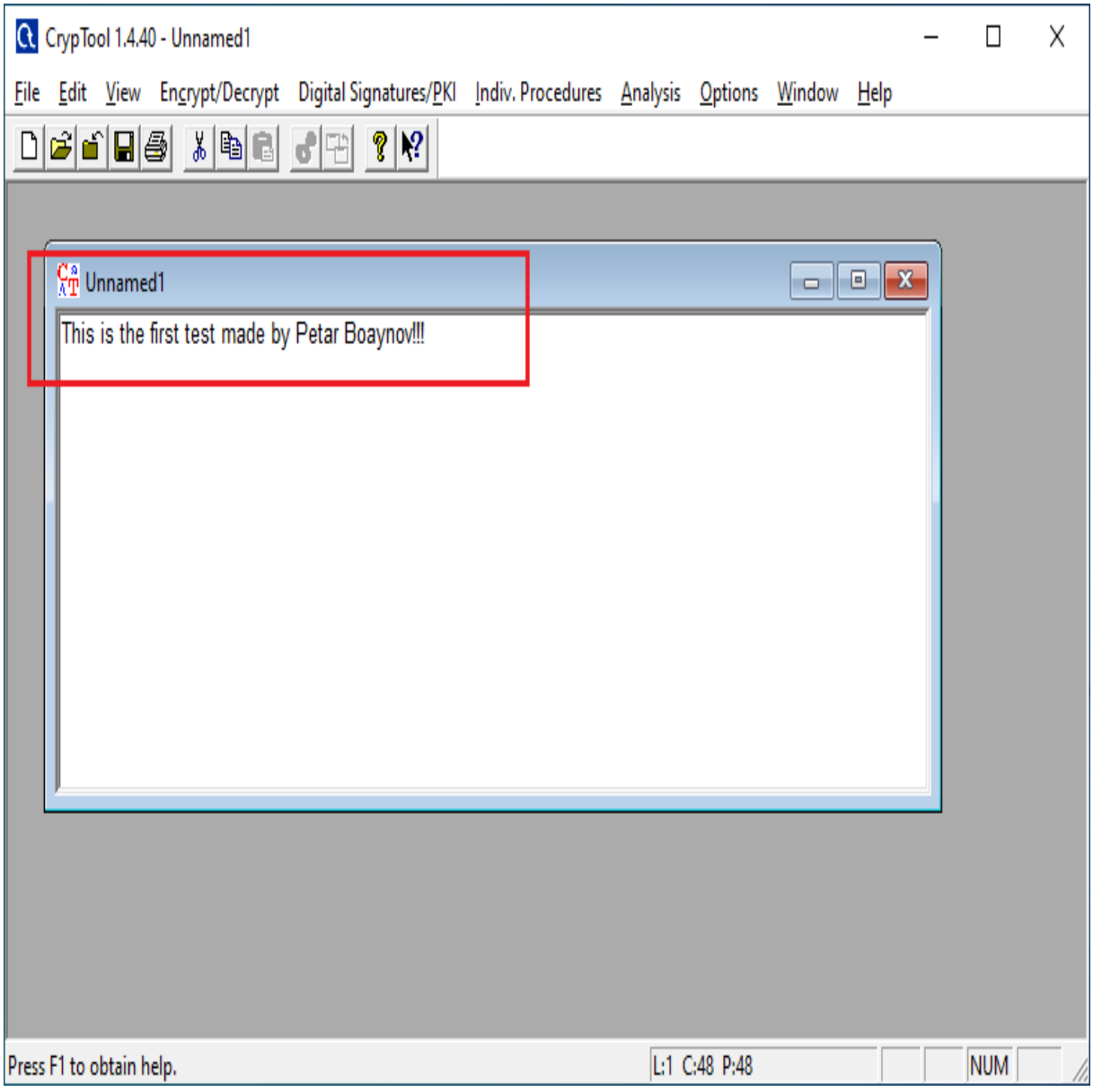

Fig. 2. The created plaintext for encryption

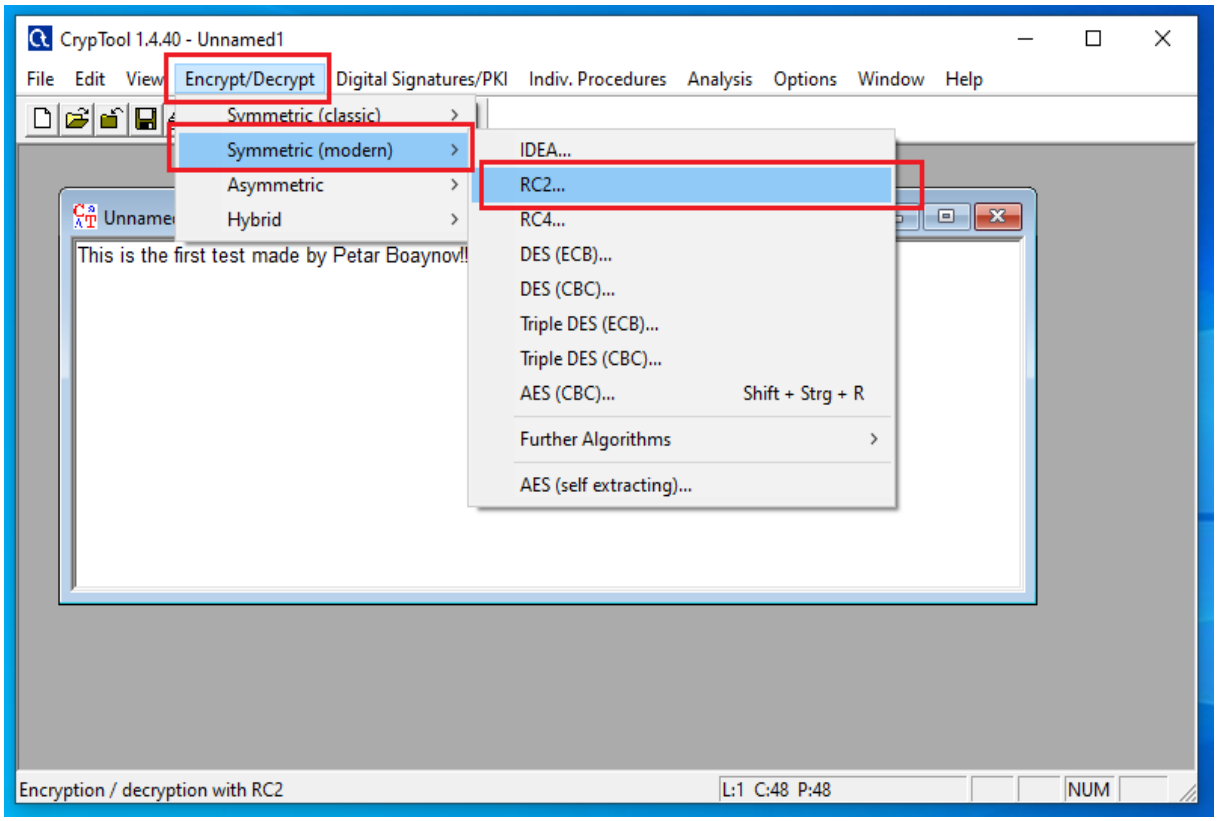

Fig. 3. Choosing a symmetric encryption algorithm

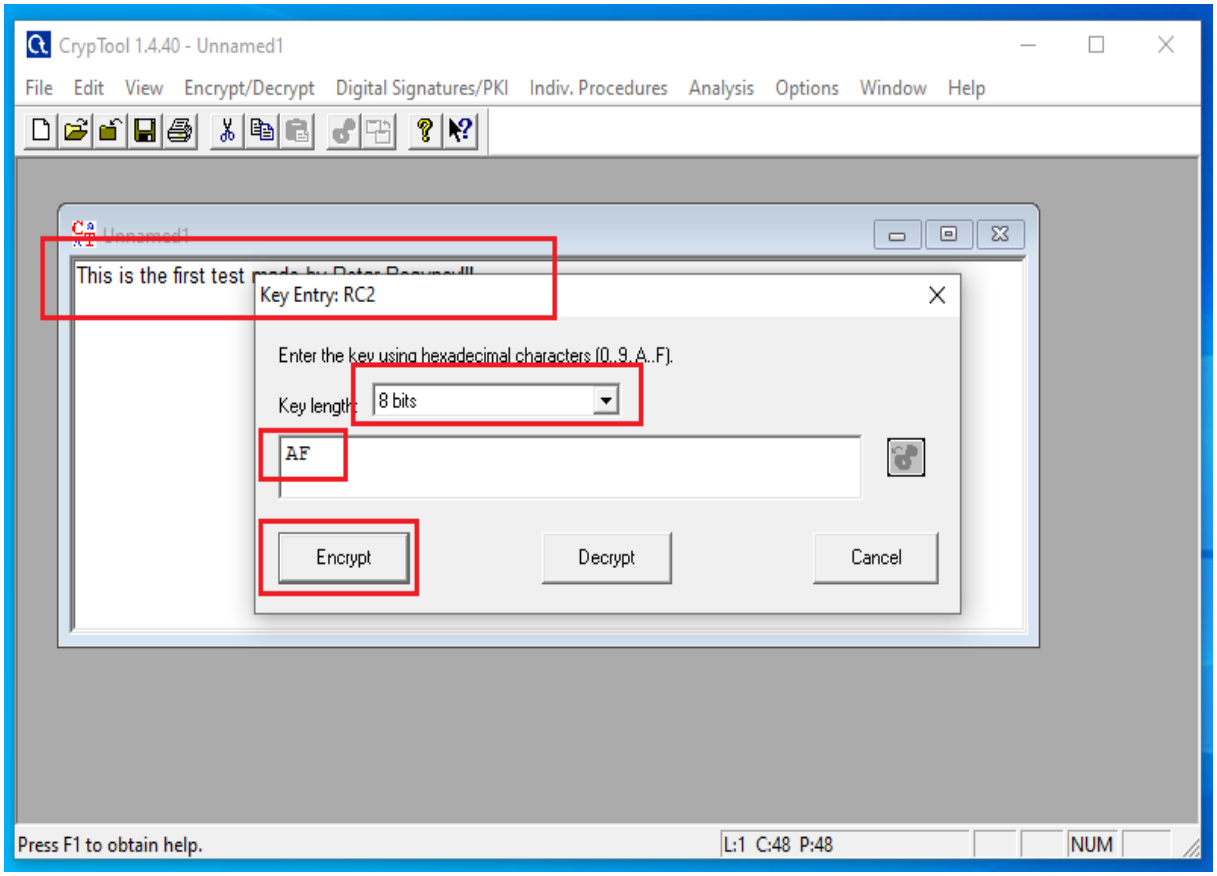

Fig. 4. The plaintext encryption's settings

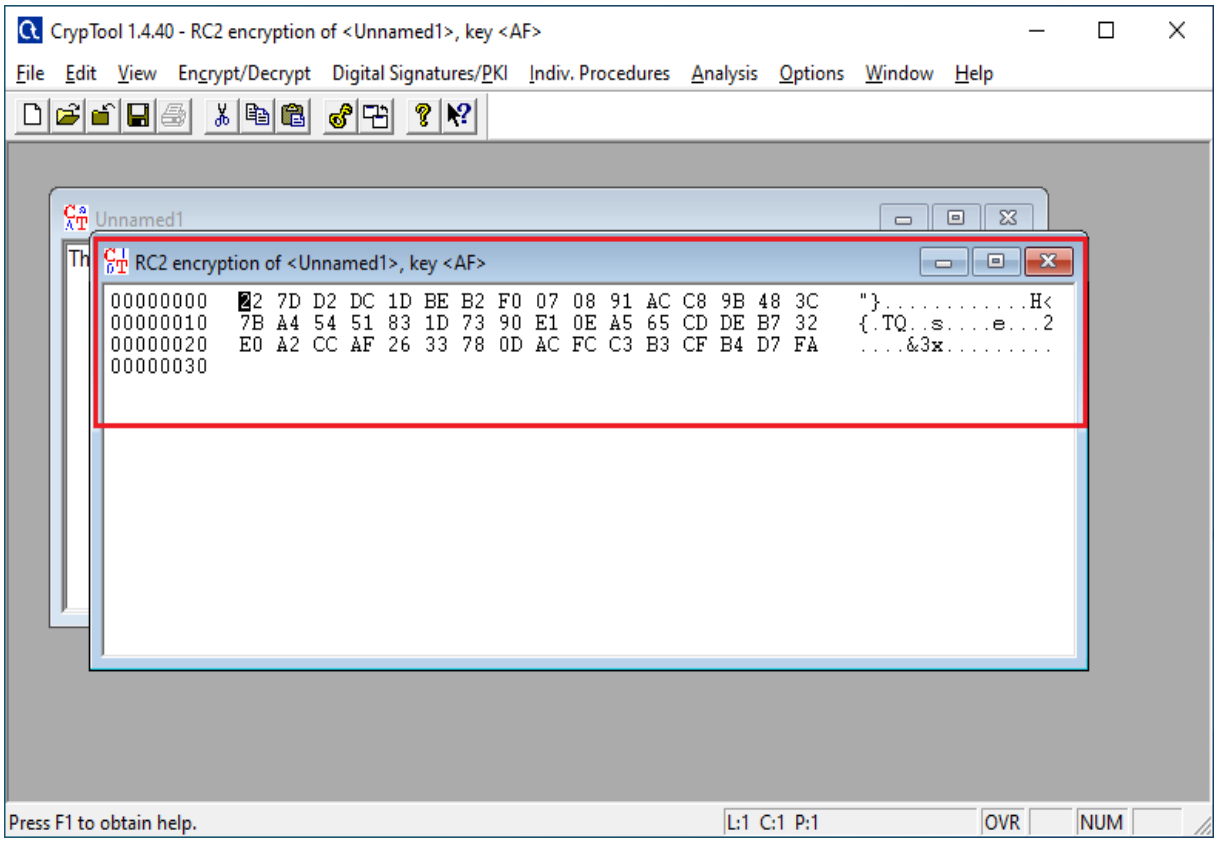

Fig. 5. The encrypted text with RC2 algorithm

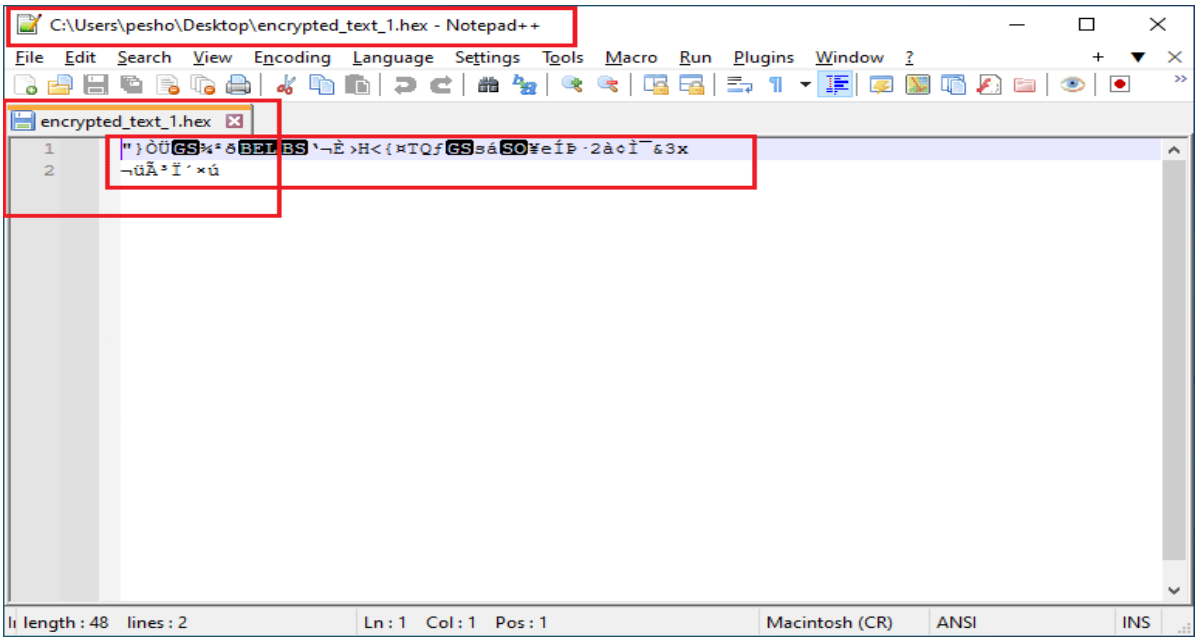

Fig. 6. The opened encrypted plaintext with Notepad++

The second plaintext contains the following:
“This is the second test made by Petar Boyanov!!!
Date: 21_10_2024
Location: Konstantin Preslavsky University of Shumen”.

The steps for plaintext encryption with Triple DES (ECB) [3,21,24,26,31] are repeated with those shown earlier in this paper. The first difference with this encryption algorithm is that the key length is 128 bits. The second difference is that the key length consists of the following 64 bits combination: “AF AF AF AF AF AF AF AF AF AF AF AF AF AF AF AF”. This is shown in fig. 7.

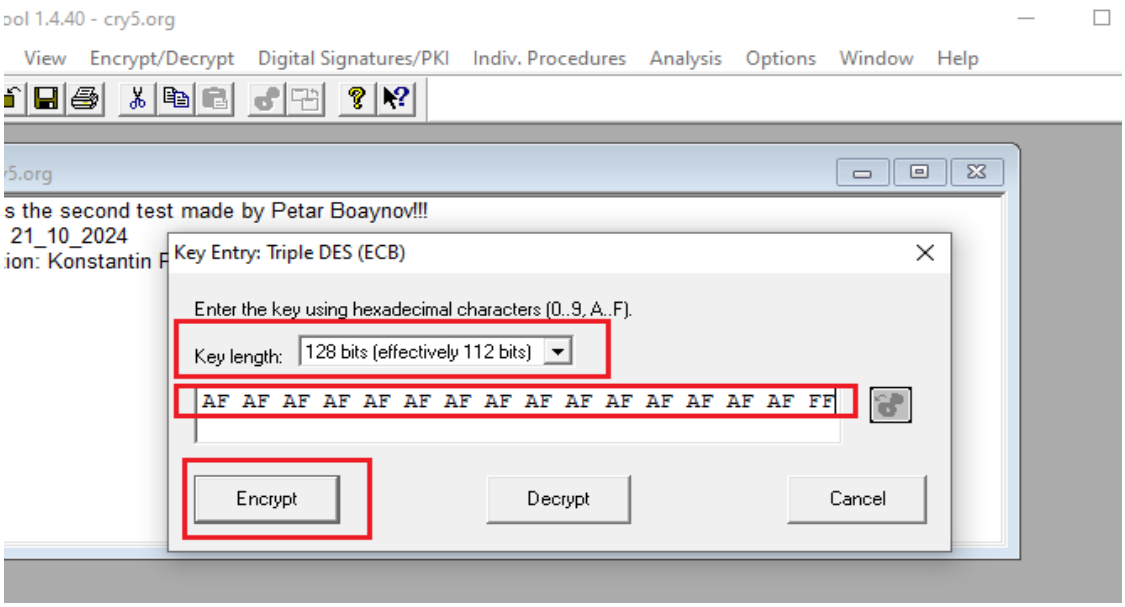

Fig. 7. The encryption’s setting for Triple DES (ECB)

The encrypted plaintext with name “encrypted_text_2” and file extension “.hex” is saved. The software editor Notepad++ for opening the encrypted file is used. All these steps in fig. 8 are illustrated.

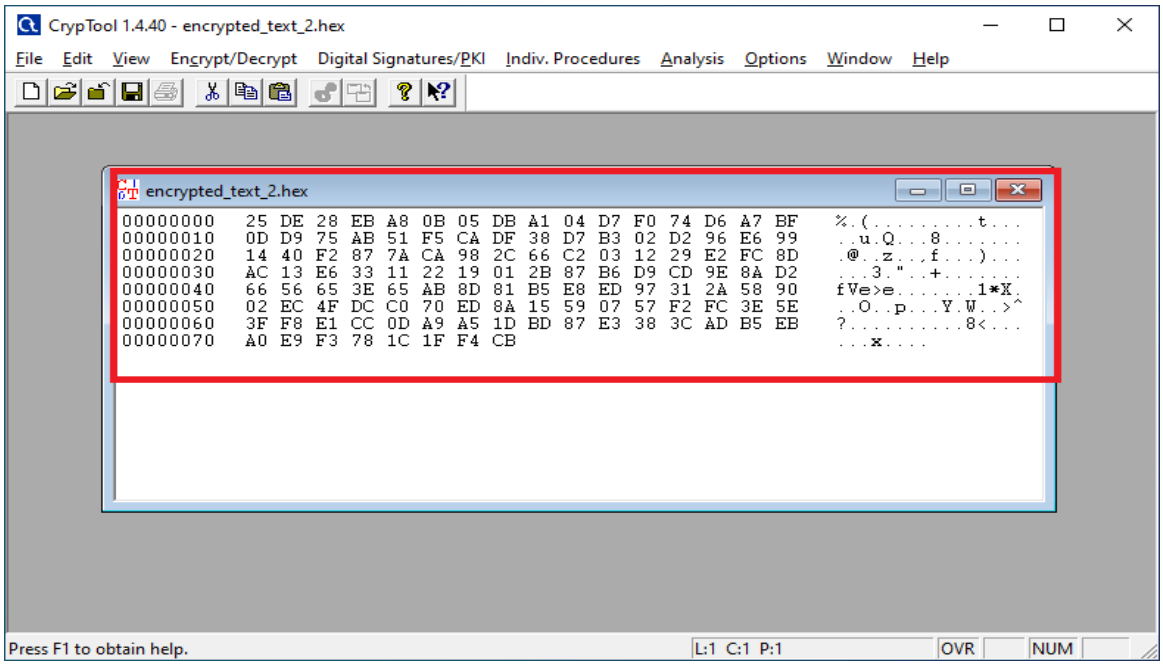

Fig. 8. The encrypted text with Triple DES algorithm

4. Results

Decryption of the first ".hex" file is done by selecting the RC2 algorithm and entering the key "AF". This is shown in fig. 9.

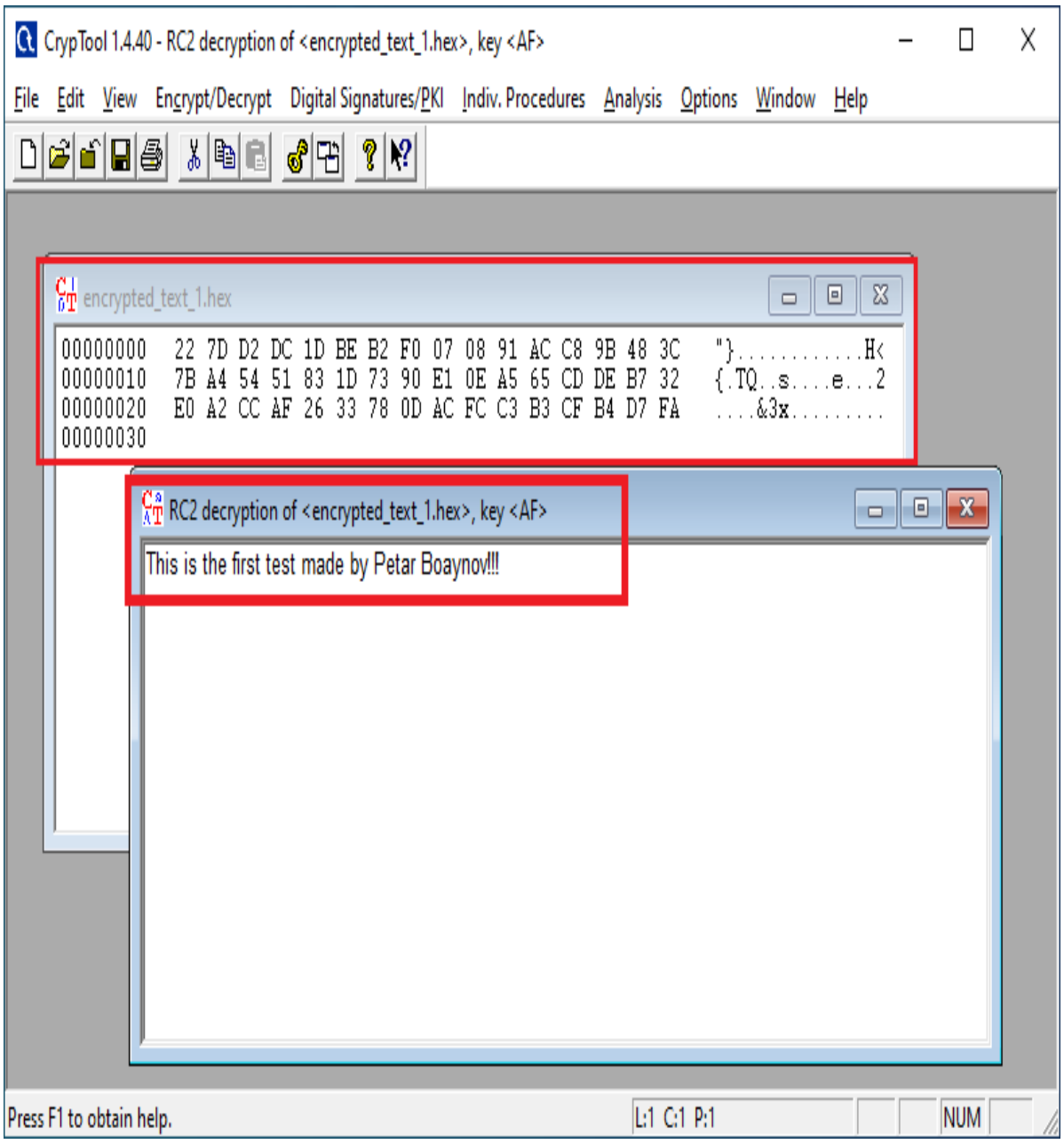

Fig. 9. Decryption of the first file "encrypted_text_1.hex"

Decryption of the second ".hex" file is done by selecting the Triple DES (ECB) algorithm and entering the key "AF AF AF AF AF AF AF AF AF AF AF AF AF AF AF FF". This is shown in fig. 10.

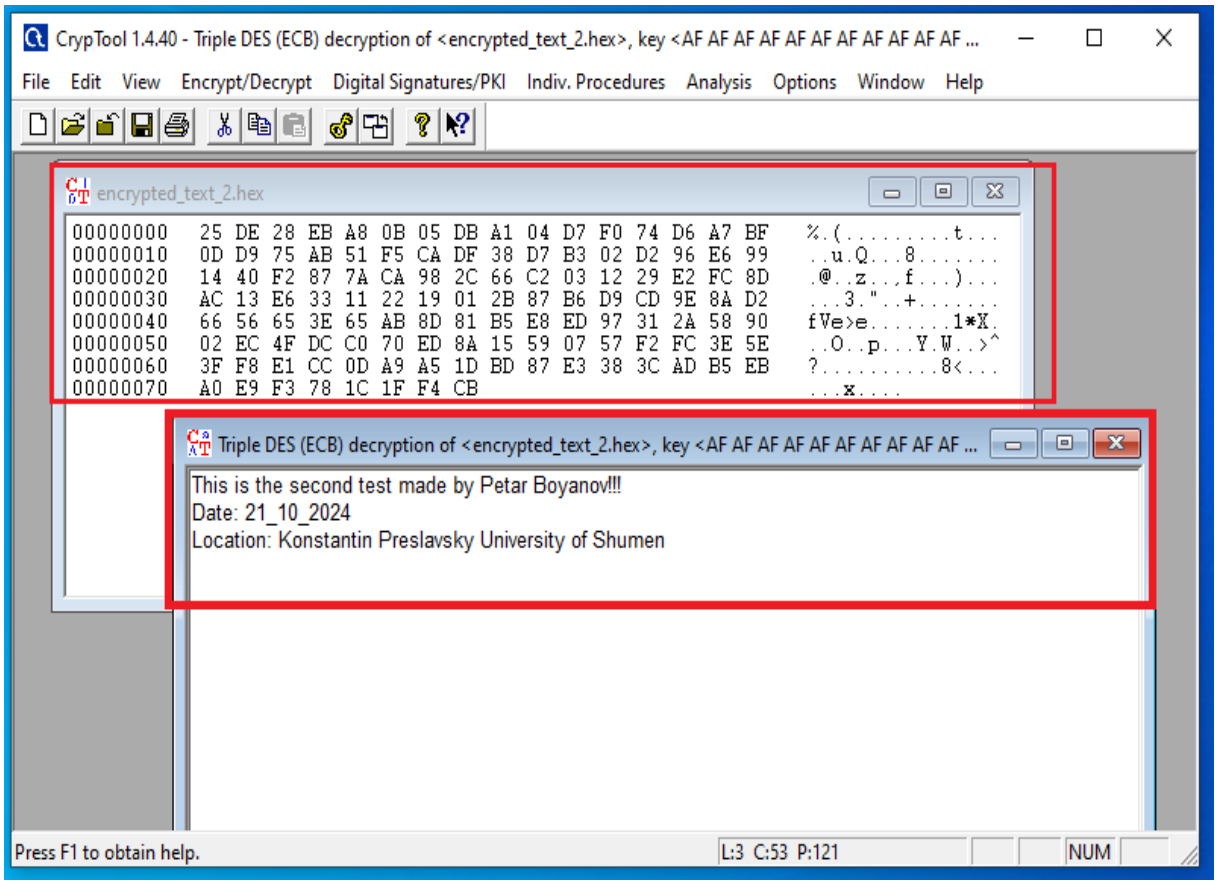

Fig. 10. Decryption of the second file “encrypted_text_2.hex”

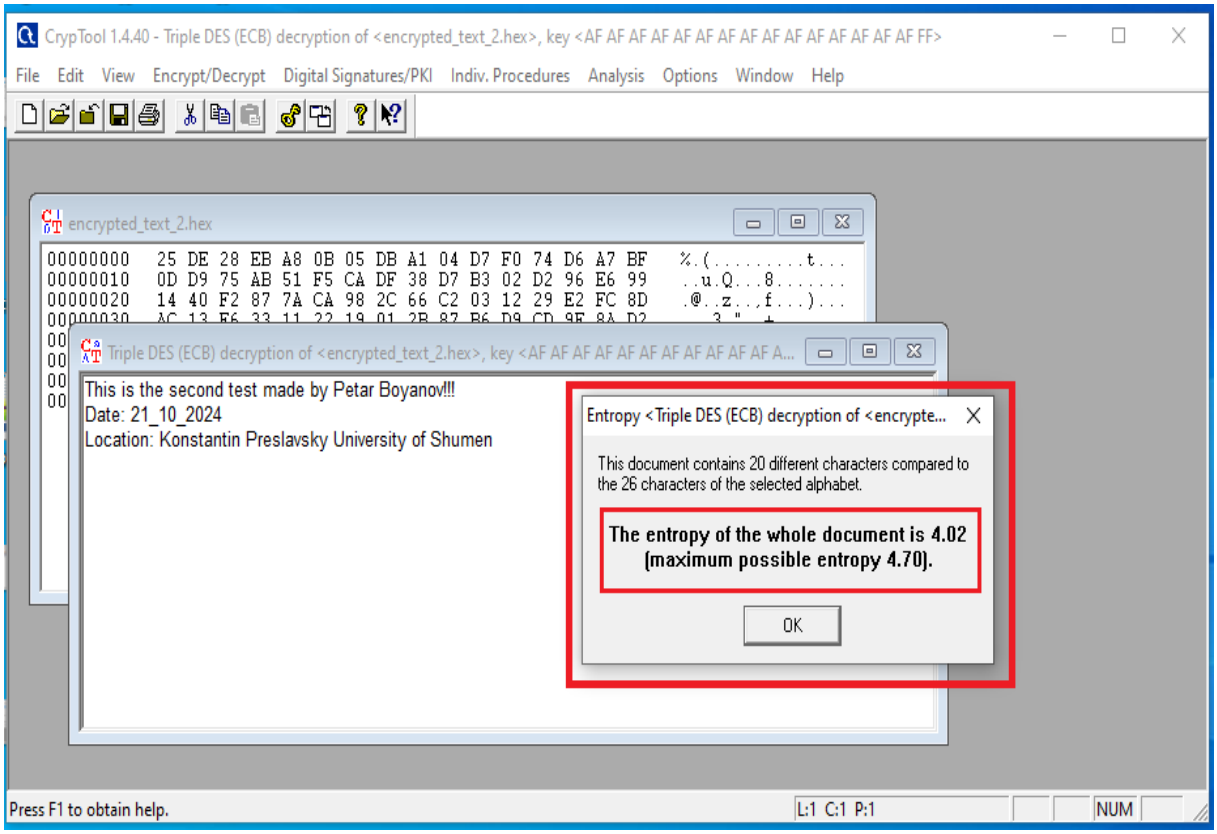

Fig. 11. The entropy of the second file “encrypted_text_2.hex”

Through this software program, a deep analysis can be performed and based on it, certain statistics about the text content of the text file can be presented. On fig. 11 the entropy of the whole document and the maximum possible entropy is presented. The ASCII histogram of frequency (%) of the second file is illustrated in fig. 12.

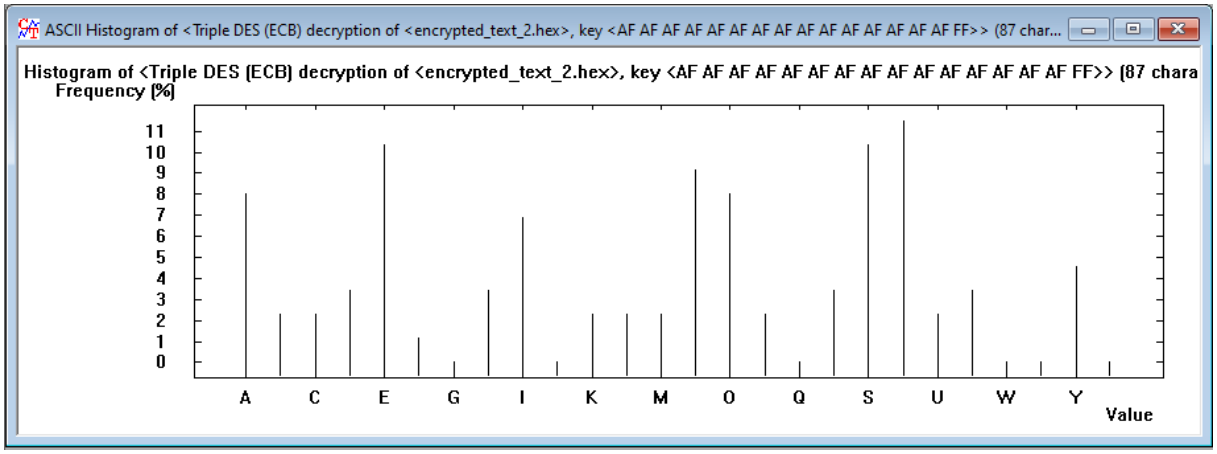

Fig. 12. The ASCII histogram of frequency (%) of the second file "encrypted_text_2.hex"

The N-gram list of the file "encrypted_text_2.hex" in fig. 13 is presented.

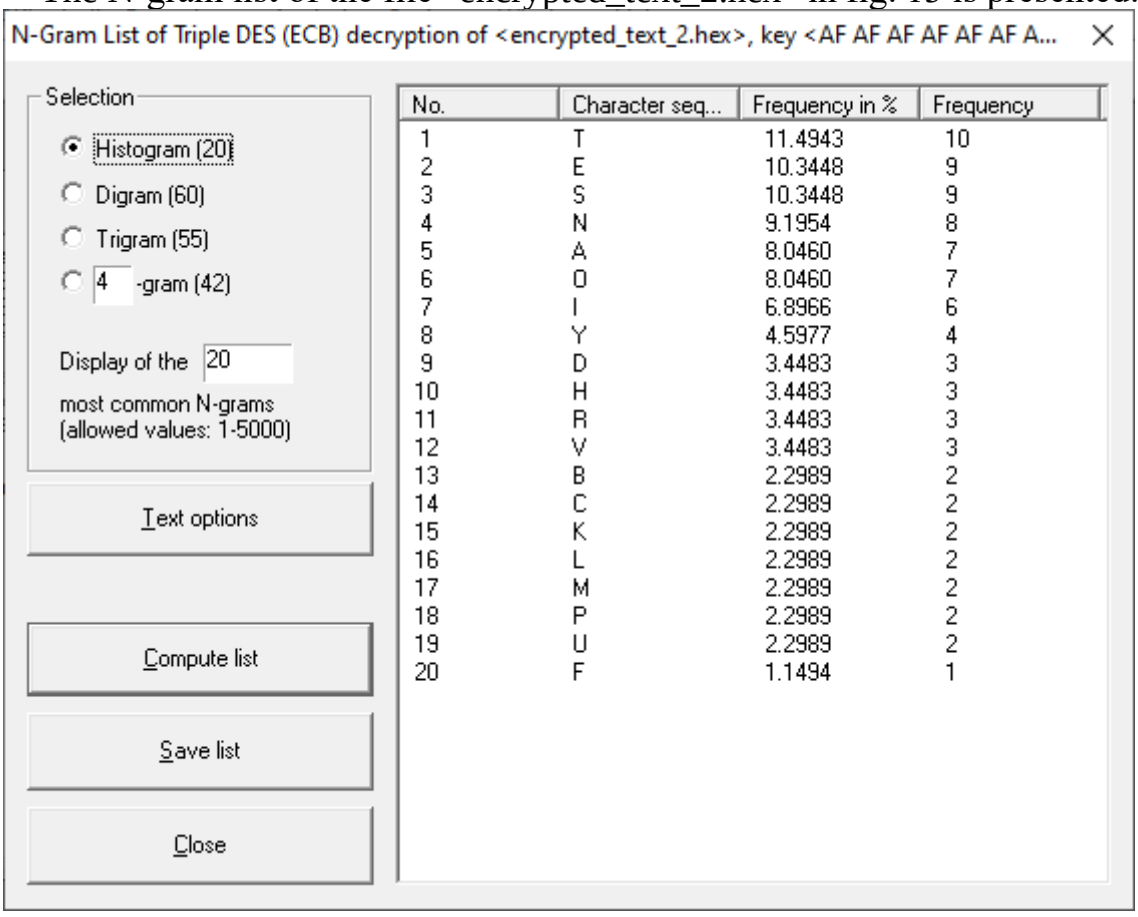

Fig. 13. The N-gram list of the file "encrypted_text_2.hex"

The floating frequency of file “encrypted_text_2.hex” in fig. 14 is shown.

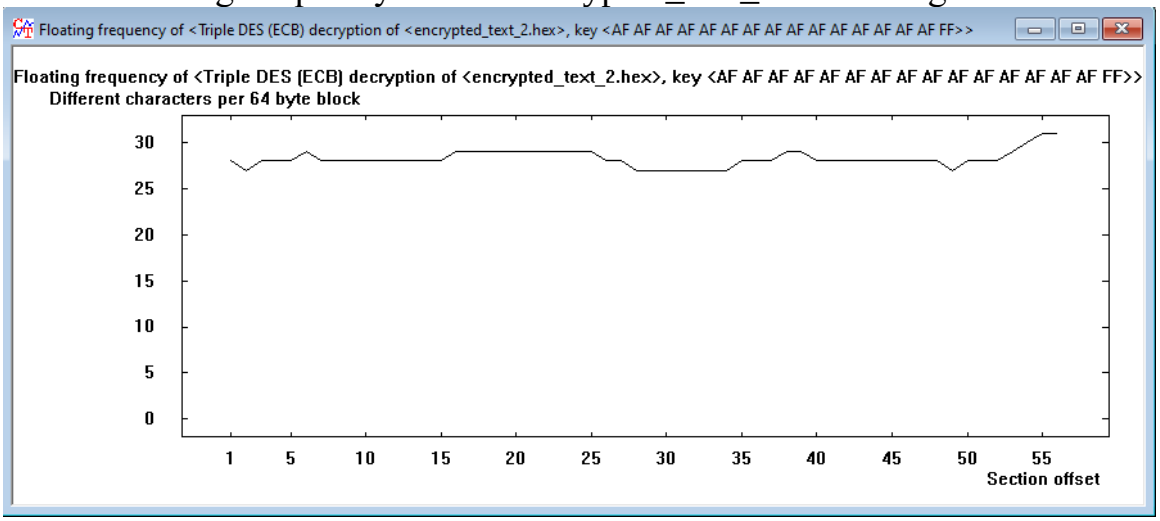

Fig. 14. The floating frequency of file “encrypted_text_2.hex”

The program allows the user to find out what the value of the hash function of the original file is and accordingly, if changes occur in the file, to display the new value of the hash function. The MD5 hash function in this research is used. This is shown in fig. 15 and 16.

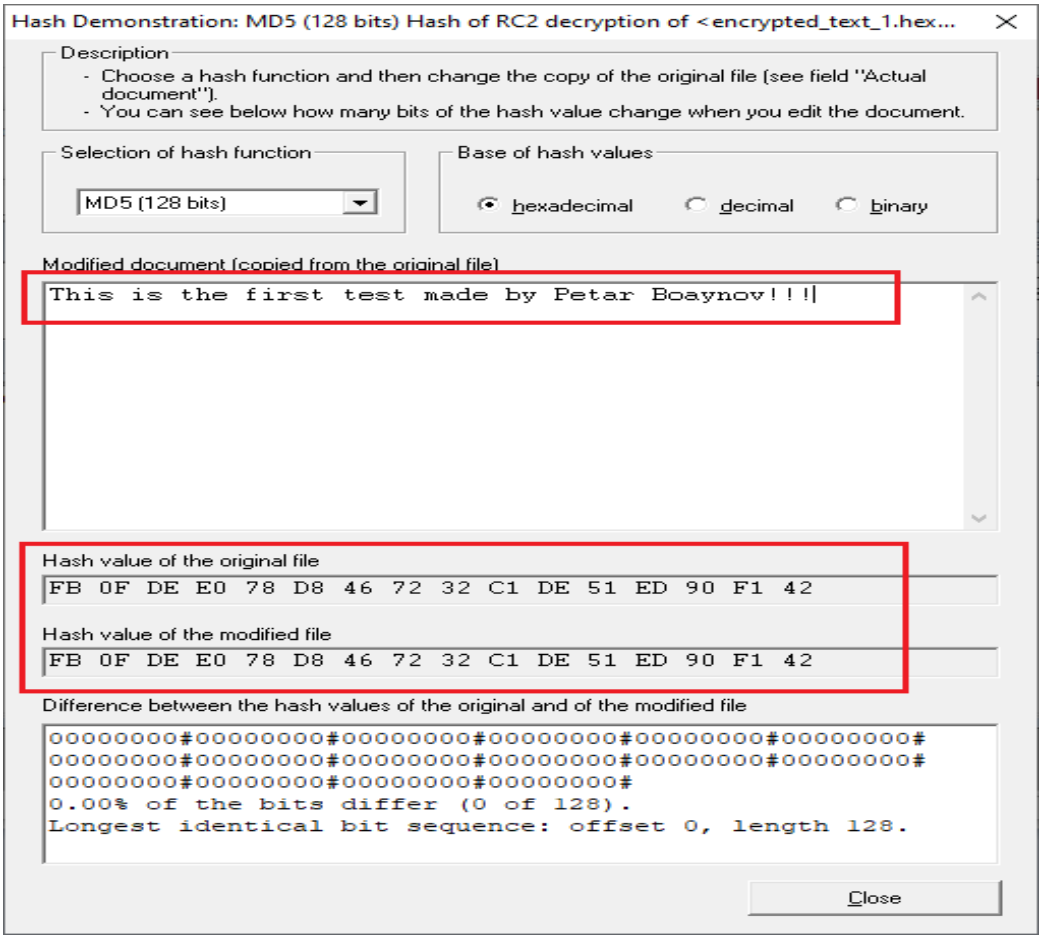

Fig. 15. The first plaintext without modifications

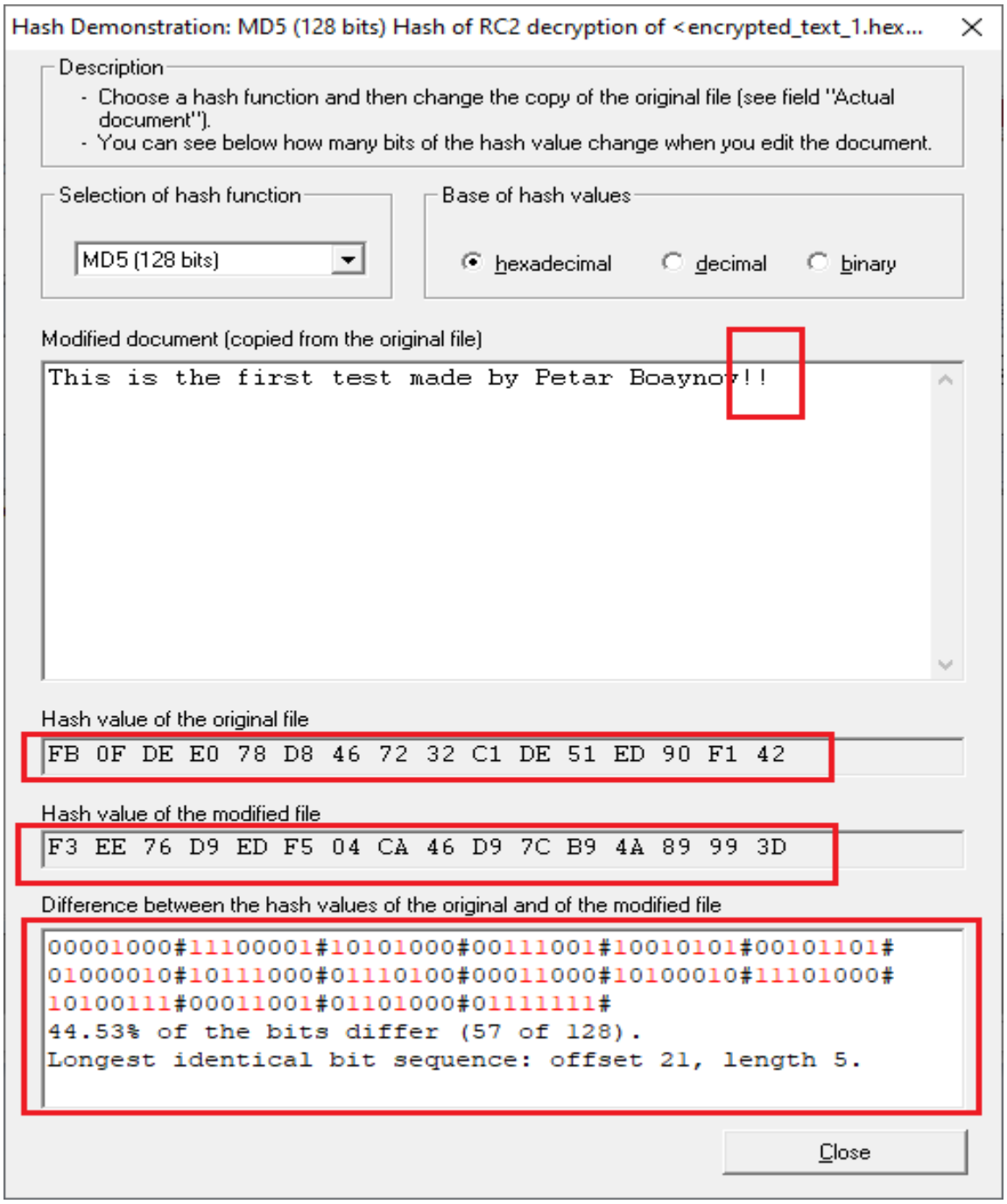

Fig. 16. The first plaintext with modifications

While both algorithms have vulnerabilities, Triple DES [3,21,24,26,31] offers higher security due to its longer effective key length. RC2, with its variable key length, provides flexibility but is generally less secure compared to 3DES [3,21,24,26,31].

Given its faster performance and lower resource requirements, RC2 may be suitable for less sensitive applications that prioritize speed over security. Triple DES [3,21,24,26,31], despite its limitations, remains a viable choice for applications requiring strong encryption with compatibility for legacy systems.

5. Conclusion

In this paper, the capabilities of CrypTool in analyzing symmetric key algorithms, focusing on RC2 [37] and Triple DES [3,21,24,26,31] in ECB mode are explored. Thanks to the obtained results, it was found that while RC2 [37] is faster and less resource-intensive, it has significant security limitations [1,6,7,9,11,15,18,19,20,22]. On the other hand Triple DES is more secure but has become outdated due to its computational demands and pattern vulnerability in ECB mode. The software program CrypTool [23,24,26,27,32,33,36,43,44] proves to be an effective tool for understanding and evaluating these algorithms, making it valuable for educational and preliminary cryptographic analyses. In this regard the exceptionally well-equipped laboratories at the Faculty of Technical Sciences at the Konstantin Preslavsky University of Shumen [4,5] give great opportunities to students majoring in "Communication and Information Systems", "Computer Technologies in Automated Manufacturing" and "Signal Security Systems and Technologies" to gain extensive theoretical and practical experience in field of the digital cryptology and cryptanalysis [4,5].

References:

[1] Balasubramanian, K. (2021). Experiments with the Cryptool Software. In Research Anthology on Blockchain Technology in Business, Healthcare, Education, and Government (pp. 424-432). IGI Global.

[2] Bedzhev, B., Trıfonov, T., & Nıkolov, N. (2010). A multicore computer system for design of stream ciphers based on random feedback shift registers. İstanbul Aydın Üniversitesi Dergisi, Turkey, 2(7), 1-15., https://dergipark.org.tr/en/download/article-file/319309. [Last accessed on 25 September 2024]

[3] Biryukov, A., De Cannière, C.: Data Encryption Standard (DES). In: van Tilborg H.C.A., Jajodia S. (eds.) Encyclopedia of Cryptography and Security, p. 296. Springer, Boston, MA (2011)

[4] Boyanov, P., Using modified sniffer scripts, implementing linear algorithms for detection of network port scan attacks in Linux based operating systems. A refereed Journal Scientific and Applied Research, Konstantin Preslavsky University Press, Vol. 24, Shumen, 2023, ISSN 1314-6289 (Print), ISSN 2815-4622 (Online), pp. 78-88, DOI: https://doi.org/10.46687/jsar.v24i1.371.

[5] Boyanov, P., Investigating the network traffic using the command-line packets sniffer Tcpdump in Kali Linux. A refereed Journal Scientific and Applied Research, Konstantin Preslavsky University Press, Vol. 25,

Shumen, 2023, ISSN 1314-6289 (Print), ISSN 2815-4622 (Online), pp. 31-44, DOI: https://doi.org/10.46687/jsar.v25i1.378.
[6] Esslinger, B. (2008). CrypTool. Available via www.cryptool.de. [Last accessed on 19 September 2024]
[7] Esslinger, B. (2024). Learning and Experiencing Cryptography with CrypTool and SageMath. Artech House, ISBN: 978-1-68569-017-5.
[8] El-Morshedy, D. S., El-Attar, N. E., Hanafy, I. M., & Awad, W. A. (2023). Cryptographic Algorithms for Enhancing Security in Cloud Computing. Alfarama Journal of Basic & Applied Sciences, 4(3), 433-455.
[9] Garg, A., Sharma, K. K., & Chauhan, S. Performance Analysis of Password-Based AES Encryption and Decryption Using Cryptool.
[10] Gueorguiev N.L., Nesterov K.N., Minev S., An approach to information exchange management in multimodule multi-position security systems. International Scientific Journal "Security & Future", Vol. 6, Issue 1, pp: 28-31, STUME, 2022, WEB ISSN 2535-082X; PRINT ISSN 2535-0668.
[11] Hick, S., Esslinger, B., & Wacker, A. (2012). Reducing the complexity of understanding cryptology using CrypTool. In 10th International Conference on Education and Information Systems, Technologies and Applications (EISTA 2012), Orlando, Florida, USA.
[12] Iliev, R., K. Ignatova. Cloud technologies for building data center system for defense and security. T. Tagarev et al. (eds.), Digital Transformation, Cyber Security and Resilience of Modern Societies, Studies in Big Data 84, ISBN 978-3-030-65721-5, Springer 2020, pp.13-24,https://doi.org/10.1007/978-3-030-65722-2.
[13] Iliev, R., Kochankov, M., A Generalized Net Model of Command and Control System. In Proceedings of the 15th International Scientific and Practical Conference, Environment. Technology. Resources. Rezekne, Latvia, Volume II, pp. 127-131, Print ISSN 1691-5402, Online ISSN 2256-070X, https://doi.org/10.17770/etr2024vol2.8035.
[14] Ivanov, I., & Aleksandrova, K. (2024, June). Design and Implementation of Software-Defined Doppler Radar. In Proceedings of the 15th International Scientific and Practical Conference, Environment. Technology. Resources. Rezekne, Latvia, Volume III, pp. 105-108, Print ISSN 1691-5402, Online ISSN 2256-070X, https://doi.org/10.17770/etr2024vol3.8159
[15] Jüttner, A. C. Analysis of the Functionality, Risks and Counter-Measures of Current Padding Attacks and the Implementation of an Attack in the Open-Source Program CrypTool 2.

[16] Kochankov, M., & Iliev, R. (2024, June). A Generalized Net Model for Accessing Information Resources in a Secure Environment. In Proceedings of the 15th International Scientific and Practical Conference, Environment. Technology. Resources. Rezekne, Latvia, Volume II, pp. 175-178, Print ISSN 1691-5402, Online ISSN 2256-070X, https://doi.org/10.17770/etr2024vol2.8034.
[17] Kolev, Alexander, Nikolova, Pavlina. Instrumental Equipment for Cyberattack Prevention. Information & Security: An International Journal 47, no. 3 (2020):285-299. https://doi.org/10.11610/isij.4720.
[18] Kopal, N. (2018, June). Solving Classical Ciphers with CrypTool 2. In HistoCrypt (pp. 149-010).
[19] Kopal, N., & Esslinger, B. (2022, June). New Ciphers and Cryptanalysis Components in CrypTool 2. In International Conference on Historical Cryptology (pp. 127-136).
[20] Kulshreshtha, S., Verma, V., & Kalra, R. (2011). Analytical View of Cryptographic Techniques through Cryptool. Journal of Telecommunications, 10(2), 22-26.
[21] Kumar, S., Paar, C., Pelzl, J., Pfeiffer, G., Rupp, A., Schimmler, M.: How to Break DES for BC 8,980. In: SHARCS‘06–Special-purpose Hardware for Attacking Cryptographic Systems, pp. 17–35 (2006)
[22] Lewis, B., Broadbent, M., Rotsos, C. et al. 4MIDable: Flexible Network Offloading For Security VNFs. J Netw Syst Manage 31, 52 (2023). https://doi.org/10.1007/s10922-023-09744-1.
[23] Maeref, M., & Algali, F. (2015, January). An empirical evaluation of Cryptool in teaching computer security. In Proceedings of the International Conference on Computer Science, Engineering and Applications (pp. 93-100).
[24] Manankova, O., & Yakubova, M. (2023, July). Modeling of the Modes of Operation of the AES Algorithm in the Cryptool 2 Environment. In Science and Information Conference (pp. 462-469). Cham: Springer Nature Switzerland.
[25] Manjula, R., & Anitha, R. (2011). Identification of encryption algorithm using decision tree. In Advanced Computing: First International Conference on Computer Science and Information Technology, CCSIT 2011, Bangalore, India, January 2-4, 2011. Proceedings, Part III 1 (pp. 237-246). Springer Berlin Heidelberg.

[26] Meça, A. (2023, August). Exploring Data Encryption Standard (DES) Through CrypTool Implementation: A Comprehensive Examination and Historical Perspective. In International Conference for Emerging Technologies in Computing (pp. 143-160). Cham: Springer Nature Switzerland.
[27] Mehreen, M. Usability Analysis of CrypTool-Online and CrypTool 2.
[28] Mirtcheva-Ivanova, Daniela, Application of electronic platforms to increase the knowledge of learners. In Proceedings of the 15th International Scientific and Practical Conference, Environment. Technology. Resources. Rezekne, Latvia, Volume II, pp. 448-452, Print ISSN 1691-5402, Online ISSN 2256-070X, https://doi.org/10.17770/etr2024vol2.8090.
[29] Mirtcheva-Ivanova, D., Application of Artificial Intelligence in E-Learning. In Proceedings of the 15th International Scientific and Practical Conference, Environment. Technology. Resources. Rezekne, Latvia, Volume II, pp. 208-211, Print ISSN 1691-5402, Online ISSN 2256-070X, https://doi.org/10.17770/etr2024vol2.8053.
[30] Modi, B., & Gupta, V. (2016). Cryptography with High Throughput: A survey. International journal of innovative research in technology, 2(10), 2349-6002.
[31] Noura, M., Noura, H., Chehab, A., Mansour, M., Couturier, R.: S-DES: An efficient & secure DES variant. In: IEEE Middle East and North Africa Communications Conference (MENACOMM) (2018).
[32] Nurdin, A. A., & Djuniadi, D. (2022). Securing audio chat with cryptool-based twofish algorithm. Journal of Soft Computing Exploration, 3(1), 37-43.
[33] Onete, C. (2008). Visualisation of Modern Key Exchange Schemes for more than two Parties in CrypTool and their Security Analysis.
[34] Pavlov, G., Kolev. Al., A place of GIS technologies in information Systems for crisis prevention, 6th International Conference on Application of Information and Communication Technology and Statistics In Economy and Education (ICAICTSEE – 2016), December 2-3rd, 2016, UNWE, Sofia, Bulgaria, ISSN 2367-7635 (print), ISSN 2367-7643 (online), pp. 452-457.
[35] Qureshi, M. A., Ahmed, S., Mehmood, A., Shaheen, R., & Dildar, M. S. (2024). Vulnerability assessment of operating systems in healthcare: exploitation implications techniques and security. Health Sciences

Journal, 2(2), 104-111, ISSN (Online): 2959-2259, ISSN (Print): 2959-2240, https://doi.org/10.59365/hsj.2(2).2024.98.
[36] Salmi, G. N., & Siagian, F. (2022). Implementation of the data encryption using caesar cipher and vernam cipher methods based on CrypTool2. Journal of Soft Computing Exploration, 3(2), 99-104.
[37] Sharma, N. A., & Farik, M. (2017). A performance test on symmetric encryption algorithms-RC2 Vs rijndael. International Journal of Scientific & Technology Research, 6(7), 292-294.
[38] Simion, E., & Pătrașcu, A. (2020). Applied cryptography and practical scenarios for cyber security defense. Polytech. Univ. Bucharest, Bucharest, Romania, Tech. Rep, 11.
[39] Tiawan, T., Fajari, M. S., Sihombing, R., Syastra, M. T., Novarini, R., Harahap, A. K., ... & Wijayanti, E. K. (2024). Analisis Penggunaan Wsl, VMware, Dan Virtual Box Di Atas Sistem Operasi Windows. Sentinel, 5(1), 409-420, ISSN (print): 2622-1462, doi: 10.56622/sentinel journal.v5i1.39.
[40] Trifonov T., 2019, Modeling and Calculation of Passive Audio Crossovers, Annual of Konstantin Preslavsky University of Shumen, Vol IX E Technical Sciences, ISSN 1311-834X, pp. 182-189.
[41] Trifonov, T., Performance analysis of a mobile computer equipped with solid state disk. Annual of Konstantin Preslavsky University of Shumen, Shumen, Konstantin Preslavsky University Press, ISSN 1311-834X, Vol. IV E, 2014, pp. 27–42.
[42] Weerasinghe, T. D. B. (2014). A Tool to Evaluate Symmetric Key Algorithms. International Journal of Information and Network Security, 3(1), 26.
[43] Winograd, T. CrypTool Number Field Sieve Extensions. Copyright of Baltic Journal of Modern Computing is the property of University of Latvia and its content may not be copied or emailed to multiple sites or posted to a listserv without the copyright holder's express written permission. However, users may print, download, or email articles for individual use.
[44] Wölk, C. M. (2022). Methods To Ensure Privacy Regarding Medical Data--Including an examination of the differential privacy algorithm RAPPOR and its implementation in "Cryptool 2". arXiv preprint arXiv:2210.09963.