Security of Infocommunication Systems and Internet of Things

2023 Vol 1, No 2

https://doi.org/10.31861/sisiot2023.2.02011

Received 28 November 2023; revised 18 December 2023; accepted 29 December 2023; published 30 December 2023

Information Technology and Software for Simulation, Synthesis and Research of Data Crypto Protection Methods

Heorhii Vorobets[1,*], Olexandr Vorobets[1], Ostap Luchyk[1] and Volodymyr Rusyn[2]

[1]Department of Computer Systems and Networks, Yuriy Fedkovich Chernivtsi National University, Chernivtsi, Ukraine
[2]Department of Radio Engineering and Information Security, Yuriy Fedkovich Chernivtsi National University, Chernivtsi, Ukraine

*Corresponding author (E-mail: g.vorobets@chnu.edu.ua)

ABSTRACT The described information technology for improving data protection (ITIDP) in information communication systems (ICS) is built on the basis of a system approach for the implementation of hardware and software solutions for encryption/decryption of data flows in a given continuum of hardware-software-space-time limitations. The formulation of the task for the implementation of ITIDP is substantiated, and a variant of its architecture is proposed. Examples of the development of possible hardware and software modules and resources for the creation of both ITIDP and ICS with increased protection of real-time data flows are given. The issues of choosing methods and means of data encryption in real technical systems and criteria for assessing the necessity and adequacy of encrypted protection of information flows depending on the usefulness and confidentiality of transmitted data are discussed. As a practical approbation of the application of the proposed technology for solving applied problems, examples of the synthesis and research of a special processor for a block cipher with sequential data processing and dynamic key correction, as well as the results of research and optimization of the RSA encryption model for its use in critical application mobile systems with limited hardware and software resources. It is shown that for systems with limited hardware resources in the RSA model of the cipher, it is more correct to use not the Euler function, but the Carmichael function. This approach, together with the use of a modified method of successive approximations according to the rules of modular algebra for calculating large powers of a large base with the subsequent determination of the remainder by a given modulus of a very large number, makes it possible to remove restrictions on the bit rate of data in low-power computers and speed up data decryption processes. The use of modular architecture in the proposed information technology ensures its scalability and quick reconfiguration for the study of various methods of cryptographic data protection.

KEYWORDS information and communication system, stream encryption, block code, RSA code.

I. INTRODUCTION

The modern world is increasingly being formed as a single information and communication society thanks to the introduction of the latest technologies of the Internet of Things (IoT) and cyber-physical systems into all spheres of human activity [1, 2]. However, these processes are accompanied by a significant increase in information flows in technical systems, which, accordingly, requires the search for new and improvement of existing methods, tools, and approaches for data protection in ICS. Currently, there are quite powerful methods of cryptography (DES, RSA, RC4, IDEA, etc.), steganography, coding to protect data in ICS from accidental loss, distortion or blocking of access by intruders [3, 4]. However, the more complex and advanced the protection system is, the more hardware and software resources it needs to process information. This leads to an increase in processing time and obtaining relevant data for system users and does not always guarantee its reliable protection. There are reports of hacking of one of the most secure systems based on RSA encryption [5].

At the same time, there are a number of tasks for which information is relevant within a fairly short period of time after its processing, and the communication system functions in a fairly limited space. This applies, for example, to many production systems of automated data processing and process management, some solutions for the Internet of Things technology, mobile object management systems, etc. There are also specialized technical systems (drones) of one-time use of data or hardware resources, in which the processing time of the digital stream is very limited, and the requirements for ensuring the accuracy of the received data are very high [6]. For the implementation of such systems, it is advisable to use compromise approaches according to the criteria of the ratio of cost and quality of technical solutions. In particular, it is proposed to use modified shortened code structures, systems with dynamic correction of the code key or the length of the coded fragment, specialized processors with a reconfigured computer architecture [6-8].

Implementation of such systems based on modern hardware and software resources, for example, logical environments of FPGA matrices from Altera/Intel, Spartan 3/6 from Xilinx, DE0-Nano-SoC Development Kit hardware platforms with 2-core Cortex-A9 built-in module, Raspberry 3B+, etc. can be effectively simplified by equivalently replacing them with simpler microprocessor elements [9, 10]. To do this, it is necessary

to conduct a thorough analysis of the encryption / decryption task to be solved by the processor system, the algorithms for the implementation of cryptographic methods that will allow to ensure sufficient reliability of the protection of the communication channel and data for the specific task to be solved, as well as to conduct an assessment of the necessary hardware resources and software tools that will allow to implement the necessary algorithms of system functioning. That is, the solution of the described task of analysis and synthesis of a microprocessor system must be carried out for a certain cyberphysical system that functions in a given space of phase states determined by a set (continuum) of limiting parameters *G(f)*: physical parameters of a specific applied task (*AT(p)*) of data management and processing; mathematical algorithms and sets of arithmetic and logical data processing operations for certain cryptographic algorithms (*CA(m)*) and methods; available hardware resources and software (*HR/S(r)*) for the physical implementation of the system. Such an approach can be technologically implemented within the framework of the task of system analysis for the synthesis of an intelligent cyber-physical system, similar to the synthesis of a cryptographic processor with a reconfigurable architecture [10].

Therefore, the purpose of this work was to substantiate the approach for the implementation of information technology analysis and synthesis of hardware and software solutions of the cyber component of information, telemetry, control and other cyber-physical systems with improved protection of information flows during data transmission that function in a given continuum of hardware-software-space-time limitations, determined by the tasks solved by ICS.

II. GENERAL DESCRIPTION OF ITIDP

As a rule, it can be stated that the ICS functions in a certain phase space *G* and can be during the life cycle in a certain set of fixed states *F={f}*. The problem of system analysis, which is generally solved by ITIDP, consists in finding such methods and arrays of *CA(m)* crypto-algorithms, which would, with minimal *HR/S(r)* resources, provide an opportunity to implement ICS for solving a full set of applied tasks of *AT(p)* in the process of implementing a phase ICS trajectories in all states of the phase space *G*.

In the general case, sets of data protection application tasks *P={p; p=x(t,s)}* can have a certain temporal *(t)* and spatial *(s)* distribution (Fig. 1).

Various methods and cryptographic algorithms *CA(m)* from the array *M={m; m=y(t)}*, for the implementation of which different hardware and software resources of *HR/S(r)* in ICS are used at different moments of time *R={r; r=w(t)}*. The set of these factors describes the hardware-software-space-time continuum, within the framework of which the task of system analysis and synthesis of cyber-physical ICS is further considered.

The result of the first stage of ITIDP implementation is the initial data for creating a mathematical, software (*M/P model*) and simulation model (*SM*) for the synthesized ICS: *SM={P, M, R}*, taking into account the full dynamics of the functioning of the real system in the phase space of states.

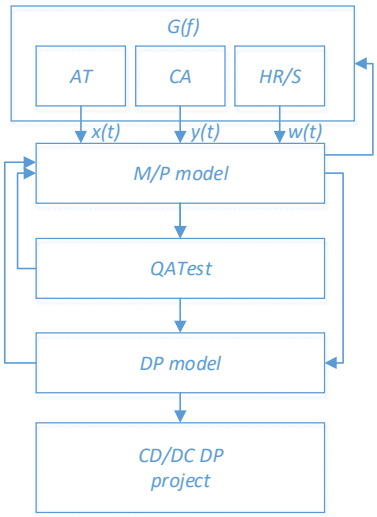


FIG. 1. Stages of implementation of information technology for improving data protection.

The complex model created in the second stage can be improved after testing (*QATest* - the third stage) (Fig. 1). The results of the second and third stages are used to create a hardware and software model (*DP model*) and a sketch project (*CD/DC DP project*) of the cyber component [2] of the cyber-physical ICS aimed at improving the protection of digital data flows during their transmission in the system.

III. TECHNICAL IMPLEMENTATION OF ITIDP

The technical implementation of ITIDP is formed in the form of a complex of software and hardware resources for modeling, analysis, synthesis and research of known and creation of new methods of cryptographic protection of digital data flows in information communication systems. The basis of the complex is a software product (Fig. 2), which allows you to study and simulate the algorithms of the functioning of various cryptography methods (DES, RSA, RC4, IDEA, etc.). Its advantage is the flexibility of setting, scalability with regard to the involvement and synthesis of new cryptography methods, orientation to different formats of data presentation and transmission.

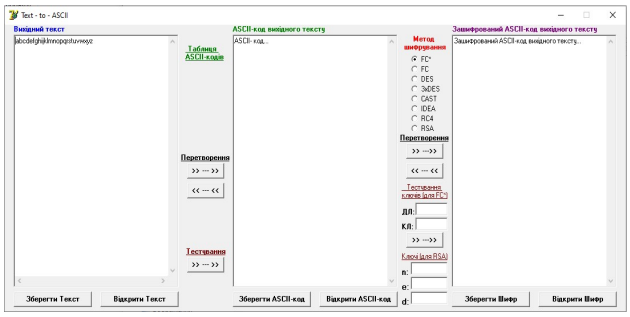


FIG. 2. The main user interface window of the base software product.

The user interface allows you to visualize the data encryption/decryption processes (Fig. 2), at the stage of modeling and researching the correctness of the functioning of crypto-algorithms. The leftmost area loads the input file for encryption. Its ASCII representation is displayed in the central part of the interface, and the encrypted version is displayed on the far right. Between the

central and right areas there is a menu for choosing an encryption method, and certain parameters of the selected cryptocode can also be displayed. Encryption / decryption processes are activated by keys between rendering windows, and when the adjacent window is cleared, they can trigger both left-to-right and right-to-left conversions.

In the lower part of the wreath there are functional keys for loading and saving the results of test processing of files. Both input and encrypted files are stored in clear and ASCII format. This makes it possible to apply modern NIST STS technology at the stage of stability analysis of the studied algorithm. Based on the results of such an analysis, a decision is made about the sufficiency of cryptoresistance of the studied model and the expediency of its use for relevant specialized tasks in the synthesized ICS [11, 12].

Additional specialized software modules are used for a more in-depth study of various modifications of known cryptomethods, or synthesis and analysis of models of new approaches to data encryption/decryption.

Sketch design of software and hardware solutions is implemented on specialized software, depending on the selected ICS technical solution [9, 10]. These are, for example, packages of proprietary software environments for working with programmable logic structures of Altera/Intel, Xilinx, microcontrollers STMxxx, etc.

IV. EXAMPLES OF ITIDP APPLICATION

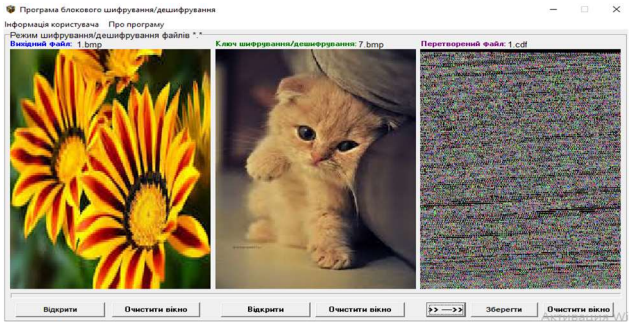
We will show the practical application of ITIDP on the examples of the synthesis of a specialized special processor of block encryption, and the study of the complexity of decryption and cryptoresistance of RSA code for mobile systems.

A. Block cipher with sequential data processing and dynamic key correction (FC code).

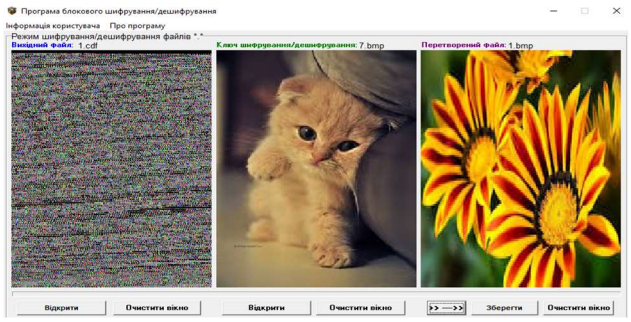
Such an encoder can be relevant for short-periodic data transmission systems in conditions of long-term scanning of communication channels by attackers who use significant computing resources to gain access to confidential data.

As a rule, cryptanalysts in such conditions scan large arrays of information flow to crack the secret key. The idea proposed in [8] consists in the use of short-term communication sessions in each of which a different key is used, and in addition, the key parameters depend on the moment of exchange of session receipts of the data transmitter and receiver and the transmitted content itself. At the moment of creation of the communication channel of the transmitter and receiver, according to their agreement, a trigger key is formed. It is clear that it is random and cannot be calculated by attackers. The modification of the trigger key takes place already with the first block of data received and depends on its content. The value (number of bits) of the next block and the number of cycles of processing new data is already determined by the next received code. In this way, it is practically impossible to determine mathematical or logical regularities during the duration of a communication session. And the next session will already use completely different startup parameters and data encryption.

Inconvenient combinations in such a technique are significant intervals of transmission of zeros or ones. But they are a priori excluded as fixed noise signals that do not carry useful information.

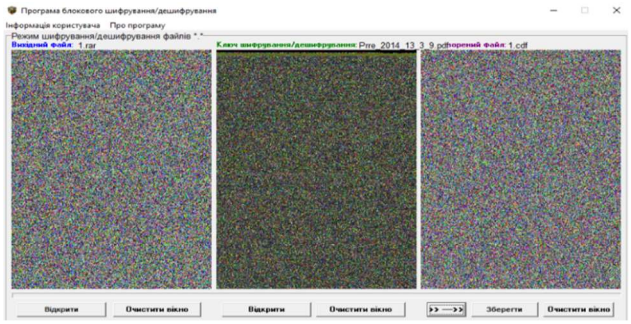


a)

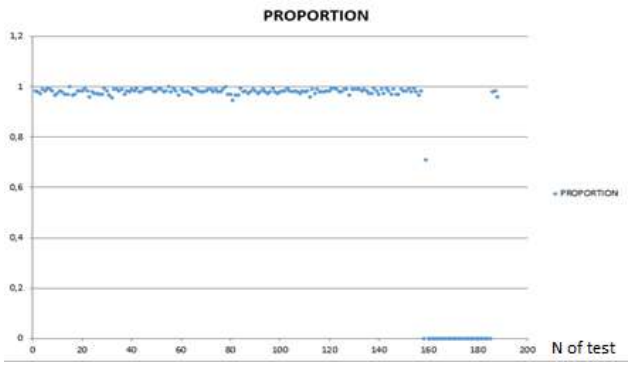


b)

FIG. 3. Encryption (a) and decryption (b) of one *.bmp format image using another "random image".



a)



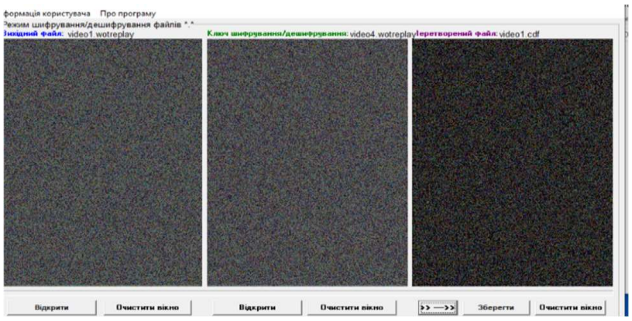
b)

FIG. 4. Results of encryption visualization (a) and statistical studies (b) of *.rar format files.

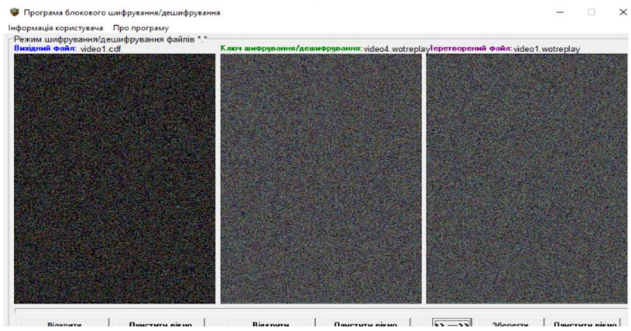
As a modified approach to such encryption, a software and hardware model is synthesized, in which any random file (text, multimedia image, etc.) (FC* code) (Fig. 3) acts as the key. This allows you to implement cascade encoding: at the moment of synchronization, and at the additional file.

Examination of different file types for modified FC* code and plain FC show high statistical parameters by NIST STS metrics. However, for files where additional data synchronization is used (audio, video), NIST STS statistics may show failures for certain groups of tests (Fig. 4 - tests N158-186).

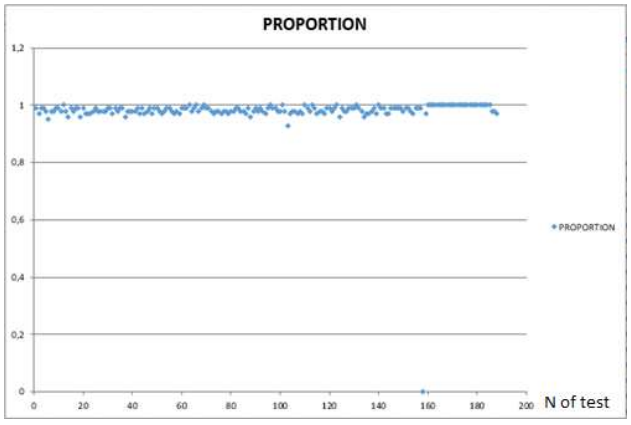
Conversely, in the case of using FC* code to encrypt video files (Fig. 5), almost all the specified tests pass with almost 100 % validation, and only isolated inconsistencies of the ciphergram with the conditions of "pseudo-randomness" of sequences of different lengths of the digital binary code are possible [10-12].



a)



b)



c)

FIG. 5. Visualization results of encryption (a), decryption (b) and statistical studies (c) of video format files.

Another method that was used to check the compliance of the obtained ciphergrams with the conditions of pseudo-randomness of digital sequences was the use of encoding executable files encrypted using the FC / FC* method for their transmission in real data transmission channels. It is known that antivirus programs, network screens (the so-called specialized hardware and software tools firewall, brandmauer) provide reliable filtering and blocking of malicious software in local and global networks. Malicious programs are identified already by service labels of executable files (*.com, *.exe programs). The study of the transmission/reception processes of this type of files encrypted using FC / FC* encoding is confirmed by 100% of their passage through ICS network channels. This may also indicate compliance with the conditions of pseudo-randomness of digital sequences obtained using the proposed FC / FC* technique of pseudo-random change of encryption keys.

The final stages of the implementation of ITIDP and examples of the implementation of a cryptographic special processor based on the Spartan 3 programmable environment of the company Xilinx are quite thoroughly described by us in [8, 10].

B. Study of the RSA encryption algorithm. The RSA encryption method is currently one of the most widely used in practice in a wide variety of fields, and until recently it was considered practically unbreakable [13]. This is confirmed by its use for creating cyphergrams of secret correspondence, forming personalized keys for digital signatures of bank clients, protecting personal data and confidential information in medical information systems, etc. Its feature and main advantage is the use of an asymmetric approach - an open and a private key, which ensures the preservation of secret information even if the value of the open part of the code is known [13].

These advantages are attractive for the use of RSA encryption in mobile systems of critical applications with limited hardware resources and, accordingly, computing capabilities and limitations on the duration of information processing [3, 10]. Such a task requires additional research into the features of encryption/decryption processes in the RSA methodology and the development of improved calculation algorithms.

The essence of the practical implementation of the RSA method in technical systems is the mutually unambiguous correspondence of the results of sequentially performed operations on large prime numbers - exponentiation and calculation of the obtained result according to the given modulus:

$$M^e = C \ (mod\ n), \quad (1)$$

$$C^d = M \ (mod\ n), \quad (2)$$

where M and C are blocks of the digital code of the source information and its encrypted value, respectively; e, d, n – are parameters calculated from a pair (p, q) of two randomly selected prime numbers, which further form open (e, n) and closed (d, n) keys, respectively, for data encryption and decryption [3, 10].

To generate the parameters of the RSA model and to study the reliability and correctness of the transformations, the basic module (Fig. 2) of the ITIDP software was slightly modified and supplemented with an additional module (Fig. 6). The latter allows simulating the RSA code starting from the automatic pseudo-random selection of a pair of (p, q) numbers, determining the parameters $e, d, n,$ calculating the value of the Euler function $\varphi(n)$ for the obtained model parameters, and performing encryption/decryption operations for a given number m [3].

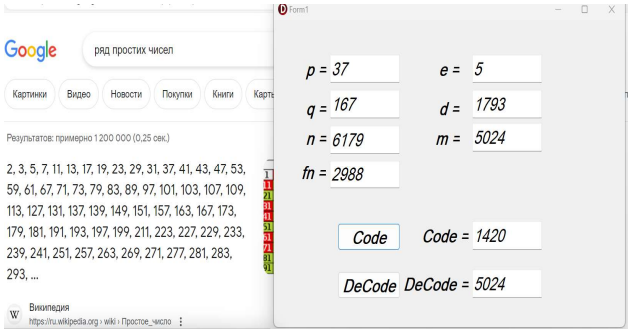


FIG. 6. An additional software module for simulating and studying the features of the RSA code.

A more thorough study of the software model based on its theoretical description and decryption results allows us to state that in order to avoid overflowing the bit grid of the calculator and compact recording of the calculation algorithm in the memory of the special processor of the mobile ICS, instead of the Euler function $\varphi(n)$, it is more appropriate to use the Carmichael function $\lambda(n)$ [13, 14]. The value $\lambda(n)$ is calculated as the least common multiple $\lambda(n)= \lambda(p,q)=lcm(p-1)(q-1)$. It also satisfies the conditions that d and $\varphi(n)$ must be mutually prime, and $d < \varphi(n)$.

In addition, in order to avoid overflowing the bit grid of the special processor when raising a large base to a large power, it is advisable to use a modified method of successive approximations. That is, the calculation of the function {*decode=code(m)^d mod n*} should be implemented by modular algebra transformations. For this, the following steps should be provided in the software model:

1) we determine the coefficients of the binary representation of the private key d using simple transformations:

m2:=d;
k1:=m2 mod 2;
m2:=m2 div 2;
k2:=m2 mod 2;
m2:=m2 div 2;
. . . . . .
k(s-1):=m2 mod 2;
m2:=m2 div 2;
ks:=m2 mod 2;

where m2 is a temporary variable in this transformation, k1÷ks are bit values of the binary representation d.

2) we exclude from the total product for the Hornen formula the transformation of the coded value m2 of the source code m1=m partial products m2(i), for which the bit coefficients k(i)=0:

if k1 = 0 then m2(1):=1;
if k2 = 0 then m2(2):=1;
. . . . . .
if ks = 0 then m2(s):=1.

3) we calculate partial modular products m2(i) (from i=1 to i=s) modulo n; m2(i):=m2(i-1) mod n; for i=0 we assign

m2(0):=code;
m2(1):=code mod n;
m2(2):=(m2(1)*m2(1)) mod n;
m2(3):=(m2(2)*m2(2)) mod n;
. . . . . .
m2(s):=(m2(s-1)*m2(s-1)) mod n.

4) we calculate the value of the total product m2 through the values defined above, which is equivalent to raising the encrypted block represented as an s-bit binary code to the d power:

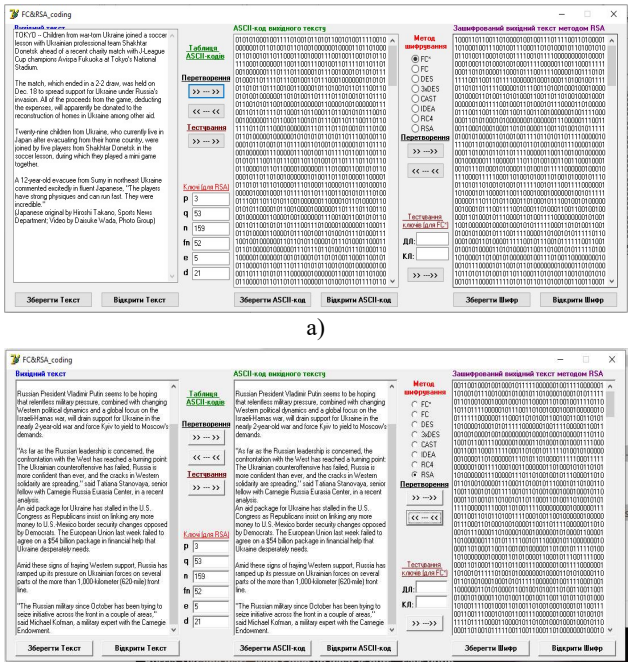
m2:=m2(1)*m2(2)*m2(3)*… *m2(s).

5) we decode the received value of the m2 variable and output the investigated element for verification:

decode:=m2 mod n;
Edit9.Text:=IntToStr(decode).

The received decoded value is recorded in the DeCode window of the additional software module in Fig. 6.

Visualization of the process of encryption / decryption of text files using the RSA method (Fig. 7) allows you to monitor the parameters of the software model during the research process, as well as in the ASCII code window (the central window of the interface (Fig. 7,*a*)) reverse conversion, which is convenient for comparison with input data recorded on the left (Fig. 7,*b*).



a)

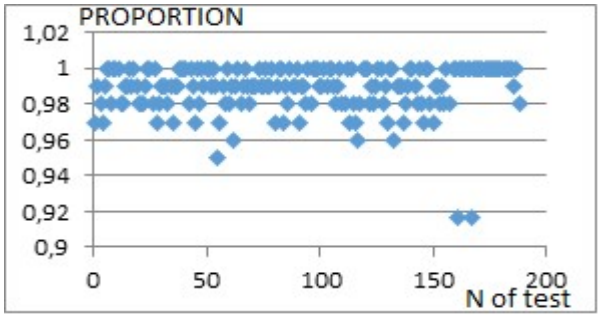
b)

FIG. 7. Visualization of the process of encryption / decryption of text files using the RSA method.

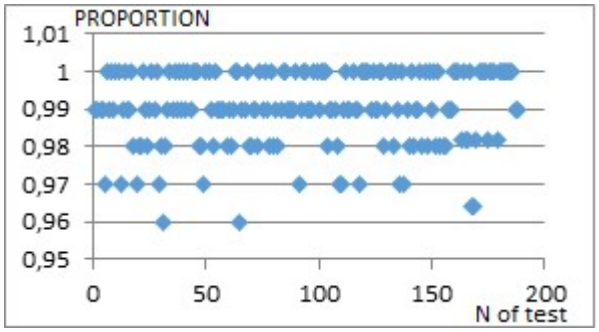
The results of statistical studies of RSA ciphergrams (Fig. 8) show a high level of statistical homogeneity with the prevailing values of the probability distribution above 0.96 for almost all NIST STS tests.

The hardware implementation of mobile ICS using the RSA method of encryption is based on high-speed microcontrollers of the STM32FXXX series. The choice of a specific type of microcontroller is determined by additional requirements regarding the functionality of the designed cyber-physical or information communication system [8, 10, 15].

Thus, the use of ITIDP allows synthesizing, researching and improving data cryptoprotection models, generating cryptographic algorithm keys, determining their compliance with the requirements of the standard based on pseudorandomness parameters, creating hardware and software solutions for mobile and other ICS, including critical infrastructure facilities.



a)



b)

FIG. 8. Results of statistical studies before (a) and after (b) of the text encrypted by the RSA method in the NIST STS package.

By the term "critical infrastructure" in this case, we mean ICS, which are designed to work in conditions of increased exposure to random or artificially generated electromagnetic interference and cyberattacks by attackers. Reliability of communication with system users in such conditions is ensured by the implementation of pseudo-random short-term data reception / transmission sessions, dynamic change of encryption keys of the digital stream, use of one-time keys with mainly passive accumulation of information.

V. CONCLUSION

The proposed approach to the implementation of ITIDP and the concept of its architecture allows in practice to systematize and organize the algorithms of analysis and synthesis of cryptosystems for the protection of data in communication channels and computer networks. The created software shell has the ability to scale according to the set of researched crypto-algorithms, as well as the possibility of including new software modules for their analysis, synthesis and research. ITIDP can be the basis for creating a decision-making support system for improving subsystems of cryptographic protection of data in cyber-physical and information communication systems.

The practical implementation of a special processor for block encryption of data with a dynamic change of the encryption key according to the ITIDP technology demonstrates a good compliance of the proposed encryption method with the requirements of statistical uniformity of the digital stream and allows to reliably encrypt and transmit files of various structures to ICS – text, image, audio and video streams, archive and executable files.

The application of ITIDP to the synthesis of open and hidden keys of the RSA encryption method is promising for the creation of mobile ICS with increased interference resistance, which can be components of critical infrastructure or autonomous systems.

A promising improvement of the proposed approach in ITIDP is the creation of autonomous software modules in basic software shells to check the stability of the studied crypto-algorithms.

ACKNOWLEDGMENT

The results of this work were used in lectures and a laboratory workshop for the master's program "IoT-Technologies for Cyber-Physical Systems", which was created as part of the Erasmus + international project "Internet of Things: New Curricula for Industry and Humanitarian Applications (ALIoT)" No. 573818-EPP -1-2016-1-UKEPPKA2-CBHE-JP in accordance with the European Union grant agreement.

AUTHOR CONTRIBUTIONS

H.V. – conceptualization, methodology, software (together with O.V.), resources, writing-original draft preparation, supervision; O.V. – methodology, software (main part, and together with H.V.) writing-review and editing, visualization; V.R. – writing-review and editing, validation, formal analysis; O.L. – software (together with O.V. and H.V.), resources, investigation, writing-original draft preparation.

COMPETING INTERESTS

This article does not use materials that would lead to competing interests or conflict of interests of the authors with third parties or organizations.

REFERENCES

[1] C. Greer, M. Burns, D. Wollman, E. Griffor. (2019). Cyber-Physical Systems and Internet of Things, Special Publication (NIST SP), National Institute of Standards and Technology, Gaithersburg, MD, [Online]. https://doi.org/10.6028/NIST.SP.1900-202

[2] H. I. Vorobets, O. I. Vorobets, V. E. Horditsa, IoT Technologies for Cyber Physical Systems, PART IV. Chapter 12. CPS and IoT as a Basis of Industry 4.0 / In : Internet of Things for Industry and Human Application. In Volumes 1-3. Volume 1. Fundamentals and Technologies / V. S Kharchenko (ed.) – Ministry of Education and Science of Ukraine, National Aerospace University "KhAI", 2019, 605p., pp. 442-495.

[3] A. Nitaj. The Mathematical Cryptography of the RSA Cryptosystem [Online]. Available: https://nitaj.users.lmno.cnrs.fr/RSAnitaj1.pdf

[4] A. Dutta. "Comparison of Modern Cryptography Methods," Preprints, 2022, 2022070389. doi.org/10.20944/preprints202207.0389.v1

[5] N. Graf zu Castell-Castell, Crashing (shattering) the RSA Code [Online]. Available: https://www.linkedin.com/pulse/crashing-shattering-rsa-code-nikolaus-castell-castell?trk=pulse-article_more-articles_related-content-card

[6] S. Toliupa, S. Shtanenko, T. Poberezhets, V. Lozunov, "Methodology for designing robotic systems based on CADIntel Quartus Prime," Systems and technologies of communication, informatization and cyber security, vol. 2, no. 2, pp. 54-62, 2022.

[7] H. Vorobets, O. Vorobets, V. Horditsa, V. Tarasenko, O. Vorobets, "Self-reconfigurable Cryptographical Coprocessor for Data Streaming Encryption in Tasks of

Telemetry and the Internet of Things," Proceedings of the 9th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS'2017), 21-23 September, 2017, Bucharest, Romania, pp. 1117-1120, 2017, doi: 10.1109/IDAACS.2017.8095259

[8] H. Vorobets, O. Vorobets, V. Horditsa, V. Tarasenko, O. Vorobets, "Features of Synthesis and Statistical Properties of a Modified Stream Encoder with Dynamic Key Correction," Conference Proceedings of 2018 IEEE 9th International Conference on Dependable Systems, Services and Technologies (DESSERT'2018), 24-27 May, 2018, Kyiv, Ukraine, pp. 160-165, doi: 10.1109/DESSERT.2018.8409118

[9] A. V. Palagin, V. M. Opanasenko "Design and Application of the PLD-Based Reconfigurable Devices," Design of Digital Systems and Devices. Series: Lecture Note in Electrical Engineering, vol. 79, pp. 59-91, 2011.

[10] G. I. Vorobets, O. I. Vorobets, V. E. Gorditsa, "Application of the system approach for the synthesis of models of basic elements of reconfigurable structures at the information transmission systems," Electrical engineering and computer systems, vol. 28, no. 104, pp. 257-267, 2018.

[11] A. Rukhin, (2010) A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications. National Institute of Standards and Technology [Online]. Available: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-22r1a.pdf

[12] V. I. Masol, S. V. Popereshnyak, "Checking the Randomness of Bits Disposition in Local Segments of the (0, 1)-Sequence," Cybernetics and Systems Analysis, vol. 56, no. 3, pp. 1-8, 2020, doi: 10.1007/s10559-020-00267-0

[13] Sh. Wang, "A Study of the Use of Euler Totient Function in RSA Cryptosystem and the Future of RSA Cryptosystem," Journal of Physics: Conference Series, vol. 2386, art. no. 012030, doi: 10.1088/1742-6596/2386/1/012030

[14] Cryptography. Why do we need Euler's totient function φ(N) in RSA? [Online]. Available: https://crypto.stackexchange.com/questions/33676/why-do-we-need-eulers-totient-function-varphin-in-rsa

[15] G. I. Vorobets, R. D. Gurzhuy, M. A. Kuz, "A computerized system with a reconfigurable architecture for monitoring environmental parameters," Eastern European journal of advanced technologies, vol. 2, no. 6, pp. 55-59, 2015.

Heorhii Vorobets

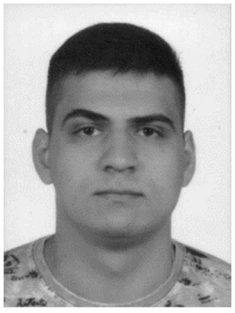
PhD, Associate Professor, Head of the Department of Computer Systems and Networks, Yuriy Fedkovych Chernivtsi National University. 2, Kotsyubynskogo Str., Chernivtsi, Ukraine, 58012. E-mail: g.vorobets@chnu.edu.ua, phone: +38-0372-50-91-73

ORCID ID: 0000-0001-8125-2047

Olexandr Vorobets

PhD, Associate Professor of the Department of Computer Systems and Networks, Yuriy Fedkovych Chernivtsi National University. 2, Kotsyubynskogo Str., Chernivtsi, 58012. Ukraine, E-mail: o.vorobets@chnu.edu.ua, phone: +38-0372-50-91-73

ORCID ID: 0000-0003-3195-8214



Ostap Luchyk

Master Student, Department of Computer Systems and Networks, Yuriy Fedkovych Chernivtsi National University. 2, Kotsyubynskogo Str., Chernivtsi, 58012. Ukraine, E-mail: o.luchyk@chnu.edu.ua, phone: +38-0372-50-91-73

Volodymyr Rusyn

PhD, Assistant Professor of the Department of Radio Engineering and Information Security, Educational and Scientific Institute of Physical, Technical and Computer Sciences, Yuriy Fedkovich Chernivtsi National University, Chernivtsi, Ukraine, E-mail: v.rusyn@chnu.edu.ua, phone: +38-0372-50-94-89

ORCID ID: 0000-0001-6219-1031

Інформаційна технологія і програмне забезпечення для імітаційного моделювання, синтезу і досліджень методів криптографічного захисту даних

Георгій Воробець[1,*], Олександр Воробець[1], Остап Лучик[1], Володимир Русин[2]

[1]Кафедра комп'ютерних систем та мереж, Чернівецький національний університет імені Юрія Федьковича, Чернівці, Україна
[2]Кафедра радіотехніки та інформаційної безпеки, Чернівецький національний університет імені Юрія Федьковича, Чернівці, Україна

*Автор-кореспондент (Електронна адреса: g.vorobets@chnu.edu.ua)

АНОТАЦІЯ Описана інформаційна технологія удосконалення захисту даних (ІТУЗД) в інфокомунікаційних системах (ІКС) побудована на основі системного підходу для реалізації апаратно-програмних рішень шифрування/дешифрування потоків даних у заданому континуумі апаратно-програмно-просторово-часових

обмежень. Обґрунтовано постановку задачі для реалізації ІТУЗД, запропоновано варіант її архітектури. Наведено приклади розробок можливих апаратних і програмних модулів та ресурсів для створення як ІТУЗД, так і ІКС з підвищеним захистом інформаційних потоків даних в реальному часі. Обговорюються питання вибору методів та засобів шифрування даних в реальних технічних системах та критеріїв оцінки необхідності і достатності шифрованого захисту інформаційних потоків у залежності від корисності і конфіденційності трансльованих даних. В якості практичної апробації застосування запропонованої технології для вирішення прикладних задач наведено приклади синтезу і дослідження спецпроцесора для блокового шифратора з послідовною обробкою даних і динамічною корекцією ключа, а також результатів дослідження і оптимізації моделі RSA шифрування для її використання в мобільних системах критичного застосування з обмеженими апаратними і програмними ресурсами. Показано , що для систем з обмеженими апаратними ресурсами в моделі RSA шифратора коректніше використовувати не функцію Ейлера, а функцію Кармайкла. Такий підхід разом з використанням модифікованого методу послідовних наближень за правилами модульної алгебри для обчислення великих степенів великої основи з наступним визначенням залишку за заданим модулем також дуже великого числа дозволяє зняти обмеження на розрядність даних в малопотужних обчислювачах і прискорити процеси дешифрування даних. Використання модульної архітектури в запропонованій інформаційній технології забезпечує її масштабованість і швидке перелаштування для дослідження різних методів криптозахисту даних.

КЛЮЧОВІ СЛОВА інформаційно-комунікаційна система, потокове шифрування, блоковий код, RSA код.