https://doi.org/10.33271/nvngu/2024-1/162

I. Syamsuddin[*1],
orcid.org/0000-0002-6017-7364,
S. Syafaruddin[2],
orcid.org/0000-0002-9915-7694

1 – Politeknik Negeri Ujung Pandang, Makassar, Indonesia
2 – Universitas Hasanuddin, Makassar, Indonesia
[*] Corresponding author e-mail: irfans@poliupg.ac.id

MODELING ARITHMETIC SYSTEMS OF ELLIPTIC CURVE CRYPTOGRAPHY USING MICROSOFT EXCEL VBA

Purpose. This study aims to develop a new teaching module to illustrate the arithmetic systems of Elliptic Curve Cryptography, a powerful yet simple algorithm for information security, by exploring the capability of the Visual Basic Applications of Microsoft Excel in user friendly way.

Methodology. The research is performed using research and development approach, which is divided into five steps utilizing VBA features of Microsoft Excel. It starts with modeling arithmetic in Microsoft Excel spreadsheet, then testing the validity through calculation and setup of the actual arithmetic of Elliptic Curve Cryptography using VBA Excel, before performing the test of the VBA application and finally visualizes the results in graphical mode.

Findings. Novel teaching software based on of Microsoft Excel Visual Basic Applications is produced that is able to simulate arithmetic system behind Elliptic Curve Cryptography in an easy way for students.

Originality. To the best of the authors' knowledge, this is the first simulation based on Excel VBA to illustrate the arithmetic systems of Elliptic Curve Cryptography for teaching purposes.

Practical value. In general, mastering cryptography will need a steep learning curve; however, using Microsoft Excel as a simulation platform will accelerate learning. The main practical value is the ease of Microsoft Excel, which will turn cryptography learning which was commonly very difficult for student to become easier and user friendly.

Keywords: *educational process, elliptic curve cryptography, arithmetic system, Microsoft Excel, Visual Basic Applications*

Introduction. Cryptography is the science of various mathematical techniques to deal with information security issues such as confidentiality, integrity and authentication of data entities [1, 2].

Cryptography concept is based on mathematics solutions perform encryption and decryption. Among powerful cryptographic algorithm developed is called Elliptic Curve Cryptography (ECC), which falls within asymmetric cryptography category [3].

ECC is argued to have equivalent strength to the RSA algorithm in terms of its robustness, but ECC beats RSA in terms of size of key and lower memory or computing requirements [3–5]. Therefore, ECC has been widely applied in many applications since it offers robust and strong security mechanism in protecting the confidentiality of information [5].

Robustness of ECC in real cryptography applications is the main motivation to include ECC as new hands-on practice within the Information Security course at The State Polytechnic of Ujung Pandang. At the moment, there is a gap found in related literature regarding the application of ECC simulator in simple format that can be used as a learning guidance. Considering the user friendliness and simplicity of Microsoft Excel along with its complex features in handling mathematics calculation, we argue its potential as a main tool in this study.

Therefore, the research aims to propose a simple and robust simulation of ECC mechanism in cryptography in order to guide students to attain knowledge about the cryptography processes. In details, the specific objective of the teaching aid simulation is to simulate fundamental mechanism in ECC algorithm called the Arithmetic System as the core concept behind the ECC [6]. This is an important point since to the best of the authors' knowledge, there has been no simulator for this specific objective [7, 8]. Microsoft Excel with Visual Basic Application is selected to realize the simulator considering its simplicity and user friendliness.

The paper is organized as follows. In the second section, framework of the basic theory of ECC is presented along with related research. Section 3 presents the research methodology to conduct the study, which is followed by results and discussion in section 4. Finally, the conclusion is given in section 5.

© Syamsuddin I., Syafaruddin S., 2024

Literature review. Recent survey research by Ullah, et al. [9] reaffirms the role of Elliptic Curve Cryptography in enhancing security in different sectors in the past two decades. They present the way ECC has been used in web applications, mobile applications, IoT applications, cloud applications and many others.

Palaniyappan [10] proposes ECC to deal with the issue of how to create energy efficient WSNs with a higher level of security, which is considered as the most important challenge of real time WSN deployment. Shukla [11] found vulnerability of Smart meter to external attack during data transmission. On the other hand, Smart meter plays an important role to various Internet-of-Things (IoT) applications in smart grid. To deal with the issue, they develop a novel digital signature based on ECC which is proven able to improve security of smart meter [11].

Another application of ECC is in securing MANET environment as presented in [12]. The paper focuses on overcoming the blackhole attack and the wormhole attack, which commonly occur in MANET. Using scalable-dynamic elliptic curve cryptography, the authors exemplify a significant drop of attack in comparison to previous approaches and finally conclude that ECC significantly improve MANET security.

ECC has also been widely implemented in enhancing Smart city security. The security issue of vehicle to vehicle communication in smart city environment is raised in [13]. ECC successfully overcomes various types of messages during exchange attacks with low overhead and latency, while maintaining high reliability.

Smart parking system is another security issue in Smart city environment. To deal with the problem, Chatzigiannakis, et al. [14] develop an IoT elliptic curve based security platform which is aimed at providing a novel privacy-preserving smart parking system.

Recent ECC research to deal with security problems of IoT Smart city is published by Arunkumar, et al. [15]. In their study, Logistic Regression machine learning with the Elliptical Curve Cryptography technique (LRECC) is combined to establish secure IoT based smart cities. ECC is applied to generate and distribute lightweight security keys that minimize the routing overhead, while LR is applied to intelligently select the best route.

Several applications of ECC to secure healthcare information and network have been reported as well. In 2014, an effort to improve IoT based healthcare network was presented by He and Zeadally [16]. In the study, ECC is applied to enhance authentication of RFID used in healthcare network. Then, study by Hureib, et al. [17] found that medical data security could be properly secured by combining ECC into image steganography.

In addition, Kumari, et al. [18] introduce a novel cloud based healthcare information system which is secured by ECC. More recently [19], ECC has been applied to secure Wireless body area networks (WBAN) in health domain which fundamentally requires secure connections and energy efficient systems.

Research methodology. The research methodology is presented in Fig. 1. The process starts with modeling arithmetic and continued testing of the arithmetic system in Microsoft Excel spreadsheet. Once all calculation requirements and manual results are satisfied, then the next step is applying them into Microsoft Excel spreadsheet. In which, all manual procedures previously calculated are transformed into Excel based file and finally develop Graphical User Interface for ECC based on Visual Basic Application of the Microsoft Excel.

Arithmetic on elliptic curve modelling using finite field (Galois Field) and the projective coordinate systems Lopez-Dahab. Galois Field (GF) on the elliptic curve is represented by multiple bits using a normal basis. Pair of points (x, y) and the key value in the Galois Field are used as input data. The output of pair of points (x, y) is then inverted. Values of the inversion result are an encryption value which is in limited field called Galois [8].

Modeling Arithmetic System. Elliptic curves in GF (2 m) is the elliptic curve by a cubic equation as follows

$$y^2 + xy = x^3 + ax^2 + b. \quad (1)$$

With all the coefficients a and b, the variables x and y are members of $GF(2^m)$ and all arithmetic operations used are the arithmetic operations over $GF(2^m)$. At this stage, the key (public key) cryptography required both public key and private key. In the process of encryption or decryption, the public key is used to encrypt the data, while the private key is used to decrypt the data. In this design, only the encryption process is carried out based on the arithmetic models made.

The formula of Massey Omura multiplication can be written on $F2^m$

$$A \cdot B = C = (a_0 a_1 a_2 a_3) \cdot (b_0 b_1 b_2 b_3). \quad (2)$$

Element C is the result of a combination product of rows and columns of A and B. To raise these points in the elliptic

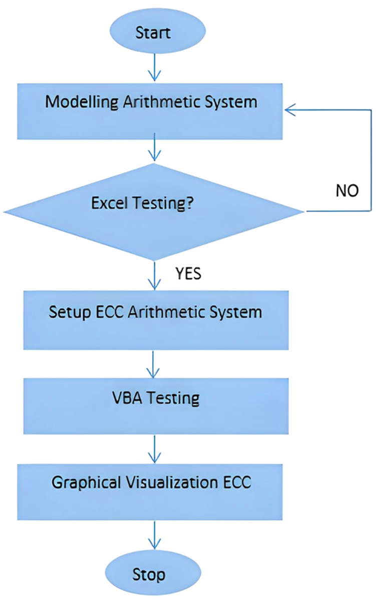

Fig. 1. Flowchart of Design Method

curve, generator (g) is needed. Element g can be determined from the arrangement of bits between 0001-1111 because it uses the normal optimal base F24. Thus, element g will be decisive in the formation of variation of g (Table 1).

Further to the integer s, $1 \le s \le m - 1$, then 2^s of the element g can be easily calculated by shifting 1 bit to the right, as follows g^(2^s) = (a_(m − s), a_(m − s + 1), ..., a_0, a_1, ..., a_(m – s – 1)). This can be verified through g^(2^m) = g [12].

If the results are correct, then continue making software in Visual Basic 6.0 and if it is not correct, re-model arithmetic. Further step is reviewing graphical results of ECC arithmetic in Excel VBA to ensure that the arithmetic system analysis of ECC is correctly visualized.

Results and Discussion. Evaluation of the simulation systems is performed in two stages: first, Spreadsheet test and secondly, Visual Basic Application evaluation. The following parts describe each stage in detail.

First: *Microsoft Excel Spreadsheet Testing*. The procedure of evaluation in this stage is as follows:

1. Determining the value of the key first, for example using $k = 1001$.

2. Determining the equations used on the elliptic curve, i.e. with and. So, the equation is

y^2 + xy = x^3 + ax^2 + ba = 0000b = 0100y^2 + xy = x^3 + b.

3. Determining the value of using dot (presented in Table 1). While used as the z value here only as a multiplier to obtain.x_1,y_1

P = (g^3, g^5) = (0100, 1010)z_1 = 1111(x_3, y_3).

4. Entering the input values in Microsoft Excel to test the encryption process(k,x_1,y_1,z_1,a,b).

The process begins by checking the first bit of the key value. Because [(*k*)]_1 = 1, then the process involves point doubling and point addition. Input is taken from the point addition and point doubling summed with *P*(). (x_3,y_3,z_3) x_1,y_1,z_1 (Fig. 2).

Then, for *k*_2 = 0, only point doubling is performed as seen in Fig. 3. Likewise, for *k*_3 = 0, only point doubling process is conducted (Fig. 4).

Furthermore, for *k*_4 = 1, both point doubling and point addition processes are required as depicted in Fig. 5.

After all the key bits are processed, then the values of.x_3, y_3, z_3 = (0100,1010,0010) are obtained.

In order to prove that the output values are exactly in the elliptic curve, the inversion process is carried out using Itoh-Tsujii method with the value of z3. The results obtained are multiplication and inversion of z^(−1), z_(3), x_3, z_3, y_3 and z^(−2) (Fig. 6).

Inversion results *x, y* = (0001,1001) are then associated to Table, which result in 25*P* = g^12, g^8 which clearly indicates the value is within elliptic curve.

Second: *Visual Basic Application Testing*. The main graphical user interface (GUI) of the ECC simulator is shown in Fig. 7. It consists of four menus, Enkripsi 4bit, Help, About and Exit. All ECC arithmetic system simulations are accessible through Enkripsi menu, while Help menu provides guidance to students on how to perform the simulation.

Selecting Enkripsi menu will show a Form Encryption. The value of a and b in the equation is predetermined, so that each form load value is already filled (Fig. 8). To perform the encryption, the key value and the value of the data are inputted to each textbox as seen in Fig. 9. After clicking the arithmetic process (Fig. 10), the point doubling and point addition will produce values based on the key value inputted (x_3, y_3).

Fig. 11 shows the inversion process. The value is obtained by shifting 1 bit to the left and multiplication by Massey Omura, thus obtained value z_3 = *AB, C,C*_2 z^(−1). If the result of this encryption is equal to one in Table 1, then encryption results can be presented correctly as shown in Fig. 12. If the val-

Table

Multiplication Scalar Elliptic Curve Point E (F24)

$1P = (g^3, g^5)$	$2P = (g^4, g^3)$	$3P = (g^{13}, g^2)$	$4P = (g, 0)$	$5P = (g^{12}, g^8)$
$6P = (g^8, g^3)$	$7P = (g^{11}, g^0)$	$8P = (g^5, g^{11})$	$9P = (g^6, 0)$	$10P = (g^0, g^9)$
$11P = (g^6, g^6)$	$12P = (g^5, g^3)$	$13P = (g^{11}, g^{11})$	$14P = (g^8, g^{13})$	$15P = (g^{12}, g^9)$
$16P = (g, g)$	$17P = (g^{13}, g^{14})$	$18P = (g^4, g^7)$	$19P = (g^3, g^{11})$	$20P = (0)$

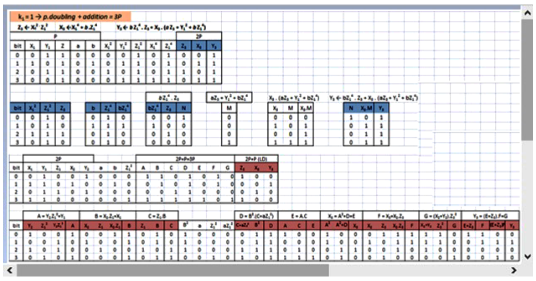

Fig. 2. Calculation Process for k_1 = 1

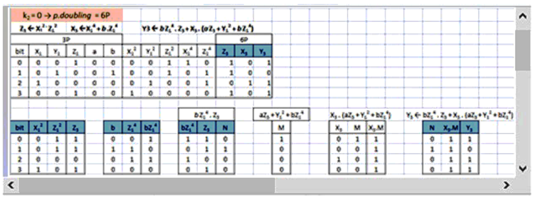

Fig. 3. Calculation Process for k_2 = 0

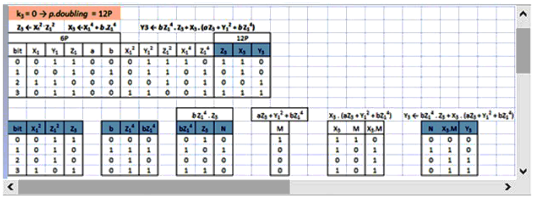

Fig. 4. Calculation Process for k_3 = 0

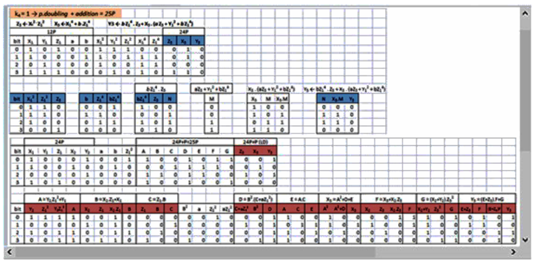

Fig. 5. Calculation Process for k_4 = 0

Fig. 6. Calculation process of Itoh-Tsujii using Bit Key 1001Kadbad

ues obtained from the simulation is not within the curve, then here will be no results appearing there.

Third: *Visualization of ECC.* Visualization of ECC is the ultimate objective of the study. Fig. 13 represents final simulation of ECC by visualizing all points based Weierstrass equation.

Conclusions. In accordance with the objective of this study, we have successfully presented a new approach in teaching El-

Fig. 7. GUI of the ECC simulator

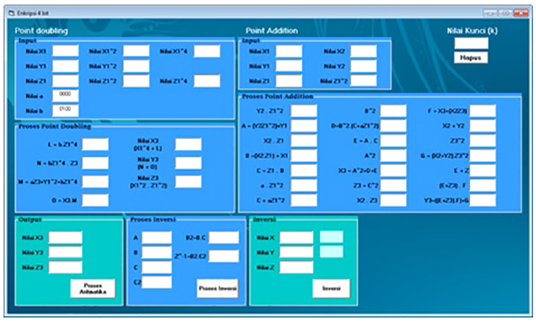

Fig. 8. Form 4 Bit Encryption

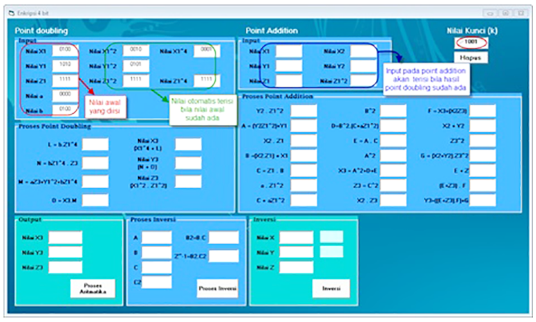

Fig. 9. Input Data Values

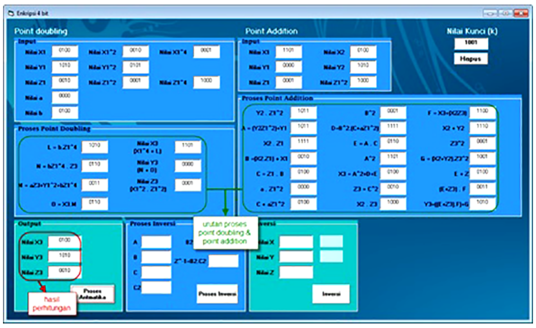

Fig. 10. Results of Calculation Process

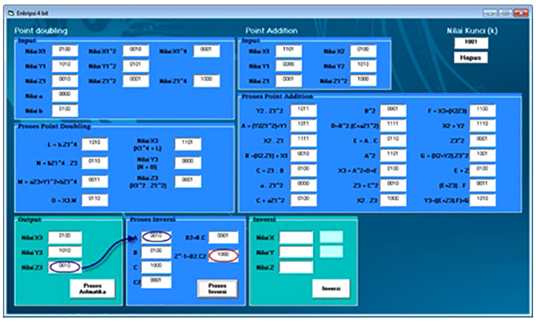

Fig. 11. Inversion Process

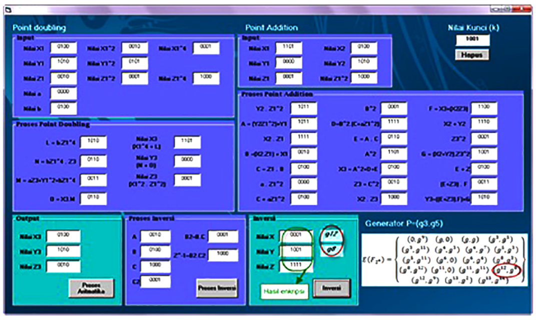

Fig. 12. Encryption result

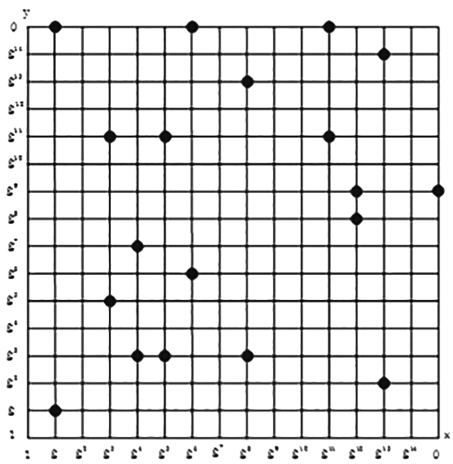

Fig. 13. Simulation result of Graph Elliptic Curve

liptic Curve Cryptography (ECC) through developing a novel simulation of Arithmetic System behind the ECC algorithm. The use of Microsoft Excel powered by Visual Basic Application is proposed to enhance the simulation for teaching purposes. The ECC simulation successfully shows the whole processes of Arithmetic System of ECC and also illustrates all points of ECC in graphical view.

In the future, the study will be extended to analyze its effectiveness of its use in class from lecturer and student perspectives as suggested in [20].

Acknowledgement. *The authors express their gratitude to the CAIR Center for Applied ICT Research (Politeknik Negeri Ujung Pandang) for technical supports.*

References.

1. Furnell, S., & Bishop, M. (2020). Addressing cyber security skills: the spectrum, not the silo. *Computer Fraud & Security, 2020*(2), 6-11. https://doi.org/10.1016/s1361-3723(20)30017-8.

2. Buchanan, W. J., Li, S., & Asif, R. (2017). Lightweight cryptography methods. *Journal of Cyber Security Technology, 1*(3-4), 187-201. https://doi.org/10.1080/23742917.2017.1384917.

3. Varma, C. (2018). A study of the ECC, RSA and the diffie-Hellman algorithms in network security. *2018 International Conference on Current Trends towards Converging Technologies (ICCTCT)*. IEEE. https://doi.org/10.1109/ICCTCT.2018.8551161.

4. Mallouli, F., Hellal, A., Sharief Saeed, N., & Abdulraheem Alzahrani, F. (2019). A survey on cryptography: Comparative study between RSA vs ECC algorithms, and RSA vs El-Gamal algorithms. *2019 6th IEEE International Conference on Cyber Security and Cloud Computing (CSCloud)/2019 5th IEEE International Conference on Edge Computing and Scalable Cloud (EdgeCom)*. IEEE. https://doi.org/10.1109/CS-Cloud/EdgeCom.2019.00022.

5. Bafandehkar, M., Yasin, S. M., Mahmod, R., & Hanapi, Z. M. (2013, December). Comparison of ECC and RSA algorithm in resource constrained devices. In *2013 international conference on IT convergence and security* (*ICITCS*), (pp. 1-3). IEEE. https://doi.org/10.1109/ICITCS.2013.6717816.

6. Hankerson, D. (2004). *Guide to Elliptic Curve Cryptography*. New York: Springer-Verlag. https://doi.org/10.1007/b97644.

7. Sen (2017). Implementing elliptic curve cryptography using Microsoft excel. *Issues In Information Systems, 18*(2), 103-112. https://doi.org/10.48009/2_iis_2017_103-112.

8. Islam, M. M., Hossain, M. S., Hasan, M. K., Shahjalal, M., & Jang, Y. M. (2019). FPGA implementation of high-speed area-efficient processor for elliptic curve point multiplication over prime field. *IEEE Access, 7*, 178811-178826.

9. Ullah, S., Zheng, J., Din, N., Hussain, M. T., Ullah, F., & Yousaf, M. (2023). Elliptic Curve Cryptography; Applications, challenges, recent advances, and future trends: A comprehensive survey. *Computer Science Review, 47*(100530), 100530. https://doi.org/10.1016/j.cosrev.2022.100530.

10. Palaniyappan, K., & Suresh, D. (2021). An Efficient Cluster Based Secure Packet Transmission Using Improved Polynomial Based Elliptical Curve Cryptography in Wireless Sensor Networks. *Journal of Computational and Theoretical Nanoscience, 18*(3), 796-804. https://doi.org/10.1166/jctn.2021.9673.

11. Shukla, S., Thakur, S., & Breslin, J. G. (2021). Secure communication in smart meters using elliptic curve cryptography and digital signature algorithm. *2021 IEEE International Conference on Cyber Security and Resilience* (*CSR*). IEEE. https://doi.org/10.1109/CSR51186.2021.9527947.

12. Shukla, M., Joshi, B. K., & Singh, U. (2021). Mitigate wormhole attack and blackhole attack using elliptic curve cryptography in MANET. *Wireless Personal Communications, 121*(1), 503-526. https://doi.org/10.1007/s11277-021-08647-1.

13. Dua, A., Kumar, N., Singh, M., Obaidat, M. S., & Hsiao, K.-F. (2016). Secure message communication among vehicles using elliptic curve cryptography in smart cities. *2016 International Conference on Computer, Information and Telecommunication Systems (CITS)*. IEEE. https://doi.org/10.1109/CITS.2016.7546385.

14. Chatzigiannakis, I., Vitaletti, A., & Pyrgelis, A. (2016). A privacy-preserving smart parking system using an IoT elliptic curve based security platform. *Computer Communications, 89-90*, 165-177. https://doi.org/10.1016/j.comcom.2016.03.014.

15. Arunkumar, R., Velmurugan, S., Chinnaiah, B., Charulatha, G., Prabhu, M. R., & Chakkaravarthy, A. P. (2023). Logistic Regression with Elliptical Curve Cryptography to Establish Secure IoT. *Computer Systems Science & Engineering, 46*(1). https://doi.org/10.32604/csse.2023.031605.

16. He, D., & Zeadally, S. (2015). An analysis of RFID authentication schemes for internet of things in healthcare environment using elliptic curve cryptography. *IEEE Internet of Things Journal, 2*(1), 72-83. https://doi.org/10.1109/jiot.2014.2360121.

17. Christo, M. S., Jesi, V. E., Priyadarsini, U., Anbarasu, V., Venugopal, H., & Karuppiah, M. (2021). Ensuring improved security in medical data using ECC and blockchain technology with edge devices. *Security and Communication Networks, 2021*, 1-13. https://doi.org/10.1155/2021/6966206.

18. Kumari, A., Kumar, V., Abbasi, M. Y., Kumari, S., Chaudhary, P., & Chen, C.-M. (2020). CSEF: Cloud-based secure and efficient framework for smart medical system using ECC. *IEEE Access: Practical Innovations, Open Solutions, 8*, 107838-107852. https://doi.org/10.1109/access.2020.3001152.

19. Azath, H., Gokulraj, J., Surendiran, J., Geetha, D., & Babu, T. R. G. (2023). Security for health information by elliptical curve Diffie-Hellman and improve energy efficiency in WBAN. *AIP Conference Proceedings*. AIP Publishing. https://doi.org/10.1063/5.0110677.

20. Syamsuddin, I. (2018). Evaluation of NgeXTEA: A cryptography learning module. *Global Journal of Engineering Education, 20*(3), 196-200. https://doi.org/10.5281/zenodo.2539847.

Моделювання арифметичних систем еліптичної криптографії з використанням програми Microsoft Excel VBA

І. Сіамсуддін[*1], *С. Сіафаруддін*[2]

1 – Політехнічний інститут Уджунг Панданг, м. Макассар, Індонезія

2 – Університет Хасануддіна, м. Макассар, Індонезія

[*] Автор-кореспондент e-mail: irfans@poliupg.ac.id

Мета. Дане дослідження має на меті розробку нового навчального модуля для ілюстрації арифметичних систем еліптичної криптографії, потужного, але простого алгоритму для забезпечення інформаційної безпеки шляхом вивчення можливостей застосунків Visual Basic у Microsoft Excel у зручний спосіб для користувача.

Методика. Дослідження виконується за допомогою підходу до дослідження й розробки, що ділиться на п'ять етапів, із використанням можливостей VBA у Microsoft Excel. Він починається з моделювання арифметики в таблиці Microsoft Excel, а потім перевіряється його валідність шляхом обчислення та встановлення фактичної арифметики еліптичної криптографії з використанням VBA Excel. Далі виконується тестування застосунку VBA, а на останньому етапі результати візуалізуються у графічному режимі.

Результати. Створено нове навчальне програмне забезпечення на основі застосунків Visual Basic для Microsoft Excel, що може моделювати арифметичну систему за еліптичною криптографією у простий спосіб для студентів.

Наукова новизна. Наскільки відомо авторам, це перше моделювання на основі Excel VBA, призначене для ілюстрації арифметичних систем еліптичної криптографії для навчальних цілей.

Практична значимість. Загалом, оволодіння криптографією вимагатиме дуже швидкого освоєння нової технології, однак використання Microsoft Excel як платформи для моделювання прискорить цей процес навчання. Основною практичною цінністю є простота використання Microsoft Excel, яка зробить вивчення криптографії, що традиційно була дуже складною для студентів, більш простою та зручною для користувачів.

Ключові слова: *навчальний процес, еліптична криптографія, арифметична система, Microsoft Excel, застосунки Visual Basic*

The manuscript was submitted 23.02.23.