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 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

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

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

162 ISSN 2071-2227, E-ISSN 2223-2362, Naukovyi Visnyk Natsionalnoho Hirnychoho Universytetu, 2024, № 1
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 can 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 output of pair of points (x_1,y_1,z_1). The main graphi
cal user interface (GUI) of the ECC simulator is shown in Fig. 9. Likewise, for k = 0, only point doubling is performed as seen in Fig. 3. Further, for k = 0, only point doubling process is conducted (Fig. 4).

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 generator (g). 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 ≤ s ≤ m − 1, then 2^s of the element g can be easily calculated by shifting 1 bit to the right, as follows g^s = (a_0, a_1, a_2, a_3, a_4, a_5, …, a_m). This can be verified through g^s = g^s = 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 + b = 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 = 1111(x_3, y_3).
4. Entering the input values in Microsoft Excel to test the encryption process(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)

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

Furthermore, for k = 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 z^3. The results obtained are multiplication and inversion of z’(−1), z(3), x, y and z’(−2) (Fig. 6).

Inversion results x, y = (0001,0001) are then associated to Table, which result in 25P = 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. 1 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-

\[
A \cdot B = C = (a_0,a_1,a_2,a_3) \cdot (b_0,b_1,b_2,b_3). \tag{2}
\]

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

<table>
<thead>
<tr>
<th>Multiplication Scalar Elliptic Curve Point E (F24)</th>
</tr>
</thead>
<tbody>
<tr>
<td>$1P = (g^3, g^2)$</td>
</tr>
<tr>
<td>$2P = (g^2, g^5)$</td>
</tr>
<tr>
<td>$3P = (g^3, g^4)$</td>
</tr>
<tr>
<td>$4P = (g, 0)$</td>
</tr>
<tr>
<td>$5P = (g^{11}, g^{8})$</td>
</tr>
<tr>
<td>$6P = (g^{3}, g^{2})$</td>
</tr>
<tr>
<td>$7P = (g^{3}, g^{3})$</td>
</tr>
<tr>
<td>$8P = (g^4, g^{11})$</td>
</tr>
<tr>
<td>$9P = (g^4, 0)$</td>
</tr>
<tr>
<td>$10P = (g^{12}, g^{3})$</td>
</tr>
<tr>
<td>$11P = (g^8, g^6)$</td>
</tr>
<tr>
<td>$12P = (g^{3}, g^3)$</td>
</tr>
<tr>
<td>$13P = (g^{3}, g^{11})$</td>
</tr>
<tr>
<td>$14P = (g^4, g^{11})$</td>
</tr>
<tr>
<td>$15P = (g^{12}, g^{3})$</td>
</tr>
<tr>
<td>$16P = (g, g)$</td>
</tr>
<tr>
<td>$17P = (g^{3}, g^{14})$</td>
</tr>
<tr>
<td>$18P = (g^4, g^{7})$</td>
</tr>
<tr>
<td>$19P = (g^{3}, g^{11})$</td>
</tr>
<tr>
<td>$20P = (0)$</td>
</tr>
</tbody>
</table>

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-
elliptic 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.


Моделювання арифметичних систем еліптичної криптографії з використанням програми Microsoft Excel VBA

І. Сіамсусудін*1, С. Сіафаруддін2
1 – Політехнічний інститут Уджунг Панданг, м. Макасар, 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 застосування 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 застосувань Visual Basic для Microsoft Excel, що може моделювати арифметичну систему еліптичної криптографії 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 вимагає дуже швидкого освоєння нової технології, однак використання Microsoft Excel як платформи для моделювання прискорить цей процес навчання. Основною практикою 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.