Sistema de Criptografía Simétrico para la Enseñanza de las Matrices Inversas Modulares
Symmetric Cryptography System for Teaching Modular Inverse Matrices

Fausto Abraham Jacques García [1], Sandra Luz Canchola Magdaleno [2] and Gloria Nelida Avecilla Ramírez [3]

[1] Facultad de Informática de la Universidad Autónoma de Querétaro, Av. de las Ciencias s/n, Juriquilla, Santiago de Querétaro, Qro., 76230. México
jacques@uaq.edu.mx
[2] Facultad de Informática de la Universidad Autónoma de Querétaro, Av. de las Ciencias s/n, Juriquilla, Santiago de Querétaro, Qro., 76230. México
sandra.canchola@uaq.mx
[3] Facultad de Psicología de la Universidad Autónoma de Querétaro, Cerro de las campanas s/n, Las Campanas, Santiago de Querétaro, Qro., 76010. México
gloria.avecilla@uaq.mx

Fecha de recepción: 18 de septiembre 2016
Fecha de aceptación: 10 de diciembre 2016

Resumen. El presente artículo describe la enseñanza de las matrices inversas modulares usando el algoritmo de criptografía simétrica Hill Cipher y su implementación en dispositivos móviles con Sistema operativo Android. El proceso de descifrado en el algoritmo Hill Cipher involucra el cálculo de matrices inversas modulares. El objetivo de este trabajo es la enseñanza del cálculo necesario para la obtención de matrices inversas modulares a estudiantes de licenciatura en las áreas de las ciencias computacionales a través del proceso de descifrado en la criptografía simétrica. Se realizó un experimento con dos grupos de estudiantes, el grupo experimental y el grupo de control. Se aplicó una prueba en ambos grupos para determinar el aprendizaje de los estudiantes. Un análisis comparativo entre ambos grupos muestra un incremento en el desempeño del grupo experimental en el cálculo de las matrices inversas modulares.

Palabras clave: Criptografía Simétrica, Hill Cipher, Matrices Inversas, Dispositivos Móviles.

Abstract. This article describes the teaching of modular inverse matrices with the symmetric cryptographic algorithm Hill Cipher and its implementation on mobile devices with Android Operative System. The decryption in the Hill Cipher algorithm involves the calculus of modular inverse matrices. The goal of this paper is the teaching of modular inverse matrix calculation to undergraduate students of Computer Sciences through the decryption in symmetric cryptography. An experiment was conducted on two groups of students, the control and the experimental groups. To measure student learning, a test was applied to both groups. Comparison of control and experimental groups results show an increase in student performance for the calculation of modular inverse matrices.

Keywords: Symmetric Cryptography, Hill Cipher, Inverse matrices, Mobile devices.

1 Introduction

Mathematics is conceived as reasoning from concepts and the problem of mathematical education is not just rigor or logical objectivity, but meaningfulness. All deductive reasoning involves an element of observation. Deduction consists in constructing the relations of whose parts shall present a complete analogy with those of the parts of the object of reasoning and of observing the result so as to discover unnoticed and hidden relations among the parts [1]. Studying modular inverse matrices solving and the basic operations involved in the process, the abstract concepts can be materialized in real computer science applications such as cryptography. This would facilitate modular inverse matrices learning. Many different approaches have been used for studying contextualized mathematics. In recent years a 32 bit symmetric cryptographic algorithm was implemented in a software system to undergraduate students to motivate them in the learning of discrete mathematics, code correcting errors, coding theory, number theory and finite field theory, as can be seen in [2]. The result was the fact that undergraduate students understood basic concepts of computer security and they showed motivation in learning mathematics. In addition, it can be seen in [3] that the Hill Cipher Cryptosystem was implemented in a computer software system to teach linear transformations and to teach the importance of eigenvectors. The author of the project observed that undergraduate students were very interested in learning more and they showed better learning results and better understanding of eigenvectors and linear spaces.

The use of mobile devices have become common among a wide range of age groups due to affordability and availability [4]. Mobile devices can be used for educational purposes. As can be seen in [5], in recent years, technology-enhanced learning research has increasingly focused on emergent technologies such as augmented

reality, ubiquitous learning, mobile learning, serious games, and learning analytics for improving the satisfaction and experience of the users in enriched multimodal learning environments.

2 State of the Art

2.1 The technology as a mediation instrument

According to [6], an instrument is part of the non-natural world produced by human culture. The instrument is not only an object with a specific form and determined physical properties. It is above all a social object whose use modalities are elaborated during collective work. It is a bearer of work operations that are crystallized in it. The instrument can be defined in terms of its action and activity.

There are three poles in instrument utilization situations: a) The subject, b) The instrument and c) The object. The subject is an actor who interacts with the instrument. It can be a user, an operator, a worker, an agent or a student. The instrument is the mediation tool. It can be a computer, a mobile device, a system, a utensil or a product. The object is directed toward the action aided by the instrument. There is a triad model that brings out the complexity and multiplicity of relations and interactions between the different poles as shown in Fig. 1, unlike the usual bipolar models of subject-object interaction situations.

Beyond direct subject-object interactions (dS-O), so many other interactions must be considered: interactions between the subject and the instrument (S-I), interactions between the instrument and the object on which it allows to act (I-O), and finally subject-object interactions mediated by an instrument (S-Om). These interactions are thrown into an environment made up of all the conditions that the subject must take into consideration in his finalized activity. As mentioned above, each of the poles and each of the interactions are themselves liable to be in interaction with the environment thus defined.

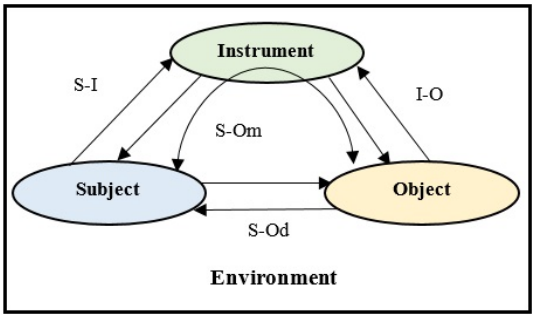

Fig. 1. Subject mediated by instrument.

2.2 Cryptography

According to [7], cryptography is probably the most important aspect of security in communications, and is becoming a cornerstone in computer science. Cryptography comes from the greek Krypto (κρυπτός) meaning "hide," and Graphos (γράφειν) meaning "writing," so that cryptography is the secret writing. Cryptography has three aspects: a) Symmetrical, b) Public Key, and c) Hash Algorithms.

Symmetric cryptography is a form of cryptosystem in which the process of encrypting and decrypting can be done using the same key or a transformation thereof. This cryptosystem transforms plaintext (original text) into ciphertext (encrypted) using a secret key and an encryption algorithm. Using the same key or a transformation thereof and the corresponding algorithm to decrypt, the plaintext can be retrieved as shown in Fig. 2.

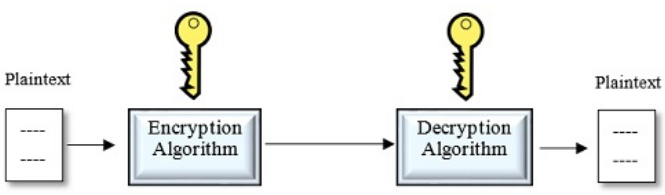

Fig. 2. Symmetric Encryption.

2.3 Hill Cipher

Hill Cipher is an algorithm created by the mathematician Lester Hill. According to [7], this algorithm takes m successive plaintext characters and replaces them with m cipher characters. Such replacement is made using m linear equations in which each character is assigned a value i.e., a = 0, b = 1, …, z = 25. If m = 3, the system can be expressed as follows:

$$c1 = (k_{11}p_1 + k_{12}p_2 + k_{13}p_3) \bmod n \quad (1)$$
$$c2 = (k_{21}p_1 + k_{22}p_2 + k_{23}p_3) \bmod n \quad (2)$$
$$c3 = (k_{31}p_1 + k_{32}p_2 + k_{33}p_3) \bmod n \quad (3)$$

Also represented as:

$$C = E\,(KP) \bmod n \quad (4)$$

Letters C and P denote 3 rows and 1 column vectors (3 x 1). The ciphertext is denoted by C and the plaintext is P. The key to encrypt is denoted by K in (6) and it is a square matrix composed by 3 rows and 3 columns (3 x 3). It can be seen that modular operations represented by n are taking place, which is given a value according to the number of symbols considered for the encrypt-decrypt process. To decrypt we use the following modular linear equation:

$$P = D\,(K^{-1}C) \bmod n \quad (5)$$

In (5) K^{-1} denotes the modular inverse of the key matrix K. As a testing method the product of the key and its transformations are equal to the identity matrix as follows:

$$(KK^{-1}) \bmod n = (K^{-1}K) \bmod n = I \quad (6)$$

Identity matrix or unit matrix in (6) is the n x n square matrix with ones in the main diagonal and zeros elsewhere. It is denoted by I in (6). As can be seen in [8], a modular inverse matrix can be obtained using modular operations by two ways: a) Using determinants and the adjunct of a matrix, and b) Using Gauss-Jordan method. The determinant is a function that assigns a number to a square matrix, which is equals to the sum of all products that can be formed by taking exactly one element from each row and one element from each column and performing subtraction product terms. There is the Gauss-Jordan method that consists of performing elementary operations on the rows, so that the matrix can be increased with the identity matrix as follows:

$$(A \mid I) \sim (I \mid A^{-1}) \quad (7)$$

3 Methodology Used

This study was designed to answer the following research question: How does symmetric cryptography implemented in mobile technology affect the learning of modular inverse matrix calculation? This study is based on action research methodology. The goal is to enable students to calculate de modular inverse matrix.

This study was conducted in a linear algebra course in the Computer Science School at the Autonomous University of Queretaro, Mexico. A total of 44 undergraduate students were enrolled in two groups to take the same course. Student ages ranged from 17 to 24 years old. There were 3 females and 19 males in the control group, and 2 females and 20 males in the experimental group. The two hour class met twice weekly. The lectures covered 76 hours, of which 12 were dedicated to covering concepts and exercises required for the study of modular inverse matrices. A test was administered to 22 students of the control group after the 12 hours described. The same test was administrated to 22 students of the experimental group after the 12 hours and the teaching of the Hill Cipher cryptosystem in the classroom and after the experiment described below.

3.1 Hill Cipher implementation

It was intended to decrypt the cipher text using a modular inverse matrix calculated by hand. The process by which the experiment was conducted to the experimental group consists of six chronological steps described below:

The first step was the programming of the Hill Cipher cryptosystem in Java language with the Android SDK. The eclipse IDE was used. The application development lasted two months. Once the application was developed, it was proceeded to the second step. The second step was the teaching in the classroom of the modular inverse matrix calculation to obtain a matrix with integer and positive values. This matrix can be used de decrypt a cipher text. The teaching of these topics lasted 12 hours. In the third step, the Hill Cipher cryptosystem was taught in the classroom. Then, participants were asked to install the developed application. They were also asked to calculate the modular inverse matrices for each modulo and matrix size and type them in the application so it could decrypt the cipher text. Students calculated the modular inverse matrix for 2 x 2 and 3 x 3 square matrices with modulo 26, 28 and 29. In step four, students were asked to take the test mentioned before. In step five, test results were analysed to evaluate modular inverse matrix calculation. The last step was to generate conclusions of the experiment performed.

Modular arithmetic was considered with 26, 28, and 29 values. This means that the character system used is formed by 26, 28, and 29 letters or symbols which are defined by the user, depending the alphabet that is considered. For example, working with modulo 26, we have this sequence of values: A = 0, B = 1, C = 2, …, Z = 25.

3.2 Procedure

Below the activity made by students is presented. Students had to calculate the modular inverse matrix to decrypt the cipher text. The encrypted text was “UNIVERSIDAD AUTONOMA DE QUERETARO.” Fig. 3 shows the encryption-decryption process using a 3 x 3 square matrix with modulo 26.

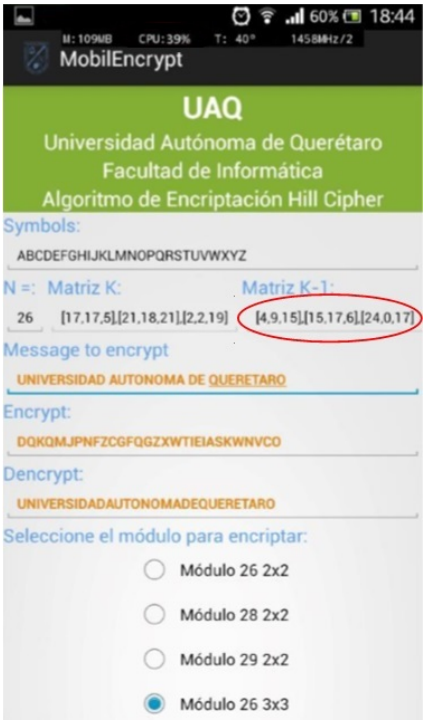

Fig. 3. 3 x 3 square matrix with modulo 26.

It can be observed the modular inverse matrix to decrypt the cipher text given by the user. This matrix has nine positive and integer values. If the matrix was correct, the application would decrypt the cipher text successfully. The students had to calculate the modular inverse matrix using modulo 26 in this case, but in general, the students of the experimental group calculated six modular inverse matrices, three 2 x 2 matrices with modulo 26, 28, and 29, and three 3 x 3 matrices with same modulo.

4 Experimental Results

This section describes the findings of the study. Research question: How does symmetric cryptography implemented in mobile technology affect the learning of modular inverse matrix calculation? In this section, the results obtained from the implementation of the software developed on the linear algebra undergraduate course are presented and analyzed. As mentioned before, we worked with two groups, a control group, and an experimental group. In both groups a test based on [8] was applied. The test, described in Table 1, consisted of two 4 x 4 square matrices. Students had 120 minutes to calculate the two modular inverse matrices. Students could use any of the two methods described before.

Exercise	Matrix
1	$\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 2 & -1 & 2 \\ 1 & -1 & 2 & 1 \\ 1 & 3 & 3 & 2 \end{pmatrix}$
2	$\begin{pmatrix} 1 & -3 & 0 & -2 \\ 3 & -12 & -2 & -6 \\ -2 & 10 & 2 & 5 \\ -1 & 6 & 1 & 3 \end{pmatrix}$

Table 1. Test applied.

The data, depicted in Fig. 4, indicates that 45.45% of students in the control group did not know how to calculate the modular inverse matrix for matrices 1 and 2, 31.81% of the same group solved one of the two matrices, and just 22.72% solved the two matrices. On the other hand, 9.09% of students in the experimental group did not know how to calculate the modular inverse matrix for matrices 1 and 2, 36.36% of the same group solved one of the two matrices, and 54.54% solved the two matrices.

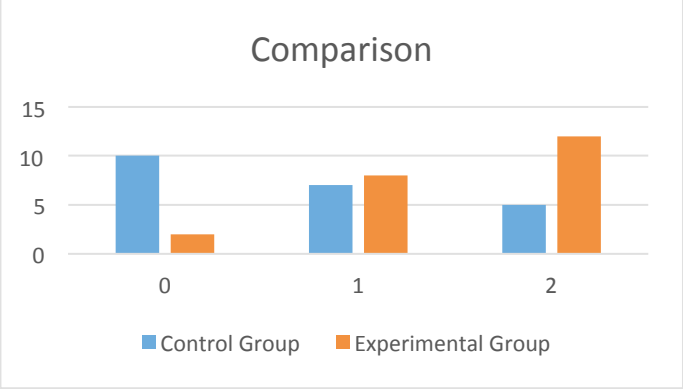

Fig. 4. Comparative of number of matrices solved.

The statistic t-test was used to determine whether there was a significant difference in the control and experimental group scores. As shown in Table 2, the *p-value* is 0.004, and *t* is 0.4983. Since $p<0.05$. There is a significant difference between the control and experimental groups at the 5% (0.05) significance level. In other words, there was a substantial increase in the experimental group performance.

	N	Mean	Std. Deviation	t-test	Sig (1-tailed)
Control Group	22	0.7727	0.8125	0.4983	0.004
Experimental Group	22	1.4545	0.6709		

Table 2. Mean analysis of control and experimental groups.

These findings may support the teaching of symmetric cryptography and the use of technology for teaching mathematics, in this case, for teaching modular inverse matrix calculation. Linear algebra was materialized in a real application so that students could learn the abstract concepts, rules, and operations.

5 Conclusions and Directions for Future Research

Teaching modular inverse matrix calculation in the classroom along with the mobile application that encrypts and decrypts using the Hill Cipher algorithm can be implemented in a Linear Algebra course with educational purposes, as an option to propitiate learning, to motivate, and to enthuse undergraduate students in the learning of these topics. The results indicate that the experimental group showed a better performance in the calculation of the modular inverse matrix. We observed that students like cryptography and that they found it entertaining to decrypt a cipher text.

There is so much future work left to do. In the first instance, the improvement of the application with the calculus of inverse matrices of size n x n, being executed in mobile devices. We also want to implement both methods to calculate the modular inverse matrix in a mobile device and measure the CPU usage. In this way students can observe which method is faster and use less hardware resources. Hill Cipher cryptosystem can be applied in different research areas.

Acknowledgments. We would like to thank the reviewers for their pertinent comments and UAQ for their economical support for the development of this research.

References

[1] M. Otte, Mathematical Epistemology From a Peircean Semiotic Point of View. *Educational Studies in Mathematics*, pp. 11-38, 2006.

[2] M.T. Sakalli, How to Teach Undergraduate Students a Real Cipher Design. *Proceedings of the International Conference on Information Technology Based Higher Education and Training (ITHET)*, Cappadocia, Turkey, pp. 328-335, 2010.

[3] I. Siap, Motivating the concept of eigenvectors via cryptography. *Teaching Mathematics Applications*, Oxford Journals, pp. 53-58, 2008.

[4] E. Baran, A Review of Research on Mobile Learning in Teacher Education. *Educational Technology & Society*, 17(4), pp. 17-32, 2014.

[5] J. Bacca, S. Baldiris, R. Fabregat, S. Graf and Kinshuk, Augmented Reality Trends in Education: A Systematic Review of Research and Applications. *Educational Technology & Society*, 17(4), pp. 133-149, 2014.

[6] P. Rabardel, *Les hommes et les technologies: une approche cognitive des instruments contemporains*. Editeur Armand Colin, 1995.

[7] W. Stallings, *Cryptography and Network Security Principles and Practices*. Prentice Hall Press, 2011.

[8] S. Grossman, *Álgebra Lineal*. McGraw-Hill, 2008.