

The implementation of computer based instruction model on Gost Algorithm Cryptography Learning

Tonni Limbong¹, Janner Simarmata², ARS Tambunan², Parulian Siagian³, Joel Panjaitan⁴, Lestina Siagian³, Erbin Sitorus⁴, Marvin Frans Sakti Hutabarat⁵, Abba Suganda Girsang⁶, Katen Lumbanbatu⁷

¹Universitas Katolik Santo Thomas, Jalan Setia Budi No.479 F, Tanjung Sari, Tj. Sari, Medan Selayang 20132, Medan - Indonesia

²Universitas Negeri Medan, Jalan Willem Iskandar Pasar V Medan 20221, Medan - Indonesia

³Universitas HKBP Nommensen, Jalan Sutomo No.4A, Perintis, Medan Timur 20235, Medan - Indonesia

⁴Akademi Teknik Deli Serdang, Jl. Sultan Hasanuddin, Tj. Garbus Satu, Lubuk Pakam 20518, Deli Serdang – Indonesia

⁵Institut Sains dan Teknologi TD Pardede, Jl. Dokter TD Pardede No.21, Medan Baru 20152, Medan – Indonesia

⁶Computer Science Department, BINUS Graduate Program Master of Computer Science, Bina Nusantara University, Jakarta, Indonesia

⁷STMIK Kaputama, Jl. Veteran No. 4A - 9A, Tangsi 20714, Binjai - Indonesia

E-mail: tonni.budidarma@gmail.com

Abstract. The objective of this study is to develop learning media by using the Computer Based Instruction (CBI) model for GOST algorithm cryptographic material (Gosudarstvennyi Standard). Besides, the study serves to present learning using computer media, especially in the Informatics Engineering study program. The method used in this study uses the Research and Development (R & D) method. The results of this development research are learning media products in the form of tutorial CDs with the contents of the material: GOST Cryptographic Theory, Encryption Process and Decryption process using alphabet text data. Based on the results of the application and testing of the program, it can be concluded that this application is easy to use. Learning the Gost algorithm in the encoding method utilizing the Computer Based Instructions (CBI) method helps to understand the material and facilitate the learning process.

1. Introduction

In cryptography, there are many algorithms found, one of which is the Gost Algorithm. Gost is an abbreviation of "Government Standard" which means government standard, Gost algorithm is a chipper algorithm. Cryptography The Gost algorithm is Modern cryptography, in contrast to classics which are generally character oriented, modern bit-oriented encoding because current encoding uses computer media to process messages. The message in a shared password is not always a series of characters; it can be a series of bits, such as videos or image files.

Computer Based Instruction (CBI) is a teaching material arranged systematically and designed with a programming language or with software. A computer system presents a series



of teaching programs by interacting with a computer system, the need for the availability of learning programming that utilizes the Learning Method Computer-Based Instruction (CBI) increasing and using strategic learning methods with materials, exercises, questions, quizzes. Learning media that is packaged in a computer program aims to help understand the material to facilitate the teaching and learning process.

In connection with the description of the background of the above problems can be formulated the issues to be studied include how cryptographic learning is easy to understand by applying the Computer-Based Instruction (CBI) model in cryptographic education with multimedia-based Gost Algorithm material. The aim is to facilitate students or students in the cryptographic learning of the Gost Algorithm in learning the stuff and providing convenience in the teaching and learning process.

2. Research Method

This study uses research and development models or Research and Development (R & D). The R & D method is a research used to produce specific products and 10 (ten) stages, namely (1) Analysis and Potential Problems, (2) data collection, (3) product design, (4) design validation, (5) design revision, (6) product trials, (7) product revisions, (8) usage trials, (9) product revisions and (10) mass production. But in this study, it only uses eight stages because the product made is not mass produced.

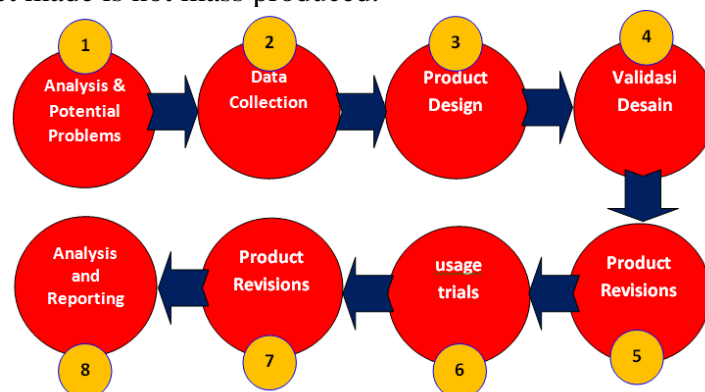


Figure 1. Research Method R & D

In this study, the instrument is used to collect data that will be used as a reference assessment by experts on the products produced. The research instruments used in this study are as follows:

1. Validation sheet, this instrument is used to determine the feasibility of the media that has been produced and obtain advice from media experts, content experts, and design experts to correct the shortcomings of the learning media produced
2. Questionnaire on student responses, this research instrument is used to determine student responses to the press that has been produced. For the grid, the student response sheet is the same as the validation sheet because the object being observed is the same.
3. Learning outcomes, Tests are ways that can be used or procedures that need to be taken in the framework of measurement and research in the field of education.

Assessment of the validity of learning media is done by giving responses to questionnaires with very valid, less valid and invalid criteria. While the evaluation of student responses to learning media is done by responding to surveys with rules that are very good, good, not good

and not good. To analyze the validator answers and student responses used descriptive statistics on rating results, which are described as follows:

$$HR = \frac{\sum_{i=1}^4 n_i x_i}{nk \times n \times x_{i_{max}}} \times 100\%$$

3. Basic Theory

The learning process is a process in which there are students, educators and learning resources in a learning environment. Learning activities will run smoothly if the three aspects exist. Submission of sound and more specific material referring to the learning objectives will make students feel interested in learning the content delivered by the teacher. In addition to teaching materials to students, it is also best to do exam tests following the material presented to find out how understanding students understand about the material presented by educators, so that the learning objectives can be measured or not achieved.

3.1. Cryptography and Gost Algorithm

Cryptography is the science and art of maintaining the confidentiality of messages by encoding them in a form that cannot be understood anymore. Cryptography is used for important communication security.

Gost or Gosudartstavany Standard, meaning government standard namely encryption algorithm and developed in 1970, the gost was made by Soviet as an alternative to the United States. DES standard encryption algorithm, GOST is structurally similar to DES. The GOST structure uses the Fietsel network. One GOST round for Ki-1 rounds, private ki key is used. One Gost round with DES is considered in the formula below:

$$Li = Ri-1 \dots\dots\dots(1)$$

$$Ri = Li-1 \oplus f(Ri-1, Ki) \dots\dots(2)$$

3.2 Key Generation Process

The generation of the internal key is done by dividing the 256-bit external key (k1, k2, k3, k4, ..., k256) into eight parts, each of which is 32 bits long.

The division is as follows:

$$K0 = (k32, \dots\dots, k1)$$

$$K1 = (k64, \dots\dots, k33)$$

$$K2 = (k96, \dots\dots, k65)$$

$$K3 = (k128, \dots\dots, k97)$$

$$K4 = (k160, \dots\dots, k129)$$

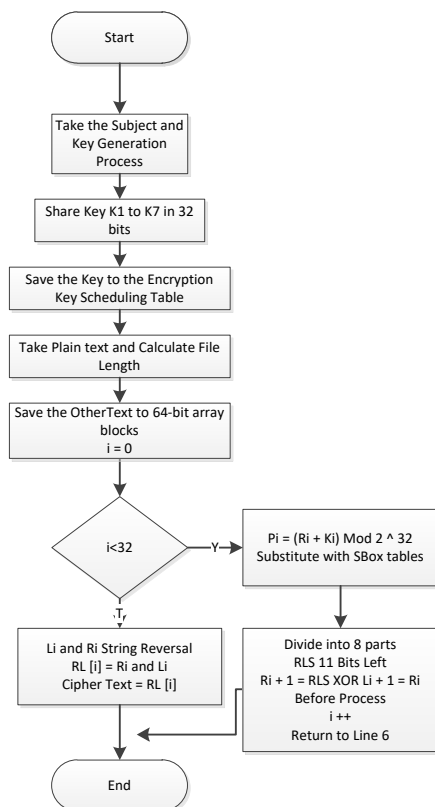
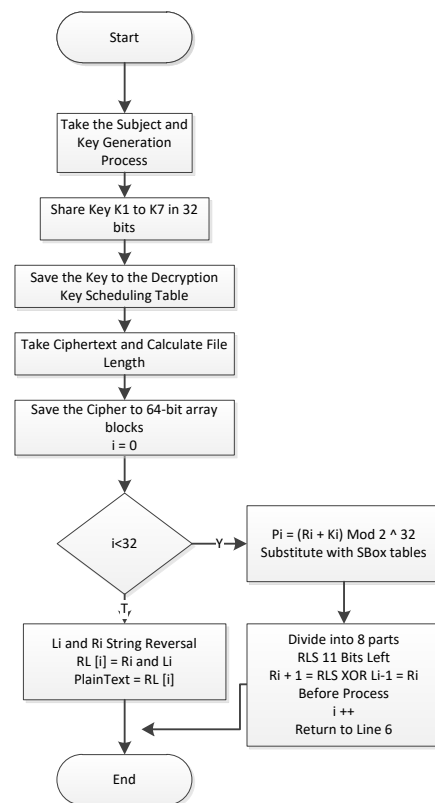
$$K5 = (k192, \dots\dots, k161)$$

$$K6 = (k224, \dots\dots, k193)$$

$$K7 = (k256, \dots\dots, k225)$$

3.3 Encryption and Decryption Process

This algorithm explains the encryption and decryption process and is a continuation of the compose page.

**Figure 2.** Read Flow for Encryption**Figure 3.** Read Flow for Decryption

4. Result and Discussion

This main menu displays the menu options that you want to run or use. In the main menu there are four menu options, namely:

a. Tutorial

In this tutorial menu, some materials discuss cryptographic learning. The tutorial menu can be seen in Figure 2

b. Exercise

In this menu, the items that discuss cryptography and GOST algorithm are displayed, the menu display can be seen in the picture below

c. Game

In this menu, there are only practice questions changing the plaintext to the ciphertext form in which the timeout is given.

d. About Me

This menu will display the name of the program maker

The menu can be seen from figure below:

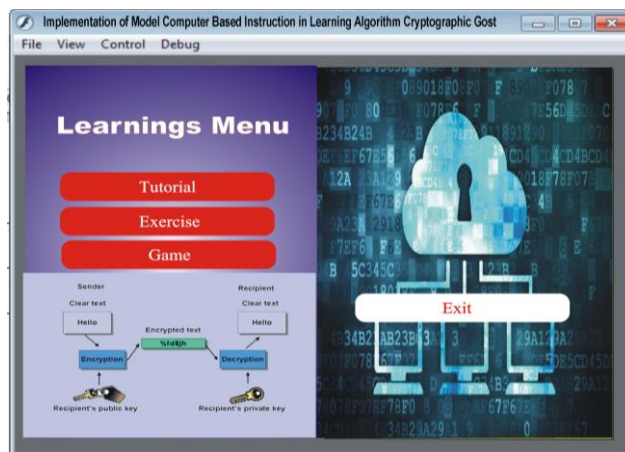


Figure 4. Main Menu Display

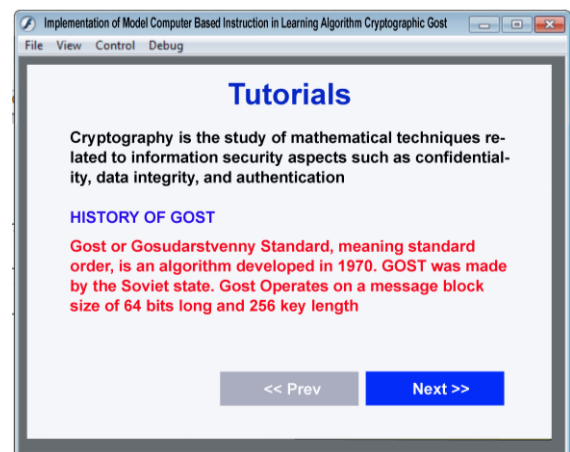


Figure 5. Menu Display Tutorial

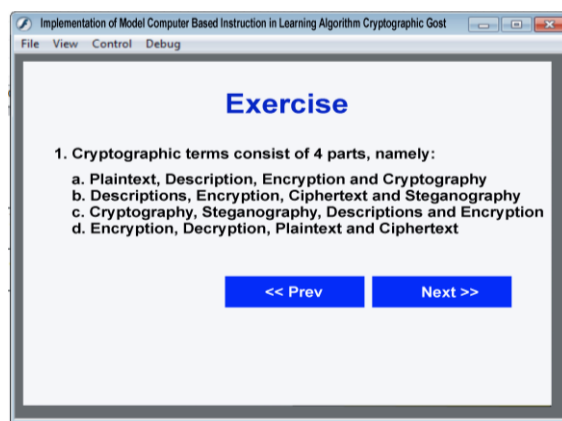


Figure 6. Display Training Menu

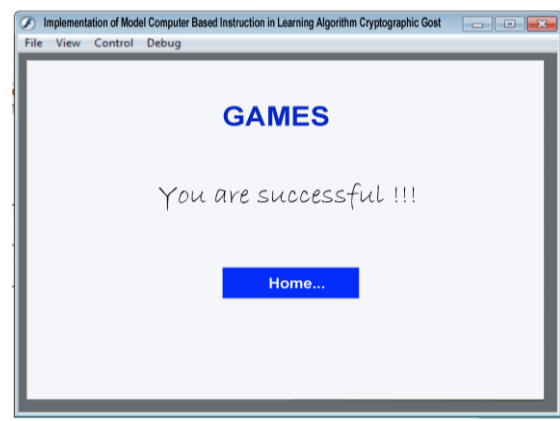
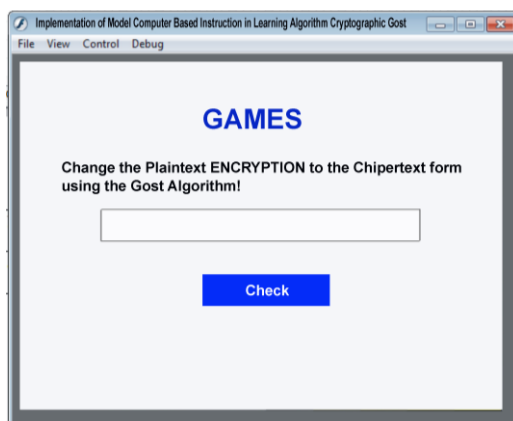
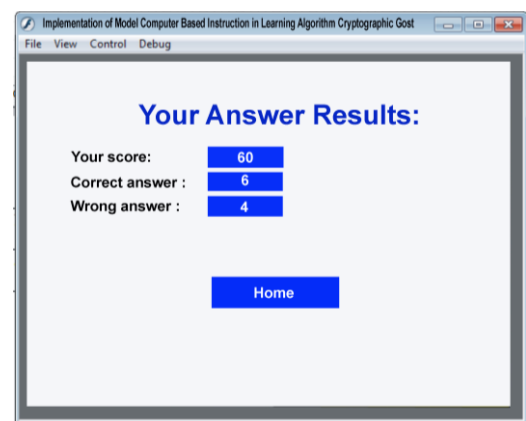


Figure 7. Game Menu Display

5. Conclusions

In closing the discussion in the study, the authors conclude as well as provide advice to readers who use the algorithm Gost's cryptographic learning application. The obtained

findings are that the Gost algorithm cryptographic learning application with the Computer Based Instruction model as a tool used to get good learning and produce a quick and clear knowledge containing Cryptographic Theory learning material, Gost Algorithm, Encryption Process and Decryption Process where the presentation in the form of exciting display materials using multimedia and animation can improve user understanding.

References

- [1] J. Simarmata *et al.*, “Learning Application of Multimedia-Based-Computer Network Using Computer Assisted Instruction Method,” *Int. J. Eng. Technol.*, vol. 7, no. 2.13, pp. 341–344, Apr. 2018.
- [2] S. Sriadhi, S. Gultom, R. Restu, and J. Simarmata, “The Effect of Tutorial Multimedia on the Transformer Learning Outcomes Based on the Students’ Visual Ability The Effect of Tutorial Multimedia on the Transformer Learning Outcomes Based on the Students’ Visual Ability,” *IOP Conf. Ser. Mater. Sci. Eng.* 384 012059, 2018.
- [3] J. Simarmata, “Prototype Application Multimedia Learning for Teaching Basic,” vol. 7, pp. 264–266, 2018.
- [4] T. Limbong, P. Manullang, and E. Napitupulu, “Dikte Test Applications (IMLA) Using Computer Assisted Instruction (CAI) Model.”
- [5] T. Limbong *et al.*, “The Implementation of Multi-Objective Optimization on the Basis of Ratio Analysis Method to Select the Lecturer Assistant Working at Computer Laboratorium,” *Int. J. Eng. Technol.*, vol. 7, no. 2.13, pp. 352–356, Apr. 2018.
- [6] J. Simarmata, A. Djohar, J. P. Purba, and E. A. Djuanda, “IMPLEMENTASI MODEL PEMBELAJARAN BERBASIS BLENDED LEARNING UNTUK MENINGKATKAN HASIL BELAJAR SISWA.”
- [7] J. Simarmata, A. Djohar, J. P. Purba, and E. A. Djuanda, “Perancangan Prototype Model Pembelajaran Berbasis Blended Learning Untuk Meningkatkan Proses Pembelajaran,” 2017.
- [8] J. Piaget and M. Cook, *The origins of intelligence in children*, vol. 8, no. 5. International Universities Press New York, 1952.
- [9] D. Napitupulu *et al.*, “Analysis of Student Satisfaction Toward Quality of Service Facility,” *J. Phys. Conf. Ser.*, vol. 954, no. 1, 2018.
- [10] J. Simarmata, A. Djohar, J. Purba, and E. A. Juanda, “Design of a Blended Learning Environment Based on Merrill’s Principles,” *J. Phys. Conf. Ser.*, vol. 954, no. 1, 2018.
- [11] R. M. Gagne and L. J. Briggs, *Principles of instructional design*. Holt, Rinehart & Winston, 1974.
- [12] G. Gunawan *et al.*, “Mobile Application Detection of Road Damage using Canny Algorithm,” in *Journal of Physics: Conference Series*, 2018, vol. 1019, no. 1, p. 12035.
- [13] J. Simarmata, “Pengenalan Teknologi Komputer dan Informasi,” *Yogyakarta Andi*, 2006.
- [14] J. Simarmata and T. Chandra, “Grafika Komputer,” *Yogyakarta Penerbit Andi*, 2007.