ASTEEC Conference Proceeding: Computer Science
3rd International Conference on Information Science and Technology Innovation (ICoSTEC)
July 27, 2024, Yogyakarta, Indonesia

Securing Data Files Using RSA-ElGamal and Diffie-Hellman Algorithms

Ameliana Sihotang[1], Rika Rosnelly[2], Zakarias Situmorang[3]

JL. KL. Yos Sudarso Km. 6,5 No. 3-A, Tanjung Mulia, Kec. Medan Deli, Kota Medan, Sumatera Utara 20241,Jl. Jl. Setia Budi No.479, Tj. Sari, Kec. Medan Selayang, Kota Medan, Sumatera Utara

[1]amelianasihotang123@gmail.com, [2] rikarosnelly@gmail.com, [3]zakarias65@yahoo.com

Abstract

*Data security involves efforts to protect and ensure three key aspects in the cyber realm: the confidentiality, integrity, and availability of data. It assures cyber users that their privacy is safeguarded, whether on personal computers, mobile devices, or during internet browsing activities. The objective of this study is to authenticate data while applying the SHA-256 function in cryptographic algorithms. Utilizing a combination of the Diffie-Hellman, RSA, and ElGamal algorithms can offer a strong solution to enhance the security of PDF files against various security threats.**Keywords: Keamanan ,Diffie-Hellman ElGamal*

1. Introduction

Cryptography is the study of encoding techniques, where encryption, a method within cryptography, transforms data of various lengths into data of fixed length. Encryption is the primary, effective, and efficient method in data security, ensuring secure, accurate, and efficient data communication between parties. Prior studies have also concentrated on employing hash functions and cryptographic techniques like RSA and ElGamal to secure sensitive data. This study attempts to validate data while integrating the SHA-256 function into cryptographic algorithms, showing that ElGamal is superior to RSA in terms of signature generation and encryption, while RSA is superior in terms of encryption and verification of signatures. A further study, "Application of Image and Text Encryption Using Diffie-Hellman and ElGamal Algorithms," which was carried out in January 2020, also emphasizes the significance of data security for information storage, especially for message exchange, and the necessity of symmetric and asymmetric encryption techniques.

2. Research Methods

2.1 Cryptography

Cryptography is the study of encoding techniques, where encryption, a method within cryptography, transforms data of various lengths into data of fixed length. Encryption is the primary, effective, and efficient method in data security, ensuring secure, accurate, and efficient data communication between parties. Previous research has also focused on securing sensitive data using RSA and ElGamal cryptographic algorithms with hash functions. This study aims to authenticate data while incorporating the SHA-256 function into cryptographic algorithms, illustrating that RSA performs better than ElGamal in encryption and signature verification, while ElGamal excels in decryption and signature creation. Additionally, another study titled "Application of Image and Text Encryption Using Diffie-Hellman and ElGamal Algorithms," conducted in January 2020, underscores the crucial importance of data security in information storage, particularly in message exchange, necessitating encryption methods, including symmetric and asymmetric encryption.:

Communication Elements: Messages, Plaintext, and Ciphertext

1. A message, also known as plaintext or clear text, refers to data or information that is legible and understandable in its content.

2. Participants in Communication: Sender and ReceiverData exchange involves the transfer of messages between two entities. The sender is the entity transmitting a message, while the receiver is the entity receiving it.

3. Encryption and Decryption Processes
   Encryption, alternatively termed enciphering according to ISO 7498-2, involves encoding plaintext into ciphertext. Decryption, or deciphering, reverses this process, converting ciphertext back into its original plaintext.

4. Cipher Techniques and Keys
   Cryptographic algorithms, known as ciphers, dictate the rules for encryption and decryption. They may employ distinct algorithms for each process. These algorithms rely on mathematical principles governing the relationship between sets containing plaintext and ciphertext elements. Encryption and decryption functions serve to map elements between these sets.

2.2. *The Key Generation in the Diffie-Hellman algorithm*

The Diffie-Hellman key exchange algorithm is valuable for securely exchanging secret keys in symmetric cryptography communications. Its strength lies in the difficulty of computing discrete logarithms. The process entails the following steps: 1. Let's

assume Sender and Receiver are the communicating parties. Initially, Sender and Receiver agree on two large numbers (preferably primes), P and Q, such that P < Q. The values of P and Q need not be kept secret; Sender and Receiver can even discuss them through an insecure channel. 2. Sender generates a large random integer, x, and sends the following calculation result to the Receiver: X = Px mod Q. 3. The Receiver generates a large random integer, y, and sends the following calculation result to the Sender: Y = Py mod Q. 4. Sender calculates K = Yx mod Q. 5. Receiver calculates K' = Xy mod Q. If the calculations are done correctly, K = K'. Thus, Sender and Receiver have obtained the same key without being known by others. The security level of the ElGamal algorithm relies on the complexity of computing discrete logarithms. Its advantage lies in key generation using discrete logarithms and encryption/decryption methods involving extensive computational processes, resulting in encrypted data twice the size of the original. With the same plaintext, different ciphertexts are obtained in the encryption process, while the same plaintext is obtained in the decryption process. ElGamal can be used to secure data because its algorithm forms one of its keys using prime numbers and emphasizes the strength of its key in solving the discrete logarithm problem, thus ensuring the security of the key. Despite its weaknesses, the ElGamal algorithm has many more advantages.sehingga dalam paper ini menggunakan algoritma ElGamal enhances data security, but its drawback lies in requiring significant resources and processors capable of handling extensive computations.

Regarding the Rivest-Shamir-Adleman Algorithm (RSA), some experts suggest that 1024-bit keys might become vulnerable in the near future (though this remains a topic of debate), whereas there's general consensus that 2048-bit keys will remain secure for the foreseeable future. If the key length is 256 bits or shorter, RSA keys can be found in just a few hours using available software on a PC. For key lengths of 512 bits or shorter, it could take hundreds of hours, as demonstrated in 1999 using numerous computers. Theoretical concerns about the security of 1024-bit keys were raised by hardware like TWIRL and explanations from Shamir and Tromer in 2003. Currently, it's recommended that keys be at least 2048 bits long.

5. Results and Discussions

The planned steps for this research are outlined as follows:

Literature Review

This phase entails gathering relevant literature and research materials on cryptography algorithms such as Diffie-Hellman, RSA, and ElGamal from diverse sources including books, journals, articles, and other scholarly references.

Research Analysis

The research analysis involves utilizing the cryptographic key generation of the Diffie-Hellman algorithm to encrypt data in both the RSA and ElGamal algorithms.

Testing

System testing will be conducted at this stage to evaluate the performance of each algorithm after integrating the cryptographic key generation of the Diffie-Hellman algorithm into RSA and ElGamal.

3.1. Interface Implementation

To streamline system operation, the interface will be implemented in various types, each tailored to its specific function. This interface acts as the user-computer interaction point, facilitating input and output of data to provide information to users. The interface design prioritizes user-friendliness to ensure ease of use for program users.

3.1.1. Main Menu Form

This form serves as the program's initial display, featuring buttons for file encryption and decryption functions.

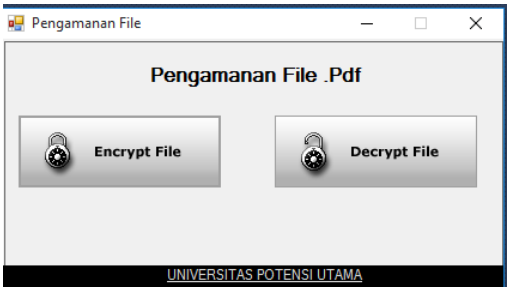
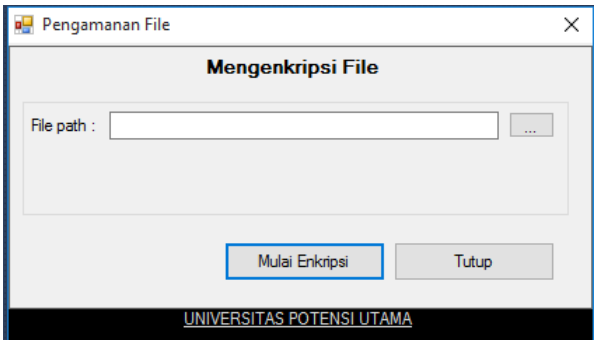


Figure 1. Main Menu Form

3.1.2. File Encryption Form

This form serves as the interface for encrypting files within the program.



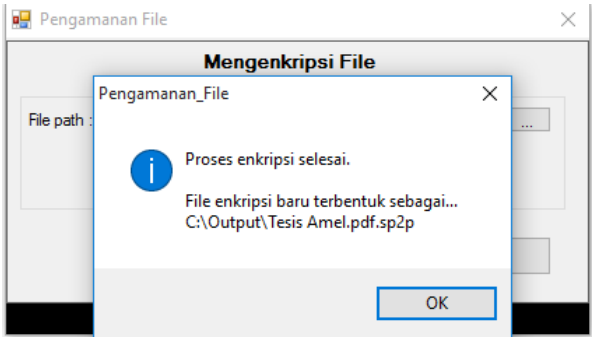


Figure 2. File Encryption Form

3.1.3. File Decryption Form

This form is utilized for decrypting files that have been previously encrypted in the encryption menu.

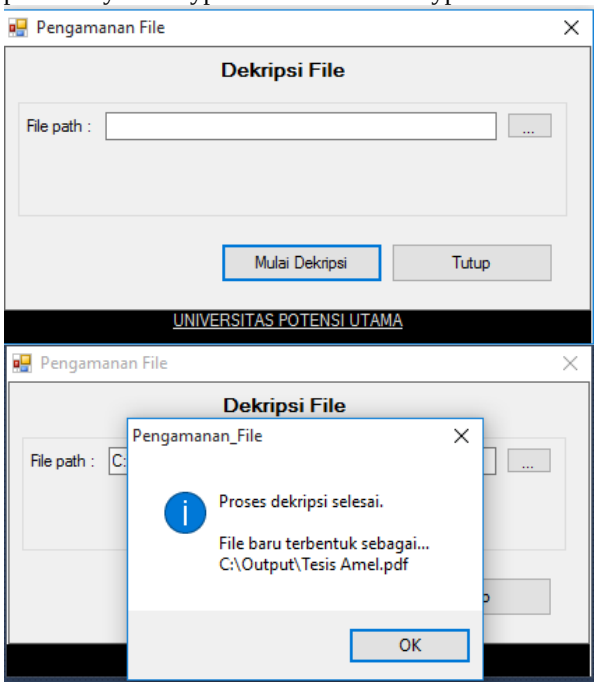


Figure 3 File Decryption Form

3.1.3. File Decryption Form:

The encrypted file will revert to its original PDF format once it has been decrypted. The visual representation of the file can be observed in the image below.

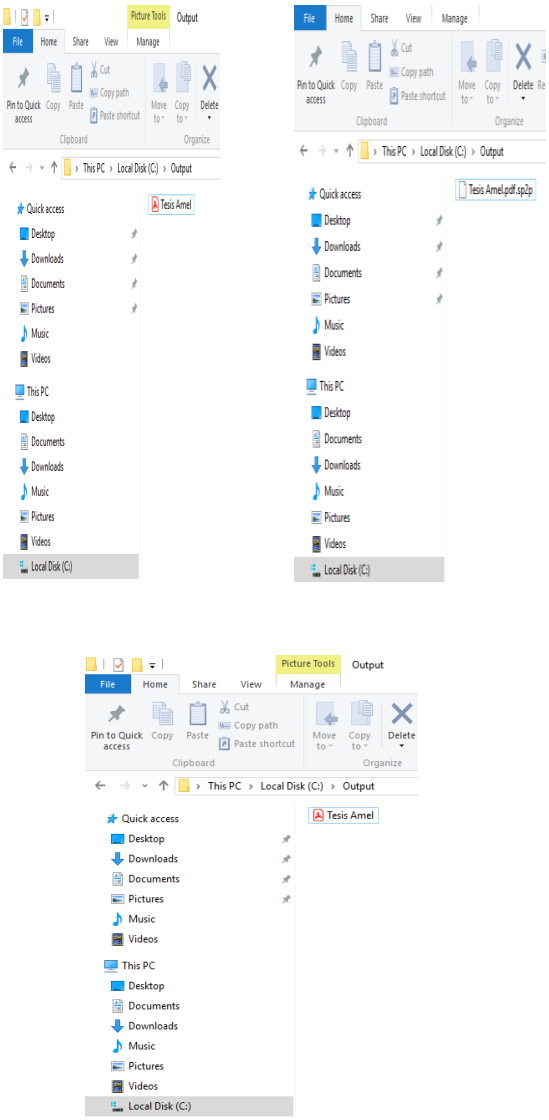


Figure 4 .Form Dekripsi File

.

In this application, the author conducted functional testing to ensure the system operates as intended. The testing process evaluated the system's functionalities by comparing its outputs with expected results. If the outcomes match the expectations, it indicates the software aligns with the predetermined design; if not, further investigation and adjustments are needed. System testing involved all user groups as planned in earlier stages, and acceptance testing concluded once all user groups expressed satisfaction based on predefined criteria.In this regard, the author will detail the implementation steps taken to complete this application based on the theories studied. These steps include designing the system architecture using Visual Basic 2010 and creating use cases, sequence diagrams, activity diagrams, program models, and input-output models for the database security application. This aims to clarify the program's direction, enhance reader comprehension, facilitate user understanding, and explain the program's purpose.

b. Hardware and Software Provisioning

In this phase, the author acquires the necessary hardware and software components for developing the application, including computers, operating systems, and programming languages.

c. Programming Code Implementation

The author translates the system design instructions into computer code using the chosen programming language. The code is sourced from various resources, such as books and online materials, and may be adapted to suit the project's requirements.

d. System Testing

System testing is conducted to ensure that the programming tasks are performed correctly, resulting in the desired functionalities. This phase also aims to identify any limitations or weaknesses in the system, allowing for possible improvements to be made.

4. Conclusions

Based on the conducted testing and discussions, several conclusions can be drawn:

1. The testing results demonstrate that the combination of these algorithms provides a high level of security in transmitting and storing sensitive information, particularly in key exchange and encryption processes.
2. The implementation of this algorithm combination effectively ensures data confidentiality, ensuring that only authorized parties can access encrypted information.
3. The testing reveals that there is an additional time and overhead in the encryption and decryption processes compared to simpler methods, but the security obtained justifies these sacrifices.
4. The success of this implementation depends heavily on selecting appropriate parameters and implementation techniques.. Incorrect parameter usage or implementation errors can reduce the security effectiveness of this algorithm combination.
5. Therefore, it can be concluded that the combination of Diffie-Hellman, RSA, and ElGamal algorithms can serve as a robust solution to enhance PDF file security against various security threats.

References

[1] Gunawan, I., Cepu, R., & Teknologi, S. T. (N.D.). Data Integrity: Theory and Practice. http://www.Jejakpublisher.Com"Classification of Malaria Complication Using CART (Classification and Regression Tree) and Naïve Bayes," R. Irmanita, S. Suryani Prasetiyowati, and Y. Sibaroni, RESTI, vol. 5, no. 1, pp. 10 - 16, Feb. 2021. https://doi.org/10.29207/resti.v5i1.2770

[2] Adeniyi, E. A., Falola, P. B., Maashi, M. S., Aljebreen, M., & Bharany, S. (2022). Secure Sensitive Data Sharing Using Rsa And Elgamal Cryptographic Algorithms With Hash Functions. Information (Switzerland), 13(10). Https://Doi.Org/10.3390/Info13100442

[3] Nisa, L., Indriypenerima, T., & Ruswiansari, M. (2020). Utilizing Diffie-Hellman and Elgamal Algorithms for Image and Text Encryption Applications. In Journal of Technology and Management (Vol. 1, Issue 1).

[4] Nandar Pabokory, F., Fitri Astuti, I., & Harsa Kridalaksana, A. (2015). Implementasi Kriptografi Pengamanan Data Pada Pesan Teks, Isi File Dokumen, Dan File Dokumen Menggunakan Algoritma Advanced Encryption Standard. In Jurnal Informatika Mulawarman (Vol. 10, Issue 1).

[5] Pembangkit, T., Algoritma, K., Menggunakan, R., Diffie, A., Pada, H., Citra, K., Prastya, R., Pardede, A. M. H., Fauzi, A., Stmik, K., & Binjau, J. (2022). Teknik Pembangkit Kunci Algoritma Rsa Menggunakan Algoritma Diffie Hellman Pada Keamanan Citra (Vol. 04, Issue 01).

[6] Elgamal Dengan Pertukaran Kunci Diffie Hellman Pada Aplikasi Keamanan Citra Sidik Jari Berbasis Android Nurul Yalisa, A., & Arhami, M. (2018). A-1 (Vol. 2, Issue 1).

[7] Irawan, C., & Rachmawanto, E. H. (N.D.). Keamanan Data Menggunakan Gabungan Kriptografi Aes Dan Rsa.

[8] Nisa, L., Indriypenerima, T., & Ruswiansari, M. (2020). Application of Image and Text Encryption Using Diffie-Hellman and Elgamal Algorithms. In Journal of Technology and Management (Vol. 1, Issue 1).Pramitasari, R. (N.D.). Algoritma Optimasi Chaos Pada Ridge Polynomial Neural Network Untuk Kriptanalisis Kunci Publik Elgamal.

[9] Studi, P., Informasi, S., Teknologi, J., & Saintek, F. (2018). Analysis and Design of Hybrid Cryptography Algorithm for Company Data Security Strategy Management. Ilham (Vol. 3, Issue 2).Allan, J., Andjarwirawan, J., & Dewi, L. P. (N.D.). Implementasi Algoritma Aes, Elgamal, Dan Sha3 Untuk Keamanan File Digital.

[10] Pendahuluan, I., Yusfrizal1, Y., Agustin4, F., Meizar2, A., Kunci, M., Kombinasi, M., Pertukaran, D., Diffie-Hellman, K., & Aes, E. (N.D.). The 6th International Conference On Cyber And It Service Management (Citsm 2018).

[11] Fatima, S., Rehman, T., Fatima, M., Khan, S., & Ali, M. A. (2022). Comparative Analysis Of Aes And Rsa Algorithms For Data Security In Cloud Computing †. Engineering Proceedings,20(1). Https://Doi.Org/10.3390/Engproc2022020014