JSCE (Journal of System and Computer Engineering)
Vol.6, No.1, Januari 2025, pp. 1-9
ISSN (online): 2723-1240
DOI : https://doi.org/10.61628/jsce.v6i1.1511

Application of Advanced Encryption Standard (AES) Algorithm in E-Commerce Login System for User Data Security

Aulyah Zakilah Ifani [1,a,*]; Rezki Nurul Jariah S.Intam [2,b]; Andi Irfandi Syair [3,c] ; Husnawati [4,d]

[1] *Sistem Teknologi Informasi, Teknologi dan Bisnis, Institut Teknologi dan Bisnis Nobel Indonesia*
[2,3,4] *Teknik Informatika dan Komputer, Fakultas Teknik, Universitas Negeri Makassar*
[a] *aulyahzakilah123@gmail.com;* [b] *rezkinuruljariah@gmail.com;*[c] *andiirfan616@gmail.com;* [d] *h6153728@gmail.com*
** Corresponding author*

Abstract

E-commerce has become an electronic media that uses a login system used by users. User data in the form of usernames and passwords is vulnerable to hacking. One technique to improve user security is the implementation of AES algorithms on login systems in E-Commerce applications. The purpose of this study is to apply the AES algorithm in the login system of e-commerce websites and analyze the improvement of information security for users after the implementation is carried out. The research method used is an experiment with the application of the use of the AES algorithm before and after. Therefore, the application of the AES algorithm on the login system of e-commerce websites can be used as a solution to improve user data security. Testing using Wireshark and Burpsuite tools. The results obtained are that AES successfully secures the username and password on the e-commerce login system .

Keywords— *AES algorithm, Burpsuite, Cryptography, E-commerce, Wireshark*

1. Introduction

The use of the internet in the business world is increasingly widespread and growing rapidly which is used as a tool for marketing, sales, customer service (Agunawan et al., 2023). One of the most commonly used communication tools today is Internet Technology, as Information Technology provides so many advantages and benefits. With the existence of Information Technology, the implementation of information delivery and marketing activities becomes more practical because it is not bound by time and place. The use of information technology in information delivery and marketing also has the potential to reduce costs and time required in the transaction process (Husain et al., 2023).

One example of popular use of the Internet is the use of web applications. A website is a medium used to provide information through the Internet (Ifani et al., 2024). Apart from being a means of disseminating information, websites can also be used to create an online store. A website consists of a collection of pages that are usually in a domain or subdomain on the World Wide Web (WWW) on the Internet (Judijanto et al., 2024). Each web page is a document written in HTML (Hyper Text Markup Language) format and can usually be accessed via the HTTP protocol. Through a web browser, information stored on the website's server can be displayed to the user. With the existence of many websites scattered, a very wide information network has been formed (Sinlae et al., 2024).

Websites provide many advantages and benefits in promoting or conducting buying and selling transactions in the business world through online media. In today's era, many companies

sell products and product promotions through E-Commerce and E-Business, where sales and transaction activities are carried out electronically via the internet. Web applications are not only one type but there are many types, such as online stores and websites that contain information (Aminu & Ichwani, 2024). However, the security of e-commerce websites, especially in the login system, is very vulnerable to the threat of Trappdor malware attacks to gain unauthorized access to sensitive data, so it is necessary to maintain and improve the integrity of user data or information (Riadi et al., 2021).

A trapdoor attack is a type of cybersecurity attack that is exploited by using a loophole or secret entrance (Login system) in a system or application. Users who have access to the entrance can use it to gain access without going through the proper security procedures. Trapdoors themselves can be used by programmers for the purpose of debugging and testing programs, but can be a threat if misused by irresponsible programmers to gain unauthorized access. Trapdoor attacks can be carried out by injecting malware into the system to create a secret entrance that allows the perpetrator to gain unauthorized access. The threat of trapdoor attacks is increasing along with the increasing use of multiuser operating systems and networks, because this attack allows perpetrators to bypass security facilities and gain direct access to data (Laia & Barmawi, 2024).

One way to improve the security of e-commerce websites from hackers who want to take user data is to apply the AES (Advanced Encryption Standard) algorithm to the login system. AES is a symmetric cryptographic algorithm that can encrypt and decrypt data securely and effectively. The implementation of AES in the login system will increase security by encrypting the login information sent by users, so that the information is not easily intercepted by unauthorized parties (Ignasius & Sakti, 2022).

In the previous research conducted by Sulaimon in the Design and Implementation of Secured E-commerce Digital Learning for the Educational System in Nigeria. The study tested the security of the login system he had secured using the AES algorithm. This study explains that implementing the AES algorithm on E-commerce websites can provide security at the time of login. The disadvantage of this study is that there has been no testing of security tools after using the AES Algorithm (Sulaimon, H.A, n.d.).

This research aims to secure the existing login system in e-commerce applications using the Advanced Encryption Standard (AES) algorithm. The research was conducted with two scenarios, namely before using the AES Algorithm and after using the AES Algorithm. After the implementation of AES, tests were then carried out with several tools such as Wireshark and Burpsuite. The purpose of conducting this test is to test whether the data from the user when logging in has not been detected by a third party.

2. Method

2.1 Research Object

The Login System is the object used in this study. The login system that we will test is the login system found on the E-commerce Website called Baggie.Id. The login system on this website requires users to enter their username and password first in order to access the main page of the Baggie.Id website. On this login system page, it is very vulnerable to crime by irresponsible people to break into or hack victim data. Therefore, in this study, we used the application of the AES algorithm to install a login system on Baggie.Id e-commerce website, and will be tested using a Trappdor attack.

2.2 Cryptography

Cryptography is an art and science used to create an encryption system that is able to ensure the security of information (Sonko et al., 2024). Cryptography is closely related to the protection of digital data. This science consists of design mechanisms based on mathematical

algorithms that provide a number of basic information security services (Dam et al., 2023). Over the years, the development of cryptography technology has experienced very significant progress. There have been major changes in terms of data and message security, encryption and decryption techniques used, and various other aspects (Riadi et al., 2022). Encryption technique is a process used in changing messages, data, or information (usually called plaintext or original message) into a form that cannot be read by unauthorized parties (ciphertext). In this process, plaintext is changed into ciphertext, which is a form of information that cannot be understood or read by people who do not have the correct key or algorithm. Encryption ensures that information sent or stored remains secure and cannot be accessed by unauthorized parties (Dung, n.d.).

2.3 Advanced Encryption Standard Algorithm

AES (Advanced Encryption Standard) is a symmetric cryptographic algorithm used to secure data in electronic communications or data storage. AES was developed by two cryptographers, Joan Daemen and Vincent Rijmen in 1998. The AES algorithm uses a symmetric key to encrypt and decrypt data. Encryption is done by changing the original data (plaintext) into encrypted data (ciphertext) using an encryption key, while decryption is done by changing the encrypted data into the original data using the same decryption key. AES encryption uses a repetitive process called rounds. The number of rounds used by AES depends on the length of the key used. Each round requires a round key and input from the next round, the round key is generated based on the given key (a'laa hussein ali et al., 2024). AES has three key variations, namely AES-128, AES-192, and AES-256. The AES-128 key variation uses a 128-bit key, AES-192 uses a 192-bit key, and AES-256 uses a 256-bit key (Al-Khafaji & Rahma, 2024).

2.4 Wireshark

Wireshark is an application that is used as a tool to analyze data packets in an ongoing network. (Insani, 2023). This application can be used to monitor various types of networks, both wired and wireless. By using Wireshark, a network administrator can easily monitor the network because the data captured by Wireshark can be saved and reopened for further analysis (Sirmayanti et al., 2023).

Wireshark has a weakness in detecting devices using wireless connections. When used to detect devices with wired connections, Wireshark can recognize wireless drivers only with the name "Microsoft" or only limited to the WLAN network protocol. However, Wireshark can still read packets that use the 802.11 protocol, which is a common protocol for wireless networks. However, Wireshark may have difficulty detecting specific wireless devices or with different drivers (Ifani et al., 2024).

2.5 Burpsuite

Burp Suite is a platform used in web application security testing. It is one of the most popular and widely used tools by security professionals, security researchers, and ethical hackers. Burp Suite is developed by PortSwigger, a UK-based security company. Burp Suite consists of several components that work together to perform comprehensive security testing of web applications (Hilmi & Yunan, 2022).

2.6 System Flowchart

The testing conducted in this study uses two scenarios. The first scenario is before using the AES Algorithm and the second scenario is after using the AES Algorithm. The flowchart in this study can be seen in Figure 1.

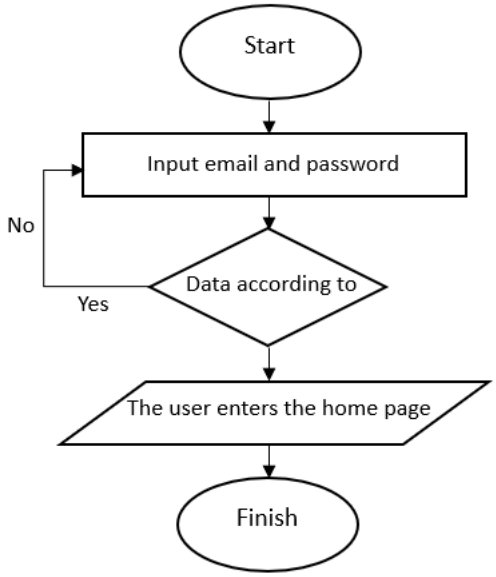

Figure 1. System Flowchart Before Using AES Algorithm

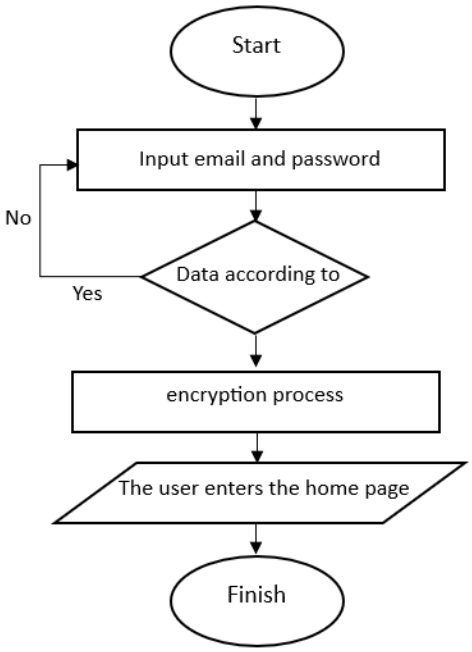

Figure 2. System Flowchart After Using AES Algorithm

Figure 1 and Figure 2 are the system flowcharts before using the AES algorithm and after using the AES algorithm. The AES algorithm as a security used in e-commerce applications.

3. Results And Discussion

This system utilizes Advanced Encryption Standard (AES) cryptographic algorithms to secure user data in the form of usernames and passwords. Figure 3 is the login page where the user is asked to re-enter the email and password that was registered on the create account page. On this page, the AES algorithm will be used so that the data entered by the user can be encrypted or changed into cipher text. The hacking scenario can be seen in Figure 4 and Figure 5.

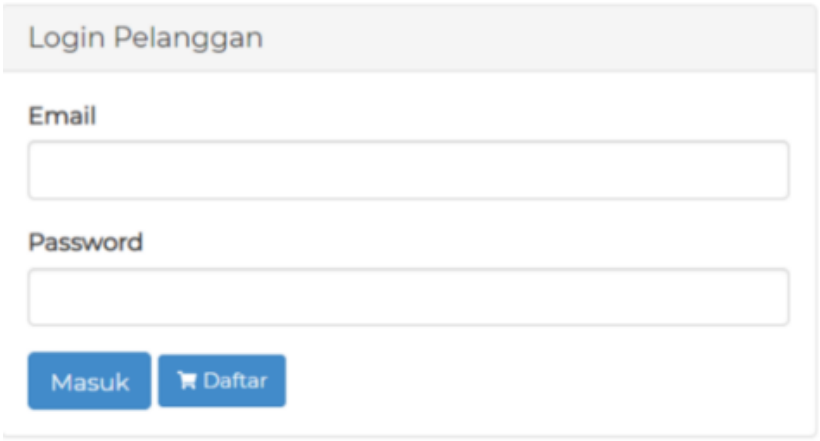

Figure 3. Initial View of the Login System

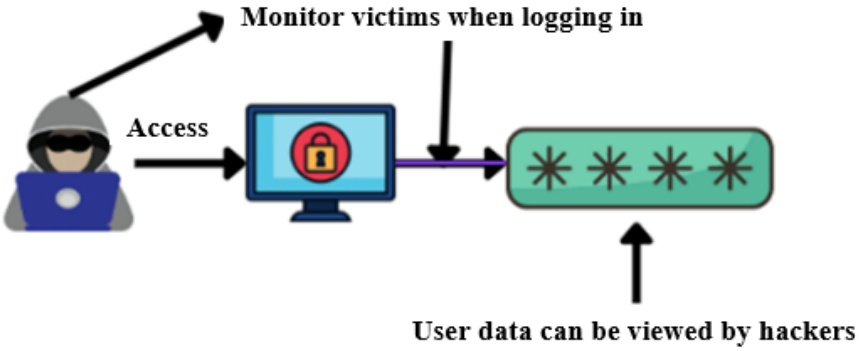

Figure 4. Hacking Scenario Before Using AES Algorithm

Figure 4 shows a scenario that occurs when a hacker wants to take user data by spying on the user when they log in. When a user logs in to a login system that does not have security, it is easier for hackers to see or steal data from the user.

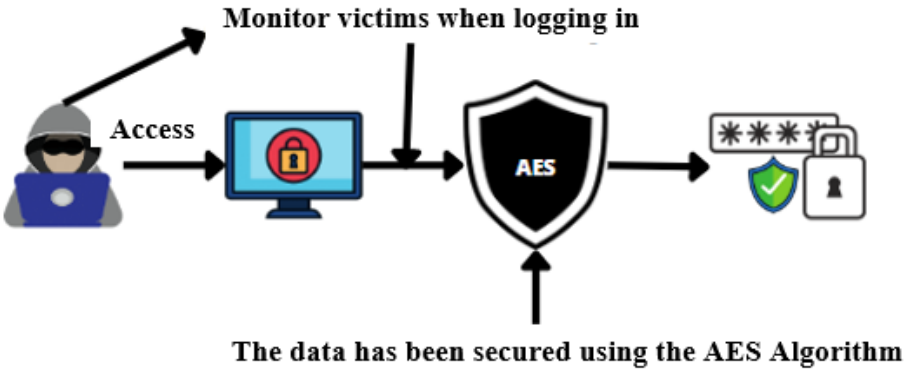

Figure 5. Hacking Scenario After Using AES Algorithm

Figure 5 is the scenario above, it can be seen that hackers are trying to steal data in the form of usernames and passwords on e-commerce websites, but it turns out that the system is already protected by the AES algorithm so that the username and password are already in a cipher text state.

```
<script src="https://code.jquery.com/jquery-3.6.0.min.js"></script>
<script src="https://cdnjs.cloudflare.com/ajax/libs/crypto-js/4.0.0/crypto-js.min.js"></script>
<script>
    $(document).ready(function() {
        $('#loginForm').submit(function(e) {
            e.preventDefault();

            var email = $('input[name="email"]').val();
            var password = $('input[name="password"]').val();

            // Enkripsi email dan password menggunakan CryptoJS
            var encryptedEmail = CryptoJS.AES.encrypt(email, 'encryptionKey').toString();
            var encryptedPassword = CryptoJS.AES.encrypt(password, 'encryptionKey').toString();

            // Update nilai input dengan data terenkripsi sebelum mengirim
            $('input[name="email"]').val(encryptedEmail);
            $('input[name="password"]').val(encryptedPassword);

            // Submit form
            this.submit();
        });
    });
</script>
```

Figure 6. AES Algorithm Implementation Code

Figure 6 shows the code used to implement the AES algorithm on the login system. The tools used to implement the code in the image are Android Studio. The JavaScrip language is used to implement the AES Algorithm and there is an import library used so that AES Encryption can be used.

The testing stage uses the Wireshark and Burpsuite tools to analyze the security on the login system.

```
▼ HTML Form URL Encoded: application/x-www-form-urlencoded
  > Form item: "email" = "kaka@gmail.com"
  > Form item: "password" = "123"
  > Form item: "simpan" = ""
```

Figure 7. Login System Before Using AES with Wireshark

Figure 7 shows that when testing the login system before it was secured using the AES algorithm, the user's email and password were very easy to see because the data was still in plain text or original messages.

```
▼ HTML Form URL Encoded: application/x-www-form-urlencoded
  > Form item: "email" = "U2FsdGVkX19ctKUQeXrt4ot15vZjHsd5v6WZAumLG40="
  > Form item: "password" = "U2FsdGVkX190QuxCXOJwackTPyw5OQpy3wT2+k2GWmE="
```

Figure 8. Login System After Using AES with Wireshark

Figure 8 shows the results of the login system test, where the test uses the wireshark tool to analyze the network accessed by wifi. The results obtained are that the email and password are successfully encrypted and cannot be seen by hackers who want to take user data.

```
6  sec-ch-ua-mobile: ?0
7  sec-ch-ua-platform: "Windows"
8  Upgrade-Insecure-Requests: 1
9  Origin: http://localhost
10 Content-Type: application/x-www-form-urlencoded
11 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.3
12 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avi
13 Sec-Fetch-Site: same-origin
14 Sec-Fetch-Mode: navigate
15 Sec-Fetch-User: ?1
16 Sec-Fetch-Dest: document
17 Referer: http://localhost/wisata/
18 Accept-Encoding: gzip, deflate
19 Accept-Language: en-US,en;q=0.9
20 Cookie: PHPSESSID=ro4rirhc4p84u56mdiphdt8t24
21 Connection: close
22
23 email=rezkifee%40gmail.com&password=12345&submit=
```

Figure 9. Testing the Login System Before Using AES with Burpsuite

Figure 10. Testing the Login System After Using AES with Burpsuite

Figure 10 is the result of the login system test, where the test uses the burp suite tool to analyze the network accessed by wifi. The results obtained are that the email and password are successfully encrypted and cannot be seen by hackers who want to take user data.

4. Conclusions

Based on the results of the research conducted, it was concluded that the application of the AES (Advanced Encryption Standard) algorithm to the login system of an e-commerce website is highly recommended to be used to improve user data security. By implementing the AES algorithm in the login system, e-commerce websites can secure user data such as Email and Password. The AES algorithm works by encrypting data using a key that is only known to the server and authorized users. This prevents unauthorized access to sensitive user information. The AES algorithm works well so that user data cannot be seen by hackers because the data is already in cipher text. There are several things to consider when you want to use the AES Algorithm as security on the login system, namely the key used must be confidential and avoid key leakage to unauthorized parties. Wireshark and Burp Suite tools can be used in website testing to find out whether the website has security or not by analyzing or scanning the website to be tested.

References

Agunawan, Dirwan, Kamaluddin, L. A., Nianty, D. A., Ifani, A. Z., Paula, E. W., Cahyani, W., & Mustamin, M. A. (2023). PEMANFAATAN TEKNOLOGI INFORMASI DAN LAPORAN KEUANGAN UNTUK MENINGKATKAN DAYA SAING DI ERA

SOCIETY 5.0. *Nobel Community Services Journal*, *3*(1), Article 1. https://doi.org/10.37476/ncsj.v3i1.4199

A'LAA HUSSEIN ALI, EKHLAS KHALAF GBASHI, HAYA ALASKAR, & ABIR JAAFAR HUSSAIN. (2024). A Lightweight Image Encryption Algorithm Based on Secure Key Generation. *IEEE Access*.

Al-Khafaji, B. J., & Rahma, A. M. S. (2024). *A Modern Encryption Approach to Improve Video Security as an Advanced Standard Adopted*.

Aminu, Y., & Ichwani, A. (2024). Penggunaan Algoritma User-Based Collaborative Filtering Pada Aplikasi E-Commerce Berbasis Website Pada Toko Pakaian Biostuff.id. *Simetris: Jurnal Teknik Mesin, Elektro dan Ilmu Komputer*, *15*(1), Article 1. https://doi.org/10.24176/simet.v15i1.10719

Dam, D.-T., Tran, T.-H., Hoang, V.-P., Pham, C.-K., & Hoang, T.-T. (2023). A Survey of Post-Quantum Cryptography: Start of a New Race. *Cryptography*, *7*(3), Article 3. https://doi.org/10.3390/cryptography7030040

Dung, L. H. (n.d.). *A TYPE OF POST – QUANTUM CRYPTOGRAPHIC ALGORITHM*. *13*(01).

Hilmi, M. A. A., & Yunan, R. K. (2022). Pengujian Keamanan Fitur Upload File pada Sistem Aplikasi Web. *Jurnal Informatika: Jurnal Pengembangan IT*, *7*(1), 37–42. https://doi.org/10.30591/jpit.v7i1.3336

Husain, H., Mite, E., Azhar, R., Widyawati, L., & Apriani, A. (2023). Distribution Network Expansion Analysis Using Branching Optical Distribution Point (ODP) and Fiber Optic Attenuation (FO) Methods. *Jurnal Bumigora Information Technology (BITe)*, *5*(1), Article 1. https://doi.org/10.30812/bite.v5i1.2959

Ifani, A. Z., Aspar, N. F., Setiawan, A. D., & Azlam, M. (2024). Pengujian Keamanan Sistem Informasi Data Kependudukan Menggunakan Metode Pentetration Testing. *Jurnal Fokus Elektroda : Energi Listrik, Telekomunikasi, Komputer, Elektronika Dan Kendali)*, *9*(2), Article 2.

Ignasius, A., & Sakti, D. V. S. Y. (2022). PENERAPAN ALGORITMA AES (ADVANCE ENCRYPTION STANDART) 128 UNTUK ENKRIPSI DOKUMEN DI PT. GUNUNG GEULIS ELOK ABADI. *SKANIKA: Sistem Komputer dan Teknik Informatika*, *5*(1), Article 1. https://doi.org/10.36080/skanika.v5i1.2118

Insani, R. (2023). *Analisis Keamanan Informasi pada Website Menggunakan Aplikasi Wireshark*. https://doi.org/10.13140/RG.2.2.21696.71680

Judijanto, L., Zulkifli, Z., Utami, E. Y., Lamatokan, S. C., & Isma, A. (2024). Analisis Peran Teknologi Internet of Things (IoT), Literasi Digital, dan Kolaborasi Industri dalam Meningkatkan Kualitas SDM dalam Industri Manufaktur di Indonesia. *Jurnal Multidisiplin West Science*, *3*(01), Article 01. https://doi.org/10.58812/jmws.v3i01.945

Laia, S., & Barmawi, A. M. (2024). Strengthening the Authentication Mechanism of Blockchain-Based E-Voting System Using Post-Quantum Cryptography. *Jurnal Online Informatika*, *9*(2), Article 2. https://doi.org/10.15575/join.v9i2.1305

Riadi, I., Herman, & Ifani, A. Z. (2021). Optimasi Keamanan Web Server terhadap Serangan Broken Authentication Menggunakan Teknologi Blockchain. *JISKA (Jurnal Informatika Sunan Kalijaga)*, *6*(3), Article 3. https://doi.org/10.14421/jiska.2021.6.3.139-148

Riadi, I., Ifani, A., & Kusuma, R. (2022). Optimization and Evaluation of Authentication System using Blockchain Technology. *Emerging Science Journal*, *4*, 225–240. https://doi.org/10.28991/esj-2021-SP1-015

Sinlae, F., Maulana, I., Setiyansyah, F., & Ihsan, M. (2024). Pengenalan Pemrograman Web: Pembuatan Aplikasi Web Sederhana Dengan PHP dan MYSQL. *Jurnal Siber Multi Disiplin*, *2*(2), 68–82. https://doi.org/10.38035/jsmd.v2i2.156

Sirmayanti, S., Tain, A., & Hamzidah, N. K. (2023). Comparative Study of QoS on Video Meeting Tool Application in 4G LTE Network using Wireshark. *SISTEMASI*, *12*(1), Article 1.

Sonko, S., Ibekwe, K. I., Ilojianya, V. I., Etukudoh, E. A., & Fabuyide, A. (2024). QUANTUM CRYPTOGRAPHY AND U.S. DIGITAL SECURITY: A COMPREHENSIVE REVIEW: INVESTIGATING THE POTENTIAL OF QUANTUM TECHNOLOGIES IN CREATING UNBREAKABLE ENCRYPTION AND THEIR FUTURE IN NATIONAL SECURITY. *Computer Science & IT Research Journal*, *5*(2), Article 2. https://doi.org/10.51594/csitrj.v5i2.790

Sulaimon, H.A, O., N. (n.d.). Design and Implementation of Secured E-commerce Digital Learning for the Educational System in Nigeria. *Faculty of Natural and Applied Sciences Journal of Mathematics and Science Education*, *5*(4), 23–32.