South Asian Journal of Engineering and Technology Research Article

Open Access Full Text Article 121(2022) 41-47 DOI: 10.26524/sajet.2022.12.07

Sims: atext-based information system using symmetric and asymmetric algorithm

Haidee A. Viñalon[a], Ariel L. Tomagan[b]

[a] Taguig City University- College of Information Communication and Technology Department
[b] Taguig City, Philippines

Corresponding author.
Correspondence: Haidee A. Viñalon
E-mail: havianlon@gmail.com

Article info
Received 25th November 2021
Received in revised form
21 January2022 Accepted 15
March 2020

Keywords
Asymmetric, Symmetric,
Encryption, Private Key, Public Key

Abstract
Information security is today's everybody's concern. Technology keeps on increasing however the issue of information theft are getting higher. The confidentiality, integrity and availability of information are being compromised and always at risk though information security are keeps on improving. This study aimed to build an information security using a text-based platform to store the data and preserved its confidentiality, integrity and availability. The study will focus on the security of information and its confidentiality, integrity, and availability. An information system was developed using Java. Once the user started to process the data, the system will automatically create a text file where data inputted from the system will be are stored. The system will generate text-based formats per user. Another text file pass dot(.) txt whew passwords are stored. The data or information are stored in different text files. The transaction data and passwords are encypted using asymmetric algorithms. Each user account should have a private key to be able to access the data. Once the user is log in to the system, user will use a public key to able to access the data. Moreover, the text files where the passwords are kept and the text files where data are stored will be encrypted using symmetric algorithm which uses a public key to all users. The researcher used descriptive research design in the project. Descriptive research is being used by the proponents to describe the assessment of the respondents in the security of an information.

I. INTRODUCTION

Information security is today's everybody's concern. According to the article of Securimagazine, the total number of data breaches through September 30, 2021 has already exceeded the total number of events in 2020 by 17%, with 1,291 breaches in 2021 compared to 1,108 breaches in 2020 (Securitymagazine, 2021). Technology keeps on increasing however the issue of information theft are getting higher. The confidentiality, integrity and availability of information are being compromised and always at risk though information security are keeps on improving. According to (Zhen-Yu Wu, 2010) secure authentication scheme will thus be need to safeguard data integrity, confidentiality, and availability. Encryption is an old tool however still very effective to secure information. Accordin to (Abdullah, AM, 2017) It is extremely difficult to hackers to get the real data when encryption by AES algorithm.

Encryption is the process of encoding data to avoid it from intruders to read the original data easily. This stage has the ability to convert the original data (Plain text) into unreadable format known as Cipher text.

Encryption

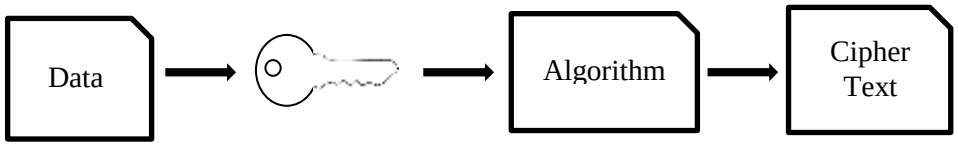

Figure 1. Encryption Process

The next process that has got to perform by authorized person is Decryption. In order to return the cipher text to its original form, a decryption process is needed. It's the method to convert cipher text into plain text without missing any words within the original text. To perform this process cryptography relies on mathematical calculation together with some substitutions and permutations with or without a key.

Decryption

Figure 2. Decryption Process

The symmetric key is more effective and faster than Asymmetric. Some of the common symmetric algorithm is Advance Encryption Standard (AES), Blowfish, Simplied Data Encryption Standard (S-DES) and 3DES. Asymmetric Encryption encrypts and descrypt the information using two separates yet mathematically connected cryptographic keys. The keys are known as "Public Key" and a "Private Key".

Information security is must in every system however it is very difficult to maintain it due to the technology used by informationtheft and hackers. We cannot stop hackers from hacking the system bur we can do something not to compromise the confidentiality and integrity of data. The proponents goal it to prevverse the confifentiality and integrity of information by using asymmetric and symmetric encryption algorithm.

Asymmetric Algorithm

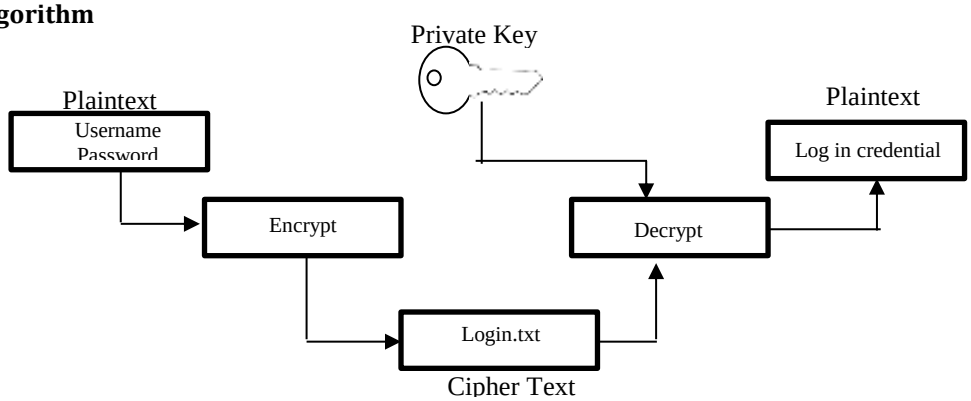

Figure 3. Encryption using Private key. Asymmetric Algorimth

The diagram shows that login credentials are encrypted/decrypted using a Private key.

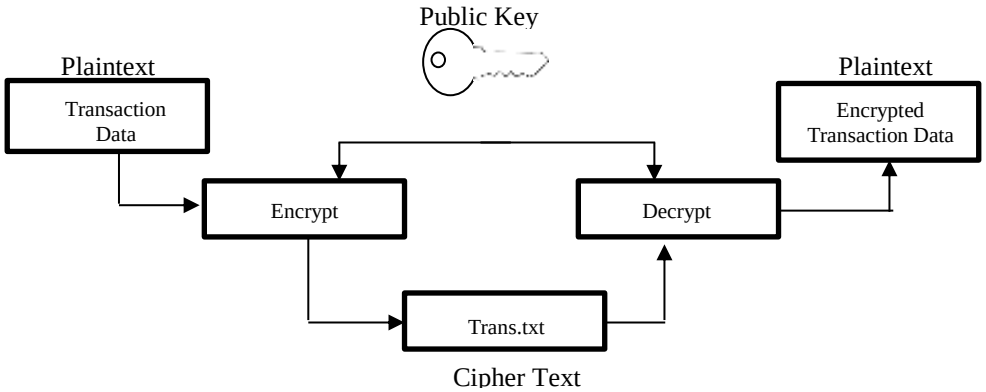

Figure 4. Encryption using Public key. Asymmetric Algorithm

Diagram shows that the transaction data are being encrypted/decrypted using a public key.

The two previous diagrams shows that asymmetric algorithm needs both private key and public key to be able to do transactions into the system, the login credentials are encrypted/decrypted using a private key. Moreover, after login-in, the user can perform transaction processes and the data are being encrypted/decrypted using a public key. The entire process is a asymmetric algorithm.

Symmetric Algorithm

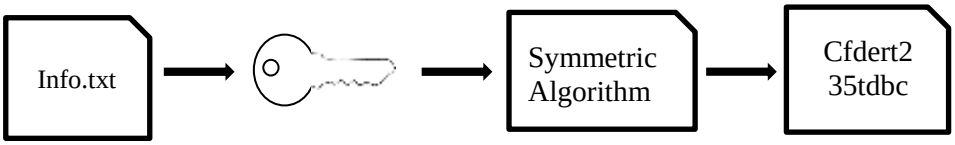

Figure 5. Encryption using Public key. Symmetric Algorithm

The diagram shows that the file name which originally in TXT format will be encrypted. The process of encryption/decryption is an example of symmetric algorithm and will be converted into encrypted format.

The two algorithms, asymmetric and symmetric, when work together, will tighthen the data security, hence will further preserve the confidentiality and integrity of the information.

II. LITERATURE REVIEW

The recent studies have indicated that cryptography uses a different method of encrypting data and decrypting data from sender to receiver sides. Symmetric and Asymmetric Algorithms are the main types of Cryptography. In symmetric key encryption use the same key among the encryption as well decryption techniques. The key advantage of this algorithm is that it requires less computing power and it works fast during the encryption process. According to (Panhwar et al., 2019) The symmetric approach combines the same key for both encryption and decryption, whereas the asymmetric algorithm requires a separate key for both encryption and decryption.

Symmetric encryption is a typical method wherein the encryption key and the decryption key are the same. A computer may generate a relatively strong, smaller key based on the algorithm it performs to encrypt data in a relatively short amount of time and hence for a relatively little amount of money. Thereafter, the key is transmitted to the end-user, eho uses it for decryption while asymmetric encryption generates two different keys, one private and one public. These keys are not the same, and the public key may be shared with anybody, while the private key can ony be shared with those who have permission to access the data.

Based on the study of (Misha and Birudu, 2017) states that encryption has two drawbacks. First, keyword protection may be ensured only for keywords that are a prior difficult to guess by the adversary. Second, because the encryption is deterministic, some reports of an information flow must inevitably go via the cipher tect of the keywords. As a result, encryption is only usable in limited circumstances.

According to Connor H. (2020), Cryptography's main goal is to provide a variety of solutions for achieving security privacy. It's useful within today's computer networks in addition to safety improvements. A recent study by Sardar (2020) concluded that traditional techniques are no longer viable in today's generation. A massive system of electronic communication, commerce, and intellectual property that would otherwise be intercepted by those with hostile motives must be secure across continents. There are four essential goals in Cryptography (1) Data Confidentiality, (2) Identification and Authentication, (3) Integrity, and (4) Non-Repudiation. This paper also elaborates the fields mentioned: Data Confidentiality requires the protection of information from unauthorized access. This is performed by encrypting a sent message using a key known to both the sender and recipient. An interceptor may be able to get an encrypted message, but not decrypt it. Furthermore, it shows how encryption is being used in making information "Confidentiality". Identification and Authentication, is the process of identifying an object or a user before initiating communication or other operations. Further communication can begin once the Sender has authenticated the Recipient. It reveals how authentication works in one direction. Although the actual procedure is far more complicated, they use this simple example to demonstrate the fundamentals of cryptography.). Integrity, in storage or transit, information must not be altered. Any changes must be detectable. Message Digesting Algorithms, such as SHA-2 and, more recently, SHA-3, are used in modern cryptography applications. Non-Repudiation, the message's creation/transmission cannot be denied. This gives a transaction "digital" legality and traceability. The paper also provides a simplified representation of the digital signature production, transmission, and verification processes.

Developers should identify and secure any sensitive data, even if it is stored on the hard disk. They must ensure the sensitive data cannot be easily overwritten. It is best to keep these secrets hidden even from the administrator (Varecode, 2021).

III. RESEARCH METHODOLOGY

The researchers used descriptive research design in the study. Descriptive research design is being used by the proponents to explain the evaluation in terms of securiting the information. Descriptive research is mainly done because the researcher wants to gain a better understanding for a topic.

The respondents of this study are the Taguig City University- College of Information Communication Technology, MIS Department personel and IT Professional who have the enough knowledge technically and in the development of computerized system.

The proponent used the survey questionnaire for acquisitions of the perceptions of the respondents with regards to design features of the development systems that are capable in terms of its accuracy, reliability, usability and maintainability. For computing weigthed mean, likert scale (five-point rating scale) and percentage is used to evaluate the assessment of the respondent's opinion on the study.

IV. FINDING AND DISCUSSION

The proponents conducted a survey to learn about the needs and wishes of the users. The turn out of the survey findings are great, and respondents are amazed with regrads to how information security are handled in the information system. As a result, proponents conclude that in terms of development and implementation, the approach is both viable and for long-term. The program will protect the system information, it confidentiality, integrity, and availability. The method of protecting the data or information uses two different encryption algorithms that surely thighten the information security.

Evaluation of IT Professional, MIS, and CICT Professors at Taguig City University on the proposed SIMS: A Text-Based Infomration System using Symmetric and Asymmetric Algorithm based on ISO/IEC 25010 in terms of the following variables:

Table 1. Table for Functional Suitability

Indicators	IT Professional		MIS Personnel		CICT Professor			Average
	W. M.	Interpretation	W. M.	Interpretation	W. M.	Interpretatio n	W. M.	Interpretation
Functional Completeness	4.75	Excellent	4.50	Excellent	4.71	Excellent	4.65	Excellent
Fucntional Correctness	4.75	Excellent	4.67	Excellent	4.29	Very Satisfactor	4.57	Excellent
Functional Appropriateness	4.75	Excellent	4.67	Excellent	4.57	Excelent	4.66	Excellent
Overall Weighted Mean	4.75	Excellent	4.61	Excellent	4.52	Excelent	4.63	Excellent

Table 1 presents the evaluation of IT Professionals, MIS Personnel and CICT Professors at Taguig City University on the proposed SIMS: A Text-Based Information System using Symmetric and Asymmetric Algorithm in terms of Functional Suitability. It was revealed that the overall weighted mean of the indicators has a rating of 4.63 which is interpreted as "Excellent". It also shows that all respondents evaluated the proposed system as "Excellent". It can be seen that the IT Professionals garnered the higher rate of 4.75 compared to the CICT Professors who obtained 4.52. It is also shown that the indicative statement "Functional Appropriateness" garnered the highest rating of 4.66 which is interpreted as "Excellent", while the indicative statement "Functional Correctness" obtained the lowest rating of 4.57 which was interpreted as "Excellent". This means that the proposed system is functionally compliant but needs to enhance its functional correctness.

Table 2. Table for Performance Efficiency

Indicators	IT Professional		MIS Personnel		CICT Professor			Average
	W. M.	**Interpretation**	**W. M.**	**Interpretat ion**	**W. M.**	**Interpretation**	**W. M.**	**Interpretation**
Time Behavior	4.63	Excellent	4.33	Very Satisfactor	4.86	Excellent	4.62	Excellent
Resource Utilization	4.88	Excellent	4.33	Very Satisfactor	4.57	Excellent	4.59	Excellent
Capcity	4.63	Excellent	4.33	Very Satisfactor	4.71	Excellent	4.56	Excellent
Overall Weighted Mean	4.71	Excellent	4.33	Very Satisfactor	4.71	Excellent	4.59	Excellent

Table 2 presents the evaluation of IT Professionals, MIS Personnel and CICT Professors at Taguig City University on the proposed SIMS: A Text-Based Information System using Symmetric and Asymmetric Algorithm in terms of Performance Efficiency. It was revealed that the overall weighted mean of the indicators has a rating of 4.59 which is interpreted as "Excellent". It also shows that both IT professionals and CICT Professors evaluated the proposed system as "Excellent" and MIS Personnel as "Very Satisfactory". It can be seen that both IT Professionals and CICT Professors garnered a higher rate of 4.71 compared to MIS who only obtained 4.33. It is also shown that the "Time Behavior" garnered the highest rating of 4.61 which is interpreted as "Excellent", while the indicative statement "Resource Utilization" obtained the lowest rating of 4.59 which is interpreted as "Excellent". This means that the proposed system is functional compliant but needs to enhance its Resource Utilization.

Table 3. Table for Usability

Indicators	IT Professional		MIS Personnel		CICT Professor			Average
	W. M.	Interpretation	W. M.	Interpretation	W. M.	Interpretation	W. M.	Interpretation
Appropriateness Recognizability	4.88	Excellent	4.17	Very Satisfactor	4.43	Very Satisfactor	4.49	Very Satisfactor
Learnability	4.63	Excellent	4.67	Excellent	4.29	Very Satisfactor	4.53	Excellent
Operability	4.88	Excellent	4.50	Excellent	4.43	Very Satisfactor	4.60	Excellent
User Error Protection	4.88	Excellent	4.50	Excellent	4.57	Excellent	4.65	Excellent
User Interface Aesthetic	4.00	Very Satisfactor	4.33	Very Satisfactor	4.43	Very Satisfactor	4.25	Very Satisfactor
Accesibility	4.88	Excellent	4.67	Excellent	4.2	Very Satisfactor	4.61	Excellent
Overall Weighted Mean	4.69	Excellent	4.47	Excellent	4.40	Excellent	4.52	Excellent

Table 3 presents the evaluation of IT Professionals, MIS Personnel and CICT Professors at Taguig City University on the proposed SIMS: A Text-Based Infromation System using Symmetric and Asymmetric Algorithm in terms of Usability. It was revealed that the overall weighted mean of the indicators has a rating of 4.52 which is interpreted as "Excellent". It also shows that both MIS and CICT Professionals evaluated the proposed system as "Very Satisfactory". It can be seen that the IT Professors garnered the highest rating of 4.69 compared to the CICT Professors who only obtained 4.40. It is also shown that the "User Error Protection" garnered the highest rating of 4.65 which is interpreted as "Excellent", while the indicative statement "User Interface Aesthetics" obtained the lowest rating of which 4.25 is interpreted as "Very Satisfactory". This means that the proposed system is functionally compliant but needs to enhance its user interface aesthetics.

Table 4. Table for Reliability

Indicators	IT Professional		MIS Personnel		CICT Professor			Average
	W. M.	Interpretation	W. M.	Interpretation	W. M.	Interpretation	W. M.	Interpretation
Maturity	5.00	Excellent	3.67	Very Satisfactor	4.71	Excellent	4.46	Very Satisfactor
Availability	4.63	Excellent	3.67	Very Satisfactor	4.71	Excellent	4.34	Very Satisfactor
Fault Tolerance	4.75	Excellent	3.83	Very Satisfactor	4.29	Very Satisfactor	4.29	Very Satisfactor
Recoverability	4.88	Excellent	3.67	Very Satisfactor	4.71	Excellent	4.42	Very Satisfactor
Overall Weighted Mean	4.81	Excellent	3.71	Very Satisfactor	4.61	Excellent	4.38	Very Satisfactor

Table 4 presents the evaluation of IT Professionals, MIS Personnel and CICT Professors at Taguig City University on the proposed SIMS: A Text-Based Information System using Symmetric and Asymmetric Algorithm in terms of Reliability. It was revealed that the overall weighted mean of the indicators has a rating of 4.38 which is interpreted as "Very Satisfactory". It also shows that both IT Professionals and CICT Professors evaluated the proposed system as "Excellent". It can be seen that the IT Professionals garnered a higher rate of

4.81 compared to the MIS who only obtained 3.71 . It is also shown that the indicative statement "Maturity" garnered the highest rating of 4.46 which is interpreted as "Very Satisfactory", while the indicative statement "Fault Tolerance" obtained the lowest rating of 4.29 which is interpreted as "Very Satisfactory". This means that the proposed system is functionally compliant but needs to enhance its fault tolerance.

Table 5. Table for Security

Indicators	IT Professional		MIS Personnel		CICT Professor			Average
	W. M.	Interpretation	W. M.	Interpretation	W. M.	Interpretation	W. M.	Interpretation
Confidentiality	4.75	Excellent	3.83	Very Satisfactor	4.57	Excellent	4.38	Very Satisfactor
Integrity	4.63	Excellent	3.83	Very Satisfactor	4.86	Excellent	4.44	Very Satisfactor
Non-repudiation	4.75	Excellent	3.67	Very Satisfactor	4.57	Excellent	4.33	Very Satisfactor
Authenticity	4.63	Excellent	4.00	Very Satisfactor	4.43	Excellent	4.35	Very Satisfactor
Overall Weighted Mean	4.69	Excellent	3.83	Very Satisfactor	4.61	Excellent	4.38	Very Satisfactor

Table 5 presents the evaluation of IT Professionals, MIS Personnel and CICT Professors at Taguig City University on the proposed SIMS: A Text-Based Information System using Symmetric and Asymmetric Algorithm in terms of Security. It was revealed that the overall weighted mean of the indicators has a rating of 4.38 which is interpreted as "Very Satisfactory". It also shows that both IT Professionals and CICT Professors evaluated the proposed system as "Excellent". It can be seen that the IT Professionals garnered a higher rate of 4.69 compared to the MIS who only obtained 3.83. It is also shown that the indicative statement "Integrity" garnered the highest rating of 4.44 which is interpreted as "Very Satisfactory", while the indicative statement "Non-Repudiation" obtained the lowest rating of 4.33 which is interpreted as "Very Satisfactory". This means that the proposed system is functionally compliant but needs to enhance its non- repudiation.

Table 6. Table for Maintainability

Indicators	IT Professional		MIS Personnel		CICT Professor			Average
	W. M.	Interpretation	W. M.	Interpretation	W. M.	Interpretation	W. M.	Interpretation
Reusability	4.63	Excellent	4.33	Very Satisfactor	4.57	Excellent	4.51	Excellent
Analyzeability	4.75	Excellent	4.33	Very Satisfactor	4.86	Excellent	4.65	Excellent
Overall Weighted Mean	4.69	Excellent	4.33	Very Satisfactor	4.72	Excellent	4.58	Excellent

Table 6 presents the evaluation of IT Professionals, MIS Personnel and CICT Professors at Taguig City University on the proposed SIMS: A Text-Based Information System using Symmetric and Asymmetric Algorithm in terms of Maintainability. It was revealed that the overall weighted mean of the indicators has a rating of 4.58 which is interpreted as "Excellent". It also shows that both IT Professionals and CICT Professors evaluated the proposed system as "Excellent". It can be seen that the CICT Professors garnered a higher rate of 4.72 compared to MIS who only obtained 4.33. It is also shown that the indicative statement "Analyze Ability" garnered the highest rating of 4.65 which is interpreted as "Excellent", while the indicative statement "Reusability" obtained the lowest rating of 4.51 which is interpreted as "Excellent". This means that the proposed system is functionally compliant but needs to enhance its reusability.

V. CONCLUSION AND FURTHER RESEARCH

Conclusion

On the forgoing significant finding, the following conclusions were derived:

1. The respondents were working as faculty of College of Information and Communication Technology Department, MIS Department personnel and as well as some IT Perfessional.
2. Majority of the respondents are aware with information security.
3. Majority of the respondents rated the overall function of the information system Excellent.
4. The respondents assessed the security features of the information system attain its goal.

Recommendation

Based on the results from the surveys of the Text-based Information System using Symmetric and Asymmetric Algorithm, it was given highly recommended ratings by the respondents which are CICT professors and staff fom MIS department. The respondents appreciate the new way of developing system and securing information inputted from the system. However, to further enhance the capability of the information security, it is recommended that:

1. Enhance the security by developing information system as a mobile appilicetion.
2. Enhance the security by storing the text-based file into cloud.

Therefore, it is heighly recommended the use of asymmetric and symmetric algorithm in securing information and should continuously be modified to further enhance the condifentiality, integrity and availability of the information.

REFERENCES

1. https://www.securitymagazine.com/articles/96667-the-top-data-breaches-of-2021
2. Zhen-Yu Wu, Yueh-Chun Lee, Feipei Lai, et al. (2020). A Secure Authentication Scheme for Telecare Madecine Information Systems.
3. Abdullah, Ako Muhamad (2017). Advance Encryption Standard (AES) Algorithm to Encrypt and Decrypt Data.
4. Ibrahim, Mr S. Jafar Ali, K. Singaraj, P. Jebaroopan, and S. A. Sheikfareed. "Android Based Robot for Industrial Application." *International Journal of Engineering Research & Technology 3, no. 3 (2014).*
5. Panhwar, Muhammad Aamir, Khuhro, Sijjad Ali, Panhwar, Ghazala, Memon, Kamran Ali (2019). SACA: A Study of Symmetric and Asymmetric Cryptographic Algorithms. Vol. 19 No. 1, IJCSNS International Journal of Computer Science and Ntework Security.
6. Shelupanov, Alexander, Evsyutin, Oleg, Konev, Anton, et al. (2019). Information Security Methods – Modern Research Directions
7. Jeyaselvi, M., M. Sathya, S. Suchitra, S. Jafar Ali Ibrahim, and N. S. Kalyan Chakravarthy. "SVM-Based Cloning and Jamming Attack Detection in IoT Sensor Networks." *Advances in Information Communication Technology and Computing, pp. 461-471. Springer, Singapore, 2022.*
8. Karthikeyan, B., K. Alhaf Malik, D. Bujji Babbu, K. Nithya, S. Jafar Ali Ibrahim, and NS Kalyan Chakravarthy. "Survey of Cooperative Routing Algorithms in Wireless Sensor Networks." *Annals of the Romanian Society for Cell Biology (2021): 5316-5320*
9. Sarma, D. (2018). An Asymmetric Key based Disk Encryption Scheme. International Journal of Computer Applications, 181(24), 26–27. https://doi.org/10.5120/ijca2018918030
10. Sami, M., Bhatti, S., Baloch, J., & Shah, S. (2018). How to keep your systems records safe. International Journal of Information Technology, 11(2), 287–293. https://doi.org/10.1007/s41870-018-0104-5