International Journal of Computing Sciences Research (ISSN print: 2546-0552; ISSN online: 2546-115X)
Vol. 5, No. 1, pp. 584-594
doi: 10.25147/ijcsr.2017.001.1.59
https://stepacademic.net

Short Paper

Modified Transposition Using TDEA Encryption for FishCoral-PRSA Management System

Benedicto B. Balilo Jr.
Bicol University, Legazpi City, Philippines
bjbbalilo@bicol-u.edu.ph
(corresponding author)

Ronnel R. Dioneda Sr.
Bicol University, Legazpi City, Philippines
rsrdioneda@bicol-u.edu.ph

YungCheol Byun
Jeju National University, South Korea
yungcheolbyun@gmail.com

Date received: September 20, 2020
Date received in revised form: November 17, 2020
Date accepted: November 17, 2020

Recommended citation:

Balilo Jr, B. B., Dioneda Sr., R. R., & Byun, Y. C. (2021). Modified transposition using TDEA encryption for FishCoral-PRSA management system. *International Journal of Computing Sciences Research*, 5(1), 584-594. doi: 10.25147/ijcsr.2017.001.1.59

Abstract

Purpose – The purpose of this study is to developed an encryption technique with a modified transposition technique using TDEA for FishCoral-PRSA Management Information System. A project component of Participatory Resource and Socio-Economic Assessment (PRSA) was implemented under the Fisheries, Coastal Resources and Livelihood (FishCORAL) project of the Bureau of Fisheries and Aquatic Resource of Department of Agriculture (DA-BFAR).

Method – The developed encryption algorithm followed the concept of a rational unified process. The characteristics of the existing transposition and 3DES algorithms were analyzed including the plaintext parameters, entropy, block size, and others. The algorithm was developed in PHP language and simulated through login authentication to evaluate the ciphertext and speed performance.

Results – Businesses and organizations are providing security mechanisms to prevent security breaches or attacks to the system which could result in data loss and disruption of service with cost to the organization. The results of this study aimed to introduce a new encryption algorithm by merging the features of the transposition technique and characteristics of the 3DES algorithm placing several parameters (as salt) in the entropy. Thus, it reveals that the results in-placed with reference code generated a complex ciphertext—a challenge to consider in the future.

Conclusion – The developed algorithm makes use of modified transposition in 2-layered order and 3DES algorithm to secure the login account. The encryption and decryption times were 0.15044 ms and 0.78666 ms, respectively. The encryption sequence order follows the row read-off order while the decryption implemented a column read-off sequence order based on defined column order. The transposition sequencing added ingredients to the encryption process and generated a complex symbol.

Recommendations – There is no detailed approach on how to prevent an attack and avoid security breaches in the system. A complex or simple idea that led to the introduction of a new encryption algorithm provides an opportunity for login authentication, protection for file content, and securing transactions and messages.

Research Implications – The developed algorithm is significant to the FishCoral-PRSA project as this offers exclusivity to the system features especially user login authentication. Furthermore, this offers challenges and opportunities, especially for cybersecurity novice.

Keywords – cryptography, transposition cipher, 3DES, security, management system

INTRODUCTION

In recent years, cybersecurity played a crucial role in protecting an organization's information. Any security breaches or attacks to the system could result in data loss or assets and disrupt the service with cost to the organization. According to Cyber Security Breaches Survey Report 2019, around 32% of businesses have reported breaches or attacks and some of the common types of attacks are phishing (80%), impersonation (28%), and 27% reported for viruses, spyware, or malware including random attacks (Department for Digital, Culture, Media, and Sport, 2019). Based on historical cybercrime figures the predicted damage could reach $6 trillion by 2021. The damage includes the destruction of data, stolen money, lost productivity, theft of intellectual property, theft of personal and financial data, embezzlement, fraud, post-attack disruption of normal business operation, and deletion of hacked data and system (Morgan, 2019). Because of this, many companies and organizations are generally becoming aware and cyber secure. They have integrated security in the planning activities, employed technical approach and

highly strategies, and provided secured defenses against any type of attacks. In the process, some have adopted a system to narrow breach detection, the establishment of hardware and software mechanisms, or employ a new method of encryption techniques.

The early encryption techniques were simply relying on transposition and substation (Kessler, 2017). Like, in the transposition technique, the plaintext is arranged in a grid and assigned a number (in column) ordering system. The symbols are shifted based on assigned order and those generate the ciphertext. The acceptance and recognition of transposition cipher open the way which attracted modern cryptanalysis to a generate complex symbol like combining other techniques, converting each character into its binary representation and convert to hexadecimal, and divide the plaintext symbols into blocks to generate complex ciphertext symbols.

Advances in technology led to an opportunity with greater encryption. The 3DES is derived from Data Encryption Standard (DES) which is a type of symmetric-key encryption that uses three (3) individual 56-bit keys (or 168-bit key) and will be deprecated in 2023 (Lake, 2019). At one time, many businesses and organizations including industries used 3DES to secure their information. Over the past years, a new encryption algorithm was developed challenging the advantages of not just 3DES but also other encryption techniques. Over the past years, several encryption techniques are presented either new or modification to the existing algorithm. This paper aims to modify the transposition in row sequencing order and utilize the 3DES algorithm to secure the account for PRSA users. This will generate a 6x6 grid with 36-bytes length from a combination of password and random character codes. The random characters will depend on the password to complete the length. It is always a challenge for researchers to develop an encryption algorithm that is free from attack. This combination will simplify the generation of the plaintext but manage to generate complex symbols.

LITERATURE REVIEW

In early encryption, substitution and transposition ciphers are commonly used. A substitution cipher is a technique that substitutes a different symbol at random points in the text. Caesar cipher substitution is the simplest and common technique in which each symbol in the plaintext is shifted. Due to its simplicity, many kinds of research have attempted to enhance the cipher technique. Imran and Abdulameerabdulkareem (2014) presented different methods from counting of words in the message to counting the characters of the first word in the message before applying the formula equal to *ciphertext= plaintext +4 mod 26*. The simplicity of which allows future and novice researchers to understand the concept of cryptography. To increase the strength and overcome the limitations of Caesar cipher, a randomized approach with double columnar transposition was proposed. The technique expanded the symbols by including all ASCII and extended ASCII characters to generate the keys from a single key to enhance security. The attacker needs to use 256 possible combinations of keys before the message will be decrypted (Jain, Dedhia, & Patil, 2015). Renuka Devi and Harshini (2019)

concluded that caesar cipher substitution has less encryption time compared to columnar transposition which is more complex and secure to use in encrypting a message.

According to Sokouti, Sokouti, and Pashazadeh (2009) transposition ciphers are stronger than simple substitution ciphers. The researchers added 8 bits equivalent to 1 character using two (2) mathematical functions and changed the position of the bits in the binary tree using the in-order tour. They concluded that the use of an in-order tour of the binary tree can highly protect the cipher with the secured key management process. Similarly, Al-Farraji (2015) proposed to use two (2) keys and delete some bits from plaintext after converting it to its binary code while putting the bits to another place in plaintext. While others are busy doing the enhancements, Wulandari, Rismawan, and Saadah (2015) simulated an attack using differential evolution--a permutation of integer problem. The simulations successfully decipher the message with 9 permutation length but generated half of the incorrect answers when the length has reached 10.

A continuous effort was encouraged to develop new cryptographic algorithms. In 1973, a publication notice was posted in the Federal Register where a group of cryptographers submitted a proposal called Data Encryption Standard (DES). DES is a 16-round Feistel block cipher with a 64-bit block size and is based on shuffling and substitution (Wilson, 2016). The primary factors of DES were speed and complexity which makes the algorithm attractive making it the building block for pseudorandom number generators and one-way hash function. It was also used in many crypto-based applications such as ATM pins, login passwords, smart cards (Atkins, 2004), email messages, video transmissions, stored data files, and internet digital content (Coppersmith et al., 1997). Because of the limited key size (64-bit), the algorithm becomes vulnerable to attack. Several attacks have been noted on DES such as exhaustive search, meet-in-the-middle attack, davies attack, differential cryptanalysis, and linear cryptanalysis (Biryukov, 2005). With this, many developments on DES took place such as 2DES and 3DES. Triple Data Encryption Algorithm (TDEA or 3DES) will officially disallow its use after 2023, which means the use of the algorithm and key length will no longer be allowed (Henry, 2018). Bhargavan and Leurent (2016) made a breakthrough when they demonstrated an attack on 3DES. The attack exploited the collisions on short block ciphers made on HTTPS to recover a secret session cookie and show that a similar attack on Blowfish can be used to recover HTTP BasicAuth credentials sent over OpenVPN connections. In the case of the proposed study, the transposition sequencing added ingredients to the process as the plaintext that will be subjected to 3DES encryption will still be subjected to reverse transposition to expose the plaintext.

METHODOLOGY

The study is a developmental type of research that utilized the features of rational unified process (RUP). The analysis of the existing characteristics of the transposition technique and TDEA allows the study to determine the opportunity leading to the

enumeration of the objectives. Figure 1 shows the conceptual framework which shall carry out the RUP phases.

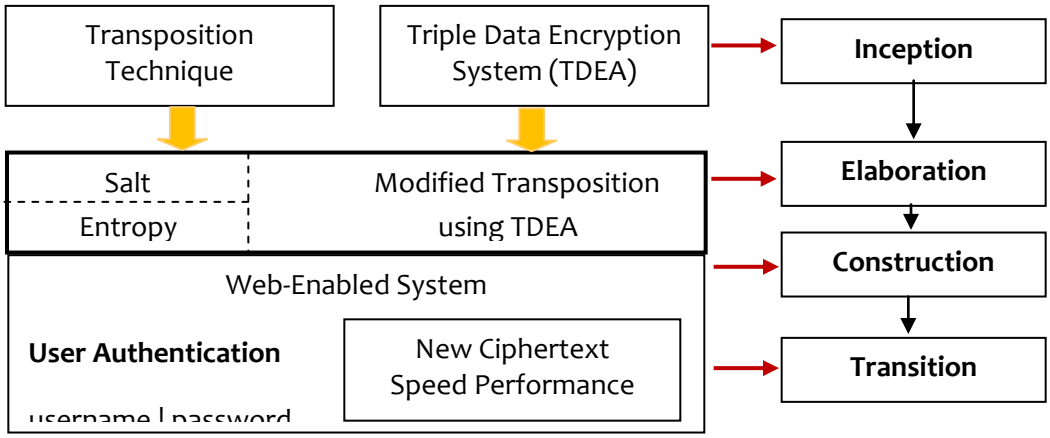

Figure 1. Conceptual Framework with RUP concept

The sources of entropy come from several parameters including sequence modifications of transposing the characters in the grid matrix. These formed the modified transposition using the TDEA algorithm used for encrypting and decrypting the login authentication process. Along with the enhancements, the algorithm was simulated using a web-enabled system for ciphertext analysis and performance evaluation.

RESULTS AND DISCUSSION

This section presents the results based on simulation conducted with the encoded password and system-generated reference code. The simulations are performed ten (10) times both for encryption and decryption of the text or symbols.

The Proposed Method

The transposition technique was the simplest method of hiding the message with simple operations the message was converted into complex symbols "ciphertext" which only the sender and the receiver understand. The technique has been exposed to several modifications including the sequence of transposing the characters in the grid matrix. In the proposed algorithm, the encryption and decryption process was transformed from column to row read-off sequence. Figure 2 shows the pseudocode of generating the plaintext. The plaintext is composed of a combination of the user password, random reference code, and another random symbol that completes the 36-bytes (288-bits) plaintext.

Similar to a one-time password (OTP) concept, the user needs to input the correct reference code to get the actual password. In this method, the code shall be part of the

information known to a user upon registration. The user has the freedom to reset the code in order not to compromise the account details.

To give complication to common plaintext generation, the study modified the transposition read-off sequence of the symbols in the matrix. Figure 3 presented the concept of placing the symbols in columns but read them in rows until they reached the last symbol.

1. *let reference_code = call function refcode*
2. *let pwd = password and reference_code*
3. *let length = length of pwd*
4. *let cntlen = 36 - length*
5. *if the length of pwd is less than or equal to cntlen*
6. *let pwdcnt = cntlen*
7. *let plain= call plain (pwd, pwdcnt)*
8. *else*
9. *let plain = actual password*

Figure 2. Pseudocode code of generating the plaintext

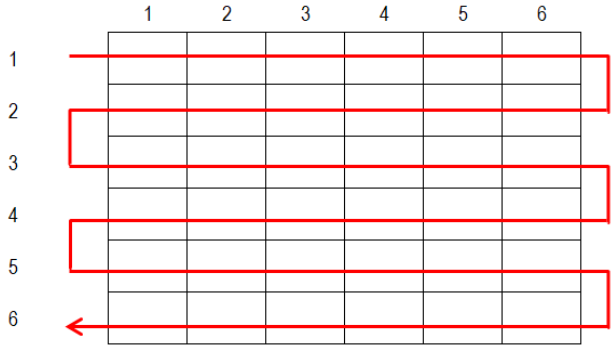

Figure 3. row read-off encryption transposition sequencing

The symbols are placed based on a defined column sequence. Given the password "*890YpU231*" and reference code "*Jde7*" *shall produce* "*890YpU231Jde7wmv7do2j7qpytjsbtojadoh*". And, setting the sequence order to [*4,2,5,1,3,6*] shall generate values "*o2y87o23t9wjj1joma7JsYvdqdbp7opetUdh*" following the row-read off sequence. The sequencing order complicates the plaintext to free the account from any form of attack. In decryption, the plotting of the symbols was in a row but used column read-off order to get the proper and arranged order of the plaintext (Figure 4).

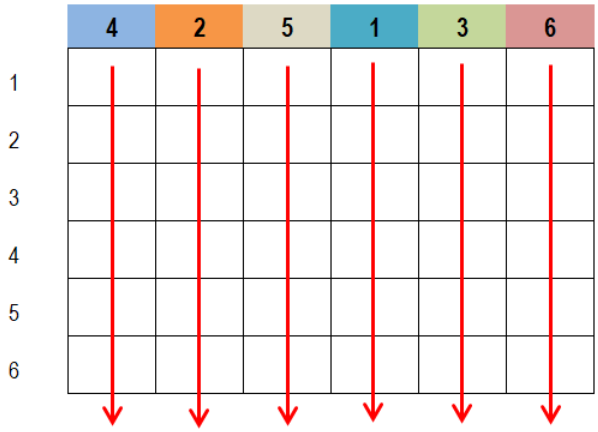

Figure 4. Column read-off transposition sequencing

To test the algorithm, a password random generator application was used. Table 1 presented the transposition results and encrypted text using a 3DES algorithm. The developed algorithm produced a complex symbol regardless of whether the password is simple or considered difficult. Commonly used passwords (*in blue colors*) like 111111, abc123, santosjose and considered difficult passwords *(in red colors*) like EfAMb8t, 890YpU231, and others generated a complex symbol with no trail of reflecting the original text. A total of 56-bytes (448-bits) characters were generated with a combination of alpha characters, numbers, and symbols.

Regardless of the password length, the system generated a random output. This performance showed the characteristics of good encryption. Even well-known encryption algorithms are prone to different kinds of attacks same with the developed algorithm. That's why cryptographers and researchers are continuously analyzing the current pieces of literature and security developments to secure and protect the information. In the study, the user performed login authentication wherein codes are stored in the database and inputted in an interface (see Table 1).

In Table 2, the speed performance of the developed algorithm was presented. With the inputted password and generated reference code, the system produced a statistically random output. The average encryption and decryption process was 0.15044 ms and 0.78666 ms, respectively. In the encryption process, the interval speed was 0.0030 ms (arranged from highest-lowest). This means combining the features of the two (2) algorithms does not affect the speed performance of the system and is considered useful in the authentication process (like this study).

For the decryption process, the results showed that there was a total difference of 0.6322 ms in the encryption and decryption cycle. Or, an average interval difference of 0.0138 ms per testing simulation. Interval difference means computing the previous speed performance versus the current performance (i.e., 0.7588 – 0.7981 would result in -

0.0393). Still, the decryption process has an average of 0.7866 ms which means it can process the request in less than 1 millisecond.

Table 1. Sample generated ciphertext using transposition and 3DES encryption algorithm

#	Password	Password Length	Reference Code	3DES
1	santosjose	10	u8ic	932Nkd25M+6xCynARjc6yz/MCmX89AuegzeIv2TiTIru9dFnzlyGAg==
2	millaminaX2020	14	elVK	7RmECkrAH11Zo+Y+263wgYdJ4P+1uyXT1sPEBi6YX7BPwnWy9aOaJQ==
3	Hy25william	11	TwIm	O9JKiRH9q3s7PEnVJzN9oisEGxGSP/yQmehUKs3uU9xwl/hSsxPItg==
4	Py89Xua	7	LAd3	izTNFyJn3rRo24uZ7H2hrcBqdrirrmgvfUPQByvubkhfekzqRaXwkw==
5	rey0987	7	Jjf4	Mxj1C6uq1zHrYyD9vPxtR2zAijHtoErfeFBV6C1BzdXp9NUytzzrHg==
6	EfAMb8t	7	4Vyv	DTaLhSZd+1OYnHMARAytVml4Rwqjg5YSmIKrbd0poRIIZeWzT7gvfQ==
7	111111	6	EuTx	CyA2jgBzyEw2DNToch3jZ4KKbs4lmv06tdF/ZaevA7tgWz+RQfOrLg==
8	v4zPM6f	7	fdrS	Upymyuh4wx6RXLWJS72MKW9sZwbRYTTunzTGKw2jlikUkMWRxGyAMw==
9	abc123	6	5zhH	8Rjld9RNLjXI8qAEIDOYdOi0Lox3UXIKaiV62GpshpVPoA0e9NGFMg==
10	890YpU231	9	9Blv	hSYOolusNHt6NfkL8ZdPpLfDbbj6AoEmToacGoUN/YRg0KkVuZyYaA==

The algorithm was used as part of the login authentication process for the Participatory Resource and Socio-Economic Assessment Management System to hide the password of the user. Figure 5 shows the login account interface for FishCoral-PRSA Management System. To access the system, the user needs to register and a reference code will be generated. The reference code shall serve as a second validation key aside from the assigned password.

Table 2. The speed performance of the developed algorithm

#	Transposed Symbols	Speed *(in ms)*	
		Encryption	Decryption
1	iEc10q2uj1lu4Tq1jdixs1inxtz1eazch1fc	0.1631	0.8613
2	1aiPzjpLwypdrAf84obdl9xx434Xitkutukj	0.1628	0.8550
3	wjmsi6dogacx3s3n550ektj78ugoxh98cssu	0.1618	0.8352
4	af0vgcffu4ihudlzrpzrkPg6xSsMp0ouq6o8	0.1604	0.7441
5	1tlEzzy4kfrisVyAqkaylMq3mvob972qj8u7	0.1528	0.7588
6	kliHw5lloyIftiy2mpna15uoxmqweqmTminp	0.1450	0.7981
7	qikm2u1n8i0u2a1leyuXnllcp2jaVn20pmKe	0.1440	0.7410
8	m5uai90zxb9nmhuc2rkHb14jmzv2roi8v3qs	0.1399	0.7771
9	47qrz34Jqe0uvjuyg9ff506ua4w9tr5ps85j	0.1389	0.7590
10	62r8vlt3c9e701s05cj9xYipiB5pqwnldUqq	0.1357	0.7370
		0.1504	0.7866

***** *recorded less performance in interval testing simulation (previous - current)*

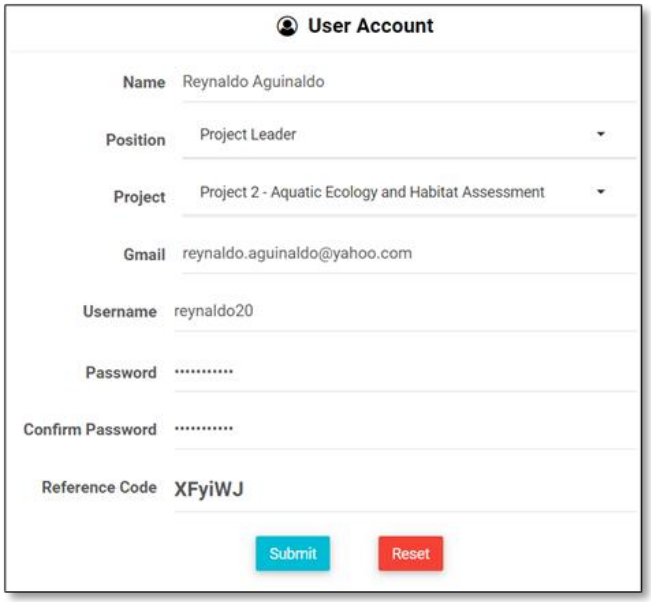

Figure 5. Login account interface for FishCoral-PRSA Management System

CONCLUSIONS AND RECOMMENDATIONS

The developed algorithm makes use of modified transposition in 2-layered order and 3DES algorithm to secure the login account. The encryption and decryption times were 0.15044 ms and 0.78666 ms, respectively. The encryption sequence order follows the row read-off order while the decryption implemented a column read-off sequence order based on defined column order. The transposition sequencing added ingredients to the encryption process and generated a complex symbol. The developed algorithm can be used as login security encryption for user validation, file content, transaction, and messages.

ACKNOWLEDGEMENT

The Participatory Resource and Socio-economic Assessment (PRSA) was funded by the Bureau of Fisheries and Aquatic Resources (BFAR) of the Department of Agriculture under the FishCoral Project in partnership with Bicol University (BU) as the lead institution and Partido State University, Masbate Institute of Fisheries and Technology (MIFT), Camarines Sur Institute of Fisheries and Marine Sciences (CASIFMAS), and Ragay National Agricultural and Fisheries School (RNAFS).

REFERENCES

Al-Farraji, O. I. (2015). New algorithm for encryption based on substitution cipher and transposition cipher. *International Journal of Current Research, 2*(12) 23610-23612. Retrieved from http://www.journalcra.com/sites/default/files/issue-pdf/11860.pdf

Atkins, W. (2004). *Security, privacy, and risk Management: The Smart Card Report (Eight Edition)*. Retrieved from sciencedirect.com

Bhargavan, K., & Leurent, G. (2016). On the practical (in-) security of 64-bit block ciphers: Collision attacks on HTTP over TLS and OpenVPN. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security* (pp. 456-467).doi: http://dx.doi.org/10.1145/2976749.2978423

Biryukov, A. (2005). Meet-in-the-Middle Attack. In: H.C.A. van Tilborg (ed.) *Encyclopedia of Cryptography and Security*. Springer: Boston, MA.

Coppersmith, D., Holloway, C., Matyas, S.M., & Zunic, N. (1997). The data encryption standard. *Information Security Technical Report, 2*(2) 22-24.

Department for Digital, Culture, Media, and Sport. (2019). *Cyber Security Breaches Survey 2019: Statistical Release.* Ipsos MORI, Social Research Institute, University of Portsmouth. Retrieved from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/813599/Cyber_Security_Breaches_Survey_2019_-_Main_Report.pdf

Henry, J. (2018). *3DES is being officially retired*. Retrieved from https://www.cryptomathic.com/news-events/blog/3des-is-officially-being-retired

Imran, I. I. & Abdulameerabdulkareem, F. (2014). Enhancement caesar cipher for better security. *Journal of Computer Engineering* (IOSR-JCE), *16*(3), 1-5. Retrieved from http:// www.iosrjournals.org

Jain, A., Dedhia, R. & Patil, A. (2015). Enhancing the security of caesar cipher substitution method using a randomized approach for more secure communication. *International Journal of Computer Applications, 129*(13), 6-11. Retrieved from https://arxiv.org/ftp/arxiv/papers/1512/1512.05483.pdf

Kessler, A. (2017). *The evolution of encryption. Thales a Security Blog.* Retrieved from https://blog.thalesesecurity.com/2017/04/04/the-evolution-of-encryption/

Lake, J. (2019). *What is 3DES and how does it works?*. Retrieved from https://www.comparitech.com/blog/information-security/3des-encryption/

Morgan, S. (2019). *Cybercrime Damages $6 trillion by 2021. CyberCrime Magazine.* Retrieved from https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/

Renuka Devi, N. & Harshini, G.N. (2019). Analysis and comparison of substitution and transposition cipher. *International Journal of Research and Analytical Review*, *6*(2) 549-555. Retrieved from https://pdfs.semanticscholar.org/a320/27c4f2db2dab2b7b4764459ca8ce80fd6638.pdf

Sokouti, M., Sokouti, B., & Pashazadeh, S. (2009). An approach in improving transposition cipher system. *Indian Journal of Science and Technology, 2*(8),9-15. doi: 10.17485/ijst/2009/v2i8/29502

Wulandari, G.S., Rismawan, W., Saadah, S. (2015). Differential evolution for the cryptanalysis of transposition cipher. Paper presented at the *2015 3rd International Conference on Information and Communication Technology (ICoICT)*, pp. 45-48. IEEE