

Cryptographic Algorithm for Scout Activity Message Signal Codes Using Permutation and Expansion Techniques

Cryptographic Algorithm for Scout Activity Message Signal Codes Using Permutation and Expansion Techniques

Wahyu Saptha Negoro^{a1}, Zati Hulwani^{b,2}

^{1,2} Universitas Potensi Utama, Kota Medan, 20124, Indonesia
wahyusaptha1707@gmail.com¹, zatihulwani18@gmail.com²

ABSTRAK

Cryptography is the science or art of guarding messages or securing messages in text that is of interest to be kept secret. In cryptographic algorithms there is the term cipher which is a mathematical equation consisting of encryption and description. Usually these two equations have a close relationship and are bound to maintain the security of the message with a given key based on cryptographic techniques. This research aims to explain the scout message signal code using a cryptographic algorithm. The data collection technique used in this research is by using data collection techniques in the form of literature studies to look for references through trusted journals. To create signal messages in scouting activities in this research, researchers chose to use a cryptographic algorithm method with permutation and expansion security techniques. This can be used as a variation of signal codes in communicating during scouting activities so that the authenticity of the messages conveyed is maintained.

Keywords: Cryptography, Permutation, Expansion, Scouting, Signal Code

Info Artikel :

Disubmit: 12 Mei 2024

Direview: 16 Juni 2024

Diterima : 18 Juli 2024

Copyright © 2024 - Journal UPU. All rights reserved.

1. INTRODUCTION

Scouting is non-formal education that is enriched with educational values, scouting and is organized according to scouting methods [1]. Scouting education teaches a progressive independent learning process for young people to develop themselves. Efforts to develop oneself include forming a disciplined leadership character [2], forming a disciplined character in worship [3], and cultivating a spirit of nationalism in every child [4].

Apart from teaching responsibility, discipline and leadership. Scouting education also teaches how to communicate using signal codes. Sign code is a language that uses lip, body and hand movements to express intentions in communication [5]. In Scouting, communication can convey messages through writing or body movements. One of them is Morse code, which is a type of writing made using dots and minus symbols [6]. There is also sign language to communicate conveying messages in scouting using body movements assisted by flags, usually called semaphores [7].

Cryptography is the science of maintaining the confidentiality of messages by encoding them in a form that cannot be understood anymore. In cryptography there are two processes, namely encryption and decryption [8]. Cryptography has a classic history, namely encryption methods that use paper and pencil, or other simple tools. Cryptography itself has the aim of ensuring that messages cannot be read easily by unauthorized parties, ensuring that messages are original or not manipulated and protecting the communicating entity [9].

This time cryptographic algorithms will be used to communicate in scouting activities. Usually the signal code in scouting activities to communicate uses Morse code or semaphore code. However, this time the researcher will examine what would happen if the signal code in scouting activities used permutation techniques and expansion techniques. Is the use of these two methods effective in maintaining the security of messages sent during scouting activities? Apart from that, the use of this technique can also be used as a variation of supporting signal codes in scouting activities.

2. RESEARCH METHODS

This research uses data collection techniques in the form of literature studies. This research was carried out by searching for literature studies from journals which are reference sources for the research discussed in this journal. Literature studies are taken to be supporting material so that the results of this research journal can be accepted and the results of the research can be trusted. Apart from that, this research also uses a cryptographic algorithm method in communicating during scouting activities with two techniques, namely the permutation technique and the expansion technique.

A. Permutation Technique

The permutation technique or commonly called transposition is an encryption technique in cryptography to move or rotate characters according to certain rules [10]. Almost similar to the substitution technique, but the permutation technique has a difference, if the character substitution technique is in a fixed position but its identity is randomized. However, in the permutation technique, the opposite is true, namely the identity is fixed but the position is random. Generally, plaintext in permutation techniques is divided into blocks of the same length. The general form of the permutation technique can be seen in Figure 1 below:

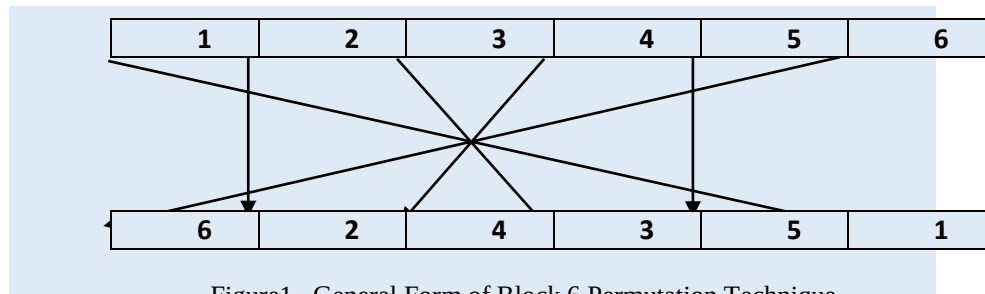


Figure1. General Form of Block 6 Permutation Technique

Figure 1 is the general form of block used in the permutation technique from plaintext to ciphertext with the block-6 rule. And if the message delivered later has an excess of words other than block-6, then you can use the permutation technique with block-5, block-4 and up to block-1, according to how many blocks are left at the end of the message. The following will be presented in Figure 2 for the division of blocks other than block-6.

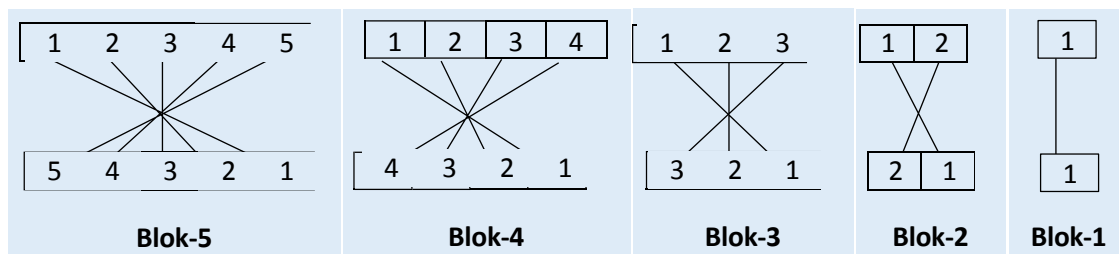


Figure 2. Block derivative form in permutation techniques

B. *Expansion Technique*

The second technique in this research uses the expansion technique, where the expansion technique is a simple method for randomizing the messages sent so that they are not easily known by other people by stretching the message according to certain rules. One rule is to use consonants and vowels, as follows.

- Can start with the letter "consonant or odd number" and end with the word suffix "an"
 - Can start with the letter "Vowel or even number" and end with the word suffix "i".
- The vowels are: A, I, U, E, O
Consonant letters are: b, c, d, f, g, h, j, k, l, m, n, p, q, r, s, t, v, w, x, y, z

Figure 3. General form of rules in expansion techniques

From Figure 3, there are general rules for permutation techniques. However, what coding provisions will be used to secure messages sent in scouting in this research, depends on the researcher. However, it still adheres to the general provisions of the expansion technique.

3. RESULTS AND DISCUSSION

The message signal code for scouting activities in this study uses a permutation technique with the general form of block-6 and the remainder of the message conveyed will use the rules from Figure 2 according to the end of the message. And for expansion techniques, researchers use the general rules that have been explained in the research methods section of this research, discussed using message signal codes which will be presented in the discussion chapter of this research.

A. *Encryption Process and Description*

In cryptography there are two familiar terms, namely encryption and description. Encryption itself is an encoding process which will later be described. The message to be encrypted is called plaintext [11]. Usually plaintext contains information in the form of a message that involves a key to secure the message sent. In this section, description is the reverse process of encryption, where the arrangement of characters and symbols from the encryption is rearranged into its original text form, so that the message recipient can know the entity of the original message [12].

In the cryptographic algorithm for communication signal codes in this scouting activity, researchers will focus on discussing the encryption process using permutation and expansion techniques. Because the description process itself is quite easy to implement. The description process itself only needs to reverse the ciphertext to plaintext to get the original message.

B. Permtation Engineering Process

The process begins by determining the original text or message in the form of plaintext. In this research, researchers used plaintext for encryption in the form of message information from scout codes and promises. The following is the content of the plaintext message in this research:

Demi kehormatanku aku berjanji akan bersungguh-sungguh
Menjalankan kewajibanku terhadap Tuhan, Negara Kesatuan Republik Indonesia dan
mengamalkan Pancasila. Menolong sesama hidup dan mempersiapkan diri
membangun Masyarakat. Menepati Dasa Dharma

Figure 4. Original or Plaintext Message

From the plaintext above, this research will modify or encode it using permutation and expansion techniques. The general form of these two techniques has been explained in the research methods section of this researcher. The following is the process of changing plaintext into ciphertext messages using the following permutation technique:

D e m i K	e h o r m a	t a n k u	A k u B e
K e i m D	a h r o m e	a k n u t	e k u B A
r j a n j i	A k a n	B e r s u n	g g u h - s
i j n a j r	A a k n		s g h u - g
u n g g u h	M e n j a		K e w a j
h n g g u u	a M n e j		j K w e a
i b a n k u	T e r h a	d a p T u	h a n , N
u b n a k i	a T r e h		N a , n h
e g a r a a	K e s a t u	a n R e p	u b l i k
g r a a e	u e a s t K	p n R e a	b i l k u
I n d o n e	s i a D a	n M e n g	a m a l k a
e n o d n l	a i a D s	g e M n n	a m l a k a

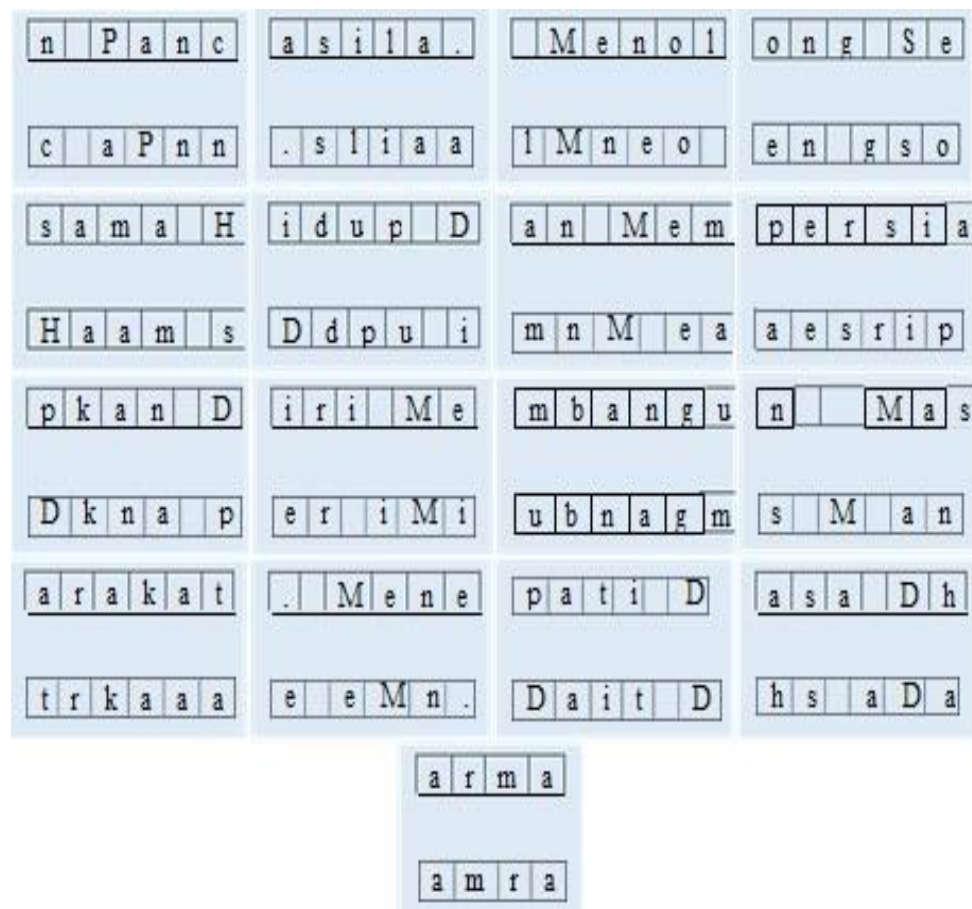


Figure 5. Plaintext Encryption to Cipertext Permutation Technique

Figure 5 shows the permutation technique process when plaintext is converted into ciphertext, usually called the encryption process. In this process the plaintext is located in the block above the arrow and the ciphertext is located below the arrow. Then the plaintext will be grouped into 6 blocks like the general form of permutation techniques, all letters and symbols in the plaintext are encrypted including dots, commas and spaces. So the process will form many blocks, and the remainder of the plaintext in Figure 5 above becomes Block-4 because there are only 4 letters left in the plaintext. So the final plaintext uses the derivative block rules as explained in Figure 2 previously.

So the results of the plaintext to ciphertext encryption process using this permutation technique are:

Keim Dahrome aknutek uBAijnajr Aakn nesruBsghu-ghngguuaMnej
naknaljKwea ubnakiaTreh ua pTdNa,n h graaeueastKpnR ea bilkuenodnIai aDsg
eMnnamlakac aPnn.sliaalMneo en gsoHaam sDdpu immM eaaesripDkna per
iMiubnagms M antrkaaae eMn. Dait Dhs aDaamra

Figure 6. Results of Plaintext Encryption to Cipertext Permutation Technique

C. Expansion Engineering Process

In the expansion technique process, researchers still use the same plaintext, namely in Figure 4. In this expansion technique process, the original message or plaintext will be converted into ciphertext, which is usually called the encryption process. During the encryption process, the tester uses the following expansion techniques:

- If there is a word that begins with a vowel, then the first letter of the word is added with the letter (X) and after the word the letter (Y) ends.
- If there is a word starting with a consonant/odd letter, then the first letter of the word is added with a number (8) and after the word ends with a number (4).

Figure 7. Expansion Technique Encryption Key Instructions

Figure 7. Expansion TecIn the expansion technique we only need to analyze the key instructions provided to encrypt plaintext into ciphertext, the key instructions can be seen in Figure 7. For plaintext, we still use the original message presented in Figure 4. So the encryption process can be seen as follows:

D8emi4 k8ehormatanku4 aXkuY b8erjanji4 aXkanY b8ersungguh-sungguh4
M8enjalankan4 k8ewajibanku4 t8erhadap4 T8uhan4, N8egara4 K8esatuan4
R8epublik4 IXndonesiaY d8an4 m8engamalkan4 P8ancasila4. M8enolong4 s8esama4
h8idup4 d8an4 m8empersiapkan4 d8iri4 m8embangun4 M8asyarakat4. M8enepati4
D8asa4 D8harma4

Figure 8. Plaintext to Cipertext Encryption Using Expansion Techniques

4. CONCLUSION

The perfection of this research is that scouting activities can be collaborated with permutation and expansion techniques when communicating using iconic message codes. Apart from being able to maintain confidentiality, it can also be a variation of security that not many people know about. Rapid technological developments are also closely related to cryptographic algorithms, especially security with permutation and expansion techniques. From the techniques used in this research, future researchers can implement this research into the system created. To see the accuracy of passwords in the security of signal codes in scouting activities when communicating. The aim is none other than to maintain the confidentiality of the message and the authenticity of the message when it is sent and

reaches the recipient of the message. In this research, the scouting honor code plaintext is used to become the original message that will be encrypted to the recipient. On the other hand, other researchers can also use other plaintexts according to their individual needs when carrying out scouting activities.

THANK-YOU NOTE

I would like to thank the team who helped solve this research well and collaborate with each other and thank you also to the OJS team at the Infosys journal who have helped in the processes leading up to the publication of this research with the hopes of the researchers.

REFERENSI

- [1] Nurwana, Titin Dwiyaniti & Mastang. (2022). Analisis Kebijakan Wajib Pramuka Terhadap Pengembangan Karakter Religius Peserta Didik. Jurnal Moral.
- [2] Alfi Nur Hidayati. (2021). Peran Pendidikan Kepramukaan Sebagai Media Pembentukan Karakter Kepemimpinan Siswa Sekolah Dasar. Jurnal Riset Madrasah Ibtidaiyah. 1(1),11-20.
- [3] Muhammad Nur Hakim, Joko Subando. (2023). Strategi Penanaman Karakter Disiplin Beribadah Melalui Kegiatan Ekstrakurikuler Pramuka. Jurnal Ilmiah Ilmu Pendidikan. 6(12),10571-10577.
- [4] Nurlaila Ramadhani, Anggraeni Dewi & Yayang Furi. (2022). Meningkatkan Nasionalisme Dalam Karakter Pendidikan Kepramukaan. EDUMASPUL Jurnal Pendidikan. 6(1),646-651.
- [5] Reza Haris, Mardi Ssiwo, Herny & Eko. (2022). Pembangunan Aplikasi Penerjemahan bahasa Isyarat Dengan Metode CNN Berbasis Android. Jurnal Teknoinfo. 16(2),183-197.
- [6] Ade Hastuty, Sudirman. (2023). Aplikasi Konversi Code Morse Berbasis Android. Jurnal Sintaks Logika. 3(2),58-64.
- [7] Andi Muh, Mina Ismu & Faiqunisa. (2019). Aplikasi Game Semaphore Berbasis Android. Jurnal Teknologi Informasi Dan Komunikasi. 8(1),1-10.
- [8] M.Azhari, Dadang Iskandar, Faizal Joko & Firhan Ali. (2022). Implementasi Pengamanan Data Pada Dokumen Menggunakan Algoritma Kriptografi Advanced Encrypto Standard (AES). Jurnal Pendidikan Sains dan Komputer. 2(1),163-171.
- [9] Fresly Nandar, Indah Fitri & Awang Harsa. (2015). Implementasi Kriptografi Pengamanan Data Pada Pesan Teks, Isi File Dokumen, dan File Dokumen Menggunakan Algoritma Advanced Encryption Standard. Jurnal Informatika Mulawarman. 10(1),20-31.
- [10] Ragil Arya, Aries Suharso. (2022). Analisis Teknik-Teknik Kriptografi Terhadap Serangan Jaringan Local. Jurnal Ilmiah Wahana Pendidikan. 8(16),467-476.
- [11] Victor Saputra Ginting. (2020). Penerapan Algoritma Vigenere Chipper Dan Hill Chipper Menggunakan Satuan Massa. Jurnal Teknologi Informasi. 4(2),241-246.
- [12] Abdurahman Ridho, Cut Mutia & Amelia Putri. (2022). Analisis Enkripsi dan Deskripsi Cipher Teks Menggunakan Kombinasi Gronsfield Cipher Dengan Reverse Cipher. Jurnal Teknik Informatika Kaputama (JTIK). 6(1),87-94.
- [13] R. A. Megantara and F. A. Rafrastara, Super Enkripsi Teks Kriptografi Menggunakan Algoritma Hill Cipher dan Transposisi Kolom, Prosiding SENDI, Pp. 85-92, 2019.
<https://e-journal.potensi-utama.org/ojs/index.php/INFOSYS/> | redaksijurnalupu@gmail.com

- [14] Putri, I., Wibowo, P., Ratricia, P., & Ikhwan, A. (2022). Pengamanan Pesan Menggunakan Metode Hill Cipher Dalam Keamanan Informasi. *Bulletin of Information Technology(BIT)*, Vol. 3 No. 4 pp. 341-342.
- [15] Yusna Warni Hasibuan , Isnarto Isnarto , Rahayu Budhiati Veronica, (2022) Perancangan dan Implementasi Aplikasi Kriptografi Algoritma Hill Cipher dalam Dekripsi Enkripsi Data Keuangan Nasabah Bank Samporna Menggunakan Kode ASCII, *Unnes Journal of Mathematics*, 11(1)
- [16] Nurharianna S, Ilham F, Divi H. (2022) Menerapkan Algoritma Hill Cipher dan Matriks 2x2 Dalam Mengamankan File Teks Menggunakan Kode ASCII, *Jurnal Ilmu Komputer dan Sistem Informasi (JIRSI)*, 1(2) 70-83.
- [17] Rio Wiranata, Husnul Khair, Suci Ramadani. (2020) . Implementasi algoritma kriptografi modular Multiplication – based block cipher (mmb) Pada keamanan data, *Jurnal Teknik Informatika Kaputama (JTIK)* 4(2) 100-110
- [18] Adetya Maharani Marpaung, Fauziatun Husnah, Sinta Dara Efita, Adnan Buyung Nasution. (2023) Perancangan Sistem Keamanan Website Dengan Metode Hill Cipher, *Jurnal Jurnal Sains Dan Teknologi (JSIT)* 3(1) 101-129
- [19] A. Rifa'i and L. C. Sumartini, "Implementasi Kriptografi Menggunakan Metode Blowfish Dan Base64 Untuk Mengamankan Database Informasi Akademik Pada Kampus Akademi Telekomunikasi Bogor Berbasis Web- Based," *J. EKomtek*, vol. 3, no. 2, pp. 87–96, 2019, doi: 10.37339/ekomtek.v3i2.133.
- [20] A. Sutoyo, Nurhayati, and I. Gultom, "Implementasi Super Enkripsi Algoritma One Time Pad (OTP) dan Beaufort Cipher untuk Mengamankan Data," *J. Sist.Inf. Kaputama*, vol. 3, no. 1, pp. 1–5, 2019, [Online]. Available: <https://jurnal.kaputama.ac.id/index.php/JSIK/article/view/144> [2] I. Febriana and G. A. S, "Penerapan Teknik Kriptografi Pada Keamanan Smsandroid," *JOEICT (Jurnal Educ. Inf. Commun. Technol.)*, vol. 1, no. 1, pp. 29–36, 2017.
- [21] F. Alfiah, R. Sudarji, and D. Taqiyyuddin Al Fatah, "Ciledug Raya, RT.10/RW.2, Petungkana Utara," p. 12260, 2020.
- [22] N. P. Efendi, N. P. Efendi, and N. putra efendi, "Jurnal Pengamanan Aplikasi Pesan dengan Algoritma Caesar Cipher dan Affine Cipher," 2021, [Online]. Available: <http://dx.doi.org/10.31219/osf.io/y4acn>