PAPER • **OPEN ACCESS**

The modification of caesar cryptosystem based on binary vertices colouring

To cite this article: K A Santoso *et al* 2020 *J. Phys.: Conf. Ser.* **1538** 012006

The modification of caesar cryptosystem based on binary vertices colouring

K A Santoso[1], I H Agustin[2], R M Prihandini[3]
[1,2,3,4]CGANT Reseach Group, Jember University
E-mail: kiswaras@gmail.com

Abstract. Recently information technology has developed rapidly like the development of computer hardware and software. By the existence of internet technology, the process of data transfer can be done by others from a separate place and outside the system environment. The ease of data access remotely (using the internet) does not mean that they are always positive or good, but they also make new problems for the information world. The biggest problems when using the internet are slow access speeds and security when transferring data. Communication via internet is very susceptible to data loss or changed that caused by system errors or actions from non responsible persons. According to Kadir (2011) errors in data transfer via internet are caused by two reasons, that are the existence of human error or improper user intervention and the existence of technical errors from its system. Many efforts have been made by internet users to solve the problem of data transfer, including encoding data that will be sent in order to no user can read the data except the person has the right to receive it. Just not encoding, there is also an authentication process or validation of the data received, this is done to ensure that the data received is correct or does not changed. In this paper, the author propose a modification of the caesar cipher where if the key used previously is a real number, then we change the key into the coloring of vertices on the graph. So the key that used in this method is a graph. The core of this research is that every character of the plaintext has affiliation with each vertex of the graph, so that if the vertex of the graph gets 4 colors for example, then the characters of the plaintext affiliated with that vertex are also added with 4. This process will be repeated until all characters in the plaintext are coded according to the color of vertex. If the number of the characters plaintext is greater than the number of vertices, then the repeat process will occur until all the characters from the plaintext have affiliation with the vertex on the key graph.

1. Introduction

The message security issue called confidentiality if definitely to its destination intact, so the contents of the message that you send have not been changed or manipulated by someone or unauthorized parties (Data Integrity). Safe can also mean that the recipient must be sure that the message reaching him is the message you sent not from someone else who acts like you and you are sure that the message you sent also reaches the right recipient (Authentication). If you are the recipient of a message, you certainly do not want the message sender to deny having sent the message to you. (Repudiation). [1] Even though you believe that you received a message from someone, but if the sender said that the message not from him then you need to prove its denial (Non-Repudiation). The security problems that have been mentioned above can occur to all of us without exception especially in modern era like today where daily activities are already using passwords. Habitually in making passwords for social media accounts, or pin of the bank we used predictable words such as name, date of birth, address and others. it is very vulnerable to the actions of hackers to find important passwords that we use. Dictionary attack is one way for hackers to find out the important passwords that we have. Dictionary attack is a way to find passwords using computer assistance by trying all possible combinations of letters and numbers. To speed up the attack or search for a password, a combination

of letters and numbers will be designed according to the words that often appear so as form a dictionary. [2] Passwords that easy to guess are very dangerous if unauthorized people find out. For example, if the cloud storage password that contains work data or our work is known, then other people can abuse it or worse is the occurrence of piracy of the work. This problem can be solved by cryptography, in this case, the most easily of cryptography that is understood by ordinary people is substitution methods such as the Caesar cipher algorithm. [3] The development of technology allows humans to communicate and exchange information/data remotely. Between regions, even countries are no longer an obstacle in doing communication or data exchange, along with that demand for security to increase the confidentiality of information exchanged. Security and confidentiality when exchanging data and information are very important in the current era of information and communication technology. To anticipate this problem, science was developed that studies the method of securing data by encoding and known as Cryptography. In cryptography, there are two main concepts namely encryption and decryption. Encryption is the process in which information/data that be sent is converted into a form that is not recognized as initial information by using a particular algorithm. Description is the opposite of encryption, that is to change back the disguised data becomes original information. Many cryptographic methods have been made recently, one of which is the caesar cipher. Caesar Cipher is a cryptographic technique that is done with substitute each alphabet of the message to be encrypted by shifting the alphabetical order according to the key alphabet. For example, each letter is substituted with the next fifth letter. In this case, the key is the number of shifts of the letter, the key is 5. [4] XOR Cipher is a cryptographic method developed with computers. Is consists in encrypting a binary message with a repeated key using a XOR operation. XOR is symbolized by $\oplus$.

Graph is a structure that represents the relationship between objects. In the graph theory, the vertices are used to represent an object while the relationship between objects / points is expressed by an edge. The adjacency matrix is binary matrix A which has the order VxV, where V is the number of points on the graph. Element $A_{i,j}$ is 1 if there is an edge from vertex i to vertex j and else the element $A_{i,j}$ is 0. Figure 1 shows the example of some graph with its adjacency matrix.

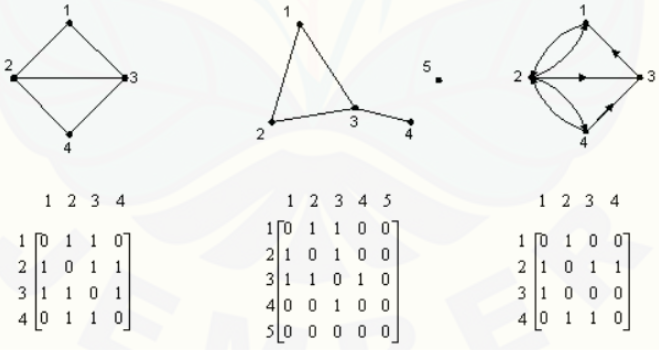
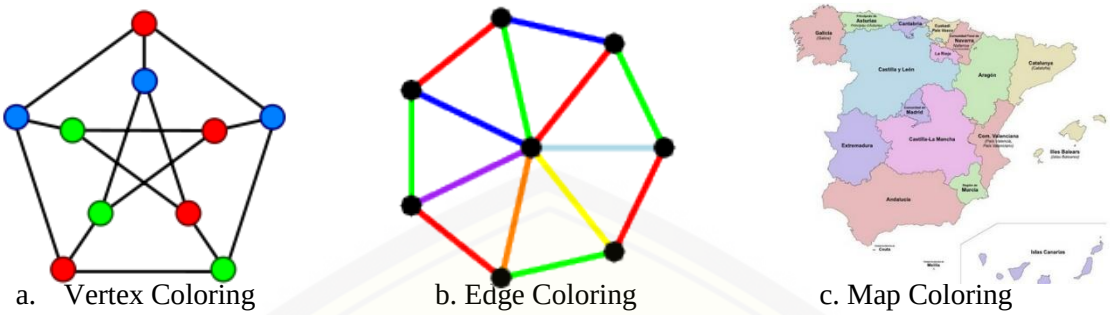


Figure 1. Example of Graphs with its Adjacency Matrix

Graph coloring is a special case of graph labeling. Labeling in this case means, namely to give color at vertex, edge or map by minimum color [5]. Generally, there are three types of graph coloring. Firstly, vertex coloring is coloring to each vertex so that no adjacent vertex has the same color. In order more clear we show an example in figure 2a where ten vertices are colored by three colors. The second, edge coloring, which gives different colors to the neighboring sides so that no two neighboring sides have the same color. In order clearer we show an example in figure 2b The third, coloring the map, which gives color to the fields so that no neighboring map has the same color. In order more clear we show an example in Figure 2c



a. Vertex Coloring b. Edge Coloring c. Map Coloring

Figure 2. Example Of Graph Coloring

Logic Gate is the basis for a Digital Electronic System that functions to convert one or several Inputs to the Logical Output. Logic Gate operates based on a binary number system that is a number that only has 2 symbol codes, 0 and 1 using the Boolean Algebra Theory. The XOR gate will only produce output with logic 0 if all inputs are simultaneously low value or all inputs are high value or it can be concluded that the XOR gate will produce output with 0 if the inputs are all equal value. In order more clear we show the XOR operation in Table 1 as follows

Table 1. XOR Operation

Inputs		Output
A	B	X
0	0	0
0	1	1
1	0	1
1	1	0

2. Methods

Caesar cipher is one of the substitution algorithm. This coding is one of the coding system used during Julius Caesar's government. The technique used is to shift the position of plaintext letters of the alphabet, and known as the ROT3 algorithm. On this algorithm, each letter in the alphabet is shifted 3 positions to the right (shift parameter, k = 3). In order more clear we show an example on figure 3 where the alphabet are shifted by k = 3. The mechanism of the Caesar's algorithm is shift the entire sequence of alphabetic according to value of the key that is given, k for example. For example key k = 3 then alphabet A is shifted three into D, alphabet B is shifted three into E, and so on until alphabet Z is shifted three into C. The weakness of this algorithm is the definite change that will be easily detected, meaning that the alphabet A always changed to D and the alphabet Z always changed to C and so on for the key k = 3. To understand easily the shifting mechanism can be seen in Figure 3 below.

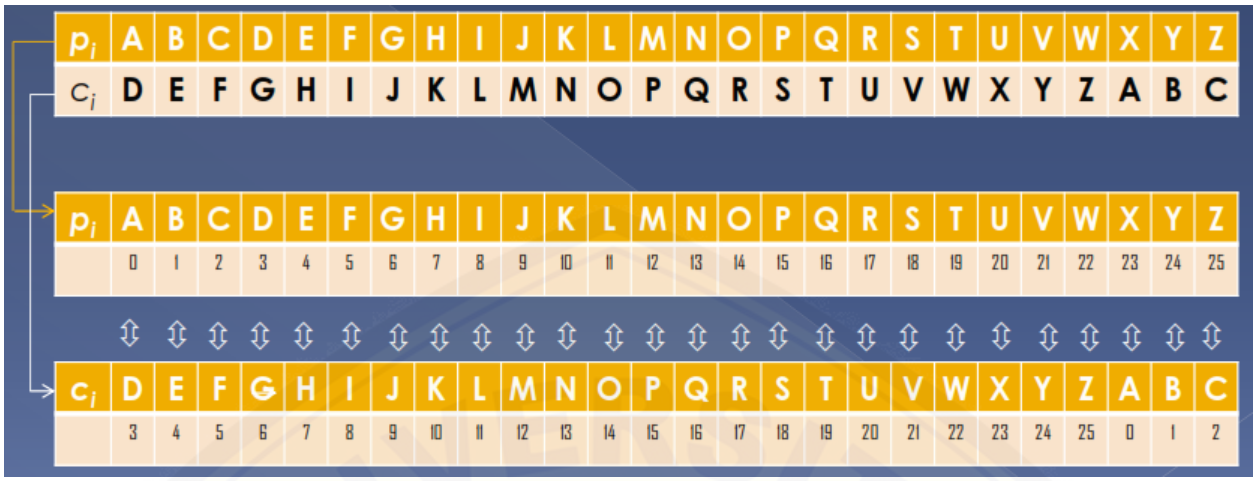


Figure 3. Alphabetical order with the shift by 3

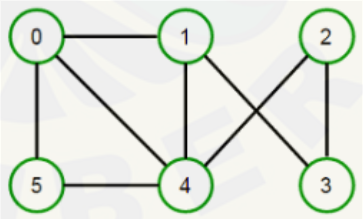
3. Results

In this paper, the authors modify the caesar cipher algorithm based on a combination of binary values of the plaintext character with the vertex coloring algorithm in the graph as the key. The algorithm is presented as follows:

1. Convert plaintext into real numbers based on ASCII tables
2. Convert the alphabet value has gotten on step-1 into 8 bit (binary digits)
3. Coloring the vertex on the graph. (The color represented by a real number). In this case, the graph supposed as the key
4. Convert the vertex color have gotten on step 3 to 8 binary digits
5. Do the XOR operation between the binary value of alphabet plaintext and the binary value of vertex color on the key graph
6. Convert the result of the XOR operation to the ciphertext character based on the ASCII table

Because of this algorithm is part of symmetric cryptography, so to decrypt this algorithm as same as the encryption process. To describe this algorithm the following example is given:

Plaintext : **Hello World** Key :



The first step takes the plaintext alphabet value based on the ASCII table (in this case the character value is in decimal form). Next, we change the decimal form into bit (binary digits) where each alphabet is represented by 8 bits. For details can be seen in Table 2 below.

Table 2. Conversion Between Alphabet of Plaintext to Bits

Plaintext		
TEXT	**ASCII**	**BIT**
H	72	01001000
E	45	00101101
L	76	01001100
O	79	01001111
W	87	01010111
R	82	01010010
D	68	01000100

The third step, we do the coloring of the vertex on the graph and based on the result of vertex coloring can be shown figure 4 below:

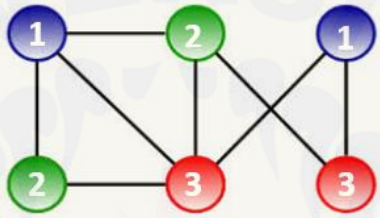


Figure 4. Vertex Coloring on key graph

To make it clear the change from the color represented in decimal form to 8 binary digits can be seen in Table 3 below.

Table 3. Conversion of Color into bits

KEY		
Vertex	**Color**	**BIT**
0	1	00000001
1	2	00000010
2	1	00000001
3	3	00000011
4	3	00000011
5	2	00000010

Then the XOR operation is performed between the plaintext bit and the key bit as follows

Plaintext : Hello : 01001000001011010100110001001100010011111
Key : 01234 : 00000001000000100000000100000011000000010 ⊕
XOR : 01001001001011110100110101001111010011101

The results of the XOR operation are converted to decimal form to get the alphabet based on the ASCII table. The encryption process of this algorithm can be seen in Table 4 below:

Table 4. Encryption Process

Plaintext		Key		XOR	Ciphertext	
TEXT	BIT	Vertex	BIT		ASCII	TEXT
H	01001000	0	00000001	01001001	73	I
E	00101101	1	00000010	00101111	47	G
L	01001100	2	00000001	01001101	77	M
L	01001100	3	00000011	01001111	79	O
O	01001111	4	00000011	01001100	76	L
W	01010111	5	00000010	01010101	85	U
R	01010010	0	00000001	01010011	83	S
L	01001100	1	00000010	01001110	78	N
D	01000100	2	00000001	01000101	69	E

Based on the example above, Plaintext "HELLO WORLD" after being coded with this technique uses key node coloring on the main graph change to "IGMOLUSNE".

By this algorithm, it can reduce the weaknesses of the caesar algorithm where each alphabet has a fixed replacement alphabet. In this algorithm an alphabet can be replaced with another non-permanent alphabet, for example the L alphabet in the word HELLO. The first L alphabet is replaced by the M alphabet, while the second L alphabet is replaced by the O alphabet. Differences in the substitute alphabet are caused by differences in the vertex color of the key graph. This non-permanent alphabet change is the strength of this algorithm which is a modification of the caesar algorithm.

4. Conclusion

Based on the results of the study, it can be concluded several things, (1) Cryptography with the Caesar cipher algorithm shifts the alphabetical order on the plaintext with the specified key; (2) The modification of Caesar algorithm based on XOR operation between the plaintext bit and the vertex color bit in the key graph causes the alphabet on the plaintext to be exchanged with another alphabet; (3) On the security side, this algorithm modification is safer than the original Caesar algorithm because the ciphertext alphabet that is replaced from the plaintext alphabet cannot be predicted (depends on the color of the vertices of the key graph).

Some suggestions for the developer of cryptographic algorithms are, (1) Applying the algorithm for other media except for text, for example, images; (2) Take the benefit of graph labeling besides vertex coloring to modify existing cryptographic algorithms

Acknowledgment

This paper is supported by University of Jember 2020

References

[1] Kumari V 2015 Symmetric Diffusion-Double Substitution Based Image Encryption *International Journal of Advanced Reseach in Computer Science and Software Enginering* **5** (8) 888-892

[2] Pakshwar R 2013 Image Encryption Using Random Scrambling and XOR Operation *International Journal of Engineering Reseach & Technology* **2** (3) 1-7

[3] Singh A 2015 DIP Using Image Encryption and XOR Operation Affine Transform *IOSR Journal of Computer Engineering* **17** (2) 07-15

[4] Tamimi A 2015 An Image Encryption Algorithm with XOR and S-box *International Conference Comp Vision and Pattern Recognition* 166-169

[5] Shariefuddin P and Ashay D 2017 A Colorful Path *Journal of the Korean Society for Industrial and applied Mathematics* **11** (4)

[6] Santoso K A, Fatmawati and Suprajitno H 2017 Image Encryption Technique Based on Pixel Exchange and XOR Operation *Proceeding of International Basic Science Conference* 286-288