Artikel Gost Algorith Prosiding Scopus.pdf

by

Submission date: 09-Aug-2022 01:46PM (UTC+0700)
Submission ID: 1880572727
File name: Artikel Gost Algorith Prosiding Scopus.pdf (756.51K)
Word count: 1820
Character count: 9723

Combination Base64 and GOST algorithm for security process

Journal of Physics: Conference Series **1402** (2019) 066054 doi:10.1088/1742-6596/1402/6/066054

Combination Base64 and GOST algorithm for security process

R Rahim[1,*], S Sumarno[2], M T Multazam[2], S Thamrin[3] and S H Sumantri[3]

[1] School of Computer and Communication Engineering, Universiti Malaysia Perlis, Perlis, Malaysia
[2] Universitas Muhammadiyah Sidoarjo, Sidoarjo, Indonesia
[3] Indonesia Defense University, Bogor, Indonesia

*usurobbi85@zoho.com

Abstract. Cryptography in various communications both online and offline is very necessary and generally cryptography is used to secure data in the form of text while non-text data requires special algorithms. Base64 is an encoding algorithm that can convert non-text data into binary data so that the data can be secured with cryptographic algorithms such as the GOST algorithm. The combination of the BASE64 and GOST algorithms is expected to be able to secure all types of data that exist and have the ease of returning to their original form without damaging the original data, besides this combination will increase data security because the combination of these two algorithms produces ciphertext that is difficult to know if the process is done cryptanalyst by third parties. The results of the combination of Base64 and GOST algorithms are expected to be able to deliver dynamic security contributions to various existing data objects so that they can be used both online and offline.

1. Introduction

The attack on ciphertext to get plaintext is commonly done by cryptanalysis by using various types of attacks so that the plaintext is obtained and the information contained therein can be misused or to get its own benefit [1-3]. The GOST Cryptography algorithm is an encryption algorithm that has a process of 32 rounds and uses 64-bit block ciphers with 256 key keys and uses 8 S-Boxes, XOR operations and Rotate Left Shift and one of the fastest algorithms for encryption and decryption for data text types and not for other media such as images, for example [4-6]. To facilitate the security of other objects, a special BASE64 technique is needed which is used to convert the image object to printable text so that the image can be secured and can be distributed to the entitled recipient in the form of ciphertext [7,8].

Security in non-text media is now very necessary because communication using media has become a necessity [9]. Audio, video and images are objects that are widely used in communication when this is primarily an image that is almost certainly used in all communications [10-12]. Security in images can be done directly by encrypting the image file using cryptographic algorithms such as AES, DES, 3DES or using the GOST algorithm, but this will cause suspicion because the file is encrypted.

The use of Base64 in this article is used to convert image objects into printable text so that the process of indirect encryption of image objects but text and for cryptanalysis will give a relatively longer time to find out whether the data is text or image, hopefully this combination can provide a better way of securing image objects for users. It is expected that using the GOST and Base64 algorithms to secure

certain objects can secure images more easily and not reduce image quality or also change certain object bytes.

2. Methodology

The use of the Base64 and GOST algorithms is done in stages as in the diagram shown in figure 1:

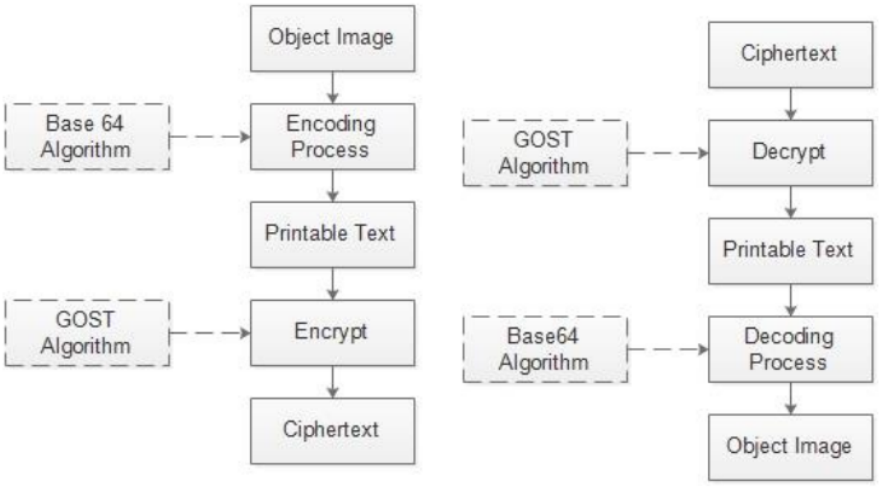

Figure 1. Base64 and GOST algorithm combination.

The combination of Base64 and GOST algorithms in securing data in this case is testing an object image done in Figure 1 above, gradually the process is carried out starting from the Base64 algorithm and continued with the GOST algorithm, here is the Base64 process table used for encoding and decoding can be seen in table 1.

Table 1. Base64 value.

Index	Value	Index	Value	Index	value	Index	value	Index	value
0	A	13	N	26	a	39	n	52	0
1	B	14	O	27	b	40	o	53	1
2	C	15	P	28	c	41	p	54	2
3	D	16	Q	29	d	42	q	55	3
4	E	17	R	30	e	43	r	56	4
5	F	18	S	31	f	44	s	57	5
6	G	19	T	32	g	45	t	58	6
7	H	20	U	33	h	46	u	59	7
8	I	21	V	34	i	47	v	60	8
9	J	22	W	35	j	48	w	61	9
10	K	23	X	36	k	49	x	62	+
11	L	24	Y	37	l	50	y	63	-
12	M	25	Z	38	m	51	z		

GOST is an abbreviation of "Gosudarstvennyi Standard" or "Government Standard". GOST method is a block cipher algorithm developed by a Soviet Government [12]. This approach was developed by the Soviet government during the cold war to hide confidential data or information during communication

[11,12]. This algorithm is a simple encryption algorithm that has a total of 32 processes and uses 64-bit block ciphers with 256-bit keys. GOST method also uses eight different S-Box and XOR and Left Circular Shift operations [11,12].
The components of the GOST method [11,12] is:

- The Key Store Unit (KSU) stores 256-bit strings by using 32-bit registers (K0, K1... K7).
- Two 32 bit registers (R1, R2).
- 32-bit adder modulo 232 (CM1).
- Bitwise Adder XOR (CM2).
- Substitution block (S) is eight pieces of 64 bit S-Box.
- Left shift register (R) rotation is 11 bits.

3. Results and discussion

Image security testing using the Base64 algorithm and GOST appears in the following process:

Figure 2. Object image.

Figure 2 is an object that will be secured and as a test pixel samples of size 3 x 3 are taken so that the values are as follows after being processed with Base64.

ABFEAAAQAAAABAAAAAFEBAAMAAAABAAEAAFECAAEAAAAMAAAAAPlEDAAEAAA
ABAAAAAAAAAABTfYnD1rSkxJGhwo4wmn18pIbV4ssjlnlfhJC0zaM5cX0flXhHoYdaq5K80awr
bGqZrbU7moLM1dm5xcyAm6VLeYUVdnUrcnuesbkybnpMlYxbgo6VqrPa5dJZhnfk6Oqltb3x8vOa
u4vd4uRBnIX19vYSZXIsbHjJ0dZihpIvdX0JZHG1wsiqucAbaHQybWslhnZqknxliJQZZ3NomZb4+v
pNjo06cWwVZnN=

Encoding results are then encrypted using the GOST algorithm using key ***semuakarenascopus*** so that the following results are obtained:

kMiqcZBeCfU/f6YliKKhFmsILTGUlQ2sBX8EnzVm6oWJYlfHugQ7VOZL0wWq/rdUcJA95Eminh
JZEx27BEAGgR9SBXXy/E1/NXLPKAWqpOScdwfwqTMgWuh1ee0RXFNlOtoR4FzQFir3CzFBq
MloJg/erpVhe0eD1o7fOQKFReigUDg2fSkJL3Z6/3hGbvO8IKq1WA5f05s6KJ/wASM5Z4V8BG7U4
WutXJ319OFEC27biWOojGQPTRUKuaQlI4KE20WpYiw6J/gG0QjsUrHsGMT/dSh/+vLqbaa2JFV
NTJvhPlh46feZwZ0uy1Oc6b2R4tJrvtlnqT2c5dqWpLJlWVRJdD2k4Dqj7HRZHDJVu1GId5MlkDr+
nHKUF9yki3REaSvOf5ajBThl5/9U12RRHqMjZJjaeFRi8UBIQ3o3wjtKr81+1MyEvjzMoekJmNKn7
83IetnC89GlUpS0E3cDO42pqAOru2G6Wz1J0wOzW3c1ZSS15Rmp5NeHP6brwaEg

Ciphertext results above are the security process of the 3 x 3 image object that is secured and to return the ciphertext in the form of an image, the process is done in reverse where the decryption process with the GOST algorithm is done first and then decoding with the Base64 algorithm.

The above test proves that the security process using the Base64 and GOST algorithms can work well and the tests carried out by researchers such as Nurdiyanto and Yu and Liu in using the GOST and Base64 algorithms to secure data can run well [4,8,13].

4. Conclusion

Security using the Base64 and GOST algorithms can secure image objects as well as text in general, making it difficult for cryptanalysis, the use of Base64 as a process of encoding and decoding in addition to images can also be used for other objects and of course with different results. This combination is quite good but to improve performance you need to add a compression algorithm so that the ciphertext results are compressed and the results will be smaller.

Acknowledgment

Thank you for Universitas Muhammadiyah Sidoarjo for funding support of this research publication.

References

[1] Jamshidi M, Bazargan H, Shaltooki A A and Darwesh A M 2019 A Hybrid Key Pre-Distribution Scheme for Securing Communications in Wireless Sensor Networks *JOIV: International Journal on Informatics Visualization* **3**(1) 41-46

[2] Al-Azzeh J, Zahran B, Alqadi Z, Ayyoub B and Mesleh M 2019 A Novel Based On Image Blocking Method To Encrypt-Decrypt Color *JOIV: International Journal on Informatics Visualization* **3**(1) 86-93

[3] Sujito S and Muttaqin W M 2019 Hashing Variable Length Application For Message Security Communication *Arpn Journal Of Engineering And Applied Sciences* **14**(01)

[4] Nurdiyanto H and Rahim R 2017 Enhanced pixel value differencing steganography with government standard algorithm *In 2017 3rd International Conference on Science in Information Technology (ICSITech)* 366-371

[5] Iqbal M, Sahputra Y and Siahaan A P U 2016 The understanding of gost cryptography technique *International Journal of Engineering Trends and Technology (IJETT)* **39**(3) 168-172

[6] Limbong T, Simarmata J, Tambunan A R S, Siagian P, Panjaitan J, Siagian L and Lumbanbatu K 2018 The implementation of computer based instruction model on Gost Algorithm Cryptography Learning *IOP Conference Series: Materials Science and Engineering* **420**(1) 012094

[7] Fiscus K and Shinburg D 2011 Base64 Can Get You Pwned *SANS Reading Room*

[8] Liu Z, Liu L, Hill R and Zhan Y 2011 Base62x: An alternative approach to Base64 for non-alphanumeric characters *In: Proceedings - 2011 8th International Conference on Fuzzy Systems and Knowledge Discovery, FSKD* 2667–2670

[9] Khan R, Khan S U, Zaheer R and Khan S 2012 Future internet: The internet of things architecture, possible applications and key challenges *In: Proceedings - 10th International Conference on Frontiers of Information Technology* 257–260

[10] Rastogi N and Hendler J 2017 WhatsApp security and role of metadata in preserving privacy *arXiv Prepr arXiv170106817* 269–275

[11] Sethi P and Kapoor V A 2016 Proposed Novel Architecture for Information Hiding in Image Steganography by Using Genetic Algorithm and Cryptography *In: Procedia Computer Science* 61–66

[12] Cheddad A, Condell J, Curran K and Mc Kevitt P 2010 Digital image steganography: Survey and analysis of current methods *Signal Processing* **90** 727–752

[13] Yu L, Wang Z and Wang W 2017 The Application of Hybrid Encryption Algorithm in Software Security *Fourth Int Conf Comput Intell Commun Networks* 762–765

Artikel Gost Algorith Prosiding Scopus.pdf

ORIGINALITY REPORT

7%	7%	3%	4%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	research.aalto.fi Internet Source	3%
2	es.scribd.com Internet Source	2%
3	Submitted to School of Business and Management ITB Student Paper	1%
4	www.iis.sinica.edu.tw Internet Source	1%

Exclude quotes	On	Exclude matches	< 1%
Exclude bibliography	On		