Protection of Important Data and Information using Gronsfeld Cipher

[1] **Zuhri Ramadhan,** [2] **Andysah Putera Utama Siahaan**
Faculty of Science and Technology, Universitas Pembangunan Panca Budi, Medan, Indonesia
Email: [1] ramadhanzoe@pancabudi.ac.id, [2] andiesiahaan@gmail.com

Abstract: *Data security is a way to ensure that stored data is safe from corruption and that access to it is accordingly controlled. Data security helps to ensure privacy. It also helps protect personal data from theft. Data theft is one that often occurs on global computer networks. It includes criminal acts in the internet world. Chronology of theft is that an intruder enters a system and retrieves essential information without the owner's knowledge. Intruders use data that has been taken for various crimes. Various ways that intruders take to retrieve the data. This action is proven by the amount of internet traffic that is looking for a gap to infiltrate a system. Cryptography is needed to protect essential data. One of the classic algorithms used is Gronsfeld Cipher. This algorithm works by exchanging characters in messages using substitution tables. The key used is a number that determines the shift of plaintext and key. The resulting ciphertext is the result of plaintext substitution with the key table. This algorithm is constructive for users to secure their essential information when it will be sent through a global network.*

Key Words: *Gronsfeld cipher, encryption, decryption, algorithm.*

1. INTRODUCTION:

Security is something that must be applied to prevent others from committing a crime [1]. Computer security is a precautionary measure against attacks by computer or network users who do not want to be held responsible. Computer security is related to self-prevention and also the detection of intruder actions that are not recognized in computer systems [2]. In sending data, many things must be considered. One of the ways that data is transmitted is safe from data theft. Not only theft, data modification often occurs so that the authenticity of the data is not guaranteed. Prevention technique is needed to secure data. Cryptography is the solution to the problems that occur. Many cryptographic techniques can be done in maintaining data from crime [3]. The Gronsfeld method is one of the cryptographic techniques that can be used to avoid data theft. The Gronsfeld algorithm is straightforward to implement. This algorithm has a key in the form of a numeric number that has an unlimited length. Keys can be created as long as the plaintext will be tested. The longer the key, the higher the level of security [4]–[7]. A key that is shorter than the plaintext will be repeated continuously until it reaches the length of the plaintext. The use of this method is expected to increase the level of security on global networks [8].

2. THEORIES:

2.1 Aspects of Computer Security

Computers will be unsafe if they are connected to a global network, especially the internet [9]. The sites visited sometimes have viruses, malware or the like that can steal personal data from a computer and then send it to people who install the device. Computer security is essential to avoid data theft. The essence of computer security is to protect the computer and its network with the aim of securing the information inside [10]. Computer security itself includes several aspects, such as:

- Privacy is something that is confidential. The point is prevention so that unauthorized people do not access the information. Prevention is possible is to use encryption technology, so only the information owner can find out the real information.
- Confidentiality is data that is given to other parties for special purposes but is still maintained in its distribution. It will be seen when asked to prove someone's crime, whether the information holder will give information to the person who requested it or maintain the client.
- Integrity, the emphasis is that information must not be changed except by the owner of the information. Sometimes the encrypted data is not maintained by integrity because there is a possibility that the ciphertext of encryption will change.

- Authentication is done when the user is logged in using the username and password, whether it is suitable or not if it is accepted and will not be rejected. It is usually related to one's access rights, whether he is a legitimate accessor or not.
- Availability, this aspect relates to whether a data is available when needed. If a data or information is too tight, security will make it difficult to access the data. Besides that, slow access also prevents the full availability. The attack that is often carried out on this aspect is a denial of service (DoS), which is a service failure when there is a data request so that the computer cannot service it. Another example of this denial of service is sending an excessive request that causes the computer to no longer be able to accommodate the load, and finally, the computer goes down.

2.2 Cryptography

Cryptography was originally from Greek. This word consists of two syllables, namely "Crypto" and "Graphia." Crypto means hiding [11]. Graphia means writing. Cryptography is the science of learning word techniques using mathematics [12]. It aims to protect data from several aspects of information security such as data confidentiality, data validity, data integrity, and data authentication. However, not all aspects of information security can be solved by cryptography. Cryptography can also be interpreted as science or art to maintain the security of messages [13]. Cryptography has four main components such as:

1. A Plaintext is a message that can be read.
2. A Ciphertext is a random message that cannot be read.
3. A Key is a key to performing cryptographic techniques (symmetric and asymmetric).
4. An algorithm is a method to do encryption and decryption.

Then, the process of manipulating information includes two fundamental cryptography processes such as [14]:

1. Encryption
2. Decryption

2.3 Gronsfeld Cipher

Gronsfeld Cipher is a cryptography method that works like a Vigenere Cipher. Gronsfeld Cipher uses keys from decimal numbers instead of letters, but sometimes it can uses ASCII as the key substitustion. The key will be repeated periodically with the intention that each plaintext has a key. It has the same length as plaintext. When the user enters a key that is smaller in length than plaintext, the key will automatically be repeated from the beginning for the next plaintext [15].

There are two models of use of characters in the Gronsfeld algorithm. This algorithm can use 256 ASCII characters or use only 26 alphabetical characters. The following equations are the formulas used to implement the Gronsfeld algorithm.

Encryption:

$$E\,(x) = (P\,(x) + K\,(x))\, mod\ 26$$

$$E\,(x) = (P\,(x) + K\,(x))\, mod\ 256$$

Decryption:

$$D\,(x) = (P\,(x) - K\,(x))\, mod\ 26$$

$$D\,(x) = (P\,(x) - K\,(x))\, mod\ 256$$

In performing the text encryption process, specify the plaintext to be encrypted and then change it in capital/uppercase form if necessary. Determine the key in the form of numbers. If the key length is not the same as the length of the plaintext, then the key is repeated periodically so that the number of key characters is the same as the number of plaintexts. The plaintext will be changed to decimal. The ASCII code will be added with a decimal value to the key. The result of the sum if it exceeds 256 will experience a modulo process. The final result is changed back to the character form [16].

Table 1. Gronsfeld map

	A	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**	**N**	**O**	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**
0	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
1	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
2	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
3	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
4	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
5	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
6	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
7	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
8	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
9	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I

Table 1 is an example of a Gronsfeld password containing the alphabet written in 10 lines. Each row is shifted one sequence to the left of the previous row. The result will form ten possibilities. Each letter is encoded using different lines, according to the key number that is repeated.

3. RESULT AND DISCUSSION:

This section explains the Gronsfeld algorithm testing. This algorithm is one of the classic cryptographic algorithms that use symmetrical keys. This method is straightforward to implement because this algorithm has an easy calculation. Even though the key is simple, this algorithm has a high complexity to solve if using a long key because the key loop is unpredictable in which part. The following is an illustration of the Gronsfeld algorithm calculation.

Plaintext = UNIVERISTY
Key =

K1	**K2**	**K3**	**K4**	**K5**	**K6**
1	2	3	4	5	6

Plaintext ASCII =

P1	**P2**	**P3**	**P4**	**P5**	**P6**	**P7**	**P8**	**P9**	**P10**
U	N	I	V	E	R	S	I	T	Y
85	78	73	86	69	82	83	73	84	89

3.1 Encryption

C1 = P1 + K1
= 85 + 1
= 86

C2 = P2 + K2
= 78 + 2
= 80

C3 P3 + K3
= 73 + 3
= 76

C4 = P4 + K4
= 86 + 4
= 90

C5 = P5 + K5
= 69 + 5
= 74

C6 = P6 + K6
= 82 + 6
= 88

C7 = P7 + K1
= 83 + 1
= 84

C8 = P8 + K2
= 73 + 2

= 75

C9 = P9 + K3
= 84 + 3
= 87

C10 = P10 + K4
= 89 + 4
= 93

Ciphertext = VPLZJXTKW]

Table 2. Encryption result

P1	**P2**	**P3**	**P4**	**P5**	**P6**	**P7**	**P8**	**P9**	**P10**
U	N	I	V	E	R	S	I	T	Y
85	78	73	86	69	82	83	73	84	89
K1	**K2**	**K3**	**K4**	**K5**	**K6**	**K1**	**K2**	**K3**	**K4**
1	2	3	4	5	6	1	2	3	4
C1	**C2**	**C3**	**C4**	**C5**	**C6**	**C7**	**C8**	**C9**	**C10**
86	80	76	90	74	88	84	75	87	93
V	P	L	Z	J	X	T	K	W	]

3.2 Decryption

P1 = C1 - K1
= 86 - 1
= 85

P2 = C2 - K2
= 80 - 2
= 78

P3 C3 - K3
= 76 - 3
= 73

P4 = C4 - K4
= 90 - 4
= 86

P5 = C5 - K5
= 74 - 5
= 69

P6 = C6 - K6
= 88 - 6
= 82

P7 = C7 - K1
= 84 - 1
= 83

P8 = C8 - K2
= 75 - 2
= 73

P9 = C9 - K3
= 87 - 3
= 84

P10 = C10 - K4
= 93 – 4
= 89

Plaintext = UNIVERISTY

Table 3. Decryption result

C1	**C2**	**C3**	**C4**	**C5**	**C6**	**C7**	**C8**	**C9**	**C10**
V	P	L	Z	J	X	T	K	W	]
86	80	76	90	74	88	84	75	87	93
K1	**K2**	**K3**	**K4**	**K5**	**K6**	**K1**	**K2**	**K3**	**K4**
1	2	3	4	5	6	1	2	3	4
P1	**P2**	**P3**	**P4**	**P5**	**P6**	**P7**	**P8**	**P9**	**P10**
85	78	73	86	69	82	83	73	84	89
U	N	I	V	E	R	S	I	T	Y

Table 2 is the result of the Gronsfeld Cipher calculation. Table 3 is the result of the decryption. The calculation results show there are no errors in mathematical calculations in both algorithm processes.

4. CONCLUSION:

Gronsfeld Cipher is a development of Vigenere Cipher. Gronsfeld Cipher is named after its inventor such as Johann Franz Graf Gronsfeld-Bronkhorst. He was the imperial commander in the Bavarian national revolt of 1705-1706. Gronsfeld is identical to Vigenere Cipher, but the difference is that this cipher key uses numbers while Vigenere uses the alphabet. The advantage of Gronsfeld Cipher is that the key is not a word, but the weakness of the cipher is the same as that of Vigenere such as the key can be rotated to produce plaintext. The power of Gronsfeld Cipher is on a long key. This algorithm is straightforward to implement and has a high speed.

REFERENCES:

1. Hariyanto dan A. P. U. Siahaan, “Intrusion Detection System in Network Forensic Analysis and,” *IOSR J. Comput. Eng.*, vol. 18, no. 6, hal. 115–121, 2016.
2. H. Ming dan S. LiZhong, “A New System Design of Network Invasion Forensics,” in *2009 Second International Conference on Computer and Electrical Engineering*, 2009, hal. 596–599.
3. V. Tasril, M. B. Ginting, Mardiana, dan A. P. U. Siahaan, “Threats of Computer System and its Prevention,” *Int. J. Sci. Res. Sci. Technol.*, vol. 3, no. 6, hal. 448–451, 2017.
4. A. P. U. Siahaan, “Dynamic Key Matrix of Hill Cipher Using Genetic Algorithm,” *Int. J. Adv. Appl. Sci.*, vol. 6, no. 4, hal. 313–318, 2017.
5. A. P. U. Siahaan, “Genetic Algorithm in Hill Cipher Encryption,” *Am. Int. J. Res. Sci. Technol. Eng. Math.*, vol. 15, no. 1, hal. 84–89, 2016.
6. I. Sumartono, A. P. U. Siahaan, dan N. Mayasari, “An Overview of the RC4 Algorithm,” *IOSR J. Comput. Eng.*, vol. 18, no. 6, hal. 67–73, 2016.
7. I. Sumartono, A. P. U. Siahaan, dan Arpan, “Base64 Character Encoding and Decoding Modeling,” *Int. J. Recent Trends Eng. Res.*, vol. 2, no. 12, hal. 63–68, 2016.
8. A. Lubis dan A. P. U. Siahaan, “Network Forensic Application in General Cases,” *IOSR J. Comput. Eng.*, vol. 18, no. 6, hal. 41–44, 2016.
9. W. Stallings, *Cryptography and Network Security: Principles and Practice*. New Jersey: Prentice Hall Press, 2013.
10. M. Abror, “Pengertian dan Aspek-Aspek Keamanan Komputer,” 2018. [Daring]. Tersedia pada: https://www.ayoksinau.com/pengertian-dan-aspek-aspek-keamanan-komputer-lengkap/. [Diakses: 01-Okt-2018].
11. D. Abdullah *et al.*, “Super-Encryption Cryptography with IDEA and WAKE Algorithm,” *J. Phys. Conf. Ser.*, vol. 1019, hal. 012039, Jun 2018.
12. A. . Paul, P. Mythili, dan K. Paulose Jacob, “Matrix based cryptographic procedure for efficient image encryption,” in *2011 IEEE Recent Advances in Intelligent Computational Systems*, 2011, hal. 173–177.
13. S. Muhammad, “Belajar Kriptografi dengan Teknik Subtitusi & Transposisi,” *New Generation*, 2014. .
14. J. A. Buchmann, *Introduction to Cryptography*, 1st ed. Berlin: Springer-Verlag, 2000.
15. Mesran, “Gronsfeld Cipher,” *Wordpress*, 2011. [Daring]. Tersedia pada: https://mesran.wordpress.com/2011/07/03/gronsfeld-cipher/. [Diakses: 01-Okt-2018].
16. D. Apriadi, “Kriptografi Kunci Simetris Gronsfeld Chiper,” *Blogspot*, 2016. [Daring]. Tersedia pada: https://dodi-apriadi.blogspot.com/2016/02/kriptografi-kunci-simetris-gronsfeld.html. [Diakses: 01-Okt-2018].