P-ISSN : 2715-2448 | E-ISSN : 2715-7199
Vol.1 No.2, 10 July 2020
Buana Information Tchnology and Computer Sciences (BIT and CS)

Password Data Authentication Using a Combination of MD5 and Playfair Cipher Matrix 13x13

Bayu Priyatna [1]
Technology Information
Faculty of Engineering Computer
Universitas Buana Perjuangan Karawang
bayu.priyatna@ubpkarawang.ac.id

April Lia Hananto [2]
School of Computing,
Faculty of Engineering
Universiti Teknologi Malaysia
hananto1983@graduate.utm.my

***Abstract*—Data security and confidentiality are the most important things that must be considered in information systems. To protect the cryptographic algorithm reliability it uses. MD5 is one technique that is widely used in password data security issues, which algorithm has many advantages including. MD5 has a one-way hash function so that the message has been converted to a message digest, and it is complicated to restore it to the original message (plaintext). In addition to the advantages of MD5 also has a variety of shortcomings including; very easy to solve because MD5 has a fixed encryption result, using the MD5 modifier generator will be easily guessed, and MD5 is not proper because it is vulnerable to collision attacks. The research method used in this study uses Computer Science Engineering by conducting experiments combining two cryptographic arrangements. The results obtained from this study after being tested with Avalanche Effect technique get ciphertext randomness results of 44.12%, which tends to be very strong to be implemented in password data authentication.**

Keywords— Information systems, MD5, Playfire Cipher.

Abstrak*—*Keamanan dan kerahasiaan data merupakan hal terpenting yang harus diperhatikan pada sistem informasi. untuk menjahganya dibutuhkan kehandalan algoritma kriptografi yang digunakannya. MD5 merupakan salah satu teknik yang banyak digunakan dalam masalah keamanan data password, yangmana algoritma ini memiliki banyak kelebihan diantaranya. MD5 memiliki fungsi hash satu arah sehingga pesan yang telah diubah menjadi message digest (pesan ringkas), dan sangat sulit untuk mengembalikannya ke-pesan semula (plaintext). Selain kelebihan MD5 juga memiliki berbagai macam kekurangan diantaranya; sangat mudah di pecahkan karena MD5 memiliki hasil enkripsi yang tetap, dengan menggunakan generator pengubah MD5 akan dengan mudah ditebak, dan MD5 kurang bagus karena rentan terhadap serangan collision attack. Metode penelitian yang digunakan pada penelitian ini menggunakan Rekayasa Computer Science dengan melakukan eksperimen penggabungan dua metode kriptografi. Hasil yang didapat dari penelitian ini setelah di uji dengan teknik Avalanche Effect mendapatkan hasil keacakan cipherteks 44,79% yang cenderung sangat kuat untuk di implementasikan pada autentikasi data password.

Kata Kunci—Sistem Informasi, MD5, Playfire Cipher.

I. INTRODUCTION

The issue of data security and confidentiality is one of the essential things of information systems [1]. The technique that can be used to maintain data content is to use cryptographic techniques [2]. Cryptographic techniques aim to provide security services, including security, to manage data authentication such as passwords [3].

MD5 is a One-Way hash function designed by Ron Rivest with a 128-bit hash value. It says the One-Way hash function because messages that have been converted to digest messages (full messages) are complicated to restore to the original message (plaintext) [4]. MD5 is one of the One Direction hash functions that is widely used to resolve the integrity of a file [5]. MD5 is implemented in networks that produce 640-bit message digest [6]. MD5 will be a high-security network for transferring data in cellular systems [7].

MD5 is the result of encryption that is made easy to guess, although one-way MD5 will be much easier to hack just using an MD5 modifier generator will produce a straightforward match. The MD5 encryption method is not suitable because it is vulnerable to collision attacks [8].

From these questions, this study discusses the authentication agreement on a password by combining the MD5 method hash function and the application of Playfire cryptography.

II. METHOD

The research method used in this research is engineering, namely Theoretical Computer Science, where researchers use a cryptographic technique with the MD5 method and combine it with the playfair algorithm using a 13x13 matrix. The systematic description of the process flow of this study is outlined in Figure II-1 as follows:

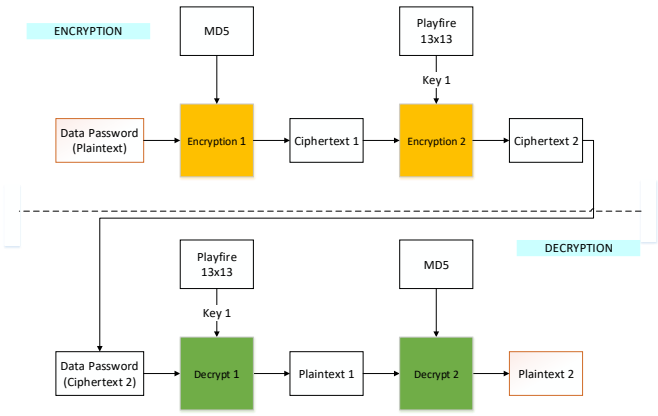

Fig. 1. Research Methods

A. MD5 Algorithm

The hash function is widely used in MD5 and SHA cryptography. In this article, the hash function that is used by MD5 algorithm [9]. MD5 accepts input in the form of messages of any size and produces a message digest that is 128 bits in length [10].

MD5 processes 512-bit blocks, divided into 16 32-bit sub-blocks. The algorithm output is set to 4 blocks, each measuring 32 bits, which, after being combined, will form a 128-bit hash value [11].

The steps in making a message digest, in general, are as follows:

1. Adding padding bits.
2. Add the original message length value.
3. Initialize the MD5 buffer.
4. Processing messages in blocks of 512 bits.

B. Playfair Matrix 13x13

Formation of a 13 x 13 Playfair matrix table of keys that have been entered, on the formation of a key consisting of letters, numbers and symbols, For example, the example key "AkuM@Ululu5". The first step is a key that consists of numbers, letters or symbols should not have more than one appearance if there are these things, then eliminate numbers, letters or symbols that have similarities. So the key from "AkuM@Ululu5" becomes "AkuM@Ul5"[2];[12]. In Table III-2 is a matrix formed by the key "AkuM@U15":

A	k	u	M	@	U	1	5	B	C	D	E	F
G	H	I/J	K	L	N	O	P	Q	R	S	T	V
W	X	Y	Z	a	b	c	d	e	f	g	h	i/j
m	n	o	p	q	r	s	t	v	w	x	y	z
0	1	2	3	4	6	7	8	9	®	©	╬	¶
Đ	┤	_	^	&	*	(	)	-	=	+	[	@
]	;	,,	:	"	\	,	.	/	<	>	?	~
£	¥	|	ß	π	σ	μ	#	∞	±	≥	≤	{
÷	{	}	Ă	Ą	È	Ė	Ę	Ě	Ì	Í	Ĩ	}
Ĭ	Đ	Ñ	Ò	Ó	Ô	Õ	Ö	Ø	Ù	Ú	Û	!
Ý	Á	á	â	ã	Å	Ω	Ç	è	É	ê	ë	⌈
ì	Í	î	ï	ð	Ñ	ò	Ó	ô	Õ	ù	⌂	$
₊	⌉	∑	≠	ğ	€	Ω	λ	Ľ	Đ	Ĭ	Ý	⊣

Fig. 2. Playfair Matrix 13x13 [2];[13].

C. Playfire Encryption Algorithm

Before doing the encryption process, the plaintext to be encrypted is set as follows:

1. All characters and spaces not included in the alphabet must be removed from the plaintext (if any).
2. If there is a letter J in the plaintext make changes with the letter I.
3. The plaintext, which is the original message, is arranged according to the letter pair (bigram).
4. When there are the same pair of letters, do it change one of the letters of the letter pairs with the letter Z or X insert using the letter X because the letter X is very minimal at all in bigram, unlike the letter Z, for example, is the word FUZZY.
5. If the letters in the plaintext have an odd number, then select additional messages then add at the end of the plaintext. Other notes can be chosen, for example, the letter Z or X [14].

D. Playfire Decryption Algorithm

Following are the stages of the Playfair cipher algorithm:

1. If there are two letters on the same key line, then each letter is changed using the message to the left.
2. If there are two letters in the same column, later each letter is changed by the message above.
3. If two letters are not located in the same row and column, then replace them with the word in the intersection of the first row of words with the column letter two.
4. Later the second letter is changed using the word at the vertex of the rectangle made from the letter used [15].

III. RESULT AND DISCUSSION

A. Interface System

The application interface built can be seen in Figure 3:

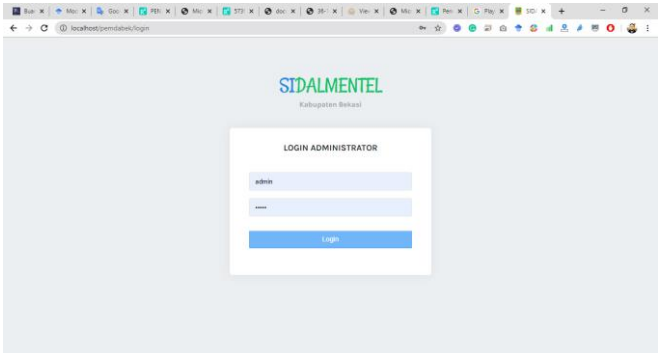

Fig. 3. Form Login Admin

B. Database System

On this system, a database is created with one of the table names db_user as the sample used. Here is Figure 4 that shows the attributes of the user table and Figure 5 shows the results of encryption:

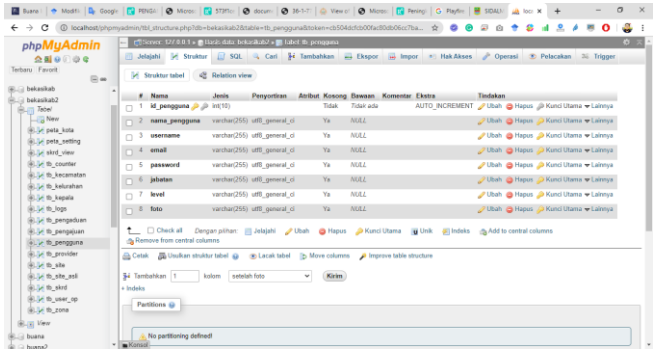

Fig. 4. User Table Structure

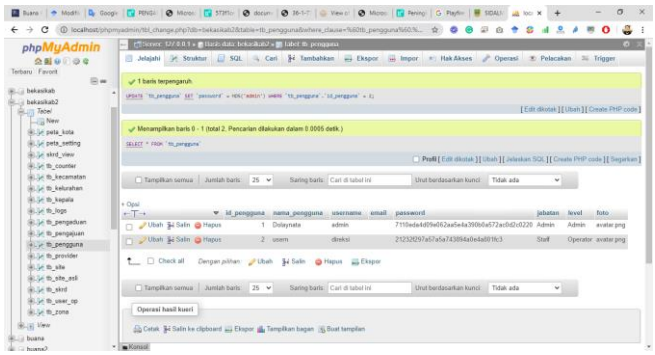

Fig. 5. Password Encryption Results

C. Ciperteks Randomness Test

In the ciphertext randomness test, 30 trials were performed with random sample parameters based on the same data size, character length, and key. The results of the experiment using the calculation of the Avalanche Effect method with the formula:

$$\textit{Avalanche Effect} = \frac{\text{number of bit changes}}{\text{the total number of chipload bit}} \text{ x } 100\% \quad (4.1)$$

In general, bits in ciphertext will change from the number of bits in plaintext by 50%. The avalanche effect is approved well if the resulting bit change gets 45-60% (about half): the more changes that occur, the more difficult cryptographic algorithms to be completed or have high complexity. Landslide Implementation Effect of the number of bit changes obtained from the XOR calculation from the plaintext and ciphertext distribution to binary numbers, then prove the combined MD5 with the Playfair 13x13 algorithm. Graph of Landslide Effects:

Table III-1 Comparison of Ciphertext Randomness Test Results

No	Data Password	Plaintext length (bit)	Afvalanche Effect
1	Sample 1	142	43,18
2	Sample 2	482	41,31
3	Sample 3	993	45,07
4	Sample 4	1287	47,06
5	Sample 5	1.981	47,51
6	Sample 6	2.212	40,87
7	Sample 7	3.580	45,34
8	Sample 8	3.780	47,31
9	Sample 9	4.324	44,96
10	Sample 10	5.520	45,15
11	Sample 11	5.804	46,93
12	Sample 12	6.916	48,77
13	Sample 13	7.882	44,92
14	Sample 14	8.576	45,01
15	Sample 15	18.796	45,97
16	Sample 16	10.940	38,81
17	Sample 17	16.980	43,62
18	Sample 18	12.176	45,43
19	Sample 19	31.992	44,94
20	Sample 20	19.840	39,61
21	Sample 21	33.372	40,14
22	Sample 22	35.796	39,96
23	Sample 23	25.692	44,40
24	Sample 24	38.680	44,80
25	Sample 25	58.286	44,48
26	Sample 26	70.212	40,10
27	Sample 27	95.890	44,73
28	Sample 28	121.748	44,49
29	Sample 29	138.780	44,15
30	Sample 30	141.468	44,63
Avalanche Effect Average Score			**44,12**

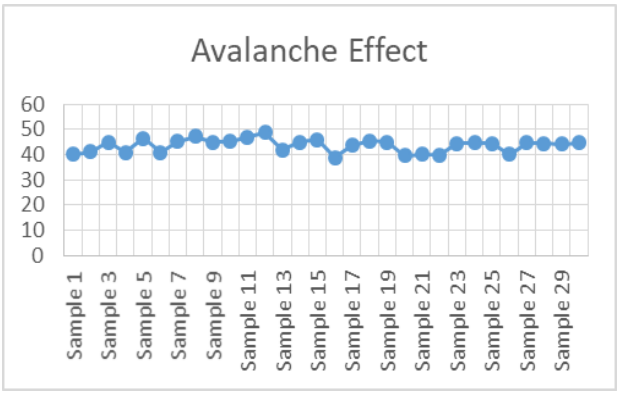

Fig. 6. Avalanche Effect Test Results

CONCLUSION

Based on the results of research conducted, password authentication data security can answer the hypothesis at the beginning of the study by applying the MD5 algorithm and then combining it with Playfair 13x13, which can improve

the security data on the previous MD5 password algorithm, with the Avalanche Effect test results of 44.79%. Besides having the strength of the MD5 encryption technique with a combination of Playfire 13x13 can cover the deficiencies found in the MD5 method.

REFERENCES

[1] Inayatullah, "Analisis Penerapan Algoritma MD5 Untuk Pengamanan Password," *J. Algoritm.*, vol. 3, no. 3, pp. 1–5, 2017.

[2] D. Kurniawan and B. Priyatna, "Pengamanan Data Berbasis Mobile Android Dengan Penggabungan Linear Feedback Shift Register (LFSR) Dan Modifikasi Matriks Kunci Algoritma Kriptografi Playfair Cipher," *J. Telemat. MKOM Vol*, vol. 10, no. 1, 2018.

[3] B. Priyatna and A. L. Hananto, "ZFONE SECURITY ANALYSIS OF VIDEO CALL SERVICE USING GENERAL NEWORK DESIGN PROCESS METHOD (GNDP)."

[4] A. L. Hananto, A. Solehudin, A. S. Y. Irawan, and B. Priyatna, "Analyzing the Kasiski Method Against Vigenere Cipher," *arXiv Prepr. arXiv1912.04519*, 2019.

[5] N. Hayati, M. A. Budiman, and A. Sharif, "Implementasi Algoritma RC4A dan MD5 untuk menjamin Confidentiality dan integrity pada file teks," *SinkrOn*, vol. 1, no. 2, 2017.

[6] D. Sharma, P. Sarao, and S. Dudi, "Implementation of Md5-640 Bits Algorithm," *Int. J. Adv. Res. Comput. Sci. Manag. Stud.*, vol. 3, no. 5, pp. 286–293, 2015.

[7] A. Qashlim and Rusdianto, "Implementasi Algoritma Md5 Untuk Keamanan Dokumen," *J. Ilm. Ilmu Komput.*, vol. 2, no. 2, pp. 10–16, 2016.

[8] T. F. Prasetyo and A. Hikmawan, "Analisis Perbandingan Dan Implementasi Sistem Keamanan Data Menggunakan Metode Enkripsi RC4 SHA Dan MD5," *INFOTECH J.*, vol. 2, no. 1, 2016.

[9] M.-J. Wang and Y.-Z. Li, "Hash function with variable output length," *2015 Int. Conf. Netw. Inf. Syst. Comput.*, pp. 190–193, 2015.

[10] Z. Musliyana, T. Y. Arif, and R. Munadi, "Peningkatan Sistem Keamanan Autentikasi Single Sign On (SSO) Menggunakan Algoritma AES dan One-Time Password Studi Kasus: SSO Universitas Ubudiyah Indonesia," *J. Rekayasa Elektr.*, vol. 12, no. 1, p. 21, 2016.

[11] I. Hmac-sha and H.-P. Ipsec, "Implementasi Hmac-Sha1,Tripledes-Cbc,Hmac-MD5-96 Pada IPsec," no. May, 2016.

[12] D. Kurniawan, A. L. Hananto, and B. Priyatna, "Modification Application of Key Metrics 13x13 Cryptographic Algorithm Playfair Cipher and Combination with Linear Feedback Shift Register (LFSR) on Data Security Based on Mobile Android," *Int. J. Comput. Tech. -–*, vol. 5, no. 1, pp. 65–70, 2018.

[13] A. L. Hananto and A. R. Priyatna, Bayu, "Android Data Security Using Cryptographic Algorithm Combinations," *Int. J. Psychosoc. Rehabil.*, vol. Volume 24, no. Issue 7, pp. 3307–3318, 2020.

[14] R. M. Marzan and A. M. Sison, "An Enhanced Key Security of Playfair Cipher Algorithm," in *Proceedings of the 2019 8th International Conference on Software and Computer Applications*, 2019, pp. 457–461.

[15] E. H. Nurkifli, "Modifikasi Algoritma Playfair Dan Menggabungkan Dengan Linear Feedback Shift Register (Lfsr)," vol. 2014, no. Sentika, 2014.