Indonesian Journal of Electrical Engineering and Computer Science
Vol. 14, No. 3, June 2019, pp. 1286~1290
ISSN: 2502-4752, DOI: 10.11591/ijeecs.v14.i3.pp1286-1290

Data cryptography based on musical notes on a fingerboard along with a dice

Asis Kumar Tripathy, Tapan Kumar Das and Navaneethan C
Schhol of Information Technology and Engineering, VIT, Vellore, India

Article Info

Article history:

Received Jul 6, 2018
Revised Sep 7, 2018
Accepted Feb 22, 2019

Keywords:

Dice
Finger board
Musiacal notes
Security

ABSTRACT

The security of an online system is the foremost necessity nowadays. With huge growth of the IT power and with the invention of new technologies, the number of threats a user faces is growing exponentially. Cryptography is a combination of security engineering and mathematics. It is the best technology for securing distributed systems. Cryptography consists in processing plain information by applying a cipher and producing encoded output, unknown to a third-party who does has no idea about the key. In cryptography both encryption and decryption phase are processed by one or more keys. Encryption is extremely important for a safe and secure environment for the computers and the Internet.

Corresponding Author:

Asis Kumar Tripathy,
Schhol of Information Technology and Engineering,
VIT, Vellore, India.
Email: asistripathy@vit.ac.in

1. INTRODUCTION

In cryptography, encryption is the process of encoding messages (or data) in such a way that provides access only to the authorized parties and it safe from drudgers, hashers and hackers. In an encryption scheme, the message or data (referred to as text) is encrypted using an encryption algorithm, converting it into an unreadable coded text. Decryption is the reverse process to Encryption. In the proposed system the encryption and decryption concepts is dealt using the musical notes that is represented by different patterns over a music board (FRET) [1], [2]. The Cryptography algorithm uses the layout of the musical notes on a finger board in standard tuning combined with a random key generated through a predefined function similar to that of throwing a dice. The proposed algorithm provides a speedy secure system that uses keys from two different platforms instead of using decimal numbers as both the keys [3]. This technology can be used for securing online systems and for cloud computing systems as well that makes the servers secure [4].

1.1. Background

This section includes an introduction to the musical board. Since the system deals with cryptography it uses conversion of decimal numbers to binary numbers. Hence the user should be familiar with the conversion of decimal to binary and vice versa.

1.2. Problems on Music Notes

A fret board also know as musical board consists of various divisions known as frets. Over each fret board are the cords which when pressed against a fret produces a musical note. Each fret on a music board produces a unique note on a distinct cord.

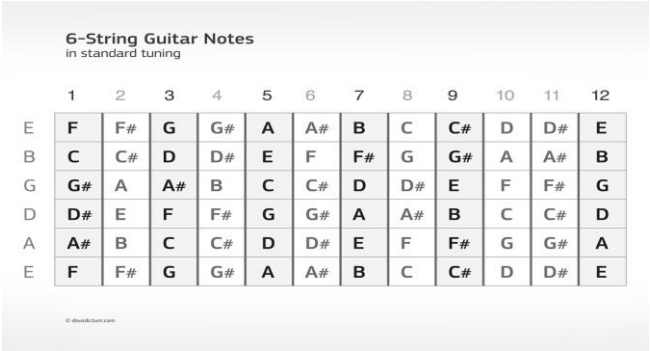

Figure 1. Six-String Guitar Notes

2. PROPOSED SYSTEM

The System consists of a method to encrypt and decrypt messages using a combination of musical notes and a dice.

2.1. Encryption

The algorithm starts by throwing a dice and selecting randomly (1, 2, 3, 4, 5, 6) and then the corresponding note is derived whose position on the FRET will be the required fret (1 to 12).

Group = ((ASCII values of alphabet)-65)/7

Table 1 shows the division of alphabets into the group and the notes used to denote them. Table 2 shows the ASCII encodings of English Alphabets.

Table 1. The Division of Alphabets

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

Group is selected from the data present in Table 1 and Table 2 the corresponding note is selected according to the Table 1. Then the fret number is observed on the random string at which the corresponding note is located, as shown in Figure 1. The final output contains the following parts:

Group number + (Fret Number + Dice Value) + Fret Number

The group number consists of 4 bits. If all the bits are 1 (i.e. 1111) then the encoded character is a space. In case the first two bits are 11 then the encoded letter is a small case letter and if the first two bits are 00 then it is a capital letter.

For Example: Encrypting a string “MeN”.

a) First a dice is thrown to select a random guitar string. Let 1 be the selected string for ‘M’.
b) Group Calculation: (77-65)/7=1.
c) From the table we can see that musical note corresponding to letter ‘M’ is ‘F’.
d) Now on string 1 musical note ‘F’ can be found on 1st fret. So M will be encoded as 1 2 1 in binary i.e. 0001 0000010 0001.
e) For letter ‘e’ let the random string selected be 4.
f) Now the group selected will be 0 and corresponding musical note will be ‘E’ so on the third string the ‘E’ note will be at fret number 2. So ‘e’ will be encoded as 0 6 2 converting to binary 0000 0000110 0010 but because of small case output will be 1100 0000110 0010.
g) Similarly taking random number for N as 6.
h) N will be encoded as 1 13 7.

Table 2. The ASCII Encodings of English Alphabets

Decimal	Character	Decimal	Character
65	A	97	a
66	B	98	b
67	C	99	c
68	D	100	d
69	E	101	e
70	F	102	f
71	G	103	g
72	H	104	h
73	I	105	i
74	J	106	j
75	K	107	k
76	L	108	l
77	M	109	m
78	N	110	n
79	O	111	o
80	P	112	p
81	Q	113	q
82	R	114	r
83	S	115	s
84	T	116	t
85	U	117	u
86	V	118	v
87	W	119	w
88	X	120	x
89	Y	121	y
90	Z	122	z

Hence the final code is:

Input	Encrypted Code
M	0001 0000010 0001.
E	1100 0000110 0010.
N	0001 0001101 0111

2.2. Decryption

While decrypting first the input is observed. Set of 15 bits are considered if first four bits are not 1111. If first four bits are 1111(blank space) the next 15 bits are considered. Encrypted code is divided into 3 parts 4bits 7bits and 4bits. These set of numbers represent Group number with type, (Fret Number + Random String) and Fret Number respectively. The first two bits of first set are considered to check the case of letter (upper-00 or lower-11). The randomly generated dice value is calculated by subtracting third set of number from second set of number. Musical Note is found according to the fret board diagram using the random string number and the fret position in that string. Then using the Note and group number the code is decrypted.

For Example: Let **0001 0000010 0001 1100 0000110 0010 0001 0001101 0111** be the input string.

1. To decrypt the above code, we consider the first 15 bits (first 4 are not 1111) and divide it into 4 bit-7bit-4bit.So for above code it will be: **0001 0000010 0001**.
2. Since first two bits are 00, the letter is capital.
3. The group number is calculated by using the next two bits 01 i.e. Group 1.
4. Fret Number is found using third set of numbers 0001 i.e. 1 and Dice Value is 2-1=1.
5. So in 1st string on fret number 1 musical note is '**F**'.
6. Then using the group table (Table 1) the character can be found as '**M**'. Hence the first character is decrypted as 'M'.

On further processing the code is decrypted as MeN.

3. RESULT ANALYSIS

The proposed algorithm worked fine in converting a 32 kb file and the time required was in competence with the existing algorithms. The simulation result shown in Figure 2 exihibits the proposed methodology gives better performance compared to DES but it takes more time as compared to AES and RSA. The proposed system due to its multifactor encryption provides extra security as it uses multiple

parameters to generate the key and decryption also uses multiple parameters which includes random number dice function that makes the system more secure.

Table 3. Conversion Time for 32kb File

Algorithm Name	Encryption Time	Decryption Time
DES	0.27	0.44
RSA	0.13	0.15
AES	0.15	0.15
Proposed algorithm	0.18	0.22

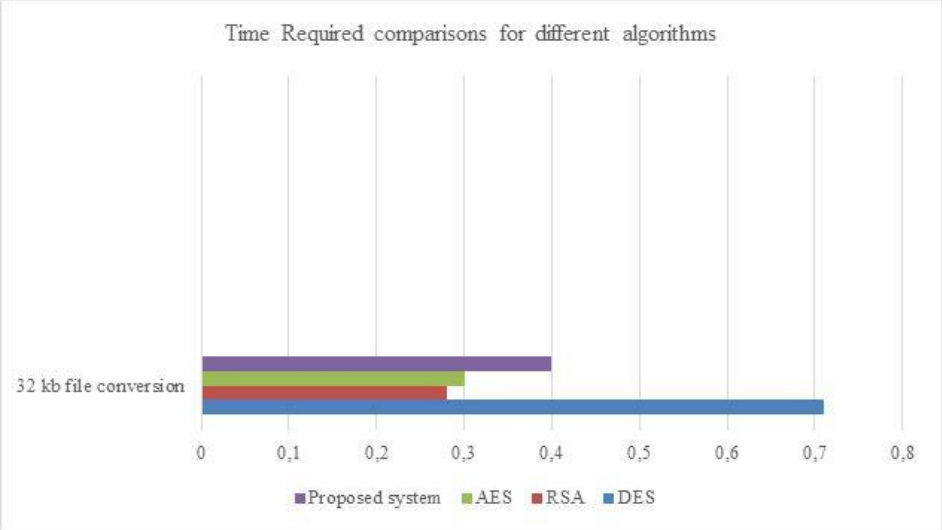

Figure 2. Time comparison graph for a 32kb file

4. CONCLUSION

In this paper the proposed system is a combination of two existing encryption environments and hence provides double safety encryption to transfer a message to the receiver using the layout of a FRET board as a key. Since the keys of FRET are unknown to most of the people it is difficult to decrypt and the existence of a random number generation through dice provides extra safety for the algorithm. For encryption of any alphabet six different codes are available, as a random string is chosen out of six different strings using a dice. This increases the system security by a great extent. So the proposed algorithm is very efficient and safe to use.

REFERENCES

[1] M. Yamuna, Mukesh Kumar Dangi, Kishan Singh, "Encryption of a binary string using DNA sequence", The International Journal of Computer Science & Application, 2 (2), April 2013.
[2] V.M. Chandrasekaran, A. Manimaran, Akhil Ranjan,"Cryptography using a Pair of Dice", International Journal of Pharm Tech Research, 7(1) (2014), 85-89.
[3] Jiang, Xia. "Analysis of Music Content Based on Audio Authentication Algorithm." AGRO FOOD INDUSTRY HI-TECH28, no. 3 (2017): 2317-2320.
[4] Manimaran, A., V. M. Chandrasekaran, Manish Gaur, Ayush Gupta, and Pulkit Narwani. "Data Encryption and Decryption Using Guitar Strings." International Journal of Pharmacy and Technology 7, no. 3 (2015): 9774-9778.
[5] Kumar, Chandan, Sandip Dutta, and Soubhik Chakraborty. "A Hybrid Polybius-Playfair Music Cipher." International Journal of Multimedia and Ubiquitous Engineering 10, no. 8 (2015): 187-198.
[6] Kumar, Chandan, Sandip Dutta, and Soubhik Chakraborty. "Hiding Messages using Musical Notes: A Fuzzy Logic Approach." International Journal of Security and Its Applications 9, no. 1 (2015): 237-248.
[7] Changkai, Xu, Xiao Jinlin Du Jiagang, and Sun Wei. "Digital music copyright protection engineering based on encryption and digital watermarking." Green Communications and Networks 54 (2014): 355.
[8] Yamuna, M., A. Sankar, Siddarth Ravichandran, and V. Harish. "Encryption of a Binary String using music notes and graph theory." International Journal of Engineering and Technology 5, no. 3 (2013): 2920-2925.
[9] Dutta, Sandip, Chandan Kumar, and Soubhik Chakraborty. "A symmetric key algorithm for cryptography using music." International Journal of Engineering and Technology 5, no. 3 (2013): 3109-3115.

[10] Kumar, Chandan, Sandip Dutta, and Soubhik Chakraborty. "Hiding Messages using Musical Notes: A Fuzzy Logic Approach." International Journal of Security and Its Applications 9, no. 1 (2015): 237-248.
[11] Xu, Chang-Kai, and Yao-Cai Wang. "Music Protection Based on Digital Watermarking and Encryption." Journal of China University of Mining and Technology 13, no. 1 (2003): 60-65.
[12] Han, JungKyu, Hye-Young Chang, Seongje Cho, and Minkyu Park. "EMCEM: an efficient multimedia content encryption scheme for mobile handheld devices." In 2008 International Conference on Information Science and Security (ICISS 2008), pp. 108-114. IEEE, 2008.
[13] Kaur, Chandanpreet, and Ravi Kumar. "Classification of melodic structures using fuzzified n-gram matching scores." In 2016 IEEE International Conference on Fuzzy Systems (FUZZ-IEEE), pp. 685-690. IEEE, 2016.
[14] Dutta, Sandip, Soubhik Chakraborty, and N. C. Mahanti. "Using Raga as a Cryptographic Tool." In International Conference on Network Security and Applications, pp. 178-183. Springer, Berlin, Heidelberg, 2011.
[15] Wyld, David C., Michal Wozniak, Nabendu Chaki, Natarajan Meghanathan, and Dhinaharan Nagamalai, eds. Advances in Network Security and Applications: 4th International Conference, CNSA 2011, Chennai, India, July 15-17, 2011, Proceedings. Vol. 196. Springer, 2011.