E-Health System Based KED and DNA Cryptosystem

Htet Htet Naing
University of Computer Studies
Yangon, Myanmar
htethtetnaing@ucsy.edu.mm

Zin May Aye
University of Computer Studies
Yangon, Myanmar
zinmayaye@ucsy.edu.mm

Soe Kalayar Naing
University of Computer Studies
Yangon, Myanmar
soekalayarnaing@ucsy.edu.mm

***Abstract*— Today, technology change is very fast. Security and fast processing are necessary for data transformation. The health system is related to important roles in any country for its national interest. E-health care system include patient treatment result, diagnostic report. Patient Health Information (PHI). Patient health information is securely stored and accesses this data so that only authorized entities can update and retrieve the data over the Internet. Safety becomes an important issue when providing an electric healthcare system because confidential patient data is collected and shared by different users and organizations. Two types of cryptography: Symmetric Key and Asymmetric Key. Using the same keys is Symmetric key and Asymmetric key is using Separate key. In this paper, a Symmetric Key algorithm called as KED (Key Encryption Decryption) using modulo92 is used. Two keys are used in which one is a natural number which is relatively prime to 92. In this paper, KED (Key Encryption and Decryption) algorithm combines AES S-box and DNA cryptography for electronic healthcare security system. In this system, propose an MCS (Medical Center Server) that connects to the patient and the doctor. The proposed system is fast in computing and can withstand cryptographic attacks such as differential and linear cryptanalysis attacks.**

Keywords— Key Encryption and Decryption, E-health care, S-box, DNA, medical center server

I. INTRODUCTION

The security requirements for the healthcare system involve authorization, authentication, non-repudiation integrity, privacy, and confidentiality [3]. The privacy of PHI applies to the individuals and right person to prevent their private information and personal from being accessible [8]. The privacy of PHI is required to be of the highest standard. Physicians generally take out previous PHI data all along a new treatment session, and the currently generated PHI is recollection and updated with new medical records [5]. A patient physically reserves a doctor each time a treatment analysis is needed, after that the patient and generates the patient's diagnostic data are treat to doctor, designated by PHI [2]. The physician uploads the total data of the PHI treatment to the MCS and the patient obtains a copy of the text data of his PHI from the MCS to know the result of the treatment [1]. The security standards of the patient's right to understand how their PHI will be used and stored must be maintained proposed combine symmetric and asymmetric key algorithm called KED (Key Encryption Decryption), AES, DNA cryptography[4]. The same key is used for both decryption and encryption using modulo 92 [8].

II. RELATED WORK

Many cryptographic algorithms have already been proposed and implemented to provide security to the user that your message will remain secure at the moment of communication through the web. But nowadays privacy has become a common practice in society which made such cryptographic algorithms no longer safe. In this article we have studied several symmetric key algorithms and selected one of them to reference in the proposed algorithm.

Proposed an algorithm based on Modulo 37 by Prakash Kuppuswamy, Dr. Saeed Q Y Al-Khalid, in the year 2012.

- two keys are uses: k1=positive integer, k2=negative integer, modulo 37 are using both of inverse to fine, giving k1', k2'.
- Assigning A=1, C=3.Z=26,0=27,9=36, Space=37 for message synthetic value.
- Encryption: CT= (integer value*k1) mod37, CT1=(CT*k2) mod37=Cipher Text. Calculate with modulo 37
- Decryption: (CT1*k1'*k2') mod37,
- In this algorithm have been used for only alphabets and numbers.

III. RESEARCH METHOD

A. *KED key generation*

KED (Key Encryption Decryption) is key generation method and symmetric key algorithm. The proposed algorithm is used for two keys of encryption and decryption process, using modulo92. The encryption process is shown in figure 1. Two keys will be used key1 and key2. The first key key1, is a natural number and k2 can be a combination of English characters A-Z, numbers0-9 and special characters will be derived from the key entered by the user. And m=92.

Key 1= length of the key
Key 2=

$$K2= \left(\sum_{i=0}^{kl-1} 2^{i} * kl * val \right) \bmod m \quad 92$$

i = character of key position.
val= integer value
k1= natural number

B. *Algorithm of KED Encryption*

```
for (i=0; i<messagelength; i++)
{
num1=hm.get(str. charAt(i));
n1=(num1*key1);
n2=(n1+k2)%92;
for(Map. Entry < Character, String > entry:
hm1.entrySet())
{
str1=""+n2;
if (entry. get Value (). equals(str1))
{
Ch.=entry. get Key();
encrypted=encryptedmsg+Ch;
}
}
}
```

C. *DNA cryptography and AES algorithm*

DNA (deoxyribonucleic acid) cryptography achieve more advance calculations processing than binary computations [6]. Four components are using, namely of DNA cryptography C, A, T, and G for computation, considered from the compounds C-Cytosine, A-Adenine, T-Thymine and G-Guanine [3]. The computation instead of their counter binary parts are using these four components.

TABLE 1. DNA COMPONENTS

DNA component	**Binary equivalent**
A	**00**
G	**01**
C	**10**
T	**11**

D. *S-Box in AES*

Substitution box S-Box is used in Rijndael encryption, on which the AES cryptographic algorithm is based. S-boxes provide an invertible (reversible) transformation of plaintext segments during encryption, and the reverse during decryption. The AES (Advanced Encryption Standard) algorithm takes in blocks of 128 ,192 and 256 applies a sequence of permutations and substitutions. The substitutions apply an “S-box”, named the Rijndael S-box after its designers [2], that works on 8 bits at a time an invertible nonlinear transformation. There are 16*16=256 possible 8-bit numbers, and inputs to outputs mapping in 16 by 16 represented in S-box. AES chosen one encryption algorithm is unique nonlinear operation in S-box, and it determines the performance of AES. AES S-box are analyzed the complexity and security of the system. The system proposes the complexity and security increase of AES S-box by combine KED and DNA cryptosystem.

IV. PROPOSED SYSTEM

In proposed system KED that uses module 92, DNA cryptosystem, and AES algorithm. KED, AES and DNA cryptosystem are used in information transform over the internet by key generation uses. The encryption and decryption respectively will be used in AES S-Box Table. Proposed a hybrid of KED (Key Encryption Decryption) that uses module 92, AES algorithm, and DNA cryptography (Key-Adv DNA cryptosystem). The contribution of system is AES which hybrid DNA cryptography for S-Box, advanced encryption standard for fast processing and secured algorithm. The encryption process is using KED, DNA and S Box, to arrange the advance security from the attacks like differential and linear cryptanalysis attacks.

AES S -box changing it into DNA cryptography. DNA cryptography is more advance in computational processing than binary calculations. The combination of DNA cryptography, advanced encryption standard for fast processing and secure algorithm. The AES S-Box algorithm is developed by update and advance DNA cryptography. AES S-Box uses a symmetric key that can be generated by an algorithm.

A. *KED_ADV DNA cryptosystem*

KED (Key encryption Decryption), ADV is use in initial of (Advance encryption Standard) AES and DNA is (deoxyribonucleic acid). KED_ADV DNA is using encryption and decryption of E-health care system. Firstly, the KED is using, user enter the plaintext is convert to integer value by using Table 2. And then, multiply to key K1 and Add to Key K2. The result is mod to 92. After that, using AES S-box value is assigning and the value is converted to Binary value. Lastly, convert to DNA property.

B. *Integer Assigning*

This below table is replaced in integer to encryption and decryption process. This table include 26 characters of A to Z, 26 characters of a-z, special character, space and Number 0-9 etc.

TABLE 2: INTEGER ASSIGNING

<table>
<tr><td>A</td><td>B</td><td>C</td><td>D</td><td>E</td><td>F</td><td>G</td><td>H</td><td>I</td><td>J</td></tr>
<tr><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>9</td><td>10</td></tr>
<tr><td>K</td><td>L</td><td>M</td><td>N</td><td>O</td><td>P</td><td>Q</td><td>R</td><td>S</td><td>T</td></tr>
<tr><td>11</td><td>12</td><td>13</td><td>14</td><td>15</td><td>16</td><td>17</td><td>18</td><td>19</td><td>20</td></tr>
<tr><td>U</td><td>V</td><td>W</td><td>X</td><td>Y</td><td>Z</td><td>a</td><td>b</td><td>c</td><td>d</td></tr>
<tr><td>21</td><td>22</td><td>23</td><td>24</td><td>25</td><td>26</td><td>27</td><td>28</td><td>29</td><td>30</td></tr>
<tr><td>e</td><td>f</td><td>g</td><td>h</td><td>i</td><td>j</td><td>k</td><td>l</td><td>m</td><td>n</td></tr>
<tr><td>31</td><td>32</td><td>33</td><td>34</td><td>35</td><td>36</td><td>37</td><td>38</td><td>39</td><td>40</td></tr>
<tr><td>o</td><td>p</td><td>q</td><td>r</td><td>s</td><td>t</td><td>u</td><td>v</td><td>w</td><td>x</td></tr>
<tr><td>41</td><td>42</td><td>43</td><td>44</td><td>45</td><td>46</td><td>47</td><td>48</td><td>49</td><td>50</td></tr>
<tr><td>y</td><td>z</td><td>0</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td></tr>
<tr><td>51</td><td>52</td><td>53</td><td>54</td><td>55</td><td>56</td><td>57</td><td>58</td><td>59</td><td>60</td></tr>
<tr><td>8</td><td>9</td><td>!</td><td>@</td><td>#</td><td>%</td><td>^</td><td>&</td><td>*</td><td>(</td></tr>
<tr><td>61</td><td>62</td><td>63</td><td>64</td><td>65</td><td>66</td><td>67</td><td>68</td><td>69</td><td>70</td></tr>
<tr><td>)</td><td>+</td><td>-</td><td>_</td><td>=</td><td>:</td><td>“</td><td><</td><td>></td><td>?</td></tr>
<tr><td>71</td><td>72</td><td>73</td><td>74</td><td>75</td><td>76</td><td>77</td><td>78</td><td>79</td><td>80</td></tr>
<tr><td>/</td><td>.</td><td>,</td><td>\</td><td>|</td><td>[</td><td>]</td><td>{</td><td>}</td><td>:</td></tr>
<tr><td>81</td><td>82</td><td>83</td><td>84</td><td>85</td><td>86</td><td>87</td><td>88</td><td>89</td><td>90</td></tr>
<tr><td>‘</td><td>S</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>91</td><td>92</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
</table>

C. Encryption Process

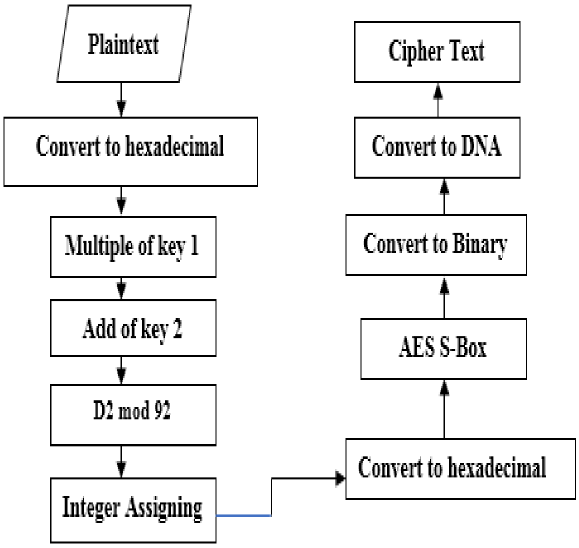

Figure 1: Encryption Process

D. Cryptography based E-health care system

In proposed system, A patient and doctors must register with identity card to MCS (Medical Center Server), which contains all healthcare information. After registration, MCS server send OTP code to doctors and Patients. They are Log in with OTP code and MCS check with their OTP code to Database in this system. Patient or Doctor ID is correct they enter in this system and send Detail information to MCS by using KED_ADV DNA cryptosystem encryption Process. MCS decrypt with Patient information and accessed via the internet for secure handling of patient PHI.

MCS stored Patients and Doctors information and will contact the doctor who can cure the disease of the patient. After the completion of patient PHI treatment session is upload to the MCS and a copy of the same is securely sent to the patient by using KED_ADV DNA cryptosystem. Hybrid of KED algorithm that uses modulo 92, DNA cryptography, and AES algorithm. Two-factor authentication (2FA), sometimes referred to as *two-step verification.* In this system using OTP (One-time password) for Authentication.

A key component is more secure information confidentiality would be encryption. The security of Encryption can read the information is only the right people. KED and AES algorithm used encryption for Confidentiality.

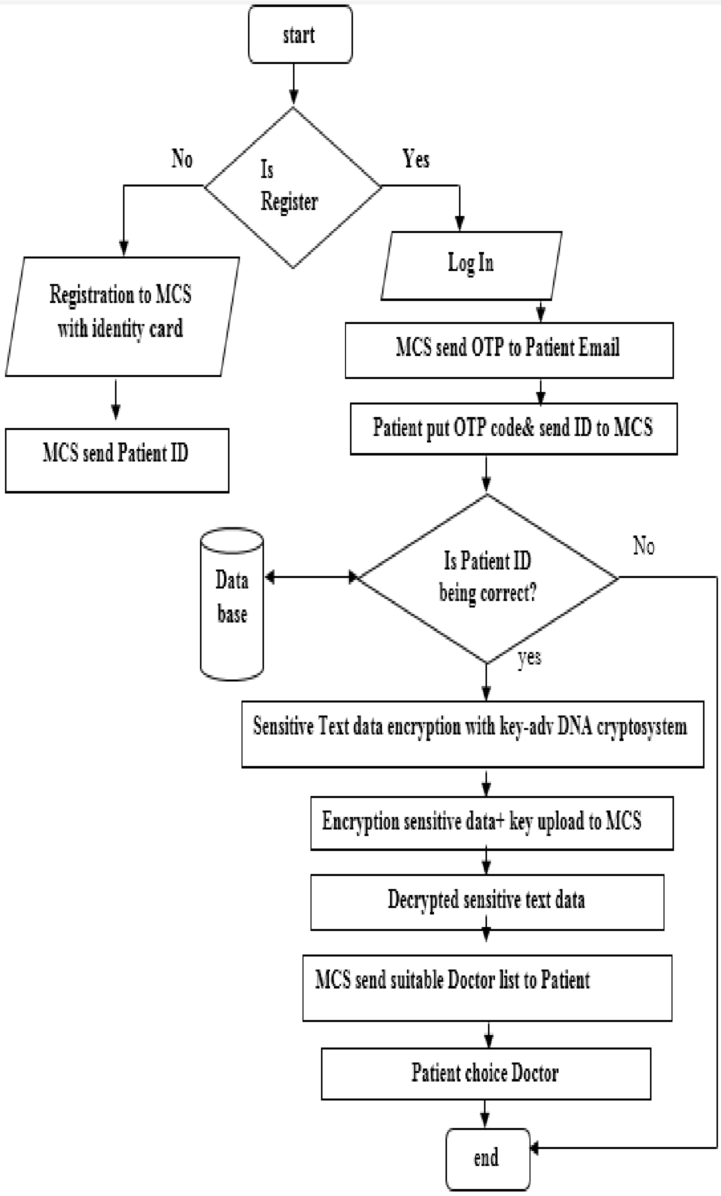

Figure 2: General structure of E -health care system

E. Structure of E-health care system

In this system, patient and doctor must register to MCS. This step patient sends his/her information to MCS. This information includes Patient Name, Address, Male/Female, marital status, Date of Birth, Phone no, E-mail, Symptoms, Disease type. MCS receive patient information form, it sends OTP code to patient and then patient log in to OTP code. MCS save patient information in Database. Doctors registration include Doctor Name, Address, Phone No, E-mail, Degree, graduated country, Treatable disease, Number of Doctor receive. Table 3 is used already have AES S-Box table. The Table 4 process is using to KED (Key encryption and decryption algorithm).

F. MCS (Medical Center Server)

MCS receive doctor and patient information forms, it sends OTP (One Time Passcode) code to Patient/Doctor and then they log in to OTP code. Doctor/Patient information is transfer to MCS by using KED_ADV DNA cryptosystem. The function of MCS is store in patients and doctors of detail information in database. MCS check to their information in database and made between the doctor and patient are connected. MCS sends good doctors list to patients and they choose Doctor. And then, the other side Doctor is chosen to be suitable for the patients.

TABLE 3: AES S-BOX

	00	01	02	03	04	05	06	07	08	09	0a	0b	0c	0d	0e	0f
00	63	7c	77	7b	f2	6b	6f	c5	30	01	67	2b	fe	d7	ab	76
10	ca	82	c9	7d	fa	59	47	f0	ad	d4	a2	af	9c	a4	72	c0
20	b7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1	71	d8	31	15
30	04	c7	23	c3	18	96	05	9a	07	12	80	e2	eb	27	b2	75
40	09	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84
50	53	d1	00	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	58	cf
60	d0	ef	aa	fb	43	4d	33	85	45	f9	02	7f	50	3c	9f	a8
70	51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	f3	d2
80	cd	0c	13	ec	5f	97	44	17	c4	a7	7e	3d	64	5d	19	73
90	60	81	4f	dc	22	2a	90	88	46	ee	b8	14	de	5e	0b	db
a0	e0	32	3a	0a	49	06	24	5c	c2	d3	ac	62	91	95	e4	79
b0	e7	c8	37	6d	8d	d5	4e	a9	6c	56	f4	ea	65	7a	ae	08
c0	ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8b	8a
d0	70	3e	b5	66	48	03	f6	0e	61	35	57	b9	86	c1	1d	9e
e0	e1	f8	98	11	69	d9	8e	94	9b	1e	87	e9	ce	55	28	df
f0	8c	a1	89	0d	bf	e6	42	68	41	99	2d	0f	b0	54	bb	16

V. RESULT AND ANALYSIS

A. *Key Generation Process of KED*

Plaintext: The Students are learning.
K1= 3@! $
Position i= 0 1 2 3
Key length Key 1= 4

$k2=(\sum_{i=0}^{kl-1} 2^i * kl * val) \bmod$ **) 92**

= {(20*4*56) +(21*4*64) +(22*4*63) + (23*4*92)} mod 92
= (224+512+ 1008+ 2944) mod 92
= 4688 mod 92
=88

select a natural number say, Key 1=5

TABLE 4: ENCRYPTION PROCESS OF KED_ADV DNA SYSTEM

Plain text	Integer value (V1)	V1*K1 (C1)	C1+K2 (C2)	C2mod 92	Synthetic Value
T	20	100	188	4	D
h	34	170	258	74	_
e	31	155	243	59	6
S	9	45	133	41	o
t	46	230	318	42	p
u	47	235	323	47	u
d	30	150	238	54	1
e	31	155	243	59	6
n	40	200	288	12	L
t	46	230	318	42	p
s	45	225	313	37	k
a	27	135	223	53	0
r	44	220	308	32	f
e	31	155	243	33	g
l	38	190	278	2	B
e	31	155	243	59	6
a	27	135	223	39	m
r	44	220	308	32	f
n	40	200	288	12	L
i	35	175	263	79	>
n	40	200	288	12	L
g	33	165	253	69	*

Binary value	Hexadecimal Value	AES S-Box	Binary Value	DNA sequence	Cipher text
01000100	44	1b	10001011	CACT	CACT
01011111	5F	cf	11001111	TACT	TACT
00110110	36	05	00001010	AACC	AACC
01101111	6F	a8	10101000	CCCA	CCCA
01110000	70	51	10100010	CCAC	CCAC
01110101	75	9d	10011101	CGTG	CGTG
00110001	31	c7	11000111	TACT	TACT
00110110	36	05	00001010	AACC	AACC
01001100	4C	29	10100100	CCGA	CCGA
01110000	70	51	10100010	CCAC	CCAC
01110101	75	9d	10011101	CGTG	CGTG
00110000	30	04	00001000	AACA	AACA
01100110	66	33	11001100	TACA	TACA
01100111	67	85	10000101	CAGG	CAGG
01000010	42	2c	10001100	CACA	CACA
00110110	36	05	00001010	AACC	AACC
01101101	6D	3c	11001100	TACA	TACA

01100110	66	33	11000011	TAAT	TAAT
01001100	4C	29	10100100	CCGA	CCGA
00111110	3E	b2	10110010	CTGC	CTGC
01001100	4C	29	10100100	CCGA	CCGA
00101010	2A	e5	11100101	TCGG	TCGG

V CONCLUSION

In conclusion, health security needs Confidentiality, Integrity, Authentication, and other important features such as Brute Force Attack, Time Attack, Differential Cryptanalysis Attack, and Linear Cryptanalysis Attack. The possibility of using symmetric encryption algorithm, such as AES, DNA combination with KED, was also studied and implemented. In proposed system, Patient's PHI is stores in MCS, which is securely retrieved / updated by Doctor and MCS, and the patient also their updated PHI receives from MCS. The proposed cryptosystem was able to combine KED using modulus 92 AES and DNA cryptosystem

REFERENCES

[1] J. Warjri, Dr. E. George Dharma Prakash Raj. "KED-A Symmetric Key Algorithm for Secured Information Exchange Using Modulo 69*," I.J Computer Network and Information Security*, vol. 10, pp 37-43, 2013.

[2] Q. Zhang and A. Qunding, "Digital image encryption based on Advanced Encryption Standard(AES) algorithm," *5th Int. Conf. Instrum. Meas. Comput. Commun. Control. IMCCC 2015*, pp. 1218–1221, 2015.

[3] P. K. Panda, "A Hybrid Security Algorithm for RSA Cryptosystem," 2017.Y.

[4] O. A. Dawood, A. M. S. Rahma, and A. M. J. Abdul Hossen, "New Symmetric Cipher Fast Algorithm of Revertible Operations' Queen (FAROQ) Cipher," *Int. J. Comput. Netw. Inf. Secur.*, vol. 9, no. 4, pp. 29–36, 2017.

[5] S. Oukili and S. Bri, "High throughput FPGA Implementation of Data Encryption Standard with time variable subkeys," *Int. J. Electr. Comput. Eng.*, vol. 6, no. 1, p. 298, 2016.

[6] Jie Cui,Liusheng Huang, Hong Zhong, Chinchen Chang, "An improved AES S-box and its performance analysis".International Journal of innovative computing, information and control IJICIC, May 2011.

[7] Edwin R. Arboleda, Carla Eunice R. Fenomeno, Joshua Z. Jimenez. "KED-AES algorithm: combined key encryption decryption and advance encryption standard algorithm.. **IJAAS.** Vol. 8, No. 1, March 2019, pp. 44~53 ISSN: 2252-8814, DOI: 10.11591/ijaas.v8.i1.pp44-53.

[8] G. Jaswanth Varma ,B. Ajani Kumar , Fazal Noorbasha , Harikishore Kakarla , M. Manasa. "DATA SECURITY BASED ON DNA CRYPTOGRAPHY USING S-BOX ENCRYPTION". International Journal of Pure and Applied Mathematics Volume 115 No. 7 2017, 429-434 ISSN: 1311-8080 (printed version); ISSN: 1314-3395 (on-line version)