

Towards Securing Electronic Health Records using Caesar And Affine Cryptographic Techniques

Kolapo Ridwan Olayinka and Sakpere Wilson

Computer Science Department.
Lead City University, Ibadan, Oyo State, Nigeria.

Abstract

The introduction of cryptography has brought plenty of improvement to health informatics, but not really employed in health institutes and this is often as results of the protection issues that come together with the employment of e-Health systems. Security issues is taken into account a significant concern which is why health institutes still opt to follow the normal way of addressing health records. This study aim to ensure data security in health record using enhanced Caesar Cipher, Affine Cipher Cryptographic Techniques.

This method used is considered a double enhanced encryption algorithm because it combines an enhanced Caesar encryption method with Affine Cipher encryption technique to enhance security of medical health records. The integration of the enhanced Caesar and affine ciphers is as follows: First, each field in the record is encrypted with the enhanced Caesar cipher encryption method, and the encrypted output is used as the input for the affine cipher encryption method. The result of this study is presented as a mathematical setup to show how the caesar technique and the affine technique is being implemented to aid the development of this system as a software solution in further studies.

In conclusion, the main aim of cryptographic system is to protect the confidentiality of data both at rest and in transit. With the mix of the enhanced Caesar Cipher method and Affine cipher, these techniques has helped to enhance effectiveness.

Keywords: e-Health, cryptography, encryption, algorithm, Caesar Cipher, Affine Cipher.

1. INTRODUCTION

As the world of technology has progressed, it is also helped within the advancement of health-care sector. Technology has been a major tool within the improvement in fields like diagnosis, medicine, treatment and patient monitoring¹. Securely collecting, maintaining and sharing patient records between hospital servers are often both arduous and costly. In recent years, health personnel in countries round the world are investigating the likelihood of migrating a number of their medical systems to the cloud . Cloud computing is said to be the practice of having a network of resources to store, process and manage data on the web instead of a stationed physical infrastructure.

Information and communication technology (ICT) has brought about the thought of central business model in electronic health. E-Health is defined as “the cost-effective and secure use of data and communications technologies in support of health and health-related fields, including healthcare services, health surveillance, health education, knowledge and research. E-health record basically are stored on a physical devices which makes recovery have certain limitation and might be damaged but a cloud-based electronic health record cannot be damaged unless the cloud cease to exist. A good number of advantages of e-Health are reported, it can reduce time to diagnosis, improve equity of access for patients in remote areas, improve quality of life, and improve patient satisfaction. Additionally, e-Health has the potential to create health care workers more efficient and produce system benefits and technological spin-offs.

Cryptographic techniques play an important role within the field of health informatics, the simplest thanks to secure a message is cryptography. Today, many methods of encryption are supported by public keys. Public-key cryptography is claimed to be the best method in the field of cryptography because it is used for both confidentiality and authentication. In this work, the Caesar method was combined with a block cipher with a higher level of security than the traditional Ceaser method. However, this procedure applies only to type 1024 bits. In this study, the Ceaser and Affine Cipher are combined as a method to improve the effectiveness and security level of the eHealth record system. The Ceasar method is one of the most effective ways to protect your messages and is still in use today, we also use the Affine Cipher method because it has the same properties as the Ceaser method.

2. RELATED WORKS

Munura Maihankali and Esther Chinwe Eze [1] proposed a Symmetric Cryptography for Confidential Communications Implemented by using an Enhancing the Caesar Cipher. The proposed system uses Ceasar Technique with 97 key possibilities and has the limitation of there proposed system that Considering the fact that possible key shift was increased from 26 to 98, this still does not increase data security to a higher extent though better than the conventional ceasar technique.

Mohit Mittal [2] performed an evaluation on 3 encryption algorithm which are DES, 3DES, RUNDAL encryption techniques, in this study metric of evaluation uses just a metric and an outline for implementation was not well outlined.

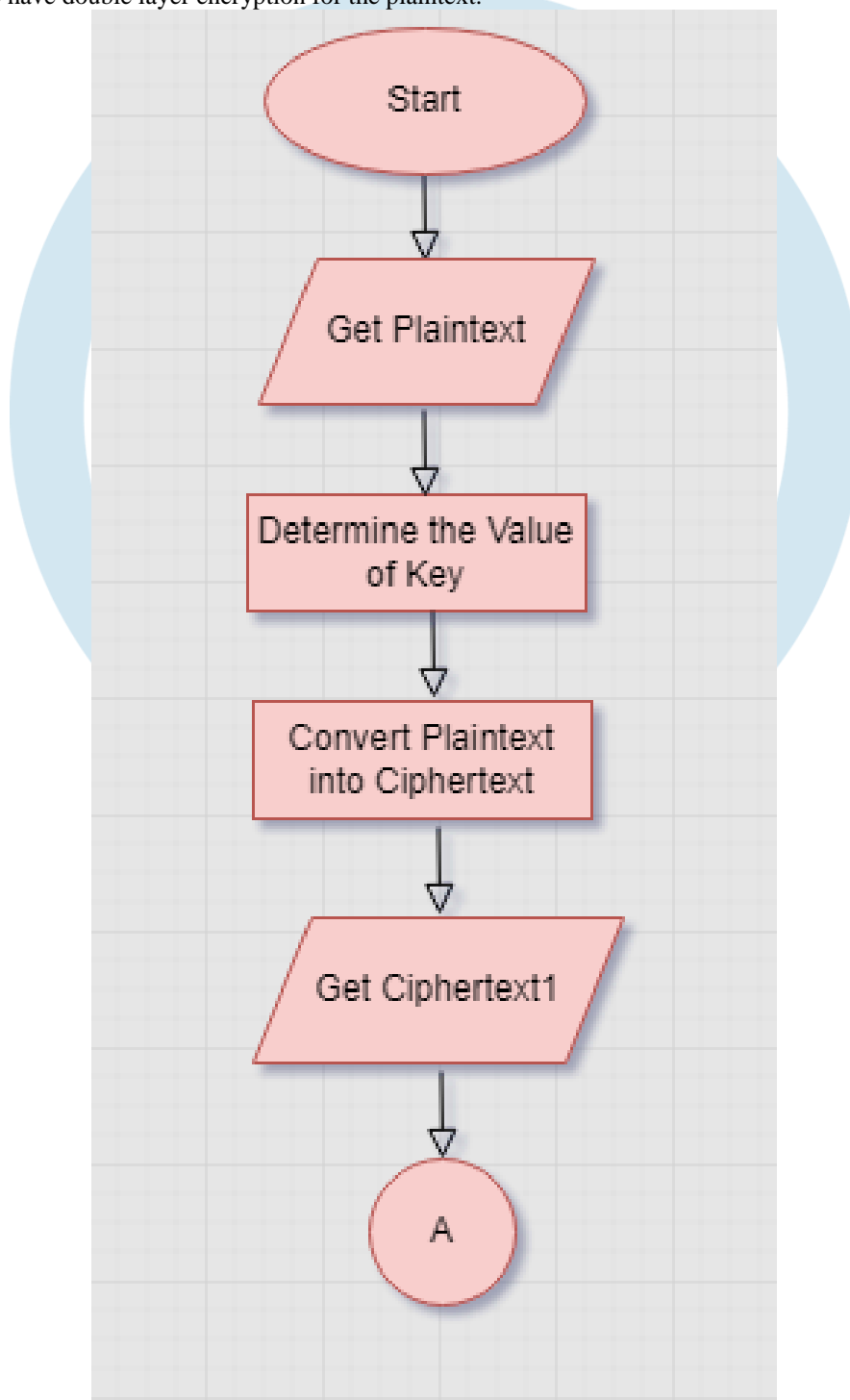
In Ganapathy, Sannasi[3] a proposed system whereby a new LSB-S image steganography method blend with cryptography for secret communication. A method of image coding is proposed that hides the information along a selected pixel and on the next value of the selected pixel, that is, pixel + 1. International journal of advanced research in computer science & software engineering. MATLAB provides more security for secret communication.

In Kumar, Deepak,[4] a system whereby large-scale JPEG image steganalysis using hybrid deep learning framework was proposed. It was proposed that a generic hybrid deep-learning framework for JPEG steganalysis incorporating the domain knowledge behind rich steganalytic models. Digital image steganography using modified LSB & AES cryptography. The cryptographic algorithms are AES, RSA, DES, 3DES and blowfish algorithms, & the steganography technique in LSB.

3. METHODOLOGY

The scheme below illustrates the flow which has the following cryptographic operations performed;

1. After the key has been determined, the medical health records are encrypted using the first crypto technique which is Ceasar Cipher Technique (Ciphertext 1).
2. The cipher text obtained from the first encryption is used as input to the second encryption phase which is the Affine Technique (Ciphertext 2).
3. Therefore, we have double layer encryption for the plaintext.



To encrypt the Caesar cipher:

1. Convert the message character in the plain-text into ASCII code

2. Determine the value of k, then employ the use of transformation

$$CX \equiv V + K \text{ Modulus } 256, 0 \leq P \leq 255$$

3. Convert the code obtained in step 2 into message character

4. The result in step 3 is the cipher-text message

To decrypt the Caesar cipher:

1. Convert the message character in the cipher-text into ASCII code

2. Determine the value of k, then employ the use of transformation

$$P \equiv CX - K \text{ Modulus } 256, 0 \leq P \leq 255$$

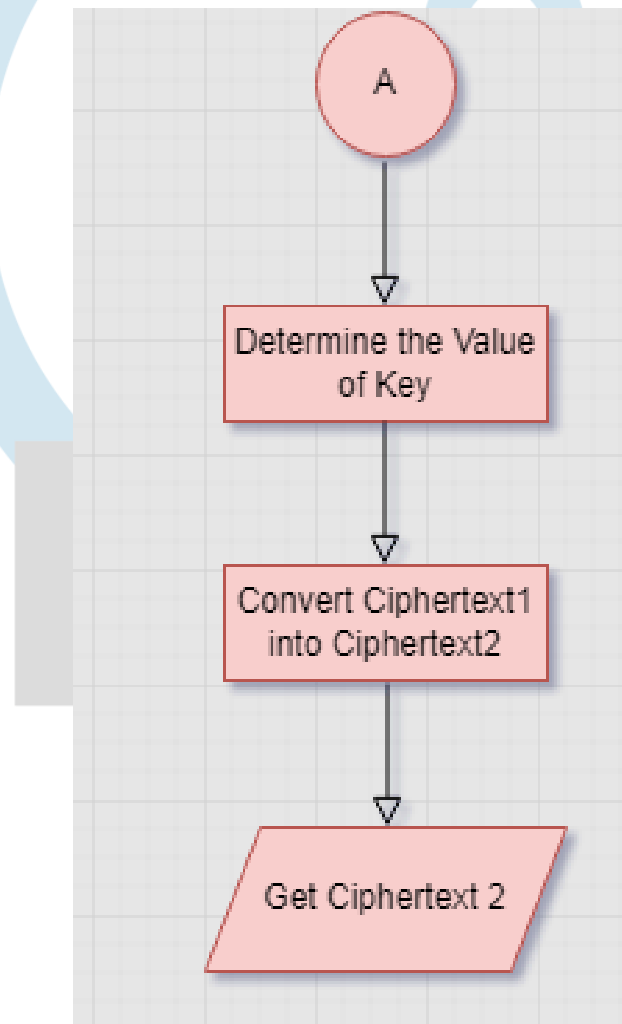
3. Convert the number obtained in step 2 to the message character

4. The results in step 3 are plain-text messages

Where a and b are integers. b is the number of alphabet shifts required. a must be disjoint so that congruence can be expressed in 256 or vice versa [1, 10]. Plaintext (P) based on the description of the relationship between ciphertext (CX) and plaintext (PX).) Is obtained. The plaintext (PX) can be expressed by the following congruence function as the opposite of the ciphertext (CX).

$$P \equiv (\bar{a} (c - b)) \text{ Modulus } 256, 0 \leq c \leq 255$$

Where \bar{a} is the inverse of a (Modulus 26) . \bar{a} can be searched using congruence $\bar{a} \equiv a^{\phi(256)-1} \text{ (Modulus } 256)$. Or you can use the definition that “given an integer a with $(a,m) = 1$, an integer solution x of $ax \equiv 1 \text{ (Modulus } M)$ is called an inverse of a Modulusulo m.” .



To encrypt the affine cipher:

1. Convert the message character into ASCII code

2. Determine the values of a and k, then employ the use of transformation

$$C \equiv ((a * p) + b) \text{ Modulus } 256, 0 \leq P \leq 255$$

3. Convert the code obtained in step b into the message character

4. The results in step c are the cipher-text message

To decrypt the affine cipher:

1. Convert the message character into ASCII code
2. Determine the values of \bar{a} and k , then employ the use of transformation
 $PX \equiv (\bar{a}(c - k)) \text{ Modulus } 256, 0 \leq C \leq 255$
3. Convert the code obtained in step b into the message character
4. The results in step c are plain-text messages

4. RESULTS

Implementation of the encryption Algorithm

If the keyword to be encrypted is the name of a prescription say for instance; PARACETAMOL.

Encryption is done on this particular keyword using the combination of Ceasar and Affine Cipher.

Given that the keys are 8 and 9

$K = 8$ and $a = 9$

$\bar{a} \equiv a^{\phi(256)^{-1}} \text{ (Modulus } 256)$

$\bar{A} = 9 \equiv 9^{\phi(256)^{-1}} \text{ (Modulus } 256) =$

$57 \text{ (Modulus } 256)$ or $9x \equiv 1 \text{ (Modulus } 256)$

$9 \times 57 \equiv 1 \text{ (Modulus } 256)$

Then $x = 57 = \bar{a}$

Encryption 1 will be done using Ceasar Cipher

Implementation of Ceasar Cipher algorithm

Plain Text: PARACETAMOL

The first step is to change the plaintext into ASCII code

	P	A	R	A	C	E	T	A	M	O	L
ASCII	80	65	82	65	67	69	84	65	77	79	76
CX	88	73	90	73	75	77	92	73	85	87	84
Ciphertext1	X	I	Z	I	K	M	\	I	U	W	T

To get the value of CX we use the mathematical formula;

Where V is the ASCII;

$C \equiv V + 8 \text{ Modulus } 256;$

$C \equiv 80 + 8 \text{ Modulus } 256$

$C \equiv 88 \text{ Modulus } 256$

$C \equiv 88$

$C = CX.$

The above mathematical steps shows are CX is derived for one of the letters in the plaintext.

Implementation of Affine Cipher

Since Ciphertext 1 is obtained from the Ceasar encryption, the Ciphertext 1 serves as a Plaintext for Affine Cipher which means the Plaintext to be encrypted using Affine Cipher is the Ciphertext obtained from the encryption using Ceasar cipher.

The first step is to change the plaintext (Ciphertext1) into ASCII code

	X	I	Z	A	K	M	\	I	U	W	T
ASCII	88	73	90	73	75	77	92	73	85	87	84
CX	32	153	50	153	171	189	68	153	5	23	252
Ciphertext2	SP	TM	2	TM	<<	^{1/2}	D	TM	ENQ	ETB	ü

To obtain the values for CX for Affine Cipher we use the mathematical expression;

Where V is the ASCII;

$CX \equiv ((9 * V) + 8) \text{ Modulus } 256, 0 \leq V \leq 255$

$CX \equiv ((9 * 88) + 8) \text{ Modulus } 256 = 32$

$CX \equiv ((9 * 73) + 8) \text{ Modulus } 256 = 153$

$CX \equiv ((9 * 90) + 8) \text{ Modulus } 256 = 50$

$CX \equiv ((9 * 73) + 8) \text{ Modulus } 256 = 153$

$CX \equiv ((9 * 75) + 8) \text{ Modulus } 256 = 171$

$CX \equiv ((9 * 77) + 8) \text{ Modulus } 256 = 189$

$CX \equiv ((9 * 92) + 8) \text{ Modulus } 256 = 68$
 $CX \equiv ((9 * 73) + 8) \text{ Modulus } 256 = 153$
 $CX \equiv ((9 * 85) + 8) \text{ Modulus } 256 = 5$
 $CX \equiv ((9 * 87) + 8) \text{ Modulus } 256 = 23$
 $CX \equiv ((9 * 84) + 8) \text{ Modulus } 256 = 252$

Implementation of the decryption Algorithm (Affine Decryption)

To have the Ciphertext decrypted, we decrypt the ciphertext 2 first by converting the ciphertext 2 into ASCII code, then using the mathematical expression;

$T \equiv (57(CX - 8) \text{ Modulus } 256, 0 \leq CX \leq 255)$

Implementation of the Affine Decryption

Ciphertext2	T _M	Z	I	K	M	\	I	<<	W	T	
ASCII	32	153	50	153	171	189	68	153	05	23	252
T	88	73	90	73	75	77	92	73	171	87	84
Plaintext 1	X	I	Z	I	K	M	\	I	<<	W	T

Decryption using Caesar Cipher

The plaintext Obtained from the decryption process using Affine cipher is seen as a ciphertext and is decrypted using Caesar Cipher.

Firstly, this ciphertext is changed into numbers and then this mathematical expression is applied;

$P \equiv (V - k) \text{ Modulus } 256, 0 \leq C \leq 255$

Where V is the ASCII

And we know k to be 8;

Plaintext1	X	I	Z	I	K	M	\	I	<<	W	T
ASCII	88	73	90	73	75	77	92	73	85	87	84
P	80	65	82	65	67	69	84	65	77	79	76
Original Text	P	A	R	A	C	E	T	A	M	O	L

5 CONCLUSIONS

The combination of Caesar Cipher encryption technique alongside Affine cipher encryption technique used as a cryptographic technique in this study makes it difficult to solve sensitive medical data that are encoded using this two technique. If solving Caesar cipher comes within a short time using any of the bruteforce attacks, combining the caesar cipher encryption technique with Affine cipher makes it more difficult to break and even if there will be any successful attack on this two encryption techniques then the computational time to attack both technique will be higher or greater than the time it will take to attack just one of these technique, and if we have attacks taking longer time then before the success the admin of the system might have been aware that there is any intruder breaking the layers of encryption.

REFERENCES

- Munura Maihankali & Esther Chinwe Eze. Symmetric Cryptography for Confidential Communications: Implemented by Enhancing the Caesar Cipher International Journal of Computing and Engineering . ISSN 2788-6344 (Online) . Vol. 2, Issue No. 1, pp 1- 13, 2021
- Mohit Mittal. Performance Evaluation of Cryptographic Algorithms. International Journal of Computer Applications (0975 – 8887) Volume 41– No.7, March 2012.
- Ganapathy, Sannasi. "A secured storage and privacy preserving model using CRT for providing security on cloud and IoT-based applications." Computer Networks 151 (2019): 181-190.
- Kumar, Deepak. "Hiding Text In Color Image Using YCbCr Color Model: An Image Steganography approach." 2019 International Conference on Issues and Challenges in Intelligent Computing Techniques (ICICT) 1 (2019): 1-5.
- Y. Hu & G. Bai. A Systematic Literature Review of Cloud Computing in E-Health. Health informatics-An international journal (HIJ) Vol 3, No 4. 2019.
- R. L. Bashshur , G. Shannon , E. A. Krupinski, J. Grigsby. Sustaining & realizing the promise of telemedicine. AvailableOnline:http://europepmc.org/abstract/MED/23289907.
- B. Thimma Reddy, K. Bala Chowdappa, & S. Raghunath Reddy. Cloud Security using Blowfish and Key Management Encryption Algorithm. International Journal of Engineering and Applied Sciences. 2015 ISSN: 2394-3661, Volume-2, Issue-6.
- V. Joshua & L. D. Gamm. "Health Information Exchange: Persistent Challenges and New Strategies." Journal of the American Medical Informatics Association 17(3) 2014, 288–94.
- S. Bhawar & K. Joshi. "A Review on Cloud Security Based Encryption and Decryption Techniques. International Journal of Engineering Research and Technology 2021, Volume 10, Issue 02.
- T. Chuang Wang Zhi-xiang Zhu Hybrid Encryption Algorithm Based on Wireless Sensor Networks IEEE International Conference on Mechatronics and Automation (ICMA) 2019 ISBN: 978-1-7281-1699-0 DOI: 10.1109/IEEE Tianjin, China.