ISSN 2320 -2610

Volume 8, No.1, January – February 2019

International Journal of Multidisciplinary in Cryptology and Information Security

Available Online at http://www.warse.org/IJMCIS/static/pdf/file/ijmcis01812019.pdf

https://doi.org/10.30534/ijmcis/2019/01812019

Electoral result transmission model based on RSA and AES algorithm

Dr. Stanley Githinji, PhD

United States International University-Africa, Kenya, stanley.githinji@outlook.com

ABSTRACT

In this paper a new Electoral Result Transmission Model (ERTM) is developed based on Advanced Encryption Standard (AES) and RSA algorithm. The model provide mechanisms for encrypting electoral text results and scanned image files before they are submitted to third party networks.

The model enables returning officers to submit encrypted digital files to IEBC Servers and only authenticated IEBC officials at National Tallying Centre (NTC) will have rights to decrypt and to verify that the results are exactly as sent by authorized returning officers. The model aims at preventing against active and passive attacks on electoral results during transmission process.

.

Key words: Encryption**,** ERTM**,** IEBC, AES, RSA.

1. INTRODUCTION

According to Article 86 of Kenya constitution (2010), the election results should be secure, accurate, verifiable, accountable and transparent [7]. Kenya's IEBC (Independent Electoral and Boundaries Commission) had an ambitious technology plan referred to as Kenya Integrated Electoral Management System (KIEMS) which used in the biometric voter registration, voter identification as well as the transmission of election results from polling stations simultaneously to the Constituency Tallying Centre (CTC) and the National Tallying Centre (NTC).

Presidential petition no one of 2017, the first respondent indicated that Safaricom limited and OT-Morpho employees were involved in hacking and manipulation of August eight presidential results in favor of the third respondent. Based on evidence provided, the ruling was that, IEBC failed in the process of relaying and transmitting results [10].

IEBC had contracted OT-Morpho to develop a result transmission software and to supply required hardware for the systems. The software was used to transmit text results and scanned copy of form 34A and 34 B [8]. The role of Safaricom limited was to provide a dedicated secure tunnel to transmit data from KIEMs kits to the IEBC server. IEBC had granted OT-Morpho and Safaricom limited access To its servers. According to Phil Zimmerman, trust is not transitive and security of transmitted results extended beyond trust domains [11]. The researcher proposed a model that will provide returning officers with capabilities of submitting encrypted results and forms to IEBC Servers and only authenticated IEBC officials at National Tallying Centre (NTC) will able to decrypt and verify that the results are exactly as sent by returning officers.

2. RESEARCH OBJECTIVE

1. To identify security requirements for electoral result transmission system.
2. To develop electoral result transmission model based on RSA and AES cryptosystem

2.1 The Research Process

Research process consists of series of actions that are necessary to effectively carry out research [4]. The research process for this study was done in one phase that aimed at achieving specified research objectives. The research approach be adopted in this study was a Design-Science Research (DSR), which complements the natural science approach [13].

Table 1: Data analysis phases

	Micro Level
Phase	**Phase 1**
Objective	Understand the domain of voting process and possible attacks on data
Purpose	Exploratory
Method	Literature review, Field studies,

3. ERTS MODEL BASED ON AES AND RSA ALGORITHM

The Advanced Encryption Standard is a block cipher with a fixed block length of 128 bits. It supports three different key lengths: 128 bits, 192 bits, and 256 bits [3]. Advanced Encryption Standard (AES) algorithm not only for security but also for great speed. Both hardware and software implementation are faster still [9]. The process of encrypting image with AES algorithm requires conversion of digital image into a binary matrix [14]. Decryption process is the inverse of the encryption process. In the process of the image transmission it will be not susceptible to tampering or eavesdropping [9]. The process of image encryption based on AES is shown in figure 1 below.

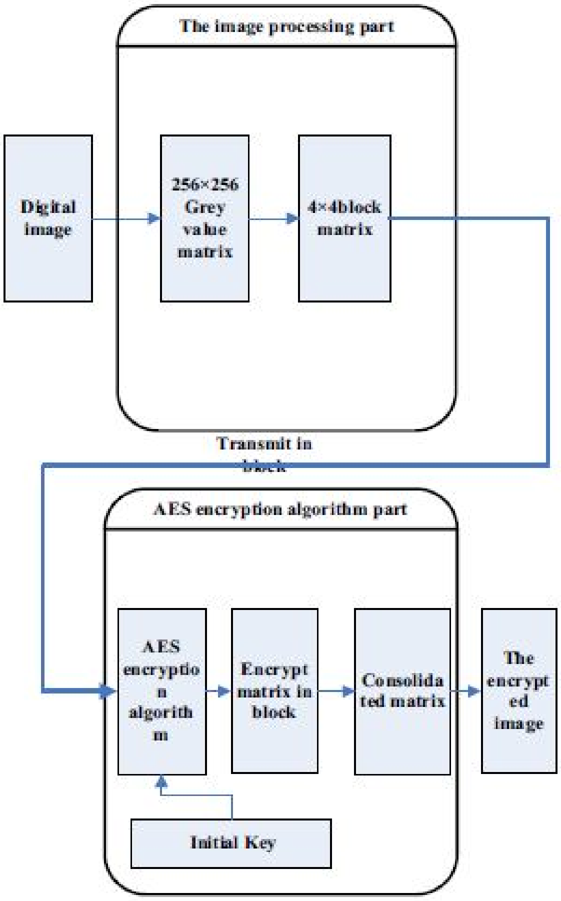

Figure 1: The process of image encryption based on AES

3.1 RSA Algorithm

The RSA algorithm is a public key cryptosystem which involves three steps: key generation, encryption and decryption. Key generation: The steps for implementation of RSA algorithm are given below [6]. Participant in communication randomly and independently choose two large primes p and q number, and multiplies them to produce n=pq. This is the modulus used in the arithmetic calculations of the RSA algorithm. For security purposes, the integer's p and q should be chosen at random, and should be of similar bit-length. Prime integers can be efficiently found using a primarily test [2].

The steps for implementation of RSA algorithm are given below [6].

1. Select p and q (both should be prime numbers)
2. Calculate n=pq
3. Calculate z=(p-1)(q-1)
4. Select integer d which is relatively prime to 2.
Gcd φ(n) d=1(φ9n)=z)
5. Calculate ed-1 mod(φ(n))
6. For Encryption: $C=P^{e}$mod n
7. Where P is Plaintext, C is Cipertext (encryption)
8. For Decryption: $P=C^{d}$mod n

Public key encryption algorithm uses a public key of PU=(e,n) and private key of PR=(d,n).

3.2 ERTS Key Generation

Each polling station will be randomly be assigned two large primes p and q number, to produce n=pq. This will be the modulus used in the arithmetic calculations of the RSA algorithm. For security purposes, the integer's *p* and *q* will be chosen at random, and will be of similar bit-length. The RSA Algorithm will be used to create a private- public key pair. The decryption of data will only be done on the receiver's system using the same program and the private key tied to public key of each polling station.

3.3 Discussions

One major advantage of using ERTM, it will allow options to encrypt results at the polling station before they are transmitted. The decryption module of transmitted results will only be at the National Tallying Center. Returning officers will be required to provide text results and image of form 34A and 34B. The key generation and encryption module will produce a digital envelope that will automatically be forwarded to the IEBC Server through identified ISP receiver. The decryption of data will only be done on the receiver's system using the private key tied to public key of each polling station.

4. CONCLUSION

The electoral result transmission model based on RSA and AES image encryption mechanism will ensure that data received is exactly as sent by an authorized entity and it will provide protection against tampering of results and non-repudiation where by no entity can deny having participated in the transmission of results. Implementing this model requires the IEBC to invest in a Public Key Infrastructure (PKI) for election results to be secure, accurate, verifiable, accountable and transparent.

REFERENCES

1. Devashish, lakshmi & Jaiswal(2016). **Modified key based image encryption using RSA algorithm**. *International Journal of Innovative Research In Technology*,12(2),252-361
2. Deen, El-Sayed, Sameh & Gobran(2014). **Digital Image Encryption Based on RSA Algorithm.** *Journal of Electronics and Communication Engineering* 9(1), *69-73* https://doi.org/10.9790/2834-09146973
3. Gulom Tuychiev (2014). New encryption algorithm based on network RFWKPES8-1usingofthe transformationsof the encryption algorithm AES. International Journal of Multidisciplinary in Cryptology and Information Security 6(3),31-34
4. Kothari, C.R., 2004. ***Research Methodology Methods and Techniques***. 2 edn. New Delhi: New Age International.
5. IEBC.(2018,January 15).**Result Transmission Systems**. Retrieved From https://www.iebc.or.ke/election/technology/?Results_Transmission_And_Presentation_(RTS)
6. Saranya, Vinothini & Vasumathi (2014). **A Study on RSA Algorithm for Cryptography**. *International Journal of Computer Science and Information Technologies*, 5 (4) , 5708-5709
7. **The *Constitution* of *Kenya***. Revised Edition 2010 (current to 2014), published by the National Council for Law Reporting with the Authority of the Attorney General.
8. OT-Morpho(2018, Janaury 9). **Press Release Details on Upcoming Kenyan Presidential-Election Results Transmission-SystemRTS** Retrieved From https://www.morpho.com
9. Prerna Mahajan & Abhishek Sachdeva (2013).**A Study of Encryption Algorithms AES, DES and RSA for Security**. Global Journal of Computer Science and Technology Network, Web & Security,15(13),1-9
10. Presidential Petition. (2018, January 9). **Judgement on Presidential Petition No. 1 of 2017**, Retrieved From Http://Www.Judiciary.Go.Ke/Portal/Blog/Post/Presidential-Petition-1-Of-2017.
11. Philip R. Zimmermann.**The Official PGP User's Guide**.MIT Press, USA, May 1995.
12. Saranya, Vinothini & Vasumathi (2014). **A Study on RSA Algorithm for Cryptography**. *International Journal of Computer Science and Information Technologies*, 5(4) ,5708-5709.
13. Venable, J., 2006. **A framework for design science research activities**. In: m. Khosrow-pour,ed, *Emerging Trends and Challenges in Information Technology Managament.* Idea Group Inc, pp. 184-188.
14. Zhang & Qunding (2015).**Digital Image Encryption Based On Advanced Encryption Standard(AES) Algorithm**. 2015 Fifth