Journal of Theoretical and Applied Information Technology
28th February 2023. Vol.101. No 4

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

A NOVEL CRYPTOSYSTEM OF AN UPGRADED CLASSICAL CIPHER AND RSA ALGORITHM FOR A SECURE AND AN EFFICIENT ELECTRONIC VOTING SYSTEM

SRAVANI JAYANTI[1], K CHITTIBABU[2], PRAGATHI CHAGANTI[3], CHANDRA SEKHAR AKKAPEDDI[*]

[1,2]Research Scholar, Department of Mathematics, GITAM, Visakhapatnam, India
[3]Associate Professor, Department of Mathematics, GITAM, Visakhapatnam, India
[4]Professor, Department of Mathematics, GITAM, Visakhapatnam, India
E-mail: [1]sjayanti@gitam.in , [2]121962101201@gitam.in , [3]pchagant@gitam.edu , [*]cakkaped@gitam.edu

ABSTRACT

Election is a fair decision making process by an authorized group of individuals to elect a person or a party to provide them power to take further decisions for the welfare of the voted people. Traditionally, elections were conducted using Ballot-paper system which is less efficient with a threat of confusion, tampering of votes and more time-consuming. In the digital world, Electronic Voting Systems (EVS) are introduced which are less time-consuming, efficient and prevent tampering of votes. Several research works have invaded different EVS such as Mix-net Based e-voting, Homomorphic e-voting, Blockchain e-voting etc using cryptographic tools. This paper draws attention towards developing an Electronic voting model applying a modified classical cipher and RSA cryptosystem. The developed method is implemented using a C++ program. The performance of the developed E-Voting System is analyzed in terms of the security provided, time and memory requirements.

Keywords: *Cryptology; Electronic Voting; Affine-Hill Cipher; Quadratic residues; RSA*

1. INTRODUCTION

The security of information is the vitality of the present digital world. Several algorithms are invented and implemented to communicate data quickly, safely, and securely. These algorithms are derived from Cryptology which is the study of developing encrypting and decrypting techniques for exchanging information between two parties robustly and securely. It is a combination of cryptography and cryptanalysis.

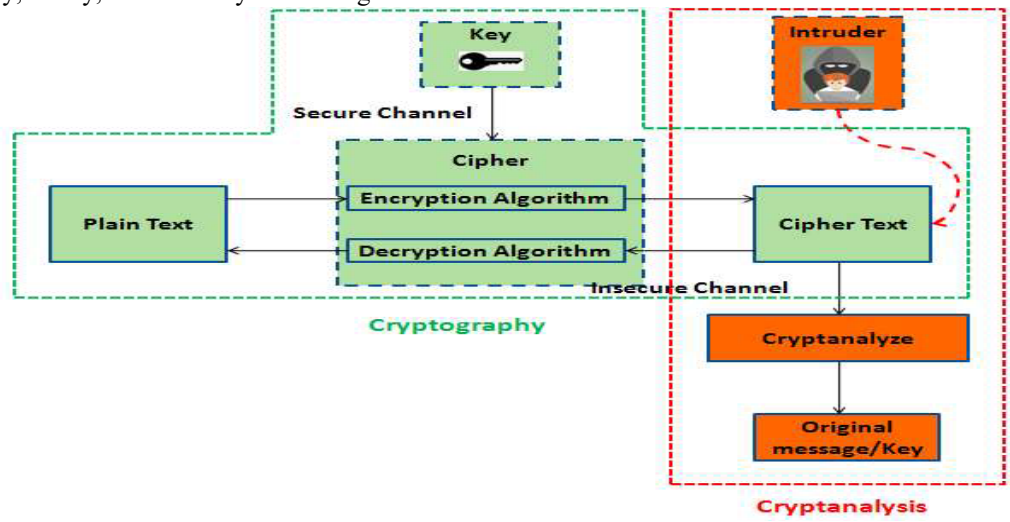

Figure 1: Cryptology

This field uses several concepts from mathematical subjects such as number theory, linear algebra, etc., to develop ciphers that are not vulnerable to attacks. In the ancient period, classical ciphers such as Caesar, Affine, Hill, Playfair etc were developed for carrying out communication. With the rise in technology, modern cryptosystems such as AES and DES were designed to meet the memory and security requirements. Different types of cryptanalytic attacks can be carried out on a developed cryptosystem to trace the information. Designing cryptosystems and dishonest attacks to hack the information go hand in hand. Thus, the development of compatible ciphers is still a welcoming task.

Cryptology experiences a lot of real-time applications. The secure cryptosystems are responsible for the smooth functioning of safe money transfers in the Banking sector, Electronic Voting Machines to conduct fair elections, ATMs to dispense and deposit cash, secret message transfers in Defense and many more. This paper focuses on developing efficient Electronic Voting System applying mathematical and cryptographic tools.

An Electronic Voting System helps to cast and count the votes casted in the favor of a nominee electronically. It ensures that the elections are conducted in a fair manner by allowing only the authorized voters to cast their vote anonymously preserving privacy. The main security aspects taken into consideration for developing a strong Electronic Voting Model are Privacy, Anonymity and Verifiability. Privacy guarantees the secrecy of vote from others. Anonymity assures that secrecy of the voter. Verifiability includes individual, Universal and eligibility. Individual verifiability permits a voter to verify whether his/her vote is considered in the final election results. Universal Verifiability permits the voters or the election organizers to verify whether the final election results correspond to the votes casted. Eligibility Verifiability permits the voters and the election organizers to verify the authenticity and the non-duplication of a vote. Cryptographic algorithms are established to conduct fair elections by retaining the verifiability, privacy and anonymity of the casted votes. Several E-Voting models are proposed balancing the security and efficiency aspects [1][2][3]. In [4], various Electronic Voting models are compared and their analysis is carried out. The requirements for future research direction in developing an E-Voting System is conveyed in [5][4].

Several research works are carried out concerning the advancement and analysis of classical ciphers for applications[6][7]. Affine-Hill Cipher is applied in cryptosystem for securing digital images [8]. Many research works are carried out to upgrade the security of the Classical Ciphers. In [9], a more robust version of Hill Cipher is designed, making use of a combination of keys along with a permutation. In [10], an enhanced Classical cipher is designed resistant to the Known-plaintext attack (KPA), which is time-saving. In [11], a technique based on the said cipher is developed for image encryption using a self-invertible key matrix making the algorithm computationally less complex. In [12], a public key cryptosystem with reduced time and space complexity is developed using the Affine-Hill cipher and Fibonacci matrix.

In [13], a block cipher is developed by altering the classical Hill cipher. The so developed cipher creates confusion making it resistant to KPA and retains Avalanche effect. In [14], a secure variant of the Hill cipher is developed by using Affine-Hill Cipher where the Affine-Hill Cipher does not undergo the conventional computations. This variant is resistant to KPA, Cipher Text Only Attack, Chosen Plaintext Attack and Chosen Cipher text Attack. In [15], an upgraded version of the Affine-Hill Cipher is developed which applies the mathematical concept of Fibonacci matrix and its eigen values ensuring the security of the cipher.

The algorithm applied in designing the E-Voting System in this paper employs an RSA cryptosystem and an upgraded Affine-Hill Cipher using the mathematical concept of Quadratic Residues.

1.1 RSA Cryptosystem

RSA is an asymmetric cryptosystem whose security relies on the Integer Factorization Problem [16][17]. The algorithm to encrypt data using RSA is:

Select two large primes p_1 and p_2.

Calculate $m = p_1 * p_2$.

Select an integer $k_1 \ni 1 < k_1 < m \; and \; \gcd(k_1, \emptyset(m)) = 1$.

Calculate $k_2 \ni k_1 * k_2 \equiv 1(mod \; \emptyset(m))$.

Journal of Theoretical and Applied Information Technology
28th February 2023. Vol.101. No 4

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Public Key: (k_1, m)

Private Key: (k_2, m)

Encryption: For a plain text $P < m$, cipher text $\mathbf{C \equiv P^{k_1} (mod\ m)}$.

Decryption: $P \equiv C^{k_2} (mod\ m)$

1.2 Affine-Hill Cipher

Affine-Hill Cipher is a combination of two classical ciphers Affine and Hill. In an Affine-Hill Cipher, two key matrices are used for encryption [16][17].

The cipher text matrix is obtained as:

$$[C] = [K_1] * [P] + [K_2] (mod\ n) \quad (1)$$

where $[C]_{m\times 1}$ is the cipher text matrix, $[P]_{m\times 1}$ is the plain text matrix, $[K_1]_{m\times 1}$ and $[K_2]_{m\times 1}$ are the key matrices.

The decryption is performed as:

$$[P] = [K_1^{-1}] * ([C] - [K_2])\ mod\ n \quad (2)$$

where $\det(K_1) * [K_1]^{-1} \equiv 1 (mod\ n)$.

1.3 Quadratic Residues

Quadratic residues, a concept in Number Theory is of great use in Cryptography [18][19]. An IBES is developed using Quadratic Residues [20]. Research in Cryptography is also carried out using the Quadratic residuosity problem. One of the major applications of the Quadratic Residuosity Assumptions is the Blum-Blum Shub generator whose basis relies on the concept of Quadratic Residues [21].

For an integer $n > 1$ and $a \in Z_n^*$, a is a Quadratic Residue modulo n if $x^2 \equiv a (mod\ n)$ for some $x \in Z_n$; Otherwise, a is Quadratic non-residue modulo n. The Quadratic Congruence $x^2 \equiv a (mod\ p)$ where $gcd(a, p) = 1$ has a solution if and only if a is a Quadratic Residue modulo p. If one solution is x_0 then the other solution is $(p - x_0)$. For an odd prime p, there are $\left(\frac{p+1}{2}\right)$ quadratic residues (counting zero) and $\left(\frac{p-1}{2}\right)$ quadratic non-residues.

In this paper, we work on Quadratic Residues modulo a prime to develop an upgraded version of the Affine-Hill Cipher that is applied in the E-Voting System to achieve efficiency, privacy, anonymity and universal verifiability.

2. PROPOSED CIPHER

A mathematical model constituting an Affine-Hill Cipher over Quadratic Residues, a pseudo-random stream generator and an RSA cryptosystem is proposed for implementing in an Electronic Voting System. The methodological approach of the proposed model is:

The parameters used in the method:

n = prime

p = *prime such that* $\frac{p+1}{2} > n$

$[P]_{3*1}$ = Plain text Matrix

$[C]_{3*1}$ = Cipher text Matrix

$[K_1]_{3*3}, [K_2]_{3*1}$ = Key Matrices (Private key)

2.1 Key generation

2.1.1 Pseudo-code to generate the Pseudo-Random Key Stream (PRKS):

```
Start
Input s  //Seed Value
Input n
a1[0] = s % n
a1[1] = (s + 1) % n
for i = 3 to 11
Start
a1[i] = (a1[i − 1]^a1[i−2] + i) % n
End
for i = 1 to 11  //Output the PRKS
Start
Output a1[i]
End
End
```

2.1.2 Pseudo-code to generate the key matrices:

The key stream is arranged in the form of a square matrix of order 3×3. The matrix so obtained is $[K_1]_{3\times 3}$.

```
while(det(K1) mod n == 0)
{
    [K1]3*3 = [K1]3*3 + [I]3*3
}
```

$[K_2]_{3*1}$ is derived from $[K_1]_{3*3}$ as: $k_{2_{i1}} = (k_{1_{i1}} + k_{1_{i2}} + k_{1_{i3}}) \bmod n$

2.2 Encryption and Decryption process

Step 1: Select a prime number p such that the total number of quadratic residues modulo p is greater than n i.e. $\frac{p+1}{2} > n$.

Step 2: Establish a one-one correspondence: $1,2,\ldots,n \leftrightarrow$ *Quadratic residues mod p*.

Step 3: Select s to generate the key matrices $[K_1]$ and $[K_2]$ by using the key generation algorithm.

Step 4:
Encryption:
For the plain text $[P]$,
$[C] = [K_1] * [P] + [K_2](mod\ n)$.

Map the obtained values in $[C_1]$ to the corresponding quadratic residues to obtain $[C_2]$.

The values in the final cipher text matrix $[C]$ are the solutions to the quadratic congruence $x^2 \equiv c_{2_{ij}}(mod\ p)$. Since there are two solutions to the Quadratic congruence therefore the character at even position is mapped to the solution x_0 and the one at the odd position is mapped to $(p - x_0)$.

Step 5:
Decryption:
From the cipher text $[C]$, the values in $[C_2]$ are retrieved from $[C]$ by computing: $c_{1_{ij}} \equiv c_{ij}\ (mod\ p)$.
From $[C_2]$ and the one-one correspondence, $[C_1]$ is obtained.
The original plain text is obtained as:

$$[P] = [K_1^{-1}] * ([C_1] - [K_2])\ (mod\ n)$$

2.3 Example

The proposed cipher is illustrated through an example for n = 29 and p = 71. The numbers from 1 to 29 and the quadratic residues modulo 71 are mapped as:

Table 1: One-One correspondence between numbers and the quadratic residues

Numerical equivalent (modulo 29)	Quadratic residues modulo 71
1	0
2	1
3	2
4	3
5	4
6	5
7	6
8	9
9	10
10	12
11	15
12	16
13	18
14	19
15	20
16	24
17	25
18	27
19	29
20	30
21	32
22	36
23	37
24	38
25	40
26	43
27	45
28	48
29	49

For s = 5 and the plain text matrix $\begin{bmatrix}1\\1\\1\end{bmatrix}$, the key matrices and the corresponding cipher text are $\begin{bmatrix}7 & 0 & 5\\7 & 23 & 9\\15 & 7 & 18\end{bmatrix}$, $\begin{bmatrix}12\\10\\11\end{bmatrix}$ and $\begin{bmatrix}31\\39\\6\end{bmatrix}$ respectively.

2.4 Security Analysis of the proposed Cipher

The proposed cipher is resistant to the following attacks:

2.4.1 Brute-force Attack

The attack carried out to hack the original plaintext by trying all the possible keys is Brute-force attack. In the proposed cipher, the number of possible key matrices is dependent upon the seed value s which is dependent on n. The total number of possible key matrices is n^9. Thus by selecting large primes n and p, the cipher's resistance against Brute-force attack can be increased.

2.4.2 Known-Plain text attack

In KPA, a part of the plain text and its corresponding cipher text is known to the intruder which is used to reveal the key used for encrypting the data.
In the proposed model, suppose that the intruder has the following data: $n = 29$, plain text: $\begin{bmatrix}19\\5\\1\end{bmatrix}$ and its corresponding cipher text: $\begin{bmatrix}10\\49\\28\end{bmatrix}$. Then the matrix representation of the data is:

$$\begin{bmatrix} a_1 & a_2 & a_3 \\ b_1 & b_2 & b_3 \\ c_1 & c_2 & c_3 \end{bmatrix} * \begin{bmatrix} 19 \\ 5 \\ 1 \end{bmatrix} + \begin{bmatrix} (a_1+a_2+a_3) mod\ n \\ (b_1+b_2+b_3) mod\ n \\ (c_1+c_2+c_3) mod\ n \end{bmatrix} = \begin{bmatrix} 10 \\ 49 \\ 28 \end{bmatrix}$$

From the above matrix representation, 3 equations in 3 variables are obtained which cannot be solved to obtain the key values because the cipher text values are mapped to quadratic residues modulo p where the value of p is unknown. Also, both the solutions of a Quadratic congruence lead to the mapped Quadratic residue thus creating confusion. Hence, the proposed model is resistant to the Known Plain text attack.

Also, the proposed method is resistant to the Zero Plaintext attack (ZPA) because the zero plaintext is mapped to the quadratic residues modulo p which provide no clue to trace the key matrices.

2.4.3 Frequency Analysis

Frequency analysis is a study of number of times a character has occurred in a cipher text. This analysis helps to guess the corresponding plain text depending upon the most occurring and rare occurring characters in a character set. But this attack is possible only when same plain text characters are mapped to the same cipher text characters post encryption. In the proposed cipher, the encrypted values of the same plain text digits differ making the cipher resistant to attack by means of frequency analysis.

For example: For $n = 29, p = 59$, plain text $= \begin{bmatrix} 19 \\ 5 \\ 5 \end{bmatrix}, K_1 = \begin{bmatrix} 17 & 1 & 26 \\ 23 & 19 & 24 \\ 5 & 4 & 3 \end{bmatrix}$ $and\ K_2 = \begin{bmatrix} 15 \\ 8 \\ 12 \end{bmatrix}$, the obtained cipher text is $\begin{bmatrix} 9 \\ 65 \\ 16 \end{bmatrix}$.

2.4.4 Avalanche effect

Avalanche effect is an important property of a cryptographic algorithm which states that significant change is reflected in the cipher text whenever the plain text undergoes a minute change. In the proposed method, change in a single character of the plain text results in the change of more than one character in the cipher text.

For $n = 29, p = 71$, plain text: $\begin{bmatrix} 19 \\ 5 \\ 1 \end{bmatrix}$ and key matrices, $K_1 = \begin{bmatrix} 17 & 1 & 26 \\ 23 & 19 & 24 \\ 5 & 4 & 3 \end{bmatrix}$ $and\ K_2 = \begin{bmatrix} 15 \\ 8 \\ 12 \end{bmatrix}$, the obtained cipher text is $\begin{bmatrix} 23 \\ 36 \\ 27 \end{bmatrix}$. On replacing the 3rd character 'A' of the plain text by 'E', the obtained cipher text is $\begin{bmatrix} 9 \\ 65 \\ 16 \end{bmatrix}$ which differs from the previous cipher text in all the three bits. Hence, the developed method retains Avalanche effect.

3. PROPOSED ELECTRONIC VOTING SYSTEM

An Electronic Voting System is a development made in the field of science to conduct fair elections in an organization or a nation from any location over Internet. It must be efficient enough to preserve privacy to vote, anonymity of the voter and security of the system. The proposed architecture for E-Voting includes three major steps−Registration, Voting, Results.

3.1 Registration

The initial step in the process of conducting elections is to register the candidates to provide them the authorization to vote. This step sets a unique identification to every voter which ensures the authorization of the voter and the authenticity of the vote casted. Depending upon the total number of registrations, different booths are organized.

3.2 Voting

In this step, each authorized voter is allowed to cast their vote against their respective nominee. The encrypted version of the casted vote is collected for counting the votes.

3.3 Results

The declaration of results include the display of total number of registered voters, total number of voters who voted and the individual votes obtained by each nominee.

Journal of Theoretical and Applied Information Technology
28th February 2023. Vol.101. No 4

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

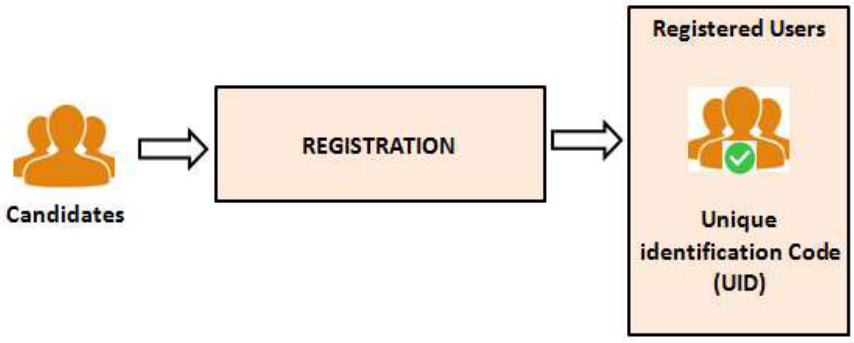

Figure 2: Registration

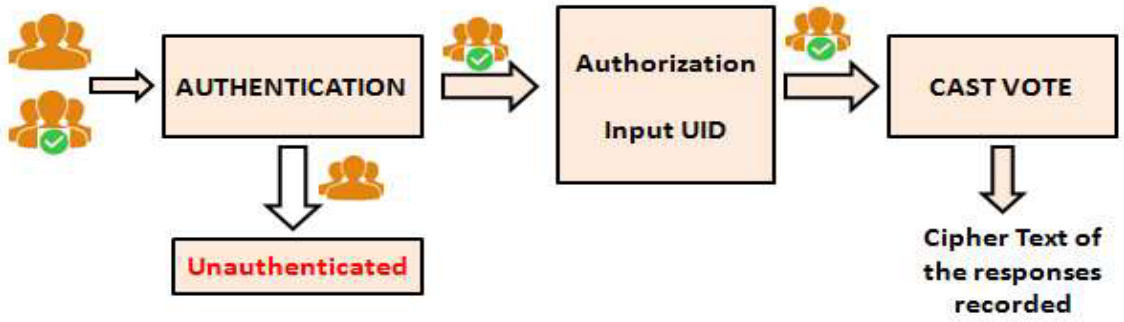

Figure 3: Voting

Figure 4: Results

An eminent E-Voting Model is proposed to meet the following security goals:

- Authenticated and Authorized Voting: Only the registered candidates are allowed to vote provided their identity is verified.
- Double-Voting Prevention: Single Voter can cast only a single vote.
- No Votes replaced: Alteration of a casted vote by a voter is not possible.
- Privacy to Vote: The vote casted remains private to the voter.
- Anonymous Voting: The identity of the voter is not disclosed.
- Immune to Modification: The votes casted cannot be altered in favor of a single party.
- Unlinkability: Post-Voting the voters and their votes cannot be linked.

The cipher developed in the section 2 is applied in the Voting and Result steps of the proposed model. The implementation of the cipher in the EVS is discussed in section 4.

4. IMPLEMENTATION

The developed cipher is incorporated in the stages 2 and 3 of the proposed E-Voting Model along with the RSA cryptosystem to meet the security aspects. The model is implemented for an election where a maximum of 2^3 nominations can compete against each other. The nominations are mapped to the following matrices $\begin{bmatrix}0\\0\\0\end{bmatrix}, \begin{bmatrix}0\\0\\1\end{bmatrix}, \begin{bmatrix}0\\1\\0\end{bmatrix}, \begin{bmatrix}0\\1\\1\end{bmatrix}, \begin{bmatrix}1\\0\\0\end{bmatrix}, \begin{bmatrix}1\\0\\1\end{bmatrix}, \begin{bmatrix}1\\1\\0\end{bmatrix}$ and $\begin{bmatrix}1\\1\\1\end{bmatrix}$.

Journal of Theoretical and Applied Information Technology
28th February 2023. Vol.101. No 4

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

The example discussed below considers three nominations $A \leftrightarrow \begin{bmatrix}1\\0\\0\end{bmatrix}, B \leftrightarrow \begin{bmatrix}0\\1\\0\end{bmatrix}, C \leftrightarrow \begin{bmatrix}0\\0\\1\end{bmatrix}$ and the chosen values of $n = 29$ and $p = 71$.

4.1 Pseudo-code to cast Vote

Start
Initialize $n = 29, p = 71$ // Values private to the EC
Generate B_i1, B_i2 // Booth i'sHead generates the keys to encrypt the seed value s
Input s, V //Input by the Voter
$S = enc_{B_i1}(s)$
$K = Gen\,(s)$ // $Gen\,(s)$ is a function to generate key matrices as in ()
$CT = Enc(V, K, n, p)$ // Encrypted Vote
End

4.2 Pseudo-code to count the votes and declare results

Start
Initialize B_i2, K, n, p, CT
$s = dec_{B_i2}(S)$
$K = Gen\,(s)$
$V = Dec\,(CT, K, n, p)$
$Count\,(V)$ // $Count\,(V)$ is a function to count the number of votes casted in the favor of a nominee
Display Results
End

The security of the proposed architecture is concerned in three major hands−Official Authority, Booth Heads and Counting Officer. The exchange of keys among them occurs over a secure channel. The Distribution of keys for conducting a fair Electronic Voting is depicted through the Figure 5.

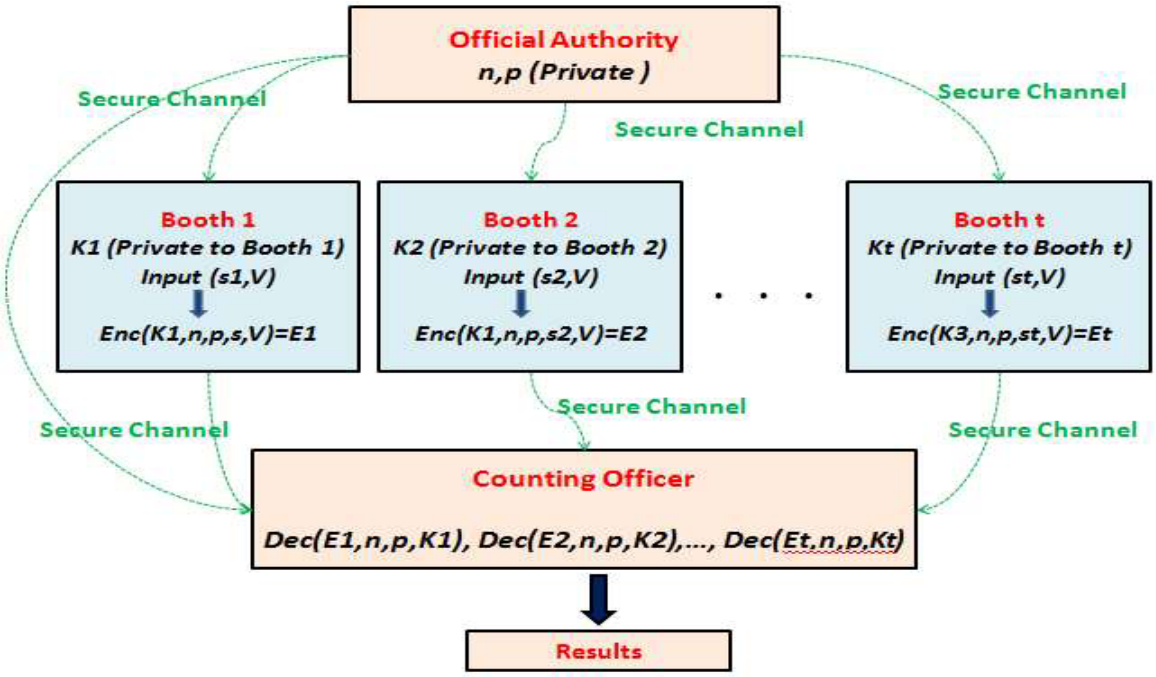

Figure 5: Keys Distribution in the proposed E-Voting model

4.3 Example

The illustrated example is discussed below for 3 nominations A, B and C. These nominations are assigned a unique matrix. Depending upon the number of registered candidates, different booths are organized which have their own private keys to conduct voting. The Official authority sets the values of n, p and shares them with the Booth heads and the Counting officer over a secure channel. The votes are casted by the voters which are encrypted using the private keys of the individual booths. The

encrypted votes and the Decryption key are communicated to the counting officer over a secure channel. The counting officer calculates the final result of the election by decrypting the casted votes with the help of the keys.

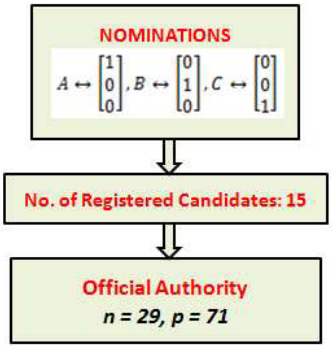

Figure 6: Initiation of Elections by the official Authority

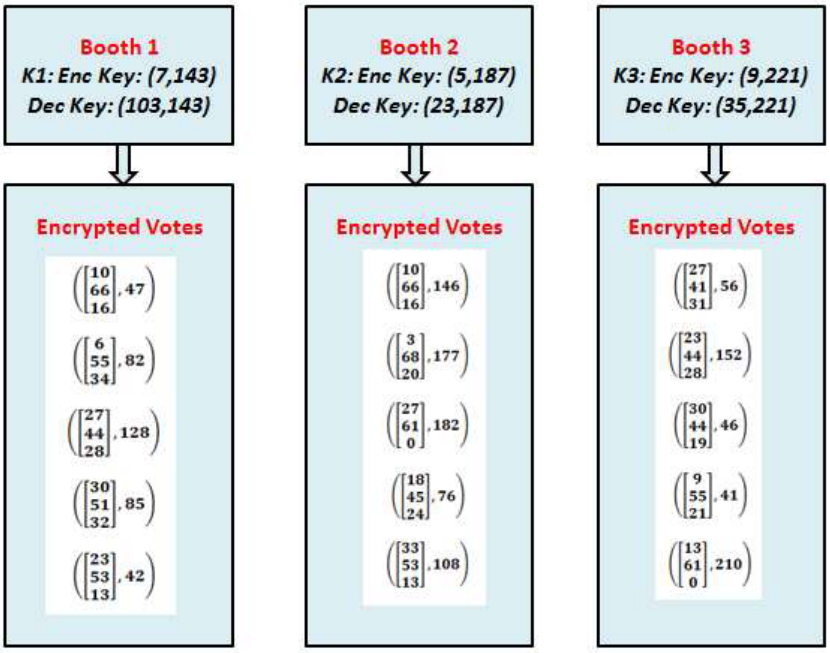

Figure 7: Voting Process at different Booths

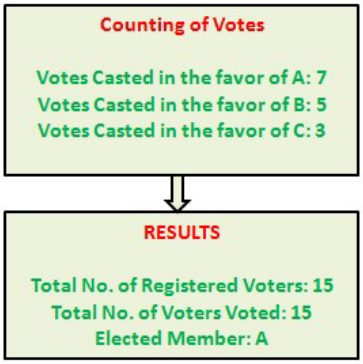

Figure 8: Declaration of Results by the Counting Officer

In the implemented model, the different inputs by the voters and the organizing committee are:
Input by Official authority: n, p
Input by Booth Head: p_1, p_2, e
Input by the voters: $Vote, s$
The input by the official authority is responsible for the establishment of the one-one correspondence between the numbers from 0 to n and the quadratic residues modulo p. The input by the booth heads is used to generate an encryption and decryption key for vote casting. The encryption key encrypts the seed value s input by the user. The seed value generates the key matrices for encrypting the votes casted by the voters. The encryption and decryption key is generated by the Booth heads using RSA algorithm while the votes are encrypted applying the developed cipher in section 2.

4.4 Time and Memory Analysis

The proposed mathematical model is implemented using a DEV C++ compiler on an Intel CORE i3 processor with a speed of 1.70 GHz and 4.00 GB RAM using Windows 8.1 64-bit Operating System. The performance of the developed cryptosystem is measured in terms of its time and memory requirements. The time and memory requirements are tabulated considering a maximum of $2^l, l > 1$ nominations participating in an election for the values of $n = 29$ and the p value is chosen between 59 and 100. The general relation stating the time and memory requirements for the proposed cipher is tabulated in the table where $T_{Enc}, T_{Dec}, M_{Enc}$ and M_{Dec} denote the Encryption time, Decryption time, Memory requirements while Encryption and Decryption respectively.

Table 2: Relation determining the time and memory requirements of the algorithm

	Encryption	Decryption
Time(in milliseconds)	$T_{Enc}^2 \propto lp$	$T_{Dec}^2 \propto lp$
Memory(in Bytes)	$M_{Enc} = 8l^2 + 12l + 3p + 71$	$M_{Dec} = 10l^2 + 12l + 3p + 59$

4.5 Comparative Analysis

The proposed Electronic Voting Model applies the upgraded Classical Cipher and RSA algorithm for encrypting votes. The comparative analysis of the developed model against the existing models [22], [23], [24] and [25] is tabulated in Table 3.

Table 3: Comparative Analysis of the developed model

E-voting Scheme	Cryptosystem	Distinctive Features	Security properties	Weakness
Liao [22]	Elliptic Curve Digital Signature, Identity Based Fully Homomorphic Encryption	Multi-candidate e-voting	Anonymity, Unicity, Completeness, Universal Verifiability	High time complexity of asymmetric encryption
Cohen and Fischer [23]	Public Key Encryption	Hide the actual votes value instead of hiding the voters	Privacy, Correctness	Do not satisfy vote secrecy
Furukawa et al. [24]	ElGamal Encryption, Elliptic Curve	Suitable to be used in a private organisation with over 20,000 voters	Universal Verifiability	Do not achieve receipt-freeness and do not guarantee the privacy of abstaining voters
Chaum[25]	RSA-based Public Key Encryption	Universally trusted authority not required	Anonymity, Privacy	Efficiency relies on the length of the cipher text
Proposed Model	Upgraded Affine-Hill Cipher over Quadratic Residues and RSA Cryptosystem	Less Complex and applies upgraded classical ciphers	Supports Anonymous Voting, Immune to Modification, Preserves Privacy to Vote, Universal verifiability	The security is guaranteed if the official authority, Booth Heads and the Counting officer are honest.

5. CONCLUSIONS

The cryptographic tool applied for vote casting in the E-Voting model proposed is an Upgraded Afiine-Hill Cipher over Quadratic Residues resistant to the cryptanalytic attacks. The proposed E-Voting System retains authenticity and authorization by providing unique identification code to the registered candidates. The security of the proposed E-Voting system relies on the three major official authorities who exchange the keys used to encrypt votes. The model is implemented using a C++ program whose time and memory requirements and the security aspects are analyzed. The developed model is compared with few of the existing Electronic Voting Models. The developed model is efficient and is independent of the length of the cipher text which achieves privacy, anonymity and universal verifiability.

FUTURE SCOPE

For the proposed E-Voting System, an efficient and secure key generation and Unique identification code generation schemes along with a secure key transfer protocol are required which would build an E-Voting system practically implementable.

ACKNOWLEDGEMENTS

We extend our sincere gratitude to GITAM for supporting our work by providing Dr. M.V.V.S. Murthi Research fellowship.

REFERENCES:

[1] Suwarjono Suwarjono, Lilik Sumaryanti, Lusia Lamalewa, "Cryptography Implementation for electronic voting security", *E3S Web of Conferences 328, ICST 2021*, 2021. https://doi.org/10.1051/e3sconf/202132803005

[2] Pavel Tarasov, Hitesh Tewari, "The future of E-Voting", *IADIS International Journal on Computer Science and Information Systems*, 2017, Vol. **12**, No. 2, pp. 148-165.

[3] Aakash, Aashish, Akshit, Sarthak , "Online Voting system", *Students of Dept. of Computer Science, Inderprastha Engineering College, Dr. A.P.J. Abdul Kalam Technical University*, 2020. https://dx.doi.org/10.2139/ssrn.3589075

[4] Yun-Xing Kho, Swee-Huay Heng, Ji-Jian Chin, "A Review of Cryptographic Electronic Voting, Symmetry", 2022, Vol. 14, No. 5: 858. https://doi.org/10.3390/sym14050858

[5] https://crypto.stanford.edu/pbc/notes/crypto/voting.html

[6] N.Vijayaraghavan, S.Narasimhan, M.Baskar, "A Study on the Analysis of Hill's Cipher in Cryptography", *International Journal of Mathematics Trends and Technology (IJMTT)*, 2018, Vol. **54, No.** 7, pp. 519-522.

[7] Qazi F, Khan F. H, Agha D, Ali Khan, S y ur Rehman S, "Modification in Hill Cipher for Cryptographic Application", 3C Tecnología. Glosas de innovación aplicadas a la pyme, 2019, Special Issue. pp. 240–257. Doi:http://dx.doi.org/10.17993/3ctecno.2019

[8] Sazaki Y, Putra R.S, " Implementation of Affine Transform Method and Advanced Hill Cipher for securing digital images", *10th International Conference on Telecommunication Systems Services and Applications (TSSA)*, 2016, pp. 1-5.

[9] V.U.K.Sastry, Aruna Varanasi, S.Udaya Kumar, "A Modified Hill Cipher Involving a Pair of Keys and a Permutation", *International Journal of Computer and Network Security*, 2010, Vol. 2, No. 9.

[10] M. Nordin A. Rahman, A. F. A. Abidin, MohdKamir Yusof, N. S. M. Usop, " Cryptography: A New Approach of Classical Hill Cipher", *International Journal of Security and Its Applications*, 2013, Vol. 7, No. 2.

[11] Saroj Kumar Panigrahy, Bibhudendra Acharya, Debasish Jena, "Image encryption using self-invertible key matrix of hill cipher algorithm", *1st International Conference on Advances in Computing*, Chikhli, India, 21-22 February, 2008.

[12] P. Sundarayya, G. Vara Prasad, "A public key cryptosystem using Affine Hill Cipher under modulation of prime number", *Journal of Information and Optimization Sciences*, 2019, Vol. **40**, No. 4, pp. 919-930. DOI: 10.1080/02522667.2018.1470751

[13] V.U.K. Sastry, N. Ravi Shankar, "Modified Hill Cipher for a Large Block of Plaintext with Interlacing and Iteration" *Journal of Computer Science*, 2008, Vol. **4**, No. 1, pp. 15-20.

[14] Toorani M, Falahati A., "A secure vaiant of the hill cipher", *Proceedings of the 14th IEEE Symposium on Computers and Communications Sousse*, 2009, pp. 313-316.

[15] Kalika Prasad, Hrishikesh Mahato, " Cryptography using generalized Fibonacci

Matrices with Affine-Hill Cipher", 2020. Available online: arXiv:2003.11936v1 [cs.CR] 25 Mar 2020

[16] B. A. Forouzan, Debdeep Mukhopadhyay. *Cryptography and Network security*, Third Edition, McGraw Hill Education.

[17] D.R. Stinson, M.B. Paterson, *Cryptography: Theory and Practice*, Fourth edition, CRC Press Taylor & Francis Group.

[18] Tom M. Apostol. *Introduction to Analytic Number Theory*, Springer Publications.

[19] Anca-Maria Nica, "Quadratic Residues and Applications in Cryptography", *Alexandru Ioan Cuza University of Iasi, Romania, Department of Computer Science,* 2020.

[20] Cocks C, "An Identity Based Encryption Scheme Based on Quadratic Residues", *B. Honary (Ed.): Cryptography and Coding, LNCS 2260*, 2001, pp. 360-363, Springer, https://doi.org/10.1007/3-540-45325-3_32

[21] Ferucio Laurentiu Tiplea, Dan Timotin, "A Brief Introduction to Quadratic Residuosity Based Cryptography", *Rev. Roumaine Math. Pures Appli*, 2021, Vol. **66**, No. (3-4), pp. 793-811.

[22] Liao, G. "Multi-Candidate Electronic Voting Scheme Based on Fully Homomorphic Encryption", *J. Phys. Conf. Ser.* 2020, 1678, 012064.

[23] Cohen, J.D, Fischer, M.J, "A Robust and Verifiable Cryptographically Secure Election Scheme", *26th Annual Symposium on Foundations of Computer Science, SFCS '85, Washington, DC, USA, 21–23 October 1985*; pp. 372–382.

[24] Furukawa, J, Mori, K., Sako, K, "An Implementation of a Mix-Net Based Network Voting Scheme and Its Use in A Private Organization. In Towards Trustworthy Elections: New Directions in Electronic Voting", *Lecture Notes in Computer Science; Chaum, D., Jakobsson, M., Rivest, R.L., Ryan, P.Y.A., Benaloh, J., Kutylowski, M., Adida, B., Eds.; Springer: Berlin/Heidelberg,* Germany, 2010, Vol. 6000, pp. 141–154.

[25] Chaum, D.L, "Untraceable Electronic Mail, Return Addresses, And Digital Pseudonyms", *Commun. ACM*, 1981, Vol. 24, pp. 84–90.