International Journal of Applied Engineering Research ISSN 0973-4562 Volume 13, Number 11 (2018) pp. 9468-9473
© Research India Publications. http://www.ripublication.com

A Secure E-Voting System Using RSA and Md5 Algorithms Using Random Number Generators

N.Aditya Sundar[1], M.V.Kishore[2], Prof . Ch.Suresh[3]

[1,2] Assistant Professor, [3] Professor,
Department of Information Technology,
[1, 2, 3] Anil Neerukonda Institute of Technology & Sciences – (ANITS)
Sangivalasa – 531162, Bheemunipatnam (Mandal), Vishakapatnam (District)
Andhra Pradesh, India

Abstract

Secure Voting System is a very secure, efficient and easy to casting of vote. In this paper we will use RSA[1,2] and MD5[1,2] algorithms for security purposes. Our proposed system provides a new e-voting system which fulfills the security requirements of e-voting process. In our project we have total three steps are required e-registration of voter, vote uploading and result display. Proposed system provides secure and efficient e-vote uploading and also paper ballot system if e-voting fail.

Keywords: RSA, MD5, Encryption, Decryption, Voting, Private Key and Public Key.

INTRODUCTION

The wide area of democratic concepts in countries especially in this time lead to implement new algorithms in management the voting which is the great tool in democracy systems that ensure to each eligible voter to be responsible.

The ancient voting system is depending on basic concepts which are ballot paper, poll booths, admin's and others. These terms have some disadvantage such as the cost of establishment the sites of voting and restrict the votes such the users whose are far from their voting polls to be near of their polls in voting time. The e-voting system is a practicable the advantages from cryptographic algorithms. Everyone can add in the election over the globally, and thus increasing the rate of e-voting. The main goal of a secure e-voting system is to ensure the secrecy of the candidates and the accuracy of votes.

E-voting can be arranged into two categories:

(a) Remote internet voting,

(b) Poll-booth e-voting.

Category solved the distance problem generates for people whose are far from their voter but the cost of establishing poll-booths is unsolved. Our E-voting system focus on the category which is solved the money and distance issues. In our system we depend on that must be source of any E-voting system proposed, these criteria are:

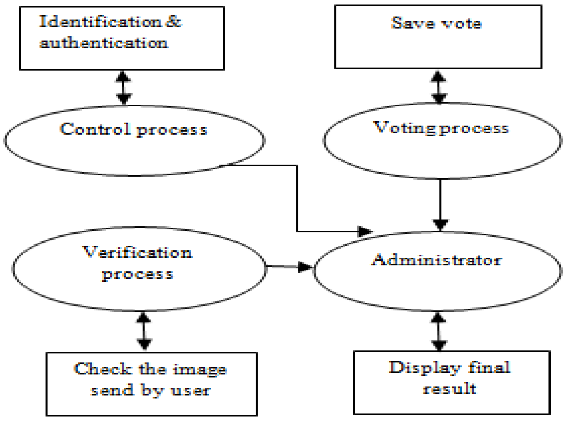
1. Eligibility: Only eligible user can vote in voting and every user having criteria can cast only one vote.
2. Uniqueness: Voter should not be able to vote more than once.
3. Accuracy: Voting systems should not be uploaded the votes incorrectly.
4. Integrity: Votes should not be able to be modified without effects.
5. Verify: Voter should able print their finger prints in certain place.
6. Audit-ability: There should not be unreliable and non-demonstrably authentic election records.
7. Reliability: Systems should work correctly, even in the face of numerous failures.
8. High secure: Everyone should able to vote their own vote without others.
9. Non-forcibility: Voters should not be able to prove how they voted.
10. Flexibleness: Equipment should not allow for a unique of ballot question formats.

LITERATURE STUDY

Voting through the internet is the updated and advanced area of research in the process of voting in this modern world.

1. Proposes e-voting system develops and digital signature system. System uses high confidentiality of voter, secrecy of paper machine, voter secrecy and no computation cost and communication overhead.
2. Propose based E-voting system is used to login without registering for voting in pre-condition and going to polling booths. System prevents repetition voting but it has big disadvantage to security, proposes system does not used any algorithm.
3. Proposed e-voting system based on public key encryption algorithm RSA[1]. Proposed system contains three parts: login, voting and election

administrator server for display. First part holds for the voter's registration with high confidentiality and verification. Voting part done by ciphering voter data using implementing RSA algorithm and last part is the election administrator server displays result of election using decryption RSA private key for sending encrypted data from server. System has disadvantages like there is no any e-registration and more expensive cost and communication overhead due to RSA algorithm.



A simple block diagram of E-Voting system.

PROPOSED WORK

In this paper we proposed that E-Voting system, for the registration phase we will use the RSA algorithm which encrypts and decrypts the data as follows:

In the registration phase the user request pair keys by send hash of his identity with the random key generator to include in his certification in order to prevent covering the voter's proof in next phases. The voter can obtain only one pair private key because the voter have one identity and password.

The voter is able to create the token by the help of server, only during the interactivity with the admin, in the login phase. The authority helps the eligible user to takes the token only once, so the voter could not obtain duplicate token. The authority has no idea how the votes appends. Likely, the validity of the token is verifiable to everyone. This is realized via digital signatures. In the voting phase, the user sends a ballot containing the valid token and his valuable vote to the authority. The authority will accept the ballot with valid token or with the token that not used. This ensures that only eligible users can vote, and that they cannot vote twice because the voters cannot obtain more than one token. Also no one can find any more about how the candidate voted except the verifying in the center but without know the voter's identity proof. The only condition is that it should be tough or impossible to extract the voter's identity from the given token from the server and that each voter have different token for their own.

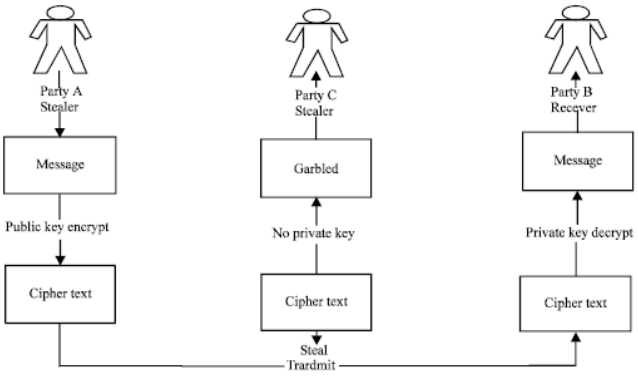


Figure 1. RSA implementation with Private Key

Step 1. Here if the original length is greater than 2^{64} then only low priority 64 bits of the length are used.

SECTIONS

RSA key implementation:[1]

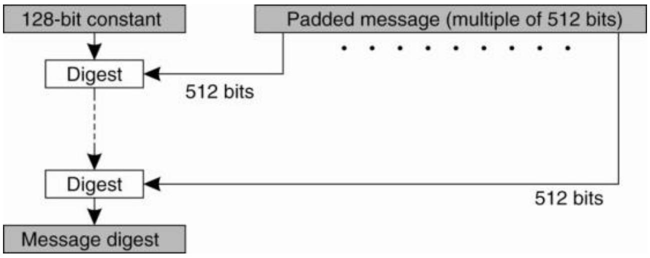
Step 1. Let c_k, c_{k-1}...c1c0 be the binary representation of c

Step 2. Set the variable E to 1.

Step 3. Repeat steps 3a and 3b for i = k, k − 1... 0:

MD5 implementation:[2]

All the attacker needs with a 128-byte block of data, aligned on a 64-byte boundary of this algorithm.



The MD5 algorithm implements as follows:

Step 1: affix padding bits which message is padded so that its length in bits congruent to 448 modulo 512.

Step 2: include length having 64 bit of length is attached to result of Step 1. Here if the original length is greater than 2^{64} then only low priority 64 bits of the length are used.

Step 3: Activation of Message Digest (MD)[2] Buffer which is adding to hold intermediate final result of hash function which consists 4 32-bit registers (A1, A2, A3, and A4). Which are hexadecimal values.

For Example:

A1=10325476

A2=98BADCFE

A3=EFCDAB89

A4=67452301

These results are stored in as low order little-byte format as 32-bit format. The activated values are stored as follows:

Word A1: 67 45 23 01

Word A2: EF CD AB 89

Word A3: 98 BA DC FE

Word A4: 10 32 54 76

Step 4: Procedure message in 16-word bit blocks is the main process in the algorithm having four rounds.

Step 5: Result will be after all K 16-word blocks have been operated then the result from the K^{th} stage is the 128-bit MD.

The behavior of MD5 as follows:

KV=I

KV_{p+1}=SUM_{32}(KVp,R1{Bp,Rh{Bp,Rg{Bp,Rf{Bp,KVp}}}})

MD=KV_1

Where

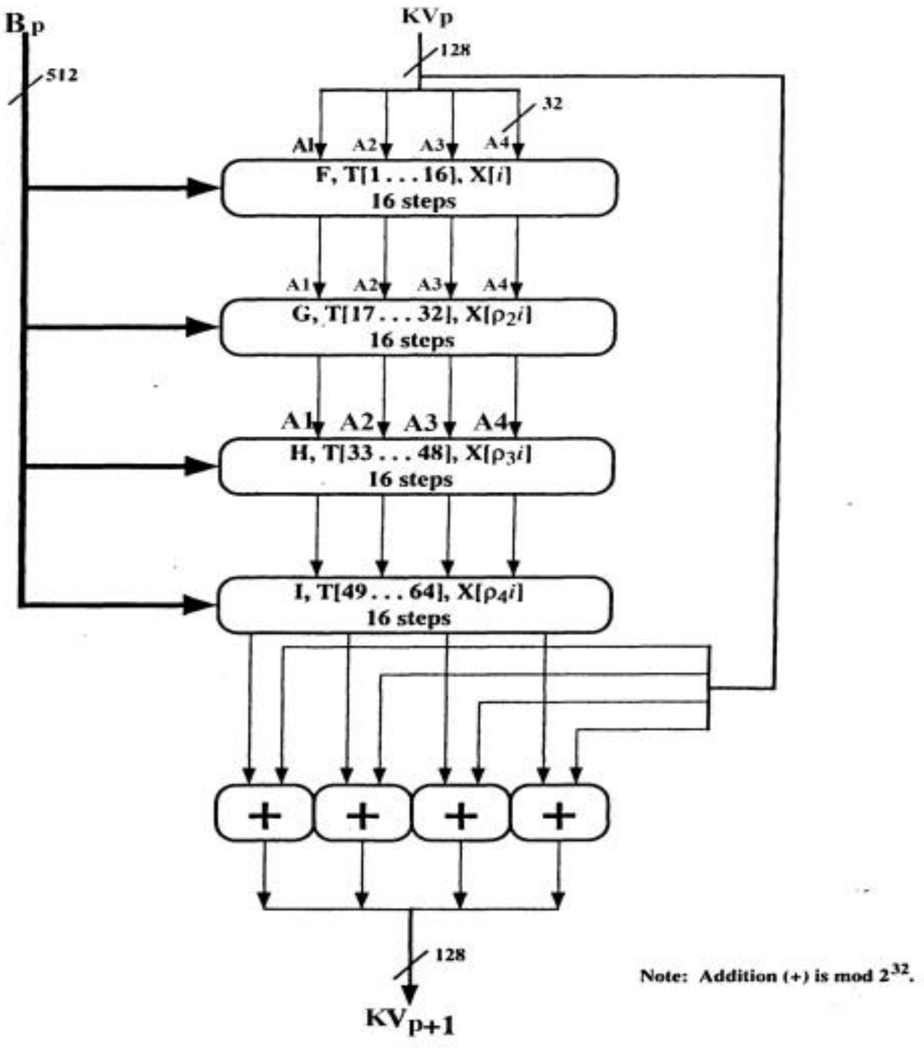
I=Initial value of the A1A2A3A4 buffer, defined in step 3.

Bp= The pth 16-word block of the message.

K= The no.of blocks in the message.

KVp=Chaining variable processed with pth block of message.

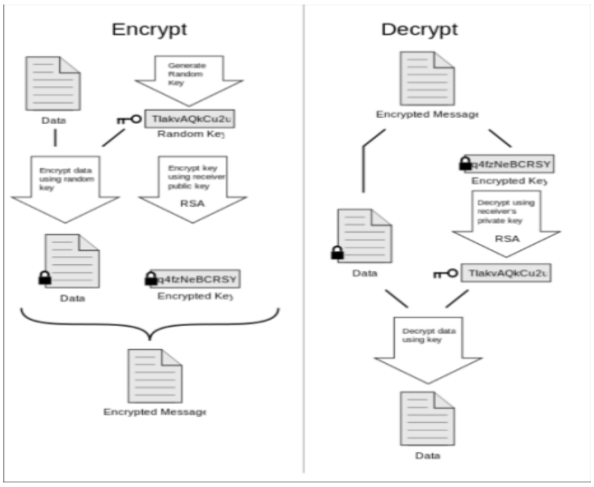
Fx=Round function.



Note: Addition (+) is mod 2^{32}.

Figure. MD5 algorithm

IMPLEMENTATION



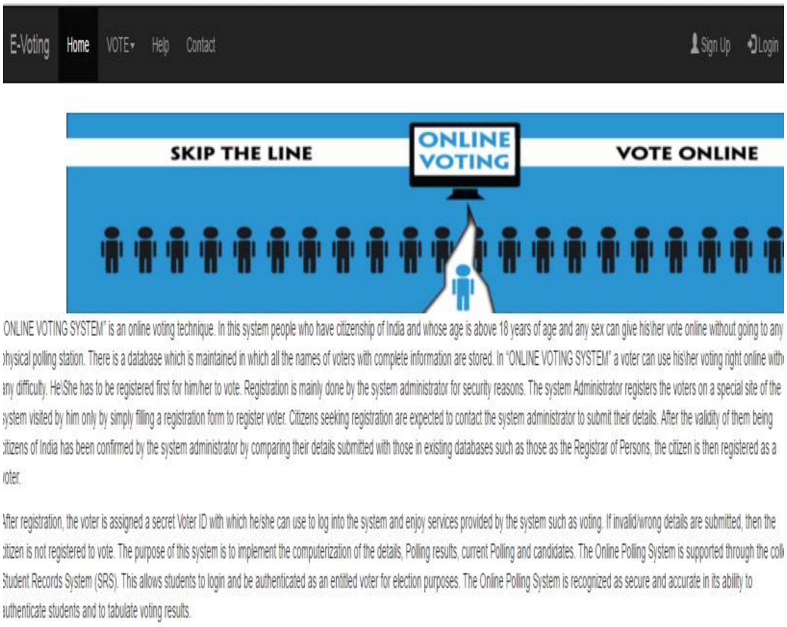
In the implementation of secure E-Voting, we use RSA and MD5 algorithms[3] which use public key encryption cryptographies and hash functions via digital signatures. For the E-Registration of the users we use RSA because it is a Stream Cipher algorithm which considers two keys one key for Encryption and other for Decryption. In RSA[4], public key can be known by everyone whereas for decryption it uses private or secret key.

In the authentication and vote upload phase, we use MD5[5] algorithm which is an hash function algorithm having hexadecimal values for encryption and decryption.

With these algorithms, we can also add Honey-Pot algorithm for providing more secure for our web applications and it deviates attackers from transferring of data through database.

SCREEN SHOTS:

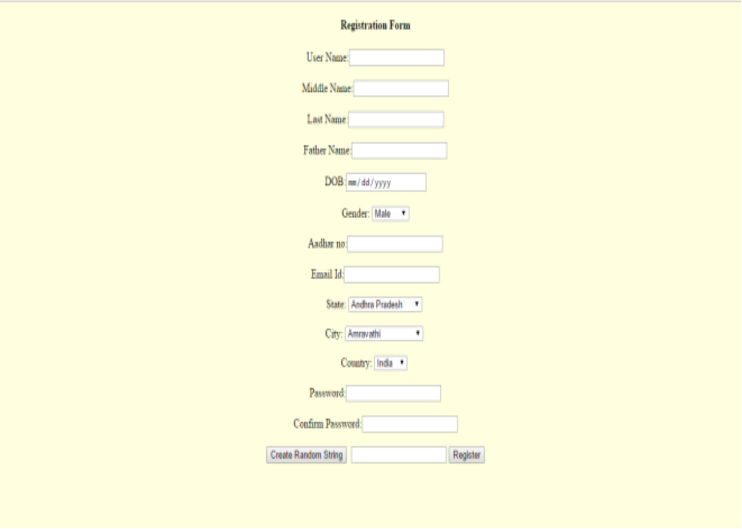
Home page:



ONLINE VOTING SYSTEM” is an online voting technique. In this system people who have citizenship of India and whose age is above 18 years of age and any sex can give his\her vote online without going to any
hysical polling station. There is a database which is maintained in which all the names of voters with complete information are stored. In “ONLINE VOTING SYSTEM” a voter can use his\her voting right online witho
ny difficulty. He\She has to be registered first for him/her to vote. Registration is mainly done by the system administrator for security reasons. The system Administrator registers the voters on a special site of the
ystem visited by him only by simply filling a registration form to register voter. Citizens seeking registration are expected to contact the system administrator to submit their details. After the validity of them being
itizens of India has been confirmed by the system administrator by comparing their details submitted with those in existing databases such as those as the Registrar of Persons, the citizen is then registered as a
oter.

After registration, the voter is assigned a secret Voter ID with which he/she can use to log into the system and enjoy services provided by the system such as voting. If invalid/wrong details are submitted, then the
itizen is not registered to vote. The purpose of this system is to implement the computerization of the details, Polling results, current Polling and candidates. The Online Polling System is supported through the coll
Student Records System (SRS). This allows students to login and be authenticated as an entitled voter for election purposes. The Online Polling System is recognized as secure and accurate in its ability to
uthenticate students and to tabulate voting results.

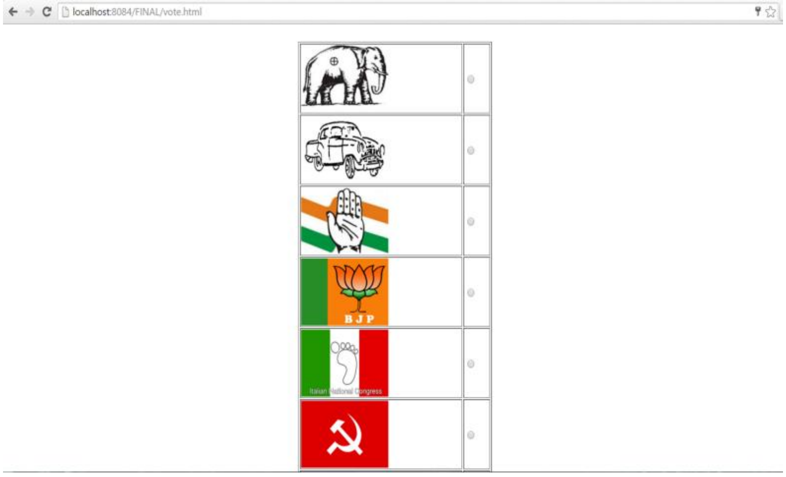
Registration phase:



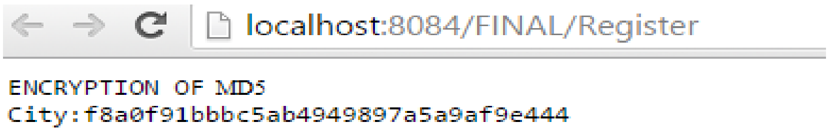
Registration Form

User Name:	
Middle Name:	
Last Name:	
Father Name:	
DOB:	mm/dd/yyyy
Gender:	Male ▾
Aadhar no:	
Email Id:	
State:	Andhra Pradesh ▾
City:	Amravathi ▾
Country:	India ▾
Password:	
Confirm Password:	

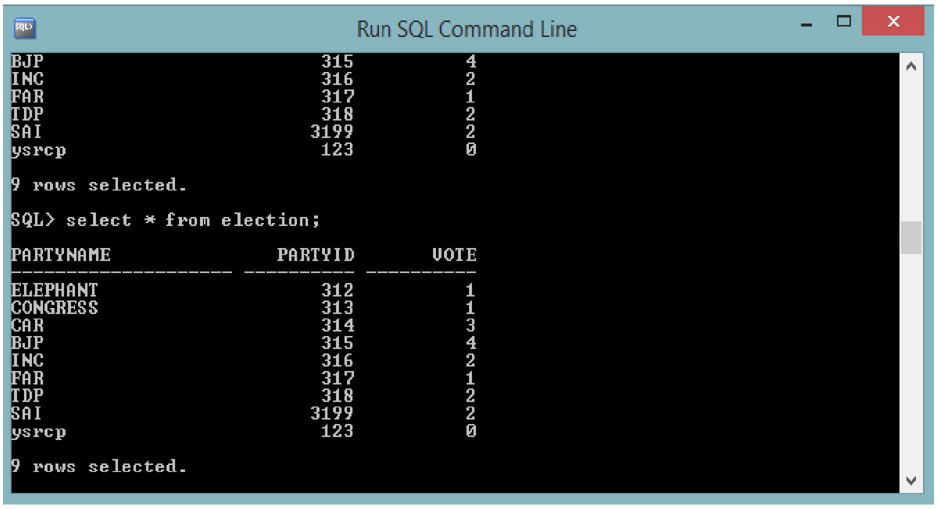
Voting Phase:



Encryption of MD5:



```
ENCRYPTION OF MD5
City:f8a0f91bbbc5ab4949897a5a9af9e444
```



```
BJP                              315          4
INC                              316          2
FAR                              317          1
TDP                              318          2
SAI                             3199          2
ysrcp                            123          0

9 rows selected.

SQL> select * from election;

PARTYNAME                    PARTYID       VOTE
-------------------- ---------- ----------
ELEPHANT                         312          1
CONGRESS                         313          1
CAR                              314          3
BJP                              315          4
INC                              316          2
FAR                              317          1
TDP                              318          2
SAI                             3199          2
ysrcp                            123          0

9 rows selected.
```

CONCLUSION:

In this paper we implemented that a secure online voting system which is used as RSA algorithm having two keys one is for encryption and another for decryption for a registration phase and another algorithm which is MD5 which is a hash algorithm having message digest which helps for voting phase in voting system. These two algorithms maintain the e-voting with high security and efficient purpose.

REFERENCES

[1] http://williamstallings.com/NetSec/NetSec3e.html

[2] http://www.ijircce.com/upload/2013/september/18_Detailed.pdf

[3] http://ijarcet.org/wp-content/uploads/IJARCET-VOL-2-ISSUE-7-2258-2261.pdf

[4] https://jhalderm.com/pub/papers/ivoting-ccs14.pdf

[5] https://www.cs.ucy.ac.cy/courses/EPL475/Cryptography_and_Network_Security_Principles_and_Practice_5thEdition.pd