ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 4, Special Issue 11, September 2015

National Conference on Emerging Trends in Computing, Communication & Control Engineering [NCET 2K15]

On 4th September, 2015

Organized by

Department of CSE, ECE & EEE, Magna College of Engineering, Chennai-600055, India.

E-Voting Protocol Based on Public-Key Cryptography

S.Bhavani

UG Student, Department of ECE, IFET College of Engineering, Villupuram, Tamil Nadu, India

ABSTRACT: In this paper we propose a new secure E-Voting protocol based on public-key encryption cryptosystem. This protocol is summarized in three processes: firstly, access control process which involves the identification and authentication phases for the applied citizens. Secondly, the voting process which will be done by ciphering the voter information using public-key encryption cryptosystem (RSA), to be submitted over an insecure network to the specified government election server. Finally, the election server administrator will sort the final result by deciphering the received encrypted information using RSA private key. Actually, this E-Voting protocol is more efficient than others E-Voting protocols since the voter can vote from his/her own personal computer (PC) without any extra cost and effort. The RSA public-key encryption system ensures the security of the proposed protocol. However, to prevent a brute force attack, the choice of the key size becomes crucial.

KEYWORDS: E-Voting, Cryptography, RSA, System Access Control, and Public-Key.

1. INTRODUCTION

A trustworthy voting system is crucial to a population's consent, as democracies are built on this consent. The base of democracy is to allow people vote freely, so the election result is accepted by voters committee.

A significant motivating factor in the introduction of electronic voting is the elimination of election forms. However, because of the electronic systems nature, the voting form removal may never be suitable with confidential elections. The technology of electronic voting (E-Voting) is used to support the citizen to contribute in decision making in a democratic way. E-Voting is an election system that allows a voter record his or her secure and confidential ballot electronically. E-Voting is casting a vote electronically by tabulating votes using the Internet. There are many E-Voting protocols have been done successfully. Among them are Cryptographic Voting Protocols , A Novel in E-Voting of Egypt and A Simple Protocol for Yes-No Electronic Voting .In Cryptographic Voting Protocols , two different cryptographic protocols were analyzed in terms of security properties. Several potential weaknesses were discovered in these voting protocols. The weaknesses became apparent only when considered in the context of an entire voting system. These weaknesses include: subliminal channels in the encrypted ballots, problems resulting from human unreliability in cryptographic protocols, and denial of service. These attacks could compromise election integrity, erode voter privacy, and enable vote coercion. Whether attacks succeed or not, will depend on how these ambiguities are resolved in a full implementation of a voting system. The expectation of a well designed implementation and deployment may be able to mitigate or even eliminate the impact of these weaknesses.

In Egyptian E-Voting protocol , the authors discovered an Electronic Voting System in Egypt (EVSE) scheme. This scheme is designed to fit in the environment and the conditions of Egypt, trying to solve problems in the old system, conventional system.This system offers a certain degree of flexibility and convenience to the voter to ensure a maximum contribution in the democratic process. If the voter is registered for voting in a particular constituency, e.g. ALX but works in another, e.g. Agouza, then he/she can vote in the Agouza polling station near his/her work place. However, he/she will only have access to the Ballot Server of ALX to participate in the local election of his/her constituency (refer to Figure 1).

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 4, Special Issue 11, September 2015

National Conference on Emerging Trends in Computing, Communication & Control Engineering [NCET 2K15]

On 4th September, 2015

Organized by

Department of CSE, ECE & EEE, Magna College of Engineering, Chennai-600055, India.

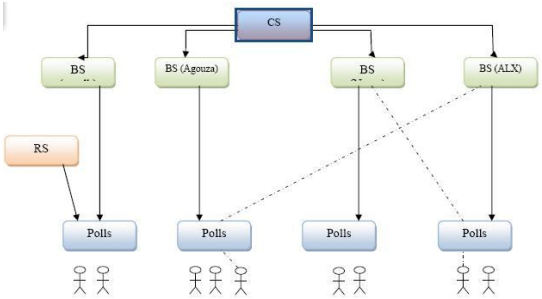


Figure 1. Egyptian E-Voting system hierarchal

A Simple Protocol for Yes-No Electronic Voting , exposed a new electronic voting protocol based on the bit operation XOR and the use of blind signatures. Specifically it is an algorithm designed expressly for the case in which is necessary to choose between two candidates or two options. It is shown that the proposed algorithm satisfies the more important requirements of any E-Voting scheme: anonymity, completeness, correctness and uniqueness.

II. INFORMATION SECURITY AND CRYPTOGRAPHY

Information security is the process which describes all measures taken to prevent unauthorized use of electronic data, whether this unauthorized use takes the form of destruction, use, disclosure, modification, or disruption. Additionally, information security and Cryptography share the common services of protecting the confidentiality, integrity and availability of the information ignoring data form (electronic document, printed document) .

2.1 Cryptography

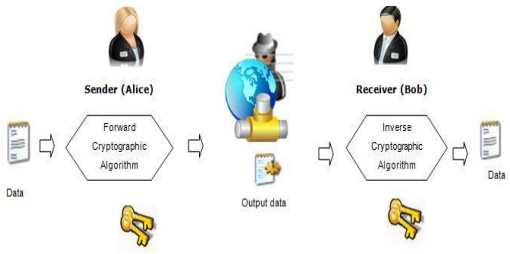


Figure 2. Cryptographic scheme

Cryptography is one of the most important fields in computer information security. It is a method of transferring private information and data through open network communication (refer to Figure 2). However, cryptography provides many services such as: confidentiality, authentication, integrity, non-repudiation, and accessibility.

Cryptography provides the information security for other useful applications such as in encryption, message digests, zero-knowlegde proof of identity, key-sharing and digital signatures. The length and strength of the Cryptography keys are considered an important mechanism. The keys used for encryption and decryption must be strong enough to produce strong encryption. They must be protected from unauthorized users and must be available when they are needed.

Cryptography also contributes to Computer Science, particularly, in the techniques used in computer and network security for access control and information confidentiality . Cryptography is also used in many applications

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 4, Special Issue 11, September 2015

National Conference on Emerging Trends in Computing, Communication & Control Engineering [NCET 2K15]

On 4th September, 2015

Organized by

Department of CSE, ECE & EEE, Magna College of Engineering, Chennai-600055, India.

encountered in everyday life such as: Electronic Voting, computer passwords, ATM cards, and electronic commerce. Generallry, Cryptography may be divided into two main categories :

1. **Asymmetric/ two key/ public-key**: Ciphering and deciphering using a pair of keys.
2. **Symmetric/ one key/ secret-key**: Ciphering and deciphering using the same key (or without key – in the case of Hash function).

2.1.1 Secret-Key (Symmetric) Algorithms

Secret-key (refer to Figure 3) is also known as single-key, or one-key algorithm. Secret-key is an encryption scheme consisting sets of encryption and decryption algorithms. The plaintext is encrypted by key e and the ciphertext is decrypted by key d, where e is the encryption key and d is the decryption key. In secret-key scheme, key d must be equal to key e as shown by Figure 3. The Data Encryption Standard (DES) is an example of the secret-key scheme.

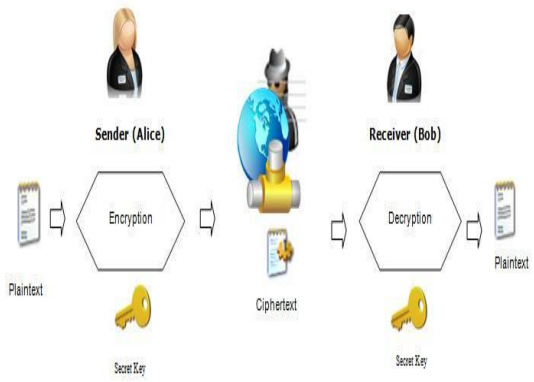


Figure 3. Secret-key cryptographic scheme

2.1.2 Public-Key (Asymmetric) Algorithms:

In public key algorithms (refer to Figure 4), there is a pair of keys, one of which is known to the public and used to encrypt the plaintext to be sent to the receiver who owns the corresponding decryption key, known as the private key.

Every public-key cryptosystem is based on a mathematical problem that is in some sense difficult to solve. These problems are called “hard problems” and are classified in two major categories according to the Cryptography classifications , as P (Polynomial) and NP (Non-deterministic polynomial). The problem is considered to be a P hard problem if the problem can be solved in polynomial time, while a problem is considered to be an NP hard mathematical problem if the validity of a proposed solution can be checked only in polynomial time.

Basically, the three major types of mathematical hard problem that had been successfully being used in Cryptography are described in the following subsections of this part. These problems are :

- the Integer Factorization Problem (IFP)
- the Discrete Logarithm Problem (DLP)
- the Elliptic Curve Discrete Logarithm Problem (ECDLP).
- Chaotic Hard Problem (CHP).

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 4, Special Issue 11, September 2015

National Conference on Emerging Trends in Computing, Communication & Control Engineering [NCET 2K15]

On 4th September, 2015

Organized by

Department of CSE, ECE & EEE, Magna College of Engineering, Chennai-600055, India.

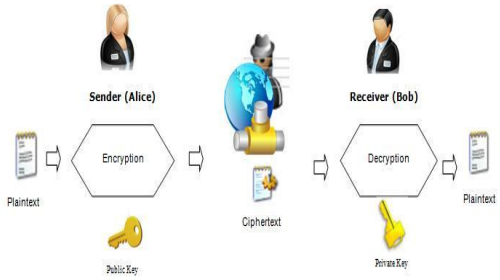


Figure 4. Public-Key cryptographic scheme

2.2 Public Key Encryption

The public-key cryptosystem concept was developed by Diffie-Hellman in 1976 . The RSA algorithm is the first encryption protocol based on the public-key concept, which was published by Revist, Shamir and Adleman in 1978. In RSA, one key is known to public (receiver's public key), and is used to encrypt the information by the sender.

The other key is known as a private key, and it is used to decrypt the encrypted data received by the receiver (receiver's private key).

There are many others public-key encryption algorithms published since the RSA was made public. Among them are ElGamal , Elliptic Curve , etc.

Only a few public-key algorithms are both secure and practical. Of these, only some are suitable for encryption. While the others are only suitable for digital signatures. This can be seen in the following list:

- Integer factorization (RSA, Rabin).
- Discrete logarithm problem (ElGamal).
- Knapsack (subset) (Merkle-Hellman, Chor-Rivest).
- Probabilistic method (Blum-Goldwasser, Goldwasser- Micali).
- Elliptic Curve (Elliptic Curve, modified Elliptic Curve).
- Algebraic code theory (Mc Eliece).
- Fractal system (Newton Raphson law).

2.2.1 RSA Public-Key Encryption Protocol

The RSA protocol (refer to Figure 5) is the most widely used public-key encryption algorithm. It may be used to provide both secrecy and digital signatures. The RSA security is based on the intractability of the integer factorization problem. However, there are three integers e, d and n used in the encryption and decryption algorithm, where $n = p \times q$, with p and q being large primes. Below are the details of the RSA algorithm.

2.3 System Access Control (Logging into Your System)

The system access control process is interconnected and shared between the information security and cryptographic aspects. This process is used to ensure that the system it is accessible only to authorized entities and is inaccessible to others. System access control process provides the computer security with the first security layer by controlling access to that system: Who's allowed to log in? How does the system decide whether a user is legitimate? How does the system keep track of who's doing what in the system?

However, logging into a system by the access control process is a kind of challenge/response scenario. This scenario should be done by identification and authentication processes.

2.3.1. Identification and Authentication

Identification and authentication (I&A) is the process that can be used to identify and verify the entity on the system. In multi-user system, the user must identify himself/herself, then the system will authenticate the identity

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 4, Special Issue 11, September 2015

National Conference on Emerging Trends in Computing, Communication & Control Engineering [NCET 2K15]

On 4th September, 2015

Organized by

Department of CSE, ECE & EEE, Magna College of Engineering, Chennai-600055, India.

before using the system. Therefore, the identification and authentication processes can be done successfully through the following three classical ways:

1. Something you know: password, or a personal identification number (PIN).
2. Something you have: smart card or token.
3. Something you are: fingerprint, voice, retina, or iris characteristics.

2.4 Human Unreliability in Cryptographic Protocols

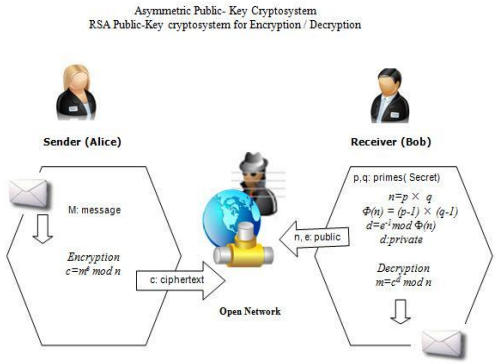
As mentioned in the previous studies, non-computer science specialists have a limited understanding of computer security concepts and how to use its applications . In addition, the previous voting protocols are asking the citizens to become experts in a cryptographic protocol as well in the direct-recording electronic (DRE) voting machine . However, the security in DRE machine relies on how the voters will make their decisions, the interactions between the DRE and voter, and the carefully monitoring for the DRE's output.

III. THE PROPOSED PUBLIC-KEY CRYPTOGRAPHIC E-VOTING PROTOCOL

As mentioned earlier, many previous studies on E-Voting method have been done and focused on facilitating the E-Voting method. These methods are suffering from various weaknesses such as voters' exhaustion, the required hardware cost, and the mandatory polling places.

In this study, the proposed method is based on the analysis of the various factors that play a significant role in the previous E-Voting methods. Therefore the proposed protocol is minimizing the voters' exhaustion since the voters can vote by using his/her own PC and the required time to collect and analyze the final results. However, the proposed protocol is based on RSA public-key encryption protocol. Whereby, the RSA is used to guarantee information it is accessible only to authorized entities and is inaccessible to others. As well RSA is used also to guarantee information remains unchanged from the source entity to the destination entity.

Generally, the proposed method describes three steps for electronic voting system by using the public-key E-Voting protocol (refer to Figures 6-9). These steps are: the system access control process that is to authenticate the voter on the election server, the voting process, and collecting data process.



I . System Access Control Process

As mentioned earlier, system access control process is one of the cryptographic services, which is used to authenticate the voter in the government election server. This process is the first step in the proposed E-Voting system that prepares the voter to be authorized in the advanced E-Voting process. Therefore, the system access control

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 4, Special Issue 11, September 2015

National Conference on Emerging Trends in Computing, Communication & Control Engineering [NCET 2K15]

On 4th September, 2015

Organized by

Department of CSE, ECE & EEE, Magna College of Engineering, Chennai-600055, India.

involves Identification phase and Authentication phase.

1. Identification phase (Registration)

In this phase, the Department of Civil Status and Passports plays the main role, whereby it verifies that the citizen can vote legally. As illustrated in Figure 6 Step 1, the citizen should visit the Department of Civil Status and Passports to verify his/her information to get the election right.

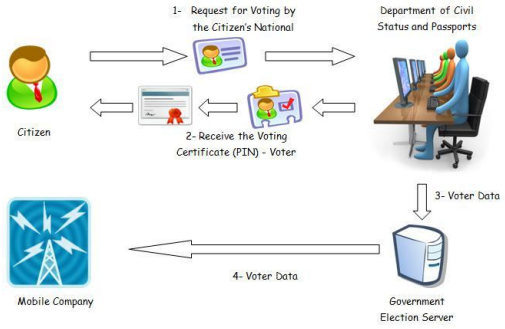
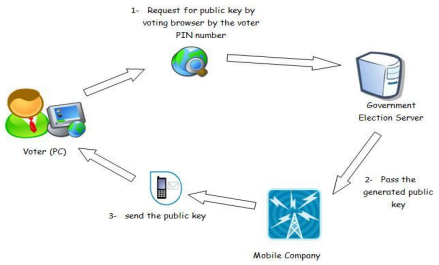


Figure 6. Identification phase

Authentication Phase (Immediately Before Voting)

Figure 7. Authentication phase

As we have mentioned, the factors that required to conducting the E-Voting process are the software and hardware related factors. In this phase, the voter can access the voting process simply by using his/her personal computer (refer to Figure 7). Moreover, the whole Voting process is clarified in Figure 7 from the beginning to the end. The voter login to the E-Voting website by using his/her national_ID and PIN numbers as shown in Figure 6. Once the voter signed to the election website (Refer to Figure 7 Step 1), the election sever will generate a computed RSA public-key (refer to Figure 5). This public key will be then direct passed by mobile company as a short mobile message (sms) to the voter (Refer to Figure 7 Steps 3 and 4). Note that, the receiving of the public key indicates that the voters are ready for voting process immediately.



Voting Process

Typically, the voting process is very critical since the voter cannot logout after receiving the public key. However, the voter is now able to select his/her candidates from the election website. As will to enhance the speed of the voting process, the election website will only display the names of candidates as the voter certain department (refer to Figure 8).

After selecting the candidates and inserting the received public-key through the election website (refer to Figure), the voter should click on the submit button to send his/her selection to the election server. Therefore, the

RSA encryption algorithm is implemented to encrypt the voter information which will be then sent as a ciphertext (encrypted text) to the government election server (refer to Figure 8).

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 4, Special Issue 11, September 2015

National Conference on Emerging Trends in Computing, Communication & Control Engineering [NCET 2K15]

On 4th September, 2015

Organized by

Department of CSE, ECE & EEE, Magna College of Engineering, Chennai-600055, India.

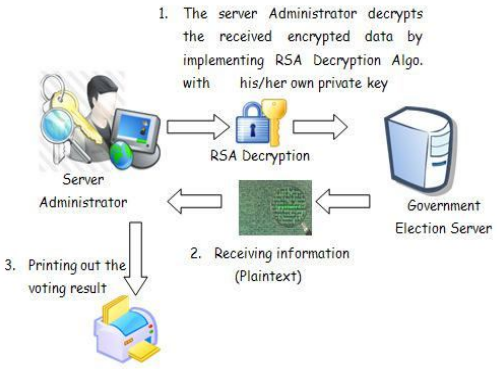


Figure 8.voting process

As will as, at the end of the scheduled time of voting, the collecting data process will be activated for counting votes and confirm the final results (refer to Section III).

IV. COLLECTING DATA PROCESS

The third step in the proposed method is that the receiver (server Administrator) uses the calculated RSA private key to decrypt the received encrypted information (refer to Figure 9). Finally, the Administrator will announce the voting result to the public.

V. CONCLUSION

This paper has shown the possibility of establishing E-Voting protocol based on public-key encryption cryptosystem. The security of the proposed E-Voting depends on RSA public key encryption protocol. As the discussion, the proposed protocol is more efficient than the others E-Voting protocol. It allows the voter to vote from his/her own personal computer (PC) without any extra cost and effort. As new technology for electronic voting protocol, this protocol is proposed to replace the unreliable previous voting system, since voters feel justifiably confident that their votes will be counted. As well as, the proposed protocol needs only the basic requirements such as; PC, internet connection, voting website and standard mobile phone.

REFERENCES

[1] C. Karlof, N. Sastry, and D. Wagner, (2005), “Cryptographic voting protocols: A Systems perspective”, 14th USENIX Security Symposium, pp. 33-49.
[2] M. Abo-Rizka, and H. Ghounaim, (2007) ” A Novel in E-voting in Egypt”, IJCSNS International Journal of Computer Science and Network Security, VOL.7, No.11.
[3] A. Pardos, A. Encinas , S. White , A. del Rey and G. Sánchez, (2007), “A Simple Protocol for Yes-No Electronic Voting”, IJCSNS International Journal of Computer Science and Network Security, VOL.7, No.7.
[4] Menezes, A., P. Van Oorschot, and S. Vanstone, (1996), Handbook of Applied Cryptography, CRC Press, pp.4-15, 516.
[5] I. Branovic, R. Giorgi, E. Martinelli, (2003) “Memory Performance of Public-Key Cryptography Methods in Mobile Environments”, ACM SIGARCH Workshop on Memory performance: Dealing with Applications, systems and architecture (MEDEA-03), New Orleans, LA, USA, pp. 24-31.
[6] M. Alia and A. Samsudin, (2007), “A New Public-Key Cryptosystem Based on Mandelbrot and Julia Fractal Sets”, Asian Journal of Information Technology, AJIT, 6(5), pp. 567-575.