# Design Secure E-voting Scheme

**A thesis submitted in partial fulfillment of the requirements for the Master degree in Computer Science**

**Omar Al Hnaity**

**Department Of Computer Science**

**Faculty of information technology**

**Supervisor**

**Professor Dr. Sattar J Aboud**

**Amman Jordan**

**June 2008**

## اقرار  تفويض

انا عمر سعد سعيد  الحنيطي افوض جامعة الشرق الاوسط للدراسات العليا بتزويد نسخ من رسالتي للمكتبات او المؤسسات او الهيئات او الافراد عند طلبها.

**التوقيع:**

**التاريخ:**

## Authorization statement

I, **Omar Saad Saed Al Hnaity,** Authorize the Middle East University for Graduate Studies to supply a copy of my Thesis to libraries, establishments or individuals upon their request.

**Signature:**

**Date:**

## Committee Decision

This Thesis (A generic menu-based interface for web querying) was successfully defended and approved on June 2th 2008

**Examination Committee signatures:**

**Professor Dr. Sattar J Aboud**

Professor Department of Computer Information Systems

(Middle East University for Graduate Studies) ……………...

**Professor Dr. Alaa Al-Hamami**

Professor Department of Computer Information Systems

(Middle East University for Graduate Studies) ……………...

**Dr. Nidal Shilbayeh**

Chairman of department computer science

(Middle East University for Graduate Studies) ……………...

**Dr. Musbah Aqel**

Associate Professor Department of Computer Information Systems

(Middle East University for Graduate Studies) ……………...

## Declaration

I do my hereby declare the present research work has been carried out by me under the supervision of Professor Dr. Sattar J Aboud and this work has not been submitted elsewhere for any other degree, fellowship or any other similar title.

Signature:

Date:

Omar Al Hnaity

## Dedication

*I dedicate my thesis to my family and many friends. A special feeling of gratitude for my loving parents.*

## Acknowledgments

I would like to express my gratitude to many people who saw me through my thesis; to all those who provided support, talked things over, read, write, offered comments, allowed me to quote their remarks and assisted in the editing, proofreading and design.

I would like to give special thanks to my favorite supervisor Professor Dr.Sattar J Aboud.

Last and not least, I beg forgiveness of all those who have been with me over the courses of the years and whose names I have failed to mention.

# Contents

## List of Figures

## List of Abbreviations

| | |
|---|---|
| **DB** | Data Bases |
| **DRE** | Direct-Recording Electronic |
| **EV** | Electronic Voting |
| **FOO** | Fujioka, Okamoto, and Ohta |
| **ID** | Identification |
| **PC** | Personal Computer |
| **REVS** | A Robust Electronic Voting System |
| **RSA** | Ron Rivest, Adi Shamir, and Leonard Adleman |
| **TCB** | Traffic Conditioning Block |
| **TCP** | Transmission Control Protocol |
| **US** | United States |
| **VH** | Vote Here A Verifiable E-Voting Protocol |
| **VVAT** | Voter Verified Audit Trail’ |

| | |
|---|---|
| **VBM** | Voting By Mail |
| **WWW** | World Wide Web |

## Terminologies

**Accuracy:** the result of the voting process must be precise. It is not possible for a vote to be altered, it is not possible for a validated vote to be eliminated from the final tally, and it is not possible for an invalid vote to be counted in the final tally.

**Anonymity**: typically refers to a person and often means that the personal identity or personally identifiable information of that person is not known.

**Auditing**: is an evaluation of a person, organization, system, process, project or product.

**Ballot**: is a device (originally a small ball see blackball) used to record choices made by voters.

**Blind signature**: blinding is a technique by which an agent can provide a service to a client in an encoded form without knowing either the real input or the real output.

**Constitutional:** is a system for governance, often codified as a written document that establishes the rules and principles of an autonomous political entity.

**Convenience:** a system is convenient if it allows voters to cast their votes quickly, with minimal equipment or special skills.

**Cryptography:** is the science and study of hiding information and secrete writings.

**Database**: is a structured collection of records or data that is stored in a computer system. A database relies upon software to organize the storage of data.

**Democracy:** describes a small number of related forms of government and also a political philosophy. A common feature of democracy as currently understood and practiced is competitive elections.

**Digital signatures:** a property that used to signing the messages.

**Electronic commerce:** commonly known as e-commerce, consists of the buying and selling of products or services over e-systems such as the Internet and other computer networks.

**Eligibility**: is a decision making process where a population chooses an individual to hold official offices.

**Authentication:** Only eligible and authorized voters can vote and each voter can vote only once.

**Electronic Voting:** commonly known as e-voting is a term encompassing several different types of voting, embracing both electronic means of casting a vote and electronic means of counting votes.

**Fairness:** nothing must affect the voting. No participant can gain any knowledge about the (partial) vote before the counting stage.

**Flexibility:** a system is flexible and simple not complex.

**Groundbreaking**: is a traditional ceremony in many cultures that celebrates the first day of construction for a building or other project.

**Homomorphism**: is a structure preserving map between two algebraic structures.

**Individual verifiability:** each eligible voter can verify that his vote was really counted.

**Mixnet:** is a collection of servers whose task is to shuffle a given input sequence of encrypted votes.

**Mobility:** a system is mobile if there are no restrictions on the location from which a voter can cast a vote.

**Privacy:** all votes must be secret. No participant other than a voter should be able to determine the value of the vote cast by that voter. In other words, neither election authorities nor anyone else can link any ballot to the voter who cast it.

**Protocols**: a set of rules governing communication within and between computing endpoints or entities.

**Reliability:** all possible steps shall be taken to avoid the possibility of fraud or unauthorized intervention affecting the system during the whole voting process.

**Receipt-Freeness:** no voter should be able to convince any other participant of his vote.

**Scheme**: it is a methodology and designing mechanisms for algorithm, it can be consider it as system.

**Transparency:** information on the functioning of an e-voting system must be made publicly available.

**Universal Verifiability:** a system is verifiable if any person can independently verify that all valid votes have been counted correctly. Any participant or passive observer can check that the published final tally is really the sum of the votes.

**Verification:** is the act of proving or disproving the correctness of intended algorithms underlying a system with respect to a certain formal specification or property, using formal methods of mathematics.

## Abstract

Design Secure E-voting Scheme by Omar Al Hnaity Supervisor Professor Dr.Sattar J Aboud.

One of the most important tools for a healthy democracy is the election system. It is the central pillar which all the democratic institutions are based upon, and it is what modern society depends on. With the advance of Information Technology, electronic voting systems emerged as a new way to conduct elections. Nowadays, several countries around the world are starting to test and use some form of electronic election system. Advantages such as quick tallies, his possibility of remote voting and cost reduction are among the main reasons for it; however there are several obstacles that still need to be solved.

This thesis propose e-Voting scheme that's solve the security requirements. The proposed e-voting scheme is a new Internet voting scheme developed using cryptography techniques. This scheme consists of three phases registration phase, voting phase, and Counting phase. In the registration phase the voters come to the registration centers to generate credentials based in public key cryptography techniques to generate tow pairs of keys. In the voting phase the vote will walk through many steps to be considers as right vote, as will the vote encrypted two times using public key cryptography techniques plus contains handshake protocol to ensure the validity of the voter. In the counting phase the votes will be counted two times from two sources to gain the highest accuracy.

The proposed e-voting scheme addresses the security requirements for e-voting over the Internet, including authentication, completeness, correctness, privacy, integrity, availability and reliability.

**Key Words**: e-voting scheme, security properties, digital signature, digital certificates, encryption scheme, handshake, Authentications.

## الملخص بالعربية:

تصميم نظام تصويت امن اعداد عمر الحنيطي واشراف الاستاذ الدكتور ستار عبود.

واحدة من اهم المواضيع التي تجعل من الديمقراطية ديمقراطية عادلة وصحيحة هي نظم الانتخابات, وتعتبر العامود الاساسي في العملية الديمقراطية, مع  تقدم تكنولوجيا المعلومات ظهرت طرق جديدة لاجراء الانتخابات مثل التصويت عبر الانترنت

عدة بلدان في جميع انحاء العالم بدأت باختبار واستخدام هذه الانظمة الجديدة وهي تمتاز بالسرعة وتوفير الوقت و الجهد والتكلفة. الا ان هناك العديد من العقبات التي لا تزال في حاجة الى حسم.

في هذة الرسالة نتعرض لاقتراح طريقة جديدة للتصويت عبر الانترنت تضمن المتطلبات الامنية.

والطريقة المقترحة  مبنية على بعض طرق التشفير وهذه الطريقة تتكون من   ثلاثمراحل وهي التسجسل و التصويت و الفرز. ففي مرحلة التسجيل يذهب الناخب الى مركز التسجيل لاعداد الارقام السرية الخاصة به  ويستخدم في هذه المرحلة نظام التشفير بالمفتاح العام لتوليد زوجين من المفاتيح. اما في مرحلة التصويت يدخل الصوت في عدة مراحل ليتم اعتماده فهو يشفر مرتين بالاضافة طرقة المصافحة لتضمن ان الناخب هو بعينه. اما في مرحلة الفرز فهي تعتمد على العد من مصدرين مختلفين لضمان الدقة.

وهذه الطريقة تضمن بعض الخصائص الواجب توفرها في النظام مثل      توثيق المعلومات ، واكتمالها وصحتها ، والخصوصيه ، والنزاهه ،الموثوقيه.

# 1. CHAPTER ONE: Introduction

## 1.1.Background

Over the last few centuries, human beings have experienced two major revolutions; the industrial revolution and the Information revolution. Concerning the first, once in 1869, Thomas Edison created electronic machine to help speed the election process Figure 1 shows this machine, then he received US patent 90,646 for an e-voting device. Edison tried to sell the invention to the Massachusetts legislative but unfortunately fail. [41]

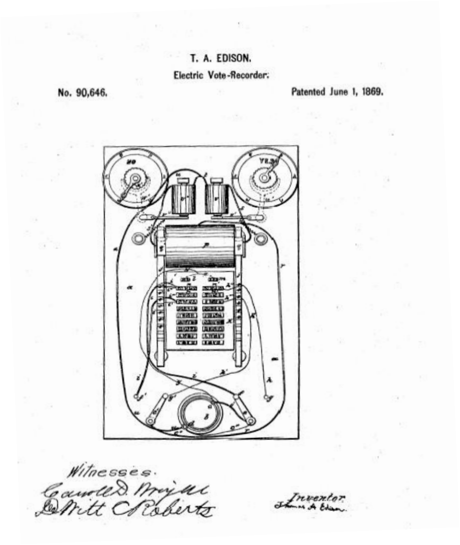


Figure 1-1: Edison Electronic Machine

Concerning the second revolution, in the last decades of the 20th century till now, witnessed the beginning of a new revolution namely the telecommunication and information technology revolution, based on computerized systems.

However the idea of e-voting again arose in the 1970s by the development Direct-Recording Electronic (DRE) systems, and has been used in voting stations in DRE cabinets, where the votes are stored electromagnetically [1]. In 1990s, a new technology arose called the Internet. Internet simply is a combination of telecommunication and computerized systems consisting of many computers connected with each other through a network across the entire world called the World Wide Web (WWW) [45]. In the past, most of the computer applications were executed on stand-alone computers. Today's applications can be developed to communicate with hundreds of millions of computers. With the recent revolution of growth on the World Wide Web, the ability to communicate more information became faster and cheaper; simply fingertips. We have email, e-newspapers, and video conferencing all leading the trend towards a paperless society. In the late 1990s, there have been attempts to apply e-solutions to make democratic process easily and simply. It seems that everything is being automated by computers today. Elections themselves have not remained completely static [1]. The e-voting idea was extended in April 1997 when Monterey County, California experimented the first voting by mail system. [1]

Some of the security problems may arise when trying to apply democracy using technology, especially in e-voting process. The fact is, progress in the field of e-voting has moved very slowly over the last decades. It was built using electrical machines as DRE and the votes were saved as electromagnetic signals, but now we are using data transfer over networks. This scheme needs some security enforcement techniques to protect the data against attackers using cryptography science. Interest in cryptography increases as it is being used further more in many critical fields like military related systems, banking systems and others. Nowadays, the recent advances in the field of cryptography can bring all these trends together and create a secure e-voting scheme. The proposed scheme use cryptography science and new technologies based on modern computer systems to produce a new voting scheme satisfying all the possible needs.

## 1.2.Problem Definition

E-voting systems are beginning to be implemented in various countries in the world. Quick tallying and cost saving are the main reasons for that, but there are still concerns related to the security of such system. Current e-voting systems lack reliable recounting processes and devices to validate votes in the elections.

Concerning voting over Internet schemes, most of the today proposed concentrate on algorithms to conduct anonymous elections, but do not address replay attacks problems that might occur in the voter's computer, which can be infected with any kind of malicious programs that can possibly change the vote or disclose the voter’s intentions, thus violating one of the fundamental points of elections, the privacy.

The problem summarized in finding secure and trust scheme for voting over Internet and make all citizens able to participate on democratic process over Internet with highest security, flexibility, transparency and accuracy.

### 1.3.Objectives

The objectives of the thesis are as follows:

1. To design e-voting Scheme to support democratic process
2. To create secure protocols to help in e-voting design
3. To apply public key cryptography techniques as much as possible in the protocols
4. To make the scheme usable as much as possible and ensure that all needed security properties and e-voting requirements in the scheme are applied and verified
5. Develop a secure, user friendly and standalone system for small scale election.

## 1.4.Motivation

Our Motivation based on the following fact:  voting is regarded as one of the most effective methods for individuals to express their opinions on a given topic. E-voting refers to the use of computers or computerized voting equipment to cast votes in an election. Sometimes, this term is used more specifically to refer to voting that takes place over the Internet. With arise of Internet technology, e-voting will become universally accepted in the upcoming years. Hence current implementations for Internet elections contain security problems; the use of cryptography protocols seems to be a suitable response to establish security in democratic elections.

E-voting has been intensively studied for over the last decades. Up to now, many electronic voting protocols have been proposed, and both the security as well as the effectiveness has been improved. However, no complete solution has been found in neither theoretical nor practical domains. The basic process of any democratic election is almost standard although a wide variety of voting schemes and protocols exist.

## 1.5.Secure e-Voting Requirements

There are a wide variety of e-voting requirements definitions with different naming convention such as requirements, properties, characteristics etc. in general e-voting scheme must respect all the principles of democratic elections and referendums. Also must be as reliable and secure as democratic elections and referendums. This general principle encompasses all electoral requirements, whether mentioned or not these requirements can be grouped and summarized as following:

**Eligibility (Authentication):** Only eligible and authorized voters can vote and each voter can vote only once.

**Privacy:** All votes must be secret. No participant other than a voter should be able to determine the value of the vote cast by that voter. In other hand, neither election authorities nor anyone else can see any vote to the voter who cast it.

**Receipt-Freeness:** No voter should be able to convince any other participant of his vote.

**Fairness:** Nothing must affect the voting. No participant can gain any knowledge about the partial vote before the counting stage.

**Accuracy:** The dishonest voter cannot disrupt the voting. No one can falsify the result of the voting. Every participant should be convinced that the election tally accurately represents the “sum” of the votes cast. It is not possible for a vote to be altered, it is not possible for a validated vote to be eliminated from the final tally, and it is not possible for an invalid vote to be counted in the final tally.

**Individual Verifiability:** Each eligible voter can verify that his vote was really counted.

**Universal Verifiability:** A scheme is verifiable if anyone can independently verify that all valid votes have been counted correctly. Any participant or passive observer can check that the published final tally is really the sum of the votes

**Reliability:** All possible steps shall be taken to avoid the possibility of fraud or unauthorized intervention affecting the scheme during the whole voting process.

**Convenience:** A scheme is convenient if it allows voters to cast their votes quickly, in one session, and with minimal equipment or special skills.

**Flexibility of the usability:** A scheme is flexible not complex

**Mobility:** A scheme is mobile if there are no restrictions on the location from which a voter can cast a vote.

**Transparency:** Information on the functioning of an e-voting scheme must be made publicly available.

**Scalability:** The ability for a voting scheme to easily expand to cover many areas.

**Efficiency:** means that a Scheme does good work without spending too many resources as machines, humans and time.

### 1.6.Significant

This work is benefit to all governments especially, Ministry of Interior in HKJ, The electoral committee in any country and any organization needs secure and accurate election process over Internet to make all participants to take part in the election from anywhere. This work also benefit in the education and scientific process.

### 1.7.Contributions

In this thesis we proposed an e-voting scheme that fulfills as much as possible the secure e-voting requirements which mentioned in section 1.4. The following are the requirements and how they are satisfied in the proposed e-voting scheme.

**Authentication:** Only the eligible and authorized voter can be vote that is fulfilled by using login procedure by entrance user name and password that is a private key.

**Privacy, Receipt-Freeness, Fairness:** All votes are secreting by encrypting each vote.

**Accuracy, Individual verifiability and public verifiability**: The existing of two data sources voters and candidates databases we can do the double count of the votes from two sources and check the results that is guarantee a high accuracy. We can guarantee the individual variability from the voter's database and guarantee the public variability from the candidate's database.

**Reliability:** All the security steps in the scheme can be guaranteed the reliability because no way to complete the voting process without assure if all these steps are completed successfully or not.

**Convenience and Mobility:** The propose scheme is convenience and mobile because it is using the Internet

**Flexibility of usability:** The scheme is flexible because the voter can do few clicks to complete the voting process

**Transparency:** All votes and credentials are kept in secrete way and we can retrieve it any time without vagueness.

**Scalability:** The proposed scheme is scalable. It means that to cover all countries on the world because of using Internet

**Efficiency:** The scheme covers almost all the requirements for the secure elections the scheme it is efficient, because it does not need many resources.

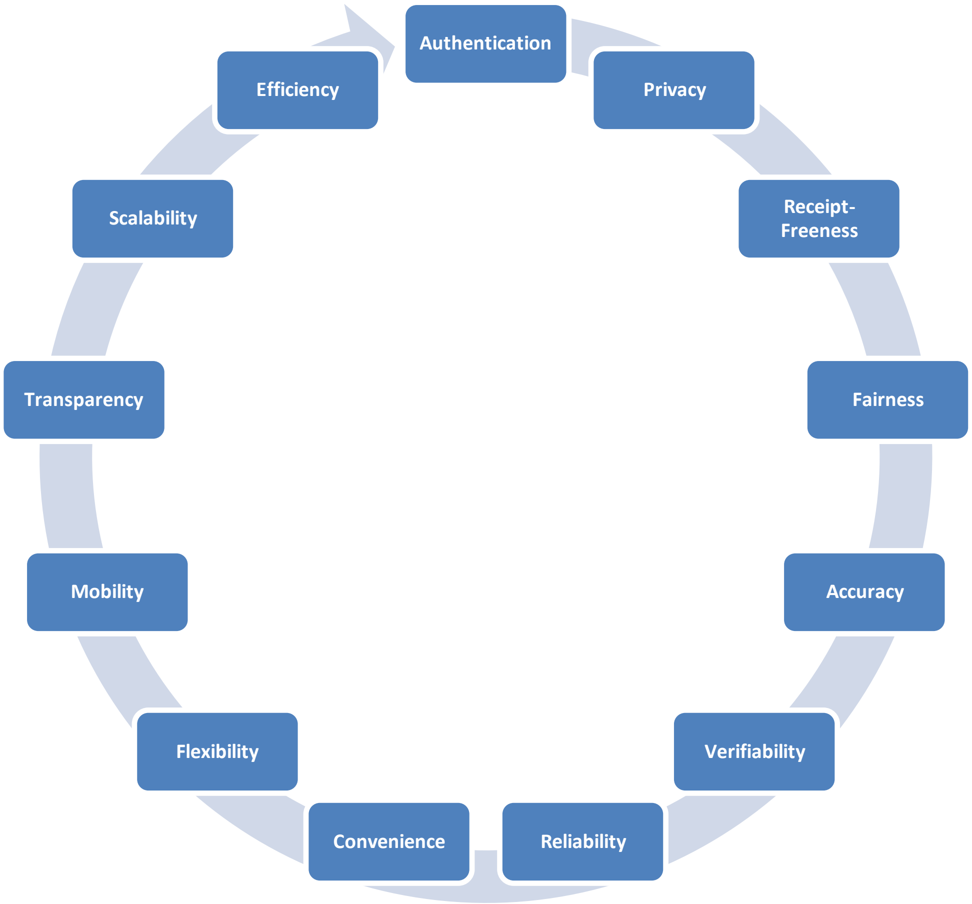


**Figure 1-2: Secure e-Voting Requirements**

## 1.8.Methodology

The thesis examines the state of security in e-voting schemes used today, and proposes a scheme that can be securely used to vote over Internet. The collection of data is made using public available information in the Internet, books, literature reviews and also from discussions with people who are involved in such process. The security analysis of the current voting schemes is based on study at many points such as privacy, integrity, transparency and verifiability. A background of the topics related to the subject is given so that the reader is acquainted with the technology and terms used throughout the thesis.

The evolution of the e-voting currently implemented is the vote over Internet. This is explored and developed from a theoretical point of view, supported by material from several sources as above noted. Finally, the conclusion sums up the main points discussed, problems and solutions found, and some of the difficulties encountered when researching the covered topics.

## 1.9.Thesis Organization

This thesis consists of six chapters Chapter one is the introduction that present the problem and the solutions. Chapter two describes the related work of e-voting schemes currently available. Chapter three presents the proposed e-voting scheme. Chapter four discusses the testing and results of the proposed scheme. Finally Chapter five gives the conclusions and Future work

# 2. CHAPTER TWO: Related Work

## 2.1.Overview

Up to date there are three general design approaches for building e-voting schemes based on strong cryptography assumptions: mixnet-based, introduced by Chaum [14] homomorphic encryption-based, introduced by Benaloh [21]; and blind-signature-based, introduced by Fujioka [16]. These approaches rely on different cryptography assumptions, have different advantages and disadvantages. The following sections briefly discuss these schemes**.**

## 2.2.Mixnet-based schemes

In a mixnet-based scheme [14], the election scheme is built around a basic cryptography primeitive called a mixnet. A mixnet is comprised of a collection of servers whose task is to shuffle a given input sequence of cipher texts that is encrypted votes. This serves as an implementation of a robust anonymous channel. To ensure that mix-servers do not drop or substitute cipher texts, it is necessary that the servers provide proofs of correct operation. A general criticism of mixnet-based schemes is that these proofs are cumbersome.

Mixnet-based scheme implementations are discussed in the following two subsections.

### 2.2.1. Scytl Pnyx

Is an innovative poll-site e-voting solution that turns a standard PC into a secure, accessible and reliable DRE voting terminal. It can be used to carry out all types of electoral processes in a secure and convenient manner with the highest usability and accessibility standards.

The main advantage of the DRE that is ensure the integrity of the votes, voters' privacy, the audit ability of election results, and offers a number of verification mechanisms that enable voters to check the correct casting and recording of their votes.

The disadvantage is the attacks on the voter client. Much of the concern about the security of electronic voting has involved attacks on DRE voting terminals. With DRE voting, the voter uses a voting machine that is provided by a local election authority, with little recourse against untrustworthy authorities [34].

### 2.2.2. VoteHere VHTi

VoteHere provides a method of voter verification of election integrity, based on receipts and complicated mathematical cryptography in the voting booth, the voter enters his ballot choices on the DRE.  The receipt defines an encrypted ballot; the receipt does not reveal how the voter voted.  After the voting process, the voter may check that a copy of this receipt is included in the official election data posted on a public web site.  Anyone, using trusted complex mathematical software of his choice, can verify that the official results are consistent with the posted data.

The main advantage is the integrity of the vote. Disadvantages  the product is not functionally complete, existing only as a reference library, application software the voter's experience in the voting booth is slightly complicated, because the scheme is complicated to understand, election officials will have to be educated in it and will also have to be able to educate voters, and some voters might not have confidence in a scheme they do not understand, voters with limited eyesight might have difficulty reading the receipt and the planned functionality for alternative user interfaces is not yet available, election officials must set up and maintain an authenticated web site, as configured; There is no attempt to maintain consistency between the Diebold and VoteHere schemes, even when both units are honest, as is true for all schemes under study, the scheme requires integration with the DRE display software.  Each unit costs approximately $500 [37].

## 2.3.Homomorphic-based Schemes

In a homomorphic encryption-based voting scheme [31], votes are added while encrypted, so no individual vote ever needs to be revealed. In order to ensure that the private decryption key of the election is not used to decrypt an individual vote, a threshold encryption scheme must be applied to distribute the key among several authorities in such a way that multiple authorities have to combine their shares in order to use it. Homomorphic encryption is the approach we followed for the proposed voting scheme. A great advantage of this approach is that voters may openly authenticate themselves to the voting servers, means that, there is no need for any anonymous channel to ensure voter privacy. Homomorphic-based Schemes implementations are discussed in the following two subsections.

### 2.3.1. ADDER

This work introduces the ADDER system, an Internet based, free and open source e-voting scheme which employs strong cryptography. The proposed scheme is a fully functional e-voting platform and enjoys a number of security properties, such as robustness, trust distribution, ballot privacy, audit ability and verifiability. It can readily implement and carry out various voting procedures in parallel and can be used for small scale boardroom department-wide voting as well as large-scale elections. In addition, ADDER employs a flexible voting scheme which allows the system to carry out procedures such as surveys or other data collection activities. ADDER offers a unique opportunity to study cryptography voting protocols from a systems perspective and to explore the security and usability of electronic voting schemes [45]. The advantage of this approach is that voters may openly authenticate themselves to the voting servers, this mean that there is no need for any anonymous channel to ensure voter privacy. Disadvantage the registration is done over the Internet without high security constrains which make the impersonation problem occur in easy way [1].

### 2.3.2. Civitas

Civitas is the first e-voting system that is coercion-resistant, universally and voter verifiable and suitable for remote voting using some of cryptography techniques to ensure full security in the voting process. The advantages of this scheme the scalability and availability Disadvantages of this scheme are Complex, and much of the concern about the security of e-voting has involved attacks on registration [29].

## 2.4.Blind signature-based schemes

Blind signature-based schemes use a method proposed by Fujioka, Okamoto, and Ohta [17]. In this scheme, voters obtain a blind signature on their ballot from an administrator. That is, the administrator signs the ballot without being able to read its contents. Subsequently, voters submit their blindly signed ballots through an anonymous channel to a voting bulletin board that will only accept ballots signed by the administrator. The main advantage of the blind signature approach is that it removes the requirement for the anonymous channel to be robust. Its main disadvantage is that the voter needs to be active in at least two phases to ensure verifiability it is not a vote-and-go voting scheme. From an implementation point of view, realizing an anonymous channel is not straightforward. In the known implementations it considered that it is easy to correlate voters with their votes or in any case, there is at most a single point of failure for anonymity [16].

Blind signature-based schemes implementations are discussed in the following two subsections

### 2.4.1. REVS

REVS is an Internet e-voting scheme based on blind signatures and designed to be robust in distributed and faulty environments. However, the execution of REVS client system, used by voters, can be tampered by intruders willing to compromise the accuracy of submitted votes or the privacy of voters. In this document the author present a new, intrusion tolerant e-voting client architecture for REVS. This architecture is based on public key cryptography, smart cards and FINREAD terminal readers. By using this TCB we hope to be able to build an intrusion-tolerant, client voting scheme formed by the TCB and an ordinary personal computer. The PC makes the required bridge between the TCB and the Internet. A compromised PC should at most interfere with the voting protocol using denial of service attacks**.**

Advantages the scheme can be sure that to accomplishes the desired characteristics of traditional voting schemes, such as accuracy, democracy, privacy and verifiability. .Disadvantages that is it allows a certain degree of failures, with server replication; and none of the servers conducting the election, by its own or to a certain level of collusion, can corrupt the election outcome [17].

### 2.4.2. Secure E-Voting System with Collision-Free AID

This paper proposed an e-voting scheme consisting of three roles: voters, authentication center and tallying center; and proceeding to three phases, register phase, voting phase, and tallying phase.

In the register phase the voter cooperates with authentication center to generate a collision-free anonymous identity to protect the voter's privacy and prevent from double-voting, and generate simple secret sharing scheme to split a ballots among the distinguish tallying center that neither of them alone can restore the ballot. Such a scheme enforces the fairness property that no one can learn the voting outcome before the tallying phase. The system ensures many of secure properties as anonymity, eligibility, farness, integrity, mobility, uniqueness and verifiability [36].

The main advantage of the scheme is high trust but at same time it is so complex. The disadvantage is that voter must be corporate with authentication center to be vote and the scheme overload the voter many steps complete the process [24].

## 2.5. Other methods

There exist other implementations not based on voting-oriented cryptographic primitives. We now review them briefly. The Diebold AccuVote-TS system is one of the most heavily criticized non-Internet-based electronic voting systems used in practice [56]. Problems pointed out include: incorrect use of cryptography, poor code quality, and possibility of smartcard forgery, among many others. Despite Diebold's rebuttal [57], the system remains mistrusted by a number of experts. The SERVE system is a Department of Defense government-funded project for Internet-based voting. SERVE works as follows: For each voting district, a local election official (LEO) generates a key pair. When a ballot is cast, it is sent with identification over the Web. This information is encrypted with the Web server's public key. The Web server verifies the eligibility of the voter, decrypts the ballot, removes the voter's name, and re-encrypts the ballot with the LEO's public key. This ballot is then sent to the LEO. SERVE was found to have much vulnerability [58] and the project was discontinued. One of the major vulnerabilities particular to SERVE is that the Web server knows the vote of each voter, and can tie it to his identity. If the Web server is compromised, voter privacy is broken entirely. RIES (Rijnland Internet Election System) [59] is an election system developed in 2003 and 2004 for the Water Board elections at Rijnland and De Dommel in the Netherlands. The system has much vulnerability, such as the use of a single master triple-DES key. EVM2003 is a project to develop a free and open source electronic voting machine. However, it seems to have undergone very little activity since its inception in 2003 and does not seem to employ any cryptographic voting protocols. Condorcet Internet Voting Service (CIVS) is a Web-based free voting system that employs the Condorcet election method. Voters submit a ranking of candidates instead of picking only one candidate. CIVS employs some cryptographic integrity mechanisms but falls short of offering cryptographic guarantees for voter privacy. GNU.FREE is a free Internet voting system released by the GNU project. In GNU.FREE, voting is not done over the Web. Rather, a stand-alone Java program is used to cast votes which are encrypted using a cipher (Blowfish). The system does not provide sufficient security (beyond preventing regular eavesdropping), and it is easy for a malicious system to correlate voters and their votes. It is worth noting that EVM2003, CIVS, and GNU.FREE are the only voting systems we have found that are free software. [1]

# 3. CHAPTER THREE: The Proposed Scheme

## 3.1.Voting Procedure

The proposed voting scheme consists of three phases; registration, voting and counting. Figure 3.1 shows the scheme.

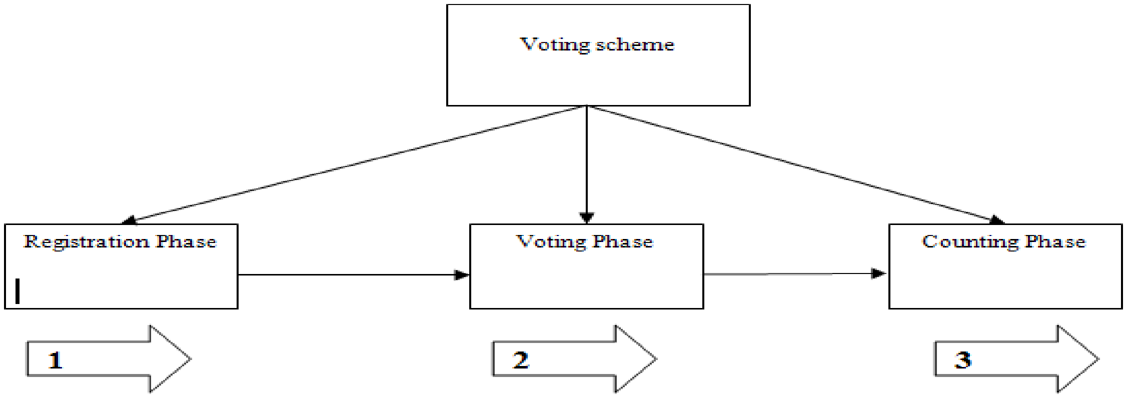


**Figure 3-1: Voting Scheme**

Registration phase consists of three steps verification, keys generation and keys delivery. Figure 3.2 shows the registration phase.

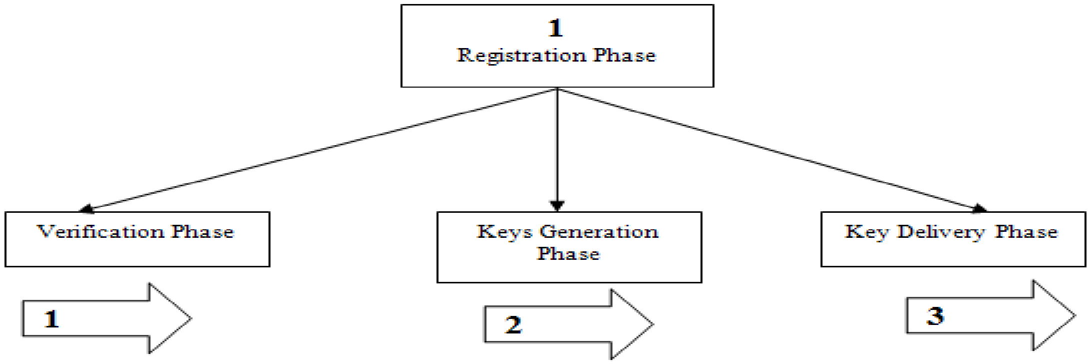


**Figure 3-2: Registration Phase**

Voting phase consists of three steps Login, voting and sending vote. Figure 3.3 shows the voting phase

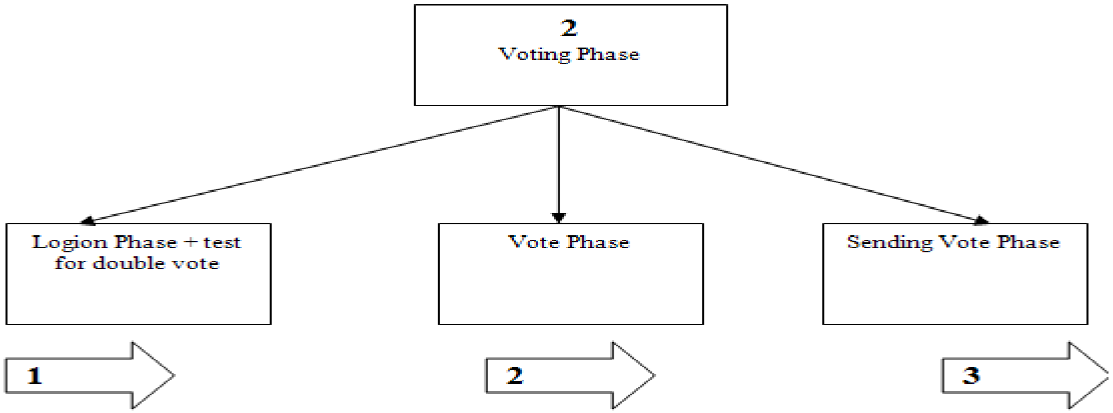


**Figure 3-3: Voting Phase**

Finally counting phase consists of two steps counting and auditing. Figure 3.4 shows the Counting phase

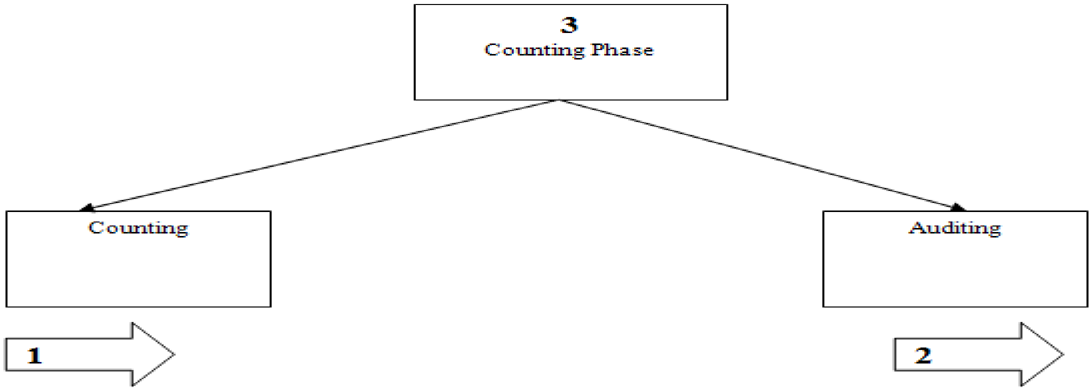


**Figure 3-4: Counting Phase**

## 3.2.Registration

During the registration phase of remote e-voting scheme, the voter obtains a credential that proves the validity of their vote later, in the voting phase [39]. The entire registration protocol suitable for real and workable voting scheme, whether remote or not. The advantage of the protocol is that it is based on weaker assumptions on the trustworthiness of the registration entities. The trust is distributed among several entities and the functionality of the trusted entities is simplified. This results in higher security and an increased degree of robustness. One criterion in the classification of e-voting protocols is the place where voters cast their votes. Accordingly, e-voting schemes belong to two groups: voting-site and remote site.

In a voting-site scheme, votes are register and cast at special locations, and those locations can be either supervised or not. These types of schemes provide a more controlled environment, which aids in achieving security but at this time it is still not flexible, not modern and not simply for those who are outside their home countries .

Remote schemes, on the other hand are designed in a way such that voters can vote from any location with Internet connection. It increases flexibility but causes additional threats. The registration protocol is the only one based on on-site category but other protocols in the scheme are based on remote category. Choosing on-site category for registration phase has many advantages most important one is personal authentication for the voter must be right and verified, if the first step is right all steps can be right to avoid any confusion that might occur. The process begins when the voter comes to the site Building Registration Center (BRC) and brings probative papers to authenticate physically his or here personalities, after the verifier verifies the identity of the voter that pass the first step in the protocol. The next step is verifying the legality of the voter, if the entity meets the legal conditions, he will be diverted to key generation step, then to the key delivery step. This protocol is similar to banking protocols for personal verification to generate accounts or some cards like visa cards, because it is the most secure and safe way to exchange information with customer, in the voting scheme we reflect that to voter. Figure 6, shows all registration phase steps in the registration center, the first four steps describe the personal verification and 5th step describes keys generation, 6th and

7th steps describe keys delivery. After registration the voter records are saved and voter have credential to vote when the voting process begin.

### 3.2.1. Preparation Requirements

1. Registration Rules for the country to be consider as requirements to built the system
2. Registration centers in Secure environments
3. Voting centers for thus cannot using internet
4. Internal registration centers for local citizens.
5. External registration centers for those who are away of country and who can not come to complete the registration, but can vote over Internet. Then they can go to embassy that contains registration center and complete the registration phase. These centers to ensure accessibility for all.
6. Database contains all information about any citizen, such as name, photo, location, date of birth to calculate age, etc ….
7. Databases to save all registered voters and keys. It contains additional fields to indicate whether the voter has voted or not yet.
8. Databases for candidates to save all candidates related information.

Figure 3.5 shows the registration process

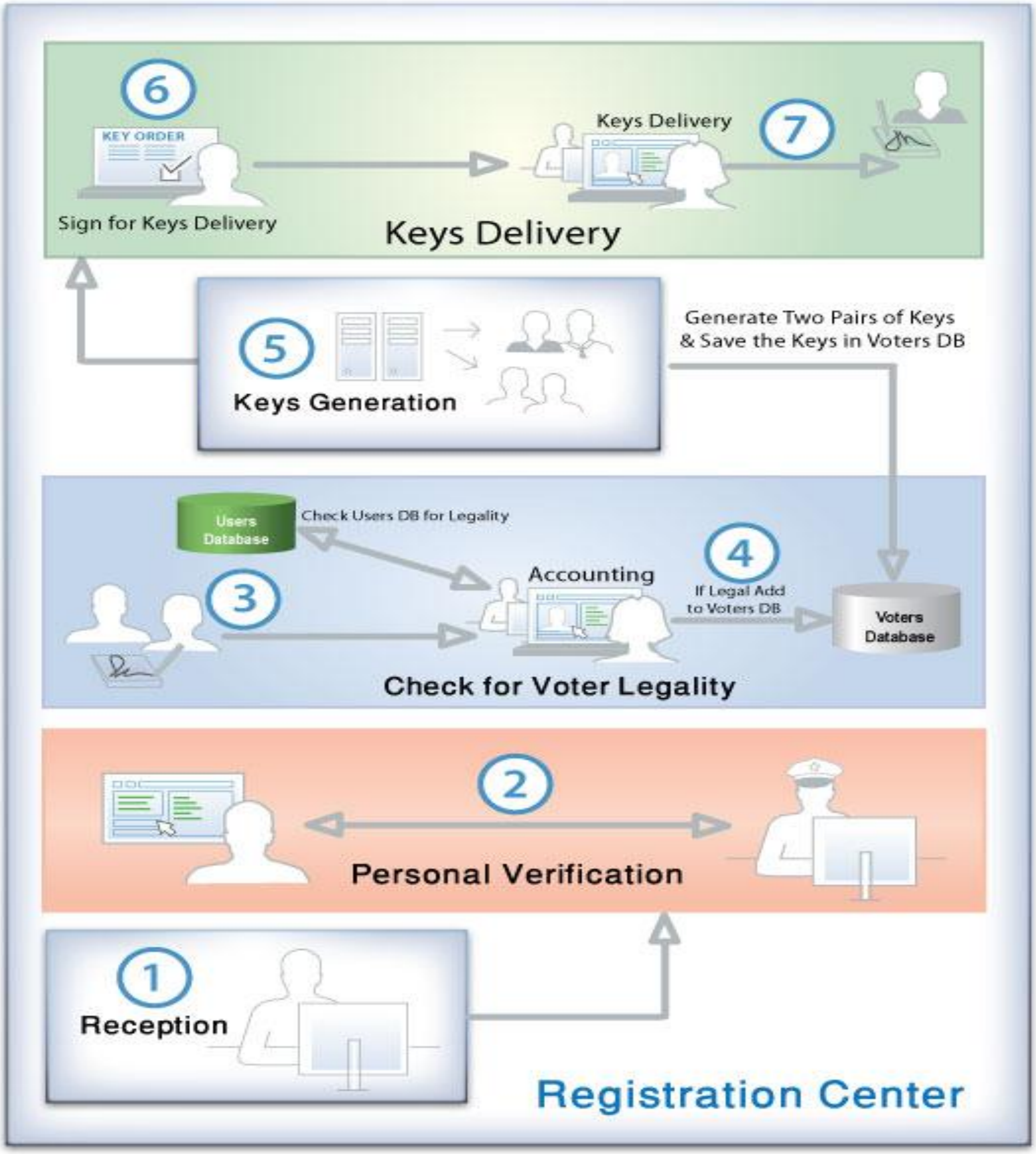


**Figure 3-5: Registration Process**

### 3.2.2. Personal Verification

Personal verification is first step in registration process to verify voter personality and legality. Personality: who is voter? Legality: is voter fulfilling all voting conditions to be able to enter in the voting process? The aim of personal verification is to ensure voter authentication before any action is done, because we need protocols to achieve good verification schemes before continuing in registration phase and advancing to the next steps.

### Voting preperation Steps

1. Voter goes to registration center and brings his probative papers like identity card and passport and family book.
2. Center employees ensure the physically voter identity.
3. Check the voter legality by checking the citizens (personal) database
4. If the voter is legal then continue
5. Add the voter as new entry in voters database

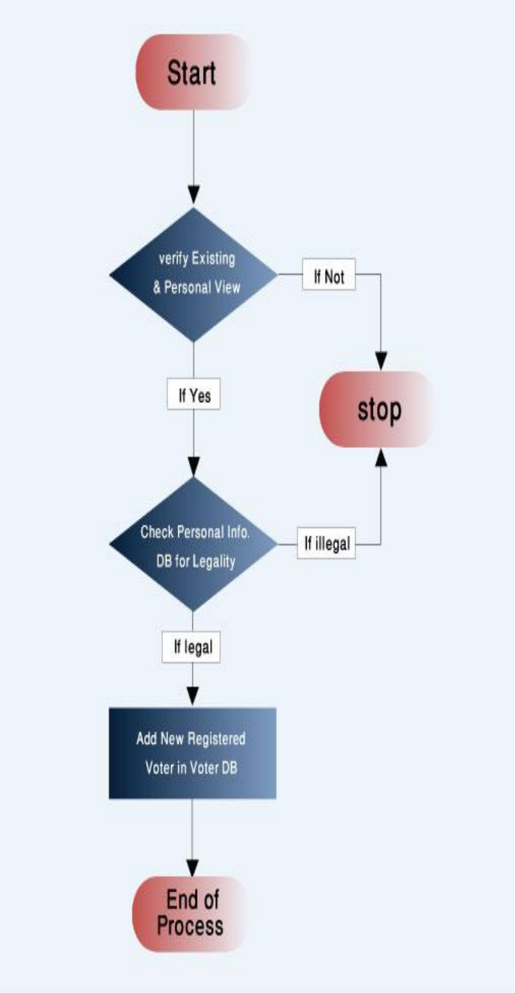

Start
verify Existing & Personal View
If Not
stop
If Yes
Check Personal Info. DB for Legality
If illegal
If legal
Add New Registered Voter in Voter DB
End of Process

Figure 3-6: Personal Verification

Figure 3.6 shows the process of the personal verification.

### 3.2.3. Keys Generation

In any encryption scheme keys are the main part of the process.

**Public key cryptography**

Also known as asymmetric cryptography is a form of cryptography in which a user has a pair of cryptography keys a public key and a private key. The private key is kept secret, while the public key may be widely distributed. The keys are related mathematically, but the private key cannot be practically derived from the public key. A message encrypted with the public key can be decrypted only with the corresponding private key.

**Key Generation Algorithm**

Before the application of the public key cryptosystem, each voter must generate two pairs of keys. This involves the following steps

**Primes Generation**

This thesis tries to generate two prime numbers using Gordon Algorithm. The RSA cryptosystem uses a modulus of the form $n = p * q$ where $p$ and $q$ are distinct odd primes. The primes $p$ and $q$ must be of sufficient size that factorizing of their product is beyond computational reach. Moreover, they should be random primes in a way that they will be chosen as a function of a random input through a process defining a pool of candidates of sufficient cardinality, which makes an exhaustive attack infeasible. In practice, the resulting primes must also be of a pre-determined bit length, to meet system specifications. The discovery of the RSA cryptosystem led to the consideration of several additional constraints on the choice of *p* and *q* which are necessary to ensure the resulting RSA system safe from cryptanalytic attack [4].

The steps of the Gordon Algorithm:

1. Generate two large random primes *s* and *t* of roughly equal bit length
2. Select an integer $i_0$. Find the first prime in the sequence $2*i*t+1, \mathit{for}\cdot i=i_0;i_0+1;i_0+2;$ denote this prime by $r=2*i*t+1$.
3. Compute $p_0=2\left(s^{r-2} \bmod r\right)*s-1$
4. Select an integer $j_0$. Find the first prime in the sequence $p_0+2*j*t+1, \mathit{for}\cdot j=j_0;j_0+1;j_0+2;$ denote this prime by $p=p_0+2*j*r*s$
5. Return (*p*). As prime.

**Example:** generate prime number using Gordon’s algorithm

$s=37, t=41$

$i=6$

**Enter first loop**

$r = 2*6*41+1 = 493$ not prime

$i = 6 + 1 = 7$

$r = (2 * 7 * 41) + 1 = 575$ not prime

$i = 7 + 1 = 8$

$r = (2 * 8 * 41) + 1 = 657$ not prime

$i = 8 + 1 = 9$

$r = (2 * 9 * 41) + 1 = 739$ prime » out of loop

**Out of loop**

$p_0 = 2*\left(37^{739-2} \bmod 739\right)*37 - 1 = 1479$ .

$J = 1;$

**Enter second loop**

$P = 1479 + (2*1*739*37) = 56165$ not prime

……….

$J = 6 + 1 = 7$

$P = 1479 + (2 \times 7 \times 739 \times 37) = 384281$ prime » out of loop

**Out of loop** Return **384281** as Prime

The primes *s* and *t* required in step 1 can be probable primes generated by algorithm the Miller-Rabin test [4], can be used to test each candidate for primeality in steps 2 and 4, after ruling out candidates that are divisible by a small prime less than some bound *β* since the Miller-Rabin test is a probabilistic primeality test the output of this implementation of Gordon algorithm is a probable prime [4].

**RSA keys Generation**

RSA scheme based on public and private keys, the key generations are as following:

Given two prime numbers *p* and *q*, to compute the modulus n, such that $n = p \times q$ and *Ø(n)* where *Ø(n)* is function get the number of the positive integers less than *n* and relatively prime to *n*, then $Ø(n) = (p-1)(q-1)$ the use the previous notations to solve the following relationship (e∗d mod *Ø(n)* = 1) Where *e* and *d* is public and private keys which needs to calculate. That is, *e* and *d* are multiplicative inverse mod *Ø(n)*. Note that, *d* and therefore *e* is relatively prime to *Ø(n)*. The following algorithm shows how to calculate RSA keys.

**RSA keys generations**

Select two large random primes, $p$ and $q$, of approximately equal size such that their product $n = pq$.

Calculate $n = pq$ and $Ø(n) = (p-1)(q-1)$.

Select an integer $e$, gcd $(e, Ø(n)) = 1$

Calculate the secret exponent $d$, since $(e\ d)$ mod $Ø(n) = 1$

The public key is $(n, e)$ and the private key is $(n, d)$. The values of $p$, $q$, and phi should also be kept secret.

$n$ is known as the *modulus*.

$e$ is known as the *public exponent* or *encryption exponent*.

$d$ is known as the *secret exponent* or *decryption exponent*.

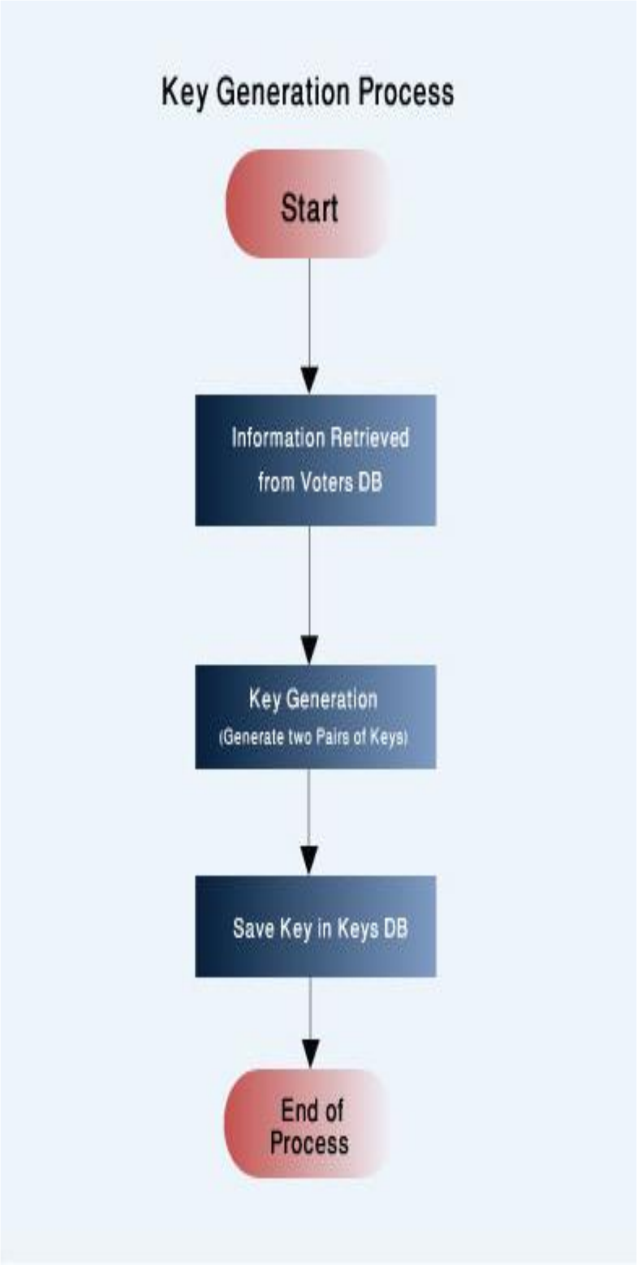


**Figure 3-7: keys generations**

**Example: keys generation**

Select two prime numbers

$P = 17$, $q= 11$

Calculate $n = p*q = 17*11 = 187$

Calculate $\emptyset(n) = (p-1)\ (q-1) = 16*10 = 160$

Calculate $e$ such that $e$ is relatively prime to $\emptyset(n) = 160$ and less than $\emptyset(n);$

we choose $e = 7$.

Calculate $d$ such that $d*e \bmod \emptyset(n) = 1$ and $d<160$. The correct value is $d= 23$. Because $23*7 = 161 = 10*160+1$.

Then resulting keys are public key *(7,187)* and private key *(23,187)*.

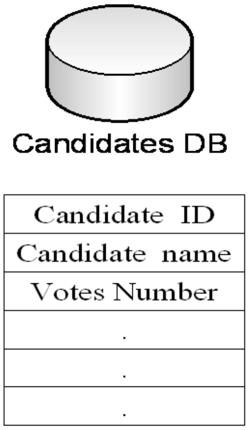
This process must worked two times one for the server side and one for the client side (voter) for each user to generate two keys one as private and the second as the public. Figure 8 shows the keys generation process.

### 3.2.4. Keys Delivery

Credential information is issued manually directly and delivered to the voter by hand in envelope like banks and confirmed by the voter. More positively, and safe to deliver credentials by hand to avoid any conflicting or a impersonation by hacking any personal information, and prevent any illegal registration to make overall process in safe side.

### 3.2.5. Candidate Registrations

Candidates can register simply by adding a new candidate record in candidate databases Figure 3.8 shows the records in candidate databases.



| |
|---|
| Candidate ID |
| Candidate name |
| Votes Number |
| . |
| . |
| . |

**Figure 3-8: Candidate Database**

## 3.3.Voting

Voting protocols are built based on cryptography techniques. The reader is presumed to have a basic understanding of public key cryptosystems. More information about public key cryptography is provided in appendix (A).

### 3.3.1. Digital Signatures

**Authentications:**

Vote authentication is concerned with:

- Protecting the integrity of a message
- Validating identity of originator
- Non-repudiation of origin (dispute resolution)

An authenticator, signature, or message authentication code is sent along with the message. The signature is generated via some algorithm which depends on both the message and some public or private key known only to the sender and receiver. Figure 3.9 shows the digital signature process

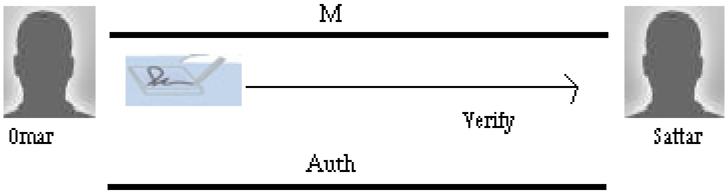


**Figure 3-9: Digital signatures**

## Public key signature schemes

1. The private-key signs the vote creates signatures, and the public-key verifies signatures.
2. Only the owner of the private-key can create the digital signature, hence it can be used to verify who created a message.
3. Any entity knowing the public key can verify the signature.
4. Digital signatures can provide non-repudiation of message origin, since an asymmetric algorithm is used in their creation, provided suitable timestamps and redundancies are incorporated in the signature.

## RSA Key Signature

1. RSA encryption and decryption are commutative; hence it may be used directly as a digital signature scheme
2. To **sign** a message *m* compute:

$s = m^d(\text{mod } r)$ : *s,r,m,d RSA Argument where m is the vote , s is the encrypted vote , r is the modules and d is the private key*

3. To **verify** a signature compute:

$m = s^e(\text{mod } r) = m^{e.d}(\text{mod } r) = m(\text{mod } r)$

4. Thus know the message was signed by the owner of the public-key

Digital Signatures is a type of asymmetric cryptography used to simulate the security properties of a handwritten signature on paper. Digital signature schemes normally give two algorithms, one for signing which involves the user private key, and one for verifying signatures which involves the user public key. The output of the signature process is called the digital signature [45].

The suggested e-voting scheme we deploy digital signatures using the RSA public key cryptography systems which work as follows. Given public key *(e,n)*, private key *(d,n)* , and modulus of *n* signs an object *m* by encrypting it with signer private key.

$s = m^d \text{ mod } n$

Note: The signer is the only person who knows the private key, signer is the only person who can create the signature. *s* for this object *m* and object here means vote. Anyone can verify that *s* is indeed his/her signature of *m* by encrypting *s* with signer public key.

$m = s^e \bmod n = (m^d)^e \bmod n = m^{de} \bmod n = m \bmod n$

### 3.3.2. Handshakes

The handshake is initiated when the two human hands touch, immediately. It is commonly done upon meeting or completing an agreement as voting process. It purpose to convey trust, balance and equality. Shaking with the right hand while delivering a secure object with the left [45].

- The proposed scheme deployed handshakes using custom protocol simply as following
- The client computer chooses random number $\alpha$ after that select a random number $r_1$
- Calculate $\alpha^{r_1}$
- Send $\alpha^{r_1}$ to the server
- The server chooses a random challenge $r_2$ and then finds the $(\alpha^{r_1})^{r_2}$
- Send $(\alpha^{r_1})^{r_2}$ to client
- Client calculate $r_2$ based in his values $\alpha, r_1$ $\sqrt[r_2]{x} = \alpha^{r_1}$ assume *x* the number which received from sever. Example: $\alpha = 5, r_1 = 3, r_2, x = 2373046875$

$\sqrt[r_2]{2373046875} = 75 \Rightarrow r_2 = 5$

- Client send $r_2$ to the server
- server check if $r_2$ which calculated in client side = $r_2$ (server) if note discard the operation if yes complete the operation

### 3.3.3. Voting

Voting process is the core protocol of the voting scheme which consists of two steps. The first step is the login and the second step is the polling. The two steps are strongly related to the registration phase based on using the keys which generated specially in the voting step. We will use digital signature and handshake protocols in specific way in the next sections. Figure 3.10 show the double encryption idea

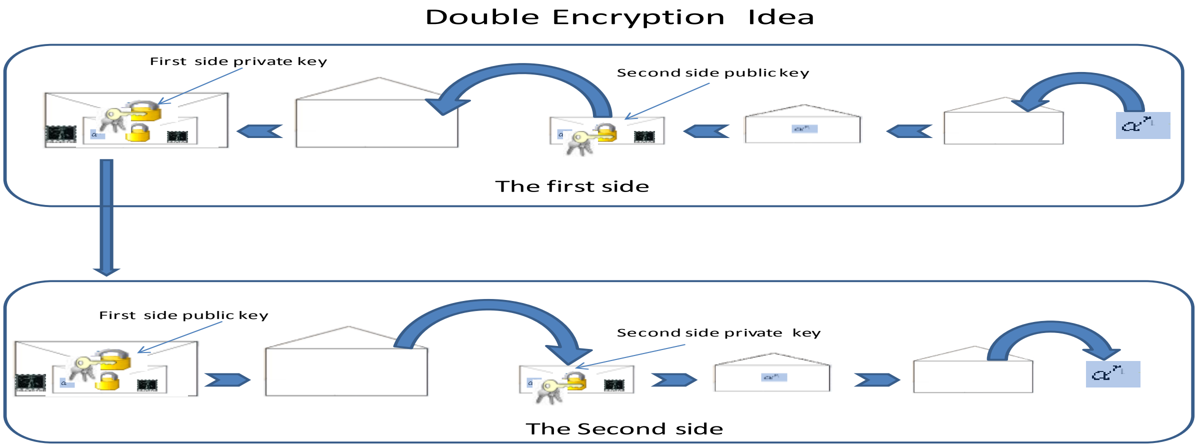


**Figure 3-10: double encryption idea**

### Voting Protocol

In this phase the legal voter have to follow the following steps to be able to enter to the voting step logging (security). The method to authorize a user to obtains access on a desired server or computer, voting protocol consisting of two stages processing in cross way

5. Handshake stage to be sure the client is valid
6. Voting stage overlapping with handshake  stage

The following procedure represent voting protocol

1. Client send request to the server to vote
2. Server respond in sending login page to client
3. Client receives the page and do the following automatically after the client enter the username and his private key  in login fields  and press submit

User name

Password Private Key

- The client computer chooses a random number $\alpha$ . and select a random number challenge $r_1$
- Calculate $\alpha^{r_1}$
- Encrypt the $\alpha^{r_1}$ using voter private key *z* to generate $e_1$ then encrypt $e_1$+(user name) using Server public key *x* to generate $e_2$
- Send $e_2$ to the server

4. The server receives $e_2$ from the voter and do the following:

- Decrypt $e_2$ using server private key $y$ to extract $e_1$ + user name
- check database if the voter vote or not to prevent occurring double voting once he\she have not voted yet continue else stop the process and send message to the voter about that
- Fetch the second user key $w$ from server database
- Then decrypt $e_1$ using voter public key *w* to extract $\alpha^{r_1}$ .
- The server chooses a random challenge $r_2$ and then finds the key $es_2$= $(\alpha^{r_1})^{r_2}$
- Send $es_2$ to client after encrypt it using *w* and *y* respectively

5. Client receives $es_2$ and do the following

- decrypt $es_2$ using $x$ and $z$ respectively to extract $(\alpha^{r_1})^{r_2}$
- Calculate $r_2$
- Repeat step three but encrypt ($r_2$ + vote ) by $z$ and $x$ respectively and send it to the server

6. Server receives encrypted $r_2$ + vote and do the following
    - Decrypt to extract $r_2$ +vote
    - Check if $r_2$ from client equals the original $r_2$ if yes then add the vote to the votes and update user database to be sure he\she cannot vote another time else discard the vote. Figure 3.12 shows the process.

### 3.3.4. Vote Processing

Voting process provides a pure vote contains information regarding candidates and the voter system will bring this information to processing the processing of votes is undertaken during the voting period and the details are kept in a secure database.

**System configuration topology**

The system consists of the following main components

Voting Server: Provides remotely-hosted interactive services which host the voting protocol. Figure 3.11 shows the voting

server

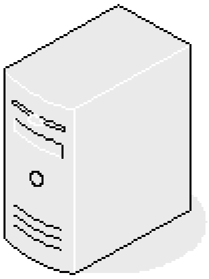
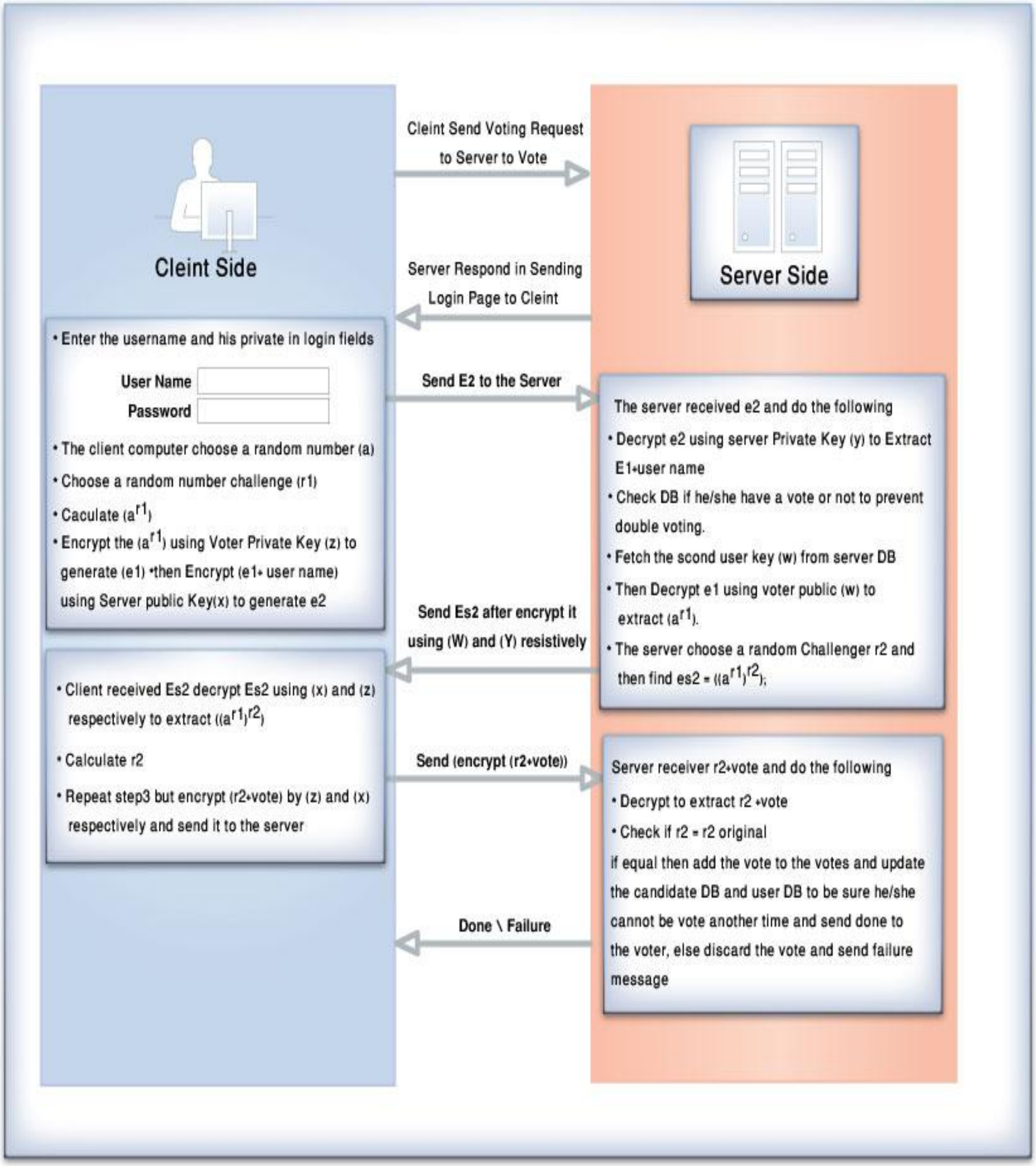


**Figure 3-11: voting server**



Cleint Send Voting Request to Server to Vote

Server Respond in Sending Login Page to Cleint

- Enter the username and his private in login fields
- The client computer choose a random number (a)
- Choose a random number challenge (r1)
- Caculate $(a^{r1})$
- Encrypt the $(a^{r1})$ using Voter Private Key (z) to generate (e1) •then Encrypt (e1+ user name) using Server public Key(x) to generate e2

Send E2 to the Server

The server received e2 and do the following

- Decrypt e2 using server Private Key (y) to Extract E1+user name
- Check DB if he/she have a vote or not to prevent double voting.
- Fetch the scond user key (w) from server DB
- Then Decrypt e1 using voter public (w) to extract $(a^{r1})$.
- The server choose a random Challenger r2 and then find es2 = $((a^{r1})^{r2})$;

Send Es2 after encrypt it using (W) and (Y) resistively

- Client received Es2 decrypt Es2 using (x) and (z) respectively to extract $((a^{r1})^{r2})$
- Calculate r2
- Repeat step3 but encrypt (r2+vote) by (z) and (x) respectively and send it to the server

Send (encrypt (r2+vote))

Server receiver r2+vote and do the following

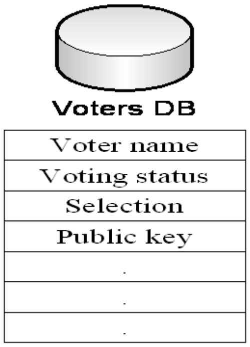
- Decrypt to extract r2 +vote
- Check if r2 = r2 original

if equal then add the vote to the votes and update the candidate DB and user DB to be sure he/she cannot be vote another time and send done to the voter, else discard the vote and send failure message

Done \ Failure

**Figure 3-12: Voting Process**

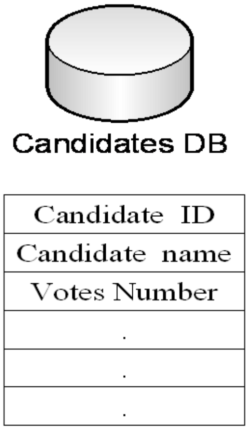
Voters Database: Provide database which contains all registered voters connected to the voting server. Figure 3.13 shows the voters database



| |
|---|
| Voter name |
| Voting status |
| Selection |
| Public key |
| . |
| . |
| . |

**Figure 3-13: Voters Database**

Candidate database: provides Database which contains all the registered candidates connected to voting server. Figure 3.14 shows the candidate database.



| |
|---|
| Candidate ID |
| Candidate name |
| Votes Number |
| . |
| . |
| . |

**Figure 3-14:** Candidate Database

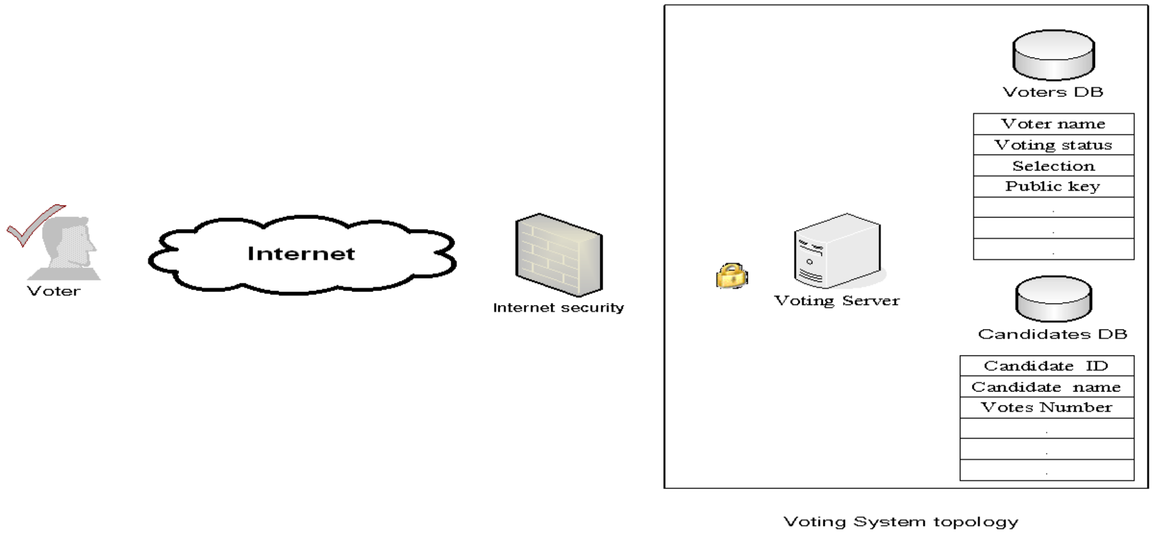


**Figure 3-15:** Voting System architecture

After voting process complete the vote will be processed as following

1. Take the vote and add it on the voters database and change voting status to prevent double voting and add the candidate ID in the selection field to be used later on the verification in the counting phase
2. increment votes number on the candidate database regarding the voter which was selected on the vote

### 3.3.5. Example

The voter side has two keys calculated as follows

Select two prime numbers $p = 19, q = 31$

Calculate $n = p * q = 19 * 31 = 589$

Calculate $\phi(n) = (p-1)(q-1) = 30 * 18 = 540$

Select integer *w* where $\gcd(\phi(n), w) = 1;\ 1 < w < \phi(n) :\Rightarrow w = 7$

Calculate integer *z* where $z \equiv w^{-1} \bmod \phi(n) \equiv 7^{-1} \bmod 540 \Rightarrow z = 463$

Public key $\Rightarrow$ {*w*,*n*} = {7,589}

Private key $\Rightarrow$ {*z*,*n*} = {463,589}

**The server side has two keys calculated as follows**

Select two prime numbers $p = 23, q = 37$

Calculate $n = p * q = 23 * 37 = 851$

Calculate $\phi(n) = (p-1)(q-1) = 36 * 22 = 792$

Select integer *x* where $\gcd(\phi(n), x) = 1;\ 1 < x < \phi(n) \Rightarrow x = 5$

Calculate integer *y where* $y \equiv x^{-1} \bmod \phi(n) \equiv 5^{-1} \bmod 792 \Rightarrow y = 317$

Public key $\Rightarrow$ {*x*,*n*} = {5, 851}

Private key $\Rightarrow$ $\{y,n\} = \{317,851\}$

**Steps**

Client send request to the server to vote via HTTP protocol.

Server respond send login page to client also via HTTP protocol.

Voting protocolenter user name and the private key as password in login fields

User name □

Password □

The client computer chooses a random numbers $\alpha = 5, r_1 = 3$

Calculate $\alpha^{r_1} = 5^3 = 75$

Encrypt the $\alpha^{r_1}$ using voter private key $z = 463$ to generate ($e_1$)

$e_1 = 75^{463} \bmod 589 = 569$ we can solve this equation using fast exponentiations algorithm. [4]

Encrypt $e_1$ using server public key $x = 5$ to generate $e_2$

$e_2 = 569^5 \bmod 851 = 251$

Send $e_2$ to the server

The server received $e_2$ from the voter and do the following:

Decrypt $e_2$ using server private key $y = 317$

$e_1 = 251^{317} \bmod 851 = 569$

Decrypt $e_1$ using voter public key $w$=7 to extract $\alpha^{r_1}$.

$$\alpha^{r_1} = 569^7 \bmod 589 = 75$$

The server chooses a random challenge $r_2 = 5$ and then finds the key

$(\alpha^{r_1})^{r_2} = 75^5 = 2373046875$

Send 2373046875 to the client

Client received 2373046875 and do the following equation to find $r_2$

$\sqrt[r2]{2373046875} = 75 \Rightarrow r_2 = 5$

Assume the voter vote 4

concatenation of 5 with 4 to be (54)

Encrypt the (54) using voter private key $z = 463$ to generate $e_1$

$e_1 = 54^{463} \bmod 589 = 480$

Encrypt $e_1$ using server public key $x$ = 5 to generate $e_2$

$e_2 = 480^{5} \bmod 851 = 332$

Send $e_2$ to the server

The server received $e_2$ from the voter and do the following:

Decrypt $e_2$ using server private key $y$ = 317

$e_1 = 332^{317} \bmod 851 = 480$

Decrypt $e_1$ using voter public key $w$ = **7** to extract the vote.

$480^{7} \bmod 589 = 54$

($r_2$ concatenate vote) = 54 $r_2$= 5, vote = 4

Check if ( ($r_2$ original = 5 ) = ($r_2$ received = 5) )original add vote to the votes else discard the vote

The system goes to the voter database and change the vote flags to sure the voter cannot vote twice, and then add this vote in the corresponding field.

The system adds the vote to the corresponding candidate database and increment the vote’s number field value by one.

The system send message to the voter to tell him that the process end successfully.

### 3.4. Counting and Auditing

The vote counting system deals with the counting of votes, which requires accuracy, speed and security. Vote counting is one of the most crucial stages in the voting scheme. To complete the count and transfer results in a quick, transparent and accurate manner which can defect public confidence in the voting and will directly affect whether candidates and political parties accept the final results.

Counting system consists of two steps. The first phase is the counting phase which is done in parallel with voting phase when we save the votes the voting counters works at same time to increment the vote numbers for each candidate vote by vote and the second step is the auditing step is worked after finish the voting phase this process to ensure that all voting process is done in efficient manner and recount the votes in other ways to ensure compatibility of results.

### 3.4.1. Counting

The counting of votes takes place in the vote scheme, separated from the web application. At the same time the voting system must be able to use a local database with candidate lists. There exist various methods through which the ballots cast at an election may be counted, prior to applying a voting scheme to obtain one or more winners in a fair way.

In the proposed scheme counting step done on two separate data bases one regarding candidates and one regarding voters each one of these data bases independent to be sure no one can hack two sources at the same time. The aim of this procedure is to help us on auditing step.

**Counting Protocol**

Once the vote is coming it will be processed as following:

1. access voters data bases by modifying the vote field by put the candidate ID
2. access voters data bases by modifying the vote status field to prevent double voting
3. Access candidates data bases by increment votes counter field for candidate
4. Return success

**Example:** Assume we have candidate number 4 have 500 vote in his counter and the coming vote contains number 4 the system will register this vote in the voter record in the voters database then the system will increment the votes field number by one in the candidates database to be 501. Figure 3.16 shows the counting process.

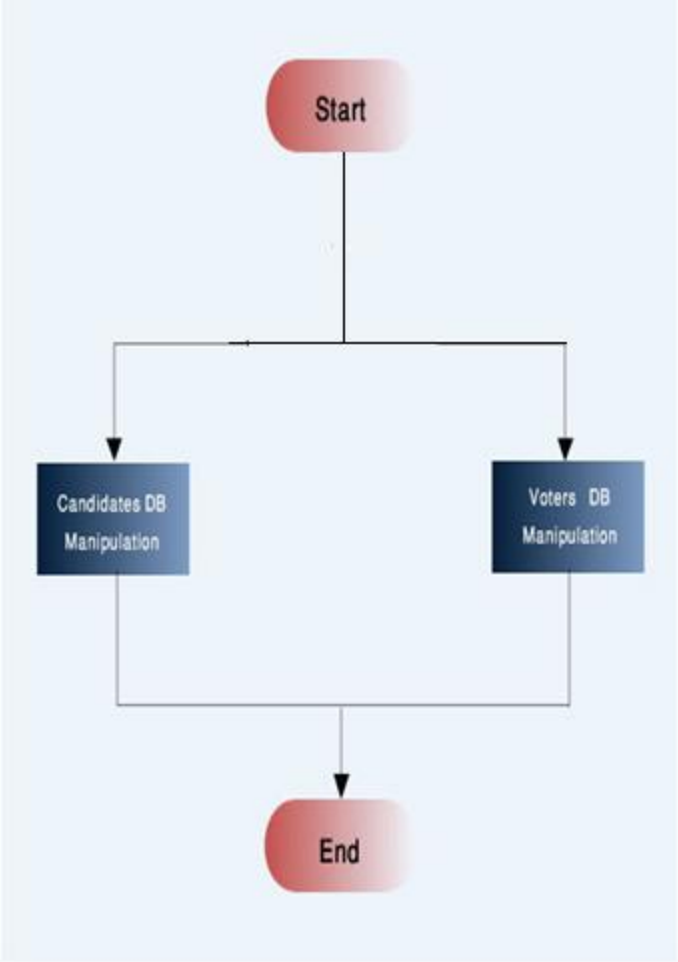


**Figure 3-16: Counting**

### 3.4.2. Audit

Just as the case with manual voting scheme, e-voting scheme have able to be audited, that mean it must be possible to examine the processes used to collect, count the votes and re-count the votes in order to confirm the accuracy of the results. The greatest danger to e-voting scheme is if external interference on scheme is possible and can go undetected affecting the results of the voting. This is why independent and extensive security monitoring, auditing, cross-checking and reporting needs to be a critical part of e-voting scheme.

There are different mechanisms to audit an e-voting scheme. Certain systems include a voter verified audit trail (VVAT), also known as voter verified paper ballots. This scheme includes paper records of the vote, which have been verified by the voter at the time of casting the vote and can be used for a recount at a later date. VVAT can only be used in non-remote e-voting scheme; since the voter has to be physically present at the place where his/her vote is actually recorded and printed for control [50].

Other e-voting scheme includes a voter verifiable audit trail. The difference between the first scheme and the second one is that in the first case, it is mandatory that the voters check their vote before they cast it in the second case voters may check their vote but they do not have to.

In some scheme, the ballots are printed only after they have been cast and are stored in a closed area. These ballots can also be used for a recount. But it is noted that the voters did not verify these printed ballots.

Whichever approach to auditing is chosen, it is crucial that the e-voting scheme has audit facilities for each of the main steps of the voting operation voting, counting. The audit system should also provide the ability for independent observers to monitor the election or referendum without revealing the potential final count/result. The audit system has able to detect voter fraud and provide proof that all counted votes are authentic. Audit systems is there by nature, gather a lot of information. However, if large information is kept, the secrecy of the vote may be compromised. A voting audit system should maintain voter anonymity and secrecy at all times. In all cases the information gathered by the audit system must protected against unauthorized access

# 4. CHAPTER FOUR: Scheme Analysis

## 4.1.Analysis

The design of a “good” voting system, whether electronic or using traditional paper ballots or, must satisfy a number of properties

Eligibility: In any voting scheme, only valid voters who meet certain pre-determined criterion are eligible to vote. Ability to verify voter’s validity and a mechanism to ensure that each entity can cast permitted number of votes is a must for a voting scheme. Privacy: In a secret ballot, a vote must not identify a voter and any traceability between the voter and its vote must be removed. Maximal privacy is achieved by a voting scheme, if the privacy of a voter is breached only with a collusion of all remaining entities (voters and authorities). Eligibility and privacy the scheme only satisfies eligibility, privacy and individual verifiability properties by Computational privacy (equivalent to breaking RSA) is provided against any external adversary properties are satisfied only the eligible and authorized voter can be vote that is fulfilled by using login procedure by entrance user name and password that is a private key and all votes are secreting by encrypting each vote, but more importantly fairness, accuracy, and universal verifiability properties are also achieved also by encrypting each vote.

Verifiability: A voter should be able to verify if its vote was correctly recorded and accounted for in the final vote tally. There are two flavors of this requirement. One is the individual verifiability where only the voter can verify its vote in the tally. The second is universal verifiability where after the tally is published, anyone can verify that all valid votes were included, and the tally process was accurate. Universal verifiability is more practical since assuming voters to verify their votes individually is not realistic. Verifiability requirement needs voter to be linked to vote, and hence is in contradiction to privacy. However, this requirement is crucial in gaining trust of the voter in the voting system. The Data sources which contain all votes provide the publicly accessible bulletin board provides universal verifiability property and individual verifiability property.

Accuracy: Voting schemes must be error-free. The votes must be correctly recorded and tallied. Votes of invalid voters should not be counted in the tally. Universal verifiability property is directly related to accuracy. Hence the scheme also satisfies accuracy. The existing of two data sources voters and candidates databases we can do the double count of the votes from two sources and check the results that is guarantee a high accuracy.

Fairness: In order to conduct an impartial election, no one should be able to compute the partial tally as the election progresses.  We can guarantee the individual variability from the voter's database and guarantee the public variability from the candidate's database.

Robustness: A scheme has to be robust against active or passive attacks (corrupt authorities/voters) as well as faults (non-participating authority/voters). A voting scheme achieving maximum robustness in the presence of corrupt authorities requires a collusion of all authorities to disrupt the election. But this also necessitates all the authorities to participate in conducting the election. Any non-participating authority can also disrupt the election, leading to zero robustness to faults.

Receipt-freeness: A voter should not be provided with a receipt with which it may be able to prove vote to any other entity. Receipt-freeness has the same notion of intractability or privacy.

Fairness and robustness are achieved. Receipt-freeness property is satisfied by encrypting each vote. Scalability: The complexity of the protocols used in a voting scheme, is a major factor in its practical implementation. An efficient voting scheme has to be scalable with respect to storage, computation, and communication needs as a fraction of the number of voters the proposed scheme achieve that because we can add resources as much as we need just plug-ins without high integration customization.

## 4.2.Comparisons

Table 4.1 shows comparison results contains many systems new and old that compared with General  properties and this comparison and the criteria take from Krishna Sampigethaya, Radha Poovendran “A framework and taxonomy for comparison of electronic voting schemes” [25].

Table 4.1: Comparison of schemes based on general security properties

| Scheme | Eligibility | Privacy | Verifiable | Accuracy | Fair | Robust | Receipt-free | Scalable | Practical |
|---|---|---|---|---|---|---|---|---|---|
| Chaum, 1981 | ✓ | Com | LND | X | X | X | X | X | X |
| Chaum, 1988a | ✓ | Com\Max | LND | X | X | X | X | X | X |
| Boyd, 1990 | ✓ | Com\Max | LND | X | X | X | X | X | X |
| Sako and Killian, 1995 | ✓ | Com | ✓ | X | C | X | ✓ | X | X |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| Chaum, 2004 | ✓ | Com | LND\CU | C | C | C | ✓ | ✓ | C |
| Cohen and Fischer, 1985 | ✓ | Com | ✓ | ✓ | X | X | X | X | X |
| Cohen and Yung, 1986 | ✓ | Com | ✓ | ✓ | C | X | X | X | X |
| Benaloh, 1987 | ✓ | Com | ✓ | ✓ | C | C | X | X | ✓ |
| Iverson, 1992 | ✓ | Com | LND | C | C | X | X | X | C |
| Sako and Killian, 1994 | ✓ | Com | ✓ | ✓ | C | X | X | X | ✓ |
| Cramer et al., 1996 | ✓ | Com | ✓ | ✓ | C | C | X | X | ✓ |
| Cramer et al., 1997 | ✓ | Com | ✓ | ✓ | C | C | X | C | C |
| Schoenmakers, 1999 | ✓ | Com | ✓ | ✓ | C | C | X | X | ✓ |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| Hirt and Sako, 2000 | ✓ | Com | ✓ | ✓ | C | C | ✓ | X | C |
| Baudron et al., 2001 | ✓ | Com | ✓ | ✓ | C | C | ✓ | C | C |
| Lee and Kim, 2002 | ✓ | Com | ✓ | ✓ | C | C | ✓ | ✓ | X |
| Kiayias and Yung, 2002 | ✓ | Com\Max | ✓ | ✓ | C | X | X | X | |
| Damga°rd and Jurik, 2001 | ✓ | Com | ✓ | ✓ | C | C | ✓ | C | C |
| Fujioka et al., 1993 | ✓ | Com | LND | X | C | X | X | ✓ | X |
| Baraani-Dastjerdi 1995 | ✓ | Com | LND | C | ✓ | C | X | X | ✓ |
| Okamoto, 1997 C | ✓ | Com | LND | X | ✓ | C | ✓ | X | X |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| Juang et al., 2002 | ✓ | Com | LND | C | C | C | X | ✓ | ✓ |
| Golle et al., 2002 | ✓ | Com | LND\CU | C | C | C | X | C | ✓ |
| Lee et al., 2003 | ✓ | Com | ✓ | ✓ | C | C | ✓ | C | X |
| Kiayias and Yung, 2004 | ✓ | Com | ✓ | ✓ | C | C | ✓ | C | C |
| Juels and Jakobsson, 2002 | ✓ | Com | LND | C | C | C | ✓ | X | X |
| Acquisti, 2004 | ✓ | Com | LND | C | C | C | ✓ | X | X |
| The propose Scheme 2008 | ✓ | Com\Max | ✓ | ✓ | ✓ | C | ✓ | ✓ | ✓ |

✓: Satisfied **X**: not satisfied **C**: conditionally satisfied **Com**: conditionally privacy

**Max**: maximal privacy **Ind**: individually verifiable **CU**: conditionally universally verifiable.

# 5. CHAPTER FIVE: Conclusions and future work

## 5.1.Conclusions

Current technological evolutions have changed the way we live, interact, communicate, etc. the modern techniques offer a new ground to architecture to take up expressing current knowledge and visualize data and information over Internet. The technological evolutions in accordance with the modern techniques can be applied by governance in order to access the ideal of direct democracy.

The e-voting scheme described provided that sufficient scheme, support democracy process through Internet, a basis for conducting e-voting at least as securely as traditional voting.

In this thesis we have introduce e-voting scheme consists of three phases, the first one is the registration phase that focus on how the citizen can be register in the scheme with highly level of security. In this phase we assure many of security properties such as transparency, confidentiality, trust, availability and privacy.

The second phase is the voting phase it is mainly consist of two protocols working parallel in cross way. We manly use in this phase public key cryptography techniques as double voting plus using handshake protocol at same time. In this phase we assure many of security properties such as eligibility, privacy, receipt-freeness, fairness, individual verifiability, reliability, convenience, flexibility and mobility.

The third phase is the counting phase it consists of two steps counting and auditing, that working to count and auditing the votes for each candidate. In this phase we assure many of security properties such as accuracy, transparency, universal verifiability and fairness.

This thesis describes a complete design scheme, and evaluation of a provably secure remote e-voting system. Based on our knowledge, this has not been done before. That provides stronger security than previously implemented voting systems. It is secure against a stronger adversary, which can corrupt most of the system and can try to coerce voters. The results show the cost, tabulation time, and security can be practical for real-world elections. This scheme is based on a homomorphic based schemes known voting scheme, but the development of a secure, scalable implementation led to new technical advances: a secure registration protocol and a scalable vote storage system. This scheme contributes to both the theory and practice of electronic voting. The many cryptographic protocols required to implement the proposed scheme (and other secure voting systems) are distributed throughout the literature, where they are described at various levels of abstraction. In a concrete form that other system builders could use.

Perhaps the most important contribution of this work is strong evidence that, contrary to conventional wisdom, secure electronic voting is possible and even feasible. We are optimistic about the future of voting systems constructed, like our work, using principled techniques.

### 5.2.Future Works

The results in this thesis also provide a strong foundation to continue for future work to build very will e-voting schemes over the entire world. One area of future work is in combining the knowledge gained about voting methodologies and online registration schemes to build online registration scheme as first step. Another area is in applying the results studied here to the many real-world situations in which needs voting schemes.

Different solutions, which could be simplified if such a standard would be employed. With one common platform, it would be easier to concentrate efforts on developing and finding problems in e-voting schemes.

There is still a vast field of research on Internet voting, which is at its first stages. Currently there are very few trials in this area, so most of the research so far presented need to be tested in a real environment.

Another area is to apply some research to make all government operations in one consistent scheme that including the voting scheme, to reach fully e-government at the end.

And we have some issues need to be developed like trustees and observers. As an Internet-based voting system, is susceptible to a number of vulnerabilities and attacks like replay attack. We will consider these vulnerabilities along with possible solutions which will be implemented in future versions of our work scheme.

E-Voter verifiability. Currently, our system does not offer to a voter a method for physically verifying that his published encrypted ballot encrypts his actual choice. Instead, the voter relies on the correctness of the client software for this task. We note that dealing with this is a complex problem, since any method for voter-based verifiability can also potentially used by the voter to prove how he voted and thus allow for vote buying.

## REFERENCES

**[1]** Aggelos Kiayias Michael Korman , and David Walluck; “An Internet Voting System Supporting User Privacy “, IEEE, ISSN:1063-9527, 0-7695-2716-7 ,pp 165-174,2006.

**[2]** Alexander H “Internet voting in Estonia”, European University Institute, Florence, 31 July 2007.

**[3]** Alexandros Xenakis and. Ann Macintosh,” Procedural Security in Electronic Voting”, Proceedings of the 37th Hawaii International Conference on System Sciences – 2004 IEEE.

**[4]** A-Menezes, P. van Oorschot, and S. Vanstone, “Handbook of Applied Cryptography”, CRC Press ISBN: 0-8493-8523-7, pp.133–168, 1996.

**[5]** Andrew Neff and Jim Adler,”A Verifiable E-Voting Protocol”, University of Maryland, February 3, 2004, Lectures.

**[6]** Avi Rubin AT&T Labs – Research Florham Park, “Security Considerations for Remote Electronic Voting over the Internet”, RXAVI Aug 2001.

**[7]** Avi Rubin, “Security Considerations for Remote Electronic Voting over the Internet”, Addison-Wesley, ISBN 0-201-71114-1, 2001.

**[8]** Ben Adida, “Advances in cryptographic voting systems”, Ph.D. thesis, Massachusetts Institute of Technology, 2006.

**[9]** Benjamin B. Bederson & Paul S. Herrnson, “Usability Review of the Diebold DRE System “, Univ. of Maryland 2003.

**[10]** Brennan Center for Justice, “Studies question e-voting security”, New York University School June 27, 2006.

**[11]** Chou-Chen Yang, Ching-Ying LIN, and Hung-Wen Yang; “Improved Anonymous Security E-Voting Over a Network”, information & security. An international Journal, Vol.15, pp. 181-195, 2004.

**[12]** Committee of Ministers of the Council of Europe on, “LEGAL, OPERATIONAL AND TECHNICAL STANDARDS FOR E-VOTING”, Council of Europe Publishing, 30 September 2004.

**[13]** Craig Burtony, Shanika Karunasekeraz§, and Aaron Harwoodz; “A Distributed Network Architecture for Robust Internet Voting Systems”, Springer LNCS 3591, ISSN 0302-9743, August, 2005.

**[14]** D. Chaum, “Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms”, ACM New York, NY, USA ISSN: 0001-0782, Volume 24, pp. 84 - 90 , February 1981.

**[15]** Guido Schryen, “Security aspects of internet voting”, In Ralph H. Sprague Jr., editor, 37th Hawaii International Conference on System Sciences (HICSS-37 2004), CDROM/

Abstracts Proceedings, Big Island, Hawaii, USA, January 2004. IEEE, IEEE Computer Society.

**[16]** Fujioka, T. Okamoto, and K. Ohta, "A Practical Secret Voting Scheme for Large Scale Elections", IEEE Vol. 718 pp. 244 - 251, March 2004.

**[17]** Geneva electoral committee, "The Geneva Internet voting system", December 16, 2003.

**[18]** Herbert Leitold, "E-Voting in Austria, Overview of technical aspects", Secure Information Technology Center – Austria A-SIT (2004).

**[19]** Howard ," Random Auditing of E-Voting Systems", Vote trust USA National Coalition for election integrity August 16, 2006.

**[20]** International Research center for Information Security, Information and Communications Univ., Korea; "Design and Implementation of Internet Design and Implementation of Internet Voting System to the Worldwide Level Voting System to the Worldwide Level", 2002.

**[21]** J. Benaloh,"Verifiable Secret-Ballot Elections", PhD thesis, Yale University, 1987.

**[22]** Jamie Brown Domari DickinsonCarl Steinebach Jeffrey Zhang, "Secure e-Voting System Project Requirements", Spring 2003.

**[23]** Jason Kitcat ; "e-voting Security Study Response", CESG report 2002.

**[24]** John Borras ,"e–Voting Standards for UK Elections", Office of the e-Envoy Cabinet Office 2004.

**[25]** Krishna Sampigethaya, Radha Poovendrand," A framework and taxonomy for comparison of electronic voting schemes", journal 2006 Department of Electrical Engineering, University of Washington.

**[26]** Lih-Chyau, Bea-Ling Chen, Lih- Woei Chen, "Secure E-Voting System with Collision-Free AID", this research was supported in part by the national science council of the R.O.C under the grant NSC94-2213-E-224-028, 2005.

**[27]** Lorrie Faith Cranor, Ron K. Cytron, "Sensus: A Security-Conscious Electronic Polling System for the Internet", IEEE, ISSN: 1060-3425, Vol 3, pp.561-570, 1997.

**[28]** Michael Clarkson and Andrew Myers, "Coercion-resistant remote voting using decryption mixes", Workshop on Frontiers in Electronic Elections, Milan, Italy, 2005.

**[29]** Michael Hickins ,"Guidelines' Imperil E-Voting Security", StudyFed, June 28, 2006.

**[30]** Michael R. Clarkson Stephen Chong Andrew C. Myers, "Civitas: A Secure Voting System", Cornell University Computing and Information Science, May 2007.

**[31]** Michel Chevallier, Michel Warynski and Alain Sandoz State Chancery, Republic and Canton of Geneva, Switzerland, "Success Factors of Geneva's e-Voting System" ,Electronic Journal of e-Government, Volume 4 , 2006.

**[32]** Naveed Zafar and Anthony Pilkaer, "E-Voting in Pakistan", Masters thesis,ISSN 1653-0187, Lulea ,April 2007.

**[33]** Neil Mitchison, “Trust and security: e-voting as a special case Tallinn”, Research Center, Italy, 19 June 2002.

**[34]** Prof. Alexander H. Trechsel, “Internet voting”, Parliamentary Elections committee in Estonia, March 2007.

**[35]** Robert Krimmer, “Electronic Voting Review and Outlook on Transforming Elections in the Age of the Internet”, TED’06 Conference Mantova, October 24th 2006.

**[36]** Rolf Oppliger; “Addressing the Secure Platform Problem for Remote Internet Voting in Geneva”, Chancellery of the State of Geneva, May 3, 2002.

**[37]** Taisya Krivoruchko “Robust Coercion-Resistant Registration for Remote E-voting” Department of Computer ScienceUniversity of Calgary, Canada June 21, 2007.

**[38]** Taisya Krivoruchko, “SureVote”, Department of Computer Science University of Calgary Calgary, AB Canada, T2N 1N4 , May 19, 2004.

**[39]** The National Election Committee, “E-Voting System”, Tallinn 2005.

**[40]** Thomas Edison, “e-voting recorder”, patent NO 90,646, June 1, 1869.

**[41]** Thomas W. Lauer, “The Risk of e-Voting”, Electronic Journal of e-Government ISSN: 1479-439X USA, Vol 2, pp 177-186, 2004.

**[42]** William Stallings, “Cryptography and network security Principles and practices”, Prentice Hall ISBN-10: 0130914290,pp. 258-274 ,2003.

## Web References

**[43]** http://www.computer.org/security. Last accessed in 25/3/2008.

**[44]** http://en.wikipedia.org/wiki/Main_Page Last accessed in 25/3/2008.

**[45]** http://www.cs.berkeley.edu/_daw/papers/cvopunpub05 Last accessed in 25/3/2008.

**[46]** http://www.esecurity.ch Last accessed in 25/3/2008.

**[47]** http://edison.rutgers.edu/patents/00090646.PDF Last accessed in 25/3/2008.

**[48]** http://www. Internet news.com/security/article.php/11803_3616656_2 Last accessed in 25/3/2008.

**[49]** http://aceproject.org/ace-en/focus/e-voting/e-voting-auditing Last accessed in 25/3/2008.

**[50]** http://en.wikipedia.org Last accessed in 25/3/2008.

**[51]** http://en.wikipedia.org/wiki/Digital_signature Last accessed in 25/3/2008.

**[52]** http://www.everyonecounts.com Last accessed in 25/3/2008.

**[53]** http://www.brennancenter.org Last accessed in 25/3/2008.

**[54]** http://www.usenix.org/events/evt06/tech/full_papers/sherman/sherman_html/ Last accessed in 25/3/2008.

**[55]** http://www.ebusinessforum.gr/engine/index.php?op=modload&modname=Downloads&action=downloadsviewfile&ctn=1564&language=el Last accessed in 25/3/2008.

**[56]** http://avirubin.com/vote.pdf Last accessed in 10/6/2008

**[57]** http://www.usenix.org/events/evt07/tech/full_papers/feldman/feldman_html/ Last accessed in 10/6/2008

**[58]** http://aeolus.ceid.upatras.gr/scientific-reports/2nd_year_reports/practical_e_voting_final.pdf Last accessed in 10/6/2008

**[59]** http://www.surfnet.nl/nl/bijeenkomsten/Pages/Default.aspx Last accessed in 10/6/2008

# APPENDICES

## APPENDIX A: Cryptography

(Or cryptology; derived from Greek κρύπτω kryptó "hidden" and the verb γράφω gráfo "to write" or λέγειν legein "to speak")[4]; Is the practice and study of hiding information. In modern times, cryptography is considered to be a branch of both mathematics and computer science, and is affiliated closely with information theory, computer security, and engineering. Cryptography is used in applications present in technologically advanced societies; examples include the security of ATM cards, computer passwords, and electronic commerce, which all depend on cryptography

### Public-key cryptography

Also known as asymmetric cryptography is a form of cryptography in which a user has a pair of cryptography keys a public key and a private key. The private key is kept secret, while the public key may be widely distributed. The keys are related mathematically, but the private key cannot be practically derived from the public key. A message encrypted with the public key can be decrypted only with the corresponding private key.

Conversely, secret key cryptography, also known as symmetric cryptography uses a single secret key for both encryption and decryption.

The two main branches of public key cryptography are:

Public key encryption a message encrypted with a recipient's public key cannot be decrypted by anyone except the recipient possessing the corresponding private key. This is used to ensure confidentiality.

Digital signatures a message signed with a sender's private key can be verified by anyone who has access to the sender's public key, thereby proving that the sender signed it and that the message has not been tampered with. This is used to ensure authenticity.

**Symmetric-Key Encryption**

With **symmetric-key encryption,** the encryption key can be calculated from the decryption key and vice versa. With most symmetric algorithms, the same key is used for both encryption and decryption, as shown below. Figure 16 shows the process.

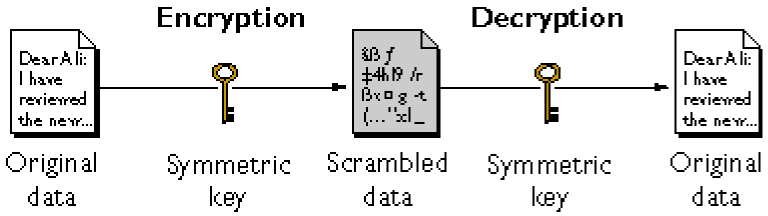


Figure 0-1: Symmetric-Key Encryption

Implementations of symmetric-key encryption can be highly efficient, so that users do not experience any significant time delay as a result of the encryption and decryption. Symmetric-key encryption also provides a degree of authentication, since information encrypted with one symmetric key cannot be decrypted with any other symmetric key. Thus, as long as the symmetric key is kept secret by the two parties using it to encrypt communications, each party can be sure that it is communicating with the other as long as the decrypted messages continue to make sense.

Symmetric-key encryption is effective only if the symmetric key is kept secret by the two parties involved. If anyone else discovers the key, it affects both confidentiality and authentication. A person with an unauthorized symmetric key not only can decrypt messages sent with that key, but can encrypt new messages and send them as if they came from one of the two parties who were originally using the key.

Symmetric-key encryption plays an important role in the SSL protocol, which is widely used for authentication, tamper detection, and encryption over TCP/IP networks. SSL also uses techniques of public-key encryption, the most commonly used implementations of public-key encryption are based on algorithms patented by RSA Data Security. Therefore, this section describes the RSA approach to public-key encryption.

Public-key encryption (also called asymmetric encryption) involves a pair of keys--a **public key** and a **private key**--associated with an entity that needs to authenticate its identity electronically or to sign or encrypt data. Each public key is published, and the corresponding private key is kept secret. Data encrypted with your public key can be decrypted only with your private key. shows a simplified view of the way public-key encryption works.

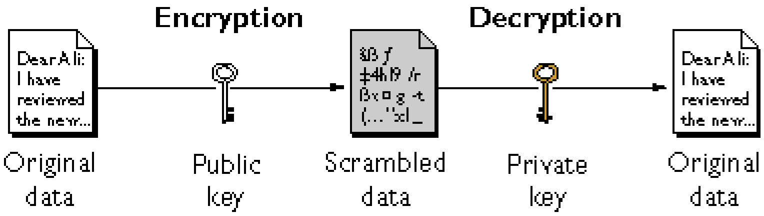


Figure 0-2: Public-Key Encryption

The scheme shown in Figure above lets you freely distribute a public key, and only you will be able to read data encrypted using this key. In general, to send encrypted data to someone, you encrypt the data with that person's public key, and the person receiving the encrypted data decrypts it with the corresponding private key.

Compared with symmetric-key encryption, public-key encryption requires more computation and is therefore not always appropriate for large amounts of data. However, it's possible to use public-key encryption to send a symmetric key, which can then be used to encrypt additional data. This is the approach used by the SSL protocol.

As it happens, the reverse of the scheme shown in above Figure also works: data encrypted with your private key can be decrypted only with your public key. This would not be a desirable way to encrypt sensitive data, however, because it means that anyone with your public key, which is by definition published, could decrypt the data. Nevertheless, private-key encryption is useful, because it means you can use your private key to sign data with your digital signature an important requirement for e-voting and other commercial applications of cryptography. E-voting can then use your public key to confirm that the message was signed with your private key and that it hasn't been tampered with since being signed.

### Digital Signatures

Encryption and decryption address the problem of eavesdropping, one of the three Internet security issues mentioned at the beginning of this document. But encryption and decryption, by themselves, do not address the other two problems mentioned in Internet Security Issues: tampering and impersonation. This section describes how public-key cryptography addresses the problem of tampering.

As mentioned in Public-Key Encryption, it's possible to use your private key for encryption and your public key for decryption. Although this is not desirable when you are encrypting sensitive information, it is a crucial part of digitally signing any data. Instead of encrypting the data itself, the signing software creates a one-way hash of the data, and then uses your private key to encrypt the message.

## APPENDIX B: CV

# Omar Al Hnaity

Mobile: 0777316780
Email: **omar_hnaity@yahoo.com**

## *Personal Information*

| | |
|---|---|
| Name: | Omar Sa'ed Al Hnaity |
| Nationality: | Jordanian |
| D.O.B: | 02/06/1983 - Amman |
| Address: | Amman\Abu Alanda\Eskan Al khrba'a |
| Hobbies: | Swimming, reading and football. |
| Material status: | engaged |
| Languages: | Arabic (Native Language), English good in (speaking, writing & reading) |

## *Education & Certificates*

Gains an OOP by C++ certification from computer Center - Hashemite University.

Gains an ASP.Net, C#.net and ADO.net Certificates from PC.Net.

A Computer Science and applications graduate from Hashemite University (2005).

## *Experiences*

May, 7th - 2006 – Till Present Estarta Solutions Company as Software Engineer, Joined the Portals Unit as a portal consultant. And helped in build the following projects:

- “AEC “Portal using MS Share point 2003 technology.
- “BAWWABAT” using MS Share point 2003 technology
- “Injazat & Bawabat” EPM & SPS using MS Office Share point 2007 (MOSS) technology.
- “Royal Court” POC using MS Office Share point 2007 (MOSS) technology.
- “Rajhi” Portal using MS Office Share point 2007 (MOSS) technology.
- “Al Jazeera children’s” Portal using MS Office Share point 2007 (MOSS) technology.
- “Al HAMRANI” Portal using MS Office Share point 2007 (MOSS) technology.
- “Al Markaz” Portal using MS Office Share point 2007 (MOSS) technology.
- “Jeddah municipality” Portal using MS Office Share point 2007 (MOSS) technology.
- “KFSC” GRP System using C#.net And Asp.net technology
- “APC” Portal using MS Office Share point 2007 (MOSS) technology.
- “UNIFEM” Portal using MS Office Share point 2007 (MOSS) technology.
- “Ithmar” Bank Portal using MS Office Share point 2007 (MOSS) technology.
- “ADFCA” Portal using MS Office Share point 2007 (MOSS) technology.
- “Estarta” Portal using MS Office Share point 2007 (MOSS) technology.

## Skills

**Developing and Programming**

- Microsoft SPS and WSS “Sharepoint”2003
- Microsoft Office SharePoint 2007 “MOSS”
- C#.NET
- VB.NET
- ASP.NET
- ADO.NET
- DATA BASES MS SQL server 2000-2005
- OOP USING C++
- JAVA J2E

**Web development**

●HTML ●XML ● CSS
●ASP.NET ● PHP ●Java script

**Design**

- Photoshop
- Flash MX ability to use action script
- Dreamweaver

## Knowledge

- e-Commerce.
- Data Mining Methods and technologies
- Neural networks
- Algorithms
- Data Structures
- Systems Analysis
- Databases
- Object Oriented Programming
- Computer Hardware & Software Maintenance
- Very good in statistics and mathematics
- Computer Security
- Image Processing
- Software Engineering
- Artificial Intelligence

**Networks Knowledge**

- CCNA
- Excellent in high speed networks and Internet
- Excellent in Distributed systems
- Excellent in TCP\IP Protocols
- Networks Security

## *Personal Skills*

- Ability to works in teams and work groups
- Ability to find quick solutions for problems
- Ability to deal with VIPs
- Ability to work anywhere
- Quick-Learner and ability to learn and utilize new methods, systems, and programming languages.
- Dedicated and Self-Motivated, with a great desire to keep learning new technical concepts.
- High Coding Skills and solid knowledge in programming standards.
- Have a Team Spirit and ability to work well under pressure.
- An Active and Adaptive team member
- Ability to Multitask and Accurate in accomplishing duties.
- Adapts quickly to changes.
- Ability to satisfy customer requirements.

**تم بحمد الله**