View metadata, citation and similar papers at core.ac.uk

brought to you by CORE

provided by BRAC University Institutional Repository

STUDY OF SMS SECURITY AS PART OF AN ELECTRONIC VOTING SYSTEM

A thesis

Submitted to the Department of Computer Science & Engineering
Of
BRAC University
By

Chowdhury Mushfiqur Rahman
ID: 02101108
Shah Md. Adnan Khan
ID: 01201055

In Partial Fulfillment of the requirements for the Degree

Of

Bachelor of Computer Science & Engineering
May 2006

BRAC University, Dhaka, Bangladesh

DECLARATION

I, Chowdhury Mushfiqur Rahman, University ID: - 02101108 have completed some modules of our proposed Thesis, Secured SMS Service in Electronic Voting System, Under CSE 400 course based on the result found by me.

I therefore declare that this project has been published previously neither in whole nor in part of any degree except this publication. I also mentioned work found by other researcher by reference.

Signature of Supervisor	Signature of Author

ACKNOWLEDGEMENT

Firstly, I’m grateful to almighty Allah for providing the strength and energy to start such a project and finally finish it successfully.

I’m really very grateful and take the honor to express my special thanks to my supervisor DR. Yousuf M. Islam, PhD for all sorts of supportive suggestions and opinions. Without his support, co-operation and resources it would be a day dream to complete my research in this due time.

My special thanks go to my Co-Supervisor Matin Saad Abdullah and Ms. Bushra Taufiq Chowdhury for their useful and important suggestions. Without their supportive consultancies my research will never have fulfilled the requirements.

I would also like to thank the senior brothers of University and friends who helped me in every possible way.

I want to specially thank my teachers and friends who always supported and helped me during my thesis work as a family member by always giving me moral support.

Finally I feel deepest admiration to my department for giving me the honor to perform the Thesis a partial fulfillment of the requirement for the Degree of Bachelor of Computer Science and Engineering.

ABSTRACT

E-voting is a new technology in voting system. Recently it was experimented in UK. Basically, this system is proposed to work via Short Message System (SMS). Using secure messaging system we are trying to develop the e-voting system here in our country. Our goal is to develop a system, which will be able to send SMS from a registered cell phone to a server located in the base polling station and cast a vote for a voter. The system must be secured so that while voting, no outside interference can be made to change the vote. So, there will be no tension of casting false vote. By the help of this system our voters will be able to cast their votes in a secure way and also the results will be available immediately when the vote casting finishes. This is going to be a pioneer change in our voting system. Some work on this proposed system has already been done. We wish to carry out the proposed system into further details. That is security aspects and implementation.

TABLE OF CONTENTS

CHAPTER 2: METHODOLOGY

CHAPTER 3: SYSTEM DEVELOPMENT

CHAPTER 1

INTRODUCTION

1.1 Background of Election System in Bangladesh

Bangladesh started her journey with Parliamentary system of Government, then switched over to Presidential system and in 1991 reverted back to Parliamentary system.

Parliament consists of three hundred members elected in accordance with law from single-member territorial constituencies. Besides this there was a provision of thirty seats reserved exclusively for woman members up to the year 2000 who were elected according to law by the members of the parliament. Parliament has tenure of 5 years unless dissolved earlier.

1.2 Criteria for Election System

Based on the traditions of the elections and voting system in the Bangladesh, election systems- whether through traditional voting methods or SMS voting are commonly expected to satisfy a number of criteria, including-

- Eligibility and Authentication- Only authorized voter should be able to vote.
- Uniqueness – no voter should be able to vote more than one time.
- Accuracy- Election system should record the vote correctly.
- Integrity- votes should not be modified, forged and deleted without detection.

- Verifiability and Audit ability – It should be possible to verify that all votes have been correctly accounted for in the final election tally and there should be reliable and demonstrably authentic election records.
- Reliability- Election system should work robustly, without loss of any votes, even in the face of numerous failures, including failures of voting machines and total loss of mobile communication.
- Secrecy- No one should be able to determine how an individual voted, and voter should not be able to prove how they voted.
- Flexibility- The election procedure must have such flexibility that they can be adapted at any point of the election subject to the demand of the current situation.

1.3 Current Voting Status in Bangladesh

According to the law, casting of votes and counting of votes are the pivotal and final tasks in the whole process of the election, though the consolidation of results and declaration of the names of returned candidates are the subsequent legal requirements.

1.3.1 Before Poll: The Returning Officer provides each Presiding Officer with necessary ballot boxes of such material and design as are approved by the Commission. Not more than one ballot box is used at a time for the purpose of the poll at any polling booth.

1.3.2 Poll: At least half an hour before the time fixed for the commencement of the poll, the Presiding Officer is required to ensure that every ballot box to be used is empty, show the empty ballot box to the contesting candidates and their election agents and polling agents whoever may be present, close and seal the ballot box and place the ballot box so as to be conveniently accessible to the elector -- visible to all present in the booth -- officials and election or polling agents as may be present. Every elector will mark his ballot paper in secret before the same is folded and inserted in the ballot box by the elector himself.

The Presiding Officer regulates the number of electors to be admitted to the polling station at a time and excludes from the polling station all other persons except those connected with the polling.

The Presiding Officer is responsible for keeping order at the polling station so that an elector can exercise his free will to cast his vote at the polling station.

Where an elector presents himself at the polling station to vote, the Presiding Officer shall, after satisfying himself about his identity, issue to him a ballot paper after giving him a personal mark made with indelible ink on his thumb or any other finger of either hand, placing a mark on the electoral roll against the number and name of the elector to indicate that a ballot paper has been issued to him and recording the elector's number and procuring signature of the elector on the counter foils of electoral roll and ballot paper respectively .

The elector, on receiving the ballot paper, shall forthwith proceed to the place reserved for marking the ballot paper, put the prescribed mark on the ballot paper at any place within the space containing the name and symbol of the contesting candidate for whom he wishes to vote and after he has so marked, fold the ballot paper and insert it in the ballot box. He has to do the whole thing at the quickest speed.

If a person represents himself to be an elector applies for a ballot paper when another person has already represented himself as that elector and has voted under the name of the person so applying, he shall be entitled to receive a ballot paper which is called a tendered ballot paper. The Presiding Officer maintains separate accounts of tendered and challenged votes and also spoilt ballot papers as per law.

The polling time is generally 0800-1600hrs local time. No person is allowed entry into the polling station enclosure after 1600hrs.

1.3.3 Count of Votes: Immediately after the close of the poll with the casting of vote by the last voter of the day, the Presiding Officer, in the presence of such of the contesting candidates, election agents and polling agents as may be present, proceeds with the count of votes.

The Presiding Officer gives such of the contesting candidates, election agents and polling agents as may be present, reasonable facility of observing the count and gives them such information with respect thereto as can be given consistent with the orderly conduct of the count and the discharge of his duties in connection therewith.

Under the law no person other than the Presiding Officer, the Polling Officer, any other person on duty in connection with the poll, the contesting candidates, their election agents and polling agents are to be present at the count. However, authorized observers are allowed by the Election Commission to observe the count as a special dispensation. The Presiding Officer shall open the used ballot box or ballot boxes and count the entire lot of ballot papers taken out from there in presence of these persons.

The valid ballot papers cast in favor of each contesting candidate are preserved in separate packets. The Presiding Officer, immediately after the count, prepares a statement of the count and if so requested by any candidate or election agent or polling agent present, gives him a certified copy of the statement of the count and the ballot paper account.

The Presiding Officer puts in good order all records of the poll and sends them to the Returning officer immediately.

The Returning Officer is required to give the contesting candidates and their election agents a notice in writing of the day, time and place for the consolidation of the results and, in the presence of such of the contesting candidates and election agents as may be present, consolidate in the prescribed manner the results of the count furnished by the Presiding Officer, including therein, the postal ballots received by him before the time aforesaid.

1.3.4 Recount : The Returning Officer shall recount the valid ballot papers in respect of any polling station if the count by the Presiding Officer is challenged in writing by a contesting candidate or his election agent and the Returning Officer is satisfied about the reasonableness of the challenge or he is directed so to do by the Commission.

Where, after consolidation of the results or the count, it is found that there is equality of votes between two or more contesting candidates and the addition of one vote for one such candidate would entitle him to be declared elected, the Returning Officer shall forthwith draw a lot in respect of such candidates and the candidate on whom the lot falls shall be deemed to have received the highest number of votes entitling him to be declared elected. The lot shall be drawn in the presence of such of the contesting candidates and their election agents as may be present.

The Returning Officer shall, after obtaining the result of the count or of the draw of the lot declare by public notice the contesting candidate who has or is deemed to have received the highest number of votes to be elected. The Commission is required as per law to publish in the official gazette the name of the returned candidate.

The Returning Officer shall supply duly attested copies of the consolidated statement and the return of election to such of the candidates and their election agents as may desire to have them.

1.4 Advanced Voting System Used Abroad

Electronic voting systems for electorates have been in use since the 1960s when Punch Card systems debuted. The newer marksense ballots allow a computer to count a voter's mark with an optical sensor. Electronic voting systems have gained popularity and have been used for government elections and referendums primarily in European countries. Electronic Voting Machines are used on a large scale in India, Brazil, UK and the United States. In 2002, in the United States, the Help America Vote Act mandated that one accessible voting system be provided per polling place, which many jurisdictions have chosen to satisfy with the use of accessible electronic voting machines.

1.5 Security Aspects of E-voting system

The aim of an electronic voting system is to translate the traditional vote to a digital context. Several experimentations have already been done, based either on black-box machines or on cryptographic frameworks. The purpose of electronic voting systems is to obtain the results immediately after the end of the poll, while (at least) preserving the security of the traditional vote. Cryptography-based frameworks are designed to enhance security while enhancing some functionality that remains mainly theoretical in traditional voting because of practical issues.

An electronic voting scheme is a protocol allowing voters to securely vote by interacting with a set of authorities who collect the votes and calculate the result of the election. We usually distinguish between two types of electronic voting: on-line voting, *a.k.a.* remote voting, for example via Internet, and off-line voting, by using a voting machine or an electronic polling booth. The main goal of a secure electronic voting system is to ensure the privacy of the voters and the accuracy of votes. Our electronic voting system fulfills the following usual requirements:

- **Eligibility:** only votes of legitimate voters shall be taken into account.

• **No reusability:** each voter shall only be able to cast one vote.
• **Anonymity:** all votes shall be secret.
• **Accuracy:** cast ballot cannot be altered.

• **Fairness:** it must be impossible to perform partial tabulation before the end of the election.

• **Vote and go (or walk-away):** once a voter has cast his vote, there is no further action he needs to take.

1.6 Our proposed voting system with Secured SMS service

The proposed system is considered to work with three phases. The workflow is described below:

1.6.1 Initial Setup of the System:

- *Mobile Phone Registration:* Each polling booth will be registered with a unique mobile number in the system's database.
- *Candidate Registration:* Each candidate will be registered in the system's database with their unique IDs.
- *Party & Constituency Registration:* Each party and constituency will be registered in the system's database with their detail information.

1.6.2 Vote Casting Process:

- *Voter Authentication:* When a voter comes to the polling center for voting he/she is manually authenticated by the polling officer whether he/she is a valid voter.
- *Electronic Voting:* Voters send the unique candidate IDs as their votes using the Electronic voting device which uses SMS technology.

- *SMS delivery notification:* Voter is notified of successful SMS delivery. The mobile network service providers like GP, Aktel & Banglalink etc will do this.
- *Invalid vote cast notification:* Voter is notified of unsuccessful vote cast like invalid voting format or mobile number.
- *Electronic Vote Recording:* Successful vote casts are updated in the database server accordingly.

1.6.3 Result Generation:

- *Electronic Vote counting:* After polling hour Super User initiates the counting command, the stored data is then retrieved from the database for counting by the system.
- *Electronic Report Generation:* Based on the counting results the system will generate following reports:

    - Result by Constituency
    - Result for each polling Center
    - Determining the Winning Candidate

1.7 Feasibility of our System:

- May be initially installed in high risk areas where the risk of hijacking ballot box is very high. We can use the system as a pilot project.
- For election it is possible to switch off all the mobile connections except registered mobiles with dedicated network.
- The possibility of the mobile network congestion will be much less numbers of mobiles under each Base Transceiver Station (BTS).
- Very simple system to operate and can be installed in a short time.

1.8 Advantages of our System:

- Simple voting interface for voters.
- Vote count and generating results are done in a short period of time.
- Less human involvement is needed with more efficiency.
- System is more secure and dependable.

CHAPTER 2

METHODOLOGY

2.1 Studies and visit undertaken

Different Steps of the process of Electronic voting using SMS service:

2.1.1 Polling booth: In the polling booth a voter first has to authenticate him/her self. Then voter will have to cast the vote using an Electronic Ballot Unit. A control unit is connected with the electronic ballot unit. The control unit will pass the signal to a Registered Cell phone.

2.1.2 Registered Cell Phone: The vote will transmit to Election Commission Server as a Short Text Message. When the vote reaches the Election Commission, vote will be received by another registered cell phone which will be connected to the EC server.

2.1.3 Election commission server: The registered cell phone will be connected with the server. When the vote will be received by the server it will automatically upgrade the database.

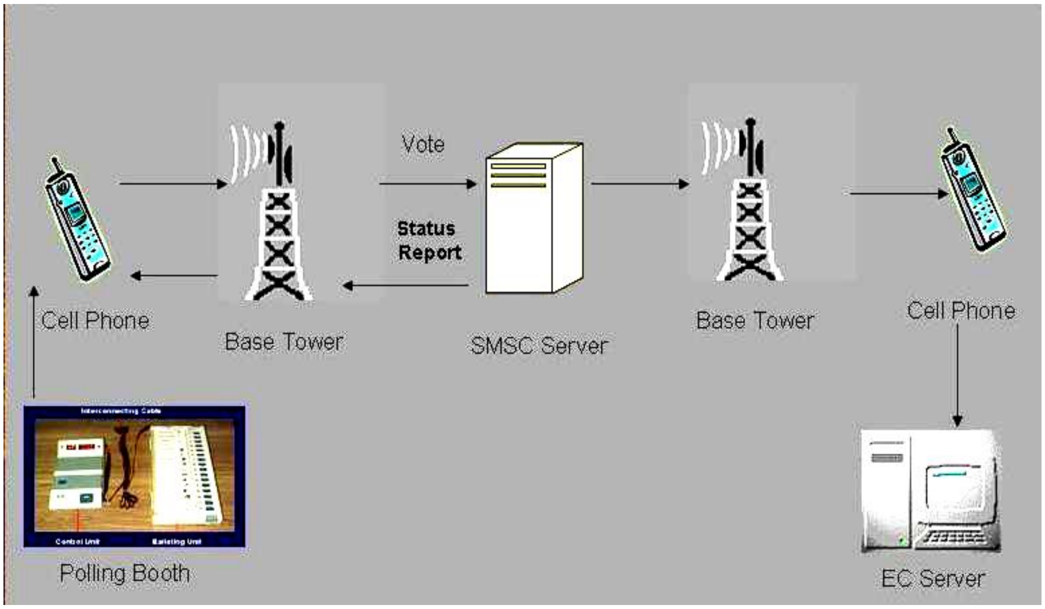


Figure: E-voting system

2.1.4 Existing SMS Gateway System of Grameen Phone:

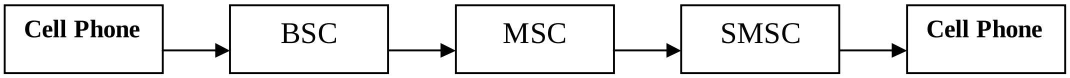


Figure: SMS Gateway of Grameen Phone

When we send a SMS from a cell phone it reaches Base Station Control (BSC) to Mobile Switching Center (MSC). In the MSC it finds its destination. Then it directly goes to the Short Message Service Center (SMSC). From the SMSC server when it reaches to its destination a delivery report generates from the SMSC server. They are using Short Message Peer –to- Peer (SMPP) protocol.

2.2 Problems and areas of security leak identified

With the help of Grameen Phone we have found out the problems and areas of security leak. In the SMS gateway only security breach can happen in SMSC Server because no one can read or delete any SMS content in Base Station Control (BSC) or Mobile Switching Center (MSC). But in the SMSC server any administrator can read or delete the SMS content. No one can change or edit the content of SMS. So security breach can happen only in SMSC server. So the critical point for us is SMSC Server.

2.3 Ideas about SMS security

- Any unauthorized person can read the content of SMS.
- SMS can be deleted in the SMS gateway.
- Delivery report can be deleted in the SMS gateway. In this case there is a chance of repeating the vote.
- Someone can send a false delivery report that the vote has been cast. In this case any unauthorized person can delete the SMS and send a false delivery report to the voter.

2.4 Security alternative

- The content of the SMS will be encrypted so that nobody can read or understand the SMS.
- We can use a counter to check the number of digit of the SMS content.
- Also other counter measures can be taken like monitoring the whole SMSC server with the help of authorized persons from the Election Commission.

2.5 Various Encryption-decryption algorithm & use

2.5.1 Quasigroups Encryption Algorithms

A groupoid is a finite set Q that is closed with respect to an operator _, that is a _ b 2 Q for all a, b 2 Q. A groupoid is a quasigroup, if it has unique left and right inverses, i.e., for any u, v 2 Q there exists unique x and y such that x_u = v and u _ y = v. This means that all operations are invertible and have unique solutions, which implies their usability as cryptographic substitution operations. With this in mind we can define inverse operations for _, call them \ (left inverse) and / (right inverse). The operator \ (resp. /) defines a new quasigroup (Q, \) (resp. (Q, /)) and for algebra (Q, \, _) x _ (x\y) = y = x\(x _ y)

A quasigroup can be characterized with a structure called Latin square. A Latin square is an n _ n matrix where each row and column is a permutation of elements of a set. In our case |Q| = n. Several other operations can be derived from the operation _ [2], but for our purposes operations _ and \ (right inverse) are sufficient.

2.5.1.1 *Encryption:*

The encryption primitive e_l on sequence $x_1x_2 . . . x_n$ is defined as

$e_l(x_1x_2 . . . x_n) = y_1y_2 . . . y_n$ where

_y_1 = l _ x_1,

y_i + 1 = y_i _ x_i+1(i = 1, . . . n − 1) (2)

The variable l is called the leader and in our application it is derived from the secret key (password). Transformation e is a mapping A +! A +. Elements x_i, y_i, 2, A are usually not characters, but entities of bits, where the bit length of the element is defined by the size of the Latin square associated with the quasigroup.

2.5.1.2 *Decryption:*

Decryption d_l: A +! A+ is naturally a reverse operation of encryption. It is defined as

$d_l(y_1y_2 . . . y_n) = x_1x_2 . . . x_n$, where

_$x_1 = l\backslash y_1$,
x_i +1 = $y_i\backslash y_i$+1(i = 1, . . .,n − 1)

In essence, the decryption primitives as well as the encryption primitives are table lookup methods, where the Latin square associated with the quasigroup is used. In encryption the previous encrypted element and the next not yet encrypted element are used to find corresponding value from the table. This value is then used as the new encrypted value. In decryption the values used for lookup are the previous already decrypted value and the next not yet decrypted value. With these a new decrypted value is found from the Latin square.

2.5.1.3 Composition of encryption and decryption:

One application of the encryption el defined earlier usually doesn't provide adequate security. For this reason the encryption method is repeated, using different leaders. The encryption E_L = e_{l1} _ e_{l2} _ . . ., e_{lk}, l_{i2}. L is a composition of consecutive applications of the encryption primitive e_l where leaders l_1, l_2 . . . , l_k 2 L are used. Also different quasigroup operations can be used in distinct primitives e_l. The decryption function D_L = d_{lk} _ d_{lk}−1 _, d_{l1}, l_i 2 L is composed similarly except that the leaders l_i 2 L are used in reverse order. The quasigroup operation used in primitive dl must correspond to the one used in e_l. In earlier papers [1], [2] it has been proved that mappings E and D are bijections and E_L (D_L (_)) = D_L (E_L (_)) = _.

For encryption purposes, primitives el and dl can be incorporated to produce a more complex encryption method. Then encryption is defined as
E_L = h_{l1} _ h_{l2} _ . . . h_{lk} , l_i 2 L, h_{li} 2 {e_{li} , d_{li}}

In this construction, primitive e_l is clearly used for decryption if corresponding primitive dl has been used in decryption.

2.5.2 Transposition Algorithm Techniques

All the techniques examined so far involve the substitution of a cipher text symbol for a plaintext symbol. A very different king of mapping is achieved by performing some sort of permutation on the plaintext letters. This technique is referred to as a transposition cipher.

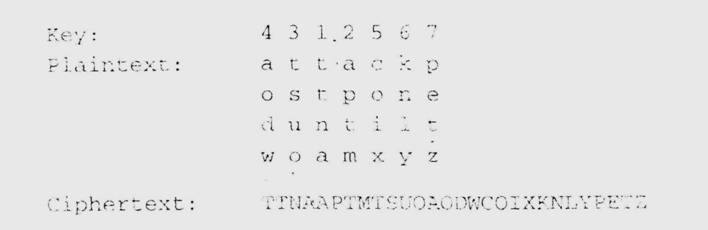
The simplest such cipher is the rail fence technique, in which the plaintext is written down as a sequence of diagonals and then read off as a sequence of rows. For example, to encipher the message "Meet me after the toga party" with a rail fence of depth 2, we write the following:

```
m e m a t r h t g p r y
 e t e f e t e o a a t
```

The encrypted message is:

MEMATRHTGPRYETEFETEOAAT

This sort of thing would be trivial to crypt analyze. A more complex scheme is to write the message in a rectangle, row by row, and read the message off, column by column, but permute the order of the columns. The order of the columns then becomes the key to algorithm. For example



```
Key:             4 3 1 2 5 6 7
Plaintext:       a t t a c k p
                 o s t p o n e
                 d u n t i l t
                 w o a m x y z

Ciphertext:      TTNAAPTMTSUOAODWCOIXKNLYPETZ
```

2.5.3 Data Encryption Standard (DES)

The scheme for DES encryption is, there are two inputs to the encryption function: the plaintext to be encrypted and the key. In this case, the plaintext must be 64 bits in length and the key is 56 bits in length.

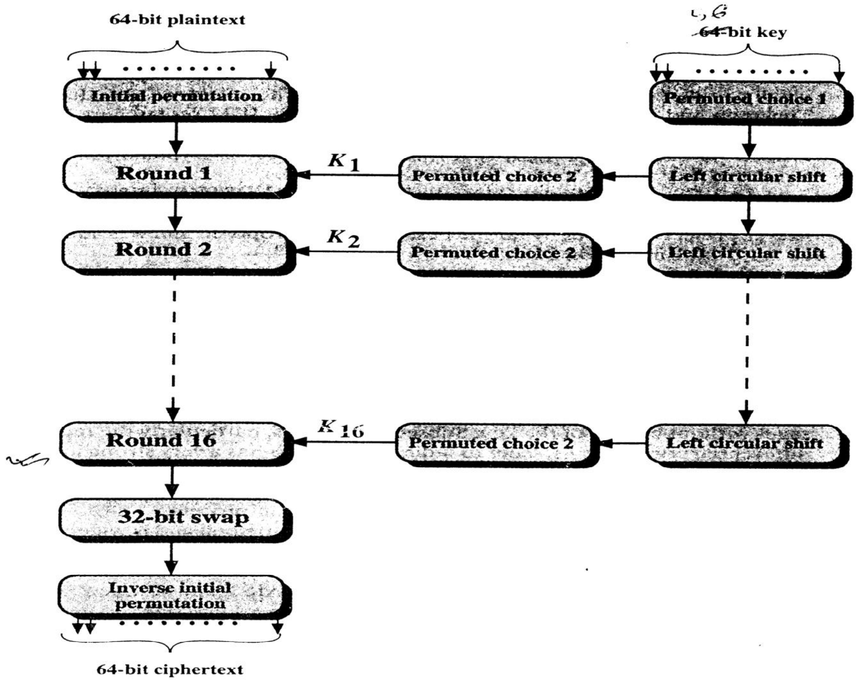


Figure: DES encryption model

Details of a Single Round:

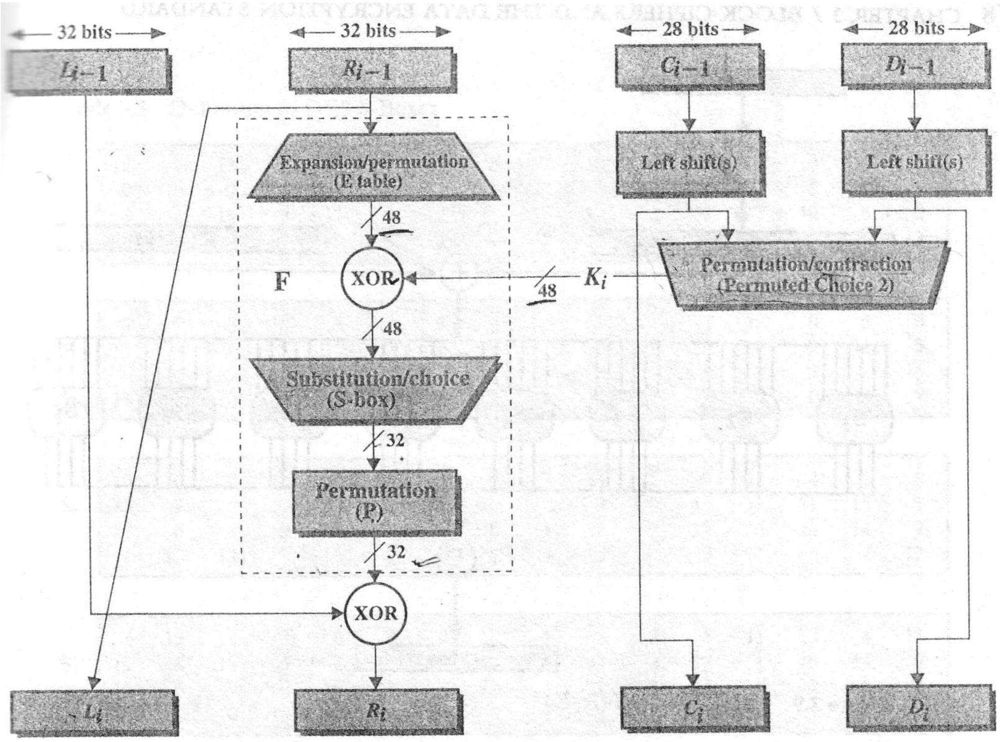


Figure: a single step of DES encryption

2.6 Optimal method of encryption for our proposed system

We have chosen an optimal encryption algorithm Polyalphabetic Cipher Text for encrypt our SMS content. It is a way to improve on the simple monoalphabetic substitution cipher. This technique has the following features:

- A set of related monoalphabetic substitution rules is used.
- A key determines which particular rule is chosen for a given transformation.

2.7 Detailed discussion about the selected encryption algorithm

In the Polyalphabetic cipher the ultimate defense against such a cryptanalysis is to choose a keyword that is as long as the plain text and has no statistical relationship to it. The system can be expressed succinctly as follows:

$$c_i = p_i \oplus k_i$$

where

$$\begin{aligned} p_i &= i\text{th binary digit of plaintext} \\ k_i &= i\text{th binary digit of key} \\ c_i &= i\text{th binary digit of ciphertext} \\ \oplus &= \text{exclusive-or (XOR) operation} \end{aligned}$$

Thus, the cipher text is generated by performing the bitwise XOR of the plain text and the key. Because of the properties of the XOR, decryption simply involves the same bitwise operation.

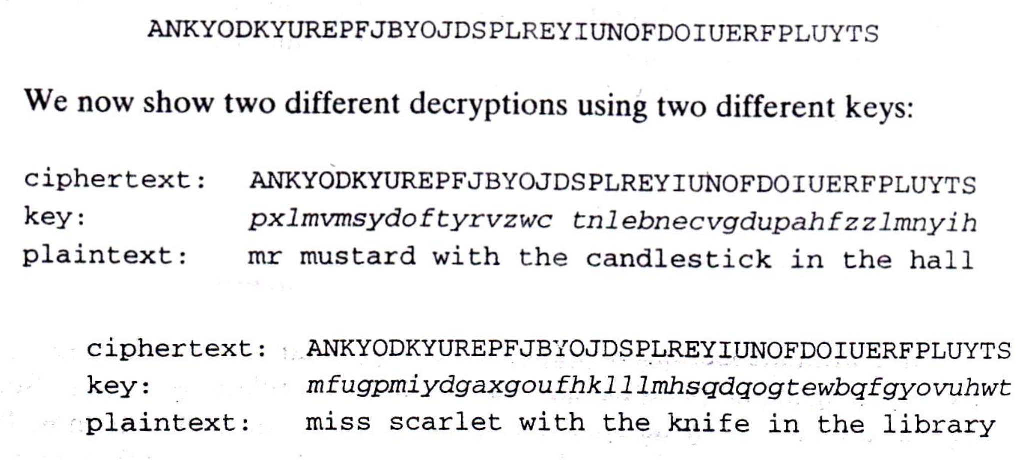
$$p_i = c_i \oplus k_i$$

The essence of this technique is the means of construction of the key. Vernam proposed the use of a running loop of tape that eventually repeated the key, so that in fact the system worked with a very long but repeating keyword. Although such a scheme, with a long key, presents formidable cryptanalytic difficulties, it can be broken with sufficient cipher text, the use of known or probable plaintext sequences, or both.

2.7.1 One time padding in Encryption

One time pad uses a random key that was truly as long as the message, with no repetitions. Such a scheme, known as a one-time pad, is unbreakable. It produces random output that bears no statistical relationship to the plain text; there is simply no way to the code.

An example should illustrate our point. Suppose that we are using a Vigenere scheme with 27 characters in which the twenty-seventh character is the space character, but with a one time pad key that is as long as the message. Thus, it must be expanded to 27 x 27. Consider the cipher text.



```
ANKYODKYUREPFJBYOJDSPLREYIUNOFDOIUERFPLUYTS
```

We now show two different decryptions using two different keys:

```
ciphertext:   ANKYODKYUREPFJBYOJDSPLREYIUNOFDOIUERFPLUYTS
key:          pxlmvmsydoftyrvzwc tnlebnecvgdupahfzzlmnyih
plaintext:    mr mustard with the candlestick in the hall

ciphertext:   ANKYODKYUREPFJBYOJDSPLREYIUNOFDOIUERFPLUYTS
key:          mfugpmiydgaxgoufhklllmhsqdqogtewbqfgyovuhwt
plaintext:    miss scarlet with the knife in the library
```

Suppose that a cryptanalyst had managed to find these two keys. Two plausible plaintexts is in correct decryption. If the actual key were produced in a truly random fashion, then the cryptanalyst cannot say that one of these two keys is more likely then the other. Thus, there is no way to decide which key is correct and therefore which plaintext is correct.

In fact, given any plaintext of equal length to the cipher text, there is key that produce that plain text. Therefore, if you did an exhaustive search of all possible keys, you would end up with many legible plaintexts, with no way of knowing which the intended plaintext was. Therefore the code is unbreakable. The security of the one time pad is entirely due the randomness of the key. If the stream of the character that constitutes the key is truly random, then the stream of characters that constitute the cipher text will be truly random. Thus, there are no patterns or regularities that a cryptanalyst can use to attack the cipher text.

In theory, we need look no further for a cipher. The one time pad offers complete security but in practice, has two fundamental difficulties:

- There is the practical problem of making large quantities of random keys. Any heavily used system might require millions of random characters one regular basis. Supplying truly random characters in this volume is a significant task.

- Even more daunting is the problem of key distribution and projection. For every message to be sent, a key of equal length is needed by both sender and receiver. Thus, a mammoth key distribution problem exists.

Because of these difficulties, the one time pad of limited utility, and is useful primarily for low-bandwidth channels requiring very high security.

2.8 Advantages of using the algorithm

There are some major advantages of using this algorithm for encryption:

- Converts each character into bit level. Bit wise XOR operation is done between each character of the plain text and key.
- The cost of breaking the cipher exceeds the value of the encrypted information.

- The time required to break the cipher exceeds the useful lifetime of the information.

CHAPTER 3
SYSTEM DEVELOPMENT

3.1 Project initialization and planning

The work done by us was a part of previously worked out research project and we have continued the project further more. The previously completed tasks were implementing an E-voting system which will work as an alternative of the current national election system. This E-voting system is proposed to work with SMS technology. Our major project requirement was to make sure that the whole SMS gateway from the polling station to the Election Commission server should be secure enough to make the whole E-voting process successful.

For this reason, we needed to study the whole SMS technology. To do that we studied a lot. We took help from Internet and also from many books. But another important aspect of our study was to work with the largest Cell phone operator in Bangladesh – Grameen Phone. We went to GP as a survey team and put our best efforts in understanding the whole process of SMS gateway that GP uses. It was a major help of our project because with out understanding the whole process practically we won't be able to complete our research. The findings in the survey have already been discussed previously.

3.2 Voting Data Security Module

As the proposed system is an election system so there has to be a voting data security module where the voting data will be encrypted and sent to the election commission server. The encrypted data that has been received through SMS will then be decrypted and stored in database accordingly. The encryption-decryption is the main core module of the system. This makes the system more reliable by protecting vulnerable data from unauthorized access. This works in the following way:

- Encrypt vote before sending to the Election commission server.
- Decrypt vote before storing in the Election Commission server.

3.3 Analysis of the Project

The project was considered to be totally based on JAVA^{TM} platform. We planned to do the project on JbuilderX environment in J2ME wireless toolkit 2.0. It was our duty to find out the feasible and best approach of how to solve the security problem. We considered many algorithms and finally came up with a solution which would satisfy the requirements of the system to be secured. To do that we needed to implement a prototype of our proposed software and demonstrate it to the advisor.

3.4 Building the prototype

To do the prototype successfully, we needed to be familiar with the JbuilderX platform using J2ME wireless toolkit V2.0 as we didn't work with this platform earlier. After getting acquainted with the environment we started the software module that actually runs inside the mobile. After completing the driver module for the mobile, we started working on the encryption – decryption procedure. This part was really tricky for us to implement as the algorithm we intended to use wasn't implemented earlier. So we maintained a constant touch with our supervisor and co-supervisor who helped us in many ways.

3.5 Feedback from the Advisor

After building the prototype, we showed a demonstration to our advisor showing all the aspects about SMS security. He gave us valuable feedback from which we were able to calculate our problem areas which were to overcome to complete the research successfully. We had to go through some minor changes in the prototype to finally disclose it as functional software.

3.6 Customization of the system to be flexible to any cell phone network operator

We had to design such software which would be able to adapt with all the cell phone operators currently functional in the country. To do that we had to work with the cell phone companies and find out their areas of differentiability. While working with Grameen Phone, we studied their network for SMS transmission thoroughly and found that all the operators work on a basic model which is SMS gateway through SMSC server. So we intended to focus our attention on the SMSC server location where the highest amount of security threat is possible. For that we needed to rethink our system a little bit and finally came up with a solution of encrypting the SMS content so that no one can see or read the content of the SMS.

3.7 Combining the modules together as a full working model

After the completion of our SMS sending software and encryption – decryption procedure, it was required to integrate both the works done by us to create the full functional software. We started by making the jar file of our software to run in the mobile environment. It was almost easy to implement as we integrated both the SMS sending part & encryption – decryption part of the software. We installed the software in mobile environment and tested it to check whether the software works successfully or not. It was a successful demo as I've stated the testing data and results later in this report.

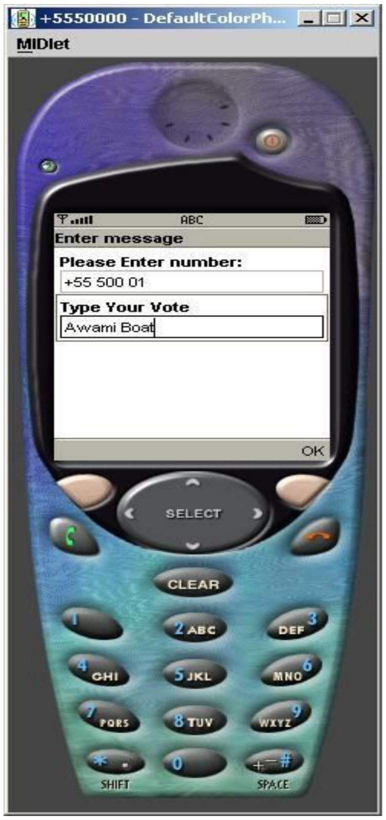
CHAPTER 4
SYSTEM TESTING

4.1 Unity and integration testing

We have tested our software in cell phones by creating jar files. All the cell phones that have JAVA^{TM} installed in it will be able to successfully run our software.

4.2 System testing

First in the simulator we use a number with +555 000 1. Now suppose we are giving vote to Awami with sign Boat, as we see in the following figure. So vote is casted as “Awami Boat” of which our target is to encrypt the content.

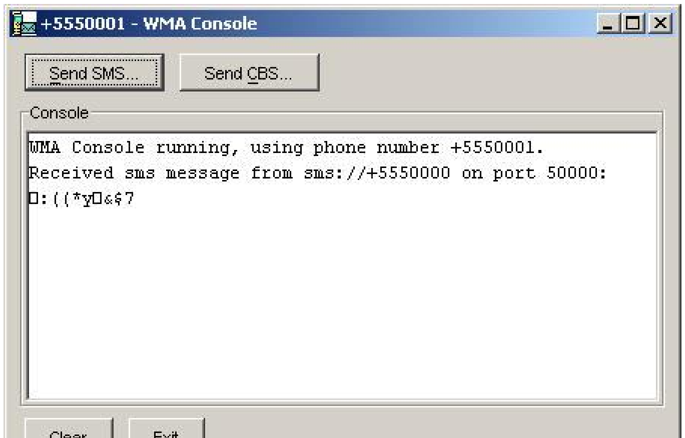


Enter message

Please Enter number:
+55 500 01

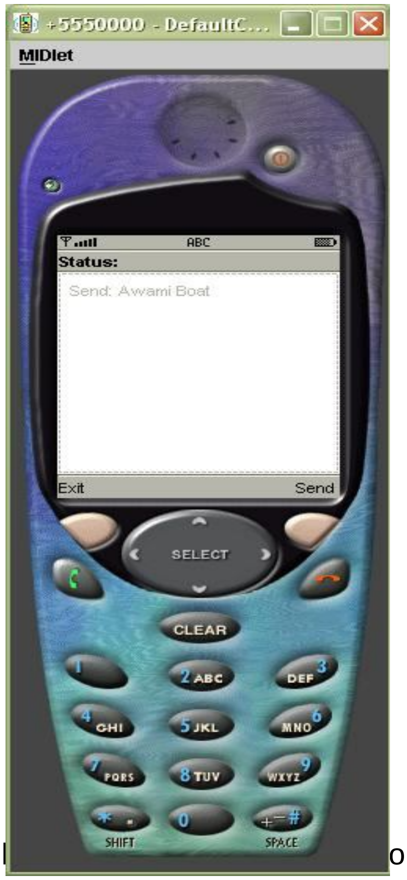
Type Your Vote
Awami Boat

Now after sending the SMS content to a certain destination using port number 50000 we see that the destination receiver receives the content encrypted & the received object is cipher text.



```
WMA Console running, using phone number +5550001.
Received sms message from sms://+5550000 on port 50000:
□:((*y□&$7
```

After that the sender receives a confirmation that vote has been successfully cast.



+5550000 - DefaultC...

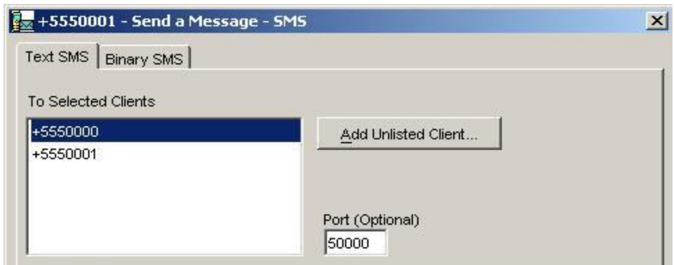
MIDlet

Status:

Send: Awami Boat

Exit Send

Now to prove that the cipl operly, we use a roll back mechanism swapping the sender to receiver and the receiver to sender. We use again the same port number 50000 and now send the cipher text to the destination number as +555 000 0.



+5550001 - Send a Message - SMS

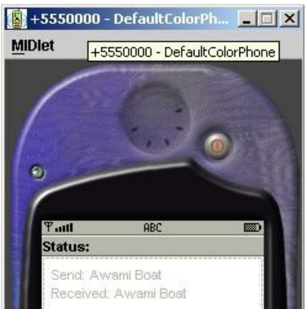
To Selected Clients

+5550000

+5550001

Port (Optional)

50000



+5550000 - DefaultColorPh...

MIDlet

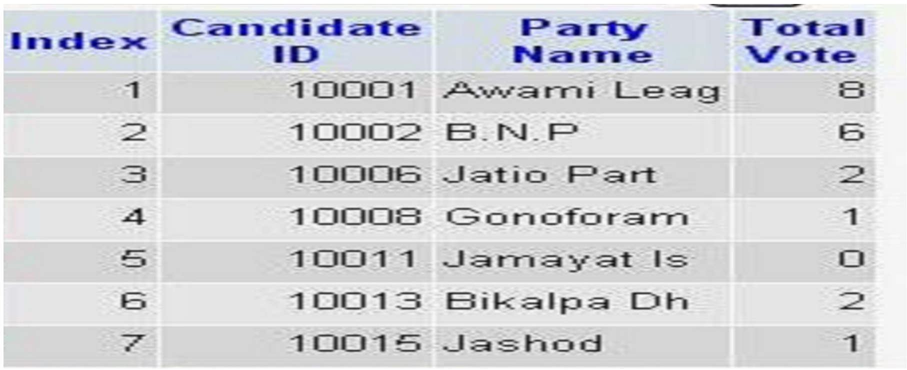
+5550000 - DefaultColorPhone

Status:

Send: Awami Boat

Received: Awami Boat

So we see that the receiver confirms the result that the same content has been sent again, which clearly shows that the content of the SMS is successfully encrypted and also decrypted.

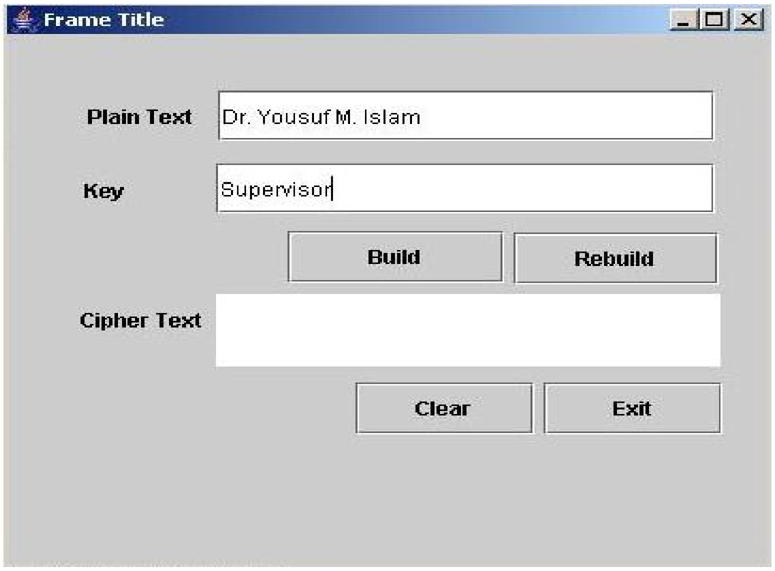


Index	Candidate ID	Party Name	Total Vote
1	10001	Awami Leag	8
2	10002	B.N.P	6
3	10006	Jatio Part	2
4	10008	Gonoforam	1
5	10011	Jamayat Is	0
6	10013	Bikalpa Dh	2
7	10015	Jashod	1

The above figure represents the result of the election of particular one polling booth as we considered only one polling booth. There is a simple database which would simply count the votes for candidates participating in the election from one station. This is a simple demonstration of how the voting is going to be counted.

4.3 Acceptance testing

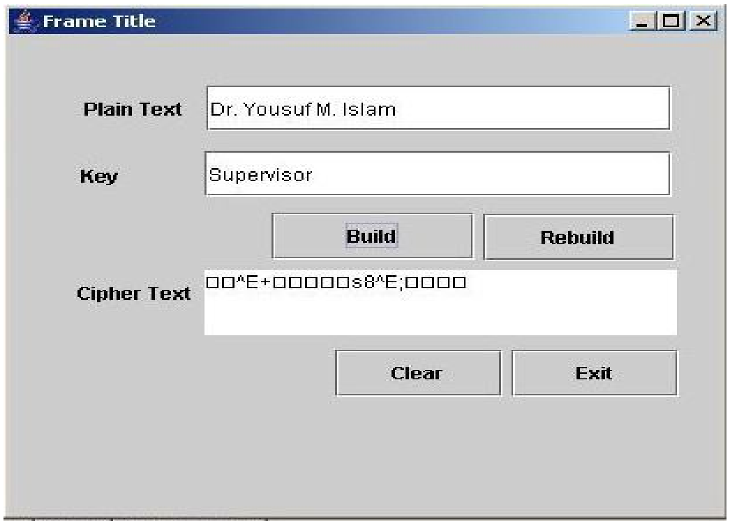
Before we build the real encryption software for mobile application we have to test the software in JbuilderX (J2ME wireless toolkit 2.0). First we have implemented the encryption software having a user interface. We have to write the plain text in the plain text field and the key in the key field.



Plain Text: Dr. Yousuf M. Islam

Key: Supervisor

In the interface when we press the button “Build” it creates the cipher text using the plain text and Key.

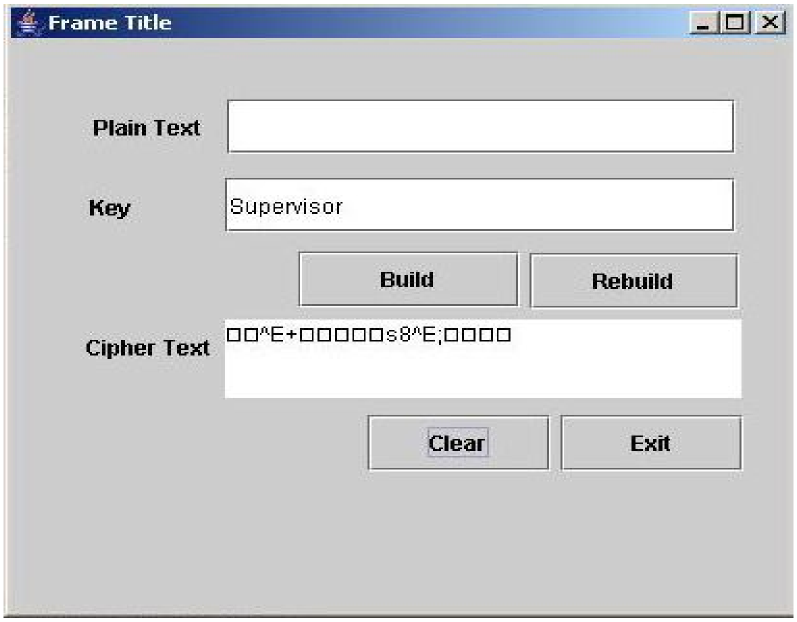


Plain Text Dr. Yousuf M. Islam

Key Supervisor

Cipher Text □□^E+□□□□□s8^E;□□□□

Cipher text will show in the interface.
After we get the cipher text then we press the clear button to clear the plain text area field.

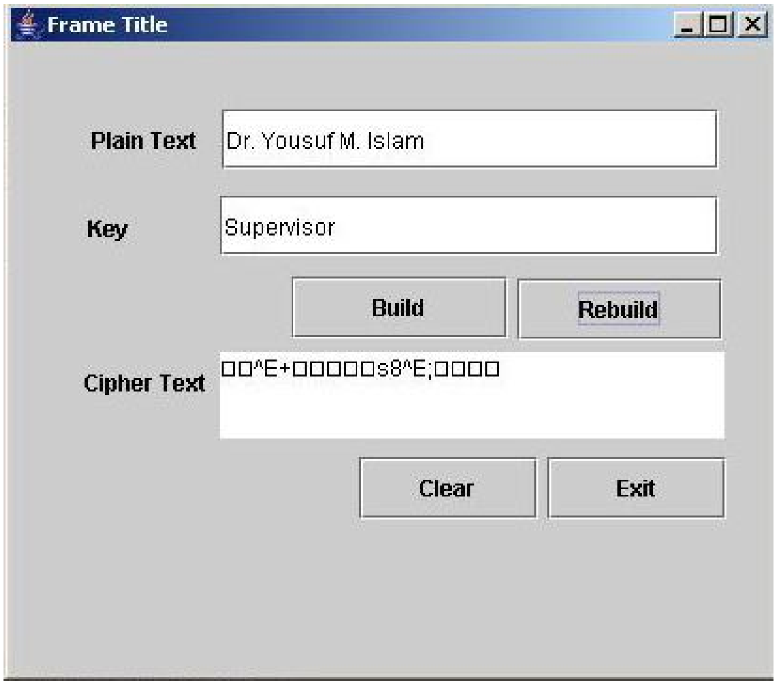


Plain Text

Key Supervisor

Cipher Text □□^E+□□□□□s8^E;□□□□

Finally when we press the Rebuild button it builds the plain text using the same key and cipher text.



Plain Text: Dr. Yousuf M. Islam

Key: Supervisor

Cipher Text: □□^E+□□□□□s8^E;□□□□

4.4 Test Data

Some manual inputs and outputs of our proposed system are shown below:

Plain text	KEY	Cipher text
BANGLADESH	YMIECLIUERN	SS]SYWUW@\
BNP PADDY	YMIECIEMX	s|c□ewuvj
AL BOAT	YMIECWZO	P~□vzwe
JP PLOUGH	YMIECIUBX	{b□dyydu{
BIKOLPO DHARA	YMIECNHGREQSP	s{x{yf~□w|tdp
BU JRC	YMIECO	sg□~gu
CSE DEPT	YMIECBVC	rav□qsaf
JAMAT DARIPALLA	YMIECPLMNJIYGVC	{s~ua□usa}ew}~r
THESIS IN BRAC UNIVERSITY	YMIECKSNZUSUSJIK JDJDIQXDUNOP	ezvg|e□{}□wdpq□a{ □gwag|bh
NATIONAL ELECTION OF BANGLADESH	YMIECKDZMHEKKUD LKIAICNQIUQZKUDKE	□sg}zxp~□qysrfz{ {□~t□vtxv~rppey

4.5 Results

We have tested the unity and integrity of our software. It encrypts the SMS properly and properly decrypt in the server end. We have tested it using several types of input and we have successfully been able to decrypt all the data. But we have considered only one polling booth database for testing. For a complete testing we have to test in a large scale. It took lots of time for studying and testing encryption algorithms. Due to lack of time we were not able to do the full database of E-voting and complete the whole testing.

CHAPTER 5

USER MANUAL

5.1 Instructions for Administrators

Election Commissioner can only login to Election Commission Server. When she / he logs in to the computer, he will directly go to the E-Voting software. When he presses the count button it automatically counts the result of the National Election. Administrator can see the result and publish the result of voting in the Internet and other media.

5.2 Instruction for Voter

Voters will have to go to the polling booth and authenticate them selves. Then they will find the electronic ballot and a confirmation button. They will have to press the button in the ballot and press the confirmation button. When his or her vote will cast, he or she will receive a status report.

5.3 Instruction for Polling booth officer

Polling booth officer will verify the voter according to the voter list. He will monitor successful vote cast. If any one fails to cast a vote successfully then he or she is given a second chance.

CHAPTER 6

CONCLUSION

The current election system is manual. In this system we found out some major flaws. The system is fully paper based like printing ballot papers and distributing them, high risk of ballot box hijacking in the remote areas, ballot paper is manually counted which requires huge man power. As a result counting errors may occur and it needs recounting, compilation of result requires many stages which is very time consuming. This problems as a whole put a big question mark on the reliability and transparency of the current election system. So we have come up with an electronic voting system which secures the voting procedure. We managed to provide security of the SMS that is the vote carrier of our proposed E-voting system. These provide more security, reliability and efficiency to the system. As our proposed system is easy to implement, initially it can be installed in high risk areas of ballot box hijacking as a pilot project. In a word our solution for the national election system improves the overall efficiency of the current election system by providing secured and simplified processing of election results.

References

1. William Stallings, Cryptography and Network Security.
2. Jeffry A. Hoffer, Joey F. George, Modern System Analysis & Design

3. http://www.cellular.co.za/news_2002/021302-uk_to_use_sms_voting.htm
4. http://www.smartmobs.com/archive/2003/02/07/sms_voting_in_u.html
5. http://www.textually.org/textually/archives/2003/05/000521.htm
6. http://www.telsis.com/0304.htm
7. http://news.zdnet.co.uk/internet/security/0,39020375,39186974,00.htm
8. http://mindprod.com/jgloss/conversion.html
9. http://forum.java.sun.com/thread.jspa?threadID=664309&messageID=3890826
10. http://www.bangladeshgov.org/ecs/
11. http://www.nesc.ac.uk/action/esi/contribution.cfm?Title=639
12. http://www.orlingrabbe.com/des_java.htm
13. http://avirubin.com/vote/
14. http://www.newscientist.com/article.ns?id=dn3987
15. http://www.computerworld.com/governmenttopics/government/policy/story/0,10801,92950,00.html
16. http://www.eff.org/Activism/E-voting/20030723_eff_pr.php
17. http://www.usatoday.com/tech/news/computersecurity/2004-07-30-evote-hack-challenge_x.htm
18. http://www.mbalance.com/products/security/firewall.aspx
19. http://www.oreillynet.com/pub/a/wireless/2001/09/28/relay.html
20. http://www.mcafee.com/us/local_content/white_papers/wp_sms_architecture.pdf
21. http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t13/ft_aes.htm
22. http://www.pentazip.com/PW/PentaSuite_Security.htm
23. http://www.abisoft.net/dev.html
24. http://www.thefreecountry.com/sourcecode/encryption.shtml
25. http://www.schneier.com/blowfish.html
26. http://www.eweek.com/article2/0,1759,1859751,00.asp
27. http://www.tero.co.uk/des/