International Journal of Engineering Research and Development
e-ISSN: 2278-067X, p-ISSN: 2278-800X, www.ijerd.com
Volume 10, Issue 3 (March 2014), PP.23-30

GSM Based Navigation of Missile

Raju, Rahul, Y.V.Chavan
Maharashtra Academy of Engineering, Alandi (D),

Abstract:- Use of advanced technology in most of the applications is always being attraction with its simplicity, affordability and utility. This should also be supported by the security. All these issues thought together in this paper, the work has been done in two parts. In the first part the command processing for the navigation for fixing the angle and position, while in the second part these commands are needed to be send to the remote places using GSM [7] technology with security, and actual execution of these command. The security is achieved by using RC4 algorithm. For the GSM a pair of Nokia- 6070 is used. For processing of the commands (AT commands) the back end programming is done in Visual Basic at the transmitter and 89c51 is at the receiver end for decoding the AT commands for execution.

Keywords:- GSM, RC4 algorithm, AT commands for GSM, programming AT commands.

I. INTRODUCTION

Any information, which is to be send, needs its sanctity to be maintained.

The Cryptography is the best available technique from ancient time. For such thing Cryptography has great importance in data security. ‘Crypto ‘means secret and ‘graphy’ means writing. Many cryptographic algorithms evolved based on need and available communication equipments [3], Figure 1 shows the block diagram of the Conventional Cryptography (Encryption). The capability of retrieving the information on the other side was purely based on the authorized key. Decoded text is called same as plain text/message.

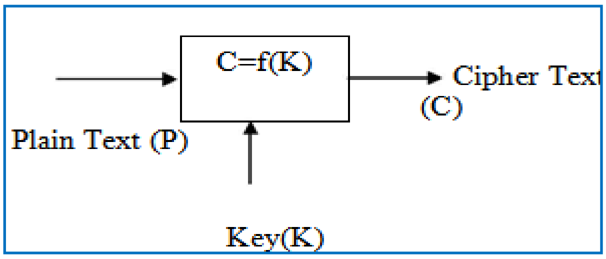


Figure 1: Block Diagram for conventional Cryptography

Data encryption is utilized in various applications and environment [2].

There are different types of algorithms used for data encryption some of them are Rivest, Shamir and Adleman RSA, Digital Signature algorithm, DSA, Data Encryption Standard DES [4]& Ron’s code RRC4 Algorithmis symmetric key algorithm in which same key is used for encryption and decryption. While RSA, DSA are asymmetric key algorithms in which different keys are used for encryption and decryption. Hence for simplified data communication we are using RC4 algorithm. In this paper we are using cryptography for the commands to be given for controlling the missile position from remote place using GSM technique.

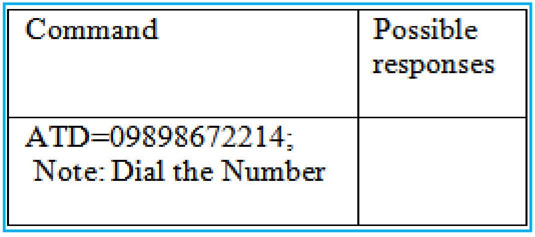
The specific utilization of encryption and the implementation of the RC4 will be based on many factors particularly on the computer system and its associated components. The next section gives the details of the commands used for the system.

II. GSM MODEM AT COMMANDS

AT (Attention Commands), the different AT commands used and referred to interface a 8-bit microcontroller system (89C51) are listed below. These commands are required at the receiving end to decode the messages for the angle and position of the missile.

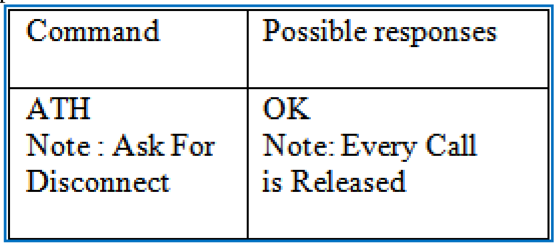
AT Commands

1) Dial Number D Syntax:
Command syntax: ATD=<nb>; Function:
This command allows the application to dial a phone number.



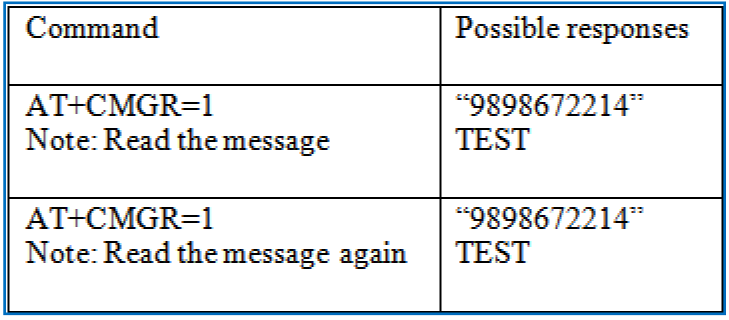
Command	Possible responses
ATD=09898672214; Note: Dial the Number	

2) Hang Up Call H Syntax:
Command syntax: ATH Function:
This command allows the application to disconnect a remote user.



Command	Possible responses
ATH Note : Ask For Disconnect	OK Note: Every Call is Released

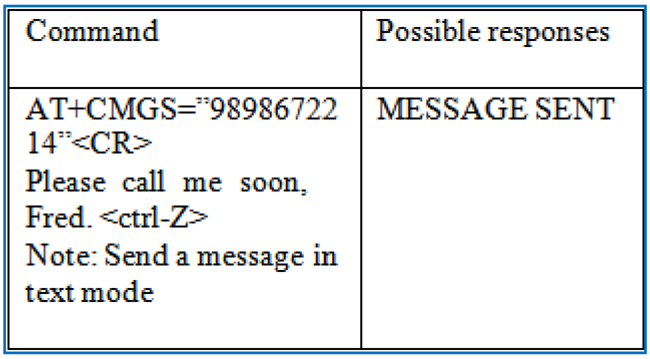
3) Read message +CMGR Syntax:
Command syntax: AT+CMGR=<index> Function
This command allows the application to read stored messages. The messages are read from the memory.



Command	Possible responses
AT+CMGR=1 Note: Read the message	"9898672214" TEST
AT+CMGR=1 Note: Read the message again	"9898672214" TEST

4) Send message +CMGS Syntax:
Command syntax in text mode: AT+CMGS= <da> [,<toda>] <CR> Text is entered <ctrl-Z / ESC > Function:

The <address> field is the address of the terminal to which the message is sent. To send the message, simply type, <ctrl-Z> character (ASCII 26). The text can contain all existing characters except <ctrl-Z> and <ESC> (ASCII 27).



Command	Possible responses
AT+CMGS="9898672214"<CR> Please call me soon, Fred. <ctrl-Z> Note: Send a message in text mode	MESSAGE SENT

1. RC4 ALGORITHM [1]: Ronald Rivest of RSA has developed RC4 algorithm, which is a shared key stream cipher algorithm. In this a secure exchange of a shared key is the basic requirement. The algorithm is used identically for encryption and decryption as the data stream is simply XOR'ed with the generated key sequence. The algorithm is serial as it requires successive exchanges of state entries based on the key sequence. Hence implementations can be computationally very intensive. This algorithm has been released to the public and is implemented by many programmers. This encryption algorithm is used by standards such as IEEE 802.11

within WEP (Wireless Encryption Protocol) using a 40 and 128-bit keys. In the algorithm the key stream is completely independent of the plaintext used. An 8 * 8 Substitution, S-Box (S 0- S255), where each of the entries is a permutation of the numbers 0 to 255. The permutation is a function of the variable length key.

Features

1. Uses a variable length key from 1 to 256 bytes to initialize a 256-byte state table. The state table is used for subsequent generation of pseudo-random bytes and then to generate a pseudo-random stream which is XOR'ed with the plaintext to give the cipher-text. Each element in the state table is swapped at least once.

2. The key is often limited to 40 bits, because of export restrictions but it is sometimes used as a 128 bit key. It has the capability of using keys between 1 and 2048 bits. RC4 is used in many commercial software packages such as Lotus Notes and Oracle Secure SQL.

The algorithm works in two phases, key setup and ciphering. Key setup is the first and most difficult phase of this encryption algorithm. During N-bit key setup (N being your key length), the encryption key is used to generate an encrypting variable using two arrays, state and key, and N-number of mixing operations. These mixing operations consist of swapping bytes, modulo operations, and other formulas. A modulo operation is the process of yielding a remainder from division. (For example, 11/4 is 2 remainder 3; therefore eleven mod four would be equal to three).

- Symmetric key Algorithm
- Stream Cipher Algorithm
- 4-bit IV appended to 40-bit key
- XOR Key stream with plaintext = Encrypted Text
- Key stream is independent of plaintext

Algorithm Strengths

- It is difficult to hackers about knowing where value is in the table.
- The difficulty of knowing which location in the table is used to select each value in the sequence.
- A particular RC4 Algorithm key can be used only once.
- Encryption is about 10 times faster than DES.

Implementation

- **Two main parts:**

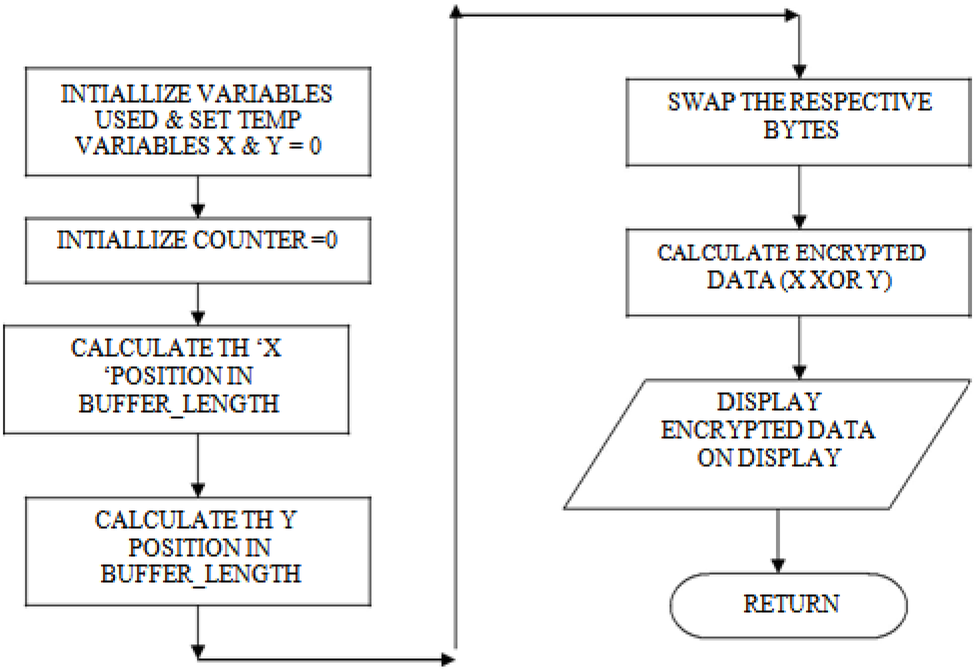
KSA (Key Scheduling Algorithm)
PRGA (Pseudo Random Generation Algorithm)

- RC4 = Ron?s code # 4 or Rivest
- Cipher = a cryptographic algorithm used for encryption and decryption.
- Symmetric key algorithm = an algorithm that uses the same key to encrypt and decrypt
- Stream cipher = algorithm that encrypts data one byte at a time
- Anonymous re-mailer =distribution system that strips off all of the sender information and re-mails the message under an anonymous name.
- State table: is a table initialized from 1 to 256 bytes. The bytes in the table are used for subsequent generation of Pseudo-Random bytes. The Pseudo-Random stream generated is XOR'ed with the plaintext to give the cipher-text.

- The RC4 encryption algorithm is used to encrypt and decrypt text files. This algorithm uses a key, with a maximum size of 256 elements, and a state array of 256 elements, to generate an encryption variable array that is used to encrypt the data. The key array consists of a random sequence of numbers. The state array consists of an array starting at 1 and going to 256.

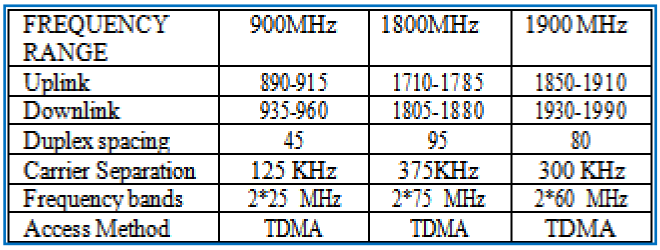
- The encryption variable array is generated using the key array and the state array. Generating the encryption variable array starts by permuting the state array based on the key array. This is accomplished by adding the [0] element of the key array and the state array, Mod 256. This produces a number "f" that is used as an index to the state array. The [f] element and the [0] element of the state array are swapped. Then the process starts again but this time beginning with the [1] element of the key array and state array. This continues to the [255] element of the key array and state array. Next take the [1] element of the state array and add zero to it, Mod 256. Use this number as an index to the state array and swap that element of the array with the [0] element of the state array. After swapping add these two elements together mod 256 to create the index [t]. Use the [t] element of the state array as the [0] element of the encryption variable array.

- To encrypt data the first byte of the data is XOR'ed with the first element of the encryption variable array. Then the second byte of data is XOR'ed with the second element of the encryption variable array. Continue in this fashion until all the data is encrypted.
- To decrypt data a similar process is used. The same key used for encryption must be used for decryption. The key array, state array, and encryption variable array are initialized in the same manner as used for encryption. The encrypted data is XOR'ed with the encryption variable array in the same manner as used in encryption and this will decrypt the original data.
- The sender A then transmits a message to the missile in the following kind of format:
  Encrypted key = ****
  Plaintext encrypted with key =
- At the receiver the encrypted message is extracted with help of same key. Typically the transmission includes plaintext, details of the encryption algorithms used, padding and encoding methods, initialization vectors and other details required by the recipient. The only secret required to be kept, as always, should be the keys.
- If there is intercept of transmission, it can either try and crack the conventionally - encrypted plaintext directly, or try and decrypt the encrypted key and then use that in turn. In the next section we will see how the GSM [8] can be useful for the system.


INTIALLIZE VARIABLES USED & SET TEMP VARIABLES X & Y = 0
INTIALLIZE COUNTER =0
CALCULATE TH 'X 'POSITION IN BUFFER_LENGTH
CALCULATE TH Y POSITION IN BUFFER_LENGTH
SWAP THE RESPECTIVE BYTES
CALCULATE ENCRYPTED DATA (X XOR Y)
DISPLAY ENCRYPTED DATA ON DISPLAY
RETURN

Flowchart for RC4 algorithm for coding of missile angle and position to detect.

2. GSM SPECIFICATION



FREQUENCY RANGE	900MHz	1800MHz	1900 MHz
Uplink	890-915	1710-1785	1850-1910
Downlink	935-960	1805-1880	1930-1990
Duplex spacing	45	95	80
Carrier Separation	125 KHz	375KHz	300 KHz
Frequency bands	2*25 MHz	2*75 MHz	2*60 MHz
Access Method	TDMA	TDMA	TDMA

GSM characteristics

- Fully digital system using 900, 1800 MHz frequency band.
- TDMA over radio carriers (200 KHz carrier spacing.
- 8 full rate or 16 half rate TDMA channels per carrier.
- User/terminal authentication for fraud control.
- Encryption of speech and data transmission over the radio path.

- Full international roaming capability.
- Low speed data services (up to 9.6 Kb/s).
- Compatibility with ISDN.
- Support of Short Message Service (SMS).
-

2. Interfacing mobile with system:

At transmitter and receiver pair of mobile is used, at transmitter it is operated through GSM AT COMMANDS and at receiver it is interfaced with microcontroller through USB connector.

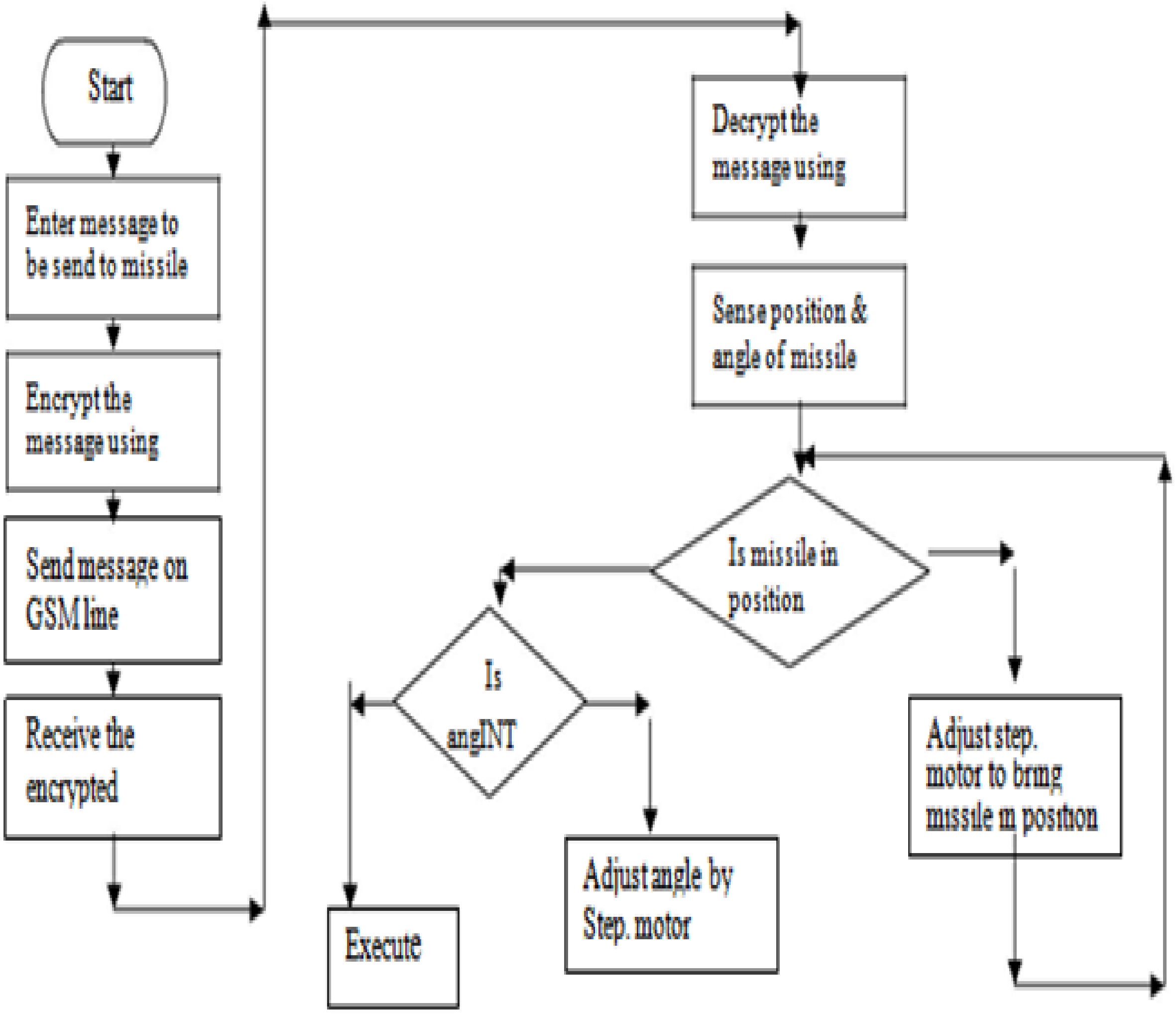

Start
Enter message to be send to missile
Encrypt the message using
Send message on GSM line
Receive the encrypted
Decrypt the message using
Sense position & angle of missile
Is missile in position
Is angINT
Execute
Adjust angle by Step. motor
Adjust step. motor to bring missile in position

Figure 2 A Complete system flow chart for Navigation using GSM

4. Microcontroller 89c51:

The requirement of the system is to receive and transmit the messages from the memory with handshaking and supporting the GSM[5]. The memory requirement is also limited for them on or for program routines. The Microcontroller 89c51 is suitable for this application Features:

1. Compatible with MCS-51™ Products

2.4K Bytes of In-System Reprogrammable Flash Memory

3. Fully Static Operation: 0 Hz to 24 MHz 4.Three-level Program Memory Lock 5.128 x 8-bit Internal RAM

6. 32 Programmable I/O Lines 7.Two 16-bit Timer/Counters 8.Six Interrupt Sources
9.Programmable Serial Channel

This has routines for: Reading the message, sending the message for positioning the missile
The system takes care for authentic user by unlocking the system. The communication is done through RS-232 cable for handshaking.

5. Stepper Motor:

Stepper motor is an electro mechanical device, which receives electrical pulses for the mechanical movements. The shaft or spindle of a stepper motor rotates indiscrete step increments when electrical command pulses are applied to it in the proper sequence. The motors rotation has several direct relationships to these applied input pulses. The sequence of the applied pulses is directly related to the direction of motor shafts rotation. The speed of the motor shafts rotation is directly related to the frequency of the input pulses and the length of rotation is directly related to the number of input pulses applied.

Advantages:

1. The rotation angle of the motor is proportional to the input pulse.
2. The motor has full torque at stand still (if the windings are energized)
3. Precise positioning and repeatability of movement since good stepper motors have an accuracy of 3 – 5% of a step and this error is non cumulative from one step to the next.
4. Excellent response to starting/stopping/reversing.
5. Very reliable since there are no contact brushes in the motor. Therefore the life of the motor is simply dependant on the life of the bearing.
6. The motors response to digital input pulses provides open-loop control, making the motor simpler and less costly to control.
7. It is possible to achieve very low speed synchronous rotation with a load that is directly coupled to the shaft.
8. A wide range of rotational speeds can be realized, as the speed is proportional to the frequency of the input pulses.

Disadvantages:

1. Resonances can occur if not properly controlled.
2. Not easy to operate at extremely high speeds.

III. CONCLUSION

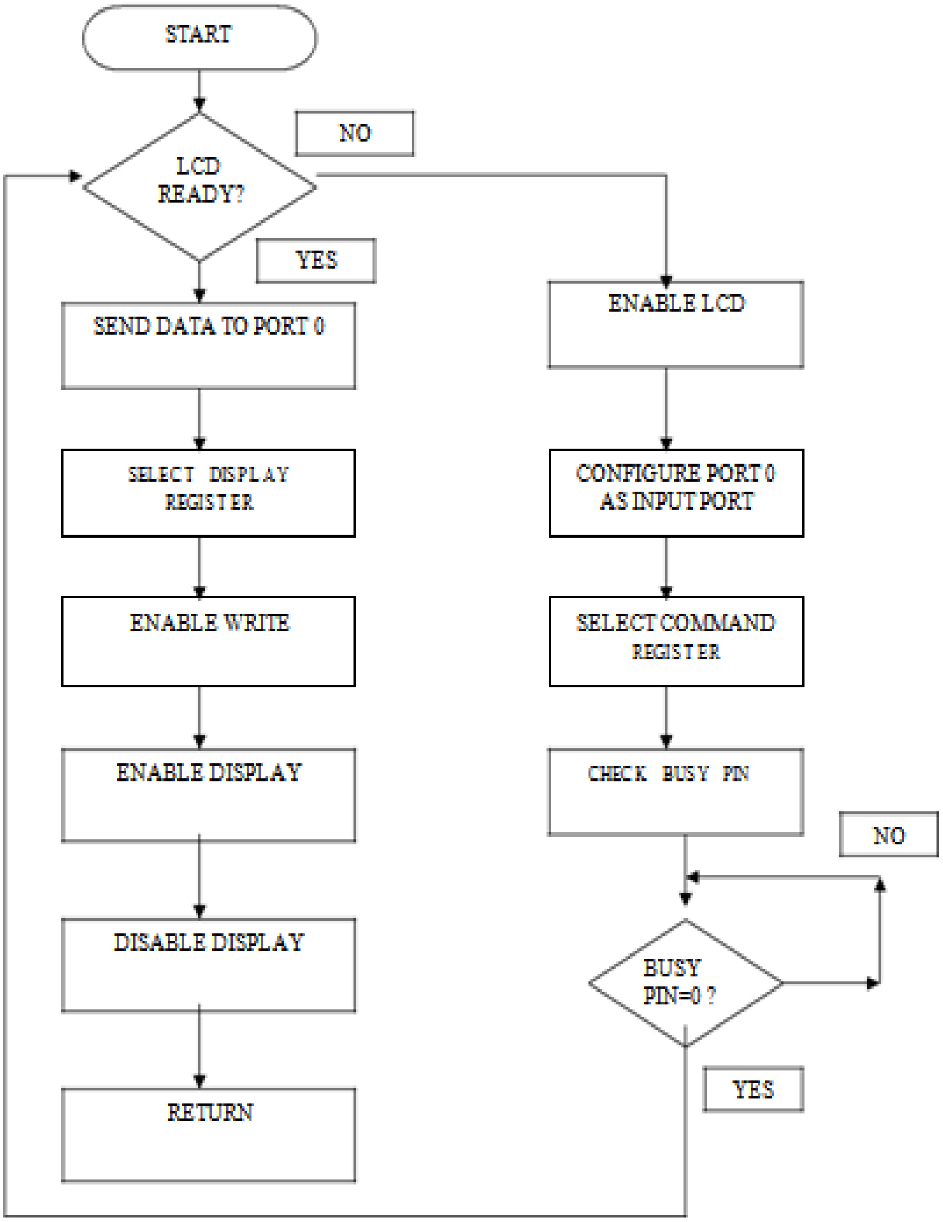
The growing use of networking is generating tremendous amount of various application for data that are transmitted at high speeds over long distances. These security aspects include determining the types of attacks that might be launched on a computer system or network, and using various protection mechanisms against these attacks to ensure the validity of information. The system implemented here uses the GSM with the help of Nokia 6070. The security issue is handled by using RC4. The coding of the command for the position and angle of the missile is done by the back end VB. The decoding at the receiver is done by 80c59 and execute with movement of the stepper motor. The system here is implemented with GSM, AT command by VB, RC4 and 80c59[6]. This can also be implemented by any other combination for the desired results and application.

The weakness of the systems are:

– 40-bit key and Shared
– Pseudorandom- IV based
– Key stream reuse
– XOR based
– Weak Keys

- One in every 256 keys can be a weak key. These keys are identified by cryptanalysis that is able to find circumstances under which one of more generated bytes are strongly correlated with a few bytes of the key.

WEAK KEYS: these are keys identified by cryptanalysis that is able to find circumstances under which one or more generated bytes are strongly correlated with small subset of the key bytes. These keys can happen in one out of 256 keys generated.



Flowchart for display of command angle and position at the receiver side using LCD display.

REFERENCES

[1]. Allam Mousa and Ahmad Hamad“Evaluation of RC4 Algorithm for Data Encryption”

[2]. Bruce Schneier “Applied cryptography (Protocols and Algorithms)”

[3]. Chavan Y.V. “Computer Networks”, second edition Umesh publication Delhi Federal Information Processing Standards (FIBS PUB) Research paper on “Data Encryption standard”

[4]. Kenneth J. Ayala “The 8051 Micro controller Architecture”

[5]. M.A. Mazadi “The 8051 Micro controller and Embedded Systems”

[6]. Rohan Mehta, Y.V. Chavan , V.K. Sharma “Implementation of Modified RSA Algorithm For Security Socket Layer In Virtual Private Network”at the National Conference for Broadband Communication system organized by VIIT, Pune

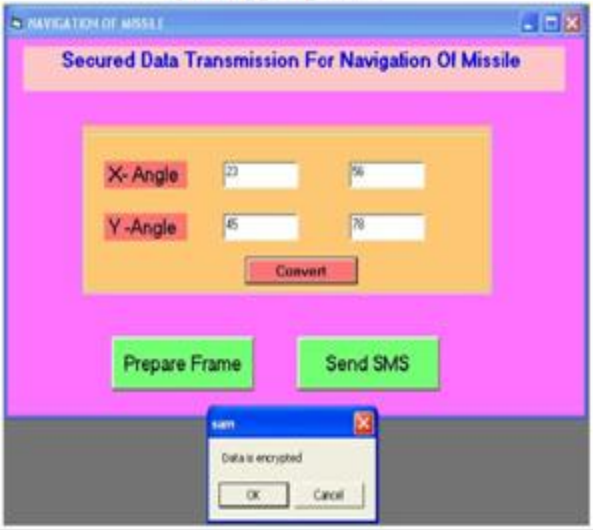
[7]. S. Muhammad Siddique, Muhammad Amir, ‘‘GSM security issues and challenges,’’ 7thACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing, SNPD 2006, 19-20 June 2006, pp. 413 – 418.

[8]. Andrew S. Tanenbaum, Computer Networks, Fourth Edition, Prentice Hall, 2003

Annexure

Front end page developed using VB (GUI)

1] Encrypting data:

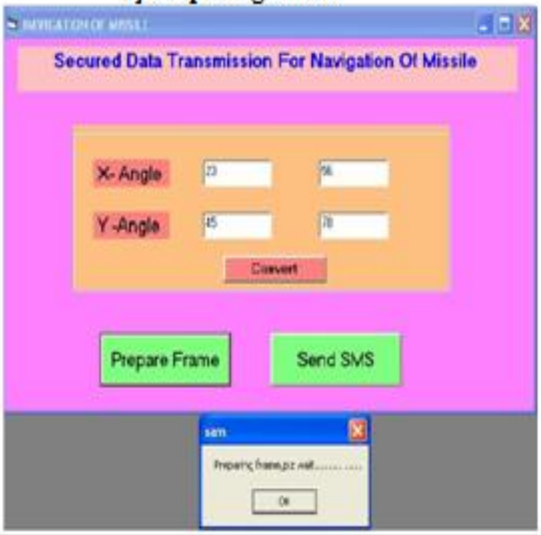


X- Angle 23 56

Y -Angle 45 78

Data is encrypted

2] Preparing frame

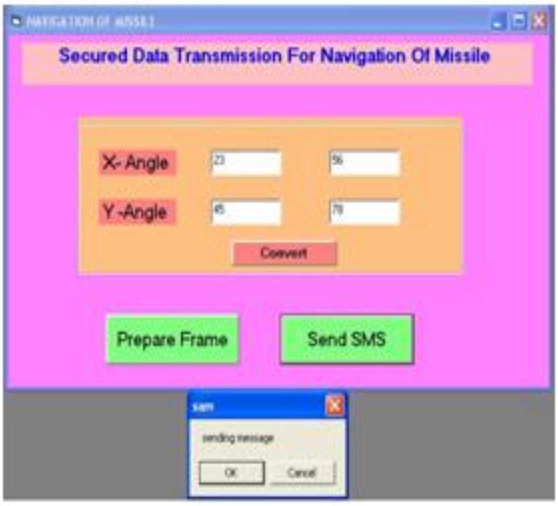


X- Angle 23 56

Y -Angle 45 78

Preparing frame,pz wait.........

3] Sending message:



X- Angle 23 56

Y -Angle 45 78

sending message