Secure Navigation of Missile through Wireless Communication Using IDEA Algorithm

Prof. Anuradha S. Deshpande[1], Omkar D. Cherekar[2], Aniket S. Patil[3], Abhijeet S. Patil[4]

Abstract— **Data security has the first preference for every communication system. There are many ways to secure the data that is being communicated. In D-day, security from hackers has more importance in wireless communication .This project describes the design of effective security for data communication by designing standard algorithm for encryption and decryption. The input information is generated by a key pad and this will be encrypted and transmitted through RF communication. The receiver will check the data and decrypt it according to a IDEA algorithm and displays on LCD. IDEA algorithm has more efficiency and security for real time processing. It can be efficiently implemented in both software and hardware. We have designed an encryption system based on the IDEA algorithm on ARM 7.**

Index Terms—**Encryption, Decryption, Secret Key, IDEA, GUI**

I. Introduction

Precision guided weapons have played an increasingly major role in recent conflicts and much media attention has been focused on the surgical precision provided by modern high-tech weapons. However, the concepts behind today's guided weapons are used in the Second World War and in some cases even to the First World War. It is, however, clear that the technological progress has only recently made it possible to work on the concept of guided weapons.

In today's world, enemy conflict is an essence factor of any nation's security. The national security mainly depends on army (ground), navy (sea), air-force (air).The important and major role is played by the army's artillery such as scud missile

We design and realize an encryption model which is based on the IDEA algorithm on ARM 7, which can encrypt and decrypt the information in many kinds of network.

There are many security algorithms which are used for security purpose. IDEA is one of the most secure algorithm which provides security. The block cipher IDEA uses 64-bit plaintext and cipher text blocks and 128-bit secret key. The fundamental excogitation this algorithm is the use of operations from three different algebraic groups. The algorithm is used in such a way that different key sub-blocks are used, the encryption process is similar to the decryption process.

II. Literature Survey

The weapons can be divided into two major categories, Go-Onto-Target (GOT) and Go-Onto-Location-in-Space (GOLIS). A GOT missile has ability to target on either a moving or a fixed target, whereas a GOLIS weapon has ability to target on a stationary or a near-stationary target.

These guidance systems uses the radars and a radio or wired link communication between the control point and the missile

The missile tracker is on the control unit. These missiles are totally controlled by the control unit which sends all control orders to the missile

When this control information transmitted to the missile, information need to be secured. So we introduce a encryption based system for transmission of secured control information

The Symmetric key algorithms are computationally faster than asymmetric key algorithm. In practice, symmetric key algorithms are nearly hundreds to thousands times faster than asymmetric key algorithms. Symmetric Key algorithms have lower overload on system resources.

DES- DES is an outdated version of cryptography which uses 64-bit block cipher and 56-bit secret key. It is highly insecure and unreliable and hence it will get replaced by 3DES.

3DES- 3DES is the next version of DES but is still outdated and slow. It uses three separate 56-bit keys for an effective key length. 3DES is computationally slower by today's standards and would not be practically useful in encrypting the large files.

RSA- RSA has longest encryption time and also memory inefficient.

In the case of change in data type such as image instead of text, it was found that IDEA has benefit over RC4, RC2 and Blowfish algorithm in terms of time consumption.

IDEA is a block cipher; it uses 64-bit plaintext blocks. The key is 128 bits long. The same algorithm is used for both encryption process and decryption process.

The design philosophy behind the algorithm is accumulation of operations from different algebraic groups. Three algebraic groups are being accumulated, and they are all easily implemented in both hardware and software. All these operations (there are no bit-level permutations) uses 16-bit sub-blocks. This algorithm is even compatible to 16-bit processors.

III. LOCK DIAGRAM

A. *Transmitter-*

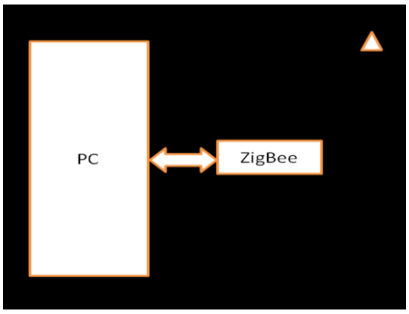


Fig.1 Block diagram of transmitter

B. *Receiver-*

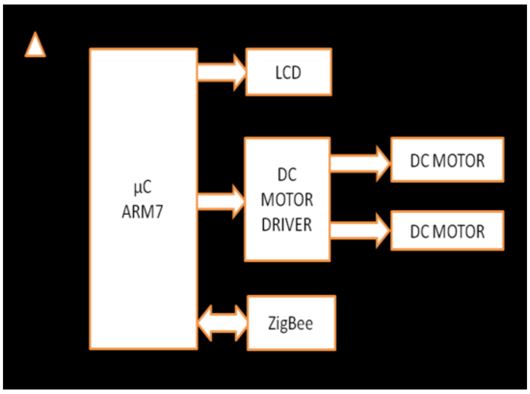


Fig.2 Block diagram of receiver

C. *Block diagram description–*

Transmitter will transmit the data by doing encryption operation through ZigBee

Receiver will receive the encrypted data via ZigBee & decrypt it. The decrypted data will displayed on LCD according to which DC motor Rotate.

.

IV. ALGORITHM

A. *Encryption-*

IDEA does an encryption of a 64-bit block of plaintext to 64-bit block of ciphertext. It operates on 128-bit key. The algorithm consists of eight similar rounds and a “half” round in final transformation.

The algebraic idea behind IDEA is the accumulation of three incompatible algebraic operations on 16-bit blocks: bitwise XOR, addition modulo 216, and multiplication modulo 216 + 1.

For each of the eight complete rounds, the 64-bit plaintext block is split into four 16-bit sub-blocks: P1, P2, P3, P4. The 64-bit input block is the concatenation of the subblocks: P1||P2||P3||P4, where || denotes concatenation.

The 128-bit key is divided into eight 16-bit blocks, which forms eight subkeys.

1. Multiplication of P1 and the first subkey Z1.
2. Addition of P2 and the second subkey Z2.
3. Addition of P3 and the third subkey Z3.
4. Multiplication of P4 and the fourth subkey Z4.
5. The results of steps 1 Bitwise XOR with step 3.
6. The results of steps 2 Bitwise XOR with step 4.
7. Multiplication of the result of step 5 and the fifth subkey Z5.
8. Addition of the results of steps 6 and step 7.
9. Multiplication the result of step 8 and the sixth subkey Z6.
10. Addition of the results of steps 7 and step 9.
11. The results of steps 1 Bitwise XOR with step 9.
12. The results of steps 3 Bitwise XOR with step 9.
13. The results of steps 2 Bitwise XOR with step 10.
14. The results of steps 4 Bitwise XOR with step 10.

Except the final transformation, swap occurs for every rou, and the input to the next round is: result of step 11||result of step 13||result of step 12||result of step 14, which becomes P1||P2||P3||P4, the input for the next round.

After the 8th round, a ninth i.e. half round, final transformation occurs:

1. Multiplication of P1 and the first subkey.
2. Addition of P2 and the second subkey.
3. Addition of P3 and the third subkey.
4. Multiplication of P4 and the fourth subkey.

B. *Key Scheduling-*

Total six subkeys require for complete eight rounds, and the final transformation i.e. half round requires four subkeys; so, the whole process requires total 52 subkeys.

The 128-bit key is divided into eight 16-bit subkeys. Then bits have left shift of 25 bits

The resulting 128-bit string is divided into eight 16-bit blocks which become the next eight subkeys. The same process is repeated until 52 subkeys are generated.

Six subkeys are used in each of the 8 rounds. The final 4 subkeys are used in the ninth i.e. half roundin final transformation.

The shifts of 25 bits will take care that repetition does not occur in the subkeys.

C. *Decryption-*

K^i_J denotes the j-th decryption key of decryption round i.
Z^i_J denotes the j-th encryption key of encryption round i.

For the 1st decryption round:

1. $K^1_1=(Z^5_1)^{-1}$
2. $K^1_2=-Z^5_2$
3. $K^1_3=-Z^5_3$
4. $K^1_4=-Z^5_4$
5. $K^1_5=-Z^5_5$
6. $K^1_6=-Z^5_6$

The decryption keys are similarly generated for all the remaining decryption rounds.

The decryption keys for the final transformation i.e. half round are:

1. $K^1_1=(Z^1_1)^{-1}$
2. $K^5_2=-Z^1_2$

3. $K^{1}_{2}=-Z^{5}_{2}$
4. $K^{5}_{3}=-Z^{1}_{3}$
5. $K^{5}_{4}=(Z^{1}_{4})^{-1}$

V. Conclusion

We have designed an efficient system the secure missile navigation System based on an IDEA algorithm which is an optimized option over other cryptography algorithm like AES & RC4. As compared to other algorithms, IDEA is fast and energy efficient for encryption and decryption.

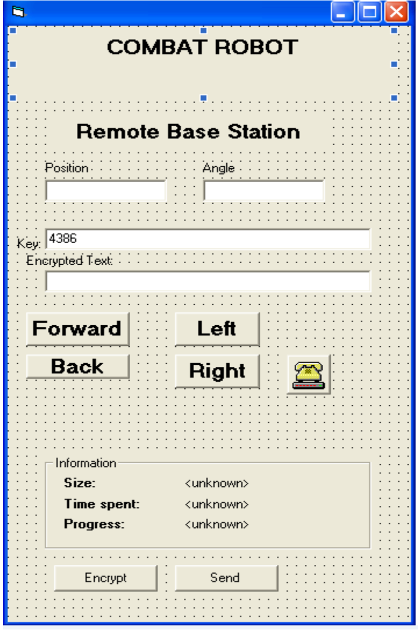
IDEA algorithm is more efficient for real time processing. It is a variable key size stream cipher with byte oriented operations .Moreover, by using IDEA algorithm the transmission of information takes place with enhanced security.

Hence our system will be very useful for secure data transmission.

VI. Result

A. GUI-

GUI stands for Graphic User Interface. Through GUI we are giving angle and position to the missile. Angle and Position are combinely encrypted with secret key and send.



COMBAT ROBOT

Remote Base Station

Position:

Angle:

Key: 4386

Encrypted Text:

Information

Size: <unknown>

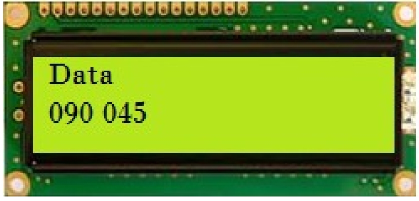
Time spent: <unknown>

Progress: <unknown>

Fig.3 GUI

B. LCD output-

After receiving data, decrypted data is shown on LCD. First three bit reveals angle and last three bit reveals position.



```
Data
090 045
```

Fig.4 LCD output

C. Final model-

Final model includes the LCD, ZigBee at transmitter and receiver side, computer as a transmitter, DC motors attached to chasis etc.

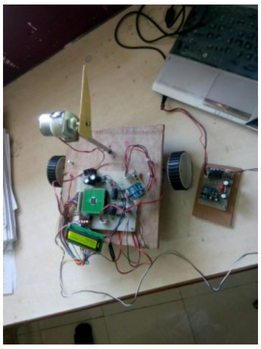


Fig.5 Final model

REFERENCES

[1] Harivans Pratap Singh1, Shweta Verma2, Shailendra Mishra 3, ” Secure-International Data Encryption Algorithm” International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering Vol. 2, Issue 2, February 2013.

[2] Alanazi Hamdan.O., Zaidan B.B., Zaidan A.A., Jalab Hamid.A., Shabbir.M and Al-Nabhani.Y, “New Comparative Study between DES,3DES andAES within Nine Factors” Journal of Computing, Volume 2,Issue 3, March2010, ISSN 2151-9617, pp.152-157.

[3] Salama Diaa, Kader Hatem Abdual, and Hadhoud Mohiy, “Studying the Effects of Most Common Encryption Algorithms” International Arab Journal of e-Technology, Vol. 2, No. 1, January 2011, pp.1-10.

[4] AL.Jeeva, Dr.V.Palanisamy and K.Kanagaram “Comparative Analysis Of Performance Efficiency And Security Measures Of Some Encryption Algorithms” International Journal Of Engineering Research And Applications (IJERA) ISSN: 2248-9622 Vol. 2, Issue 3, May-Jun 2012,Pp.3033-3037.

Prof. Anuradha S. Deshpande,BE ECE, ME Electronics She is an Assistant Professor at JSPM’s ICOER, SPPU. She published “DWT based satellite color image resolution enhancement” Vol. 3 Issue 2 in IJMER

Omkar D. Cherekar, Student of BE ECE at JSPM’s ICOER, SPPU, Pune.

Aniket S Patil, Student of BE ECE at JSPM’s ICOER, SPPU, Pune.

Abhijeet S. Patil, Student of BE ECE at JSPM’s ICOER,SPPU, Pune.