



Designing of an Encryption Technique Suitable For Wireless Ad-Hoc Sensor Network

Mr.Nisarga Chand

E&C Engineering Department
Mallabhum Institute of Technology
India

Mr.Bappaditya Roy

E&C Engineering Department
Mallabhum Institute of Technology
India

Mr.KrishanuKundu

E&C Engineering Department
Birbhum Institute of Engineer & Technology
India

Abstract— In present era sensor networks have gained enough popularity. In every important sector these networks are used to collect information or to transfer them with a high level of security. An Ad-Hoc network generally consists of nodes, on which sensors are embedded to provide security measures. The main challenge of these sensors is to provide security of data and also to work effectively within a limitation of power and memory[1]. Tackling this problem is a great research attention today. In this paper a new public key encryption technique for sensor network has been suggested which is simple as well as a low memory application [2][3]. It is a two stage application. The first stage is to provide confidentiality and the second stage is to provide authentication. In the first stage, Play Fair Cipher matrix has been used with a modification by adding four iteration steps to it. In the second stage, RSA public key encryption technique with ASCII conversion has been used for authentication.[10] Finally, the security strength of the whole system has been analyzed and tried to fulfill the requirement of limited memory space.

Keywords- Ad-Hoc network, Play Fair Cipher matrix, RSA public key encryption, ASCII conversion, Authentication.

I. INTRODUCTION

The **Play fair cipher** or **Play fair square** is a manual symmetric encryption technique and was the first literal digraph substitution cipher[5][9]. The scheme was invented in 1854 by Charles Wheatstone, but bears the name of Lord Play fair who promoted the use of the cipher. The technique encrypts pairs of letters (digraphs), instead of single letters as in the simple substitution cipher. The Play fair is thus significantly harder to break since the frequency analysis used for simple substitution ciphers does not work with it. Frequency analysis can still be undertaken, but on the 600 possible digraphs rather than the 26 possible monographs. The frequency analysis of digraphs is possible, but considerably more difficult – and it generally requires a much larger cipher text in order to be useful. For providing authentication in public key encryption technique, RSA (Rivest-Shamir-Adleman) algorithm, has been used because both public key and private key are used in this technique. Using this RSA algorithm, the plain text message can be converted to cipher text message.

II. IMPLEMENTATION OF PLAY FAIR CIPHER

The Play fair cipher uses a 5 by 5 table containing a key word or phrase. Memorization of the keyword and 4 simple rules was all that was required to create the 5 by 5 table and use the cipher. To generate the key table, one would first fill in the spaces in the table with the letters of the keyword (dropping any duplicate letters), then fill the remaining spaces with the rest of the letters of the alphabet in order (usually omitting "Q" to reduce the alphabet to fit, other versions put both "I" and "J" in the same space)[10]. The key can be written in the top rows of the table, from left to right, or in some other pattern, such as a spiral beginning in the upper-left-hand corner and ending in the center. The keyword together with the conventions for filling in the 5 by 5 table constitute the cipher key. To encrypt a message, one would break the message into digraphs (groups of 2 letters) such that, for example, "Hello World" becomes "**HE LL OW OR LD**", and map them out on the key table. The two letters of the digraph are considered as the opposite corners of a rectangle in the key table. Note the relative position of the corners of this rectangle. Then apply the following 4 rules, in order, to each pair of letters in the plaintext:

- i) If both letters are the same (or only one letter is left), add an "X" after the first letter. Encrypt the new pair and continue. Some variants of Play fair use "Q" instead of "X", but any uncommon monograph will do.
- ii) If the letters appear on the same row of your table, replace them with the letters to their immediate right respectively (wrapping around to the left side of the row if a letter in the original pair was on the right side of the row).
- iii) If the letters appear on the same column of your table, replace them with the letters immediately below respectively (wrapping around to the top side of the column if a letter in the original pair was on the bottom side of the column).
- iv) If the letters are not on the same row or column, replace them with the letters on the same row respectively but at the other pair of corners of the rectangle defined by the original pair. The order is important – the first letter of the encrypted pair is the one that lies on the same row as the first letter of the plaintext pair.

To decrypt, use the INVERSE (opposite) of the first 3 rules, and the 4th as-is (dropping any extra "X"s (or "Q"s) that don't make sense in the final message when finished).

PROCEDURE:-Using "play fair example" as the key, Table becomes:

P	L	A	Y	F
I	R	E	X	M
B	C	D	G	H
K	N	O	Q	S
T	U	V	W	Z

Here we shift the alphabets in such a way that no one can read the code word without knowing the procedure. It is totally for security purpose or prevent from hackers. So the steps are as follows:

Encrypting the message - "HIDE THE GOLD IN THE TREE STUMP": HI DE TH EG OL DI NT HE TR EX ES TU MP

1. The pair HI forms a rectangle, replace it with BM.
2. The pair DE is in a column, replace it with OD.
3. The pair TH forms a rectangle, replace it with ZB.
4. The pair EG forms a rectangle, replace it with XD.
5. The pair OL forms a rectangle, replace it with NA.
6. The pair DI forms a rectangle, replace it with BE.
7. The pair NT forms a rectangle, replace it with KU.
8. The pair HE forms a rectangle, replace it with DM.
9. The pair TR forms a rectangle, replace it with UI.
10. The pair EX (X inserted to split EE) is in a row, replace it with XM.
11. The pair ES forms a rectangle, replace it with MO.
12. The pair TU is in a row, replace it with UV.
13. The pair MP forms a rectangle, replace it with IF.

Thus the message "HIDE THE GOLD IN THE TREE STUMP" becomes "BMODZBXDNABEKUDMUIXMMOUVIF".

ADDITION OF FOUR ITERATION STEPS TO INCREASE THE RANDOMNESS OF THE CIPHER TEXT:-

Here to make the encryption technique more stronger four iteration steps have been introduced. In each step there will be four different keys and the message (for first iteration)/cipher (for rest of the iterations) will be encrypted using the encryption matrix according to the new key [7]. This encryption technique is used only for confidentiality. This technique has been programmed using C Language.

III. IMPLEMENTATION OF RSA ALGORITHM

In cryptography, RSA (which stands for Rivest, Shamir and Adleman who first publicly described it) is an algorithm for public-key cryptography. It is the first algorithm known to be suitable for signing as well as encryption, and was one of the first great advances in public key cryptography. RSA is widely used in electronic commerce protocols, and is believed to be secure given sufficiently long keys and the use of up-to-date implementations. The RSA algorithm involves three steps [4]: key generation, encryption and decryption.

Key generation:

RSA involves a public key and a *private key*. The public key can be known to everyone and is used for encrypting messages. Messages encrypted with the public key can only be decrypted using the private key. The keys for the RSA algorithm are generated the following way:

1. Choose two distinct prime numbers p and q . For security purposes, the integers p and q should be chosen at random, and should be of similar bit-length.
2. Compute $n = pq$. n is used as the modulus for both the public and private keys
3. Compute $\phi(n) = (p - 1)(q - 1)$, where ϕ is Euler's totient function.
4. Choose an integer e such that $1 < e < \phi(n)$ and $\gcd(e, \phi(n)) = 1$, i.e. e and $\phi(n)$ are co prime. e is released as the public key exponent.
5. Determine $d = e^{-1} \pmod{\phi(n)}$; i.e. d is the multiplicative inverse of $e \pmod{\phi(n)}$.

This is often computed using the extended Euclidean algorithm.

d is kept as the private key exponent.

Encryption:

Receiver transmits public key (n, e) to sender and keeps the private key secret. Sender then wishes to send message M to receiver. It first turns M into an integer m , such that $0 < m < n$ by using an agreed-upon reversible protocol known as a padding scheme. He then computes the cipher text c corresponding to

$$c = m^e \pmod{n}.$$

Decryption:

Receiver can recover m from c by using her private key exponent d via computing
 $m = c^d \pmod n$.

Given m , receiver can recover the original message M by reversing the padding scheme.

ADDITION OF ASCII VALUES IN RSA ALGORITHM TECHNIQUE:

In this case, I have to design a complete public key encryption technique for wireless sensor network which provides confidentiality as well as authentication. Here in public key encryption technique, I used the RSA (Rivest-Shamir-Adleman) algorithm, because both public key and private key are used in this technique [4][5].

Using this RSA algorithm, I can convert the plain text message to cipher text message. To make this technique more stronger, I used the ASCII conversion. So using this ASCII value at first, plain text message converted to its corresponding ASCII value, then this value encrypted using RSA algorithm. After that, the encrypted message also decrypted and recovered the original text message using the ASCII conversion again.

IV. FINAL IMPLEMENTATION

Using C language the program has achieved of encryption and decryption confidentiality as well as authentication. At the first stage, plain text message encrypted using the PLAY-FAIR CIPHER MATRIX[5]. To make this technique more strong, four iteration steps have been used here (in fig 1). After completing the four iteration stages, the final cipher text message is achieved. At the second stage, using ASCII code, the final cipher text message is converted into its corresponding numerical value. Then this numbers are again encrypted as well as decrypted using the public key encryption technique i.e.- RSA Algorithm,fig 2. After that the numerical value again converted into text message using ASCII conversion. At the final stage of the program, the decrypted message of the public key encryption technique again decrypted using the PLAY-FAIR CIPHER MATRIX. After the final decryption, the plain text message is achieved fig 3.

V. FLOWCHART

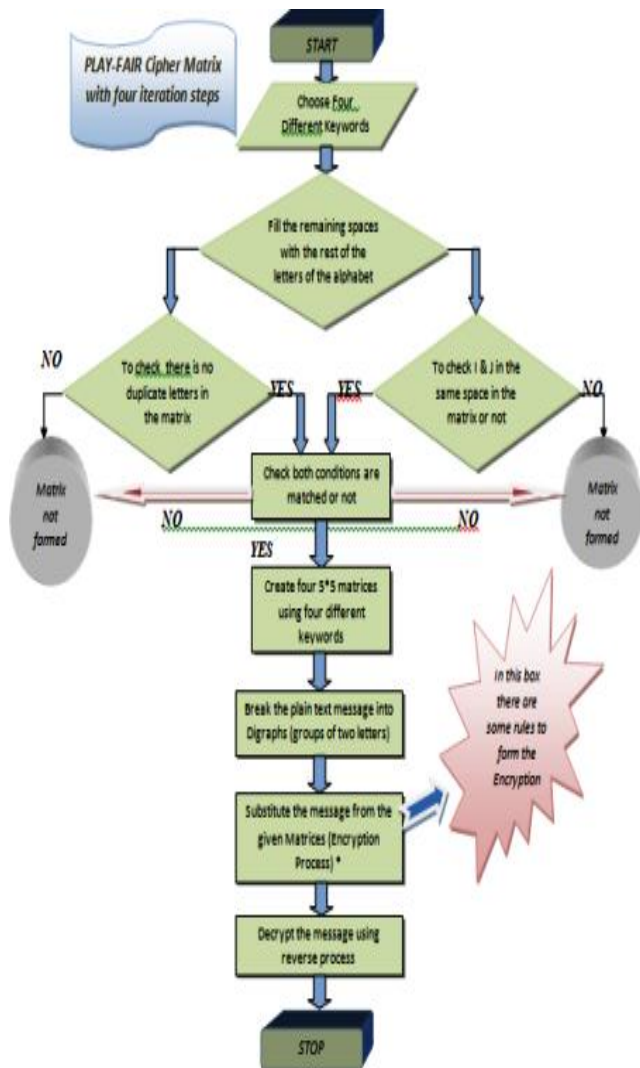


Fig 1.-Play Fair Cipher Matrix with four iteration steps

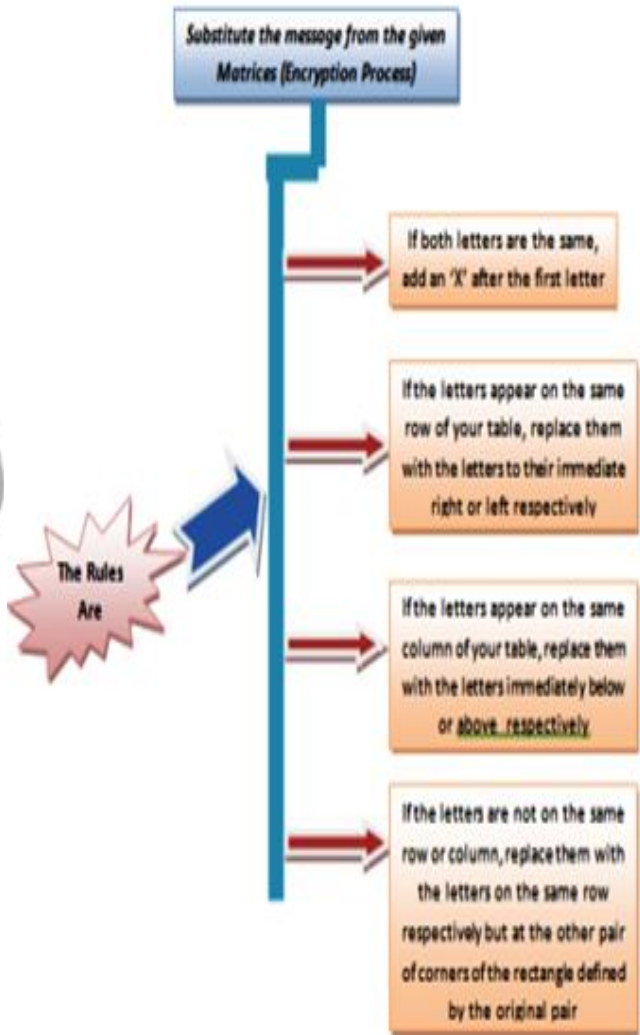


Fig 2.-Rules of the encryption process of Play Fair Cipher Matrix

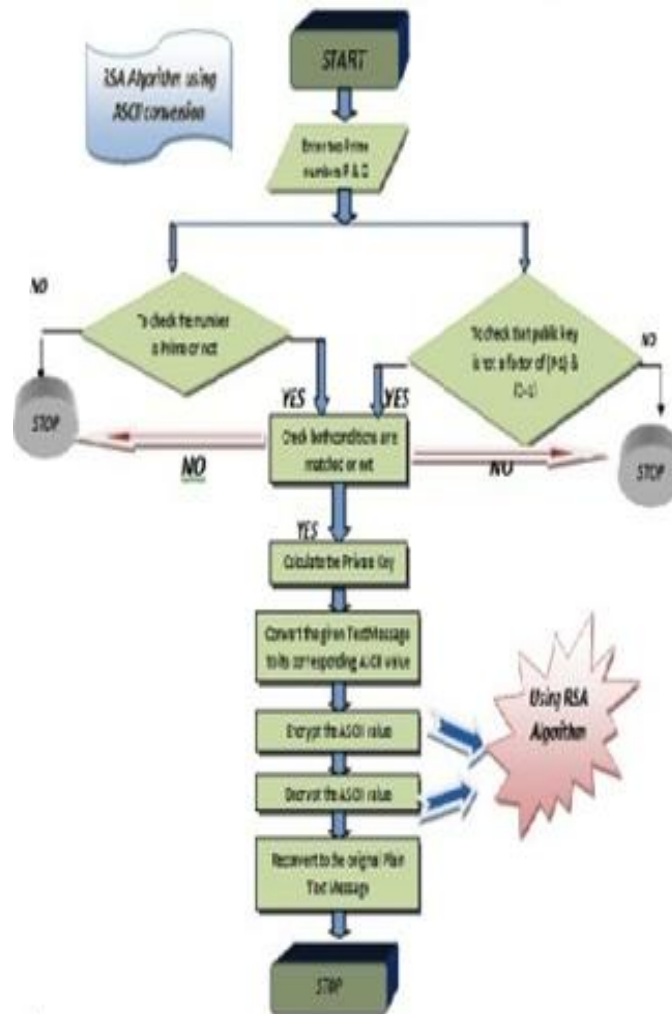


Fig. 3-RSA algorithm with ASCII conversion

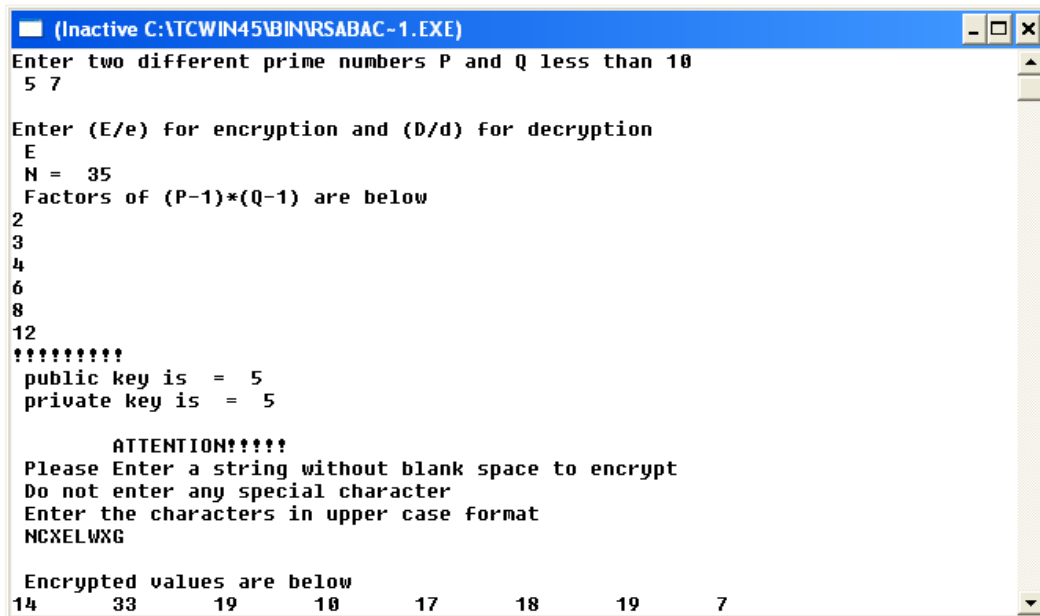
VI. RESULT

- i) Encrypt the message using PLAY- FAIR CIPHER MATRIX:

```

    C:\VC\BIN\ENCRYPT.EXE
    Enter the Message :: STUDENT
    After 1st stage :TLZCGMSZ
    After 2nd stage :UPUHHXZF
    After 3rd stage :EBZBGZMH
    After 4th stage :NCKELWKG
    
```

ii) Encrypt the message using public key encryption technique



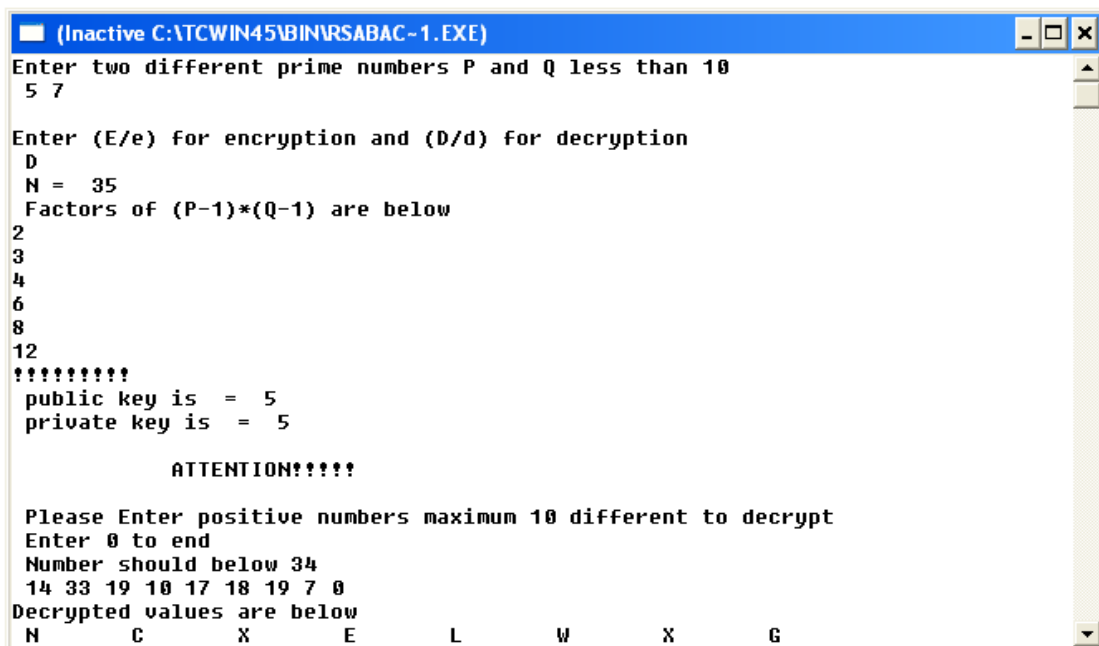
```
(Inactive C:\TCWIN45\BIN\RSABAC-1.EXE)
Enter two different prime numbers P and Q less than 10
5 7

Enter (E/e) for encryption and (D/d) for decryption
E
N = 35
Factors of (P-1)*(Q-1) are below
2
3
4
6
8
12
?????????
public key is = 5
private key is = 5

ATTENTION!!!!
Please Enter a string without blank space to encrypt
Do not enter any special character
Enter the characters in upper case format
NCXELWXG

Encrypted values are below
14 33 19 10 17 18 19 7
```

iii) Decrypt the message using public key encryption technique



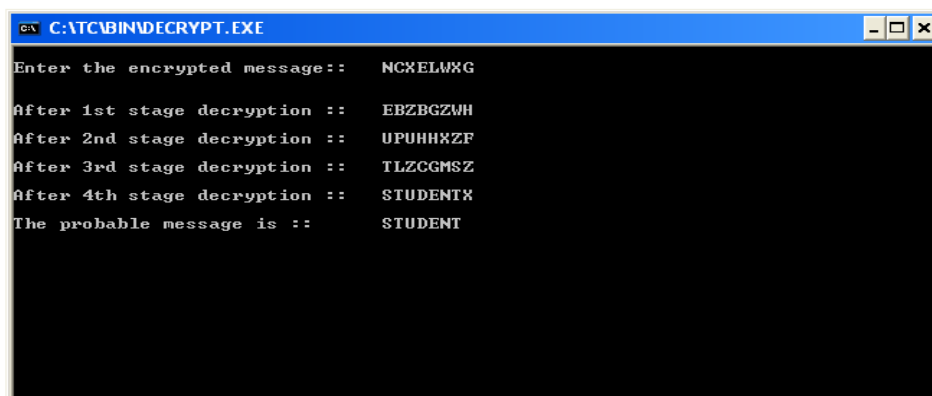
```
(Inactive C:\TCWIN45\BIN\RSABAC-1.EXE)
Enter two different prime numbers P and Q less than 10
5 7

Enter (E/e) for encryption and (D/d) for decryption
D
N = 35
Factors of (P-1)*(Q-1) are below
2
3
4
6
8
12
?????????
public key is = 5
private key is = 5

ATTENTION!!!!

Please Enter positive numbers maximum 10 different to decrypt
Enter 0 to end
Number should below 34
14 33 19 10 17 18 19 7 0
Decrypted values are below
N C X E L W X G
```

iv) Decrypt the message using PLAY- FAIR CIPHER MATRIX



```
C:\TC\BIN\DECRYPT.EXE
Enter the encrypted message:: NCXELWXG

After 1st stage decryption :: EBZBGZWH
After 2nd stage decryption :: UPUHXXZF
After 3rd stage decryption :: TLZCGMSZ
After 4th stage decryption :: STUDENTX
The probable message is :: STUDENT
```

VI. CONCLUSION

So far encryption technique adopting the concept of PLAY-FAIR CIPHER MATRIX has been programmed and four iteration steps have been introduced to it to make the technique more stronger one[6]. Then a public key encryption system has been designed which provides both confidentiality and authentication, but there are some limitations. The previous encryption technique is also a part of this system. After completion of the program the strength of the technique has been checked and this encryption technique can also be used for other networks such as Banking network.

REFERENCES

- .Z. J. Haas, et al., eds., Special Issue on Wireless Ad Hoc Networks, IEEE J. on Selected Areas in Communications, Vol. 17, No. 8 (August 1999).
- [1] I. F. Akyildiz et al., "A Survey on Sensor Networks," IEEE Communications Magazine, August 2002, pp. 102-114.
 - [2] X.-Y. Li, et al., "Coverage in Wireless Ad Hoc Sensor Networks," IEEE Trans. on Computers, vol. 52, pp. 753-763 (June 2003).
 - [3] I. Branovic, R. Giorgi, and E. Martinelli. Memory Performance of public-Key cryptography Methods in Mobile Environments. In ACM SIGARCH Workshop on Memory performance: Dealing with Applications, systems and architecture (MEDEA-03), pages 24–31, New Orleans, LA, USA, September 2003.
 - [4] JoonsangBaek, Han Chiang Tan, Jianying Zhou, and Jun Wen Wong. Realizing Stateful Public Key Encryption in Wireless Sensor Network. In Proceedings of The IFIP TC-11 23rd International Information Security Conference (SEC '08), pages 95–107. Springer, 2008.
 - [5] T. E. Gamal. A public key cryptosystem and a signature scheme based on discrete logarithms. In Advances in Cryptology – proceedings of CRYPTO 84, volume 196 of Lecture Notes in Computer Science, pages 10–18. Springer-Verlag New York, Inc., 1985.
 - [6] Secure Encryption in Wireless Sensor Network – JiaChenjium, Liao Yongjan, Chen Kangshen.
 - [7] Practical ID-based Encryption for Wireless Sensor Network – Cheng-Ken Chu, Joseph K. Liu, Jianying Zhou, FengBao, Robert H. Deng.
 - [8] International Journal of Advanced Computer Science, Vol. 1, No. 3, Pp. 113-117, Sep. 2011- Universal Playfair Cipher Using MXN Matrix. AftabAlam, SehatUllah, Ishtiaq Wahid, & Shah Khalid.
 - [9] Proof Checking the RSA Public Key Encryption Algorithm Robert S. Boyer and J Strother Moore. Technical Report #33 September 1982.
 - [10] http://en.wikipedia.org/wiki/Playfair_cipher.