Secured Wireless Data Communication

Dnyanda Namdeo Hire
Amrutvahini College of Engineering, Sangmner,
Tal – Sangamner, Dist- Ahmednagar, Maharashtra, India.

ABSTRACT

Security of data in army stations is an important issue. In early systems, at the time of information transmission between two army stations, it can be hacked by terrorists, spies and enemies. Cryptography is a very important system employed for this purpose. There are various types of algorithms available for encryption and decryption of data and new algorithms are evolving. Polyalphabetic substitution cipher is a strong algorithm used for security of data in army stations. In this paper, various techniques of security of data and one the algorithm using polyalphabetic substitution cipher are discussed.

General Terms

Pattern Recognition, Security, Algorithms, DS-SS, et. al.

Keywords

Cryptography, Encryption, Decryption, et. al

1. INTRODUCTION

Now-a-days, security is one of the most important factors in life. It can be useful any where any time. In banks, shops as well as in our daily life also we need security. One can use password to his computer for securing private information. This is also one of the types of data security. If in our daily life we require security then think about security of our security system i.e. our national security (defense). Especially, at the war time the terrorists and spies tries a lot to leak information so that they can capture the important information useful to win the war. Even in business and share market the competitors try a lot to hack the site of front person but if our data will be in coded form even if they are successful in hacking they will not understand the message/data.

Present techniques having many drawbacks such as, anyone can receive, transmitted encoded message then these systems never provides the applications such as[1],

- **Privacy:** The transmitted message must be such that only the intended receiver should able to read it. No one else should be able to read it.
- **Message authentication:** In message authentication, the receiver needs to be sure about the sender's identity.
- **Integrity:** The meaning of integrity is that data arriving at the receiver exactly as it was sent. There should not be changed absolutely.
- **Nonrepudiation:** The meaning of nonrepudiation is that the receiver should able to prove that, the message it has received has come from a specific sender.

In this paper, various methods for security of data are discussed. There are following methods for security of data: Spread spectrum technique, Cryptography technique. The rest of paper is organized as follows. In subsequent sections we describe the Spread spectrum technique, Cryptography technique, then the detailed algorithm using polyalphabetic substitution cipher, and at last conclusion of paper.

2.DESCRIPTION OF SECURITY TECHNIQUES

2.1 Spread Spectrum Technique

Since the late 1940's spread ***spectrum technique*** have been used for military applications in which clandestine operation is a major objective. Spread spectrum technique provides excellent immunity to interference. Possibly the result of international jamming and allow transmission to be hidden within background noise. Recently, spread spectrum technique has been adopted for civilian application in wireless telephony system. But the main drawbacks with these systems were that ***they were very easy to hack***. Hence there was a need to have a more secure system.[2]

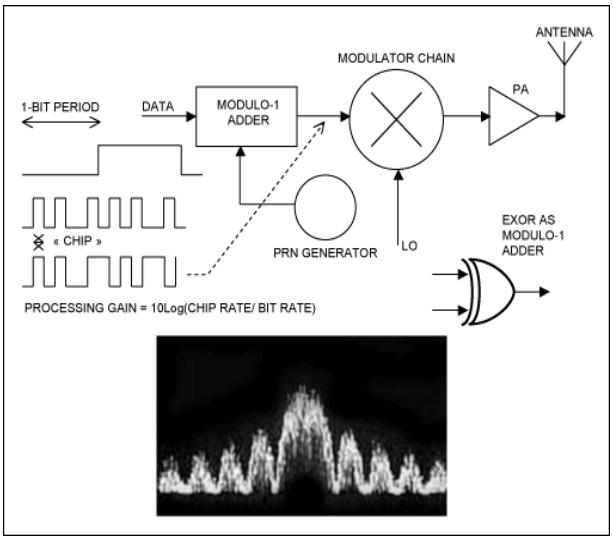

Fig 1: Block diagram of DS-SS technique[2]

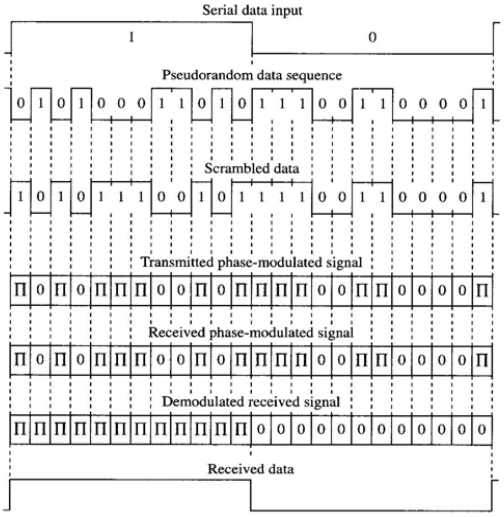

Fig 2: Waveforms of DS-SS technique

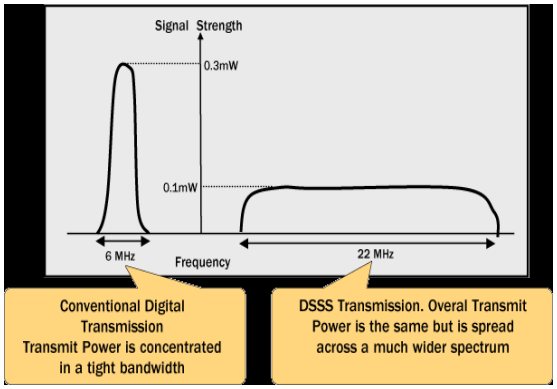

Fig 3: Power diagram of DS-SS Signal

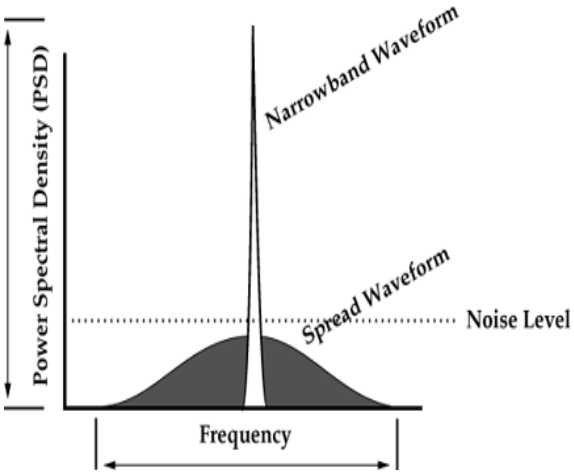

Fig 4: Graph of DS-SS technique

In this technique as shown in fig.1, the serial data input is given to modulo-1 adder, at the same time pseudo-random noise signal (PRN) is applied to modulo-1 from PRN generator. The output of adder is given to the chains of modulator to modulate it with the local oscillator (LO) frequency to generate modulated signal. This modulated signal is applied to power amplifier to amplify the signal and then it is transmitted in air as an electromagnetic wave with the help of transmitting antenna. The corresponding waveforms at the output of each block are shown in fig. 2.

2.2 Cryptography Technique

Because of ***high bandwidth requirements in DS-SS system*** we switched to the next system which is the cryptography technique to achieve security.

Fig. 5 shows cryptographic technique in which the data is encrypted using encryption algorithm. For this symmetric key is used as shown in fig.5. Symmetric key means the same key is used for encryption and decryption. At the receiver, the encrypted data is decrypted and converted into plaintext using decryption algorithm. Thus security is achieved by cryptographic technique. There are many techniques as below:

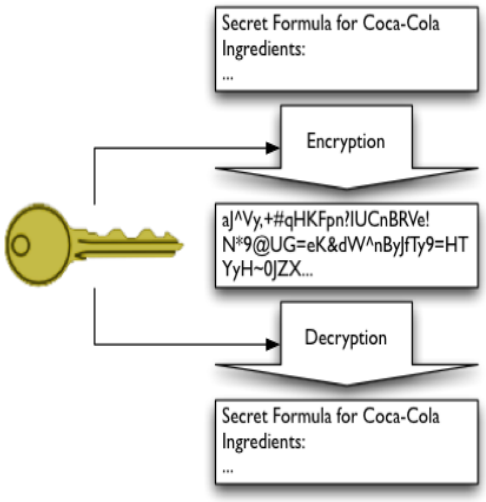

Fig 5: Cryptography technique

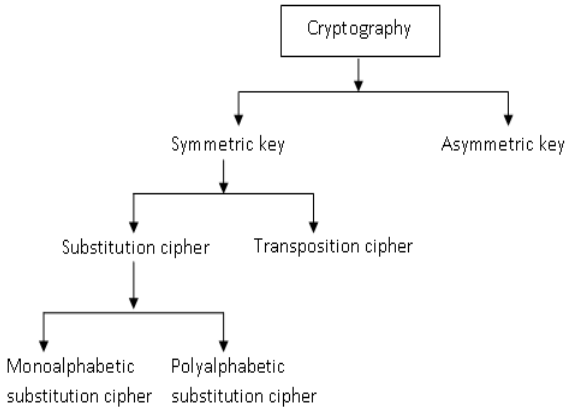

Fig 6: Types of Cryptography technique

Symmetric key algorithm has two types as substitution cipher and transposition cipher. The substitution cipher is more advantageous than transposition cipher. And hence used in many applications for security purpose. Symmetric key algorithm again subdivided into two types as, monoalphabetic substitution cipher and polyalphabetic substitution cipher. Among these two algorithms the polyalphabetic substitution cipher algorithm is more advantageous and used in various applications.

- **Monoalphabetic Substitution Cipher**

In this type of substitution, a character in the plaintext is always substituted by some other character in the ciphertext regardless of its position in the text.[5]

Example:

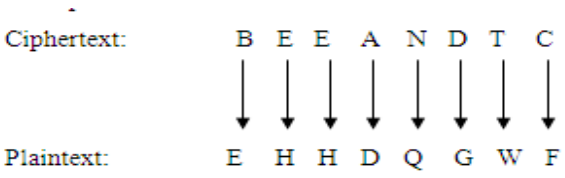

Fig 7: Example of monoalphabetic substitution cipher

Here each plaintext character is shifted down by 3.

Disadvantages:

- The code can be attacked very easily.
- The code can easily be decoded by trial and error method.

- **Transposition Cipher**

In this type of cipher, the characters retain their plaintext form, but change their positions when ciphertext is created[5]. The plaintext is arranged in the form of a two dimensional table as shown in fig.5.

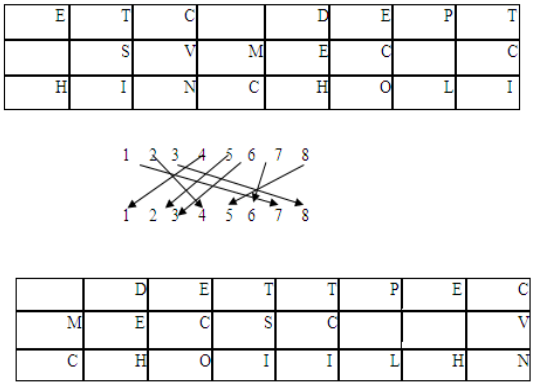

Fig 8: Example of transposition cipher

Disadvantages:

- Transposition cipher is not very secure.
- It is still possible to attack it by trial and error.

- **Asymmetric Key Cryptography**

Asymmetric key cryptography is also known as public key cryptography. In this system the sender uses the public key to encrypt the message to be sent. At the receiver, this message is decrypted with the help of receiver's private key. The public key used for encryption is different from the private key used for decryption. The public key is known to everyone but the private key is available only to an individual.

Disadvantages:

- The algorithms used are highly complex.
- It takes a long to calculate ciphertext from plaintext.
- It is necessary to verify the association between a sender and this public key.

- **Polyalphabetic Substitution Cipher**

The Polyalphabetic substitution cipher has several advantages over other algorithms.

Advantages:

- More secured than monoalphabetic substitution cipher.
- Easy to implement the algorithm.
- A same character can be replaced by different characters in message when it occur number of times.

3. POLYALPHABETIC SUBSTITUTION CIPHER ALGORITHM

In this paper we are going to implement the Polyalphabetic substitution cipher algorithm. In this technique each character in the plaintext is replaced by a group of characters to obtain the ciphertext. Another important point to be noted is that a character B can be changed by E at the beginning of the text but it may be changed to P in the middle of the text. An example of Polyalphabetic substitution is the ***Vigenere cipher.*** [2]

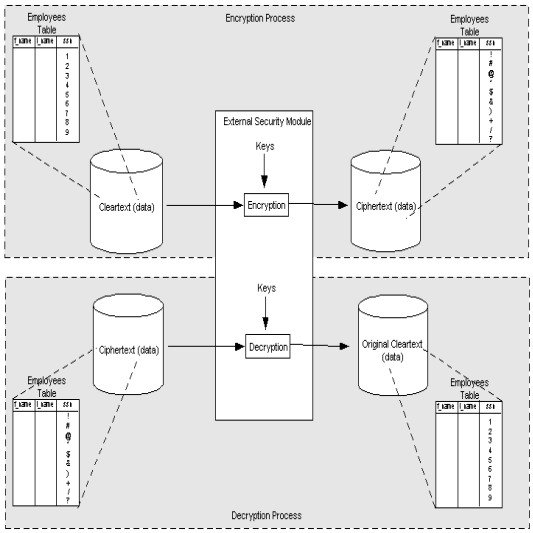

Fig 9: Encryption and decryption process

3.1 Algorithm and Flowchart for Encryption

Algorithm:

- START
- Take the character from ciphertext and represent each letter in ciphertext by a number from 0-25 (i.e. 'a'=0,'b'=1, 'z'=25).
- Add 26 to ciphertext number.
- Subtract corresponding key from that addition.
- Subtract 26 from that addition.
- And write corresponding letter of above number.
- Repeat the procedure up to end of text.

Flowchart:

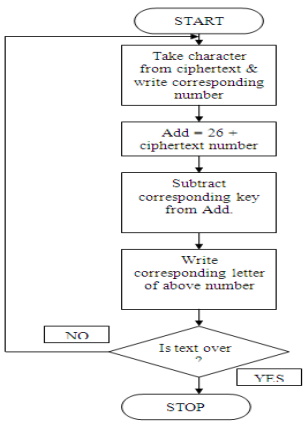

Fig 10: Flowchart for encryption

3.2 Algorithm and Flowchart for Decryption

Algorithm:

- START
- Take the character from plaintext and represent each letter in plaintext by a number from 0-25 (i.e. 'a'=0,'b'=1… 'z'=25).
- Add the key number corresponding to plaintext number.
- If addition is > 25, subtract 26 from addition and write down letter corresponding to that number as ciphertext.
- And if addition is between 0-25 write down corresponding letter as ciphertext.
- Repeat the procedure up to end of text.

Flowchart:

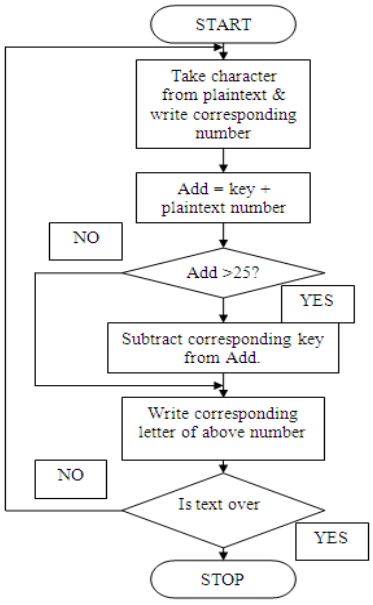

Fig 11: Flowchart for decryption

4. CONCLUSIONS

Cryptography is the best method for security of data. Among the various types of cryptographic technique Polyalphabetic Substitution cipher is the best method. To maintain privacy and to prevent an unauthorized person from extracting information from communication channel, this paper will help. So we will try to implement the algorithm for secured communication over a long distance. This algorithm will help in getting high degree of security from terrorists, spies or any other harmful person. So we can send the important information from source to destination using wireless communication.

5. ACKNOWLEDGMENTS

I like to thanks my guide Prof. Mrs. S.S. Katariya for her guidance for successful publication of this paper. Also, I like to thanks my friends and family for their support.

6. REFERENCES

[1] A.S. Tanenbaum, "Computer Networks", 2nd Edition, PHI.

[2] http://www.cryptojinas.com-information of cryptography

[3] William Stallings, "Cryptography and Network Security", 3rd Edition, Pearson Education.

[4] Evangelos Kranakis, "Primality and Cryptography", John Wiley & Sons.

[5] Douglas A. Stinson, "Cryptography, Theory and Practice", 2nd Edition, Chapman & Hall, CRC Press Company, Washigton.

[6] http://www.truecrypt.org

[7] B. B. Edwards Jr. *Master Keying by the Numbers (2/e)*. Security Resources. Pensacola, FL, USA. 1997.

[8] B. W. Lampson. "Hints for computer system design." *ACM Operating Systems Rev.* 15, 5 (Oct. 1983),pp 33-48.

[9] M. W. Tobias. *Locks, Safes and Security (2/e).* Charles Thomas Publisher, Ltd. Springfield, IL, USA. 2000.

[10] J. Andrews. *Fundamentals of Master Keying.* Associated Locksmiths of America. 1990.

[11] Matt Blaze Cryptology and Physical Security: Rights Amplification in Master-Keyed Mechanical Locks, AT&T Labs – Research, *IEEE Security and Privacy*, March/April 2003.

[12] http://www.freeotfe.org

[13] Andrews, M., and Whittaker, J. *"Computer Security."* IEEE Security and Privacy, September/October 2004.

[14] National Institute of Standards and Technology. *An Introduction to Computer Security: The NIST Handbook.* Special Publication 800-12, October 1995.

[15] Gardner, M. *Codes, Ciphers, and Secret Writing.* New York: Dover, 1972.

[16] Garrett, P. *Making, Breaking Codes: An Introduction to Cryptology.* Upper Saddle River, NJ: Practice Hall, 2001.

[17] http://www.hpccsystems.com

[18] Kahn, D. *The Codebreakers: The Story of Secret Writing.* New York: Scribner, 1996.

[19] Korner, T. *The Pleasures of Counting.* Cambridge, England: Cambridge University Press, 1996.

[20] Kumar, I. *Cryptology.* Laguna Hills, CA: Aegean Park Press, 1997.

[21] Nichols, R. *Classical Cryptography Course.* Laguna Hills, CA: Aegean Park Press, 1996.

[22] Nichols, R., ed. ICSA *Guide to Cryptography.* New York: McGraw-Hill, 1999.

[23] Sinkov, A. *Elementary Cryptanalysis: A Mathematical Approach.* Washington, D.C.: The Mathematical Association of America, 1966.

[24] http://www.cryptool.com