International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 03 Issue: 09 | Sep-2016 www.irjet.net p-ISSN: 2395-0072

A study on encryption algorithm for pilot signal transmission

Dr. Senthil Kumar M [1], Ms.Suganya S [2]
[1]Associate professor,Department of CSE,Valliammai Engineering College,Tamilnadu,India
[2]PG Scholar,Department of CSE,Valliammai Engineering College,Tamilnadu ,India

Abstract-*Pilot signal is an wireless transmission between various nodes. while transmitting a signal from sender to receiver it need to be encrypted in other form to avoid eavesdropping by adversaries. Algorithms used to encrypt the signal or information may be symmentric key encryption or assymmentric key encryption algorithms.This paper provides a comparative study between various algorithms and also to choose best among them for wireless environment.*

Keywords *:-Pilot signals, eavesdropping , adversaries,Symmentric , assymentric etc.*

INTRODUCTION

In this growing technological era , while transmitting a signal / information among various places it need to be in an secured manner.So it lead to the study of cryptography concepts. It mainly focuses on ensuring the Confidentiality ,Integrity and Availability (CIA).
Basic cryptographic terms:-

- Plain text
- Cipher text
- Key
- Encryption algorithm
- Decryption algorithm

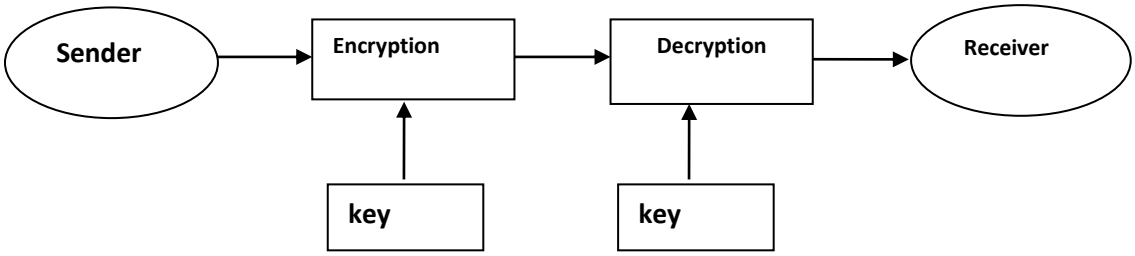


Fig- 1 Basics of cryptography

Plain text

Original message from the legitimate transmitter.

Cipher text

Encrypted form of plain text.

Encryption algorithm

Algorithm used for converting plain text to cipher text in transmitter end.

Decryption algorithm

Algorithm used for converting cipher text to plain text at the receiver end.

Figure 1 shows that a legitimate sender sends a plain text(P) which is encrypted by encryption algorithm using key to produce a Cipher text (C) ie C= E(P) , then at the receiver end it need to be decrypted using decryption algorithm to obtain Plain text (P=D(C)).

LITERATURE SURVEY

Based on key ,cryptographic algorithms is classified as such represented in Figure 2

- Keyless
- Symmetric key encryption
- Asymmetric key encryption

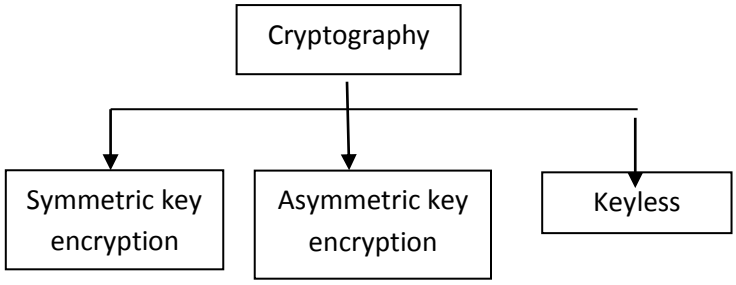


Fig-2 Classification of cryptography

Symmetric key encryption :-

In this both the encryption as well as decryption process uses a same key .This is also called as private key encryption. Some of them uses symmetric key techniques are DES,RC4 etc.

Asymmetric key encryption:-

Encryption as well as decryption process uses a different key for its processing eg. If sender uses a public key for encryption then at the receiver end uses a private key for it decryption process . This is also called as public key cryptography.Asymmetric key techniques followed in RSA ,

Keyless

It doesn't have key, instead it performs hash function by using XOR operation.

SHA-1 etc.

In this symmetric key encryption , it is done in two ways they are

- Block cipher
- Stream cipher

Block Cipher :-

Block cipher allows a single block of bits to process at a time to produce corresponding output. Example of block cipher is DES.DES is abbreviated as Data Encryption Standard .It allows the plain text of 64 bits and key size of 56 bits along with 8 parity bits.It performs three phases is clearly stated in Figure 3.They are

- Initial permutation with plain text of 64 bit size and key input(permuted) and it follows for 16 rounds.
- Swap the value with the permuted input.
- Perform inverse initial permutation .

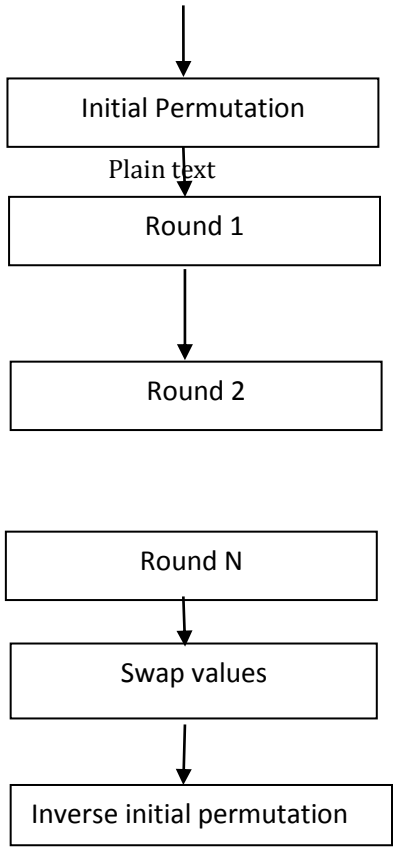
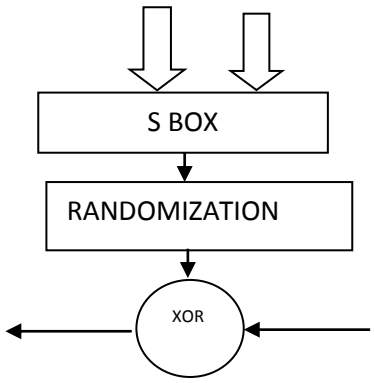


Fig-3 DES Operations

Stream cipher:-

Stream cipher is also a symmetric type of encryption in which allows only one bit to process at a time .RC4 algorithm uses stream cipher process .It allows s box to generate key and decryption also done with the available key value in s-box. Figure 4 shows that key is generated from the array in random manner and performs randomized process to avoid redundancy and perform XOR operation with the original information (plain text).



Plain/cipher textPlain/ cipher text

Fig- 4 RC4 operations

PUBLIC KEY CRYPTOGRAPHY:-

These cryptosystems uses different keys for encryption and decryption. If sender uses a public key for encryption at the receiver end they use a private key for decryption.RSA algorithm is one of the public key cryptography process . It accepts only plain text and cipher text between 0 to n-1 where *n*is less than 2^1024.

Hashing algorithms:-

It is neither an symmentric key encryption nor assymentricalgorithm , since it is an one way function where no decryption algorithm. It mainly uses for verification and validation process based on checksum value. It involves a single operation ie XOR.SHA (Secure Hash Algorithm) it process the plain text of variable-length input (up to 2^64 bitslong), and reducing to to 160-bit encrypted output. It involves 80 rounds.

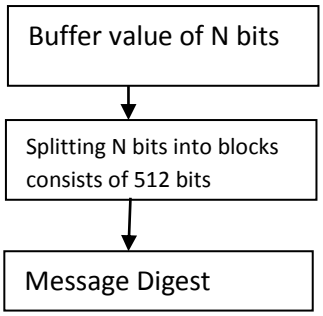


Fig- 5 SHA operations

Figure 5 shows that plain text of any size is split into various blocks which is provided with 512 bits to form a Message digest.

Comparative study of algorithms:

Monika Agrawal et al. 2012 gives a detailed study of the popular symmetric key encryption algorithms such as DES, TRIPLE DES, AES, and Blowfish. Symmetric Key algorithms run faster and the memory requirement of S is also lesser than Asymmetric encryption algorithms. Further, the security aspect of Symmetric key encryption is superior than Asymmetric key encryption

Factors	DES	RC4	RSA	SHA
Plain text size	64		0 to n-1	$<2^{64}$
Key size	56	256-byte array	0 to n-1	160
Rounds	16	Until XORed output obtains	1	80
Merits	Avalanche effect	Simple for implementation	Simplicity	Input of any length maps to an output of fixed length (160 bits)
Demerits	Complex process	not used for highly classified data.	Vulnerable to chosen ciphertext attack	weak against collision attacks .

CONCLUSION

It concludes that while transmitting pilot signal we need to use an secure encryption algorithm for that we need to know above algorithms and its features separately and also comparative study of them. In this wireless transmission we need to minimize its complexity , fast as well as secure transmission must ensured.

REFERENCES

[1] W. Stallings, *Cryptography and Network Security: Principles and*
Practice, 3rd ed. Upper Saddle River, NJ, USA: Prentice Hall, 2003.
[2] C. E. Shannon, "Communication theory of secrecy systems," *Bell Syst.*
Tech. J., vol. 28, no. 4, pp. 656–715, Oct. 1949.
[3]Dasgupta, Sanjoy et al. Algorithms. New York: McGraw-Hill Companies, Inc., 2008.
[4] Schneier, Bruce. Applied Cryptography, Second Edition. Protocols, algorithms, and
source code in C. New York: John Wiley & Sons, Inc., 1996.
[5] Secure Hash Standard (SHS), FIPS PUB 180-3, 2008.
[6] National Bureau of Standards, " Data Encryption Standard," FIPS Publication 46, 1977.
[7] Simar Preet Singh, and Raman Maini "COMPARISON OF DATA ENCRYPTION ALGORITHMS" International Journal of Computer Science and Communication Vol. 2, No. 1, January-June 2011, pp. 125-127
[8]Monika Agrawal, Pradeep Mishra," A Comparative Survey on Symmetric Key Encryption Techniques", International Journal on Computer Science and Engineering (IJCSE), Vol. 4 No. 05 May 2012, PP877-882.S