International Journal of Trend in Scientific Research and Development (IJTSRD)
International Open Access Journal
ISSN No: 2456 - 6470 | www.ijtsrd.com | Volume - 2 | Issue – 2

Symmetric Key Cryptography Algorithm for Data Security

Tushar Anil Patil
ME (E & TC), D. Y. Patil college of Engg. & Tech. Kasaba Bavada, Kolhapur, Maharashtra, India

Prof. Dr. Mrs. K. V. Kulhalli
D. Y. Patil college of Engg. & Tech. Kasaba Bavada, Kolhapur,Maharashtra, India

ABSTRACT

Ambiguous Multi-Symmetric Cryptography (AMSC) that hide multiple plain-texts in a cipher-text using the same number of keys. The goal of this method is to overcome the problem of symmetric cryptography failure when the shared key is exposed. The proposed method AMSC is a cryptographic primitive that preserves plausible deniability after a cryptographic key is discovered. We evaluate AMSC in terms of security and complexity. The security analysis shows that our scheme withstands all security attack models with different knowledge of the adversary. In terms of time complexity, AMSC produces the cipher-text in polynomial time with respect to the number and size of the plaintexts and keys. AMSC has two main applications: a) It sends multiple messages for multiple receivers through one cipher-text. b) It sends one real message and multiple decoys to defeat attacks by providing security beyond conventional brute-force bounds. For both applications, AMSC can be used to deny encryption.

Keywords: *Symmetric cryptography, Brute force attack, Cipher-text only attack, Deniable encryption, Multi encryption, Ambiguous encryption, Honey encryption*

INTRODUCTION

Cryptography is the technique to provide secure communication to maintain information securities such as data confidentiality, data integrity, authentication, and non-repudiation. Ambiguous Multi Symmetric Cryptography (AMSC) that conceals multiple plain-texts in a cipher-text using the same number of keys. AMSC produces

Cryptography is the technique to provide secure communication to maintain information securities such as data confidentiality, data integrity, authentication, and non-repudiation. Ambiguous Multi Symmetric Cryptography (AMSC) that conceals multiple plain-texts in a cipher-text using the same number of keys. AMSC produces. AMSC can be used in different applications. One is to broadcast messages. One video channel for example could be

Decrypted to different contents by each receiver. Another application is to defeat the adversary via concealing the genuine message by grouping it with decoy messages. Our method stands out against traditional approaches like concatenation of multiple ciphers. One problem with these approaches, is the management of offsets, which have to be resent each time the cipher-text size changes. AMSC overcomes this issue as offsets are not used.

AMSC

AMSC used to send one cipher-text with multiple messages to different receivers. This can be used in different domains. One interesting domain is message broadcasting. Send one message to different receivers on the same IP address. Each receiver will decrypt and get a different content.

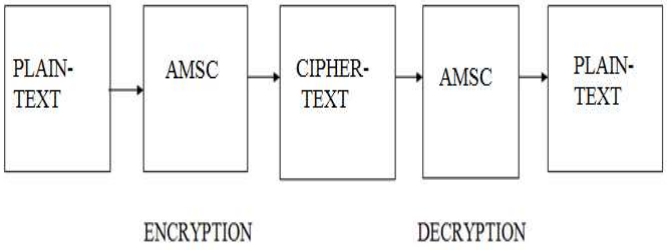


Fig.1:- Block Schematic

Plain-text:-This is original data or message that is fed into the algorithm as input. Data that can be read and understood without any special measures. The plain-text includes message, audio-video files, ATM, credit card and other banking information, private data.

Encryption algorithm:-The encryption algorithm performs various substitutions and transformation on the plain text. In the encryption plaintext is hide and unreadable form. The encryption ensures that information is hidden from anyone. There are different symmetric key algorithm Advanced Encryption Standard (AES), Data Encryption Standard (DES), Triple DES (3DES).

AMSC:-The AMSC can implement by AMSC1 and AMSC2. The AMSC produces the one cipher text from multiple plain texts using same number of key. The AMSC1 and AMSC2 compare then which one better performance that can be chosen.

Secret key:-The secret key is also input to the encryption algorithm. The value of key independent of the plaintext and of the algorithm. The algorithm will produce a different output depending on the specific key being used at the time. The exact substitution and transformation performed by the algorithm depend on the key. The symmetric key algorithm use same keys are both sender and receiver.

Cipher-text:-This is the scrambled message produced as output. It depends on the plaintext and the secret key. The cipher text is an apparently random stream of data and as it send. The block cipher processes the input one block of elements at a time, producing an output block for each input block. The stream cipher processes input elements constantly, generating output one element at a time.

Decryption algorithm:- This is essentially the encryption algorithm run in reverse. It takes the Cipher text and secret key and produces the original plaintext. The decryption process of degenerate Cipher text to its original plaintext.

Scope:

AMSC used to send one cipher-text with multiple messages to different receivers. This can be used in different domains. One interesting domain is message broad casting. Send one message to different receivers on the same IP address. Each receiver will decrypt and get a different content.

B) Objective:

- Encrypt multiple variable size plain text with multiple variable size keys into one cipher text.
- Decrypt cipher text with particular key to obtain particular original message.
- Implement AMSC algorithm.
- Plot the timing of encryption with different number of plain texts.
- Compare the results with other symmetric key technique.

C) Methodology:

The proposed work will be implemented by following techniques.

AMSC1:-

The AMSC1 is based on (n-1) linear Diophantine equations. AMSC1 takes n plain-text and n keys with variable size and forms different equations in the form:

$$C=Ki*ai+ Pi$$

Using these equations generate the cipher-text. The necessary encryption steps to compute cipher text C using linear Diophantine equations.

AMSC2:-

The Chinese Remainder theorem used in AMSC2. Expect that m1, m2,…,mr are pair wise relatively prime positive integers, and let a1, a2,…,ar be integers. Then the system of congruence, $x \equiv ai \pmod{mi}$ for $1 \leq i \leq r$, Has a unique solution modulo M = m1 * m2 * …* mr, which is given by:

$$x \equiv a1M1ya + a2M2y2 + \ldots + arMryr \pmod{M},$$

Where $Mi = M/mi$ and $yi \equiv (Mi)^{-1} \pmod{mi}$ for $1 \leq i \leq r$.

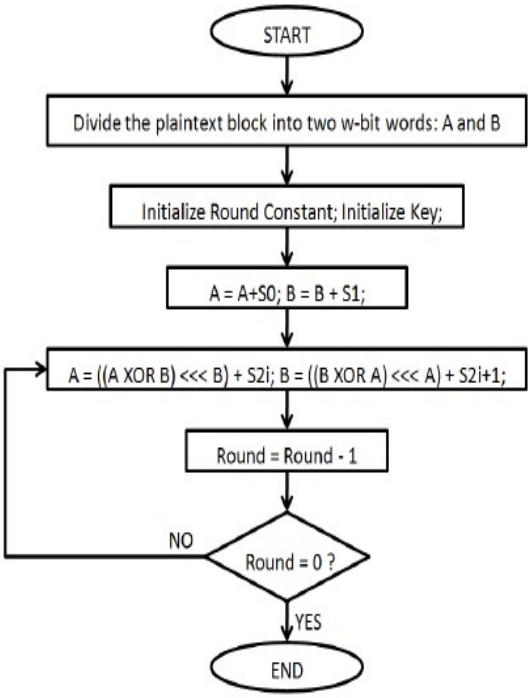
AMSC2 takes the same input as AMSC1 to generate the cipher-text. Decrypts cipher-text to plain-text in both AMSC1 and AMSC2 use same algorithm. The attacker access one cipher-text a brute force attack is one way to crack the encryption. Because of security use primes and co-primes keys. Co-primes have better security because they will more computations to find key.

RC5 :

In cryptography, RC5 is a symmetric-key block cipher great for its easiness. Designed by Ronald Rivest in 1994, RC imply "rivest cipher", or sooner, "Rons code". RC5 should be a symmetric block cipher. The equivalent secret cryptographic key is used for encryption and for decryption. The plaintext and cipher text are fixed length bit sequences. RC5 should be iterative in structure, with a variable number of rounds, The user can explicitly manipulate the trade-off between higher speed and higher security. The number of rounds r is a second parameter of RC5.
RC5 should have a variable-length cryptographic key. The user can choose the level of security appropriate for his application, or as required by external considerations such as export restriction. The key length b in thus a third parameter of RC5. One significant feature of the design of RC5 is its clarity; encryption is based on only three activity: addition, exclusive-or, and rotation. Thus, it makes RC5 both easy to implement, and very importantly, more amenable to analysis than many other block ciphers. The connection between simplicity of design and simplicity of analysis, was indeed one of Rivest's goals. Another distinguished feature of RC5 is the heavy use of data-dependent rotations in encryption.
The description of the encryption algorithm is given in the pseudo-code below. Assume that the input block is given in two w-bit registers A and B, and that the output is also placed in the registers A and B.

A = A + S [0]
B = B + S [1]
For i = 1 to r do
A = ((A _ B) <<<B) + S [2i]
B = ((B _ A) <<< A) + S [2i + 1]

The decryption normal is easily derived from the encryption normal.



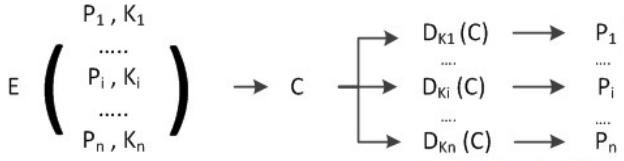
Performance Parameter:

The performance of proposed work is evaluated with following parameters:

- Speed
- Size
- Security
- Processing power
- Time

Transmitter Side:

This method encrypts multiple variable size plain-texts using multiple variable size keys into one cipher-text, hence the name Multi-Symmetric. Fig. shows the system model where P1; P2; :: Pn are the plain texts, K1;K2; ::Kn are the keys respectively, E is the encryption algorithm, D is the decryption algorithm and C is the cipher-text.



Definition 1: Let P1; P2 ;:: Pn be plain-texts, K1;K2; :: Kn be keys accordingly.
Transmitter generates cipher-text:

C = EAMSC ([K1;K2; :::Kn]; [P1; P2; :::Pn])

Cipher-text C represents all plain-texts, and can be decrypted by any key Ki to plain-text Pi.

Receiver Side:

At the receiver side decrypts cipher-text C using his key Ki,

Where Pi = C mod Ki.

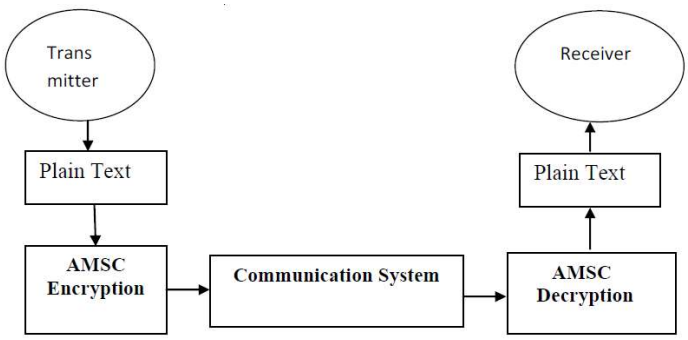


Fig. 2: Standardized Communication Diagram For Transmitter and Receiver

CONCLUSION:

In this paper, proposed method that conceals multiple plain-texts in a cipher-text. The AMSC can be Used in different applications like TCP/IP multicast, secure Communications, etc. Moreover, we presented AMSC as a Method for enigmatic secure communication, where in all Applications, regardless of the knowledge of the adversary, AMSC endures different security attacks. Compared AMSC and symmetric key algorithm to other approaches such as concatenating cipher-texts and showed the security and overhead advantages.

REFERENCES:

1. Dhenakaran S.S, Naganathan E.R, "A New Approach to Multiple symmetric keys" International journal of computer science and network security, vol.7, issue 6, pp 254-259, 2007.
2. H. Bojinov, E. Bursztein, X. Boyen, and D. Boneh., "Kamouflage: lossresistant password Management." ESORICS, pp 286-302, 2010.
3. A. Juels and T. Ristenpart., "Honey encryption: Security beyond the brute-force bound." EUROCRYPT 2014, pp. 293-310, 2014.
4. Bidisha Mandal, Sourabh Chandra, SK Safikul Aalam, subhendu Sekhar Patra, "A Comparative and Analytical Study on Symmetric key cryptography, pp 131-136, 2014.
5. N. Ruangchaijatupon and P. Krishnamurthy, "Encryption and power consumption in wireless LANs-N, "The Third IEEE Workshop on Wireless LANs, pp. 148-152, Newton, Massachusetts, 2001.
6. D. Salama, A. Elminaam and etal, "Evaluating The Performance of Symmetric Encryption Algorithms", International Journal of Network Security, Vo1.10, issue 3, pp 216-222, 2010.
7. Stallings, W.: Cryptography and Network Security: Principles and Practice, 6e, Pearson Prentice Hall, 978-0-13-335469-0, 2014.