© 2017 IJSRST | Volume 3 | Issue 6 | Print ISSN: 2395-6011 | Online ISSN: 2395-602X
Themed Section: Science and Technology

Enhanced Security For Hybrid Encryption Strategies With Key Reausability

Narasimha Raju Dodda, Katikireddy. Ratna Kumari
Department of Computer Science and Engineering, Shri Vishnu Engineering College for Women, Bhimavaram Andhrapradesh, India

ABSTRACT

Symmetric key cryptography is a common cryptographic technique using the same key at both the transmitter and receiver side. The main advantage of symmetric key encryption is its less computational cost compared to its counterpart-public key encryption. In this work a new symmetric key encryption scheme is proposed. This proposed algorithm provides new step to avoid shortcomings. We use some famous algorithms to encrypt a data as follows. At first, we create new algorithm in order to provide security issue and time constraint of operation then we combine AES and CAST-128 algorithm, then we encrypt data using the proposed algorithm. This can enhance the security and complicates the Encryption. And the major advantage of this algorithm is key reusability. In this paper we provide both the encryption and decryption that supports in real time application and algorithm has a practical value.

Keywords : AES, Cryptography, CAST-128, DES, Symmetric, Key, Cipher Text

I. INTRODUCTION

Cryptography is a mechanism in which information is encrypted or transformed into some unreadable format called cipher text. Only the authorized user having the secret code can decrypt or decipher the received message. A number of encryption techniques are available in literature. All encryption algorithms can be divided in two major groups which are Symmetric key encryption algorithms, and Asymmetric key encryption algorithms. In Symmetric key encryption or secret key encryption, only one key is used for both encryption and decryption. In asymmetric key encryption two keys are used i.e. public key and private key. This type of encryption is also called public key encryption. Symmetric key encryption algorithms are faster than asymmetric key encryption algorithms. Key should be exchanged between the communicating entities before the transmission of data. Key is one of the important factors of these algorithms. Weak keys can be easily attacked by the attackers as compared to longer keys which are difficult to break. Symmetric key encryption algorithms are still widely used as powerful techniques in insecure communication channel. Some widely used encryption schemes are discussed below. Following are some most common secret key cryptographic algorithms

Data Encryption Standard (DES):

It is a Feistel-type Substitution-Permutation Network (SPN) cipher, specified in FIPS PUB 46. The result of a 1970s effort to produce a U.S. encryption standard. DES uses a 56-bit key which can be broken using brute-force methods, and is now considered obsolete. A 16 cycle Feistel system is used, with an overall 56-bit key permuted into 16 48-bit sub keys, one 154 for each cycle. To decrypt, the identical algorithm is used, but the order of sub keys is reversed. The L and R blocks are 32 bits each, yielding an overall block size of 64 bits. The hash function "f", specified by the standard using the so-called "S-boxes", takes a 32-bit data block and one of the 48-bit sub keys as input and produces 32 bits of output. Sometimes DES is said to use a 64-bit key, but 8 of the 64 bits are used only for parity checking, so the effective key size is 56 bits. Since the time DES was adopted (1977), it

has been widely speculated that some kind of backdoor was designed into the cryptic S-boxes, allowing those "in the know" to effectively crack DES. Time has proven such speculation idle. Regardless of any backdoors in the hash function, the rapid advances in the speed of electronic circuitry over the last 20 years, combined with the natural parallelism of Feistel ciphers and DES's relatively small key size, have rendered the algorithm obsolete. In 1998, the Electronic Frontier Foundation built a DES Cracker for less than $250,000 that can decode DES messages in less than a week.

Advanced encryption standard

In the late 1990s, the U.S. National Institute of Standards and Technology (NIST) conducted competition to develop a replacement for DES. The winner, announced in 2001, is theRijndael algorithm, destined to become the new Advanced Encryption Standard. Rijndaelmixes up the SPN model by including Galios field operations in each round. Somewhat similar to RSA modulo arithmetic operations, the Galios field operations produce apparent gibberish, but can be mathematically inverted. AES have Security is not an absolute; it's a relation between time and cost. Currently, there are speculations that military intelligence services possibly have the technical and economic means to attack keys equivalent to about90 bits, although no civilian researcher has actually seen or reported of such a capability. Actual and demonstrated systems today, within the bounds of a commercial budget of about 1million dollars can handle key lengths of about 70 bits. An aggressive estimate on the rate of technological progress is to assume that technologies will double the speed of computing devices every year at an unchanged cost. If correct, 128-bit keys would be in theory be in range of a military budget within 30-40 years. An illustration of the current status for AES is given by the following example, where we assume an attacker with the capability to build or purchase a system that tries keys at the rate of one billion keys per second. This is at least 1000 times faster than the fastest personal computer in 2004..The key length should thus be chosen after deciding for how long security is required, and what the cost must be to brute force a secret key. In some military circumstances a few hours or days security is sufficient –after that the war or the mission is completed and the information uninteresting and without value. In other cases a lifetime may not be long enough. There is currently no evidence that AES has any weaknesses making any attack other than exhaustive search, i.e. brute force, possible. Even AES-128 offers a sufficiently large number of possible keys, making an exhaustive search impractical for many decades, provided no technological breakthrough causes the computational power available to increase dramatically and that theoretical research

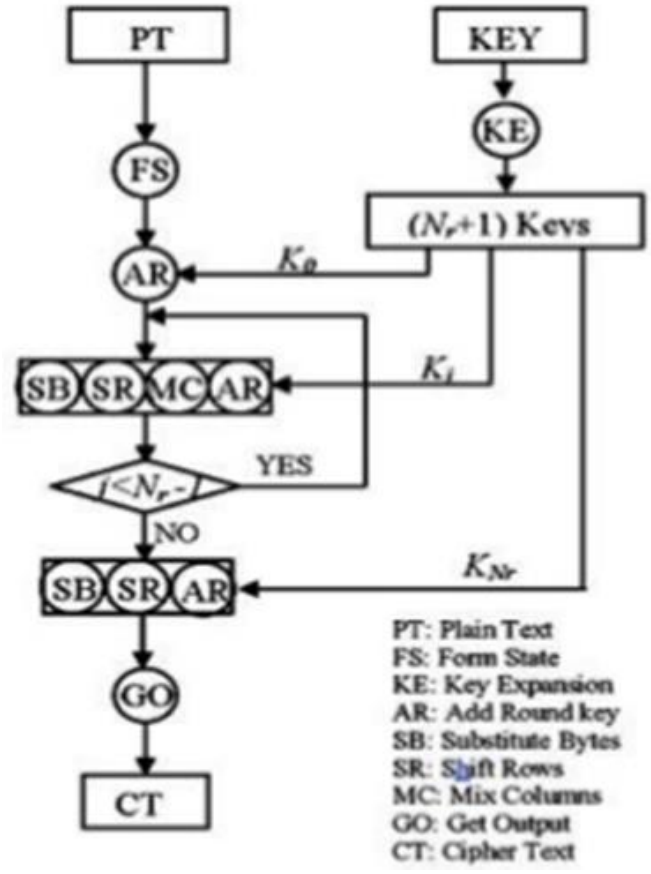

Figure 1: AES algorithm

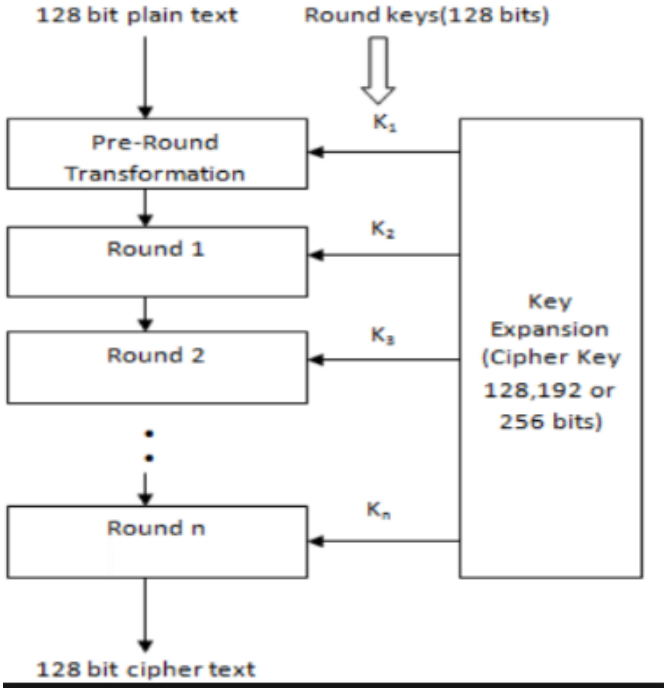

Figure 3: AES algorithm

Does not find a short cut to bypass the need for exhaustive search. There are many pitfalls to avoid when encryption is implemented, and keys are generated. It is necessary to ensure each and every implementations security, but hard since it requires careful examination by experts. An important aspect of an evaluation of any specific implementations to determine that such an examination has been made, or can be conducted. If both block length and key length are 128 bits, AES will perform 9 processing rounds. If the block and key are 192 bits, AES will perform 11 processing rounds. If the block and key are 256 bits, then it performs 13 processing rounds. Each processing rounds involves four steps: 1. Substitute bytes: Uses an S-box to perform a byte by byte substitution of the block.2. Shift rows: A simple permutation.3. Mix column: A substitution method where data in each column from the shift row is multiplied by the algorithm's matrix.4. Add round key: The key for the processing round is moored with the data.

CAST: CAST was designed in Canada by Carlisle Adams and Stafford Tavares. They claim that the name refers to their design procedure and should conjure up images of randomness, but note the authors' initials. The example CAST algorithm uses a 64-bit block size and a 64-bit key. The structure of CAST should be familiar. The algorithm uses six S-boxes with an 8-bit input and a 32-bit output. Construction of these S-boxes is implementation-dependent and complicated CAST-128 is a DES–like substitution-permutation crypto algorithm, employing 128-bit key operating on a 64-bit block. CAST-256 is an extension of CAST-128, using a128-bit block size and a variable length (128, 160, 192, 224, or 256 bit) key. CAST is named for its developers, Carlisle Adams and Stafford Tavares and is available internationally.CAST-256 was one of the Round 1 algorithms in the AES process.

II. Related Work

Here we discussed various mechanisms' regarding data security that is encryption and decryption methods.

Bradley Dunmore ET. Al. explores options for protecting computer network from attack across the Internet, emphasizing firewall solutions from Cisco, Symantec, Microsoft, and Check Point. It describes with general advice about how to set up a comprehensive system of defences (comprising a firewall, an intrusion detection system, authentication and cryptography schemes, and protocols like IPsec). It concludes with information on the specifics of configuring several products.

Fusan Mirza gives a basic introduction to block cipher design and analysis. The concepts and design principles of block ciphers are explained, particularly the class of block ciphers known as Feistel ciphers. Some modern block cipher cryptanalysis methods are demonstrated by applying them to variants of a weak Feistel cipher called Simplified TEA (STEA), which is based on the Tiny Encryption Algorithm (TEA).

Paul C. Kocher explains how attackers may be able to find fixed Differ-Hellman exponents, factor RSA keys, and break other cryptosystems by carefully measuring theamount of time required to perform private key operations. And explained techniques

for preventing the attack for RSA and Diffe-Hellman. He finally stated requirement of some cryptosystems to be revised to protect against the attack, and new protocols and algorithms to incorporate measures to prevent timing attacks.

Mark Stamp describes the information security into four major sections: i) Cryptography: Covers classic cryptosystems, symmetric key cryptography, public key cryptography, hash functions, random numbers and information hiding. Also, cryptanalytic techniques, including examples of attacks on cipher systems ; ii)Access Control: Focuses on authentication and authorization, password based security, ACLs and capabilities, multilevel and multilateral security, covert channels and inference control, coverage of security models such as BLP andBiba's Model, discussion of firewalls and intrusion detection systems (IDS); iii) Protocols: Focuses on generic authentication protocols and real world security protocols, such as SSL, IPsec, Kerberos and GSM; iv)Software: Discusses software flaws and malware, buffer overflows, viruses and worms, malware detection, software reverse engineering (SRE), digital rights management (DRM),secure software development and operating systems security functions, including discussion on Microsoft's "next generation secure computing base" or NGSCB.

Us. E. Gautier provides complete and easy to read explanations of common security and infrastructure protection terms. Special attention is given to terms that most often prevent educated readers from understanding journal articles or books in cryptography, computer security, information systems, role-based access management and applied fields that build on those disciplines. Also included in the dictionary are terms that refer to computing forensics, malware attacks, privacy issues, system design, security auditing and vulnerability testing. This essential reference tool presents cutting-edge information on the most recent terms in use, in one concisely formatted volume. Similar to dictionaries for languages, statistics, epidemiology, and other disciplines, The Information Security Dictionary will be a valuable addition to the library of any IT professional and IT student. The Information Security Dictionary is designed for a professional audience, composed of researchers and practitioners in industry. This dictionary is also suitable for students in computer science, engineering, and information sciences.

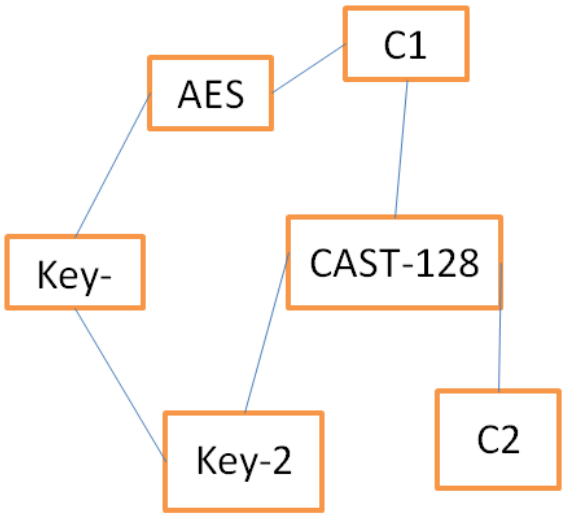

Figure 4: Hybrid encryption

III. Proposed method

In our proposed method we are using hybrid approach of combining AES method and CAST128 on same text with two different 128-bit keys as a hybrid technique. First plain text of length any size will be taken and key of 128-bit also taken apply AES on it and take this obtained cipher text C1 as input for next step and key K2 is generated from key K1 as key and applying CAST128 on it finally we will receive 128 bit cipher text.

Key generation:

First initially we take key K1 and divided that key into two parts of K->left of 32-bit and K->right of 32-bit length and apply 32-bit swap and apply x-or operation on left and right halves finally we get 64-bit key K2.

For to get back the plain text apply reverse of algorithm we will get plain text back. The procedure is shown below.

Algorithm Encryption (P, K1, K2, C1, C2)
{
Step1: take the any length of plain text P and divide into 128-bit blocks
Step2: take the length of key k1 of length 128-bit block
Step3: Apply AES operation
Step4: here we can get cipher text of 128-bit length C1
Step5: take C1 as input and K2 as second key
Step6: K2 got Key generation ()
Step7: apply CAST128 on it
Step8: we get 128 bit cipher text C2
}
Algorithm Decryption (P, K1, K2, C1, C2)
{
Step1: take 128-bit cipher text C2 as a input
Step2: and apply decryption operation of CAST128 with key K2
Step3: we obtain 128-bit cipher text C1
Step4: take C1 and key K1 and apply AES Decryption
Step5: finally we will obtain plain text P
Key generation ():
K2 is generated based on K1
Take 128 bit initial key and divide that key in two halves of 64-bit
First 64-bit key as C_{left} and second 64-bit as K_{right}
Take K_{left} and apply 32-bit swap
Take K_{right} and apply 32-bit swap
K2= (K_{left}) XOR (K_{right})

IV. CONCLUSION

This mechanism provide maximum security with operation in less time the hybrid combination of above mentioned algorithms are more secured and it also provides completion in less time as when combined and the major advantage of this method is usability of same key for double encryption which gives minimum time of computation and maximum security and cryptanalyst unable to get the key details when it encrypted twice.

V. REFERENCES

[1]. Ankid Fadia, Jaya Bhattacharjee, "Encryption, Protecting YourData", Vikash Publishing House Pvt Ltd,2007, ISBN: 812592251-2

[2]. William Stallings, "Cryptography and Network Security", FifthEdition, Person,2011, ISBN 978-81-317-6166-3

[3]. Mark Stamp, "INFORMATION SECURITY Principles andPractice", Second Edition, A JOHN WILEY & SONS INC.PUBLICATION,2011,

[4]. Urs E. Gattiker, International School of New Media, "THEINFORMATION SECURITY DICTIONARY", KLUWERACADEMIC PUBLISHERS,ISBN: 1-4020-7889-7

[5]. STEVEN FURNELL, PAUL DOWLAND, "E-mail Security APocket Guide", IT Governance Publishing, 2010, ISBN 978-1-84928-097-6

[6]. David Harley, Robert Slade, Urs Gattiker, "Viruses Revealed",Osborne/McGraw-Hill

[7]. Bradley Dunsmore, Jeffrey W. Brown, Michael Cross, "MISSIONCRITICAL! INTERNET SECURITY", Syngress Publishing Inc.,2001, ISBN: 1-928994-20-2

[8]. Fauzan Mirza, "Block Ciphers And Cryptanalysis" PhD Thesis,Department of Mathematics, Royal Holloway University of London,2001

[9]. Paul C. Kocher, "Timing Attacks on Implementations of Diffe-Hellman, RSA, DSS, and Other Systems", Cryptography ResearchInc., San Francisco, USA.

[10]. T.SubhamastanRao, M.Soujanya, T.Hemalatha, T.Revathi, "Simultaneous data compression and encryption" (IJCSIT) International Journal of Computer Science and Information Technologies, ISSN 0975-9646, Volume-2(5), 2011.

[11]. Senthil Shanmugasundaram, Robert Lourdusamy "A Comparative Study Of Text Compression Algorithms" International Journal of Wisdom Based Computing, Vol. 1 (3), December 2011.

[12]. Harshraj N. Shinde, Aniruddha S. Raut, Shubham. Vidhale, Rohit V. Sawant, Vijay A. Kotkar "A Review of Various Encryption Techniques" International Journal of Engineering And

Computer Science ISSN: 2319-7242, Volume 3, Issue 9, September 2014.
[13]. Ms. Ayushi Aggarwal, Anju "Enciphering Data for Larger Files" International Journal of Advanced Research in Computer Science and Software Engineering, ISSN: 2277 128X, Volume 3, Issue 5, May 2013.
[14]. Haroon Altarawneh, Mohammad Altarawneh "Data Compression Techniques on Text Files: A Comparison Study" International Journal of Computer Applications, (0975 – 8887), Volume 26– No.5, July 2011.
[15]. MohiniChaudhari, Dr. KanakSaxena "Fast and Secure Data Transmission using Symmetric Encryption and Lossless Compression" International Journal of Computer Science and Mobile Computing, ISSN 2320–088X, Vol. 2, Issue. 2, February 2013.
[16]. "Data Compression" by Behrouz Forouzan.
[17]. "Huffman Compression" by webopedia.
[18]. Yu-Yun Chang "Tutorial: Arithmetic Coding".
[19]. T.D.B Weerasinghe "Analysis of a Modified RC4 Algorithm" International Journal of Computer Applications, ISSN0975 – 8887, Volume 51– No.22, August 2012.
[20]. AL.Jeeva, Dr.V.Palanisamy, K.Kanagaram "Comparative Analysis of Performance Efficiency and Security Measures of Some Encryption Algorithms" International Journal of Engineering Research and Applications (IJERA), ISSN: 2277 128X, Volume 3, Issue 6, June 2013.
[21]. Mr. Vinod Saroha, Suman Mor, Anurag Dagar "Enhancing Security of Caesar Cipher by Double Columnar Transposition Method" International Journal of Advanced Research in Computer Science and Software Engineering, ISSN: 2277 128X, Volume 2, Issue 10, 2012.
[22]. Sombir Singh, Sunil K. Maakar, Dr.Sudesh Kumar "Enhancing the Security of DES Algorithm Using Transposition Cryptography Techniques" International Journal of Advanced Research in Computer Science and Software Engineering, ISSN 2249-6343, Volume 2, Issue 1, Jan 19 2012.