Hybrid Cryptography Mechanisms Using Symmetric Key For AES And CAST-128

Narasimha Raju.Dodda[1], Vinay Sita Rama Raju.Kapalli[2]
Department of Computer Science and Engineering
[1, 2]Shri Vishnu Engineering College for Women,Bhimavaram,Andhrapradesh,India.

Abstract-*Crucial methods are introduced to deploy the majority networks to acquire the required data. Because of the defect of only the single data encryption and the use of famous encryption algorithm, which was not improved in traditional methods of the registration process, a combined encryption algorithm is proposed in this thesis. 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. In this paper we provide both the encryption and decryption that supports in real time application and algorithm has a practical value.*

Keywords-Hybrid encryption, Advance Encryption Standard (AES), CAST-128, Key length.

I. INTRODUCTION

Earlier, when man was still in the process of evolution, his needs were simple, food, water, and shelter was all that was required. As man started climbing the rungs of the evolution ladder, his needs began to increase and multiply. They were no longer simple. The needs of the man brought out the industrial revolution and ushered us into the age of technology and prosperity. But as man stepped into the new era, new struggles came forth. Those struggles gave birth to the need of data security as well. How to protect privileged sensitive information from falling into wrong hands or from being stolen? The answer was cryptography. Now, cryptography is not something new. According to our historians, Roman King Julius Caesar was the first to devise and incorporate cryptography techniques during his reign. Cryptography is the study of hiding information by converting the sensitive information (or plain text) into an unintelligible text (or cipher text) using a suitable encryption technique so that it cannot be understood by any unintended individual, and then converting it back to its original form for the intended receiver using some decryption technique. Cryptography is derived from two Greek words: “kryptos” meaning ‘hidden’ and “graphein” meaning ‘to write’ i.e. hidden writing. The main feature of cryptography is the use of a secret key to encrypt and decrypt the sensitive information. Cryptography is not only restricted to providing confidentiality and privacy but also provides authentication, data integrity, non-repudiation etc. Parameters considered while adopting a cryptographic technique are memory usage, security, design, robustness, etc. Cryptographic techniques can be broadly divided into two broad spectrums: Asymmetric Key Cryptography and Symmetric Key Cryptography.

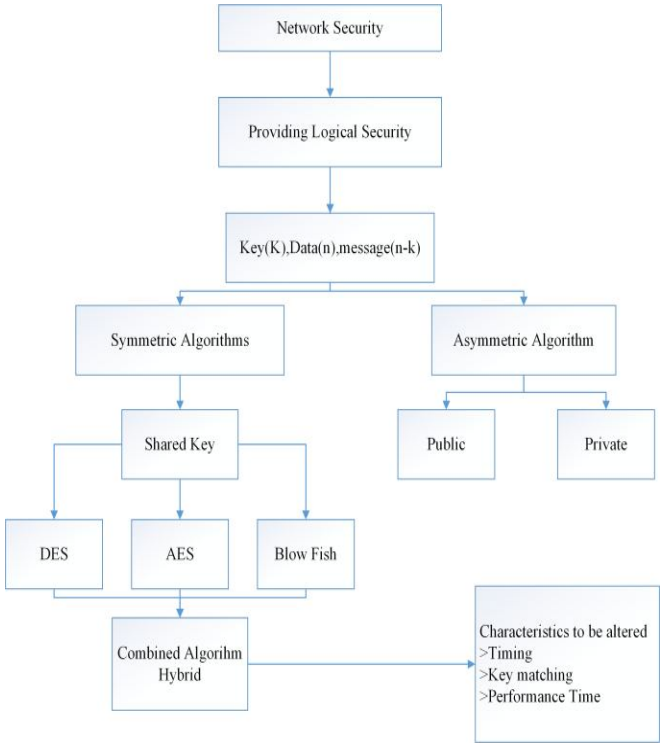


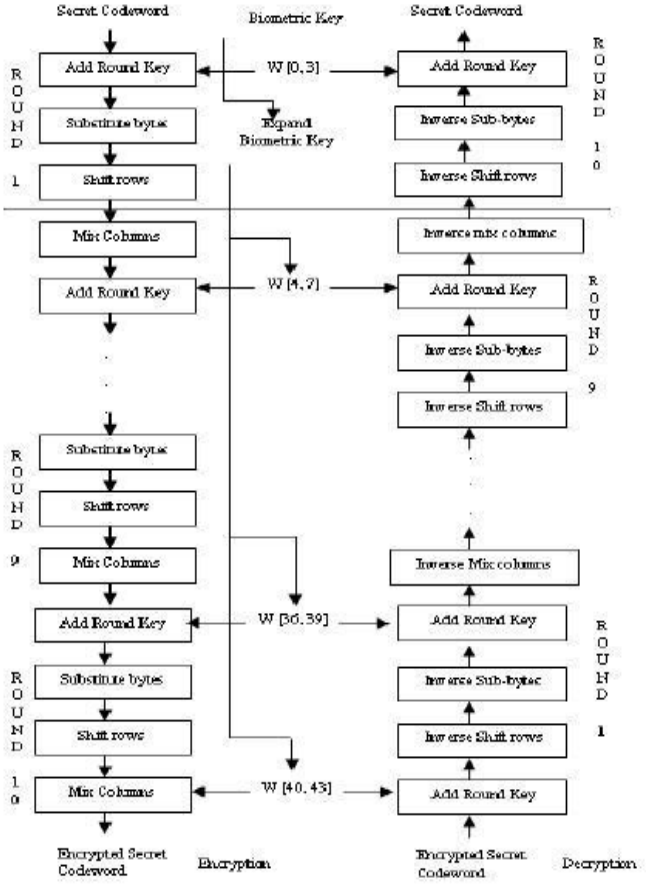
Fig1: Overview of Hybrid cryptography using symmetric encrption algorithms

A third one involving Hash Functions is also used extensively. Symmetric Key Cryptography uses a single key for the purpose of encryption and decryption, and is shared with both the sender and the receiver. Fig.1 shows the Overview of Hybrid cryptography using symmetric encrption algorithmsIt is one of the earliest used technique of cryptography. Asymmetric Key Cryptography on the other hand uses two keys for the purpose of encryption and

decryption .In this paper we are proposing a novel and hybrid algorithm for data encryption that is here we use two existing techniques AES and CAST128 and combined them and do encryption. The remaining paper is as follows. Section-2 deals about the literature survey, section-3 deals the proposed method, section-4 gives the result analysis and finally section-5 concludes the paper.

II. LITERATURE WORK

We commonly have two types of encryption algorithms (a) symmetric key encryption, (b) Asymmetric key encryption algorithm. Where symmetric key uses a shared key and other algorithm uses private key and public key. Here we analyse three algorithms they are: Advanced Encryption Standard (AES), CAST128 Algorithm. Here we discuss about AES and CAST128 algorithms in detail.



In 1997 NIST along with FIPS standard formed a new symmetric key algorithm. AES has 64 bit block size. In AES we have 128, 192 and 256 bit key size with 10, 12 and 14 rounds respectively. In AES the data and key is mixed to form key by implying, following steps.

a. Key Expansion:

Initially the key is expanded into two halves to form a bigger key using addition of padding bits.

b. Round Key:

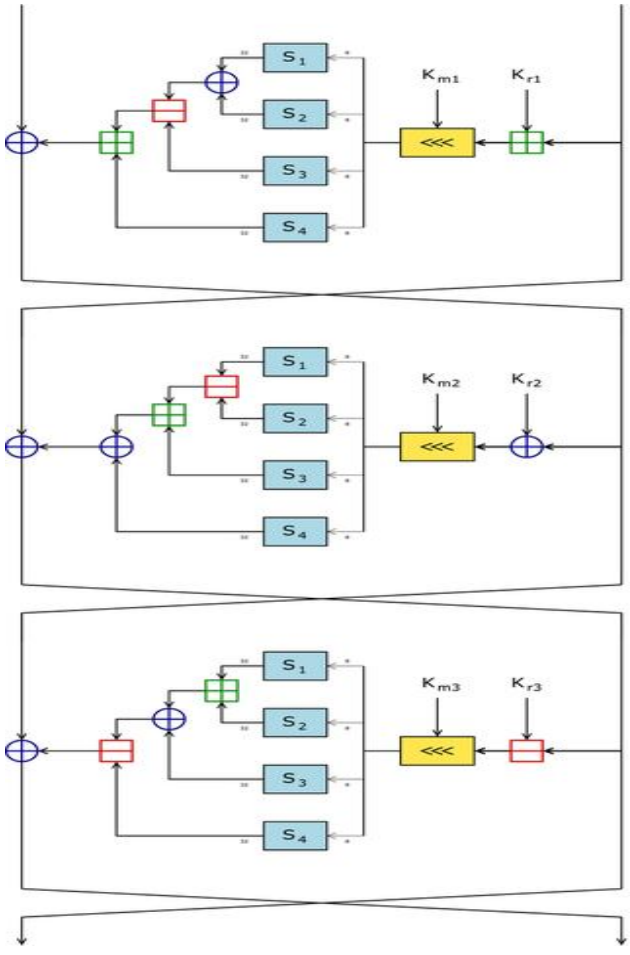
Then we add round key (k1) with the initial key using XOR operation.

c. Round operation (N-1) rounds:

Usually we have 10,12 and 14 rounds here, we usually follow the same steps for first(N-1) rounds and last round will be different , here first we do substitution operation using look up table then rows are shifted, the columns are mixed, each time round key is added to form new key.

d. Final Round:

In final round, when previous round key is added we do substitution, then shifting of rows and round key is added. Then finally all round keys are added to form a strong key.
few adaptations of GPG and PGP.



CAST128

In cryptography, CAST-128 (on the other hand CAST5) is a symmetric-key square cipher utilized as a part of various items, outstandingly as the default cipher in a It has additionally been endorsed for Government of Canada use by the Communications Security Establishment. The calculation was made in 1996 via Carlisle Adams and Stafford Tavares utilizing the CAST outline procedure. Another individual from the CAST group of ciphers, CAST-256 (a previous AES applicant) was gotten from CAST-128. As per a few sources, the CAST name depends on the initials of its designers, however Bruce Schneier reports the creators' claim that "the name ought to invoke pictures of randomness".

CAST-128 is a 12-or 16-round Feistel connect with a 64-bit square size and a key size of in the vicinity of 40 and 128 bits (yet just in 8-bit increases). The full 16 rounds are utilized when the key size is longer than 80 bits Parts incorporate substantial 8×32-piece S-boxes in view of twisted capacities, key-subordinate pivots, and measured expansion and subtraction, and XOR operations. There are three exchanging sorts of round capacity, yet they are comparable in structure and contrast just in the decision of the correct operation (expansion, subtraction or XOR) at different focuses. Despite the fact that Entrust holds a patent on the CAST plan technique, CAST-128 is accessible worldwide on an eminence free reason for business and non-business employments.

AnkitFadia and Jaya Bhattacharjee [] describe how to encrypt data in such a way so as to protect it from outsiders. It describes the definition of encryption and decryption and explanation of how encryption works with the growing need to safeguard one’s privacy in communication and transaction. They explained the concept of developing a key details, cryptography, the most popular encryption algorithms, how encryption works, digital signature, digital certificates, and most importantly. Some real-life practical examples of where encryption can be put to use is explained in chapter 6 page 248-284. They supported a statement in chapter 5 page 238 “….Encryption alone can be defeated is absolutely true”. William Stallings [] describes in different Part at his book: Part One: Provides a survey of symmetric encryption, including classical and modern algorithms at. The emphasis is on the two most important algorithms, the Data Encryption Standard (DES) and the Advanced Encryption Standard (AES). This part also covers the most important stream encryption algorithm, RC4, and the important topic of pseudorandom number generation. Part Two: Provides a survey of Asymmetric Ciphers including RSA (Rivest-Shamir-Adelman) and elliptic curve. Part Three: Begins with a survey of cryptographic hash functions. This part then covers two approaches to data integrity that rely on cryptographic hash functions: message authentication codes and digital signatures. 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 and Biba'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. Urs. E. Gattiker[] 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. STEVEN FURNELL and PAUL DOWLAND[] guides to Defend our business from attack , Use email clients to improve security, Preserve confidentiality, Protect our company's reputation The pocket guide provides a concise reference to the main security issues affecting those that deploy and use email to support their organizations, considering email in terms of its significance in a business context, and focusing upon why effective security policy and safeguards are crucial in ensuring the viability of business operations. For Our business or office relies on email for its everyday dealings with official staff, partners, suppliers and

customers. While email is an invaluable form of communication, it also represents a potential threat to our information security. Email could become the means for criminals to install a virus or malicious software on our computer system and fraudsters will try to use emails to obtain sensitive information through phishing scams. If we want to safeguard our organization's ability to function, it is essential to have an effective email security policy in place, and to ensure our staff understand the risks associated with email. This pocket guide will help businesses or office to address the most important issues. Its comprehensive approach covers both the technical and the managerial aspects of the subject, offering valuable insights for IT professionals, managers and executives, as well as for individual users of email. David Harley et. al.[] guide to defending our system against the real threat of computer viruses. It presents a soup-to-nuts, full-bodied analysis on computer virus protection by offering: i) Current information on the expanding domain of computer viruses; ii) Real world case studies of virus infestations, solutions, and methods of prevention; iii) Practical problem and solution analysis of the modern day virus threat.

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 another 128-bit key K2 as key and applying CAST128 on it finally we will receive 128 bit cipher text.

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: apply CAST128 on it
Step7: 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
}

IV. ADVANTAGES AND SHORTCOMINGS OF PROPOSED METHOD

The major advantage of this method is high secure data because up-to now no cryptanalyses attacks on AES and CAST128, here we use combination of both; it provide high security to the data.

And it is easy to implement and complex to identify.

Drawback of this method is 2 two different keys for two phases.

V. CONCLUSION

An efficient algorithm should 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.

REFERENCES

[1] Sowmya nag k., h.b.bhuvaneswari, nuthana.c, “Implementation of advanced encryption Standard-192 bit using multiple keys” ieeetranscation,vol 5,pg34-39,2012.
[2] Najib A. Kofahil ,“Performance evaluation of three Encryption/ decryption algoriithms” ISSN 0-7803-8294-3 IEEE,2014
[3] William Stallings “Cryptography and Network Security”, Third Edition, Pearson Education Asia Publication, 2007
[4] Jawahar Thakur, Des, Aes And Blowfish: Symmetric Key Cryptography Algorithms Simulation Based Performance Analysis”, International Journal of Emerging Technology and Advanced Engineering, ISSN 2250-2459, Volume 1, Issue 2, December 2011
[5] Dr. Mohammed M. Alani “DES96 - Improved DES Security”, 7th International Multi-Conference on Systems, Signals and Devices,2010.
[6] Seung-johan “The improved data encryption standard (des) algorithm”Ieee transaction ISSN 0-7803-3567-8,volume ,issue ,December 1996.
[7] Michael C.-J. Lin “A VLSI Implementation of the Blowfish Encryption/Decryption Algorithm” National Science Council, R.O.C, NSC 88-2215-E-007-025.

[8] Taiping Mo "Design of secure communications network system based on data encryption and digital signature" ISSN 978-1-61284-383-4,IEEE,2011.

[9] Daemen, J., and Rijmen, V. "Rijndael: The Advanced Encryption Standard." D r. Dobb's Journal, March 2001, pp. 137-139

[10] Lei Zhang, Futai Zhang, "Certificateless Partially Blind Signatures," The 1st International Conference on Information Science and Engineering (ICISE), pp. 2883 – 2886, Dec 26-28, 2009.

[11] Penchalaiah, N. and Seshadri, R. "Effective Comparison and Evaluation of DES and Rijndael Algorithm (AES)", International Journal of Computer Science and Engineering, Vol. 02, No. 05, 2010, 1641-1645.

[12] Rivest, R. L., Shamir, A., Adelmann, L.: "A method for obtaining digital signature and public –key cryptosystems", Commun. ACM, 1978, VOL. 21, pp. 120-126