ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Cryptanalysis of Different Data Encryption Standards to Improve Robustness

J.Santosh Kumar
Dept of Electronics and Communication Engineering, Sri Venkateswara College of Engineering and Technology, Srikakulam, AP, India.

P.Dalinaidu
Dept of Electronics and Communication Engineering, Sri Venkateswara College of Engineering and Technology, Srikakulam, AP, India.

Abstract:

Encryption techniques are used essentially by the network security service to ensure the secret of information Open or private encryption keys can be utilized, contingent upon the particular of every administration and application. A standout amongst the most performing open encryption calculations is RSA (Rivest-Shamir-Adleman). Some private encryption calculations, likewise called symmetric calculations, are DES (Data Encryption Standard), TDES (Triple DES) and AES (Advanced Encryption Standard) [3]. These calculations utilize distinctive length of the encryption keys, from 64-bits up to 256-bits. Longer encryption keys increment the heartiness of the calculations against the beast compel assault. The relationship between's the plain-content and the figure content can be misused by the attackers to conclude the encryption key or, specifically, the first information. Along these lines it is critical to decrease the relationship between's the underlying message also, the encoded form of it utilizing augmented information structures for square encryption calculation, longer encryption key arrangements and non-direct operations. The significant objective of this paper is the investigation of connection in various instances of changed encryption methods.

Keywords:
Cipher-text, Cryptography, CRC, Network Security

1. Introduction:

The Advanced Encryption Standard (AES) has been a candidate algorithm for encrypting data in Wireless Sensor Network (WSN) [1]. When AES circuit is used in the source limited WSN embedded system, low power and small area are mandatory requirements. Considering that unprotected AES hardware is vulnerable to Differential Power Analysis (DPA), ensuring the AES hardware is free of DPA is very important too. As the only non-linear structure in AES circuit, the AES SBox dominates the hardware complexity of the AES circuit. The efficiency of AES hardware implementation in terms of size, speed, security and power consumption depends largely on the implementation of S-Box [2]. Since there are many design options for the S-Box in hardware, it is challenging to find an optimal implementation for a particular purpose. Many implementations for S-Box have been proposed and their performances have been evaluated by using ASIC CMOS libraries [2,3,4,5]. However, there is no report using the full-custom design methodology, as far as the authors know. In this paper, the main research focuses on the full-custom hardware implementation of S-Box for wireless sensor node chips. Using the inverse transformation in Galois field algorithm can reduce the computation cost of the S-Box and is far better suited for hardware implementation. Wolkerstorfer et al. used the composite field GF((24)2) to achieve a compact ASIC implementation [4].

But this implementation dissipated too high power consumption to meet the requirement for the WSN applications. Moreover, this SBox circuit cannot against DPA. Therefore, we modified the implementation as follows. Firstly, since the logic style affects the power dissipation, speed, wiring load and the size of transistor, the choice of logic style needs to be considered for the full-custom circuits. Pass transistor logic (PTL) is a promising alternative to conventional CMOS logic for low-power applications due to the decreased node capacitance and reduced transistor count it offers [6]. The basic difference of PTL compared to the CMOS logic style is that the source side of the logic transistor networks is connected to some input signals instead of the power lines.

Thus, one pass transistor network (either NMOS or PMOS) is sufficient to perform logic operation. Being a kind of PTL, pass transmission gate (PTG) offers the excellent energy performance and occupies less than half the area of CMOS. It was used to design the presented S-Box. In addition, to achieve the low die-size, we also designed a novel 3-input exclusive- OR (denoted XOR) gate based on a compact three-transistor XOR cell. DES algorithm used for encryption of the electronic data. It was developed in the early 1970s at IBM and based on an earlier design by Horst Feistel, the algorithm submitted to the National Bureau of Standards (NBS) to propose a candidate for the protection of sensitive unclassified electronic government data.

It is now taken as unsecured cause of its small size and a brute force attack is possible in it. In January 1999 distributed .net and the Electronic Frontier Foundation (EFF) collaborated to publicly break a DES key in 22 hours and 15 minutes. The algorithm is believed to be practically secure in the form of Triple DES, although there are theoretical attacks. In recent years, the cipher has been superseded by the Advanced Encryption Standard (AES).

2. Related Work:

It is important to cut back the correlation between the initial message and therefore the encoded version of it using enlarged knowledge structures for block cryptography rule, longer cryptography key sequences and non-linear operations [1]. • The major advantage of pattern primarily based cryptography is that it's tough to crack, however it's straightforward to implement [2]. Most hackers exploit the correlation between the cipher and plain text thus a brand new coding theme is needed specified, although the hacker gets a touch, it ought to be tough for him to crack. The image pattern methodology will increase the information security to nice extent. during this methodology the carrier image is generated by using a particular code referred to as four out of eight-code and addition of carrier image to original image that result into the encrypted image [3] .The four to eight digit code is additionally venerable, thus instead of encrypting a picture in its original pattern, this paper provides another approach inside that image is split into entirely completely different parts so it unified in to a pattern that is entirely known to approved parties.

The rule starts with degree of initial round followed by variety of normal rounds and it ends with the ultimate round solely four completely different operations area unit necessary to cipher these rounds and a key schedule. It is possible in Rijndael to use completely different key lengths in keeping with the protection level that's needed for the applying. Rijndael is outlined as a block cipher with key lengths of 128, 192 or 256 bits. The possible input block lengths are 128, 192 or 256 for the Rijndael rule. The AES rule is strictly similar because the Rijndael rule, however it solely defines one block length of 128 bits. The Rijndael rule is such every bit depends on all bits from a pair of rounds past, e.g. full diffusion is provided. The quantity of rounds that has to be run depends on the key length. Cryptography is that the science of constructing communication unintelligible to everybody except the meant receiver(s).

It's the study of strategies of causing messages in disguised type in order that solely meant recipients will take away the disguise and skim the message. Cryptography offers economical answer to shield sensitive data in an exceedingly sizable amount of applications together with personal information security, net security, diplomatic and military communications security, etc through the processes of encryption/decryption. A cryptosystem may be a set of algorithmic program, indexed by some keys(s), for encryption messages into cipher text and secret writing them into plaintext.

3. DES(Data Encryption Standard):

DES is that the first block cipher—An formula that takes a fixed-length string of plaintext bits and transforms it through a series of difficult operations into another cipher text bit string of identical length. Among the case of DES, the block size is sixty four bits. DES to boot uses a key to customize the transformation therefore cryptography can supposedly solely be performed by those who acknowledge the particular key used to cipher. The key apparently consists of sixty four bits; however, solely fifty six of these are actually used by the algorithmic program. Eight digit code are used completely for checking parity, and are thenceforth discarded. Therefore the effective key length is fifty six bits.

The secret's nominally keep or transmitted as eight bytes, each with odd parity. in line with ANSI X3.92-1981. One bit in each 8-bit byte of the KEY might even be used for error detection in key generation, distribution, and storage. Bits 8, 16,... sixty four are to be employed in making certain that each byte is of wierd parity. Like totally different block ciphers, DES by itself is not a secure suggests that of secret writing but ought to instead use during a mode of operation. FIPS-81 specifies several modes to be used with DES. Cryptography uses identical structure as secret writing but with the keys utilized in reverse order.

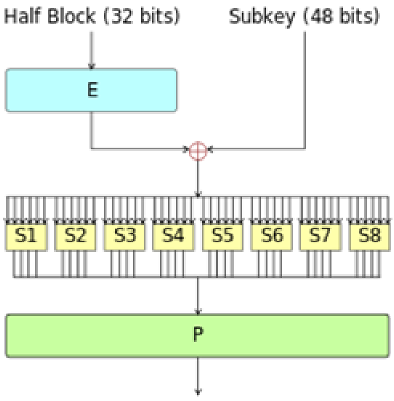


Fig 1. Function of DES

Expansion: the 32-bit half-block is expanded to forty eight bits using the enlargement permutation, denoted E within the diagram, by duplicating half the bits. The output consists of eight six-bit (8 * 6 = forty eight bits) items, every containing a replica of four corresponding input bits, and a replica of the at once adjacent bit from every of the input items to either side. Key mixing: the result's combined with a sub key using Associate in Nursing XOR operation. Sixteen 48-bit sub keys—one for every round—are derived from the most key using the key schedule. Substitution: when intermixture within the sub key, the block is split into eight 6-bit items before process by the S-boxes, or substitution boxes. Every of the eight S-boxes replace its six input bits with four output bits in line with a non-linear transformation, provided within the type of a operation table. The S- boxes offer the core of the protection of DES—without them, the cipher would be linear, and trivially breakable. Permutation: finally, the thirty two outputs from the S-boxes are rearranged in line with a set permutation, the P-box. this is often designed in order that, when permutation, every S-box's output bits are unfold across four totally different S boxes within the next spherical.

4. 3DES(Triple Data Encryption Standard):

In 1998 a standard ANS X9.52 and named Triple Data Encryption Algorithm (TDEA).

a. Block cipher with symmetric secret key

b. Block length = 64 bits

c. Key length = 56, 112 or 168 bits

3DES was created because DES algorithm, invented in the early 1970s using 56-bit key. The effective security 3DES provides is only 112 bits due to meet-in-the-middle attacks. Triple DES runs three times slower than DES, but is much more secure if used properly. The procedure for decrypting something is the same as the procedure for encryption, except it is executed in reverse. In DES, data is encrypted and decrypted in 64 -bit chunks. The input key for DES is 64 bits long; the actual key used by DES is only 56 bits in length. The least significant (right-most) bit in each byte is a parity bit, and should be set so that there are always an odd number of 1s in every byte. These parity bits are ignored, so only the seven most significant bits of each byte are used, resulting in a key length of 56 bits. This means that the effective key strength for Triple DES is actually 168 bits because each of the three keys contains 8 parity bits that are not used during the encryption process.

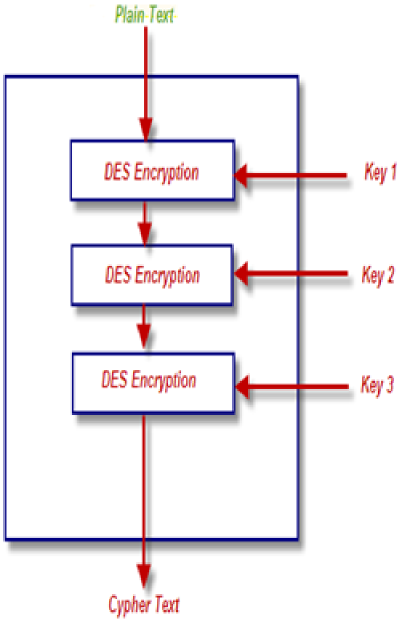


Fig 2. working of Triple DES

Triple DES is advantageous because it has a significantly sized key length, which is longer than most key lengths affiliated with other encryption modes.

DES algorithm was replaced by the Advanced Encryption Standard and Triple DES is now considered to be obsolete. It derives from single DES but the technique is used in triplicate and involves three sub keys and key padding when necessary. Keys must be increased to 64 bits in length Known for its compatibility and flexibility can easily be converted for Triple DES inclusion.

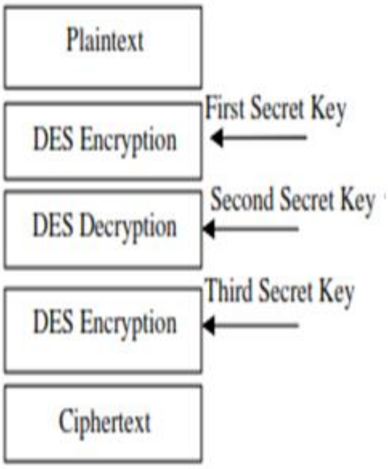


Fig 3. Block diagram of 3DES encryption

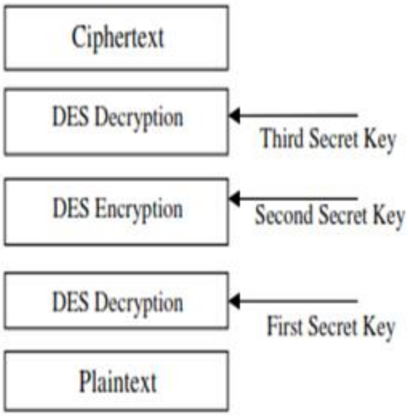


Fig 4 .Block diagram of 3DES decryption

5. AES(Advanced Encryption Standard):

In 1997 the National Institute of Standards and Technology (NIST) of the United States place out a involve proposals for a replacement regular algorithm, which is able to be referred to as the Advanced Encryption Standard (AES). The candidates for the AES algorithm had to satisfy sure normal.

First, of course the algorithm have to be compelled to be a regular algorithm and it ought to be resistant against all superb attacks. what's additional, the AES ought to be economical in performance and memory for varied platforms. The look ought to be easy, and it have to be compelled to be ready to handle fully completely different key lengths (128, 192 and 256 bits). The block length of the cipher have to be compelled to be 128 bits.

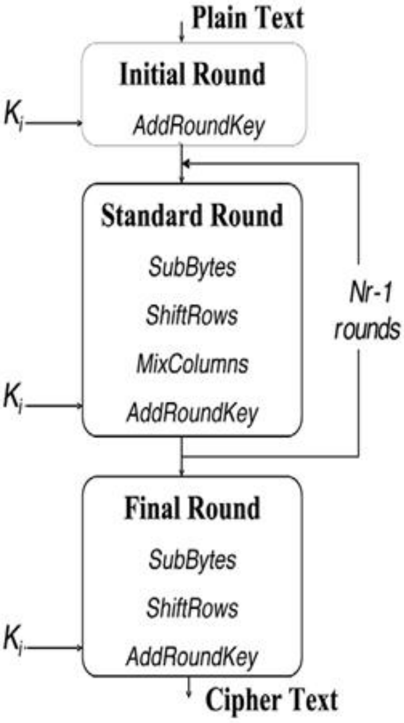


Fig 5 . Overview of AES

The rule starts with degree of initial round followed by variety of normal rounds and it ends with the ultimate round solely four completely different operations area unit necessary to cipher these rounds and a key schedule. It is possible in Rijndael to use completely different key lengths in keeping with the protection level that's needed for the applying. Rijndael is outlined as a block cipher with key lengths of 128, 192 or 256 bits. The possible input block lengths are 128, 192 or 256 for the Rijndael rule. The AES rule is strictly similar because the Rijndael rule, however it solely defines one block length of 128 bits.

The Rijndael rule is such every bit depends on all bits from a pair of rounds past, e.g. full diffusion is provided. The quantity of rounds that has to be run depends on the key length.

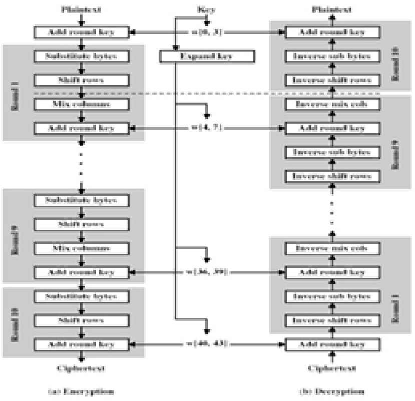


Fig 6. Overall Structure of AES

AES Key Expansion:

The key is copied into the first four words of the expanded key. The remainder of the expanded key is filled in four words at a time. Each added word **w**[i] depends on the immediately preceding word, **w**[i − 1], and the word four positions back **w**[i − 4]. In three out of four cases, a simple XOR is used. For a word whose position in the **w** array is a multiple of 4, a more complex function is used. The first eight words of the expanded key using the symbol g to represent that complex function. The function g consists of the following sub functions:

1.RotWord performs a one-byte circular left shift on a word. This means that an input word [b0, b1, b2, b3] is transformed into [b1, b2, b3, b0].

2. SubWord performs a byte substitution on each byte of its input word, using the s-box described earlier.

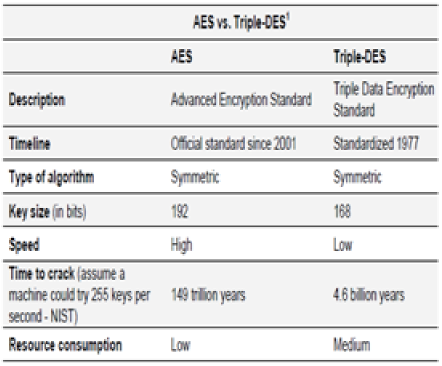
3. The result of steps 1 and 2 is XORed with round constant, Rcon[j].

The round constant is a word in which the three rightmost bytes are always 0.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Thus the effect of an XOR of a word with Rcon is to only perform an XOR on the leftmost byte of the word. The round constant is different for each round and is defined as Rcon[j] = (RC[J], 0,0,0), with RC[1]= 1, RC[j]= 2• RC[j −1] and with multiplication defined over the field GF(28).The key expansion was designed to be resistant to known cryptanalytic attacks. The inclusion of a round-dependent round constant eliminates the symmetry, or similarity, between the way in which round keys are generated in different rounds.

6. Results:

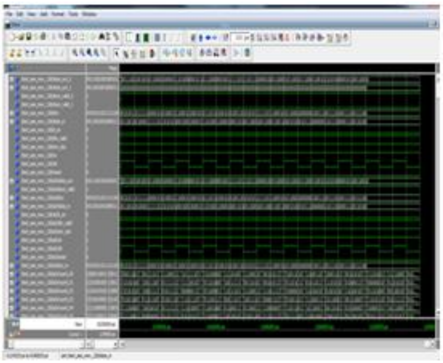


AES vs. Triple-DES[1]

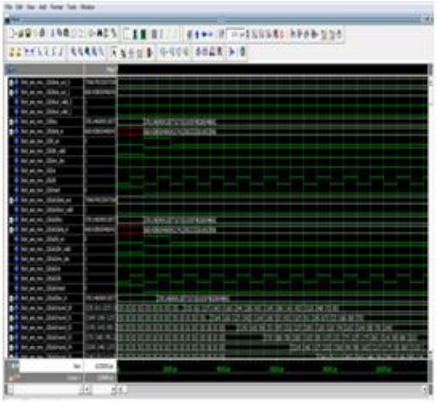
	AES	Triple-DES
Description	Advanced Encryption Standard	Triple Data Encryption Standard
Timeline	Official standard since 2001	Standardized 1977
Type of algorithm	Symmetric	Symmetric
Key size (in bits)	192	168
Speed	High	Low
Time to crack (assume a machine could try 255 keys per second - NIST)	149 trillion years	4.6 billion years
Resource consumption	Low	Medium

Comparison of AES and TDES

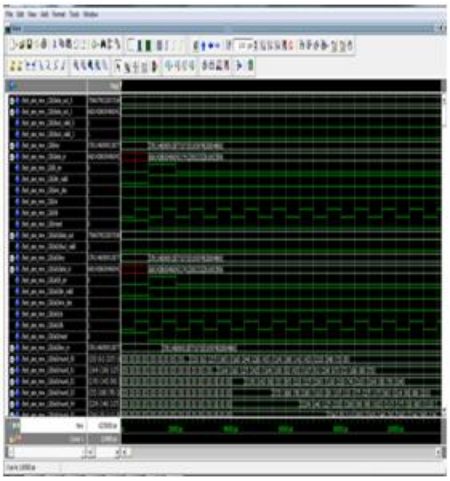
DES output:



TDES output:



AES(Encryption) output:



Decryption output:

7. Conclusion:

In today's circumstance one among the principle necessities is to utilize compelling strategies in order to shield learning from unapproved get to if relate guilty party some way or another figures out how to take the data. The paper points could be a survey of cryptography and its fluctuated components. The paper also talks about the working of DES, 3DES and DES calculations. The papers proposes different encryption standards. Three types of algorithms have been designed and from the analysis reports it is proved that AES algorithm for best encryption standard.

References:

[1].“A Study Of Methods Used To Improve Encryption Algorithms Robustness”, Scripcariu, L., IEEE 2015.

[2]“New Cryptographic Technique For Enhancing Security”,Aamir Mohammed Suhail , Anuraag Vyas, Meghana Gudivada, Prof.T.Venkat Narayana Rao ,International Journal of Scientific & Engineering Research,2015.

[3]A potent approach to enhance security extent of an image during image encryption, Kainth, K.IEEE,2015.

[4]“A Performance Comparison of Data Encryption Algorithms” Nadeem, A. ,Javed, M.Y. IEEE, 2005.

[5]“A Comparative Survey Of Symmetric Encryption Techniques For Wireless Devices”,Anjali Patil, Rajeshwari Goudar ,August , 2013.

[6]“A Review and Comparative Analysis of Various Encryption Algorithms”,Rajdeep Bhanot and Rahul Hans,International Journal of Security and Its Applications, 2015.

[7]“A COMPARATIVE ANALYSIS OF CRYPTOGRAPHY ALGORITHMS “, M.B.Nivetha1, Mr.S.Sivarama krishnan, IJIREECE,2014.

[8] “A Survey on the Applications of Cryptography”, Shivangi Goyal University School Of Information ,(International Journal of Engineering and Technology Volume 2 No. 3, March, 2012.

[9] “Text and Image Encryption Decryption Using Advanced Encryption Standard”, Kundankumar Rameshwar Saraf, Vishal Prakash Jagtap, Amit Kumar Mishra , International Journal of Emerging Trends & Technology in Computer Science (IJETTCS).

[10]“Efficient Implementation of AES”, « International Journal of Advanced Research in Computer Science and Software Engineering”, Volume 3, Issue 7, July 2013.

Author’s Details:

Jami Santhosh Kumar pursuing his M.Tech in the department of Electronics and Communication Engineering (VLSI), Sri Venkateswara College of Engineering & Technology, Etcherla, Srikakulam, A.P., India. Affiliated to Jawaharlal Nehru Technological University, Kakinada. Approved by AICTE, NEW DELHI. He obtained his B.Tech (ECE) from Sri Sivani Institute Of Technology, Chilakapalem, Srikakulam.

Paila Dalinaidu working as Assistant Professor, in the department of Electronics and Communication Engineering(VLSI), Sri Venkateswara College of Engineering & Technology, Etcherla, Srikakulam. He obtained his M.Tech from Pydah College Of Engineering And Technology, Vizag. His area of interest in VLSI and Digital Image Processing.