JES
Journal of Engineering Sciences

Vol 13, Issue 05, May /2022
ISSN NO: 0377-9254

DESIGN IMPLEMENTATION AND COMPARATIVE ANALYSIS OF ADVANCED ENCRYPTION STANDARD (AES) ALGORITHM

S. CHARAN[1], N. SAI PAVAN[1], N. SURJEETH[1], V. AKHIL[1], Dr. A. Pradeep Kumar[1]
[1]Department of Electronics and Communication Engineering, Malla Reddy Engineering College (A), Secunderabad, Telangana, India

ABSTRACT

Security is major concern in data handling, communication, messagetransmission and electronic transaction on public network. Cryptography (secret writing) is the encryption process of transformation of messages to make information secure and resistant to attack. AES is symmetric encryption standard recommended byNIST. AES is proved to be highly secure, faster and strong encryption algorithm. AESis used commonly because of its great competence and easiness. But in recent years cyber-attacks are continuously developing, therefore security specialists must stay busyin the lab inventing new schemes to keep attackers at bay. Possible attacks on symmetric algorithm can be Brute-force Attack, Differential Attack, Algebraic Attackand Linear Attack. So to provide strong security in message transmission, AES algorithm with hybrid approach of Dynamic Key Generation and Dynamic S-box Generation is proposed. In hybrid approach first we will add more complexity in data to increase Confusion and Diffusion in Cipher text by using Dynamic Key Generationand then by using Dynamic S-Box Generation we will make it difficult for attacker to do any down study of static set of S-box.

1. INTRODUCTION

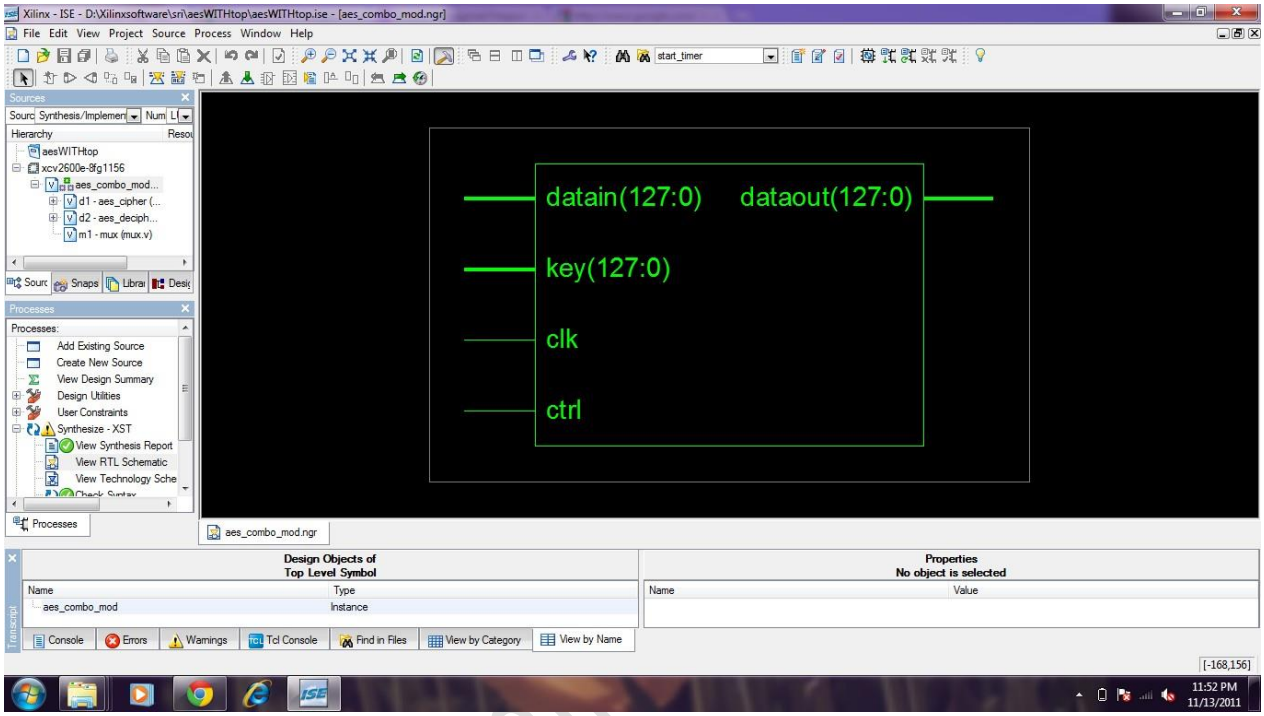
Very-large-scale integration (VLSI) is the process of creating integrated circuits by combining thousands of transistor-based circuits into a single chip. VLSI began in the 1970s when complex semiconductor and communication technologies were being developed. The microprocessor is a VLSI device. The term is no longer as common as it once was, as chips have increased in complexity into the hundreds of millions of transistors.The first semiconductor chips held one transistor each. Subsequent advances
added more and more transistors, and, as a consequence, more individual functions

2. PROPOSED METHOD

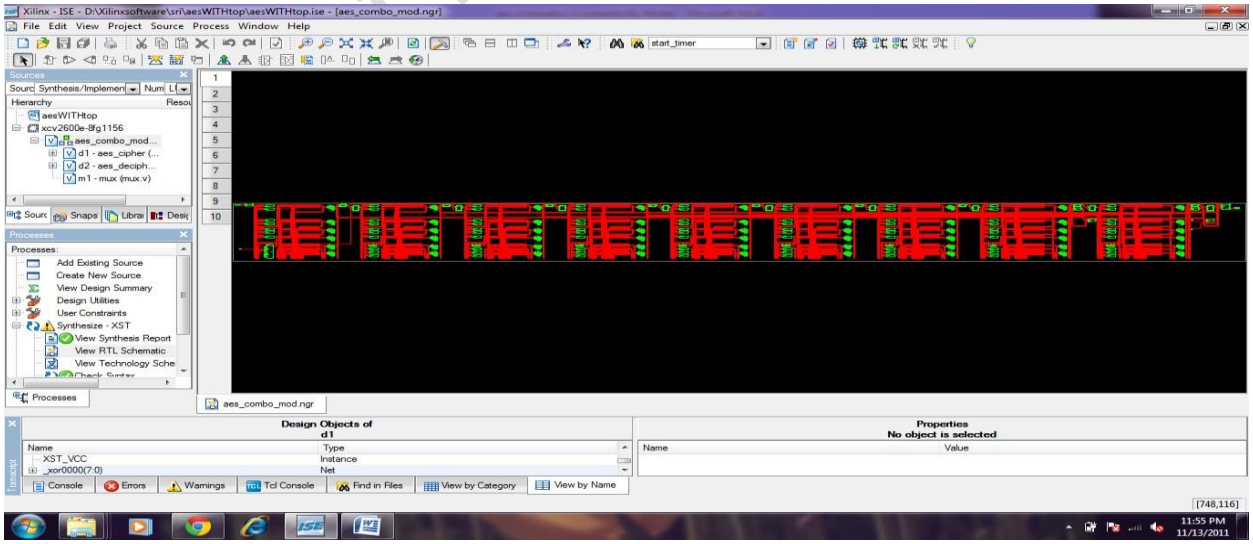
systems were integrated over time. The first integrated circuits held only a few devices, perhaps as many as ten diodes, transistors, resistors and capacitors, making it possible to fabricate one or more logic gates on a single device. Now known retrospectively as "small-scale integration" (SSI), improvements in technique led to devices with hundreds of logic gates, known as large-scale integration (LSI), i.e. systems with at least a thousand logic gates. Current technology has moved far past this mark and today's microprocessors have many millions of gates and hundreds of millions of individual transistors.At one time, there was an effort to name and calibrate various levels of large-scale integration above VLSI. Terms like Ultra-large-scale Integration (ULSI) were used. But the huge number of gates and transistors available on common devices has rendered such fine distinctions moot. Terms suggesting greater than VLSI levels of integration are no longer in widespread use. Even VLSI is now somewhat quaint, given thecommon assumption that all microprocessors are VLSI or better.As of early 2008, billion-transistor processors are commercially available, an example of which is Intel's Montecito Itanium chip. This is expected to become more commonplace as semiconductor fabrication moves from the current generation of 65 nm processes to the next 45 nm generations (while experiencing new challenges such as increased variation across process corners). Another notable example is NVIDIA’s 280 series GPU.This microprocessor is unique in the fact that its 1.4 Billion transistor count, capable of a teraflop of performance, is almost entirely dedicated to logic (Itanium's transistor count is largely due to the 24MB L3 cache). Current designs, as opposed to the earliest devices, use extensive design automation and automated logic synthesis to lay outthe transistors, enabling higher

levels of complexity in the resulting logic functionality. Certain high-performance logic blocks like the SRAM cell, however, are still designed byhand to ensure the highest efficiency (sometimes by bending or breaking established designrules to obtain the last bit of performance by trading stability).

3. RESULTS



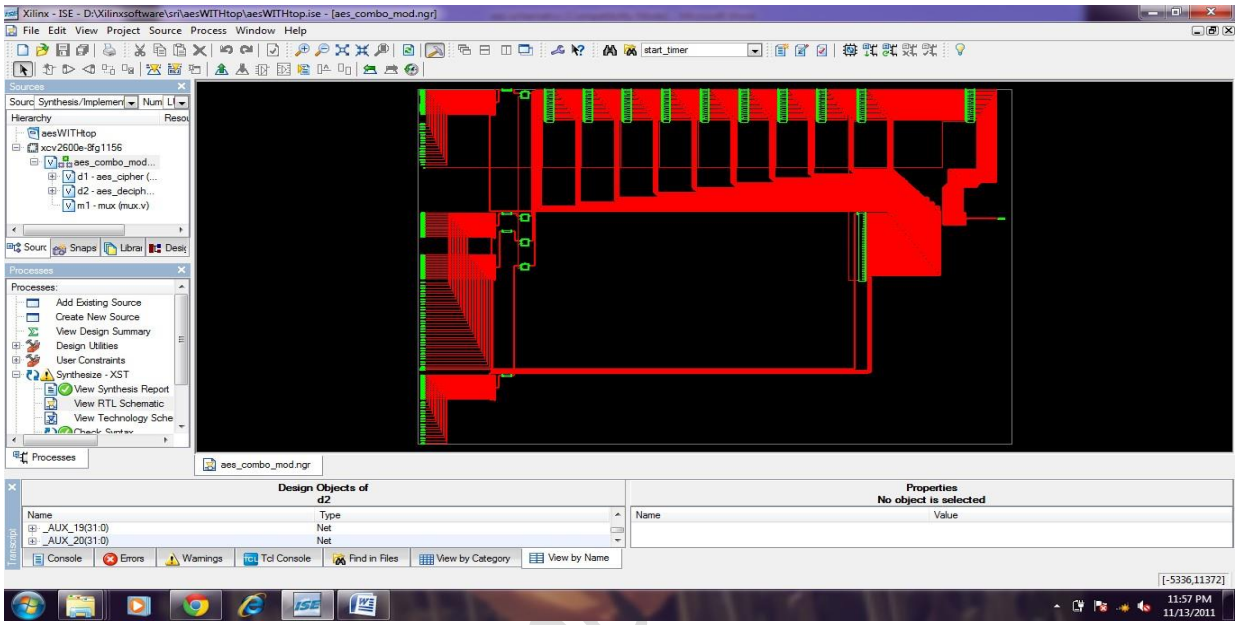
RTL SCHEMATIC OF ENCRYPTION



RTL SCHEMATIC OF DECRYPTION

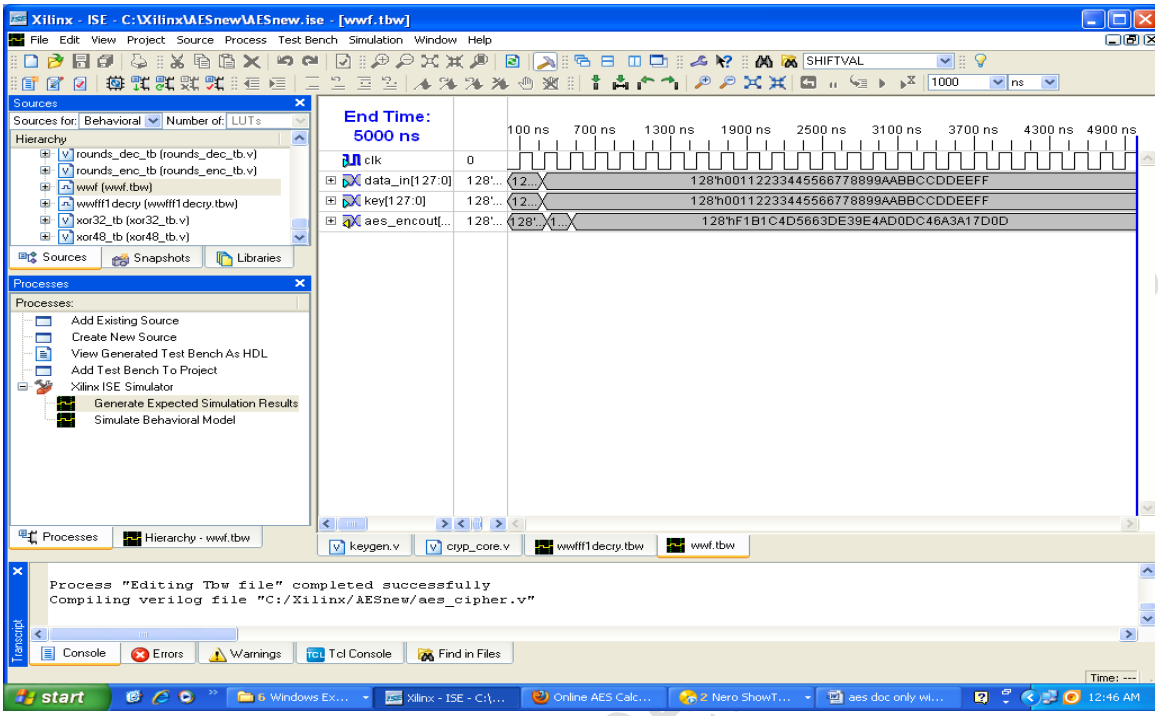
Journal of Engineering Sciences

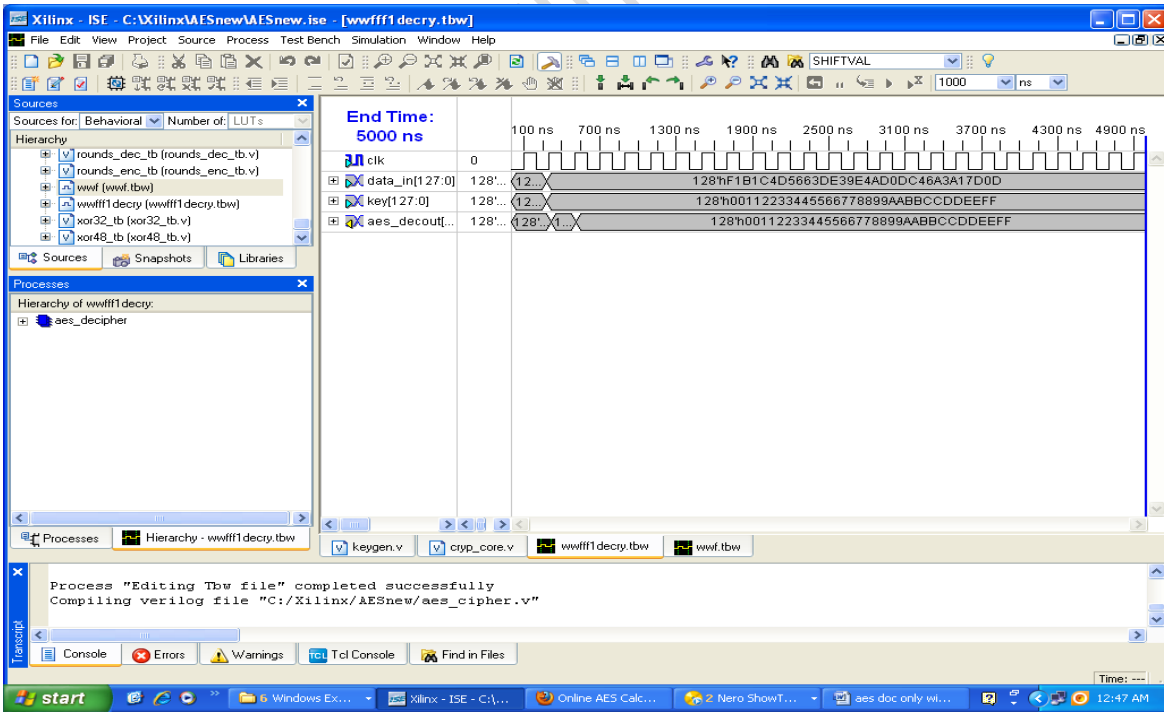
Vol 13, Issue 05, May /2022
ISSN NO: 0377-9254



Journal of Engineering Sciences

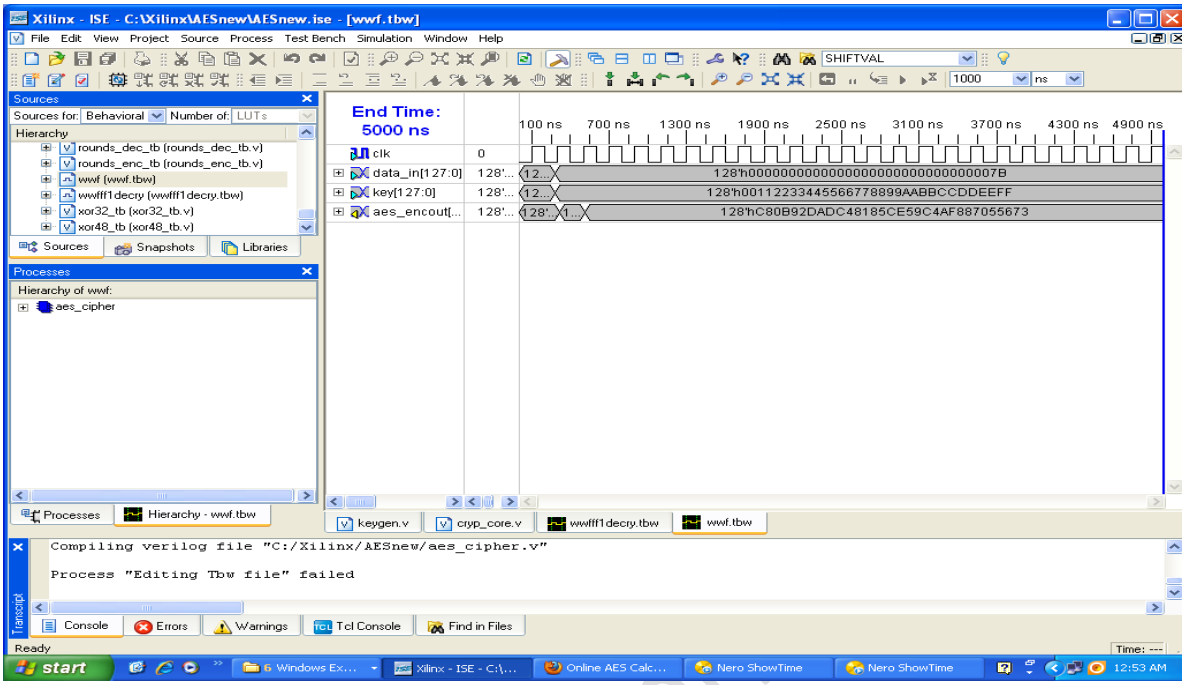
Vol 13, Issue 05, May /2022
ISSN NO: 0377-9254



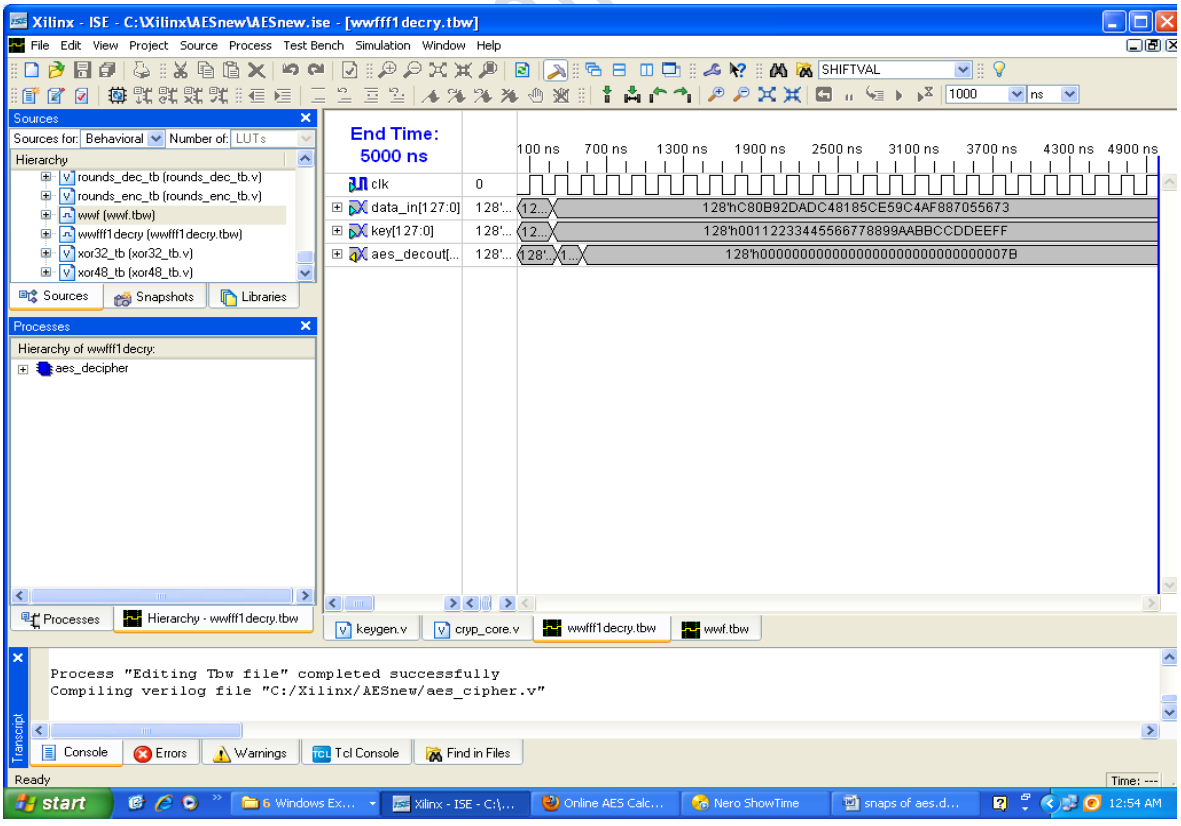


Journal of Engineering Sciences
Vol 13, Issue 05, May /2022
ISSN NO: 0377-9254

AES ENCRYPTION WITH OTHER VALUES



ANOTHER DECRYPTION



5. CONCLUSION

In this project, we have given 128 bits input and 128 bits security key and observed how it is delivered at the output with security. In this project there is no revealingof the original message to the hackers. The original message can be revealed to only senderand the receiver. So, in future, any propriety information can be transmitted securely by using this project (military or banking purposes) Modern applications of AES cover a wide variety of applications, such as secure internet (ssi), electronic financial transactions, remote access servers, cable modems, secure video surveillance and encrypted data storage. The future scope of our project is toextend 128 bits inputs to n bits (n is any integer value).

REFERENCES

1. "Biclique Cryptanalysis of the Full AES" (PDF). Archived from theoriginal (PDF) on March 6, 2016. Retrieved May 1, 2019.
2. ^ Jump up to:[a] [b] Alex Biryukov and Dmitry Khovratovich, Related-key Cryptanalysis of the Full AES-192 and AES-256, "Archived copy". Table
1. Archived from the original on 2009-09-28. Retrieved 2010-02-16.
3. ^ Jump up to:[a] [b] Daemen, Joan; Rijmen, Vincent (March 9, 2003). "AES Proposal: Rijndael" (PDF). National Institute of Standards and Technology.
p. 1. Archived (PDF) from the original on 5 March 2013. Retrieved 21February 2013.
4. ^ Jump up to:[a] [b] [c] "Announcing the ADVANCED ENCRYPTION STANDARD (AES)" (PDF). Federal Information Processing Standards Publication 197. United States National Institute of Standards and Technology (NIST). November26, 2001. Archived (PDF) from the original on March 12, 2017. Retrieved October 2, 2012.
5. ^ Joan Daemen and Vincent Rijmen (September 3, 1999). "AES Proposal:Rijndael" (PDF). Archived from the original (PDF) on February 3, 2007.
6. ^ John Schwartz (October 3, 2000). "U.S. Selects a New Encryption Technique". New York Times. Archived from the original on March 28, 2017.
7. ^ Westlund, Harold B. (2002). "NIST reports measurable success of Advanced Encryption Standard". Journal of Research of the National Institute of Standardsand Technology. Archived from the original on 2007-11-03.
8. ^ "ISO/IEC 18033-3: Information technology – Security techniques – Encryption algorithms – Part 3: Block ciphers". Archived from the original on2013-12-03.
9. ^ Bruce Schneier; John Kelsey; Doug Whiting; David Wagner; Chris Hall; Niels Ferguson; Tadayoshi Kohno; et al. (May 2000). "The Twofish Team's Final Comments on AES Selection" (PDF). Archived (PDF) from the original on2010-01-02.
10. "Efficient software implementation of AES on 32-bit platforms". Lecture Notesin Computer Science: 2523. 2003
11. ^ "byte-oriented-aes – A public domain byte-oriented implementation of AESin C – Google Project Hosting". Archived from the original on 2013-07-20. Retrieved 2012-12-23.
12. ^ Lynn Hathaway (June 2003). "National Policy on the Use of the Advanced Encryption Standard (AES) to Protect National Security Systems and National Security Information" (PDF). Archived (PDF) from the original on 2010-11-06. Retrieved 2011-02-15.
13. ^ Ou, George (April 30, 2006). "Is encryption really crackable?". Ziff-Davis. Archived from the original on August 8, 2010. Retrieved August 7, 2010.

Vol 13, Issue 05, May /2022
ISSN NO: 0377-9254