International Scientific Journal of Engineering and Management (ISJEM) ISSN: 2583-6129
Volume: 04 Issue: 06 | June – 2025 DOI: 10.55041/ISJEM04678
An International Scholarly || Multidisciplinary || Open Access || Indexing in all major Database & Metadata

Design Of Advanced Encryption Standard (AES) Algorithm Using Verilog

1.ATMAKURI KHANDESWARA RAO
PG Studies, Department of Electronics communication and Engineering, JNTUK University College. Paladugu Parvathi Devi College of Engineering & Technology Vijayawada, India
Email:khandeswararao99@gmail.com

2.Mr.PARASHURAMA.N Associative Professor, Department of electronics communication and Engineering, JNTUK University College. Paladugu Parvathi Devi College of Engineering & Technology Vijayawada, India Email:parashu.ppdv@gmail.com

3. Miss. PRASHANTHI M Assistant professor, JNTUK University College. Vikas Group of Institutions VIJAYAWADA, India
Email:shanti.maddala09@gmail.com

Abstract—Moved Encryption Standard (AES), a Federal Information Processing Standard (FIPS), is an embraced cryptographic count that is used to make sure about electronic data. Right now data, need for protection of information is more articulated than any time in recent memory. Secure correspondence is important to protect sensitive data in military and government organizations just as private people. Current encryption gauges are utilized to encode and ensure information during transmission as well as capacity too.

This paper offers a technique for combining encrypted and decrypted AES data. This approach may reduce the complexity of the design, particularly in terms of hardware resources required to implement the AES Sub Bytes and Mix columns modules, among other things. AES encryption and decryption are supported by the majority of modules. Moreover, in both encryption and decryption processes, the architecture can still provide a high data rate

KEYWORDS: ENCRYPTION, CRYPTOGRAPHY, MODELSIM, AES, FPGA,VERILOG

I.INTRODUCTION

There are different focuses to security and different plans, connecting from safe trade and parts to private correspondences and ensuring passwords. One basic perspective for safe trades is that of cryptography, which the fundamental point of convergence of this subject is. All the while it is fundamental to see that when cryptography is key for safe exchanges, it isn't self sufficient from some other individual satisfactory. The bystander is encouraged, by then, that the subjects ensured about right presently delineate the first of different advances critical for noteworthy security in any count of" conditions.

Cryptography deals with the security and integrity of the data. As a new standard for encrypting and decrypting data, AES was developed because the existing algorithms were unreliable for securing large and confidential data. At first, numerous algorithms were developed to encode and decode data. Initially it is mainly used to protect highly confidential data, later many applications in networking began using AES as a standard to protect their data.

Cryptography is a claim to fame of making in puzzle pictures and is an obsolete craftsmanship; the from the start nitty gritty use of cryptography in framing passes before long to around 1900 B.C. precisely when an Egyptian copyist utilized non-standard significant depictions in a carving.

II. MOTIVATION AND PROBLEM STATEMENT

Execution of AES-IP Core for 128 piece by using a memory less combinational structure for the time of S-box and in reverse S-box. As a decision to achieve higher speeds by clearing out memory find a workable pace decreasing all things considered locale included and power ate up by the AES focus.

The two basic hardware structure ways of thinking right now available are Language-Based (High Level) plan and Schematic Based (Low-Level) plan. Language-Based arrangement relies on mix mechanical assemblies to execute the perfect" gear. While amalgamation gadgets continue improving, they inconsistently achieve the most streamlined execution in regards to both locale and speed when stood out from a schematic use. In this way, organized plans will by and large be (insignificantly) greater and more delayed than their schematic based accomplices. Additionally, execution results can extraordinarily vacillate dependent upon the mix contraption similarly as the arrangement being organized.

III. OBJECTIVE

The objective of this venture work is to create encryption standard that advance encryption standard to make sure about correspondence channel. The AES utilizing verilog it gives 128 bits include and create 128 bits of Figure key that is 128 bits scrambled information utilizing Rijndael Algorithm. The encoded information will provide for contribution of the decoding procedure its spread the turn around activity of the encryption procedure its gives the first hex arrangement given information.

IV. LITERATURE REVIEW

A pre-cursor for any task is survey of important writing, since it helps in advancing novel ideas for venture execution. It is very basic to perform writing overview with the goal that the venture work is completed in an efficient staged manner. The overview for this specific task work was focused on the writing distributed up until this point and earlier research done in the related field. The overview in the related writing was completed from sources like papers distributed, sites, and winning" records.

V. MODELSIM

ModelSim is a multi-language HDL reproduction condition by Mentor Graphics, for reenactment of equipment depiction dialects, for example, VHDL, Verilog and SystemC, and incorporates an inherent C debugger. ModelSim can be utilized autonomously, or related to Intel Quartus Prime.

ModelSim is a simulation and verification application used for designing and testing hardware described in hardware description languages (HDLs) like VHDL and Verilog. It is a proprietary simulator developed by Mentor Graphics, now part of Siemens EDA, and offers various editions tailored to different needs and platforms

ModelSim is an application that integrates with Xilinx ISE to provide simulation and testing tools. Two kinds of simulation are used for testing a design: functional simulation and timing simulation. Functional simulation is used to make sure that the logic of a design is correct.

ModelSim is a verification and simulation tool for VHDL, Verilog, SystemVerilog. The following diagram shows the basic steps for simulating a design in ModelSim. In ModelSim, all designs are compiled into a library.

VI . Advanced Encryption Standard (AES)

Advanced Encryption Standard (AES) is a highly trusted encryption algorithm used to secure data by converting it into an unreadable format without the proper key. It is developed by the National Institute of Standards and Technology (NIST) in 2001. It is is widely used today as it is much stronger than DES and triple DES despite being harder to implement. AES encryption uses various key lengths (128, 192, or 256 bits) to provide strong protection against unauthorized access. This data security measure is efficient and widely implemented in securing internet communication, protecting sensitive data, and encrypting files. AES, a cornerstone of modern cryptography, is recognized globally for its ability to keep information safe from cyber threats.

- AES is a Block Cipher.
- The key size can be 128/192/256 bits.
- Encrypts data in blocks of 128 bits each.

That means it takes 128 bits as input and outputs 128 bits of encrypted cipher text. AES relies on the substitution-permutation network principle, which is performed using a series of linked operations that involve replacing and shuffling the input data.

VII. PROPOSED METHOD

The yield of the AES system watches out for the right half Rn. The AES rehearses merge the byte substitution, move push, mix pieces and solidify round key undertakings. The left half of the round Ln is basically the past right half Rn-1. The starting late referenced conditions are iterated over the 10 changes in consistence with the keys produced using the key timetable" process.

The key timetable for the proposed count has been clearly balanced from AES. This has been done as needs be as to decrease the computational flightiness which would have despite occurred if various game-plans of keys were used for the total of the individual models. Another contributing area was likewise that the Figure key of DES has troubles of making weak, semi delicate and supplement keys". The Figure structure of DES is equivalently flawed as the ‟ work with its s-boxes and p-boxes have unavoidable deficiencies. The concealed and last change as conferred in the standard moreover has no security benefits. Right now, have been discarded in our" model.

International Scientific Journal of Engineering and Management (ISJEM) ISSN: 2583-6129
Volume: 04 Issue: 06 | June – 2025 DOI: 10.55041/ISJEM04678
An International Scholarly || Multidisciplinary || Open Access || Indexing in all major Database & Metadata

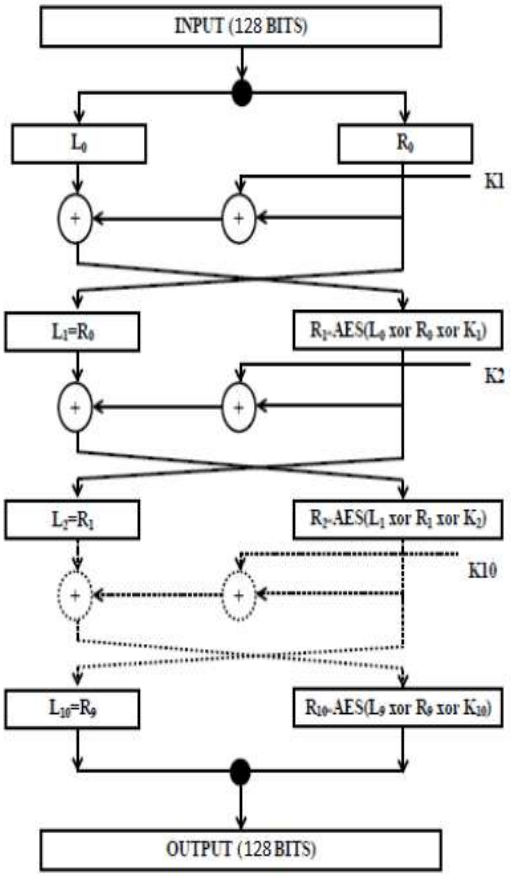


Figure-1: AES Algorithm block diagram

Key age Figure ring is same as AES tally. Regardless, during this see of unequivocal key is synchronized with express round of cross breed encryption and unscrambling. As of now encryption and disentangling utilize same key yet the synchronization grow enough of key with check is exceptional `` "

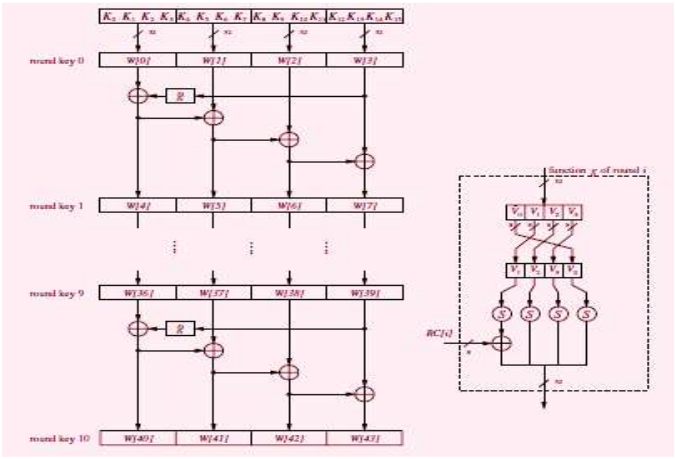


Figure-2: Synchronized Key Generation Algorithm

AES Figure is handling data squares having the length of 128 bits with a symmetric key, which may have a length of 128, 196 or 256 bits. Exercises are performed on a game plan of size 4 x 4 bytes called the state. The estimation consolidates dynamic advances. Notwithstanding, the educational file aside in the state group are merged mod 2 with the master key by the improvement Add Round Key.

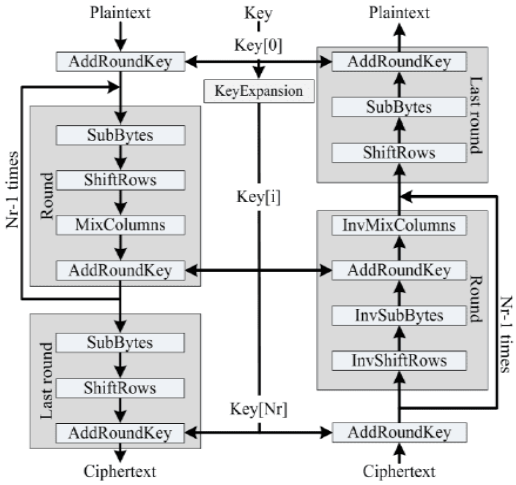


Figure-4: Block diagram

While the unscrambling structure are adequately executing a proportional technique as what encryption is doing neighboring it is playing out something disregarding the encryption framework which are Inverse Sub bytes, Inverse Shift row, Inverse mix column and Inverse Add Round key. This paper will depicts both encryption and disentangling process the square format of proposed structure is showed up in Figure 4.

VIII.RESULT&ANALYSIS

11010111001010101001101111011110001000100010010011
11110101111110111101110100010011100110111111111001
01101100111110001111100110 11

128'h 1f4 enc input
128'h d72a9bde2224fd7ef744e6ff96cf8f9b.... enc output

128'h d72a9bde2224fd7ef744e6ff96cf8f9b...dec input

"128'h 1f4 dec output

rst,sel= 1st 10,2nd 00, 3rd 11;

International Scientific Journal of Engineering and Management (ISJEM) ISSN: 2583-6129
Volume: 04 Issue: 06 | June – 2025 DOI: 10.55041/ISJEM04678
An International Scholarly || Multidisciplinary || Open Access || Indexing in all major Database & Metadata

.

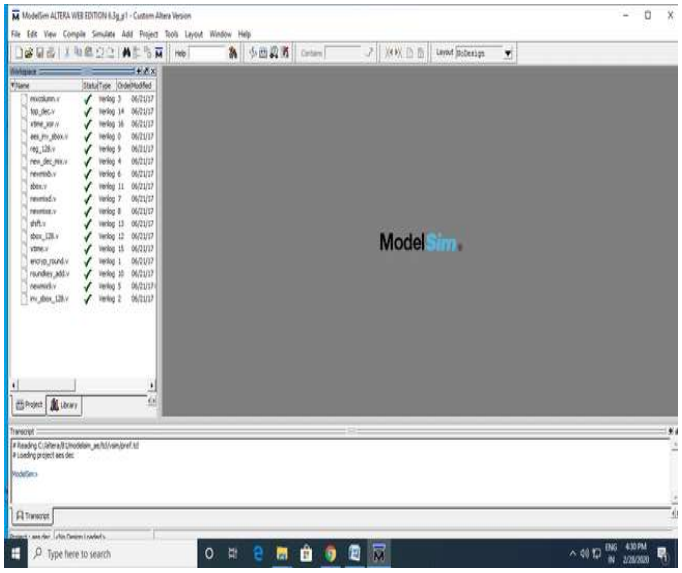


Figure-5:compile code

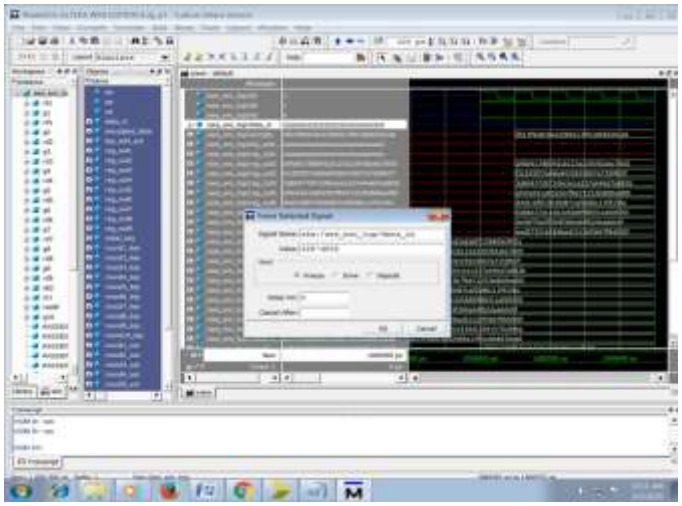


Figure-6:AES Encryption Input:128'd500

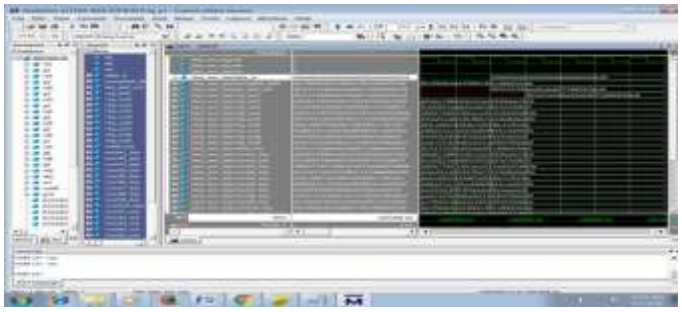


Figure-7:AES Encryption Input:128'd500 converted to hexadecimal equal to 000000000000000000000000000001F4

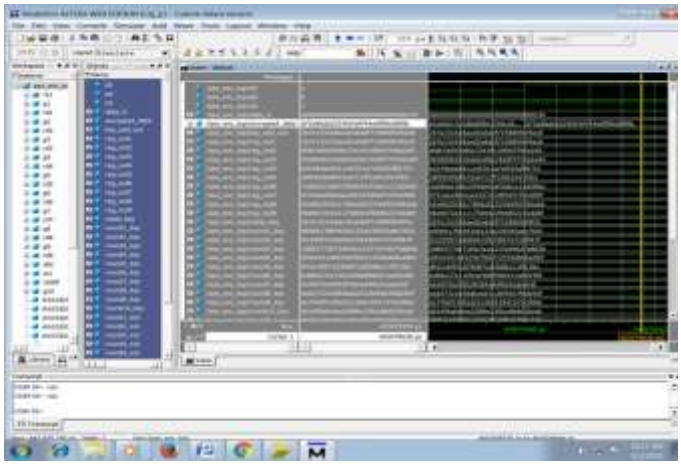
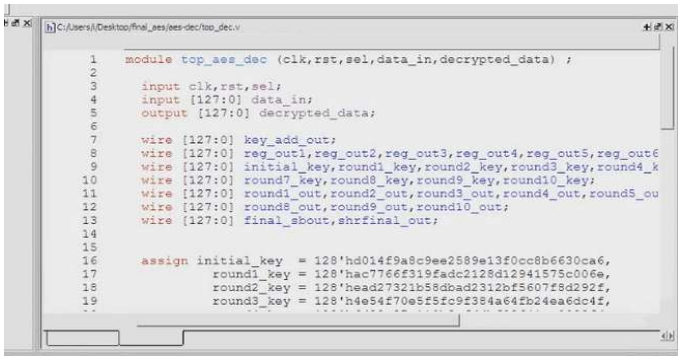


Figure-8:AES Encryption output: d72a9bde2224fd7ef744e6ff96cf8f9b

Figure-9:AES Decryption Input :128'h d72a9bde2224fd7ef744e6ff96cf8f9b The output is : 000000000000000000000000000001F4



```
1   module top_aes_dec (clk,rst,sel,data_in,decrypted_data) ;
2
3     input clk,rst,sel;
4     input [127:0] data_in;
5     output [127:0] decrypted_data;
6
7     wire [127:0] key_add_out;
8     wire [127:0] reg_out1,reg_out2,reg_out3,reg_out4,reg_out5,reg_out6
9     wire [127:0] initial_key,round1_key,round2_key,round3_key,round4_k
10    wire [127:0] round7_key,round8_key,round9_key,round10_key;
11    wire [127:0] round1_out,round2_out,round3_out,round4_out,round5_ou
12    wire [127:0] round8_out,round9_out,round10_out;
13    wire [127:0] final_sbout,shrfinal_out;
14
15
16    assign initial_key  = 128'hd014f9a8c9ee2589e13f0cc8b6630ca6,
17           round1_key = 128'hac7766f319fadc2128d12941575c006e,
18           round2_key = 128'head27321b58dbad2312bf5607f8d292f,
19           round3_key = 128'h4e54f70e5f5fc9f384a64fb24ea6dc4f,
```

Figure-10: AES DECERPATION CODE

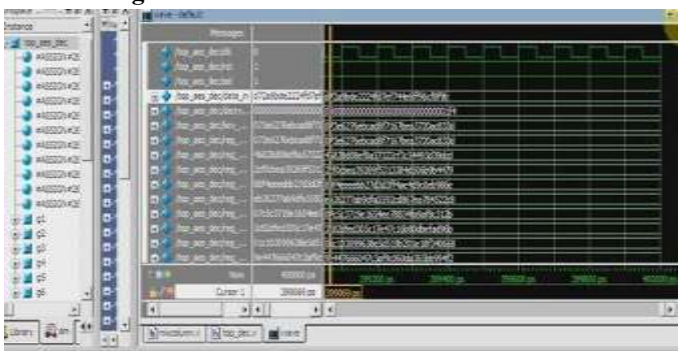


Figure-11:AECS_DEC

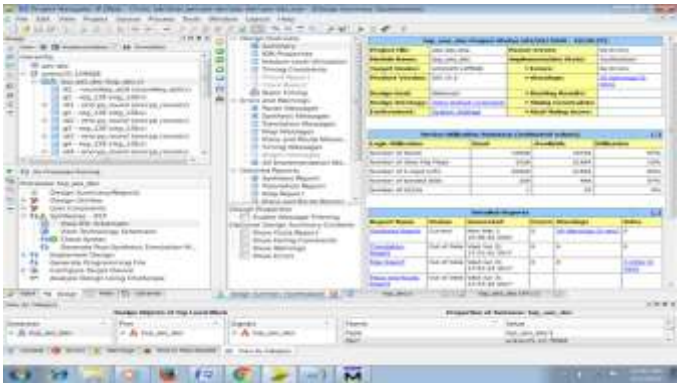


Figure-12:AES Decryption Design summary(draw table for design summary)

The Final structure synopsis of the venture is as appeared in the above Figure This design summary is finished keeping in the view that we are utilizing FPGA. Though IOBs check is very high it tends to be overseen by diminishing the information and yield parameters like accepting information and key as an information each in turn and envisioning the Figure message and translate content one at a period, this can diminish the IOBs to very low. Rest of the rationale hinders use's are very low, in this manner we can actualize our venture in the above expressed FPGA board.

IX.CONCLUSION

We have presented the potential of an improved AES-DES solution as a system that supports the current AES architecture. With these estimates, remote exchanges, electronic payment exchanges, credit cards, video It creates a generally more secure and attack-resistant encryption method that can be used in various areas such as disk systems. This article describes the use of 128 AES devices in equipment. The numbers were connected using Xilinx and Modalism, and the results were "verified using standard test vectors. Estimation is performed by Verilog. Implementing AES integration on equipment actually improves throughput efficiency, regardless of whether zone integrity and speed switching are compromised in each case due to equipment usage. The improved AES-DES considers strategies to enhance current AES plans. This model provides better nonlinearity than simple AES and converges with DES, resulting in better resolution and "less likely" logarithmic traps in the model.

X.FUTURE SCOPE

This proposed computation can be made many times more surprisingly secure by extending the number of accents in the cryptographic computation to adapt it to the required security level. You can also "apply" a retrograde process that reduces the number of accents to reduce security.

Moved Encryption Standard (AES) is the most secure symmetric encryption method with expanded overall authentication. AES is a profitable Methods such as Sub Bytes (S-Box) ensure higher security and faster encryption/decryption. Subbyte and key schedule. Extensive research has been done on S-Box/Inv movement. S-Box and Mix Columns/Inv. Mix columns in submitted ASICs and FPGAs to animate AES calculations and reduce circuit area. reduced.

REFFERNCES

1. Behrouz A. Forouzan, Cryptography and Network security, TMH
2. M.B Vishnu, S.K. Tiong, Zaini M, Koh S P, "Security Enhancement of Digital Motion Image Transmission usingHybridAES-DES
3. algorithm," 14th Asia-Pacific Conference onCommunications, APCC 2008, pp 1-5,2008
4. Maire McLoone, John V. McCanny,"HighPerformance Single Chip FPGA Rijndael Algorithm Implementations," Proceedings of the Third International Workshop on Cryptographic Hardware & Embedded Systems , Springer-Verlag London UK, ISBN:3-54
5. Sanchez-Avila, C.; Sanchez-Reillol R, "The Rijndael block cipher: A comparison with DES," 35th IEEE International Carnahan conference on Security Technology, pp229-234, 2001
6. McLoone, M. McCanny, J.V, "A high performance FPGA implementation of DES ," IEEE Workshop on Signal Processing Systems, SiPS 2000,pp 374-383,2000
7. Standaert, F.-X, Rouvroy G, Quisquater, J.- J," FPGA Implementations of the DES and Triple- DES Masked Against Power Analysis Attacks," International conference on Field Programmable Logic and Applications, FPL '06. pp 1-4, 2006
8. Saeid Taherkhani, Enver EveOrhanGemikonaklir, "Implementation of Non- Pipelined and PipelinedData Encryption Standard (DES) Using Xilinx Virtex -6 FPGA Technology," 10thComputer & Information Technology(CIT 2010), pp 1257-1262, 2010
9. Design of VLSI system by Dr Danial J. Miynek
10. William Stallings, Cryptography and NetworkSecurity: Principles and Practice, 2nd ed., Prentice-Hall, Inc. 2000.
11. http://www.xilinx.com
12. M.Pitchaiah, Philemon Deniel, Praveen 2012 "Implementation of Advanced Encryption Algorithm" International Journal of Scientific & Engineering Research ISSN 2229-5518.
13. Behrouz A. Forouzan, "Cryptography and Network Security" TMH.
14. Gireesh Kumar P,P. Mahesh Kumar 2013 "Implementation of AES Algorithm Using Verilig" International Journal of Embedded systems ISSN 2249-6556.
15. Data Encryption Standard (DES) ,Federal Information Processing Standards Publication (FIPS PUB 46-3)Reaffirmed
16. William Stallings "Cryptography and network Security" Principles and practise Fourth Edition
17. S,Lara , Accelerating algorithms in hardware, date visited:(10/06/2008)http://www.embedded.com/show/Article.jhtml?articleID=175 00157
18. NIST, Advanced Encryption Standard (AES), (FIP PUB 197) http://csrc.nist.gov/publications
19. Wikipedia: www.wikipedia.org.