JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

A COMBINED MESSAGE ENCRYPTION AND DECRYPTION CRYPTOGRAPHIC ALGORITHM BASED ON AES AND RSA ALGORITHMS

[1]K.Parvateesam, [2]K.Bhoomika, [3]P.N.V.S.S.K.Pavan, [4]M.Rohini

[1]Assistant Professor, [2]UG Student, [3]UG Student, [4]UG Student
[1]Department of Electronics and Communication Engineering
[1]Godavari Institute Of Engineering and Technology, Rajahmundry, India

Abstract : In this paper we are presenting an encryption algorithm called Advance Encryption Standard. We have designed AES algorithm using Verilog HDL and in this design we have used look up table substitution for byte in state matrix, also for low complexity and low latency hardware for efficient performance. This design was simulated in Xilinx ISE 14.7, compared results with previous design performances. The algorithm operates by first generating a random AES key, which is then used to encrypt the plaintext message. Subsequently, the AES key is encrypted using the recipient's public RSA key. The ciphertext (encrypted message) and the encrypted AES key are then transmitted. Upon reception, the recipient decrypts the AES key using their private RSA key. Finally, the decrypted AES key is used to decrypt the ciphertext, recovering the original plaintext. This hybrid approach leverages the speed of AES for data encryption and the security of RSA for key distribution.

Index Terms - Digital Communication, AES Algorithm, RSA Algorithm, Encryption, Decryption.

1.INTRODUCTION

VLSI Design presents state-of-the-art papers in VLSI design, computer-aided design, design analysis, design implementation, simulation and testing. Its scope also includes papers that address technical trends, pressing issues, and educational aspects in VLSI Design. By mid-eighties, the transistor count on a single chip had already exceeded 1000 and hence came the age of Very Large Scale Integration or VLSI. Though many improvements have been made and the transistor count is still rising, further names of generations like ULSI are generally avoided. . A lot of problems need to be sorted out before the transition is actually made.

1.1 Why VLSI?

The course will cover basic theory and techniques of digital VLSI design in CMOS technology. Topics include: CMOS devices and circuits, fabrication processes, static and dynamic logic structures, chip layout, simulation and testing, low power techniques, design tools and methodologies, VLSI architecture.

1.2 Structured Design

Structured VLSI design is a modular methodology originated by Carver Mead and Lynn Conway for saving microchip area by minimizing the interconnect fabrics area.

1.3 What Is VLSI?

In olden days, when huge computers made of vacuum tubes could occupy an entire dedicated rooms and could do about 360 multiplications of 10 digit numbers in a second. In olden days, when huge computers made of vacuum tubes could occupy an entire dedicated rooms and could do about 360 multiplications of 10 digit numbers in a second.

1.4 History & Evolution

The second age of Integrated Circuits revolution started with the introduction of the first microprocessor, the 4004 by Intel in 1972 and the 8080 in 1974. Devices, Intel, Philips, Motorola and many other firms have been established and are dedicated to the various fields in "VLSI" like Programmable Logic Devices, Hardware Descriptive Languages, Design tools, Embedded Systems etc.

1.5 Future Of VLSI

Generally, VLSI technology is used in the devices like computers, cell phones, digital cameras and any electronic gadget. There are certain key issues that serve as active areas of research and are constantly improving as the field continues to mature.

1.6 Semiconductors and Doping

By adding trace amounts of certain materials to semiconductors alters the crystal structure and can change their electrical properties in particular it can change the number of free electrons or holes.

2.LITERATURE SURVEY

[2.1] Daemen J., and Rijmen V, "The Design of Rijndael: AES-the Advanced Encryption Standard", Springer-Verlag, (2002). "The Design of Rijndael: AES—the Advanced Encryption Standard," authored by Joan Daemen and Vincent Rijmen and published by Springer-Verlag in 2002, is a seminal text that meticulously documents the creation and selection of the Advanced Encryption Standard (AES).
Summary: This book details the design principles and specifications of Rijndael, the algorithm selected as the Advanced Encryption Standard (AES).

[2.2] FIPS 197, "Advanced Encryption Standard (AES)", November 26, 2001. FIPS 197, "Advanced Encryption Standard (AES)," published on November 26, 2001, by the National Institute of Standards and Technology (NIST), officially established AES as a U.S. federal government standard for symmetric-key encryption.
Summary: FIPS 197 standardizes the Advanced Encryption Standard (AES) algorithm.

[2.3] Tessier, R., and Burleson, W., "Reconfigurable computing for digital signal processing: a survey", J. VLSI Signal Process., 2001, 28, (1-2), pp.7-27. Tessier, R., and Burleson, W.'s "Reconfigurable computing for digital signal processing: a survey," published in the Journal of VLSI Signal Processing in 2001, provides a comprehensive overview of the application of reconfigurable computing in digital signal processing (DSP).
Summary: This paper surveys reconfigurable computing architectures and their applications in digital signal processing.

[2.4] Ahmad, N.; Hasan, R.; Jubadi, W.M; "Design of AES S-Box using combinational logic optimization", IEEE Symposium on Industrial Electronics & Applications (ISIEA), pp. 696-699, 2010. Ahmad, N., Hasan, R., and Jubadi, W.M.'s 2010 paper, presented at the IEEE Symposium on Industrial Electronics & Applications (ISIEA), focuses on the "Design of AES S-Box using combinational logic optimization.
Summary: Ahmad, Hasan, and Jubadi's 2010 paper details optimizing the AES S-Box through combinational logic for enhanced hardware performance.

[2.5] Brinker, Alex Panato, Marcelo Barcelos, Ricardo Reis, "An IP of an Advanced Encryption Standard for Altera Devices", SBCCI 2002, pp. 197-202, Porto Alegre, Brazil, 9 and 14 September 2002. Panato, Barcelos, and Reis's 2002 SBCCI paper details the development of an Intellectual Property (IP) core specifically designed for implementing the Advanced Encryption Standard (AES) on Altera Field-Programmable Gate Arrays (FPGAs).
Summary: Panato, Barcelos, and Reis's 2002 paper details an optimized AES IP core for Altera FPGAs.

[2.6] Mr. Atul M. Borkar, Dr. R. V. Kshirsagar and Mrs. M. V. Vyawahare, "FPGA Implementation of AES Algorithm", International Conference on Electronics Computer Technology (ICECT), pp. 401-405, 2011 3rd Borkar, Kshirsagar, and Vyawahare's 2011 ICECT paper focuses on the hardware implementation of the AES algorithm using Field-Programmable Gate Arrays (FPGAs).
Summary: This paper presents an FPGA implementation of the AES algorithm.

[2.7] Bogdanov Andrey et al., "PRESENT: An ultra-lightweight block cipher", CHES, vol. 4727, 2007. In their 2007 CHES publication, "PRESENT: An ultra-lightweight block cipher," Andrey Bogdanov and his colleagues introduced a highly efficient symmetric key block cipher designed for resource-constrained environments.
Summary: PRESENT is introduced as an ultra-lightweight block cipher design.

[2.8] Feldhofer Martin, Johannes Wolkerstorfer and Vincent Rijmen, "AES implementation on a grain of sand", IEEE Proceedings-Information Security, vol. 152, no. 1, pp. 13-20, 2005. In their 2005 IEEE Proceedings-Information Security paper, "AES implementation on a grain of sand," Martin Feldhofer, Johannes Wolkerstorfer, and Vincent Rijmen explored the feasibility of implementing the Advanced Encryption Standard (AES) on extremely resource-constrained devices.
Summary: This paper explores ultra-low-resource AES implementations, aiming for "grain of sand" level devices.

[2.9] Abdullah Al Hasib, Abul Ahsan and Mahmudul Haque, "A comparative study of the performance and security issues of AES and RSA cryptography", Third International Conference on Convergence and Hybrid Information Technology, vol. 2, 2008. In their 2008 paper, "A comparative study of the performance and security issues of AES and RSA cryptography," Abdullah Al Hasib, Abul Ahsan, and Mahmudul Haque presented an analysis of two widely used cryptographic algorithms. Their work aimed to provide insights into the strengths and weaknesses of AES (Advanced Encryption Standard) and RSA (Rivest-Shamir-Adleman) in terms of both performance and security.
Summary: This paper compares the performance and security of AES and RSA cryptography.

[2.10] Moradi Amir, Axel Poschmann San, Ling Christof Paar and Huaxiong Wang, "Pushing the limits: a very compact and a threshold implementation of AES", Eurocrypt, vol. 6632, pp. 69-88, 2011. In their 2011 Eurocrypt paper, "Pushing the limits: a very compact and a threshold implementation of AES," Amir Moradi, Axel Poschmann, San Ling, Christof Paar, and Huaxiong Wang explored advanced techniques for optimizing the Advanced Encryption Standard (AES) in resource-constrained environments.
Summary: This paper explores highly compact and threshold implementations of AES.

[2.11] Wang Yong, Garhan Attebury and Byrav Ramamurthy, "A survey of security issues in wireless sensor networks", IEEE Communications Surveys Tutorial, 2006. This paper provides a comprehensive overview of security vulnerabilities and challenges specific to wireless sensor networks. It examines various attack types and existing security mechanisms, highlighting the unique constraints and requirements of these networks.
Summary: This survey paper reviews security vulnerabilities, attacks, and defenses in wireless sensor networks.

[2.12] Eisenbarth Thomas and Sandeep Kumar, "A survey of lightweight-cryptography implementations", IEEE Design & Test of Computers, vol. 24, no. 6, 2007. This paper surveys the field of lightweight cryptography, focusing on hardware and software implementation aspects. It examines various lightweight cryptographic algorithms designed for resource-constrained devices. It provides insights into the trade-offs between security, performance, and resource usage in these implementations.
Summary: This survey paper examines hardware and software implementations of lightweight cryptography for resource-constrained devices.

[2.13] Shibutani Kyoji, Takanori Isobe Harunaga, Hiwatari Atsushi, Mitsuda Toru Akishita and Taizo Shirai, "Piccolo: An ultra-lightweight blockci-pher", CHES, vol. 6917, pp. 342-357, 2011. This paper introduces Piccolo, an ultra-lightweight block cipher designed for resource-constrained environments. Piccolo supports two key lengths, 80-bit and 128-bit, and offers sufficient security levels against known attacks. It is suitable for applications such as RFID tags and sensor nodes where resources are extremely limited.
Summary: This paper introduces Piccolo, an ultra-lightweight block cipher designed for resource-constrained devices.

[2.14] Wu Wenling and Lei Zhang, "L Block: a lightweight block cipher" in Applied Cryptography and Network Security, Springer Berlin/Heidelberg, pp. 327-344, 2011. This paper introduces L Block, a lightweight block cipher designed for resource-constrained environments. It focuses on achieving a balance between security and implementation efficiency.
Summary: This paper proposes L Block, a lightweight block cipher optimized for resource-constrained devices.

3.METHODOLOGY

In earlier days Data encryption standard (DES) was considered as encryption standard with symmetrical key encryption with the key size of 56 bits. After certain days 56 bit key was considered to be small and for high data bit systems require key and data size to be large. In the year 1990 the National institute of standards call for papers on new encryption methods. So many researchers sent their papers to NIST, out of all those few were selected for testing. Cryptographic researchers after performing test on them only five are best among them; those are Mars, RC6, Rijndael, Serpent and Two fish. These five went onto further testing after performing these tests they have declared that Rijndael algorithm was the winner. According this AES algorithm data and key size may be any size i.e., multiple of 32 bits, with minimum of 128bits and maximum of 256 bits. This algorithm also called Rijndael algorithm of AES. AES can be implemented either in software or hardware. Software implementation requires less resources and cost and its implication also limited, having low seed.

3.1 The AES cipher

Like DES, AES is a symmetric block cipher. This means that it uses the same key for both encryption and decryption. However, AES is quite different from DES in a number of ways. The algorithm Rijndael allows for a variety of block and key sizes and not just the 64 and 56 bits of DES' block and key size. The block and key can in fact be chosen independently from 128, 160, 192, 224, 256 bits and need not be the same. However, the AES standard states that the algorithm can only accept a block size of 128 bits and a choice of three keys - 128, 192, 256bits.

3.2 Inner Workings Of A Round

The algorithm begins with an Add round key stage followed by 9 rounds of four stages and a tenth round of three stages. This applies for both encryption and decryption with the exception that each stage of a round the decryption algorithm is the inverse of its counterpart in the encryption algorithm.

3.3 Substitute Bytes

This stage (known as Sub Bytes) is simply a table lookup using a 16×16 matrix of byte values called an s-box. This matrix consists of all the possible combinations of an 8 bit sequence (28 = 16 × 16 = 256). However, the s-box is not just a random permutation of these values and there is a well defined method for creating the s-box tables. In this stage (known as Add Round Key) the 128 bits of state are bitwise XORed with the 128 bits of the round key. The operation is viewed as a column wise operation between the 4 bytes of a state column and one word of the round key. This transformation is as simple as possible which helps in efficiency but it also effects every bit of state.

3.4 Shift Row Transformation

The Inverse Shift Rows transformation (known as Inv Shift Rows) performs these circular shifts in the opposite direction for each of the last three rows (the first row was unaltered to begin with). This operation may not appear to do much but if you think about how the bytes are murdered within state then it can be seen to have far more of an impact. Remember that state is treated as an array of four byte columns, i.e. the first column actually represents bytes 1, 2, 3 and 4. A one byte shift is therefore a linear distance of four bytes.

3.5 Mix Column Transformation

This stage (known as Mix Column) is basically a substitution but it makes use of arithmetic of GF (28). Each column is operated on individually. Each byte of a column is mapped into a new value that is a function of all four bytes in the column. The transformation can be determined by the following matrix multiplication on state.
Each element of the product matrix is the sum of products of elements of one row and one column. In this case the individual additions and multiplications are performed in GF (28).

3.6 Add Round Key Transformation

In this stage (known as Add Round Key) the 128 bits of state are bitwise XORed with the 128 bits of the round key. The operation is viewed as a column wise operation between the 4 bytes of a state column and one word of the round key. This transformation is as simple as possible which helps in efficiency but it also effects every bit of state.

4.SOFTWARE IMPLEMENTATION

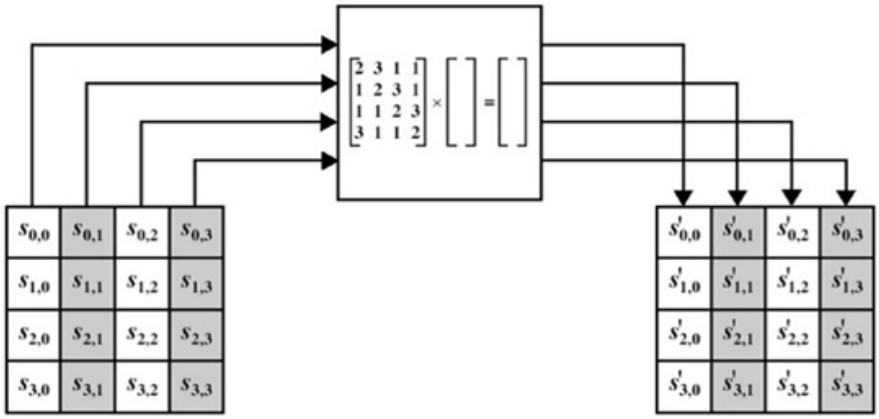
The AES key expansion algorithm takes as input a 4-word key and produces a linear array of 44 words. Each round uses 4 of these words. Each word contains 32 bytes which means each sub key is 128 bits long. Figure 7.7 show pseudo code for generating the expanded key from the actual key. The key is copied 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. Figure 7.8 illustrates the generation of the first eight words of the expanded key using the symbol g to represent that complex function. The round constant is a word in which the three rightmost bytes are always 0. 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 of a round-dependent round constant eliminates the symmetry, or similarity, between the way in which round keys are generated in different rounds.

4.1 Equivalent Inverse Cipher

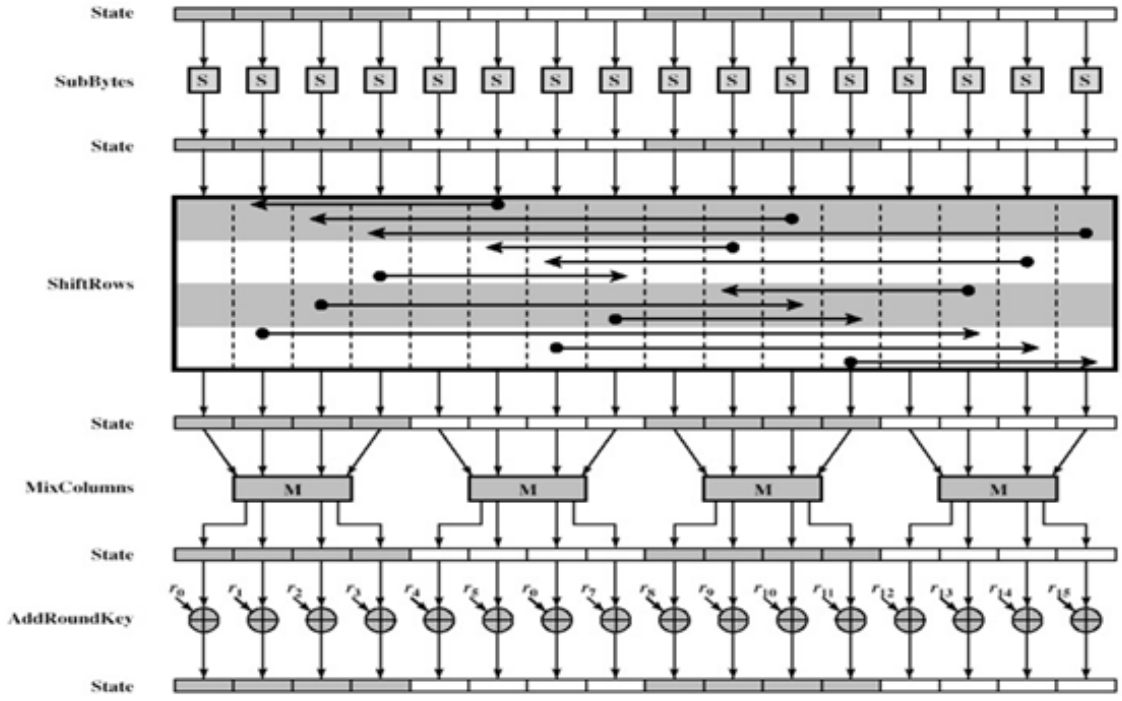
As can be seen from the decryption ciphers are not identical to the encryption ciphers. How ever the form of the key schedules is the same for both. This has the disadvantage that two separate software or firmware modules are needed for applications that requires both encryption and decryption. As well as that decryption is slightly less efficient to implement. However, encryption was deemed more important than decryption for two reasons. They are for the CFB and OFB cipher mode (which we have seen before but will study in more detail next) only encryption is used and as with any block cipher, AES can be used to construct a message authentication code (to be described later), and for this only encryption is used. However, if desired it is possible to create an equivalent inverse cipher. This means that decryption has the same structure as the encryption algorithms. However, to achieve this, a change of key schedule is needed. We will not be concerned with this alternate form but you should be aware that is exists.

We have seen previously that five modes of operation are used when applying block ciphers in a variety of applications. This section will give a more detailed view of how these modes operate. This first mode is the simplest of all five modes. Figure 7.10 shows the scheme where it can be seen that a block of plaintext (which is the same size in each case) is encrypted with the same key K. The term codebook is used because, for a given key, there is a unique cipher text for every block of plaintext.

MIX COLUMNS TRANSFORMATION OF A SINGLE COLUMN



GENERATING ROUND KEYS IN DIFFERENT ROUNDS



5.RESULT

The combination of AES for efficient bulk encryption and RSA for secure key exchange, enhancing overall security. It leverages the strengths of both algorithms to achieve robust message protection.

XILINX:

Xilinx, Inc. is the world's largest supplier of programmable logic devices, the inventor of the field programmable gate array and the first semiconductor company with a fabless manufacturing model. Xilinx's FPGAs have even been used for the ALICE at the CERN European laboratory on the French-Swiss border to map.

XILINXISE 14.7

Xilinx is the most important tool and in this tool we can perform both simulation and synthesis. In this process we are going to verify our required output to get the simulation process firstly we have to implement a top module and then in the simulation behavior we can simulate the results.

Procedure:

- Click project navigator
- Create new project
- Selection of FPGA

Xilinx snapshots

To create new project in xilinx we should open the file menu, click on new project then it will open the dialog box as below in that type the filename click on next

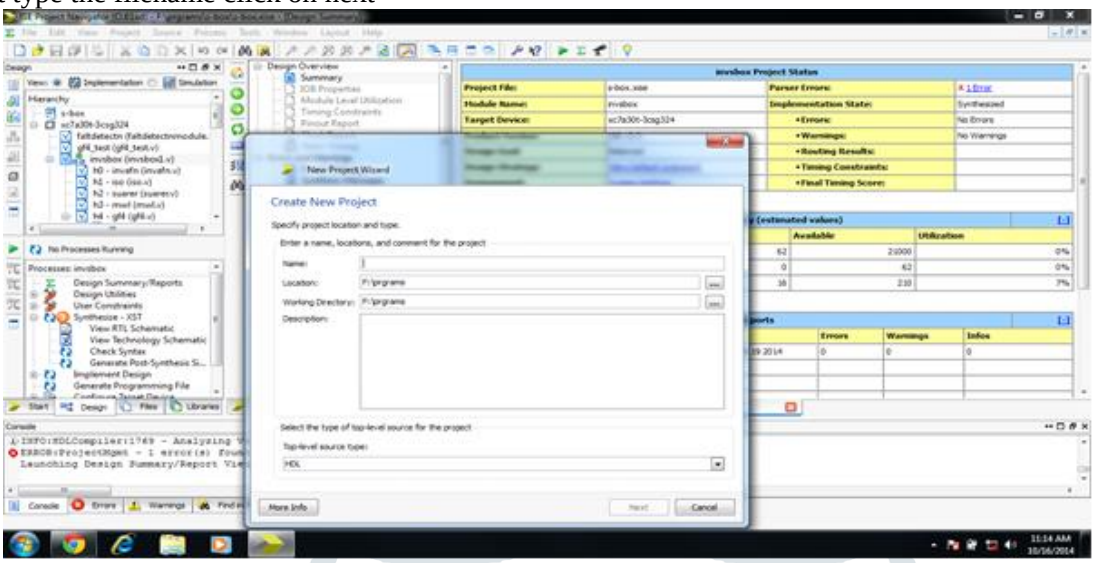


FIG 5.1: File menu

From the given options select new source then it display dialog box which is containing of list of file format now we want to create verlog file so select veilog module, and give the name to the file. Then click on next

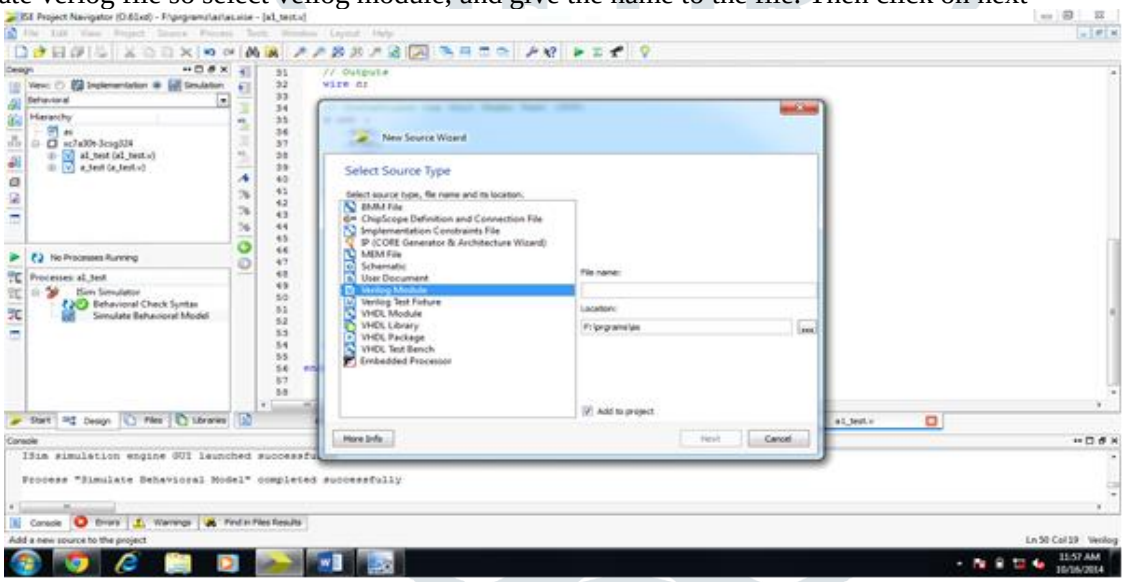


FIG 5.2: Dialog Box

After successful synthesis we should have to create test bench file with extension as test, for that again right click on the file name as shown below, give filename

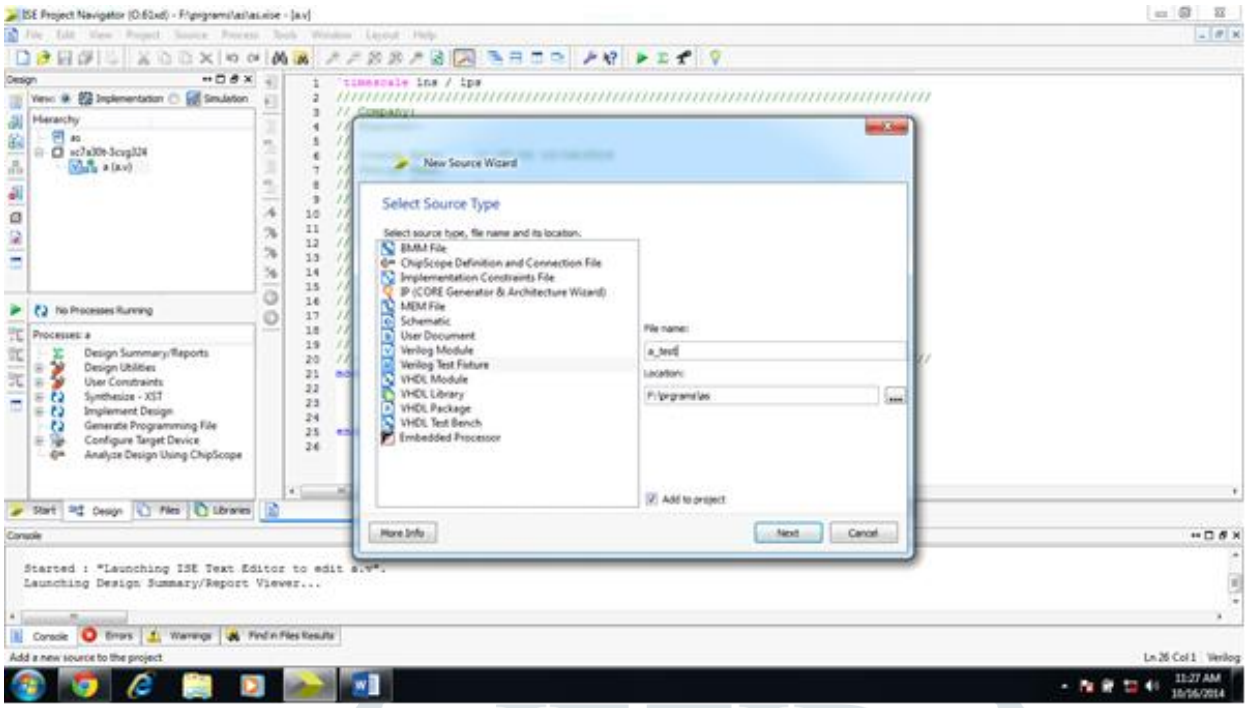


FIG 5.3: Test bench file

That wave form window having option to zoom out, zoom in to analyze the wave form clearly in order to understand behavior of design

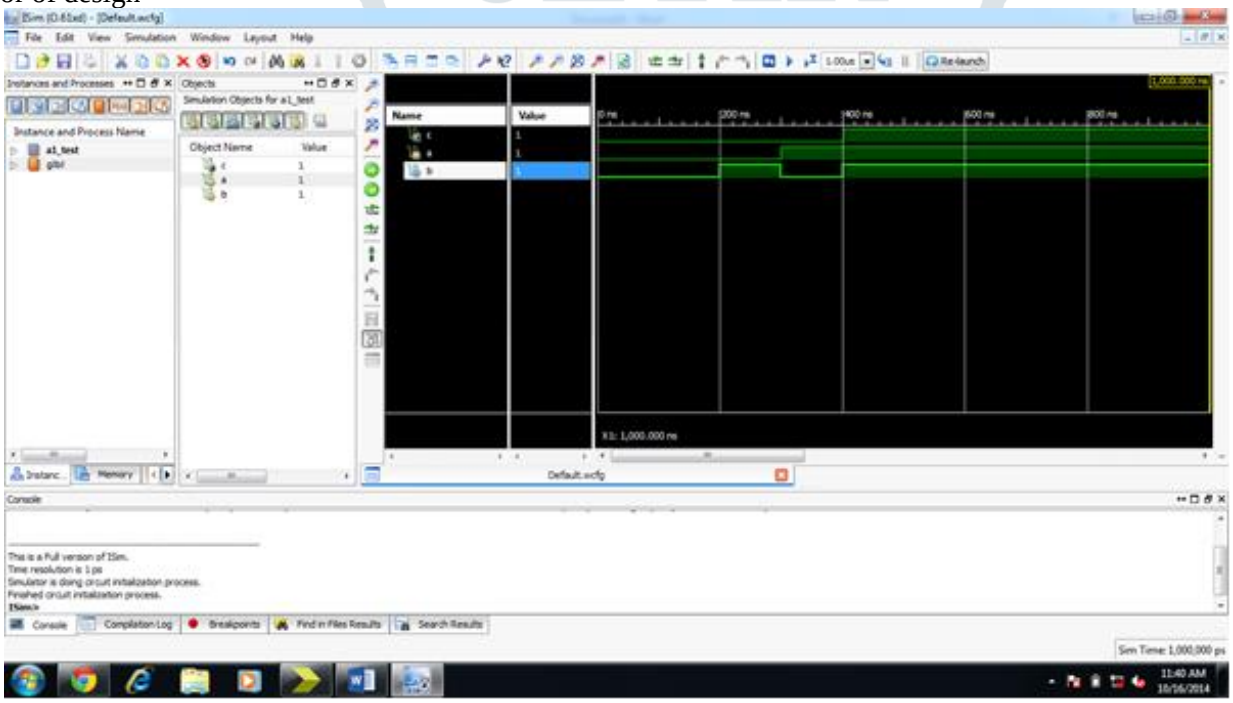


FIG 5.4: Behavior of design

CONCLUSION

A hybrid cryptographic approach, merging AES and RSA, offers a robust solution for secure communication. This combination leverages AES's efficiency for bulk data encryption and RSA's strength in secure key exchange. The result is a system that balances speed and security, addressing the limitations of each individual algorithm. AES provides rapid encryption/decryption, crucial for large data volumes. RSA ensures secure key distribution, mitigating vulnerabilities inherent in symmetric key management. This hybrid model enhances overall security by compartmentalizing critical functions. It is particularly suitable for applications requiring both high-speed processing and stringent security measures. The complexity introduced by this combination strengthens resistance against various cryptographic attacks. Thus, the AES-RSA hybrid represents a pragmatic and effective cryptographic strategy. This approach provides a layered security model, making it more resilient to breaches. Furthermore, it is adaptable to various security requirements, offering flexibility in implementation.

FUTURE SCOPE

Future research can explore optimized hardware implementations for this hybrid algorithm, focusing on reduced latency and power consumption. Investigating quantum-resistant variants of both AES and RSA is crucial for long-term security. Adaptive key management schemes, dynamically adjusting key sizes based on security needs, can enhance robustness. Exploring homomorphic encryption techniques within this hybrid framework could enable secure

computation on encrypted data. Integration with emerging technologies like blockchain for secure key distribution and data integrity is a promising avenue. Developing lightweight versions of this hybrid for IoT devices with constrained resources is essential. Further analysis of the algorithm's resistance against advanced side-channel attacks and fault injection techniques is needed. Research into efficient methods for securely storing and managing keys in distributed systems is vital.

REFERENCES

[1] Daemen J., and Rijmen V, "The Design of Rijndael: AES-the Advanced Encryption Standard", Springer-Verlag, 2002.
[2] FIPS 197, “Advanced Encryption Standard (AES)”, November 26, 2001.
[3] Tessier, R., and Burleson, W., “Reconfigurable computing for digital signal processing: a survey”, J. VLSI Signal Process., 2001, 28, (1-2), pp.7-27.
[4] Ahmad, N.; Hasan, R.; Jubadi, W.M; “Design of AES S-Box using combinational logic optimization”, IEEE Symposium on Industrial Electronics & Applications (ISIEA), pp. 696-699, 2010.
[5] Brinker, Alex Panato, Marcelo Barcelos, Ricardo Reis, “An IP of an Advanced Encryption Standard for Altera Devices”, SBCCI 2002, pp. 197-202, Porto Alegre, Brazil, 9 and 14 September 2002.
[6] Mr. Atul M. Borkar, Dr. R. V. Kshirsagar and Mrs. M. V. Vyawahare, “FPGA Implementation of AES Algorithm”, International Conference on Electronics Computer Technology (ICECT), pp. 401-405, 2011 3rd
[7] Bogdanov Andrey et al., "PRESENT: An ultra-lightweight block cipher", CHES, vol. 4727, 2007.
[8] Feldhofer Martin, Johannes Wolkerstorfer and Vincent Rijmen, "AES implementation on a grain of sand", IEEE Proceedings-Information Security, vol. 152, no. 1, pp. 13-20, 2005.
[9] Abdullah Al Hasib, Abul Ahsan and Mahmudul Haque, "A comparative study of the performance and security issues of AES and RSA cryptography", Third International Conference on Convergence and Hybrid Information Technology, vol. 2, 2008.
[10] Moradi Amir, Axel Poschmann San, Ling Christof Paar and Huaxiong Wang, "Pushing the limits: a very compact and a threshold implementation of AES", Eurocrypt, vol. 6632, pp. 69-88, 2011.
[11] Wang Yong, Garhan Attebury and Byrav Ramamurthy, "A survey of security issues in wireless sensor networks", IEEE Communications Surveys Tutorial, 2006.
[12] Eisenbarth Thomas and Sandeep Kumar, "A survey of lightweight-cryptography implementations", IEEE Design & Test of Computers, vol. 24, no. 6, 2007.
[13] Shibutani Kyoji, Takanori Isobe Harunaga, Hiwatari Atsushi, Mitsuda Toru Akishita and Taizo Shirai, "Piccolo: An ultra-lightweight blockci-pher", CHES, vol. 6917, pp. 342-357, 2011.
[14] Wu Wenling and Lei Zhang, "L Block: a lightweight block cipher" in Applied Cryptography and Network Security, Springer Berlin/Heidelberg, pp. 327-344, 2011.