Design of Hybrid Encryption Algorithm using AES and RSA for key exchange

Reshma Nadaf[1], Satish Bhairannawar[2]

[1,2]Dept. of ECE, SDM College of Engineering and Technology, Dharwad.
[1]reshma.nadaf27@gmail.com, [2]satishbhairannawar@gmail.com

Abstract: ***Nowadays, security of any confidential data which is being transmitted over a communication channel has become a primary concern. Encryption and decryption techniques are used to achieve confidentiality of sensitive information which is transmitted over channel. Symmetric cryptography faces a key exchange problem between transmitter and receiver. This research paper introduces a novel approach to address the key exchange issue which is encountered in symmetric encryption. In this paper, Advanced Encryption Standard (AES) from symmetric cryptography and Rivest Shaamir Adleman (RSA) algorithms from asymmetric cryptography are analyzed and a new key exchange protocol is developed by combining above said two algorithms to obtain Hybrid cryptography. This protocol achieves 3 major cryptographic primitives: integrity, authentication and confidentiality. The proposed hybrid encryption algorithm is simulated on Xilinx ISE 14.7. The proposed technique gives better security as it overcomes the problem of key exchange.***

Keywords: **AES, RSA, Hybrid cryptography, FPGA;**

1. INTRODUCTION

Internet has become a vital communication medium in the present digital era. Transmitting sensitive information from sender to receiver digitally faces a lot of threats from an adversary. Secure transmission of sensitive data over internet has become a primary concern. We employ encryption and decryption techniques to achieve this cryptographic primitive called confidentiality. Cryptography is an art and science of transforming sensitive data which is referred as plaintext into a scrambled message called as ciphertext. Encryption is a technique of converting plaintext into ciphertext and decryption is a technique of retrieving back plaintext from ciphertext. Encryption uses substitution and permutation as the main processes for jumbling the given plaintext. These encryption algorithms use key as major ingredient for converting plaintext to ciphertext. Cryptography concerns with the following four objectives: (i) Confidentiality: - The information is read and understood only to whom it is concerned. (ii) Integrity: - The assurance that the data received is exactly sent by an entity. It contains no deletion and no modification and can be easily detectable if it contains any insertion or deletion. iii) Non-repudiation:- It provides protection against denial of one of the entities either sender or receiver after taking part in communication. There are non-repudiation at source side and non-repudiation at receiver side. (iv) Authentication: - The assurance that the communicating entity either sender or receiver is the one that it claims t be. There are peer entity authentication and data origin authentication.

There are several ways of classifying cryptographic algorithms. They are categorized based on,

- the number of keys that are used in encryption and decryption
- the way in which they are processed
- the type of operations performed for converting plaintext into ciphertext

Depending on the number of keys they are classified as

1.1 Secret Key Cryptography (SKC): This technique uses a single or only one key for both encryption and decryption, it is called symmetric encryption or conventional encryption. It is used for privacy and confidentiality which is primary objective. The sender uses the key to encrypt or encipher the information which is in readable format known as plaintext and sends the jumbled and unintelligent information known as ciphertext to the receiver. The receiver now applies the same key to decrypt or decipher the information or message and recover the plaintext. Because a single key is used for both operations, secret key cryptography is also called symmetric encryption.

With this form of cryptography, it is understood that the key must be given to both the sender and the receiver prior to actual communication take place till this key is kept secret. The major challenge is this type of cryptographic technique is, the distribution of the key. Secret key cryptography schemes are usually either stream ciphers or block ciphers.

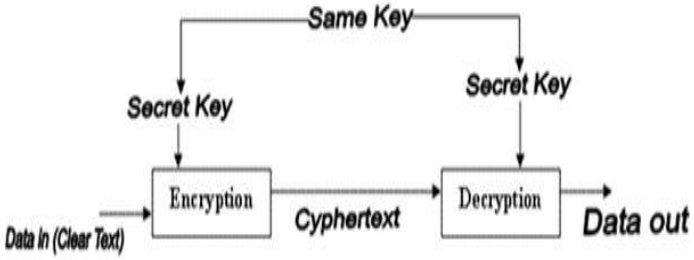

Fig 1: Symmetric Encryption

Symmetric algorithms are faster. It achieves confidentiality and authentication since only entity which possesses the secret key can decrypt a message. But key exchange is main problem in symmetric cryptosystems. The secret key is to be transmitted to the receiving system before the actual message is to be transmitted. Every means of electronic communication is insecure as it is impossible to guarantee that no one will be able to tap communication channels. So the only secure way of exchanging keys would be exchanging them personally.

1.2 Public Key Cryptography (PKC): Uses one key for encryption and related key for decryption; also called asymmetric encryption. Primarily used for authentication, non-repudiation, and key exchange. Public key cryptography (PKC) has been said to be the most significant new development in cryptography in the last 300-400 years [1]. Modern PKC was first described publicly by Stanford University professor Martin Hellman and graduate student Whitfield Diffie in 1976. Their paper described a two-key crypto system in which two parties could engage in a secure communication over a non-secure communications channel without having to share a secret key.

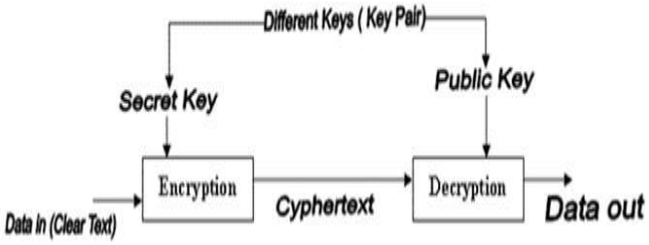

Fig 2: Asymmetric Encryption

In PKC, one of the keys is designated as the public key and may be advertised as widely as the owner wants. The other key is designated as the private key and is never revealed to another party. It is straight forward to send messages under this scheme. Suppose, Alice wants to send Bob a message. Alice encrypts some information using Bob's public key; Bob decrypts the ciphertext using his private key. This method could be also used to prove who sent a message; Alice, for example, could encrypt some plaintext with her private key; when Bob decrypts using Alice's public key, he knows that Alice sent the message (authentication) and Alice cannot deny having sent the message (non-repudiation). Public key cryptographic algorithms that are in use today for key exchange or digital signatures include: RSA, Diffie Hellman and Elliptic Curve Cryptography (ECC). In asymmetric or public key, cryptography there is no need for exchanging keys, thus eliminating the key distribution problem. The primary advantage of public-key cryptography is increased security: the private keys do not ever need to be transmitted or revealed to anyone. A disadvantage of using public-key cryptography for encryption is speed:
In cryptography, a hybrid cryptosystem is one which combines the convenience of a public-key cryptosystem with the efficiency of a symmetric-key cryptosystem. Public-key cryptosystems are convenient in that they do not require the sender and receiver to share a common secret in order to communicate securely (among other useful properties). However, they often rely on complicated mathematical computations and are thus generally much more inefficient than comparable symmetric-key cryptosystems. In many applications, the high cost of encrypting long messages in a public-key cryptosystem can be prohibitive. This is addressed by hybrid systems by using a combination of both. The hybrid cryptosystem is itself a public-key system, whose public and private keys are the same as in the key encapsulation scheme.

2. Related Work

In paper [1], Marwan Ali Albahar et.al, a communication model which produces increased reliability because key aspects in terms of data security are covered: Unidirectional encryption and decryption where the sender encrypts but only receiver of the can decrypt, Authenticity verification for both cover image and secret data where many intentional checkpoints have been intentionally added so that the smallest change in the steganographic packet breaks the seal, signalizing an unauthorized manipulation.

In paper [2], Septimiu Fabian Mare et. al, a hybrid cryptosystem is developed that assembles two cryptographic algorithms namely AES and SHA-2 algorithms. Since the architecture is very complex, high security of data is achieved. The design is synthesized using Xilinx ISE and implemented on Virtex-5 FPGA that consists of 110 million gates. The proposed design operates at a maximum frequency of 139.252 MHz with a delay of 7.181ns .

In paper [3], Vanishree prasad et.al a new hybrid security algorithm has been designed for increased security and developed. The proposed hybrid security algorithm is immune against the square attacks because of the addition of Advance Encryption Standard algorithm. The square attack on AES can be extended to 7 rounds by guessing the 16 bytes of the last round key. The proposed algorithm may solve problems with respect to practical implementation, provides less response time, efficient computation and the strength of cryptosystem.

In paper [4], author proposes a cryptographic technique which comprises of Symmetric and Asymmetric algorithms to secure the communication within an IoT devices. The combination of Symmetric and Asymmetric cryptographic algorihms reduces encryption

and decryption time compared to using only asymmetric cryptography. For each communication, a unique random key is generated and is generated using the current system timestamp as the seed. It in turn makes the communication more secure and susceptible to attacks. It also addresses the problem of session key distribution. The amount of plaintext encrypted is small, and all keys generated are unique. This increases the security of the scheme.

In paper [5], authors proposed a system which focuses on the hybrid cryptosystem which integrates algorithm like RC6, MD5 for hash function and optimized NTRU algorithm. The combination of RC6 symmetric algorithm and optimized NTRU public key algorithm are used to achieve the security requirements i.e confidentiality, authentication and non-repudiation. MD5 hash function provides the data integrity.

In paper [6], a detailed comparison of RSA and ECC algorithm performances with respect to their key size and the time taken to encrypt and decrypt the given text. During this analysis, it is found that Elliptic Curve Cryptography is the best algorithm when compared to the RSA algorithm with respect to Authentication, speed, scalability, flexibility, reliability, execution time , security and limitation that are essential for secure communication.

In paper [7], authors proposed a technique of Hybrid Encryption Algorithm which combines different algorithms and using the different key on blowfish and AES encryption are analyzed and it can be used in applications like military applications, hardware and software companies that need security in their products, banks, networks companies, big websites that have big databases and mobile networks. This paper also discusses a comparison between AES, DES, RSA, and Blowfish encryption algorithms.

In paper [8], author proposes RSA calculation architecture for FPGAs where the issues like scalability, flexible performance, and silicon efficiency for the hardware acceleration of Public Key cryptography are discussed. Using techniques based on Montgomery math for exponentiation, the proposed RSA calculation architecture is compared to existing FPGA-implementations on various parameters like speed, FPGA utilization, and scalability.

3. Algorithms used for Hybrid Cryptography

3.1 RSA Algorithm (Rivest-Shamir-Adleman):

RSA (Rivest–Shamir–Adleman) is first practically implemented public-key cryptographic algorithm and is widely used for transmitting confidential information securely. In this algorithm, the encryption key is public and the decryption key is private or secret. In RSA, this asymmetry is based on the practical difficulty of the factorization of the product of two large prime numbers.

RSA uses two keys one is public key and the other is private key. The public key is made known to everyone and it is used to encrypt secret messages. Messages encrypted using this public key can only be decrypted with the related key called private key. The two keys for the RSA algorithm are generated as follows:

Choose two large random prime numbers p and q,

1. Compute n= p x q
   n is the modulus for computing public key and the private key

2. Calculate totient function : $\Phi(n) = (p-1) \times (q-1)$

3. Choose integer e such that $1 < e < \Phi(n)$, and e is co-prime to $\Phi(n)$; e and $\Phi(n)$ share no factors other than 1; gcd $(e, \Phi(n)) = 1$. e is known as the Public key

4. Compute d to satisfy $1 \pmod{\phi(n)}$; $1+k\Phi(n)$ for some integer k. d is kept as the private key

For encrypting message m : $C=m^e \bmod n$ using e as public key
For decrypting message C : $m=c^d \bmod n$ using d as private key

RSA is a relatively slow algorithm, and because of this, it is less used to encrypt confidential messages. But, RSA algorithm used for sharing secret keys for symmetric key algorithms which in turn can perform bulk encryption-decryption operations at higher speed.

3.2 AES Algorithm (Advanced Encryption Standard):

The Advanced Encryption Standard (AES), also known as Rijndael is a specification for the encryption of electronic data established by the U.S. National Institute of Standards and Technology (NIST) in 2001. AES is based on a design principle known as a substitution–permutation network, and is efficient in both software and hardware.AES has a fixed block size of 128 bits, and a key size of 128, 192, or 256 bits producing 128 bits of ciphertext. AES operates on a 4 × 4 column-major order array of bytes, termed the state. Most AES calculations are done in a particular finite field.
The key size used for an AES cipher specifies the number of transformation rounds that convert the input, called the plaintext, into the final output, called the ciphertext. The numbers of rounds are as follows:

- 10 rounds for 128-bit keys.
- 12 rounds for 192-bit keys.
- 14 rounds for 256-bit keys.

AES consists of following functions.

1. **Sub Bytes**: a non-linear substitution step where each byte is replaced with another according to a lookup table.
2. **Shift Rows**: a transposition step where the last three rows of the state are shifted cyclically a certain number of steps.
3. **Mix Columns**: a linear mixing operation which operates on the columns of the state, combining the four bytes in each column.
4. **Add Round Key**: each byte of the state is combined with a block of the round key using bitwise xor.

Key Expansion: The AES key expansion algorithm takes asinput a four word(16 byte) key and produces stream of keys of 44 words. This is sufficient to provide 16 byte round key for the initial addround key stage and each of the 10 rounds of the cipher.

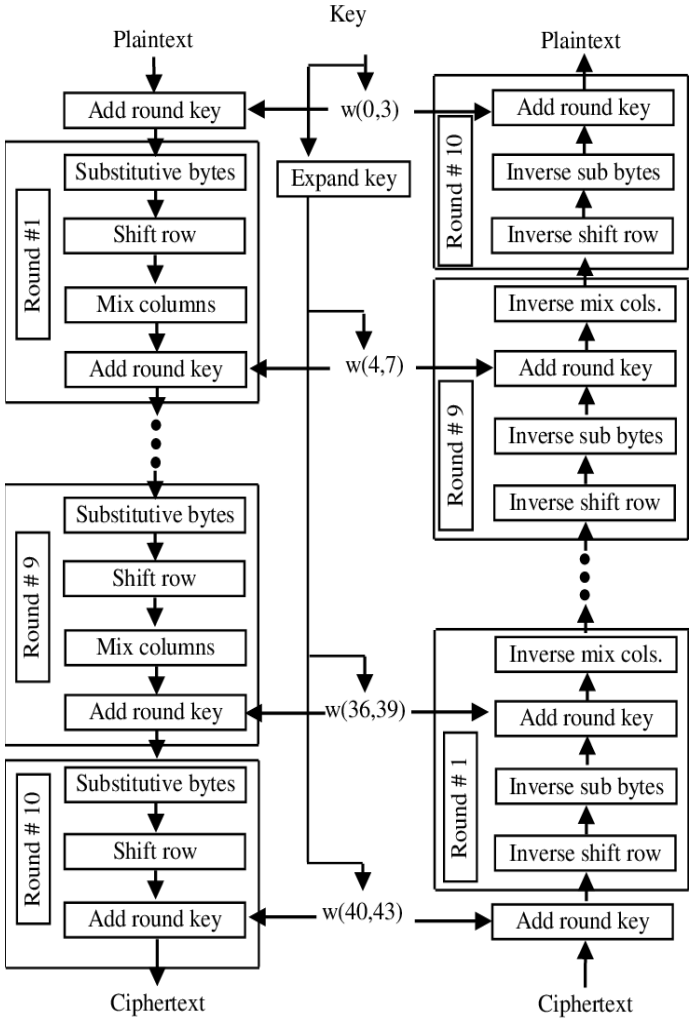

Fig 3: Block diagram of AES algorithm [9]

4. Proposed algorithm for Hybrid cryptography

As seen above, symmetric and asymmetric cryptography both have their own advantages and disadvantages. So, on combining both the cryptosystems, we get the Hybrid Cryptosystem. A hybrid cryptosystem is one which combines the convenience of a public-key cryptosystem with the efficiency of a symmetric-key cryptosystem.

The combination of encryption methods has various advantages. One is that a connection channel is established between two users' sets of equipment. Users then have the ability to communicate through hybrid encryption. Asymmetric encryption can slow down the encryption process, but with the simultaneous use of symmetric encryption, both forms of encryption are enhanced. The result is the added security of the transmittal process along with overall improved system performance. A Hybrid Cryptosystem can be constructed using two separate Cryptosystems one with a key encapsulation scheme which is a public key cryptosystem and other by a data encapsulation which is a symmetric key cryptosystem. The hybrid cryptosystem is itself a public-key system, who's public and private keys are the same as in the key encapsulation scheme.
The proposed technique in this work caters to the communication within the system .The aim is to secure the communication within the network and make it resilient to attacks. The proposed method is a combination of Symmetric and Asymmetric cryptographic techniques for transmission of data within the network. For encryption, the public key of the receiver is used, whereby the receiver, who is only the holder of the paired private key can decrypt the message encrypted key with the public key. For the proposed technique, the symmetric cryptographic algorithm used is AES algorithm. The Asymmetric cryptographic algorithm is the RSA Algorithm.

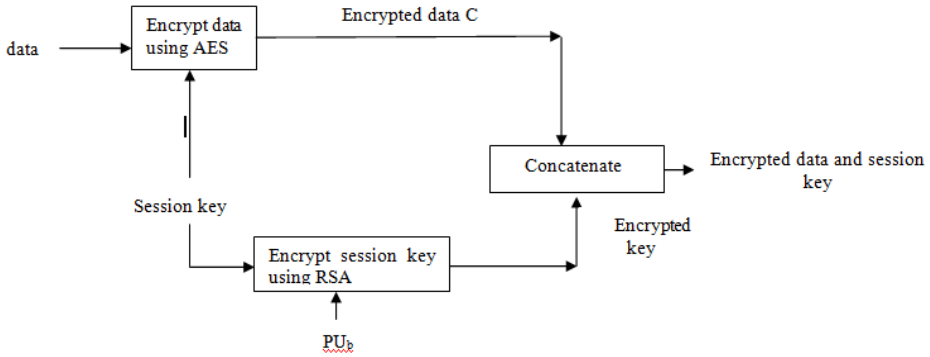

Fig 4: Block diagram of Encryption.

The above block diagram explains the encryption using Hybrid Cryptosystem. Here the key is encrypted using RSA algorithm and the same key is used to encrypt the data using AES algorithm.

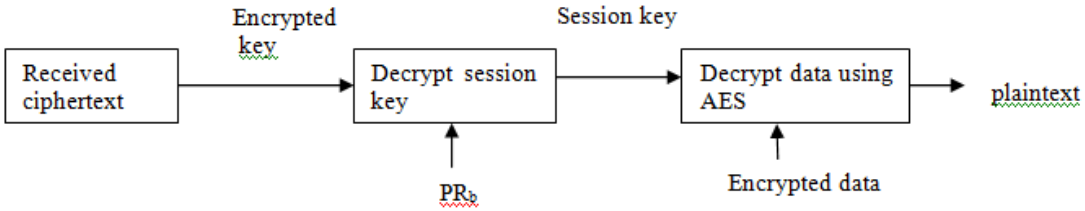

Fig 5: Block diagram of decryption.

The above block diagram explains briefly about the decryption. Here received encrypted key is decrypted using the private key and then that key is used to decrypt the data using AES algorithm and we obtain the final output.

Encryption:
$C1 = E_{ks}(M)$
$C2 = E_{PUb}(Ks)$
Concatenated data = (C1, C2)
Where
C1 => Encrypted data cipher
C2 => Encrypted secret key cipher
Ks => Secret key (or session key)
E_{ks} => Encryption using secret key (AES)
Pub => public key of receiver
E_{Pub} => Encryption using public key of receiver (RSA)

Decryption:
$ks' = D_{PRb}(C2)$
$M' = D_{ks'}(C1)$
where
C1 => Encrypted data cipher
C2 => Encrypted secret key cipher
Ks => Secret key (or session key)
Dks => Decryption using secret key (AES)
PRb => Private key of receiver
D_{PRb} => Decryption using private key of receiver (RSA)

5. Results and Discussion

The proposed algorithm is simulated on Xilinx ISE 14.7 using VHDL. The output of AES algorithm Hybrid Encryption algorithm is shown in fig.6 and fig.7 respectively. The encryption process as follows. First plaintext is encrypted with AES, cipher text is generated. Then again secret key is encrypted with RSA algorithm. Finally, ciphertext of plaintext and ciphertext of secret key are transmitted. The decryption process is as follows. At receiver side, first RSA decryption algorithm is used to retrieve secret key and using this secret key plaintext is retrieved.

Input primes: p=3 & q=5,

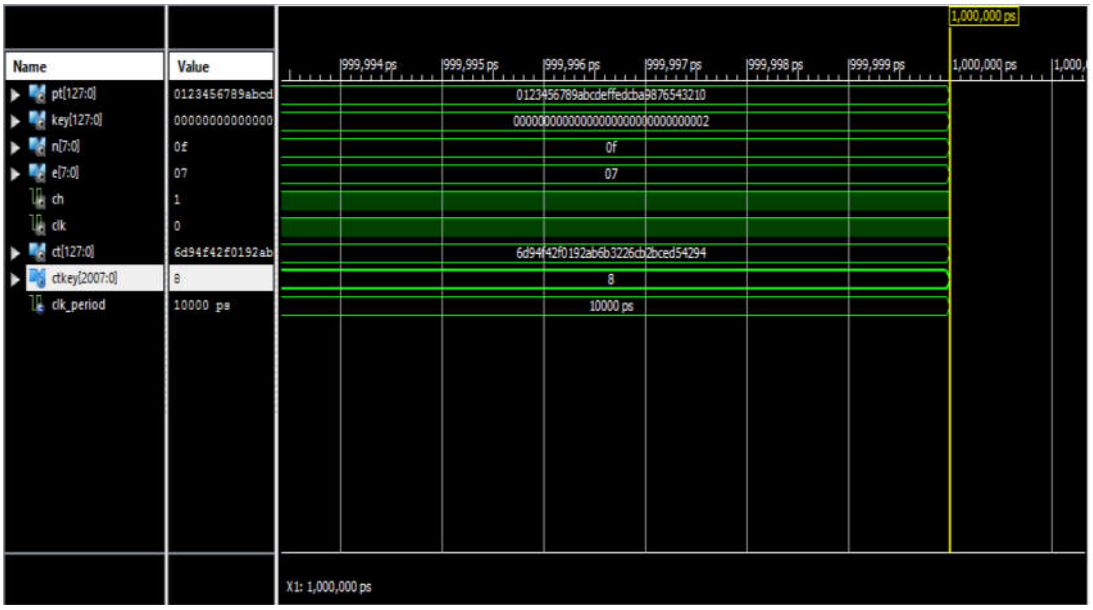

Fig 6 : Simulation results of AES encryption

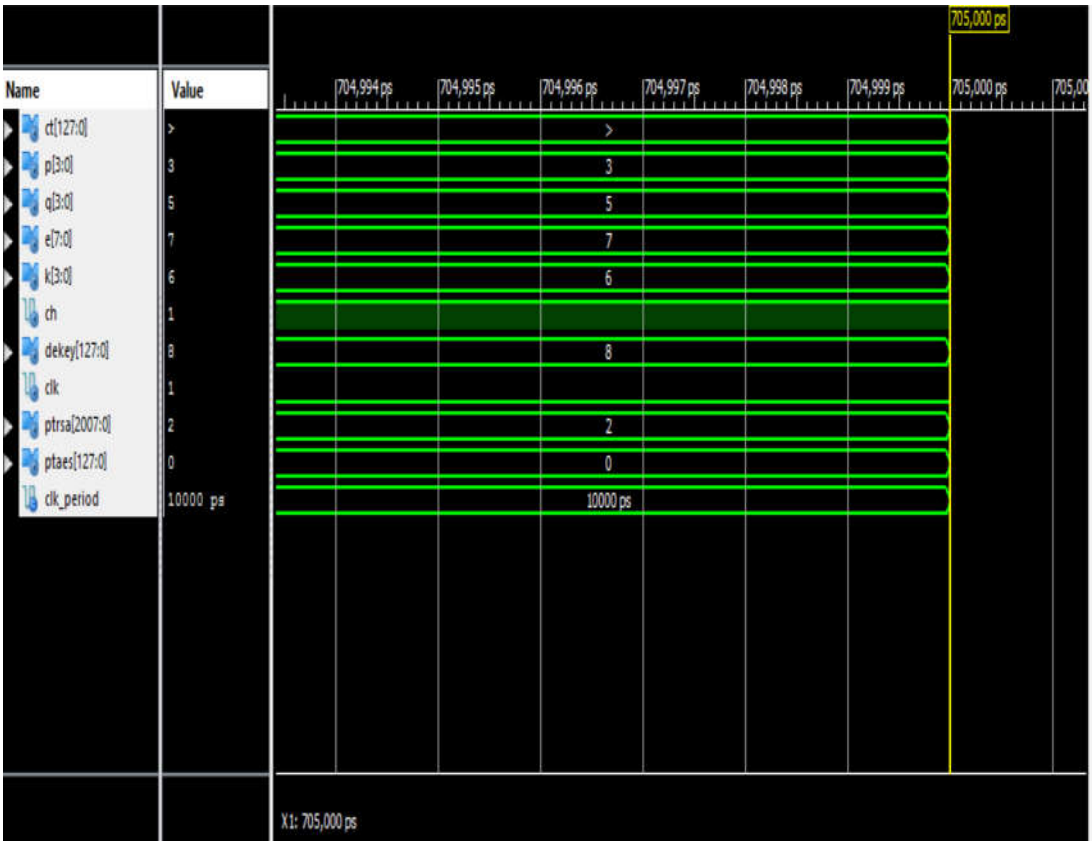

Fig 7: Simulation results of RSA algorithm

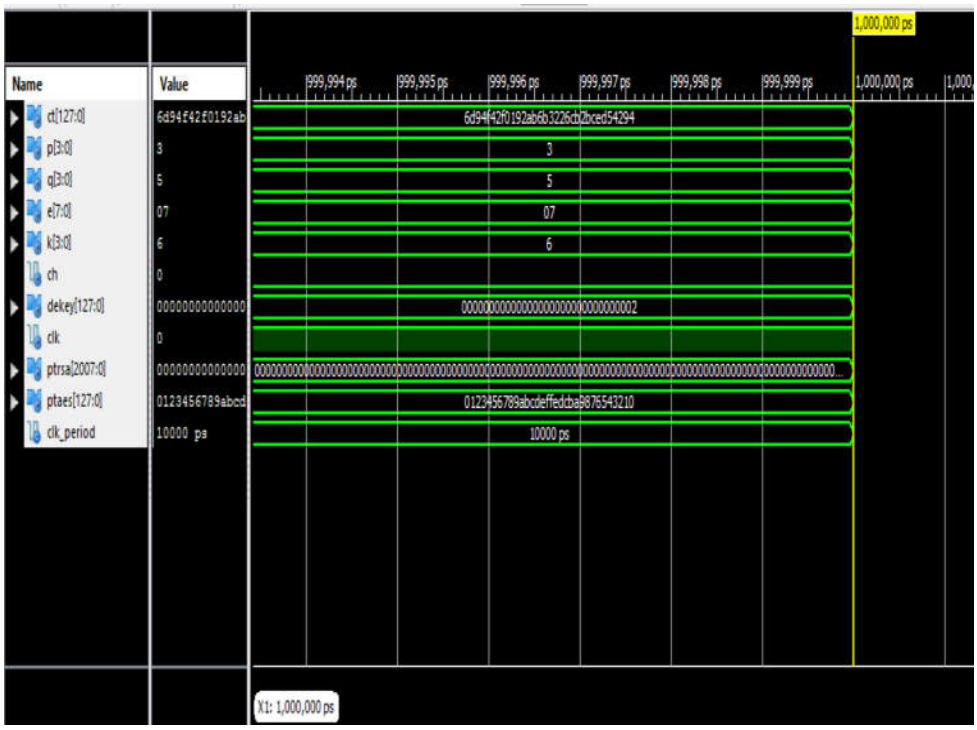

Fig 8: Simulation results of AES decryption

6. Conclusion

In this paper, a robust hybrid cryptographic scheme is designed. The advantages of symmetric cryptography and asymmetric cryptography are explored efficiently and disadvantages of both are overcome. The proposed technique uses AES as symmetric algorithm and RSA as asymmetric algorithm. It solves the problem of key exchange and gives better security. The proposed hybrid scheme is simulated on Xilinx 14.7 Isim. First plaintext is encrypted with AES, ciphertext is generated and then secret key used in AES is encrypted with RSA algorithm. Finally, ciphertext of plaintext and ciphertext of secret key are transmitted. At receiver side, first RSA decryption algorithm is used to retrieve secret key and using this secret key plaintext is retrieved. This proposed technique achieves confidentiality and authentication. It overcomes the problem of key exchange encountered in symmetric algorithms.

REFERENCES

[1] *Marwan Ali Albahar, Olayemi Olawumi, Keijo Haataja, Pekka Toivanen, "Novel Hybrid Encryption Algorithm Based on AES, RSA, and Twofish for Bluetooth Encryption". Journal of Information Security, 2018, 9, pp168-176*

[2] *Septimiu Fabian Mare, Mircea Vladutiu and Lucian Prodan, "Secret data communication System using Steganography, AES and RSA". IEEE 17th International Symposium for Design and Technology in Electronic Packaging (SIITME), 2011, pp 339-344*

[3] *Vanishreeprasad. S, K N Pushpalatha, "Design and Implementation of Hybrid Cryptosystem using AES and Hash Function", IOSR Journal of Electronics*

and Communication Engineering (IOSR-JECE), e-ISSN: 2278-2834,ISSN: 2278- 8735.Volume 10, Issue 3, Ver.II (May - Jun.2015), pp 18-24

[4] Kirtiraj Bhatele, Amit Sinhal, Mayank Pathak, "A Novel Approach to the Design of a New Hybrid Security Protocol Architecture", IEEE International Conference on Advanced Communication Control and Computing Technologies (ICACCCT), 2012, pp 429-433

[5] Michelle S Henriques , Nagaraj K. Vernekar, "Using symmetric and asymmetric cryptography to secure communication between devices in IOT", pp 1-4

[6] Thwe Thwe Ngwe, Su Wai Phyo, "Hybrid Cryptosystem for data security". International Journal of Advances in Electronics and Computer Science, ISSN:2393-2835 Volume-2, Issue-6, June-20, 2015, pp 1-6

[7] M.Gobi, R.Sridevi, R.Rahini priyadharshin, "A Comparative study on the performance and the security of RSA and ECC algorithm". Proceedings of the UGC Sponsored National Conference on Advanced Networking and Applications, 2015, PP 168-171

[8] Ali E,Taki El_Deen, "Design and Implementation of Hybrid Encryption Algorithm". International Journal of Scientific & Engineering Research, Volume 4, Issue 12, 2013, pp 669- 673

[9] E. Ramaraj, S. Karthikeyan, M. Hemalatha , "A Design of Security Protocol using Hybrid Encryption Technique (AES- Rijndael and RSA)", International Journal of The Computer, the Internet and Management Vol. 17.No.1 (January-April, 2009), pp 78-86

[10] S. Subasree and N. K. Sakthivel, " Design of a new Security Protocol using Hybrid Cryptography algorithms", IJRRAS 2 , February 2010, pp 95-103

[11] Rawya Rizk, Yasmin Alkady, "Two-phase hybrid cryptography algorithm for wirelesssensor networks", Journal of Electrical Systems and Information Technology, ScienceDirect, 2015, pp 296–313

[12] Ye Liu, Wei Gong, Wenqing Fan, "Application of AES and RSA Hybrid Algorithm in e-mail" , ICIS June 2018 ,pp 701-703

[13] Sourabh Chandra, Smita Paira, Sk Safikul alam, Goutam Sanyal, " A Comparative Survey of symmetric and asymmetric cryptography", International Conference on Electronics, Communication and Computational Engineering (ICECCE), 2014, pp 83- 93

[14] Arpit Agrawal, Gunjan Patankar, "Design of Hybrid Cryptography Algorithm for Secure Communication", International Research Journal of Engineering and Technology (IRJET), Volume: 03 Issue: 01 | Jan-2016, ISSN: 2395 - 0056, pp 1323-1326