International Journal of Applied Engineering Research
ISSN 0973-4562 Volume 10, Number 10 (2015) pp. 25207-25218

http://www.ripublication.com

An Encryption Scheme Based on AES and SHA-512

Veerpal Kaur[1] and Aman Singh[2]

[1]Department of Computer Science and Engineering,
Lovely Professional University, Phagwara, Punjab, India
[1]khaira.veerpal@gmail.com
[2]Assistant Professor, Department of Computer Science and Engineering,
Lovely Professional University, Phagwara, Punjab, India
[2]amansingh.x@gmail.com
Postal Address:
Aman Singh, 16826, Block 57, Room Number – 207
Assistant Professor, Department of Computer Science and Engineering,
Lovely Professional University, Phagwara, Punjab, India
Email: amansingh.x@gmail.com
Contact: 9988779907

ABSTRACT

As the network is growing at a much faster rate, more people are getting involved in communication with different perspectives. Some make use of the network to provide some harm to others. In order to protect such harms, there is a need to provide security to sensitive data and integrity check to verify the data if modified. To achieve this purpose, an encryption system is provided. For confidentiality, AES along with RSA is used and for integrity purpose, SHA-512 is used. AES alone provides great speed of encryption but is insecure if key get compromised. So key is secured by RSA. RSA alone for encryption is very slow. So AES-RSA hybrid is used to achieve both targets i.e. greater security with faster speed.

Keywords: RSA, SHA, AES, Hybrid Cryptography, Encryption

I. Introduction

Cryptography is a branch of network security that comprises of various techniques for data encryption and decryption. Data encryption refers to the methods used to convert readable content into unreadable one. Only the authorized entity can read it after decryption. Data decryption refers to the methods or techniques used to convert unreadable by back into readable one. A variety of algorithms are there for this purpose. These algorithms will make use of one or more keys. Some uses same keys for both encryption and decryption while others will make use of different keys. In symmetric key algorithms, same key is used for both encryption and decryption. In asymmetric key algorithms, different keys are there for encryption and decryption. It depends on the algorithm that how it will make use of different keys. There may be the case that public key is used for data encryption and private key for decryption or vice versa.

Symmetric key algorithms are popular for their ease of use and fast execution. These algorithms include AES (Advanced Encryption Standard), DES (Data Encryption Standard), 3-DES (triple-DES), Blowfish and some of their enhanced versions. Symmetric key cryptography suffers from the problem of various attacks on their keys. If intruder get the key used for encryption, it will be easy to decrypt the contents encrypted by that key. To solve key management problem, asymmetric key algorithms came into display. Asymmetric key algorithms or public-key cryptography provides great deal of security but suffers from slow execution speed. So in order to solve the problem of key management as well as speed, various research works combine the features of symmetric and asymmetric key cryptography and named it Hybrid Cryptography.

II. Algorithm for encryption

A. DES (Data Encryption Standard)

DES was one of the major advancements in the field of security. DES was published in 1977 under FIPS-46 by NBS. DES makes use of 56-bit key and processes a block size of 64 bits. Due to its short key-length, DES cannot resist Brute Force attack. The Electronics Frontier Foundation (EFF) provides successful attack on DES in just 22 hours and 15 minutes [6].

B. Triple-DES

Short key length problem is solved by DES that makes use of three keys and 168-key as a whole on the data to be transmitted as ciphertext.

$$C= \{[(P)E_{K1}]D_{K2}\}E_{K3}$$

where P is the plaintext and C is the ciphertext. Plaintext is made to pass through DES for encryption with K_1 as key, the ciphertext came from this will be passed through DES for decryption with K_2 and then this output is again enciphered by DES using K_3 key. Final ciphertext is used to send to the receiver.

Another way used by triple-DES is

$$C= \{[(P)E_{K1}]E_{K2}\}E_{K3}$$

Plaintext is made to pass through DES for encryption with K_1 as key, the ciphertext came from this will be passed through DES for encryption with K_2 and then this output is again enciphered by DES using K_3 key. Final ciphertext is used to send to the receiver.

Such a lengthy process, no doubt provides security, but lags behind in some other parameters. Those parameters are resources consumed, encryption and decryption time.

C. AES (Advanced Encryption Standard)

In order to overcome these parameter requirements, AES is used. AES provides security more than triple-DES and also faster in execution, low resource requirement, efficient and scalable architecture. So AES is a better alternative over triple-DES.

The Advanced Encryption Standard (AES) is named as Federal Information Processing Standard (FIPS-197) by NIST that is used to protect sensitive information and can be used by various military and intelligence organizations. Rijndael was the algorithm named as AES developed by Dr. Joan Daemen and Dr. Vincent Rijmen. AES is a symmetric key algorithm which is non-Fiestel in nature. Being a block cipher, AES encrypts and decrypts 12-bit block size of data. AES can make use of different key size out of 128,192 and 256 bit keys. Based on the key size used, AES is named as AES-128, AES-192 and AES-256 respectively.

III. Key Management

Symmetric key cryptography faced a problem of key management. As if the key gets compromised, complete scheme will be prone to the intruder. For this reason, RSA is used to encrypt the key of AES. RSA is a public key algorithm developed by Ron Rivest, Adi Shamir and Leonard Adleman in 1977. RSA is the most popular and secure algorithm till today. No such attack has been encountered on RSA as Brute Force Attack. The security of RSA algorithm eventually lies on our incapability to efficiently factor large integers. The RSA public key encryption method is the first case of a provably safe public key encryption method against chosen message attacks.

RSA is a block cipher technique in which the plaintext and ciphertext are integers in between 0 and n-1 for various n. A standard size for n is 1024 bits i.e. $n < 2^{1024}$. Plaintext is encrypted in blocks, with every block having a binary value fewer than various number n i.e. the block size have to be less than or equivalent to log2(n)+1 . Normally, block size is *i* bits, where $2^i<n<=2^i+1$. Encryption and decryption are of the subsequent form, for some plaintext block M and ciphertext block C.

$$C = M^e \bmod n$$

$$M = C^d \bmod n = (M^e)^d \bmod n = M^{ed} \bmod n$$

IV. SHA Family for Integrity

Secure hash algorithm was developed in 1993 and published by NIST under the name of Federal Information Processing Standard (FIPS PUB 180). Initially, SHA is referred as SHA-0 then a revised version of SHA came into display in 1995 and named as SHA-1 which is very similar in design with MD-4 hash functions family.

Secure hash algorithms are one-way hash function that are used to create a message digest. This message digest is used to check the integrity of the message transmitted. Any change in the message reflects different message digest. So secure hash algorithms to verify digital signatures and MACs (Message Authentication Codes). The digest created by different members of SHA-1 creates a hash digest of 160-bits. SHA-1 published as FIPS 180-1 is computationally infeasible because it is very difficult to calculate message back from message digest. But mathematical weaknesses have been discovered in SHA-1 and get resolved by SHA-2.

FIPS 180-2 issued by NIST in 2002 provided three new versions of SHA-2 with difference in their hash digests produced. Those are SHA-256, SHA-384 and SHA-512. SHA-2 uses same arithmetic and binary operations and has same underlying architecture as of SHA-1.

The longer the key length of an algorithm, the more secure the algorithm is against cryptanalysis. The more secure the algorithm, the longer it will take to calculate the result. SHA-512 is not only more secured but also faster.

V. Literature Review

Abdullah Al Hasib and Abul Ahsan Md. Mahmudul Haque (2008) have conducted a study to compare the performance and security issues of two cryptographic algorithms: AES and RSA. AES being a symmetric key algorithm is different from RSA which is an asymmetric key algorithm. Various security and computational issues have been provided for both the algorithms. Considering the security of AES, no successful attack has been performed since its advent. AES uses different key sizes for encryption such as 128, 192 and 256 bits. So for a successful brute force attack, an attacker has to try 2^{128}, 2^{192} and 2^{256} possible keys respectively. It would be infeasible to try such a large key space. AES is also secure against mathematical attacks as there is no such vulnerability in its mathematical computation that gives rise to any attack. But AES is less secure against side channel attacks. Considering the security of RSA, it is proven that RSA with short private key is insecure against brute force as well as mathematical attack. As the security of RSA is dependent on the difficulty of factorization into prime numbers, it is suggested to choose large keys i.e. 2048 bits to avoid these attacks. So the discussion concluded that AES is faster and provides great security as compared to other symmetric key algorithms and RSA is safer but slower algorithm. RSA provides great security against different kind of attacks and AES provides great speed. So it would be effective to combine both in such a new that AES serves the purpose of encryption and decryption and RSA eliminates the problem of key management by encrypting the key of AES [3].

Y. Wang and M. Hu (2009) presented a timing evaluation model for comparison of triple-DES, AES and RSA. Two different evaluation methods were used. One is Same Plaintext Different Keys (SPDK) and the other one is Different plaintexts Same key (DPSK). The model used for evaluation has a random number generator. When DPSK method is used for evaluation, the evaluated plaintexts standardized to 10000 with size of 4KB each. 128-bit AES and 192-bit RSA were used. Results showed that the average time consuming (AVT) factor for AES is significantly less (0.008458) than triple-DES (0.027295) and RSA (2.183258). When SPDK method is used for evaluation, the evaluated plaintexts standardized to 10000 with size of 4KB each. 128-bit AES resulted to have least AVT factor i.e. 0.008584 as compared to triple-DES (0.028606) and RSA (2.355474) [16]. From the evaluation conducted, it is clear that AES is better than triple-DES and RSA irrespective of its key size being used. No doubt, RSA provides greater security but it is used for small input whereas AES provides equivalent security to large volume of data.

Hamdan.O.Alanazi, B.B.Zaidan, A.A.Zaidan, Hamid A.Jalab, M.Shabbir and Y. Al-Nabhani (2010) implemented and analyzed various symmetric cryptosystems. The paper shows nine factors based on which the comparison between symmetric key algorithms has been made. Some of the factors considered to compare DES, triple-DES and AES:

- The key length used by the algorithm: DES uses a key of size 56-bits where triple-DES uses key lengths of 168 (K1, K2, K3 independent) and 122 (when K1 and K2 is same) and AES uses key lengths of 128, 192 and 256 bits.
- The block size that the algorithms consider for encryption: DES and triple-DES need a block size of 64 bits whereas AES uses different block sizes of 128,192 or 256 bits depending upon the requirement.
- Cryptanalysis resistance: whether the algorithm used provides good security against attacks or not. DES is vulnerable to differential and linear cryptanalysis and has a problem of weak substitution tables. Triple-DES is also vulnerable to differential attacks but secure against brute force attack due to its large key size. AES is strong against differential, linear, truncated differential, interpolation and square attacks.
- Security: due to various successful attacks, DES is proven to be infeasible to use. Triple-DES is an alternative to DES because of its resistance to attacks due to large key size. AES is considered to be secure as no such attack has been proven successful against it.
- The number of possible keys: DES provides small key space of 2^{56} possible keys to get the plaintext whereas triple-DES avails large key space of 2^{122} and 2^{168} possible keys. AES have even larger key space of 2^{128}, 2^{192} and 2^{256} possible keys.
- Time required to try all the possible key combinations in case of any attack: DES may require just 400 days trying small key combination of 2^{56} keys whereas triple-DES requires just double of it i.e. 800 days. AES needs long time duration of atleast $5x10^{21}$ years trying all possible keys. [8]

Jian Zhang and Xuling Jin (2012) have proposed an encryption system that makes use of triple-DES for encryption purpose and to achieve greater security, the keys of triple-DES have been encrypted with RSA. SHA-1 is used in the encryption system to check the integrity of the messages being transmitted. The main aim of the proposed encryption system is to provide both confidentiality as well as integrity. The ciphertext, the keys of ciphertext and the hash value generated by 3-DES, RSA and SHA-1 respectively are transmitted as a combination. The combination gets separated at the receiver end from which the hash value kept secretly. Decryption of keys and then decryption of ciphertext is done. Then the decrypted plaintext is provided to SHA-1 to produce a hash value. This hash value will be compared with the hash value originally sent along with the ciphertext and the key of ciphertext. If both the hash values matches, integrity is thought to be maintained else not [11].

A. K. Mandal, C. Parakash, and Mrs. A. Tiwari (2012) conducted a performance evaluation of AES and DES based on avalanche effect, memory required and simulation time. The paper made use of different techniques to carry out this evaluation. For avalanche effect, keeping key constant, 1-bit variation of plaintext is carried out which shows that AES has greater avalanche effect 83 compared to DES (43). Keeping plaintext constant and 1-bit variation in key provides greater avalanche effect for AES i.e. 81 as compared to DES which resulted in avalanche effect of 41. For the factor of memory required, it is necessary to implement both the algorithms. Depending upon the number of operations an algorithm performs, the memory consumption is judged. Based on this implementation, the results show that AES requires less memory for implementation 10.2 KB as compared to DES i.e. 43.3 KB. For comparison of simulation time, the algorithms need to prove themselves as fast. The simulation time for an algorithm depends on various factors such as algorithm complexity, speed of the processor on which it is running and many others. The results show that less simulation time is needed for AES i.e. 0.0304 seconds than 0.32 seconds for DES. So the paper shows that AES is better than DES in all the considered factors [4].

In "Hybrid crypto hardware utilizing symmetric-key and public-key cryptosystems", A. A. Gutub, and F. A. Khan (2012) proposed a design of the hybrid cryptosystem that made use of both symmetric and asymmetric key algorithms. The implementation has made use of a pseudorandom number generator for the purpose of random key generation. A computation unit based on GCD is used for RSA. The system will make use of symmetric key algorithms for encryption as well as decryption and public key algorithms for key management. The system works on an assumption that the public key of the receiver is already known. No explicit key management is there. Any symmetric key algorithm such as AES or DES is used for encryption and decryption and public key algorithm as RSA is used to encrypt the key of symmetric cryptosystem used [2]. The hybrid cryptosystem at the source make the user free to choose whether he wants to use AES or DES for encryption as well as decryption. The provided input is encrypted by the chosen encryption algorithm and the key for the same algorithm used is encrypted by RSA. The resultant encrypted data and the encrypted symmetric key is sent to the receiver in a single block of data. At the receiver end, first the symmetric key gets decrypted and then the same is used to decrypt the data being transmitted. This hybrid cryptosystem has two major advantages:

- Any number of keys can be used for encryption because the encrypted data and encrypted key are both the part of the same data block to be sent to the receiver
- Key management need not to be done explicitly [2]

Kirtiraj Bhatele, Prof. Amit Sinhal and Prof. Mayank Pathak (2012) proposed a new architecture for the hybrid security protocol has been presented. The design of the protocol is based on both symmetric key algorithms and asymmetric key algorithms, combination of which is known as hybrid cryptography. This approach is used for online transaction [12] and is based on the work proposed by Ravindra Kumar Chahar, Gautam Data, Prof. Navin Rajpal (2007) in "*Design of New Security Protocol"* and the work proposed by S. Subasree, N. K. Saktivel (2010) in "*Design of a New Security Protocol Using Hybrid Cryptography Algorithm".* The new enhancement has been made in the security protocol design which make use of AES for encryption, MD5 for integrity check and Dual RSA to provide security to the digest of MD5 [12]. The Dual-RSA used in the paper provides more security than RSA alone. This paper has the advantage of better message security provided by Dual-RSA as well as less execution time because AES is used.

Ravindra Kumar Chahar, Gautam Data, Prof. Navin Rajpal (2007) in "*Design of New Security Protocol"* have made use of Elliptic curve cryptography used for encryption, RSA for authentication and integrity check using MD5 [14].

S. Subasree, N. K. Saktivel (2010) in "*Design of a New Security Protocol Using Hybrid Cryptography Algorithm",* new approach has been provided for enhancing the security. This design made use of ECC for encryption, Dual RSA for authentication and MD5 for integrity check. The Dual-RSA used in the paper provides more security than RSA alone [15].

A. Ramesh and Dr. A. Suruliandi (2013) have conducted an analysis for encryption algorithms based on their performance. The performance of the algorithms included varies based on their execution time, memory required for execution and throughput. For this purpose, three encryption algorithms have been used. They are DES, AES and Blowfish. Based on the results so obtained, Blowfish is considered to be the best algorithm in factors such as less execution time, least memory usage and faster in terms of throughput. DES consumes more memory i.e. 43.2 KBytes as compared to AES (32.5 Kbytes) and Blowfish (25.2). A comparison is shown based on throughput and results show that Blowfish (2270.268 Bytes/sec) is faster than DES (1268.765 Bytes/sec) and AES being the slowest provides a throughput of 558.2886 Bytes/sec [5].

VI. PROPOSED METHODOLOGY

The proposed encryption system provides higher security that resists most commonly used brute force attack. Symmetric key algorithms are faster than public key algorithms. So a combination of both these approaches will result in an encryption system that provides higher security with faster speed. The available plaintext is encrypted by AES. Being a symmetric key algorithm, AES may face an attack on its key. So security should be provided for key management. The key of AES is then encrypted by RSA. Same plaintext is passed through SHA-512 to create a message digest. Encrypted key, encrypted text and message digest will be combined and sent to the receiver end.

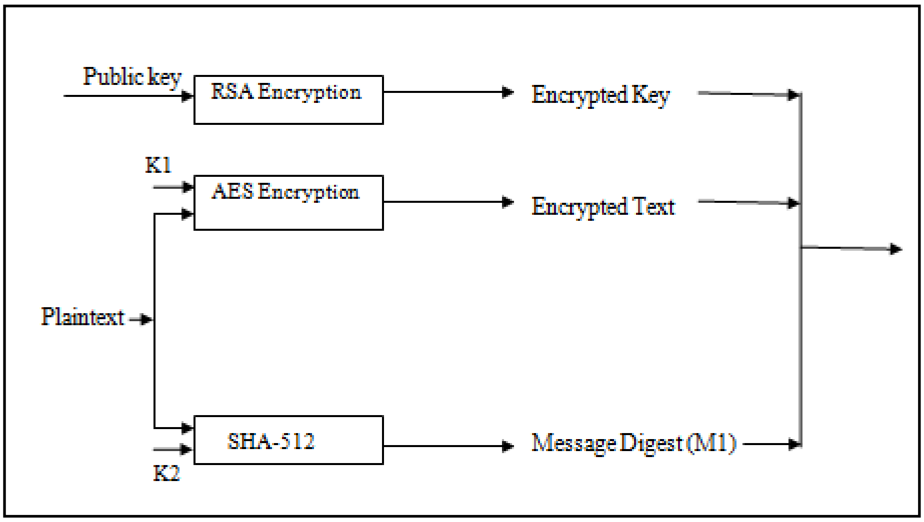

Figure 1: Proposed encryption scheme at sender site

The receiver firstly separate the encrypted key, the encrypted text and the message digest M1. The encrypted key is passed through RSA and provided to AES to decrypt the encrypted text. The resultant plaintext is given to SHA-512 and the outcome is message digest M2. M2 is then compared with the original message digest M1 to check if the message is altered during the transmission or not.

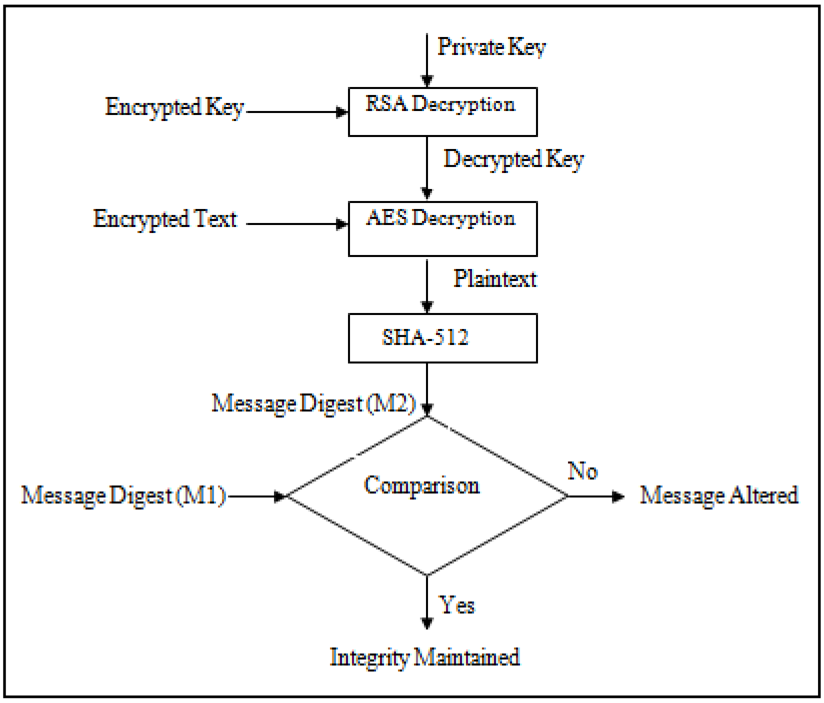

Figure 2: Proposed encryption scheme at sender site

A random function is used to combine the encrypted key; the encrypted text and the message digest M1. If intruder try to get this combination, he, firstly, has to break the combination. Then he has to break the RSA to get the key of AES. Then only he will be able to reach at the encrypted text of AES. It will take quite a long time to get the original message, till then the information is of no use.

VII. Results And Discussions

The proposed work is implemented in C# in Visual Studio Ultimate 2012 on dual core processor and running Window 8 system. Timing evaluation of AES and RSA is conducted individually and then hybrid of AES-RSA put into work. Results show that RSA consumes more time than AES as well as hybrid. AES consumes less time than both RSA and hybrid. But we can make compromise for speed if hybrid provides more security than AES alone. So hybrid provides faster implementation as well as higher security.

Table 1: Timing evaluation of hybrid with respect to individual algorithms used

	Encryption Time (in milliseconds)	Decryption Time (in milliseconds)
AES	17	260
RSA	827	1
SHA-512	3	445
AES-RSA	581	261
AES-RSA-SHA-512	298	968

A. Security Analysis

The security provided by the proposed encryption scheme has been checked. The attacker may get success when there is a ciphertext obtained through AES algorithm. The plaintext provided to the AES, for example, is “Lovely University” with “Education” as a key. The output will be:

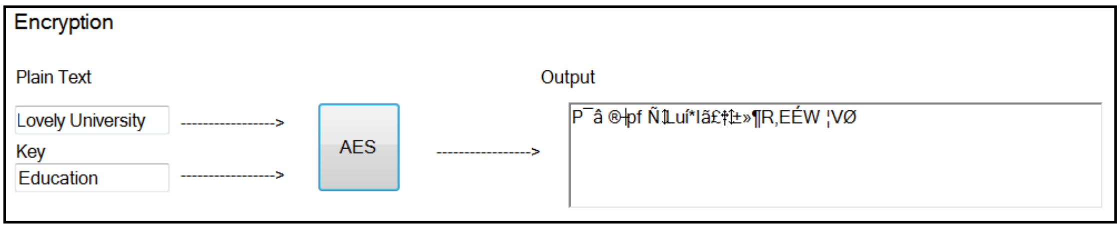

Figure 3: Output of AES encryption

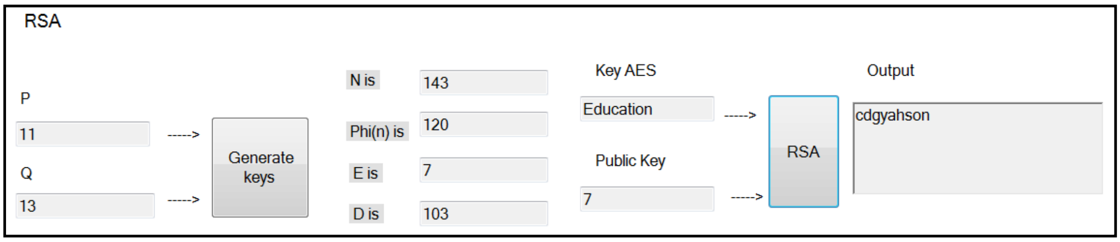

Figure 4: Output of RSA encryption

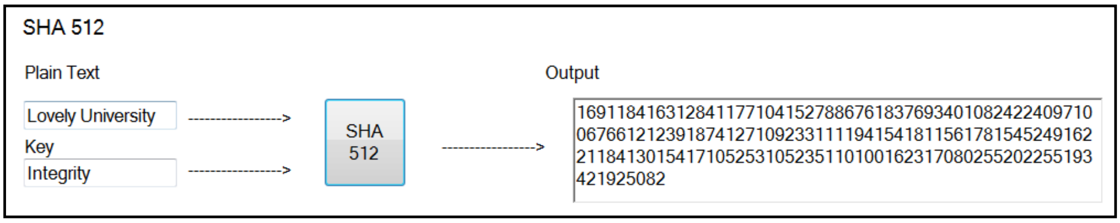

Figure 5: Hash value provided by SHA-512

The proposed encryption scheme uses a random function that jumbles the output of AES, RSA and SHA-512. The final message to be transmitted will be as:

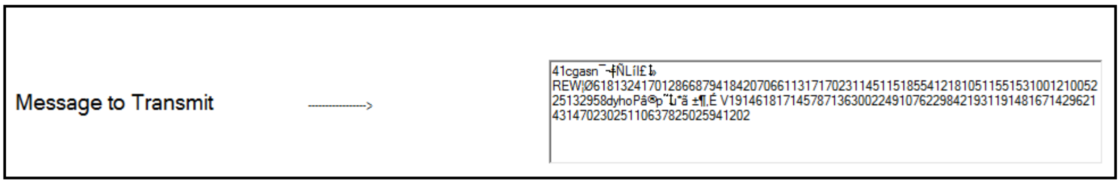

Figure 6: Jumbled output of AES, RSA and SHA-512

Considering the brute force attack, the attacker may try all the possible combination of keys on the ciphertext of AES and may get success even after a long time. But in the proposed scheme the attacker will face a problem in separating the combination into ciphertext of the message, ciphertext of key of AES and hash value calculated by SHA-512. The attacker, firstly, has to try all possible combinations to separate the outputs of these three algorithms and after that he may think of attacking the algorithms individually.

VIII. CONCLUSION

An encryption system has been proposed that provides three primitives of security i.e. confidentiality, authenticity and integrity. AES is used to provide confidentiality, RSA for authenticity and integrity check is done by SHA-512. Encryption of the key of AES with RSA offers great deal of security. It takes around trillion years to attack on the ciphertext of AES alone. The inclusion of RSA in the hybrid scheme will provide more hindrance to the attacker to crack the hybrid. Being a symmetric key algorithm, AES offers good speed for computation and resistance against square attacks. The main problem of symmetric key algorithms as AES is key management. RSA is used to solve this problem. This hybrid approach is useful where there is a need for high computational speed and security. Integrity check offers additional perks to the encryption system proposed. Instead of SHA-512, research works in near future may include SHA-3 i.e. keccak to provide more security to the encryption scheme available.

IX. REFERENCES

[1] Kahate, A., 2013, "*Cryptography and Network Security*", Tata McGraw Hill Education (India) Private Limited.

[2] Gutub, A. A., and Khan, F. A., 2012, "*Hybrid Crypto Hardware Utilizing Symmetric-Key & Public-Key Cryptosystems*", 2012 International Conference on Advanced Computer Science Applications and Technologies.

[3] Hasib A. A., and Haque, A. A. M., 2008, "*A Comparative Study of the Performance and Security Issues of AES and RSA Cryptography*", Third International Conference on Convergence and Hybrid Information Technology.

[4] Mandal, A. K., Parakash, C., and Tiwari, A., 2012, "*Performance Evaluation of Cryptographic Algorithms: DES and AES*", 2012 IEEE Students' Conference on Electrical, Electronics and Computer Science.

[5] Ramesh A., and Suruliandi, A., 2013"*Performance Analysis of Encryption Algorithms for Information Security*", International Conference on Circuits, Power and Computing Technologies.

[6] Federal Information Processing Standards Publication-197 (FIPS-197), November 26, 2001.

[7] Federal Information Processing Standards Publication (FIPS Publication 180-2), August 1, 2002.

[8] Alanazi, H. A., Zaidan, B,B., Zaidan, A. A., Jalab, H.A., Shabbir, M., and Al-Nabhani, Y., 2010, "*New Comparative Study between DES, 3-DES and AES within Nine Factors*", Journal of Computing, Volume 2, Issue 3, March.

[9] WANG, H., SONG, Z., NIU, X., and DING, Q., 2013, "*Key Generation Research of RSA Public Cryptosystem and Matlab Implement*", International Conference on Sensor Network Security Technology and Private Communication System.

[10] Ahmed, J. M., and Ali, Z., 2011, "*The Enhancement of Computation Technique By Combining RSA and El-Gamal Cryptosystems*", International Conference on Electrical Engineering and Informatics,17-19 July 2011, Bandung, Indonesia.

[11] Zhang, J., and Jin, X., 2012, "*Encryption System Design Based On DES and SHA-1*", 2012 11th International Symposium on Distributed Computing and Applications to Business, Engineering & Science.

[12] Bhatele, K., Sinhal, A., and Pathak, M., 2012, "*A Novel Approach to the Design of a New Hybrid Security Protocol Architecture*", IEEE International Conference on Advanced Communication Control and Computing Technologies.

[13] Wang, L., and Zhang, Y., 2011, "*A New Personal Information Protection Approach Based on RSA Cryptography*", IEEE.

[14] Chahar, R. K., Data, G., and Rajpal, N., 2007, "*Design of New Security Protocol*", IEEE International Conference on Computational Intelligence And Multimedia Applications, pp 132-134.

[15] Subasree, S., Saktivel, N. K., 2010, "*Design of A New Security Protocol Using Hybrid Cryptog'raphy Algorithm*", IJRRAS 2.

[16] Wang, Y., and Hu, M., 2009, "*Timing evaluation of the known cryptographic algorithms*", 2009 International Conference on Computational Intelligence and Security.

References to websites

[17] http://link.springer.com/chapter/10.1007/3-540-45811-5_6

[18] http://www.digicert.com/transitioning-to-sha-2.htm

[19] FIPS 46-3 from http://csrc.nist.gov/groups/STM/cavp/standards.html