I. J. Mathematical Sciences and Computing, **2020, 4, 35-41**
Published Online August 2020 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijmsc.2020.04.04

Hybrid Cryptography: Performance Analysis of Various Cryptographic Combinations for Secure Communication

Zuhi Subedar
Assistant Professsor, Belagavi, Karnataka,India
E-mail: zuhi.subedar@gmail.com

Ashwini Araballi
Assistant Professor, Belagavi, Karnataka,India

Received: 29 May 2020; Accepted: 15 July 2020; Published: 08 August 2020

Abstract: The amount of data that is transmitted across the internet is continuously increasing. With the transmission of this huge volume of data, the need of an encryption algorithm that guarantees the data transmission speedily and in a secure manner is a must. Hence, to achieve security in wireless networks, cryptography plays a very important role. In this paper, several hybrid combinations, which combines both symmetric and asymmetric cryptographic techniques to offer high security with minimum key maintenance is presented. This hybrid combination offers several cryptographic primitives such as integrity, confidentiality and authentication, thereby enhancing the security. Various combinations of Advanced Encryption Standard (AES), Elliptical Curve Cryptography (ECC) and Rivest, Shamir and Adleman (RSA) algorithms are used to provide hybrid encryption. Secure Hash Algorithm (SHA-256) is also used to provide authentication and integrity. The experimental results show that the proposed hybrid combinations gives better performance in terms of computation time compared to individual cryptographic schemes.

Index Terms*:* Symmetric cryptography, Asymmetric cryptography, SHA-256, Hybrid Cryptography, security etc.

1. Introduction

As the Internet and other forms of electronic communication become more prevalent, electronic security is becoming increasingly important [1]. Thus, it becomes essential to protect e-mail messages, credit card information, and corporate data, by means of encryption.

Various cryptographic algorithms have been proposed to achieve the security requirements such as Authentication, Confidentiality, and Integrity. Authentication means preventing unauthorized parties from participating in the network. Confidentiality means maintaining secrecy of information from unauthorized parties. Integrity ensures the receiver that the received data is not altered in transit by an adversary. There are basically two types of encryption techniques; symmetric and asymmetric. Symmetric cryptography is the one which uses a single key for encryption and decryption. The common symmetric encryption algorithms include Data Encryption Standard (DES)[2] and Advanced Encryption Standard (AES)[3]. Asymmetric key cryptography, on the other hand, requires special keys to encrypt and decrypt messages. The Common asymmetric encryption algorithms include RSA[4] and Elliptic Curve Cryptography (ECC) [5]. The Symmetric encryption techniques provide cost-effective and efficient methods of securing data without compromising security however; sharing the secret key is a problem. On the other hand, asymmetric techniques solve the problem of distributing the key for encryption, but; they are slow compared to symmetric encryption and consume more computer resources. Therefore, the best possible solution for encryption would be the complementary use of both symmetric and asymmetric encryption techniques, called Hybrid Encryption. Hybrid encryption attempts to exploit the advantages of both kinds of cryptography techniques while avoiding their disadvantages. In addition, Hashing creates a unique, fixed-length signature for a message or data set, which is commonly used to check data integrity. Secure Hash Algorithm (SHA-256) and Message Digest-5 (MD5) algorithms are widely used in a wide variety of security applications.

In this paper, a hybrid model is designed to provide data security and users authenticity. This model is formed with different combinations like (AES-RSA) and (ECC-RSA) to achieve confidentiality together with SHA-256 algorithm to achieve authentication and integrity. The hybrid encryption algorithm has greatly improved the security of the encryption algorithm since it combines the advantages of both asymmetric and symmetric algorithms [6]. Another hybrid combination RSA-ECC along with SHA-256 can also be considered as one of the strongest hybrid model.

2. Existing System

In the current encryption systems, individual algorithms are used to secure data. For instance, Linux systems harness MD5 hash scheme while some other exploits AES or DES algorithms to encrypt their passwords. But each of these algorithms has been cracked some or the other time, which means they are not unconquerable and can be broken by a skilled hand. Thus the security of the data (passwords in many cases) is highly and threateningly compromised. All these algorithms are very famous all around the globe and are used by many, some are even open source. This means that the algorithm's flaws are well known to all and in some cases, even the source code is well known to many. This appends up to the security woes of these algorithms. Thus, there needs to be a system which overcomes these drawbacks while upholding the positive aspects of these widely known algorithms [6].

Wei-hong [7], adopted three most widely used cryptosystems like RSA, DSA and ECC, in this ECC endeavors the highest security among current public key cryptosystems. Its characteristics are small key size, fast key generation, low power, and low hardware requirements.

Using a single encryption algorithm in communication renders it vulnerable to active and passive types of attacks. Thus, using multiple algorithms in a sequence where the output of one algorithm is the input for the next algorithm in the series provides additional security by protecting the data exponentially as well as makes it feasible to be implemented for passwords for extra protection. The multiple encryptions along with the randomness in nature of the selection of the algorithms, their sequence and the number of algorithms used, would provide highest safety with shortest key length. The computational parameters like shortest response time, highest throughput and minimum memory usage helps us in deciding the best hybrid combinations among the existing individual and hybrid encryption schemes.

3.Proposed System

The system proposed here, aspires to describe a hybrid system where encryption algorithms are used in a predefined order on an identical data set one after another to finally procure data in an encrypted form. This encrypted data or cipher text can be used to transfer the confidential data without the fear of being rigged. The only way to decrypt encrypted data is to operate the exact reverse order of the encryption process used at encryption stage [6].

The proposed hybrid crypto model aims to build an efficient and secure encryption algorithm which is based on merging the encryption schemes to make hybrid encryption algorithm that can encrypt and decrypt data efficiently in a secure manner by means of the best suited routing algorithms for optimal data transmission.

There are a variety of routing protocols that exist in ANETs and the routing protocols chosen may have an effect on the performance of network [8,9]. Paper [8] entails a comparative study of AODV, DSDV, and ZRP protocols owing to Routing Approaches, Structure, Selection, Tabulation, Maintenance, Operations, Strengths and Weaknesses.

A Secured Authenticated Scheme (SAS) that is presented in this paper combines both public and private key cryptographic techniques to form Hybrid cryptography that enhances security for secure data transmission. With the application of hashing it is robust against different types of attacks such as brute force, masquerading, replay, Denial of Service etc.

4. Implementation Model

The Hybrid Encryption model is as shown in Fig.1 in which the plaintext message is encrypted using Symmetric cryptography and the derived cipher text is communicated over a secure channel. In contrast, the hash value is computed for the same plaintext using SHA-256 and is concatenated with the symmetric key to form data and key encapsulation. Then, concatenated data is encrypted using asymmetric cryptography. Thus, the cipher-text obtained is the concatenation of Symmetric and Asymmetric Cipher.

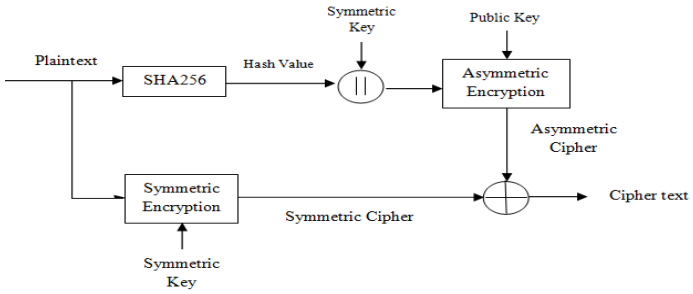

Fig.1. Hybrid Encryption Model

The hybrid decryption model is shown in Fig. 2 which details the exact reverse sequence of the operations of encryption phase to decrypt the cipher text, thus even if the algorithms used in this process are known, unless the sequence of decryption is known, the decryption is impossible.

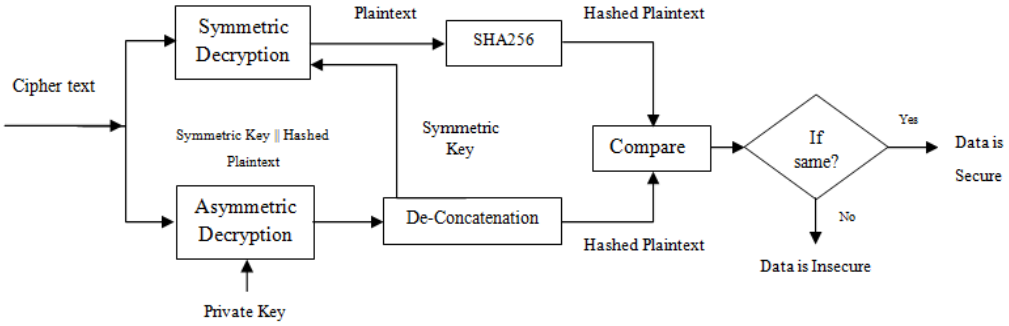

Fig.2. Hybrid Decryption Model

5. Result Representation

Extensive experiments were performed to analyze the efficiency of the implemented hybrid combinations in terms of encoding-decoding time, security proportions, memory usage and overall throughput. The hybrid cryptography algorithms were tested using MATLAB tool for different text or message lengths.

A. Time of Encryption and Decryption Processes:

The encryption time is the time taken to convert plaintext to cipher text and the decryption time is the time taken convert cipher text back to plaintext. [10]. Table 1 shows the time taken to encrypt and decrypt the data in individual algorithms such as AES, ECC and RSA. From Table 1, it can be seen that RSA takes lowest time for cryptography process than AES and ECC.

Table 1: Comparison of Data Execution Time for individual cryptographic schemes

Message Length (Bits)	**Encoding-Decoding Time (seconds)**		
	AES	**ECC**	**RSA**
48	19.51	11.55	0.2306
64	28.46	15.48	0.2350
80	37.37	23.03	0.3184
96	42.97	35.19	0.3518
128	48.72	41.22	0.4261

Table 2: Comparison of Data Execution Time for proposed hybrid combinations V/s individual schemes

Message Length (Bits)	**Encoding-Decoding Time (seconds)**	
	Proposed Hybrid Combinations	
	AES-RSA	RSA-ECC
48	10.2493	8.3266
64	14.7360	14.8445
80	21.8297	17.1274
96	34.0297	21.6842

From Table 2, it can be concluded that the proposed hybrid scheme allows the user to encrypt data with hybrid algorithms that uses two strong encryption algorithms without taking more time for both encryption and decryption for various message lengths. The same results are illustrated in Fig. 3 and Fig. 4.

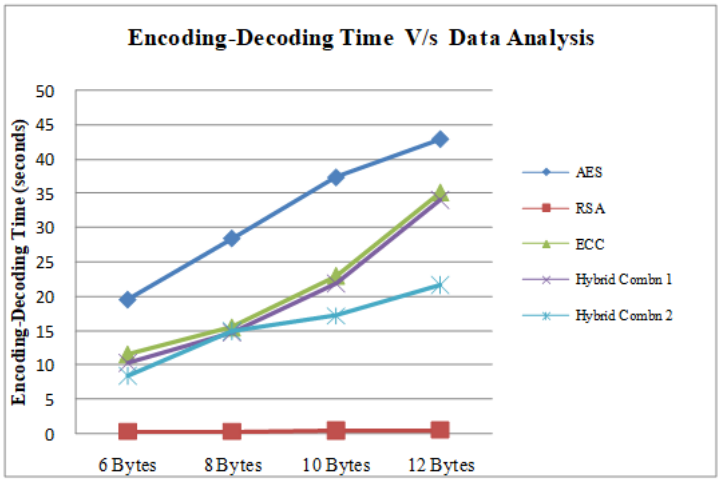

Fig.3. Plot of Encoding – Decoding time V/s Data Analysis

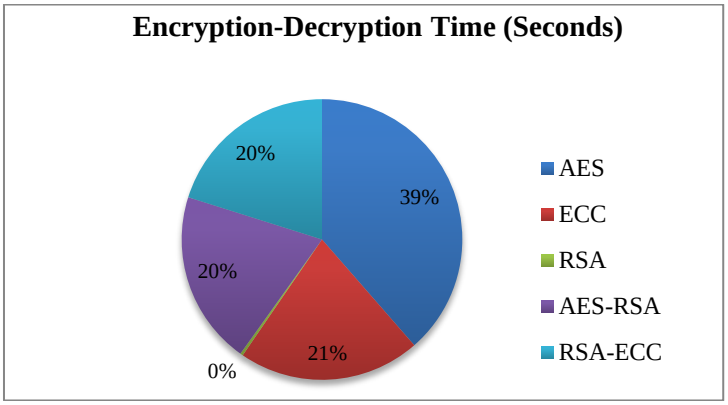

Fig.4.Percentage chart of Encoding-Decoding Time V/s various Cryptographic Schemes

Table 3: Key Length Ratio between RSA, DSA and ECC Cryptosystems in same security property [12]

Key length of (RSA/DSA)	Key length of ECC	Security Proportion
512	112	5:1
1024	160	7:1
2048	224	9:1
3072	256	12:1
7680	384	20:1

Table 3 shows the key length ratios between the cryptosystems in the same security proportions. It ensures that ECC offers better security than RSA/DSA at same security levels with different key sizes. ECC is highly complex algorithm to implement and if it is used with any other cryptographic schemes, to form hybrid system, then that hybrid scheme will be considered as highly robust and secure one.

B. Throughput:

The Throughput is based on the Encryption and Decryption time that indicate the communication speed of an encryption scheme. It is standardized as:

$$\text{Throughput} = \left(T_P(E_t + D_t)\right) * 100 \qquad (1)$$

where,

- T_p Entire plain text (Bytes)
- E_t and D_t Encryption-Decryption Time (seconds)

Table 4: Throughput of Hybrid Combination V/s Message lengths

Message Length (Bytes)	Throughput (%)		
	AES-RSA	AES-ECC	RSA-ECC
6	58.54	12.37	72.58
8	54.29	12.99	53.89
10	45.81	14.76	58.38
12	35.26	16.30	55.34
16	29.83	19.86	63.10

From Table 4, it is seen that hybrid Combination RSA-ECC offers highest throughput 56% compared to AES-RSA as well as AES-ECC combinations amongst the used three hybrid combinations with various message lengths. The same is entailed in Fig. 5 and Fig.6.

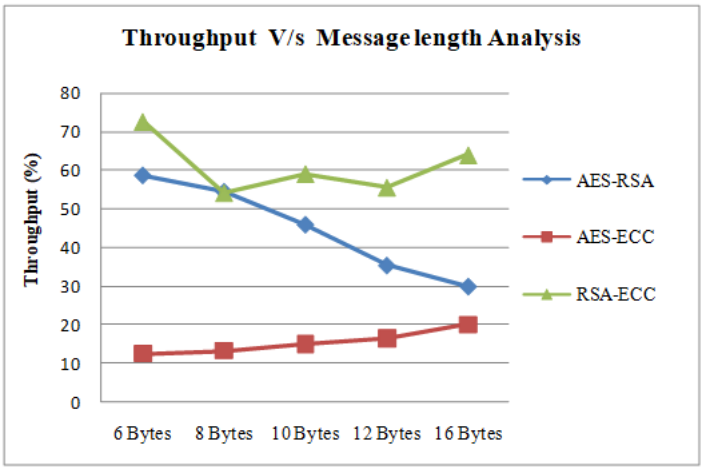

Fig.5. Plot of Throughput V/s Message lengths for Hybrid Combinations

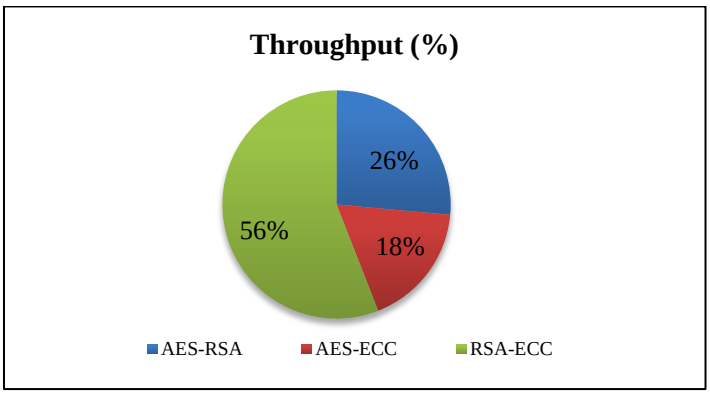

Fig.6.Percentage Chart of Throughput for Hybrid Combinations

C. Memory Consumption:

The memory consumed is the main memory required to process encryption algorithms.

Table 5: Memory Consumed for Individual schemes & Hybrid Combinations

Memory Consumed by Encryption Schemes (K-Bytes)					
Individual Schemes			**Hybrid Combinations**		
AES	ECC	RSA	AES-RSA	AES-ECC	RSA-ECC
6.75	2.17	0.20	6.908	8.916	2.372

Table 5 shows the memory consumption of Wireless network after implementing the proposed hybrid model and the existing model. The same is depicted by Fig. 7. Although memory consumed by hybrid combinations are more compared to individual encryption schemes but in terms of assuring security, hybrid combinations stand at top because of the use of two cryptographic schemes and hashing, prevailing to preservation and confidentiality of original message.

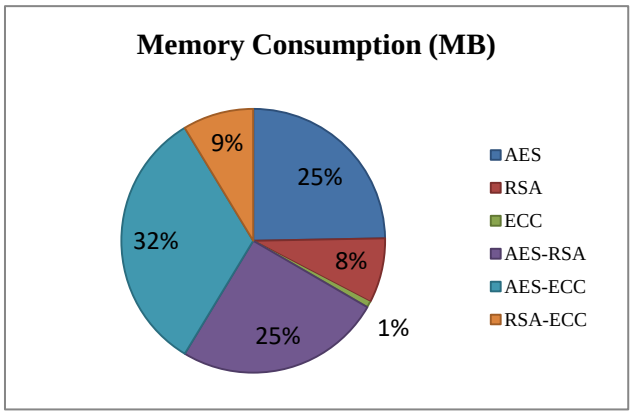

Fig.7.Percentage chart of Memory Consumed by Various Cryptographic Schemes

Conclusion

In this paper, a robust hybrid scheme for secure routing and data transmission in Wireless Networks is presented. It is specifically designed to solve the issues related to practical implications like efficient computation (i.e., overall Throughput), short response time (i.e., encryption-decryption time), and the strength (i.e., key length security proportions) of cryptographic algorithms. Conventional algorithms were easily cracked and have an easy way to encipher and they can be used in very efficient way if they are combined to form a hybrid scheme. Our proposed hybrid system tries to trap the intruder through two security levels such as encryption-decryption and hashing. Preservation of the original text is assured by Hashing whereas confidentiality is assured by Cryptographic algorithms (hybrid combinations). Additionally, hybrid system offers enhanced security with shorter encryption-decryption time and highest throughput. Out of the three proposed hybrid combinations RSA-ECC combination with hashing works efficiently since it has shorter response time, highest throughput and consumes less memory for the implementation.

References

[1] Dr. Vivek Kapoor, Rahul Yadav, A Hybrid Cryptography Technique to support Cyber Security Infrastructure, International Journal of Advanced Research in Computer Engineering and Technology,2015; Volume 4,Issue 11.

[2] Singh, G., Supriya, A study of encryption algorithms (RSA, DES, 3DES and AES) for information security, International Journal on Computer Applications, 2013; Volume 67,Issue 19.

[3] Burr, W., Selecting the advanced encryption standard, IEEE, 2003.

[4] Frunza, M., Asachi, Gh., Improved RSA encryption algorithm for increased security of wireless networks, International Symposium, 2007.

[5] Kodali, R., Sarma, N., Energy efficient ECC encryption using ECD, Emerging Research in Electronics, Computer Science and Technology, Springer, 2013; pp. 471–478.

[6] Susarla, S. and Borkar, G., Hybrid Encryption System.

[7] Wang Wei-hong, Lin Yu-bing, Chen Tie-ming, The Study and Application of Elliptic Curve Cryptography Library on Wireless Sensor Network, IEEE, 2008.
[8] Zuhi, S., Satish, D, Hybrid Cryptography Approach for securing MANETs-A Survey, IJIRCCE,2018.
[9] Sharma, A., Bhuriya, D. and Singh, U.,Secure data transmission on MANET by hybrid cryptography technique. In Computer, Communication and Control (IC4), IEEE, 2015; International Conference on (pp. 1-6).
[10] Rani, S. and Kaur, H., Implementation and comparison of hybrid encryption model for secure network using AES and Elgamal. International Journal, 2017;8(3).
[11] Jailin.S, Kayalvizhi.R, Vaidehi.V, Performance Analysis of Hybrid Cryptography for Secured Data Aggregation in Wireless Sensor Networks, IEEE, 2011.
[12] Harini, M., Gowri, K.P., Pavithra, C. and Selvarani, M.P., A novel security mechanism using hybrid cryptography algorithms. Electrical, Instrumentation and Communication Engineering (ICEICE), IEEE, 2017.
[13] Mykola Karpinskyy, Yaroslav Kinakh, Reliability of RSA Algorithm and its Computational Complexity, Computing, 2003;119-122.
[14] V Gampala, S Inuganti, S Muppidi, Data Security in Cloud Computing with Elliptic Curve Cryptography, International Journal of Soft Computing and Engineering (IJSCE),2012.
[15] Wiliam, S., Cryptography and Network Security, 2000.
[16] Rizk, R. and Alkady, Y., Two-phase hybrid cryptography algorithm for wireless sensor networks. Journal of Electrical Systems and Information Technology, 2015; 2(3), pp.296-313.

Authors' Profiles

Zuhi Subedar is working as an Assistant Professor in the Department of Electronics and Communication Engineering, Jain college of Engineering, Belagavi, Karnataka, India. She completed Bachelor of Engineering in Electronics and Communication. Then she worked in IT industry for 2 years. She completed M.Tech in Digital Communication Networking from Gogte Institute of Technology, Belagavi, Karnataka, India.

Ashwini Araballi is working as an Assistant Professor in the Department of Electronics and Communication Engineering, Jain college of Engineering, Belagavi, Karnataka, India. She completed her Bachelor of Engineering in Electronics and Communication. She completed M.Tech in Computer Networks Engineering from Visvesvaraya Technological University, Belagavi, Karnataka, India.

How to cite this paper: Zuhi Subedar, Ashwini Araballi. " Hybrid Cryptography: Performance Analysis of Various Cryptographic Combinations for Secure Communication ", International Journal of Mathematical Sciences and Computing (IJMSC), Vol.6, No.4, pp.35-41, 2020. DOI: 10.5815/ijMSC.2020.04.04