Hybrid Cryptography for Random-key Generation based on ECC Algorithm

P. Gayathri1, Syed Umar2, G. Sridevi3, N. Bashwanth4, Royyuru Srikanth5
1Department of Information Technology, GRIET, Hyderabad, India
2Department of Computer Science Engineering, MLRIT, Hyderabad, India
3Department of Computer Science Engineering, Malla Reddy Institute of Technology, Hyderabad, India
4Department of Information Technology, IARE, Hyderabad, India
5Department of Computer Science Engineering, K L University, Vaddeswaram, India

ABSTRACT
As more increase in usage of communications and developing them more user friendly. While developing those communications, we need to take care of security and safety of user’s data. Many researchers have developed many complex algorithms to maintain security in user’s application. Among those one of the best algorithms are cryptography based, in which user will be safe mostly from the attackers. We already had some AES algorithm which uses very complex cryptographic algorithm to increase the performance and more usage of lookup tables. So the cache timing attackers will correlates the details to encrypt the data under known key with the unknown key. So, for this we provide an improvised solution. This paper deals with an extension of public-key encryption and decryption support including a private key. The private key is generated with the combination of AES and ECC. In general AES, key length is 128 bits with 10 times of iterations. But with this, users won’t get efficient security for their operations, so to increase the security level we are implementing 196-bit based encryption with 12 times round-key generation iterations. By this enhancement, we can assure to users to high level security and can keep users data in confidential way.

Keyword: AES, Crypto-system, EC cipher text, Public and private keys, Random-key

1. INTRODUCTION
For the protection and necessary development of electronic commerce and information security data. Cipher is a data protection technology can be important. AES Advanced Encryption Standard is a scoring system used widely to ensure that privacy is important and necessary. (AES), high performance, and if it is suitable for normal encrypt. Encryption is elliptical (preacher) important principle of encryption and signatures. The preacher and the process of AES and AES transfer encryption and preachers confused data communication [1].

1.1. AES block Description
AES block encryption and replacement of system or network changes. According to the length of the data block and all of the key requirements of the AES. Length: 128, 192, 256, a plurality of repeated cycles with 10, 12 and 14 with the environment used. AES has three main goals: environmental changes and the mainstream media. Each change is a combination of a plurality of linear and non-linear add round important events. AES process is shown in Figure 1.
Each turn consists of four phases:

a. **Sub-Bytes changes**: In operation, the box will change with each measure of all measures of the line. Preparation of S-boxes, such as a GF measures Explosion ($2^8$), the changes applied to akin TR2.

b. **Shift Row Changes**: the market is not changing is the first measure of the country. The update cycle of the second set, the third, fourth and fifth from the left, one, two, three or four bytes respectively[2].

c. **Mix-Columns changes**: In the measurement in each column of the matrix solution in many equations in one place. Consequently, the position of the encrypted data, even if modified bytes. changes no-go corporate structure in the second column of parameterization.

d. **Add-Round Key Transformation**: In this version, the XOR is the other bit round-key (OR). work with columns at once. Even talking about conditions of round-key ground. The work was carried out through the last bit AES matrix2.

The channels so that the attention of breaking the encryption cryptanalysis killed instantly, but are weak. You can stick the channel page information data and time from a variety of options, statistics, energy conservation, and many other eye-AES appear well in this regard. Since the containers are stored, the encrypted cache or physically harmful, change the long-term encryption settings and how to insert text and encryption [3]. Side channel based on a comparison between the information provided in the sewer system and confidential information from falling into two main responses:

a. Reduction of files to prevent, or unnecessary duplication of information

b. The development of relations between the discharge documents and confidential information, confidential information that could be made, or unencrypted text databases randomly directly related to the change, so that back when the finished decoding (AES), high performance, and if it is suitable for normal encrypt. Encryption is elliptical (preacher) important principle of encryption and signatures. Description of the preacher and the mix in this study AES and send the Data [3] encrypted communication.

### 1.2. Cons and Pros of AES Cryptography

Inputs and outputs the data encrypted in the configuration data information that can be used to stop the channel, because they endanger the safety of some co-systems [4] added. The motivation of this work is to develop sufficient to reduce the approach to the problem of information security algorithms are vulnerable to attacks such solution, the hybrid encryption algorithm that tries to resolve the security and communications solution.

a. If the AES encryption key and Ecclesiastes communication, there is no reason, a secret key before sending the communication.

b. The secret is the only way out for each other, the only requirement is that the secret encryption management.

Work is a hybrid encryption algorithm, which is a member of encryption systems Advanced Encryption Standard (AES) and Elliptic Curve and encrypts the cipher-text and advanced security agents Security [5]. The study concentrates on the other monitoring and deposit attack for their actions. The model is to provide a server data security environment. Growth and time encryption to encrypt all data that will continue only AES encryption key Preacher elaborate security. Time to time information involve known details of the encryption key channel to reflect on the strange principles. Measures against side channel Wait efficiency [7] test.
2. PROPOSED METHOD HYBRID CRYPTOGRAPHY

AES symmetric encryption algorithm more lookup tables. The tables are encoded outside the result cache and cache error and the second time, the display of text encryption, decryption time changes. Re-cache and the key to the known data encryption and unknown values to a new level. For this work, and the AES, later ECC algorithm for text encryption algorithms used to prohibit the AES encryption and security software development for key security to the offense, for example, improve the parking time. The increasing efficiency is the highest form of data encryption and repeatedly with AES 192-bit key size, so that the circuit 12 in the first AES 128-bit standard active reading [10].

2.1. Proposed Model designing

To design the proposed model, which is a combination of AES and ECC Cryptography will be followed below steps

a. Initially the data block from where user can send data to encrypt for security issues and during the encryption section AES based encryption process is used. In which a dynamic security is issued during the encryption process only.

b. Then further after the AES key generation then it is encrypted with EC Cryptography and send to receiver, where the decryption process will be held.

c. During above process one dynamic key is generated and given to user for further decryption at the receiver side.

d. The total time is calculated for encryption process and will be stored at some memory storage for cross verifying with time taking for the decryption

e. At the receiver side decryption starts. In this process, AES key decryption and then data will be decrypted to original format of message sent by sender.

f. So, in general the module will be calculating the response time of encrypted data from the server/sender by generating various random keys including a valid key.

g. In the correlation program of the attacker module comparison of the timing details for both the cases is done and the possible key space per timing details which will be used to determine the correct key combination.

2.2. Analysis of AES & EC Cryptography

That begins with the pre-AES algorithm hybrid design should connect the two containers with the graphical user interface and analysis of model legislation and the comparative study of the hybrid engine ECC AES. This led to the creation of the AES encryption key. The execution of the transfer Preacher encryption keys and encrypted data and encryption key AES. The central blocks and key data encryption AES decryption. The relationship between the encoded number of errors of a few family members and decoded is not known on the process requirements analysis:

a. Length of Random key generated

b. Number of round-key & Algorithm

c. Maintenance of randomized keys

d. performance of attacker

3. EXPERIMENTAL & SIMULATION RESULTS.

The results are as follows in the book form of data encryption and 192-bit key used in the Advanced Encryption Standard. EU data is 12, replay AES export traffic.

3.1. Simulation Analysis

In Section 3.1, the user will be prompted to enter the value, the text document is encrypted with AES choose Figure 2, shows the block analysis at client side. In the Figure 3, explains the login page user where we can encrypt or decrypt the data. If the text of the most important, and the user clicks on the "encrypt" to begin the encryption of data. The results do not encrypt in general question number two AES cipher text. At the edge of the image as a good cooperation. The numbers 1-6 AES Effect encrypted number, text combinations of transport and traffic shows in Figure 4(a) and (4b). The other two AES encryption text of influence on the seventh-roundevening. The second image on the measures that AES-party collaboration. Uncoded text effects, from which seven twelve which is shown in Figure 5(a) and 5(b). Another AES and mix tags. Make the final phase of the AES Box Mix series no. The main dynamic encryption for the AES encryption method used, and the results should be controlled by user-defined code, need to change the rules.
Figure 2. Algorithm for Proposed System.

Figure 3. (a) Client side and (b) AES random key page
Hybrid Cryptography for Random-key Generation based on ECC Algorithm (P. Gayathri)
4. CONCLUSION:

In general AES is one of the best mechanism for the cryptography internally includes Symmetrical Encryption algorithm series. In SEA series utilizes a table look up, to increase the efficiency of performance. As those tables, doesn’t occupy total volume of the cache, so some faults arise during the encryption process like various lookup times and encrypting times. By this issue, cache time attacker correlates the time of encryption with known key to an unknown key. To overcome this issues during the encryption, an improvised version of AES algorithm is used to encrypt the plain text and ECC is introduced during the AES encryption process. So, thereby we can avoid attackers to steal/theft the data which are sending to the users. The advantages and future analysis can be explained in section 5.

5. USAGE AND FUTURE WORK.

By this type of encryption, users’ data can be saved in very confidential way. For an Example, as todays online payments are more using by everyone and became as one of the daily needs. In this process where payments can be done to buy or sell or any transaction should be more secure and should be more safe to all customers/users. During their payment transactions, these types of random key generated to encrypt the data will be known to user only. In future, this 192 bit Advanced AES Encryption is moved to 256 bit based AES algorithm.

REFERENCES.


