South Asian Journal of Engineering and Technology Research Article

Open Access Full Text Article 123(2022) 54-60 DOI: 10.26524/sajet.2022.12.38

Enhancement of 3-D Pythocrypt using AES Technique by generating the key using Chitra Kavya

Sumanth N[1] , Dr. Padmashree Anand[2], Shrinidhi Holla[3], Prof. Rakshatha S[4], Prajwal VS[5], Dr. Harshvardhan Tiwari[6]

[1]Dept. of ISE,Jyothy Institute of Technology,Bengaluru, India

[2]Ancient Science and Technology,Center for Incubation, Innovation, Research and consultancy(CIIRC) Bengaluru, India

[3]Dept. od ISE,Jyothy Institute of Technology,Bengaluru, India

[4]Asst. Professor, Dept. of ISE,Jyothy Institute of Technology,Bengaluru, India

[5]Dept. of ISE,Jyothy Institute of Technology,Bengaluru, India

[6]HOD, Dept. of ISE,Jyothy Institute of Technology,Bengaluru, India

Corresponding author.
Correspondence: Sumanth N
E-mail: padmashree.a@ciirc.jyothyit.ac.in

Article info

Received 2 th March 2022 Received in revised form 9 April 2022 Accepted 5 July 2022

Keywords

3-D Pythocrypt Algorithm, AES Technique, Symmetric Encryption, Decryption, Key generation, Chitra kavya, Cipher text, plain text.

Abstract

The research work describes an attempt to enhance the 3-D Pythocrypt algorithm using the AES Symmetric encryption technique by generating the key using an ancient approach of Chitra kavya. 3-D Pythocrypt is a new technique where we use the properties of 3-D geometric shapes to encrypt and decrypt plain text. AES encryption is a standard approach for encrypting and decrypting the message using a single key for both approaches. The ideology of this research is to first encrypt the plain text using the 3-D Pythocrypt technique and the cipher text obtained is fed as an input to the AES encryption technique along with the key generated using the Chitra kavya to carry out the encryption in two phases.

1. Introduction

The present web world is overwhelmed with a gigantic measure of information that is coming about information spillage and robbery of data. Bunches of difficulties emerge while moving or getting different sorts of encrypted information, messages, or data particularly utilizing public organizations. Digital wrongdoing is one of the greatest blemishes in this completely associated internetworking world. We present the strategy of enhancing 3-D Pythocrypt using the AES Symmetric encryption technique. 3-D Pythocrypt is a new technique, where the properties like area, volume, perimeter, etc. of specific 3-D geometric shapes are used to encrypt and decrypt the message which needs to be transmitted to attain confidentiality, AES Encryption technique is a traditional technique that uses the same key for both encryption and decryption. In this research, the key is generated using a different approach i.e., the Chitra kavya technique.

A.3-D Pythocrypt

There is a huge number of cryptographic systems which can be used to encrypt the message and transmit the cipher text that is generated so that the confidential information is made readable only by the intended user. Traditionally cryptographic systems are classified into two categories, Symmetric, and Asymmetric cryptographic systems. In Symmetric cryptographic systems, the same key is used for both encryption and decryption process, some of the popular symmetric techniques like the Caesar cipher model, play fair cipher model, and DES and AES Encryption model. The asymmetric cryptographic system uses different keys for encryption and decryption processes called public keys and private keys, the most popular and widely used asymmetric algorithm is RSA.

3-D Pythocrypt is a new and young technique that is used to encrypt and decrypt a given message using a known 3-D geometric shape (Jois et al., 2015). This methodology uses the geometric attributes of shapes such as

Area, Volume, Perimeter, etc., to generate an algorithm using which the plain text can be encoded into non-decipherable text. This new approach is unique compared to all other existing algorithms as it does not need a key for encryption but generates one for decryption [1].

B. AES Symmetric Encryption Technique

Advanced Encryption Standard is a symmetric encryption technique i.e., it uses the same key for both encryption and decryption process. The key needs to be kept secret for the algorithm to be secure. AES algorithm can be implemented using different key lengths i.e., AES-128 which uses a key of length 128 bits, AES-192 where the length of the key is 192 bits, and AES-256 where the key length is 256 bits (key length is 32 digits) [2]. It uses substitution and permutation techniques to encrypt and decrypt the plain text[3].

C. Chitra Kavya

Sanskrit poetry encompasses a variety of forms and structures which include Mahākāvya, Laghukāvya, Khandakāvya, Campukāvya, Gītikāvya, Muktakas, Stotras, Biographical Poems, Citrakāvya, etc. Citrakāvya is a wonderful class of poetry based on the intricate and innovative play of vowels, consonants, words, and sounds. Citrakāvya has a figurative quality wherein the elements of the verses are picturesquely patterned into designs resembling objects (bandhas) or their movements (gati) such as flower, wheel, flag, drum, etc. Also, the term Citra connotes an image or picture, uniqueness (vicitra), or wonder. Chitrakāvya is interpreted as 'image poetry' or 'marvel poetry' which embraces all ingenious forms of poetic compositions.

Ākaracitra and *Bandhacitra* are techniques by employing which verses can be designed and woven into various patterns of objects, animals, birds, etc. There are more than 200 known varieties of Bandhas. These include 12 types of *Nāga-bandha* of single or multiple coiled or uncoiled snakes; 19 types of *Āyudhas*, weapons such as sword, knife, mace, and others; 16 types of *Ābharaṇa-Chitra's* resembling ornaments such as bangle, armlet, girdle, etc; and 38 types of miscellaneous formations - *Anya-Ākāra-Citra:* those resembling umbrella (chatrabandha), banner or flag (*patākabandha*), mace (*gadābandha*) bow (dhanurbandha; Figure 2) in addition to sun, moon, Meru, bed, swing, lamp, pestle, bell and so on. Fig. 1 is the parashu bandha, in which the letters of the verse is placed in a particular sequence. We can decrypt the verse (shloka) only when the traversing pattern is known.

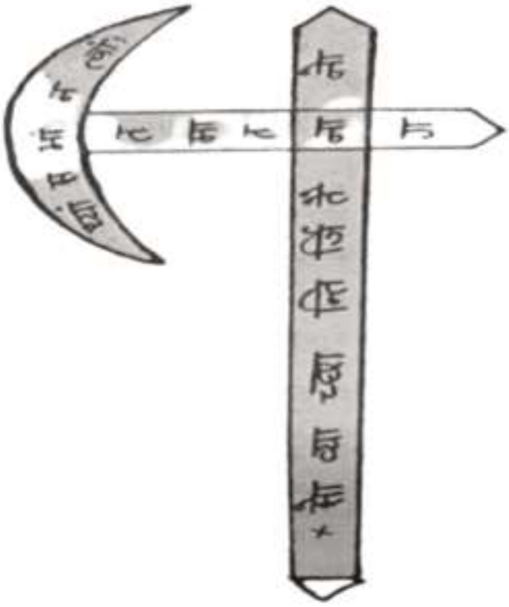

Fig. 1. Parashu Bandha

II. Proposed System

The system combines the two different techniques i.e., 3-D Pythocrypt and AES Symmetric algorithm to form a complex system that has two layers of encryption to provide better security against cryptanalysis. The plain text is converted to cipher text using the young cryptographic technique called 3-D Pythocrypt algorithm. The cipher text obtained from this process is passed to the AES encryption technique along with the key generated by the Chitra kavya technique, the output of this AES technique is used for transmission or storing the data.

III. Algorithm

A. *Encryption Phase*

1) 3-D Pythocrypt Encryption: The 3-D Pythocrypt algorithm is based on the properties of 3-D geometric shapes. This algorithm takes the properties like Area, Volume, etc. of the shapes. The message which consists of English alphabets and/or symbols is converted to its ASCII equivalent values which are in decimal format. These numbers are halved and considered as inputs to the formulae to calculate the ciphertext. In our research work, we have used different 3-D shapes to make the algorithm more secure. Whenever a user inputs a plain text, its corresponding ASCII value is generated. The entire ASCII value is halved. There are two variables in the formula namely 'a' and 'h'. The halved ASCII values are the inputs for these variables. For a particular plain text, a shape is chosen and the encryption operation is performed. The result is the cipher text obtained from the 3-D Pythocrypt encryption phase. Along with the cipher text, any one value of the variable 'a', 'a2', or 'h' can be used as the key. Table 1. Contains the different 3-D geometric shapes with their respective volumetric formula. Whenever the user inputs a new plain text, a particular shape and formula from Table 1. is chosen and is used for the encryption process. Id column in Table 1. Contains the id's assigned to the shapes which will help us to communicate the shape used at encryption to the receiver.

TABLE 1. DIFFERENT 3-D SHAPES AND THEIR CORRESPONDING VOLUMETRIC FORMULA.

Id	Shape	Volumetric Formula
1	Octahedron	$v = (2 * a^2 * h)/3$
2	Hexagonal Prism	$v = (3 *\surd 3 * a^2 * h) / 3$
3	Pentagonal Prism	$v = (\surd(5(5+2\surd 5)) * a^2 * h) / 4$
4	Octagonal Prism	$v = 2 * (1 + \surd 2) * a^2 * h$
5	Pentagonal Pyramid	$(5 * \tan(54^o) * h * a^2)/12$

2) AES Encryption Algorithm: The cipher text generated above along with the key needs to be transmitted to the receiver end. To enhance the security of the 3-D Pythocrypt algorithm, we encrypt the cipher text and the key using the AES symmetric encryption technique. However, the cipher text and the key needs to be combined using a delimiter. Here we use '.' as the delimiter hence, the actual cipher text from the 3-D Pythocrypt algorithm will be like [Output_of_algorithm.key] ex: 12345.5678. This together is passed as the input for the AES encryption algorithm.

3) Key Generation for AES Encryption: AES is a symmetric encryption technique which means it uses the same key for both encryption and decryption purposes. For generating the key for the AES encryption phase, we introduce a different technique called the Chitra kavya technique. As mentioned earlier, Chitra kavya contains different designs (bandha) where the verse (shloka) is encrypted in those designs. If we traverse those designs (bandha) in a particular order we can decrypt the verse(shloka/message). Here we construct a 21 x 21 matrix (dimension is not fixed, it can be altered) in which the elements are an orderly arrangement of numbers from 0 to 9 (as shown in Fig. 2.).

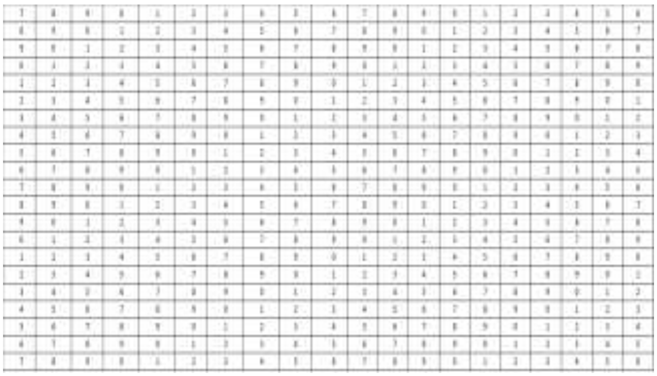

Fig. 2. A Sample 21 x 21 matrix

A dynamic seed point is obtained as the initial node and the matrix is traversed in a specific order such that the path forms the chosen design. In this research work, we have considered ***parashu bandha(design).*** We consider element 2 (5,13) (5th row and 13th column) as the seeding point. From this initial node, we traverse through the matrix in such a way that the path from the parashu bandha (Fig. 3.)

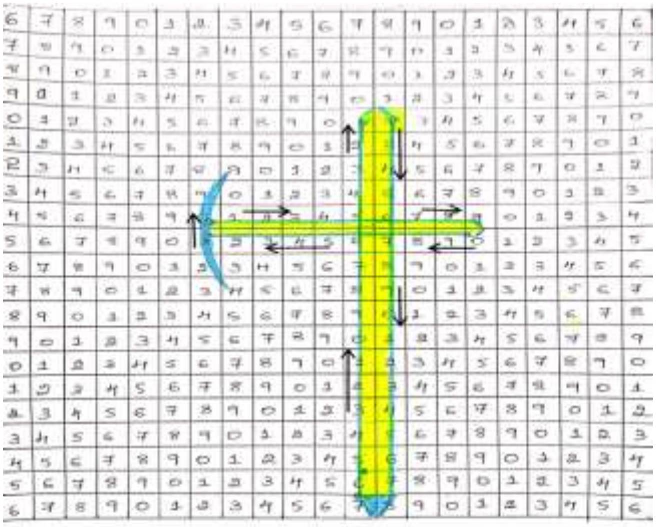

Fig. 3. Traversing the matrix to form parashu bandha(design).

The values encountered while traversing is taken as the key for the AES symmetric encryption algorithm. From fig. 3, we generate the key as 2345678909878901234567876543210987654321249990123454321. But, for the AES encryption, we only need a 256-bit key. Hence, we consider only the first 32 digits of the above-generated value as the secret key for the encryption and decryption process.

The output of the AES encryption algorithm is transmitted to the receiver.

B. *Decryption Phase*

On the receiver side, the received message(data) is first decrypted using the AES Symmetric decryption technique. The result of this is the cipher text obtained from the 3-D Pythocrypt algorithm which is decrypted to get the original plain text.

a) AES Decryption Algorithm: The encrypted cipher text of the 3-D Pythocrypt algorithm along with the seeding point used in generating the key is fed as an input to the AES Decryption algorithm. Using this seed point, the key is generated at the receiver side. Hence, the key is not transmitted from the sender to the receiver however, some knowledge about the key generation (matrix dimension, the design(bandha) used for encryption) should be known to the receiver. Using the key and the message received, the cipher text obtained from the 3-D Pythocrypt encryption technique is recovered.

b) 3-D Pythocrypt Decryption: All the information that is required to decrypt the cipher text (geometric shape used, key) is embedded in the cipher text. The key is extracted from the cipher text using the delimiter. Here the delimiter is '.'. As mentioned earlier, any one value of variables 'a', 'a2', or 'h' can be used as the key. The decryption formula changes accordingly. If we use 'a' or 'a2' as the key then, we need to find 'h'. However, if we use ‘h’ as the key then, we need to find the value of ‘a’. Table 2. Describes the different equations that need to be used to calculate the unknown value.

TABLE 2. 3-D PYTHOCRYPT DECRYPTION FORMULAE LIST.

Id	Shape	Decryption Formula		
		if key = a	If key = a^2	If key = h
1	Octahedron	$a^2 = (a * a)$ $h = (3 * v)/(2 * a^2)$	$h = (3 * v)/(2 * a^2)$	$a^2 = (3 * v)/(2 * h)$ $a = \sqrt{a^2}$
2	Hexagonal Prism	$a^2 = (a * a)$ $h = (2 * v)/(3 * \sqrt{3} * a^2)$	$h = (2 * v)/(3 * \sqrt{3} * a^2)$	$a^2 = (2 * v)/(3 * \sqrt{3} * h)$ $a = \sqrt{a^2}$
3	Pentagonal Prism	$a^2 = (a * a)$ $h = (4 * v)/\sqrt{(5(5+2\sqrt{5}))} * a^2$	$h = (4 * v)/\sqrt{(5(5+2\sqrt{5}))} * a^2$	$a^2 = (4 * v)/\sqrt{(5(5+2\sqrt{5}))} * h$ $a = \sqrt{a^2}$
4	Octagonal Prism	$a^2 = (a * a)$ $h = v /((2 * (1 + \sqrt{2}) * a^2)$	$h = v /((2 * (1 + \sqrt{2}) * a^2)$	$a^2 = v /((2 * (1 + \sqrt{2}) * h)$ $a = \sqrt{a^2}$
5	Pentagonal Pyramid	$a^2 = (a * a)$ $h = (12 * v)/(5 * \tan(54^0) * a^2)$	$h = (12 * v)/(5 * \tan(54^0) * a^2)$	$a^2 = (12 * v)/(5 * \tan(54^0) * h)$ $a = \sqrt{a^2}$

Once ‘a’ and ‘h’ values are successfully retrieved, these two are combined to form the ASCII values of the original plain text. Eventually, the original plain text is extracted from its ASCII values.

IV. IMPLEMENTATION

The design of the system contains two parts, the 3-D Pythocrypt and AES Symmetric algorithm. The message which needs to be encrypted is fed as an input to the 3-D Pythocrypt algorithm. The Pythocrypt algorithm converts this message to the ciphertext which is difficult to understand and also the key is generated. This will be in decimal format. The generated ciphertext (encrypted message. key) is fed as input to the AES encryption algorithm, which encrypts the cipher text by substitutions and permutations using the key generated using the Chitra kavya technique.

The decryption phase is the reverse of the encryption phase. The encrypted message from the AES encryption algorithm is passed to the AES decryption algorithm to retrieve the cipher text. This cipher text is passed to the 3-D Pythocrypt decryption algorithm to get the original plain text. Fig. 4 is the pictorial representation of the flow of data (plain text) from the sender to the receiver.

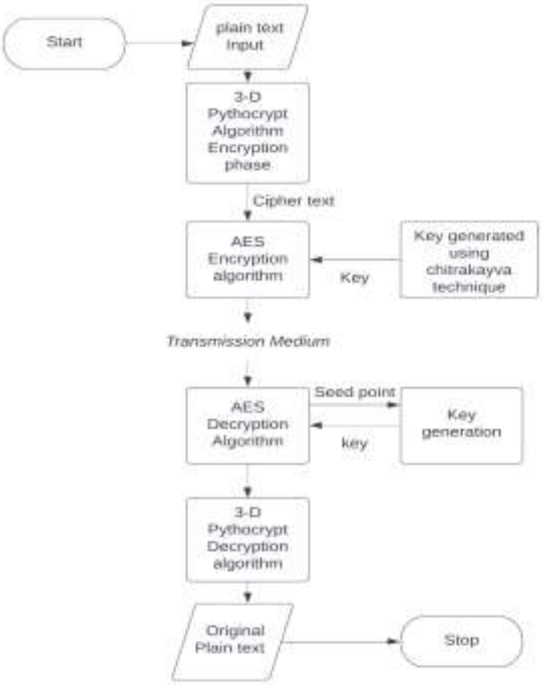

Fig. 4. A Flowchart that describes the entire process.

V. RESULT

- The plain text can be a sequence of any character which has equivalent ASCII values.

- For example: Let the plain text be, “**Hello, this is a sample message**”.
- This sample plain text is 31 characters long, and its equivalent ASCII value will be 7210110810811144321161041051153210511532973211597109112108101321091011151159710310 1.
- When this plain text is encrypted using the volume of octahedron geometric shape, the corresponding cipher text obtained from the 3-D Pythocrypt algorithm will be, 3111304744736150782528738910936595872899039332622006415139496188986641599339538648807370003023455726307917018973556705970120 73.32115971091121081013210910111511597103101 0
- Note that the dot (“.”) operator is used as the delimiter between cipher text and the key. Both cipher text and the key will be sent to the AES Encryption algorithm.
- From Fig. 3. the key for AES encryption can be 23456789098789012345678765432109876543212499901234543 21, However, for the AES encryption 256-bit (32 digits) key is sufficient. Hence, we consider only the first 32 digits of the above-generated key (23456789098789012345678765432109).
- The cipher text and the 32-digit key are passed as the input to the AES Encryption algorithm, the final encrypted cipher text will be, uqXRqTULcMqYKwOiyaZnxwfDXMIC89lsmnyTt3orjH+WlfsQp0jlEMFU3CRGZbcv5VkeK0f9E5iANZ+od1hWbxhu9nkX/VagEeSdEgDXQt0khvPv3U12+nWNdr3TPE38V+hd/j/Jv9bUn8aKf92aID+5bcxWCpbK7QBNU13LtW9bQN0OhWz4UVTv+HrzVzgbNy0F4g7evOBdxfI4VMqMNW7Wo8uAUTQ4OuT0puPxfms=
- This message is transmitted to the receiver, along with the information about the seeding point to generate the key at the receiver.
- The original plain text is obtained at the receiver side by reversing the encryption process.
-

VI. Conclusion

- The 3-D Pythocrypt algorithm is a new and young technique and is infeasible for many cryptographic attacks.
- Only some part of the numerical values can be obtained and also it is infeasible to find the original plain text by observing the pattern of ciphertext.
- Implementing the 3-D Pythocrypt algorithm along with the AES Encryption algorithm provides better security than many existing cryptographic systems.
- Generating keys using Chitra kavya is a new and powerful technique and it can be used in any scenario where dynamic key generation is required.

VII. Acknowledgment

We are immensely grateful to Ancient Science and Technology - Center for Incubation, Innovation, Research and Consultancy (CIIRC) and Jyothy Institute of Technology for their encouragement and pearls of wisdom shared during this research.

References

1. H. S. Jois, N. Bhaskar, and M. N. Shesha Prakash, “A 3-d advancement of PythoCrypt for any file type,” *Journal of Open Innovation: Technology, Market, and Complexity*, vol. 1, no. 2, Dec. 2015, DOI: 10.1186/s40852-015-0022-8.
2. D. Yehya and M. Joudi, “AES Encryption: Study & Evaluation Operating Systems View project Logic Design View project.” [Online]. Available: https://www.researchgate.net/publication/346446212

3. Muhammad Abdullah and A. Muhamad Abdullah, "Advanced Encryption Standard (AES) Algorithm to Encrypt and Decrypt Data Application of Petri Nets in Computer Networks View project Call for papers View project Advanced Encryption Standard (AES) Algorithm to Encrypt and Decrypt Data," 2017. [Online]. Available: https://www.researchgate.net/publication/317615794

4. *Karthikeyan, K. Alhaf Malik, D. Bujji Babbu, K. Nithya, S. Jafar Ali Ibrahim, N. S. Kalyan Chakravarthy (2021) "Survey of Cooperative Routing Algorithms in Wireless Sensor Networks", Annals of the Romanian Society for Cell Biology, pp. 5316–5320. Available at: https://www.annalsofrscb.ro/index.php/journal/article/view/702*

5. Jafar Ali Ibrahim. S, Mohamed Affir. A "Effective Scheduling of Jobs Using Reallocation of Resources Along With Best Fit Strategy and Priority", International Journal of Science Engineering and Advanced Technology(IJSEAT) – ISSN No: 2321- 6905, Vol.2, Issue.2, Feb-2014, http://www.ijseat.com/index.php/ijseat/article/view/62