REPORT
for

Chaos-based-AES-cryptosystem

Version 1.0
Prepared by :

1. Dhruv Choksi (202001049)
2. Kandarp Devmurari (202001052)
3. Pranav Patil (202001055)
4. Krupal Shah (202001057)
5. Vihar Shah (202001110)

Submitted to :
Prof. Manish Gupta

May 1, 2023

Contents

1 Introduction

Cryptographic systems are essential for secure communication and data storage. The AES (Advanced Encryption Standard) is a widely used cryptographic algorithm that relies on a secret key to encrypt and decrypt messages. However, the security of AES has been challenged due to the possibility of side-channel attacks that can extract the secret key by analyzing the physical characteristics of the encryption process.

In recent years, researchers have explored the use of chaotic systems in cryptography, as they can produce random and unpredictable results that can enhance the security of cryptographic algorithms. One such chaotic system is the double pendulum, a simple mechanical system that exhibits chaotic behavior due to its sensitivity to initial conditions.

In this paper, we propose a new cryptosystem that utilizes the chaotic motion of a double pendulum to generate secret keys for AES. We present two versions of our proposed system. In the first version, we generate a master key from the chaotic motion of the double pendulum and then use it to generate all round keys for the AES algorithm. In the second version, we eliminate the need for a master key and directly generate all round keys using the random motion of the double pendulum.

Our proposed cryptosystem has several advantages over traditional AES. By utilizing the random and unpredictable motion of the double pendulum, our system can resist side-channel attacks that analyze the physical characteristics of the encryption process. Furthermore, our system's computational complexity is significantly higher than that of traditional AES, making it more difficult and time-consuming for an attacker to break the encryption. Overall, our proposed cryptosystem has the potential to provide better security and performance than traditional AES, making it a promising solution for secure communication and data storage.

2 Pre-requisites

2.1 Double Pendulum

The mathematical formulation of double pendulum is explained as follows:

$$x_1 = l_1 \sin \alpha_1 \tag{1}$$

$$x_2 = l_1 \sin \alpha_1 + l_2 \sin \alpha_2 \tag{2}$$

$$y_1 = -l_1 \cos \alpha_1 \tag{3}$$

$$y_2 = -l_1 \cos \alpha_1 - l_2 \cos \alpha_2 \tag{4}$$

where x1 and x2 are horizontal components and y1 and y2 are vertical components of masses m1 and m2 respectively. Now the potential energy P for case of double pendulum is given as

$$P = -m_1 g l_1 \cos \alpha_1 - m_2 g \left(l_1 \cos \alpha_1 + l_2 \cos \alpha_2\right) \tag{5}$$

And kinetic energy K is obtained by finding derivatives of Eqs. (1)–(4), we get

$$K = \frac{1}{2} m_1 \left(\dot{\alpha}_1^2 l_1^2\right) + \frac{1}{2} m_2 \left(\dot{\alpha}_1^2 l_1^2 + \dot{\alpha}_2^2 l_2^2 + 2\dot{\alpha}_1 l_1 \dot{\beta}_2 l_2 \cos\left(\alpha_1 - \alpha_2\right)\right) \tag{6}$$

The Langrangian (L) of a system is defined as the difference of kinetic energy and potential energy, which, for the case of a double pendulum is

$$L = \frac{1}{2}\left(m_1 + m_2\right) L_1^2 \dot{\alpha}_1^2 + \frac{1}{2} m_2 L_2^2 \dot{\alpha}_2^2 + m_2 L_1 L_2 \dot{\alpha}_1 \dot{\alpha}_2 \cos\left(\alpha_1 + \alpha_2\right) + \left(m_1 + m_2\right) g L_1 \cos \alpha_1 + m_2 g L_2 \cos \alpha_2 \tag{7}$$

Then,

$$\frac{\partial L}{\partial \alpha_1} = -L_1 g \left(m_1 + m_2\right) \sin \alpha_1 - m_2 L_1 L_2 \dot{\alpha}_1 \dot{\alpha}_2 \sin\left(\alpha_1 - \alpha_2\right) \tag{8}$$

$$\frac{\partial L}{\partial \dot{\alpha}_1} = \left(m_1 + m_2\right) L_1^2 \dot{\alpha}_1 + m_2 L_1 L_2 \dot{\alpha}_2 \cos\left(\alpha_1 - \alpha_2\right) \tag{9}$$

$$\frac{d}{dt}\left(\frac{\partial L}{\partial \dot{\alpha}_1}\right) = \left(m_1 + m_2\right) L_1^2 \ddot{\alpha}_1 + m_2 L_1 L_2 \ddot{\beta}_2 \cos\left(\alpha_1 - \alpha_2\right) - m_2 L_1 L_2 \ddot{\alpha}_2 \sin\left(\alpha_1 - \alpha_2\right)\left(\ddot{\alpha}_1 - \ddot{\alpha}_2\right) \tag{10}$$

Since Langrangian of a system satisfies the Euler-Langrange differential equation

$$\frac{d}{dt}\left(\frac{\partial L}{\partial \dot{\alpha}_1}\right) - \frac{\partial L}{\partial \alpha_1} = 0 \tag{11}$$

Substituting Eqs. (9) and (10) in above equation we get

$$(m_1 + m_2)\, L_1^2 \ddot{\alpha}_1 + m_2 L_1 L_2 \ddot{\beta}_2 \cos(\alpha_1 - \alpha_2) - m_2 L_1 L_2 \ddot{\alpha}_2^2 \sin(\alpha_1 - \alpha_2) + g L_1 (m_1 + m_2) \sin\alpha_1 = 0 \tag{12}$$

Extracting $\ddot{\alpha}_1$ from the above equ, we get:

$$\ddot{\alpha}_1 = \frac{-m_2 L_2 \ddot{\alpha}_2 \cos(\alpha_1 - \alpha_2) - m_2 L_2 \ddot{\alpha}_2^2 \sin(\varphi_1 - \varphi_2) - g\,(m_1 + m_2) \sin\alpha_1}{(m_1 + m_2)\, L_1} \tag{13}$$

Similarly, we can derive an equation using Euler–Langrange equation for $\ddot{\alpha}_2$, which is as follow

$$\ddot{\alpha}_2 = \frac{-L_1 \ddot{\alpha}_1 \cos(\alpha_1 - \alpha_2) - L_1 \ddot{\alpha}_1^2 \sin(\alpha_1 - \alpha_2) - g \sin\alpha_2}{L_2} \tag{14}$$

Solving above two equations simultaneously to derive the following differential equations

$$\ddot{\varphi}_1 = \frac{-m_2 L_1 \ddot{\varphi}_1^2 \sin(\alpha_1 - \alpha_2) \cos(\alpha_1 - \alpha_2) - m_2 L_2 \ddot{\alpha}_2^2 \sin(\alpha_1 - \alpha_2) + m_2 g sin(\alpha_2) \cos(\alpha_1 - \alpha_2) - g(m_1 + m_2) \sin\alpha_1}{(m_1 + m_2) L_1 - m_2 L_1 \cos^2(\alpha_1 - \alpha_2)}$$

$$\ddot{\varphi}_2 = \frac{m_2 L_2 \ddot{\varphi}_2^2 \sin(\varphi_1 - \varphi_2) \cos(\varphi_1 - \varphi_2) + L_1 \ddot{\varphi}_1^2 \sin(\varphi_1 - \varphi_2)(m_1 + m_2) + g sin(\varphi_1) \cos(\varphi_1 - \varphi_2)(m_1 + m_2) - g(m_1 + m_2) \sin\varphi_1}{(m_1 + m_2) L_2 - m_2 L_2 \cos^2(\varphi_1 - \varphi_2)}$$

Now replacing $\varphi_1, \varphi_2, \ddot{\varphi}_1, and \ddot{\varphi}_1$ by $\zeta_1, \zeta_2, \zeta_3, and \zeta_4$ respectively. Differentiation of these yields the following four first order differential equations after substituting $\ddot{\varphi}_1$ and $\ddot{\varphi}_2$:

$$\dot{\zeta}_1 = \ddot{\varphi}_1$$
$$\dot{\zeta}_2 = \ddot{\varphi}_2$$

$$\dot{\zeta}_3 = \frac{-m_2 L_1 \zeta_3^2 \sin(\zeta_1 - \zeta_2) \cos(\zeta_1 - \zeta_2) - m_2 L_2 \zeta_4^2 \sin(\zeta_1 - \zeta_2) + m_2 g sin(\zeta_2) \cos(\zeta_1 - \zeta_2) - g(m_1 + m_2) \sin\zeta_1}{(m_1 + m_2) L_1 - m_2 L_1 \cos^2(\zeta_1 - \zeta_2)}$$

$$\dot{\zeta}_4 = \frac{m_2 L_2 \zeta_4^2 \sin(\zeta_1 - \zeta_2) \cos(\zeta_1 - \zeta_2) + L_1 \zeta_4^2 \sin(\zeta_1 - \zeta_2)(m_1 + m_2) + g sin(\zeta_1) \cos(\zeta_1 - \zeta_2)(m_1 + m_2) - g(m_1 + m_2) \sin\zeta_2}{(m_1 + m_2) L_2 - m_2 L_2 \cos^2(\zeta_1 - \zeta_2)}$$

After solving this first-order differential equation, we get the values of both the angles, knowing which we get unique co-ordinates of (x1,y1) & (x2,y2)

3 Working

3.1 Chaos based AES encryption system version-1

The version-1 encryption system is based on the following steps:

1. **Options to encrypt text or image:** On the basis of the option the user chooses, the system first converts the text string to bytes or the image(in .png form) to bytes.

2. **Randomly generating initial conditions of the 2 bobs of the double pendulum:** The initial conditions of the double pendulum system like total time, total samples to generate, initial angular displacement of bob1 & bob2, initial angular velocity of bob1 & bob2, mass of bob1 & bob2, length of string of bob1 & bob2 and value of gravity are randomly generated within a certain limit. Then these conditions are stored in a file and given to the user which acts as a key while decrypting.

3. **Generation of samples from double pendulum simulation:** To get the sample values from which we will generate the masterkey for the AES encryption, we first have to generate the samples. For this, we pass arguments like total simulation time, total samples to generate, initial angular displacement of bob1 & bob2, initial angular velocity of bob1 & bob2, mass of bob1 & bob2, length of string of bob1 & bob2 and value of gravity to the double pendulum simulation function, which uses the equations defined in the **Double Pendulum section of Pre-requisites chapter** to produce sample values for the x positions of bob1 & bob2(x_1, x_2) and the y positions of bob1 & bob2(y_1, y_2) in the form of bytes.

4. **Generation of masterkey from the above generated sample values:** The above generated sample values of x_1, x_2, y_1, y_2 are concatenated to generate the masterkey of AES encryption.

5. **AES encryption:** On the basis of the option the user chooses either the text(string) or the image(pixel array) is encrypted into bytes. For image encryption we also add several headers like image dimensions, image mode, image extension to the data value before encryption, so this information can be used after decryption to regenerate the image with its proper dimensions and extension.

The version-1 decryption system is based on the following steps:

1. **Loading the initial state of the double pendulum system:** The initial conditions which were used to generate the masterkey while encrypting are loaded fron the file that is generated in the user's system when he/she encrypted the data.

2. **Generation of samples from double pendulum simulation & Generation of masterkey :**Same as in the encryption process

3. **AES decryption:** The encrypted data is decrypted using the masterkey which is generated from the samples of the double pendulum system whose initial conditions are loaded from the key which the user gets when he/she first encrypted the data. Thus, the masterkey for decryption is generated from initial conditions key that user gets after encryption.

4. **Regeneration of the original data:** After the data is decrypted, its headers are read which gives information about the data type; if its an image it also gives information about the dimensions, mode and extension of the image. This information is then used to regenerate the original data

Difference in version-2 system over version-1 are as follows:

1. **Generating n roundkeys directly instead of the masterkey:** Instead of generating a masterkey(256 bits) from the sample values of x_1, x_2, y_1, y_2, we directly generate the n round keys(128 bits) which will be used in AES encryption and decryption. For this we would need to generate more number of samples in the single double pendulum simulation.

2. **AES library used in version-1 v/s our own AES algorithm in version-2**

4 Improvements of our proposed cryptosystem

4.1 Version 1 v/s Version 2

In the second version of the cryptosystem using a double pendulum, rather than generating the master key from the chaotic motion of the pendulum, all individual round keys are generated directly from the highly random motion of the pendulum. This change in the key generation process has several potential advantages, one of which is increased security.

The random motion of the double pendulum creates a highly unpredictable and chaotic system, making it extremely difficult for an attacker to determine the initial conditions required to accurately simulate the pendulum's motion and generate the same sequence of round keys used in the encryption process. This significantly increases the time complexity required to break the cryptosystem.

In the new version, unless an attacker has access to all the initial conditions needed to run the exact simulation, they cannot generate the same sequence of round keys and decrypt the encrypted ciphertext. As a result, the security of the cryptosystem is improved, as the time and resources required to break it using brute force or other cryptographic attacks are increased exponentially.

However, it is worth noting that the increased security comes at the cost of increased computational complexity, as generating round keys from the highly random motion of the double pendulum may require more computation than generating them from a master key. Therefore, optimizing the new key generation process implementation is essential to ensure the system remains efficient and practical for real-world applications.

4.2 Performance metrics

The performance metrics that are likely to be affected by generating all round keys using the random motion of the double pendulum in the AES cryptosystem are as follows:

1. **Security:** The primary performance metric affected by this change is security. By using the highly random motion of the double pendulum to generate round keys, the cryptosystem becomes more secure as it becomes more difficult to predict the

key sequence required to decrypt the ciphertext. As a result, the system is more resistant to brute-force attacks and other cryptographic attacks.

2. **Computational Complexity:** Generating round keys using the random motion of the double pendulum may indeed require more computation compared to generating them from a master key. The computational complexity of the system can be assessed using metrics such as time complexity and space complexity.

   Efficient and optimized algorithms are crucial for generating round keys practically and feasibly. These algorithms should be designed to handle the complex calculations involved in simulating the motion of the double pendulum and deriving the random key sequences.

   In terms of computational complexity, the proposed double pendulum-based cryptosystem offers several advantages. By generating round keys through the random motion of the pendulum, the system introduces a higher level of randomness and unpredictability. This randomness makes it significantly more challenging for an attacker to break the encryption by attempting to predict the round keys.

   The computational complexity of the system is further increased due to the requirement of knowing the exact initial conditions of the pendulum to simulate the same motion and generate the same round keys. The chaotic nature of the double pendulum system ensures that even slight variations in the initial conditions can result in significantly different outcomes, adding an additional layer of complexity for an attacker.

   Comparatively, traditional AES systems generate round keys from a master key, which provides a more deterministic and predictable process. This predictability can potentially be exploited by attackers using brute-force or other cryptographic attacks.

   With the increased computational complexity introduced by the double pendulum-based cryptosystem, it becomes much more challenging and time-consuming for an attacker to launch a brute-force attack on the encryption key. The attacker would need to perform extensive computations and simulations to accurately reproduce the same key sequences as the original system.

   Overall, the double pendulum-based cryptosystem's increased computational complexity provides an additional level of security by making it more challenging for attackers to crack the encryption. Nonetheless, it is crucial to acknowledge that more research and scrutiny are required to assess completely the computational complexity and security implications of this method.

Breaking the traditional AES cryptosystem requires an enormous computational power of approximately 2^{256}. In the proposed double pendulum-based cryptosystem, assuming each round key is 128 bits long, we would require 2^{128} computational power for each round of encryption. If there are n rounds, we need 2^{n*128} computational power. For example, if we use 10 rounds, the traditional system would require still require 2^{256} computational power but the version-2 of our proposed system would require $2^{10*128} = 2^{1280} = 2^{5*256}$ computational power, which is equal to (computational power of traditional AES)^5. Therefore, we need exponentially more computational power to break out proposed cryptosystem as compared to the traditional AES.
This makes the proposed system much more resistant to brute-force attacks, as an attacker would need significantly more computational resources to break the encryption

3. **Efficiency:** Generating all round keys through the random motion of the double pendulum may affect the efficiency of the system. This metric can be measured using throughput, latency, and response time. An efficient algorithm for generating round keys can ensure that the system remains efficient and practical.

4. **Usability:** The usability of the system may also be affected by the change in the key generation process. Users may need to be trained on the new key generation process, and additional resources may be required to implement the new process. Therefore, usability metrics such as learnability and resource requirements may need to be considered.

Overall, the change in the key generation process is likely to improve the security of the AES cryptosystem while potentially increasing computational complexity and affecting efficiency and usability. Optimizing the new key generation process and conducting thorough testing is essential to ensure the system remains efficient, practical, and secure.

4.3 Version 2 v/s Traditional AES cryptosystem

The method of generating all round keys through the random motion of the double pendulum could offer some advantages over traditional AES systems. Here are some technical reasons:

1. **Increased randomness:** While traditional AES systems rely on a deterministic and predictable key sequence generated from a master key to generate round keys, utilizing the random motion of the double pendulum to generate round keys creates a highly unpredictable and random key sequence. This increased randomness can enhance the system's resistance to cryptographic attacks.

2. **Resistance to side-channel attacks:** Resistance to side-channel attacks is one of the potential advantages of using a double pendulum system to generate all round keys in AES. Traditional AES implementations can be vulnerable to side-channel attacks, which can be used to extract sensitive information such as secret keys. These attacks exploit weaknesses in the physical implementation of the system, such as power consumption or electromagnetic radiation, to extract information that can be used to compromise the system's security.

   In the case of a double pendulum system, the randomness of the generated key sequence can reduce the information leaked through side channels. Since the key sequence is not directly derived from the master key or any other predictable source, no pattern or correlation can be exploited to extract sensitive information. Additionally, using a physical system such as the double pendulum can make it more difficult for attackers to obtain the necessary information for a side-channel attack, as it may require more advanced equipment or techniques.

   Furthermore, a double pendulum system can offer other countermeasures against side-channel attacks, such as incorporating randomization or masking techniques. For example, the system could introduce minor variations or perturbations in the pendulum's motion to increase the randomness and reduce the amount of information leaked through side channels.

   Overall, the resistance to side-channel attacks offered by a double pendulum-based AES system is a potential advantage over traditional implementations, which can be vulnerable to these attacks. However, it is essential to note that this advantage is not guaranteed and that further research and testing are needed to evaluate the security of this approach against side-channel attacks fully.

3. **No need for a master key:** Traditional AES systems require a master key, which must be kept secret and secure. By eliminating the need for a master key, the system becomes simpler and potentially more secure, since there is no centralized point of failure.

4. **Potential for better scalability:** Since the key sequence is generated through a simulation, it may be easier to scale the system to support more users or larger amounts of data. This is because the system does not rely on a central master key that must be distributed securely to all users.

5. **Potential for better performance:** Generating round keys through the double pendulum's random motion may be faster and more efficient than traditional methods of generating round keys. This is because the double pendulum system can be implemented in hardware, which can be faster than software implementations used in traditional AES systems. Additionally, the highly random nature of

the key sequence generated through the double pendulum system may reduce the number of rounds needed to achieve the same level of security, which can result in faster encryption and decryption times.

5 References

1. Stachowiak, Tomasz, and Toshio Okada. ”A numerical analysis of chaos in the double pendulum.” Chaos, Solitons & Fractals 29.2 (2006): 417-422.

2. Shruthi, K. M., S. Sheela, and S. V. Sathyanarayana. ”Image encryption scheme with key sequences based on chaotic functions.” 2014 International Conference on Contemporary Computing and Informatics (IC3I). IEEE, 2014.

3. Liu, Shubo, Jing Sun, and Zhengquan Xu. ”An Improved Image Encryption Algorithm based on Chaotic System.” J. Comput. 4.11 (2009): 1091-1100.

4. https://link.springer.com/article/10.1007/s11277-020-07052-4