# ELLIPTICAL CURVE BASED HYBRID CRPTOGRAPHY SYSTEM

Gajawada Vishwas, Racharla Sai Chaitanya, Molugu Abhinav
Dept. Computer Science and Engineering
Anurag University, Hyderabad, Telangana, India.

**ABSTRACT-** As the digital continue to evolve, ensuring the confidentiality and integrity of sensitive information becomes paramount. So the main objective of the encryption is to secure and protect the data from unauthorized access and modification. In this paper the hybrid cryptography is being introduced to provide confidentiality and increase the security for the communications taking place over the internet. This paper also focuses on the Encryption and Decryption time alongside with the key-generation time. The hybrid cryptography introduced in this paper is the combination of the ECC(Elliptical Curve Cryptography) with Diffie Hellmen the two algorithms are the latest and are considered most secure ones. This research contributes to the advancement of hybrid encryption techniques and provides a practical solution for securing sensitive data in communication channels and storage systems.

***Keywords: -*** Diffie-Hellmen, Hybrid Cryptography, Elliptical Curve Cryptography, Key-Generation.

## INTRODUCTION

Cryptography, in its essence, is the science and art of securing communication and information through the use of codes and algorithms. Its primary objective is to protect the confidentiality, integrity, and authenticity of data in transit or at rest. In today's technologically advanced world, where information is constantly transmitted over networks, the importance of cryptography cannot be overstated.

The significance of cryptography has grown exponentially with the proliferation of digital technology and the internet. Advanced technology has made data communication faster and more efficient, but it has also introduced new vulnerabilities. Without proper encryption, sensitive information such as personal data, financial transactions, and confidential business communications could be intercepted and exploited by malicious actors.

There are two fundamental types of cryptography: symmetric and asymmetric cryptography. Symmetric cryptography, also known as secret-key cryptography, uses a single secret key for both encryption and decryption. This key must be kept confidential between the sender and receiver. While symmetric cryptography is efficient and fast, it faces a challenge when it comes to securely sharing the secret key between parties, as any compromise of the key can lead to the compromise of all encrypted data.

Asymmetric cryptography, on the other hand, uses a pair of keys: a public key for encryption and a private key for decryption. The public key can be freely shared, while the private key remains secret. This approach addresses the key distribution problem but can be computationally intensive. The security of asymmetric cryptography relies on the mathematical difficulty of certain problems, such as factoring large numbers.

However, both symmetric and asymmetric cryptography can be vulnerable to attacks if the keys are revealed to an intruder. In the case of symmetric cryptography, if the secret key falls into the wrong hands, all encrypted data can be decrypted. Asymmetric cryptography relies on the secrecy of the private key, and if it is compromised, an attacker can impersonate the key holder.

To address these vulnerabilities, cryptographic protocols like the Diffie-Hellman key exchange algorithm were introduced. Diffie-Hellman allows two parties to securely exchange encryption keys over an unsecured channel without directly transmitting the keys. While it provides a secure key exchange mechanism, human intervention in key management can still introduce risks.

To mitigate these risks, a more robust approach involves the integration of elliptic curve cryptography (ECC) into the hybrid system. ECC offers strong security with shorter key lengths, making it less susceptible to attacks. By combining the Diffie-Hellman key exchange with ECC, a highly secure and efficient hybrid cryptography system can be established, providing a robust defense against potential threats.

## LITERATURE REVIEW

[1]Nguyen Minh Trung, a researcher in Vietnam, has created two secure systems using complex math on Elliptic Curves for encrypting messages. These systems rely on the difficulty of solving a math problem, ensuring the security of information.

[2]Gupta suggested a new way to keep internet messages safe by mixing two methods called RSA and Diffie-Hellman. It's like having a secret code (RSA) to lock and unlock messages, and another method (Diffie-Hellman) to safely share the keys used for the code. This makes online communication more secure.

[3]A researcher named Hazra created a double-layered security method for hiding information in files, like text or images. They used special codes to lock the files, making it hard for anyone to peek inside. It's like having two secret layers – one to lock the file, and another to share a key for unlocking it securely. This helps keep sensitive information safe when sent over the internet.

[4]Vidhya proposed a new way to make computer codes safer by combining two existing methods called RSA and ECC. This new approach creates stronger codes that are more resistant to certain types of attacks. It's like having extra layers of protection for your digital information. Their experiments show that this new method works better and is faster than the older method (RSA) alone.

[5]Ermatita and others worked on a way to keep medical images safe by using two techniques: one for hiding the information (AES) and another for exchanging secret keys (Diffie-Hellman). This method helps protect sensitive medical data and ensures that only authorized people can access it. The results show it works well in keeping medical images secure.

[6]Avaestro combined two methods called Modified Diffie Hellman (MDH) and RSA. MDH makes sure the keys used for communication are exchanged safely, and RSA encrypts and decrypts messages. It's like sending secret letters – one person changes the way they write, and the other person knows how to read it. This makes it harder for someone else to understand the message. Their new method is faster and more secure than the old one.

[7]Yassien's project investigates the role of encryption algorithms in enhancing data security within cloud computing, comparing symmetric and asymmetric approaches. It highlights the trade-offs between performance and security, offering insights into the selection of encryption methods for specific cloud applications. The study underscores the importance of safeguarding data in the era of cloud-based services.

[8]Mahibel's proposed method focuses on enhancing the security of key exchange in public channels using Elliptic Curve Cryptography (ECC). It introduces a novel protocol that leverages the difficulty of the Elliptic Curve Discrete Logarithm Problem (ECDLP) to ensure secure and authentic key transport between two parties, mitigating the vulnerabilities associated with man-in-the-middle attacks in traditional Diffie-Hellman key exchange.

[9]Swapnil's project explores the critical importance of data security in the age of internet communication and provides an in-depth analysis of both symmetric and asymmetric cryptography techniques. The proposed architecture appears to be robust, emphasizing security and efficiency. However, successful implementation and user adherence will be key factors in its overall effectiveness.

[10]Sadiq's project highlights the growing significance of cloud computing for data storage due to its cost-effectiveness and convenience. However, it addresses the security concerns associated with data breaches in the cloud. The focus on hybrid cryptography as a solution is promising, but the paper identifies gaps in user authentication and algorithm implementation that need attention. Overall, it provides valuable insights into the challenges and solutions related to securing data in the cloud.

## PROPOSED METHOD

We came up with this Hybrid Cryptography which is a combination of the two cryptographic algorithms that are Elliptical Curve and Diffie-Hellmen which provide better security than the existing method. Here ECC is used for the generation of the public and the private variables as of RSA it has a large key size which lead to more storage and more time taking process so ECC is used to reduce both storage as well as the time.

Alongside with the ECC we are using the Diffie - Hellmen to produce a Shared key between both the parties in a most secure way possible. In this the Message/Data is Encrypted using the AES and the AES ‘iv’ is encrypted using the ECC based encryption.

A.Encryption Process

Step1:- Key Generation

ECC key pairs are generated for both parties, A and B.

Step2 :- Key Exchange

Party A's private key and Party B's public key are used to perform Diffie-Hellman key exchange, resulting in shared_key_A.

Party B's private key and Party A's public key are used to perform Diffie-Hellman key exchange, resulting in shared_key_B.

Step3:- Key Derivation

HKDF (HMAC Key Derivation Function) is used to derive symmetric keys (symmetric_key_A and symmetric_key_B) from shared_key_A and shared_key_B.

Step4:- Encryption

The user inputs plain text. An AES cipher in CFB (Cipher Feedback) mode is initialized with symmetric_key_A and an IV (Initialization Vector) of zeros.

The plain text is encrypted using the AES cipher, and the resulting ciphertext is printed.

B.Decryption Process

**Step1:-** Key Exchange (for Party B)

Party A's public key and Party B's private key are used to perform Diffie-Hellman key exchange, resulting in shared_key_B.

**Step2:-** Key Derivation (for Party B)

HKDF is used to derive the symmetric key (symmetric_key_B) from shared_key_B.

**Step3:-** Decryption

The encrypted data (ciphertext) is input.

An AES cipher in CFB mode is initialized with symmetric_key_B and the same IV used during encryption (zeros).

The ciphertext is decrypted using the AES cipher, and the resulting plaintext is printed.

REFERENCES

[1] Nguyen Minh Trung and Nguyen Binh , The 2014 International Conference on Advanced Technologies for Communications (ATC'14)

[2] Shilpi Gupta and Jaya Sharma , 2012 IEEE International Conference on Computational Intelligence and Computing Research

[3] Tapan Kumar Hazra, Anisha Mahato, Arghyadeep Mandal and Ajoy Kumar Chakraborty , 978-1-5386-2215-5/17/$31.00 ©2017 IEEE

[4] E.VIDHYA, S.SIVABALAN and R.RATHIPRIYA , Proceedings of the Fourth International Conference on Communication and Electronics Systems (ICCES 2019) IEEE Conference Record # 45898; IEEE Xplore ISBN: 978-1-7281-1261-9

[5] Ermatita , Yugo Bayu Prastyo and I Wayan Widi Pradnyana, 2020 International Conference on Informatics, Multimedia, Cyber and Information System (ICIMCIS)

[6] Junnel E Avaestro , Ariel M. Sison and Ruji P. Medina , "IEEE 4th International Conference on Technology, Informatics, Management, Engineering & Environment" (TIME-E) Bali, Indonesia, November 13-15, 2019

[7] Muneer Bani Yassein , Shadi Aljawarneh and Ethar Qawasmeh ,"The International Conference on Engineering & Technology" ICET2017, Antalya, Turkey

[8] Nissa Mehibel and M'hamed Hamadouche , "The 5th International Conference on Electrical Engineering – Boumerdes "(ICEE-B) October 29-31, 2017, Boumerdes, Algeria.

[9] Swapnil Chaudhari, "INTERNATIONAL JOURNAL FOR RESEARCH & DEVELOPMENT IN TECHNOLOGY", (2018) Volume-9,Issue-5(May-18) ISSN (O) :- 2349-3585

[10] Sadiq Aliyu Ahmad and Sadiq Aliyu Ahmad , 2019 15th International Conference on Electronics, Computer and Computation (ICECCO)

[11] Ugbedeojo Musa , Marion O. Adebiyi, Oyeranmi Adigun, Ayodele A. Adebiyi and Charity O. Aremu, 2023 International Conference on Science, Engineering and Business for Sustainable Development Goals (SEB-SDG)

[12] Hema Srivarshini Chilakala , N Preeti and Murali K , 2022 IEEE North Karnataka Subsection Flagship International Conference (NKCon)

[13] Harshit Sharma, Rakesh Kumar and Meenu Gupta , 2023 2nd International Conference for Innovation in Technology (INOCON) ,(3-5 March)