A Seminar on

Fortifying Security through Hybrid Cryptography

Team Details

1. Ch. Sree Charan(20EG105307)
2. P Pramod Reddy(20EG105335)
3. P Shiva Prasad(20EG105340)

Project Supervisor
Dr. T Shyam Prasad
Asst Professor

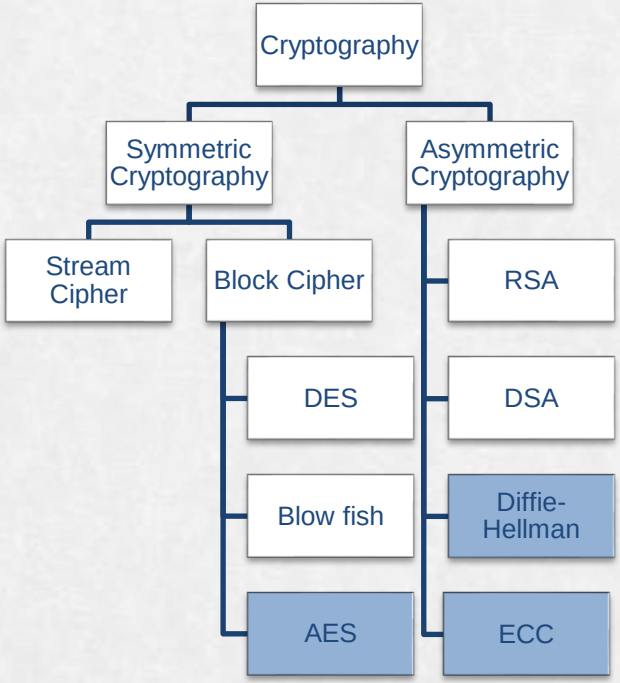
Introduction

Cryptography and Information Security: Hybrid of two algorithms ECC and Diffie-Hellman.

A hybrid algorithm that combines Elliptic Curve Cryptography (ECC) and the Diffie-Hellman key exchange can provide a secure way of key generation and exchanging process.

The ECC key exchange provides secrecy and protection against quantum attacks, while Diffie-Hellman offers a well-established method for secure key exchange.

Concept Tree



Literature

Author(s)	Strategies	Advantages	Disadvantages
V. Kapoor and Rahul Yadav	The study includes a comprehensive performance analysis, comparing the proposed technique with traditional RSA cryptography.	The bit discarding process contributes to efficient key generation, reducing key size while maintaining complexity. This enhances the overall efficiency of the encryption process.	The hybrid cryptographic technique may require a more complex implementation compared to single-algorithm approaches, potentially making it challenging to deploy and maintain.
Ali Kadhim Bermani, Tariq A. K. Murshedi & Zaid A. Abod	The focus on minimum key maintenance is a strategy to simplify the management of cryptographic keys while ensuring high security	The hybrid model combines the advantages of both symmetric and asymmetric encryption, offering a more robust security solution.	The use of multiple cryptographic algorithms and hashing may lead to increased resource consumption, particularly in terms of memory.
P. Gayathri1 , Syed Umar, G. Sridevi, N. Bashwanth, Royyuru Srikanth	The combination of AES (symmetric) and RSA (asymmetric) algorithms in the hybrid model allows for a balance between efficiency and key distribution complexities.	The hybrid model can be adapted for various types of data, making it versatile for different applications.	Managing keys for both symmetric and asymmetric algorithms, along with ensuring secure key exchange, can be challenging.

Literature(cont..)

selected strategy:

Author(s)	Method	Advantages	Disadvantages
Arpit Agarwal and Gunjan Patnakar	-RSA algorithm -Diffie-Hellman -SHA1	Scalability, Highly Efficienct, Secure key sharing.	Require technical expertise and users need to understand how to use encryption properly.
Prakash Kuppuswamy and Sayeed Q.Y. Al-khalidi Symmetric Key Algorithm - Linear Block Cipher Algorithm.	-Symmetric Key Algorithm - Linear Block Cipher Algorithm.	Better Performance, Enhanced Security, Resistance to Attacks.	Increased implementation challenges. Security of Key Exchange. Potential vulnerabilities
Dr.Vivek Kapoor and Rahul Yadav	-RSA algorithm -DES algorithm -SHA128	128-Bit Key Strength, Secure Data Transmission, Data Integrity.	Performance Impact and need high computational power.
Y Alkady, M. I. Habib and R. Y. Rizk	-RSA algorithm -ECC algorithm -MD5	better performance in terms of computation time and the size of cipher text.	High complexity , might need more resources.

Problem Statement

The collaboration of Diffie-Hellman serves as a reliable key exchange mechanism for RSA, where RSA ensures the security of the messages. Nevertheless, this approach involves extensive key lengths, significantly impacting the system's performance.

Existing Method:

Now-a-days , the exchange of sensitive information over the internet has become an integral part of our daily lives. Whether it's sending confidential emails, conducting financial transactions, or protecting personal data, ensuring the security and privacy of these communications is paramount. Two fundamental cryptographic algorithms, RSA and Diffie-Hellman, play crucial roles in safeguarding these digital interactions

Problem Statement

Disadvantage:

RSA and Diffie-Hellman are asymmetric encryption techniques that have revolutionized the way we protect data during transmission and establish secure channels for communication. These algorithms, each with its unique strengths and applications, have become the cornerstones of modern cryptography, enabling secure connections and safeguarding sensitive information against prying eyes.

Problem Illustration

The Hybrid scheme proposed is a combination of 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 (referred to as a shk) 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.

Problem Illustration

Key Generation:

- Alice generates a private key a = 123.
- Bob generates a private key b = 456.

Both compute their public keys:

- Alice: PA = a * G
- Bob: PB = b * G

Key Exchange:

- Alice calculates the shared secret SA = a * PB.
- Bob calculates the shared secret SB = b * PA.

Key Derivation:

Both parties derive symmetric keys using HKDF:

- Alice derives KA = HKDF(SA, SHA256, length=32, info='symmetric key').
- Bob derives KB = HKDF(SB, SHA256, length=32, info='symmetric key').

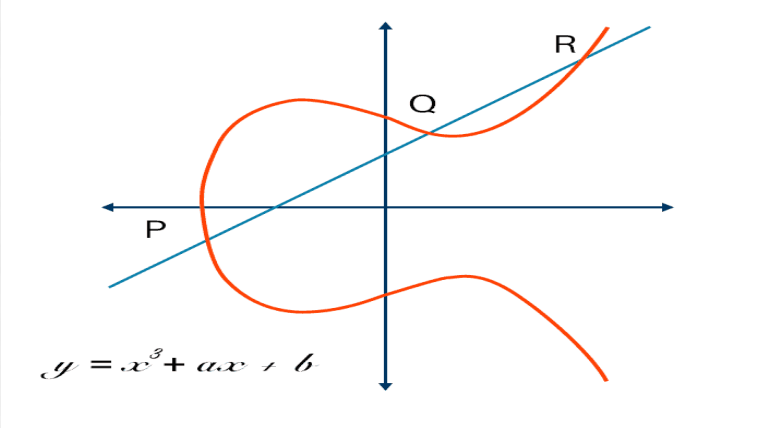
Secure Communication:

- Alice and Bob can now use symmetric keys KA and KB to encrypt and decrypt their messages securely.

Proposed Method

ECC, an alternative technique to RSA, is a powerful cryptography approach. It generates security between key pairs for public key encryption by using the mathematics of elliptic curves.

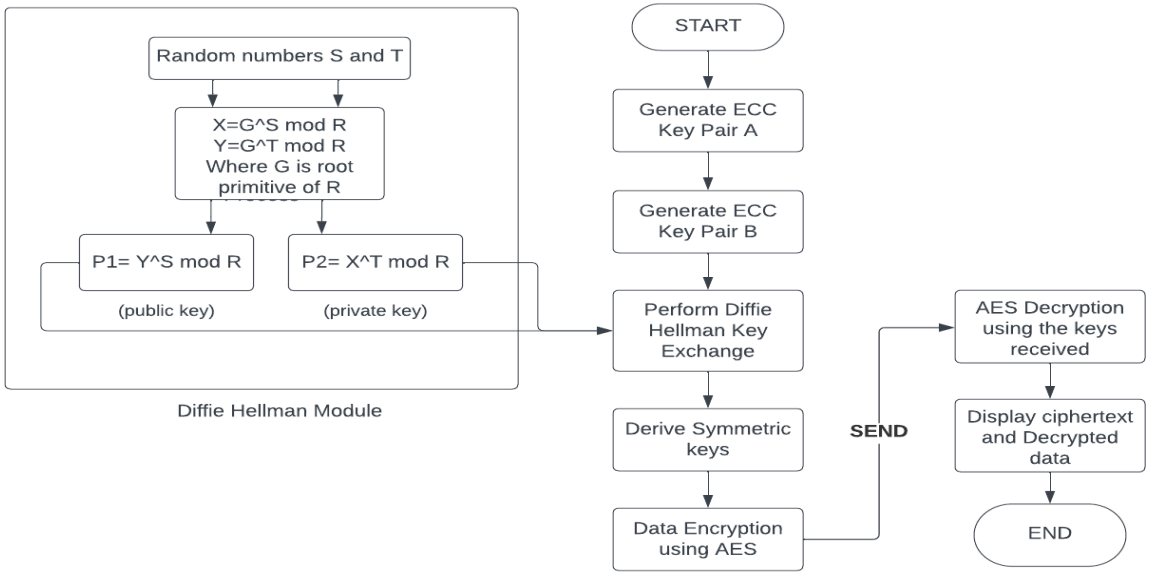
- It makes use of elliptic curves.
- The curves are symmetric to x-axis.
- A line is drawn at any random place on the curve , the points where the line touches are taken as public and private values .



Proposed Method

Start
Generate ECC Key Pair (Alice)
Select ECC Parameters (Curve, Base Point)
Generate ECC Key Pair (Bob)
Alice and Bob exchange public keys
Alice computes Shared Secret Key
Bob computes Shared Secret Key
Shared Secret Key is now established
End

Proposed Method Illustration



Proposed Method Illustration

ENCRYPTION TIME

Msg Size (Chars)	Enc. Time RSA with Diffie-hellman (Existing)	Enc. Time (Proposed)
100	91	10
200	93	14
500	97	27
1000	102	39

DECRYPTION TIME

Msg Size (Chars)	Dec. Time RSA with Diffie-hellmn (Existing)	Dec. Time (Proposed)
100	81	9
200	82	22
500	84	29
1000	91	31

Parameter

The ECC (Elliptic Curve Cryptography) and RSA (Rivest-Shamir-Adleman) are two widely used public-key encryption algorithms, and they differ significantly in terms of key sizes, security, and performance. In this discussion, we'll explore the key size considerations for ECC and RSA, and how they impact the security and efficiency of these encryption methods.

$y^2=x^3+ax+b \bmod p$

Parameters: { p, a, b, G, n }
p : filed(modulo p)
a, b : curve parameters
G : Generator Point
n : ord(G)

Experiment Environment

We use visual studio for this project

- Visual Studio Code is a highly popular and versatile code editor developed by Microsoft.
- It boasts a rich ecosystem of extensions, making it adaptable for various programming languages and development tasks.
- VS Code's sleek design, integrated Git support, and powerful debugging tools make it a top choice for developers across the globe.

Project status

S.No	Functionality	Status (Completed /in-progress/Not started)
01	Algorithm Building	Completed
02	Preparing the flowchart	Completed
03	ECC value pair generation	In progress
04	Public variables digest	In progress
05	Encryption of the plain text	Not Yet Started
06	Decryption of the cipher text	Not Yet Started

References

- A.J. Zargar and M. Manzeor, "Encryption/Decryption using elliptic curve cryptography", International journal of Advanced Research in computer science., vol. 8, no. 1, 2017.
- Sharma, S., Singla, K., Rathee, G., & Saini, H. (2020). A Hybrid Cryptographic Technique for File Storage Mechanism Over Cloud. In First International Conference on Sustainable Technologies for Computational Intelligence (pp. 241-256). Springer, Singapore
- kadhim Bermani, A., Manaa, M. E., & Al-Salih, A. (2020). Efficient cryptography techniques for image encryption in cloud storage. Periodicals of Engineering and Natural Sciences, 8(3), 1359-1373..
- P William and Dr. Abhishek Badholia, "Evaluating Efficacy of Classification Algorithms on Personality Prediction Dataset", Elementary Education Online, vol. 19, no. 4, pp. 3400-3413, 2020.

Thank you

Project seminar–I Evaluation

S.No	Rubrics	Marks
1	Concept Introduction	4
2	Literature and Parameter	5
3	Problem and Problem Illustration	8
4	Proposed Method and Illustration	8
Total		25