Enhancing Confidentiality, Integrity, Authentication & Non – Repudiation using AES & ECC in Mobile – Wallet

[1]Garima Agrawal, [2]Abhilash Sonker

[1]Student, [2] Assistant Professor
CSE/IT Deptt,
MITS, Gwalior, India

Abstract: With the Growth of Cashless Economy and Demonetization Mobile Transactions have seen an emerging trend. Mobile wallets gained popularity with emerging trends. However, Transaction through mobile wallets or payment applications is not secure due to breaching of sensitive information by the attacker. When confidential data is breached all the sensitive information is lost. Sometimes even the sender denies that message is not sent by him/her & the receiver denies that message is not received by him/her. Hence, it is required to secure transaction by encryption. This paper shows the comparison in time performance of payment application using two Cryptographic Processes to enhance Confidentiality, integrity, Authenticity & non-repudiation of private or confidential data. One Cryptographic Process includes combination of AES & 2 times ECC and Other Cryptographic process include RSA. In this paper, we have implemented by encrypting the data by AES & ECC and compared the results with RSA.

Index Terms **- Android, Authenticity, Confidentiality, ECC, Integrity, Mobile Wallet, Non-Repudiation.**

I. INTRODUCTION

The advancement in telecommunications technology has allowed people to communicate in various ways, one of them is using mobile phone device. However, security issues such as authenticity and confidentiality of data or information are still cannot be guaranteed. Messages delivered through SMS can be easily stolen by unauthorized parties because SMS sent via BTS will be accepted by Message Service Center (SMSC), where the operator can view the message contents [3]. Sometimes even the sender denies that message is not sent by him/her & the receiver denies that message is not received by him/her. Yet, clearly, there are many settings where both confidentiality and authenticity are needed, such as in secure user authentication, where each message should be authenticated and encrypted. Cryptography is a technique to hide and secure data over communication channels. Selection of the right algorithm is an important aspect, seen from the level of interest and confidentiality of data. Good algorithms that generate encryption must be unpredictable and cannot be solved using any means [3]. In this paper, we have implemented using AES & 2 times ECC and compared the results with RSA to enhance Confidentiality, integrity, Authenticity & Non-Repudiation of confidential data.

II. LITERATURE-SURVEY

Neetesh Saxena & Narendra S. Chaudhari,et.al [1] .This paper deals with security of short messaging services and analyses the most popular digital signature algorithms such as DSA, RSA and ECDSA and compared these algorithms. The results show that ECDSA is more suitable to generate the signature and RSA is more suitable to verify the signature on mobile devices.

Zhang Chuanrong, Zheng Lianqing, et. al[2] In this paper, a secure and efficient signcryption scheme based on hybrid encryption is studied**.** It can obtain the IND-CCA security for confidentiality and INT-CCA security for authentication based on its base primitives. Moreover, it provides non-repudiation and public verifiability and is insider security in a well defined security model.

Teddy Mantoro, Laurentinus, Nazori Agani, Media A. Ayu, et. al [3] This study begins with a comparative analysis of performance and security of the most useful algorithms: RC6 (Rivest Cipher) and RSA (Rivest Shamir and Adleman), then the complexity of encryption and decryption algorithms to obtain better algorithms are discussed.As proof of concept, a prototype for encryption and decryption of SMS was developed based on Android platform.

Suriyani Ariffin , Ramlan Mahmod , et.al [4] In this paper, there is proposed the use of 3D-AES block cipher symmetric cryptography algorithm for SMS transfer securing.

Zhang Chuanrong, Chi Long, Zhang Yuqing , et.al[5] This paper is based on a short ECDSA, a secure and efficient generalized signcryption scheme. It can work as the same with the original generalized signcryption scheme ECGSC and provides message confidentiality, unforgeability, non-repudiation.

Neetesh Saxena, Narendra S. Chaudhari, Gend Lal Prajapati, et.al[6] The discussion of this paper concludes that MAC functions are more secure than hash function, but having greater complexity and take more to execute. So, it's better to use hash function for maintaining the integrity of message over a network where the transmitted amount of message is very small (SMS).

III. PROBLEM STATEMENT

This paper deals with the Authenticity Confidentiality, Integrity & Non-Repudiation of secure user login authentication. User Authentication Credentials of mobile wallet pose a challenging risk of security. The password credentials lost during user Authentication are a challenge to mobile wallet security. Denial of message sent by the sender and received by the receiver is also a concern . Hence there is a need to secure Password and Username Credentials by an appropriate encryption scheme.

IV. PROPOSED METHODOLOGY

In order to assure secure encryption of user details in mobile wallet we have implemented using AES & 2 Times ECC and compared the results with RSA to enhance Confidentiality, Integrity, Non-Repudiation & Authenticity of confidential data , in this paper.

1.)AES- The algorithm consists of fourteen round transformations for a 32-byte key length ,where each round transformation is composed of four different transformations except last round.

Four different stages are used , one of permutation and three of substitution:

a) The substitute bytes Transformations

Uses an S-box to perform a byte by byte substitution of the block.

b)The ShiftRow Transformations

A simple Permutation, for encryption the 1st row remain unchanged, 2nd row is shifted 1 byte to the left, 3rd is 2 byte to the left, 4th is 3 byte to the left and 5th row is shifted 4 byte to the left. For decryption the operation is similar to that for encryption but in reverse direction.

c)The Mix Column Transformations

A substitution that makes use of arithmetic over GF(28)

d)AddRoundKey Transformations:

A simple bitwise XOR of the current block with a portion of the expanded key.

2.)ECC- Elliptic curves are Cubic curves. Elliptic curves are called elliptic because of their rapport with elliptic integrals in mathematics which can be used to determine the length of arc of an ellipse.

ECC Diffie-Hellman Key Exchange

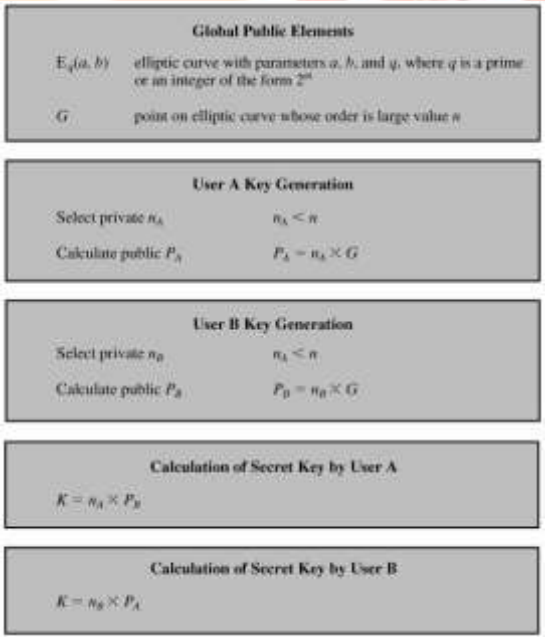

Fig: 1.(a)

P_m is the point on the curve that will be encrypted as ciphertext.

Eq(a,b) – Coordinates of curve

User A Private key- n_A

Public key = $n_A G$

To encrypt and send message P_m to B ,

K is random positive integer.

Encryption-:

Ciphertext $C_m = \{KG , P_m + KP_B\}$

Note that A has used B's public key P_B .

Decryption-:
Plaintext $P_m = P_m + KP_B - n_B(KG)$
$= P_m + K(n_B G) - n_B(KG)$

V. DESIGN & IMPLEMENTATION

a) Implementation of Encryption and Decryption of messages with RSA Algorithm Encryption & Decryption Flowchart on RSA Algorithm :

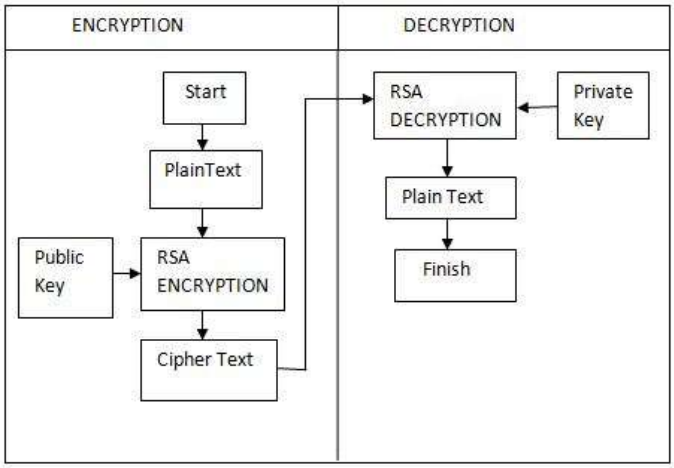

Fig: 2.(a)

b) Implementation of Encryption and Decryption of messages with AES & ECC Algorithm Encryption & Decryption Flowchart on Algorithm :

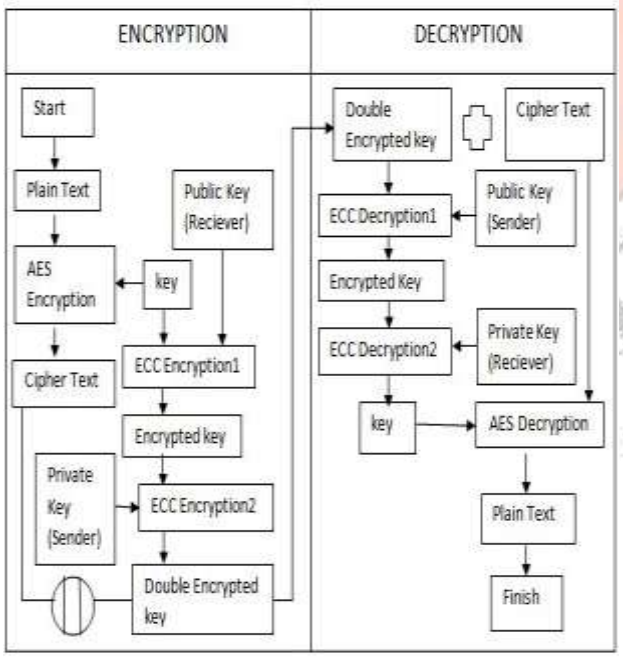

Fig:2.(b)

VI. RESULT & ANALYSIS

a) RSA Algorithm Result:

The average response time in the encryption process is 18 milliseconds/character.
The average response time in the decryption process is 44.5 milliseconds /character.

Fig:3.(a)

b) AES & ECC Algorithm Result:

The average response time in the encryption process is 3 milliseconds/character.
The average response time in the decryption process is 0 milliseconds /character.

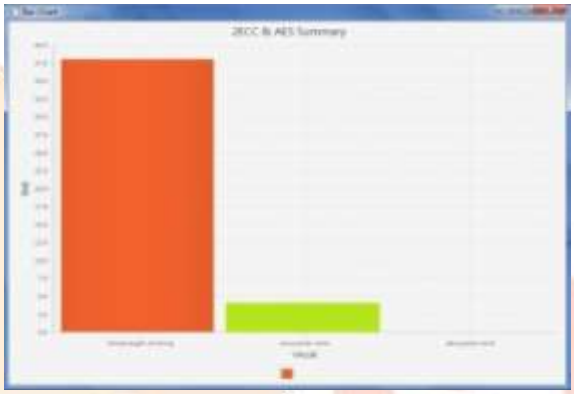

Fig:3.(b)

Application of Encryption on SMS applications using AES & ECC Algorithm and RSA Algorithm affect the length of the message that was sent while the maximum length of AES key is 256 bits. RSA becomes less effective .
ECC algorithm is much more complex than the work flow of RSA algorithm. This is because the number of calculations and generate encryption key.

VII. CONCLUSION & FUTURE EXTENSION

This study proposed on how to increase the security guarantees, authenticity, integrity , confidentiality & non-repudiation in User Authentication Credentials of Mobile Applications. One way is by measuring the respond time between RSA and implemented AES & ECC Algorithm. The following is the summary of this work:
First; there is significantly different time response of encryption & decryption message.
Second; apply cryptography on SMS Application impact on the length of message. The maximum length of an key is 256bits.
Third; the protection of ECC algorithmic rule depends upon the 2 massive prime numbers, Encryption & decryption key, the mathematical calculation are consider robust and troublesome to interrupt.
Fourth; implementation of the RSA Algorithm and AES & ECC Algorithm on SMS application is showing the increment of the security. The cipher text cannot be read without using the correct key.

VIII. REFERENCES

[1]Neetesh Saxena, Narendra S. Chaudhari "Secure Encryption with Digital Signature .Approach for Short Message Service", 2012 IEEE
[2] Zhang Chuanrong, Zheng Lianqing, Xia Mingwen, Zhang Yuqing, " Secure Signcryption Scheme Based on a Hybrid Encryption", 2010 International Conference on Computational Intelligence and Security.
[3] Teddy Mantoro, Laurentinus, Nazori Agani, Media A. Ayu, " Improving the Security Guarantees, Authenticity and Confidentiality in Short Message Service of Mobile Applications", 2016 4th International Conference on Cyber and IT Service Management.
[4] Suriyani Ariffin,Ramlan Mahmod,Ratini Rahmat, Nuzul Annisa Idris, "SMS Encryption using 3D-AES Block Cipher on Android Message Application", 2013 International Conference on Advanced Computer Science Applications and Technologies

[5] Zhang Chuanrong, Chi Long, Zhang Yuqing,"Secure and Efficient Generalized Signcryption Scheme Based on a Short ECDSA", 2010 Sixth International Conference on Intelligent Information Hiding and Multimedia Signal Processing.
[6] Neetesh Saxena, Narendra S. Chaudhari, Gend Lal Prajapati, "An Extended Approach for SMS Security using Authentication Functions", 2012 7th IEEE Conference on Industrial Electronics and Applications (ICIEA).
[7] Hasan Al Bashar Abul Ulayee, Md. Mesbah-Ul-Awal, Shahariar Newaj, "Simplified Approach towards Securing Privacy and Confidentiality of Mobile ShortMessages", 2014 Fourth International Conference on Advanced Computing & Communication Technologies.
[8] Riaz Ullah, Nizamuddin, Arif Iqbal Umar, Noor ul Amin, "Blind Signcryption Scheme Based on Elliptic Curves", 2014 Conference on Information Assurance and Cyber Security (CIACS)