IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Volume-5, Issue-9 E-ISSN: 2347-2693

# Improving Confidentiality, Integrity, Authenticity in Mobile Wallet

**Garima Agrawal[1*], Abhilash Sonker[2]**

[1*]Dept. of CSE and IT, Madhav Institute of Technology and Science, Gwalior, India
[2]Dept. of CSE and IT, Madhav Institute of Technology and Science, Gwalior, India

[*]*Corresponding Author: garima.mits26@gmail.com*

**Available online at: www.ijcseonline.org**

Received: 07/Aug/2017, Revised: 16/Aug/2017, Accepted: 14/Sep/2017, Published: 30/Sep/2017

***Abstract—*** Mobile Transactions have seen an emerging trends after Demonetization and emergence of Digital–wallets. 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. Hence, it is required to secure transaction by encryption. This paper shows the comparision in time performance of payment application using two Cryptographic Processes to enhance Confidentiality, integrity & Authenticity of private or confidential data. One Cryptographic Process includes combination of AES & ECC and Other Cryptographic process include RSA. In this paper, we have implemented using AES & ECC and compared the results with RSA.

***Keywords—*** *Android, Authenticity, Confidentiality, Demonetization, Integrity, Mobile Wallet*

## I. INTRODUCTION

The mobile phone is already an integral part of the lives of more than 1.8 billion people worldwide. With Internet rapidly developing, SMS with e-commerce plays an important role in business transactions and is conducting business communications and solutions over the networks and through computers and mobiles[3]. Confidentiality and Authenticity have been the main goals in secure communication systems [1]. 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 [8]. In this paper, we have implemented using AES & ECC and compared the results with RSA to enhance Confidentiality, integrity & Authenticity of confidential data.

Rest of the paper is organized as follows, Section I contains the introduction of Mobile Wallet use , Section II contain the related work by different Authors regarding mobile wallet security concerns , Section III contain the some measures of problem statement, Section IV contain the architecture and essential steps of proposed methodology, section V explain the implementation methodology with flow chart, Section VI describes results and analysis, Section VII contains the conclusion and Section VIII contains references.

## II. RELATED WORK

Zhang Chuanrong , Zheng Lianqing, et al. [1] 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.

Zhang Chuanrong, Chi Long, Zhang Yuqing , et al. [2] 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, et al. [3] 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.

Neetesh Saxena, Narendra S. Chaudhari, Gend Lal Prajapati, et al. [4] 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).

Suriyani Ariffin , Ramlan Mahmod , et al. [5] In this paper, there is proposed the use of 3D-AES block cipher symmetric cryptography algorithm for SMS transfer securing.

Teddy Mantoro, Laurentinus, Nazori Agani, Media A. Ayu, et al. [8] 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.

## III. PROBLEM STATEMENT

This paper deals with the Authenticity and Confidentiality 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. 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 & ECC and compared the results with RSA to enhance Confidentiality, integrity & 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**

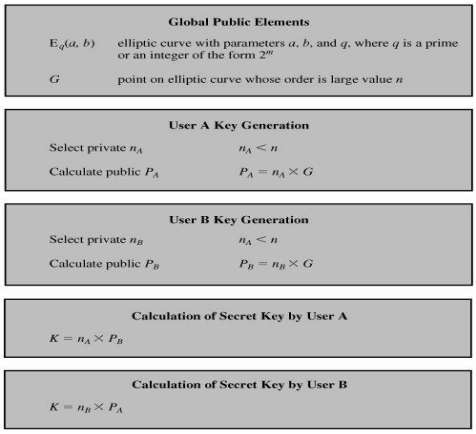


Fig: 1.(a)

$P_m$ 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 AES & ECC Algorithm
Encryption & Decryption Flowchart on Algorithm :

 

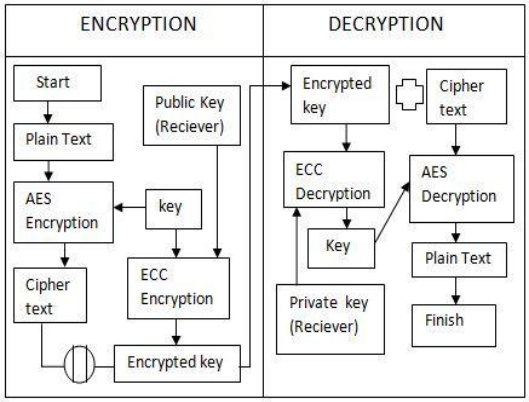


Fig: 2.(a)

b)Implementation of Encryption and Decryption of messages with RSA Algorithm

Encryption & Decryption Flowchart on RSA Algorithm :

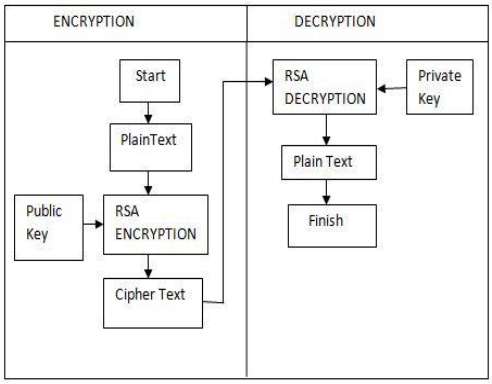


Fig: 2.(b)

## 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.

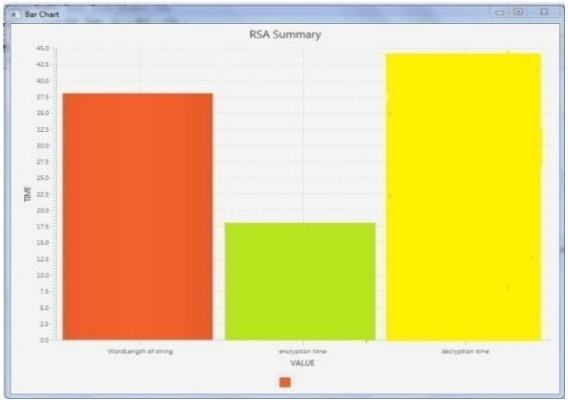


Fig:3.(a)

*b) AES & ECC Algorithm Result:*

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

The average response time in the decryption process is 72 milliseconds /character.

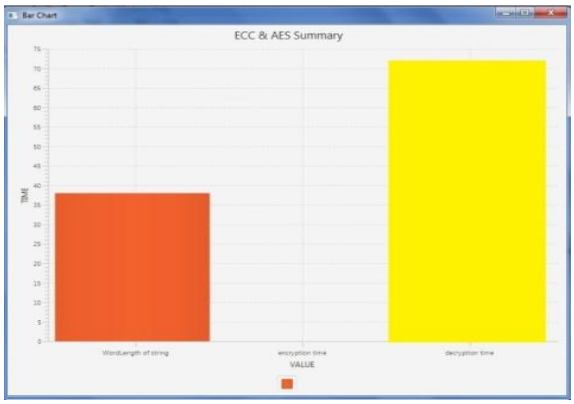


Fig:3.(b)

Fig 3(a) & Fig 3(b) shows that Encryption time of RSA is more than AES & ECC and Decryption time of RSA is less than AES & ECC and hence AES & ECC is more secure.

Fig 2.(a) & Fig 2.(b) shows that AES & ECC is more secure in terms of confidentiality , integrity, & authenticity as plaintext is encrypted by AES key and then key is encrypted by ECC public key of receiver hence more secure than RSA.

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 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

This study proposed on how to increase the security guarantees, authenticity, integrity & confidentiality in User Authentication Credentials of Mobile Applications. One way is by measuring the respond time between RSA and implemented AES & ECC Algorithm And second is applying cryptographic algorithm on plain text message. 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.

## REFERENCES


[1] Z. Chuanrong, Z. Lianqing, X. Mingwen, Z. Yuqing, " *Secure Signcryption Scheme Based on a Hybrid Encryption*", vol. 978-0-7695-4297-3/10, IEEE Computer society in International Conference on Computational Intelligence and Security,2010

[2] Z. Chuanrong, C. Long, Z. Yuqing, "*Secure and Efficient Generalized Signcryption Scheme Based on a Short ECDSA*", vol. 978-0-7695-4222-5/10 , IEEE in Sixth International Conference on Intelligent Information Hiding and Multimedia Signal Processing,2010

[3]N. Saxena, N.S. Chaudhari "*Secure Encryption with Digital Signature .Approach for Short Message Service*", vol. 978-1-4673-4805-8/12, IEEE in World Congress on Information and Communication Technologies , 2012

[4] N. Saxena, N. S. Chaudhari, G.L. Prajapati, "*An Extended Approach for SMS Security using Authentication Functions*", vol. 978-1-4577-2119-9/12, IEEE in 7th IEEE Conference on Industrial Electronics and Applications (ICIEA),2012

[5] S.Ariffin, R. Mahmod, R. Rahmat, N.A. Idris, "*SMS Encryption using 3D-AES Block Cipher on Android Message Application*", vol. 978-1-4799-2758-6/13, IEEE in International Conference on Advanced Computer Science Applications and Technologies ,2013

[6] H.A.B.A.Ulayee, Md.Mesbah-Ul-Awal, S.Newaj, "*Simplified Approach towards Securing Privacy and Confidentiality of Mobile Short Messages",* vol. 978-1-4799-4910-6/14, IEEE in Fourth International Conference on Advanced Computing & Communication Technologies, 2014

[7] R. Ullah, Nizamuddin, A.I. Umar, N. ul Amin, "*Blind Signcryption Scheme Based on Elliptic Curves*", vol. 978-1-4799-5852-8/14, IEEE in Conference on Information Assurance and Cyber Security (CIACS),2014

[8] T. Mantoro, Laurentinus, N. Agani, M. A. Ayu, " *Improving the Security Guarantees, Authenticity and Confidentiality in Short Message Service of Mobile Applications",* vol. 10.1109/CITSM.2016.7577592, IEEE in 4th International Conference on Cyber and IT Service Management, 2016

[9] William Stallings , "*ECC Diffie-Hellman Key Exchange"* , Figure 7 , pp. 295 ,Cryptography and Network Security: principles and practice, Sixth Edition published by Pearson Education, 2014.


 