Analysis of Secured Cryptography Algorithms in M-Commerce

Akanksha Srivastav
Department of Computer Science
Galgotia's college of
Engineering & Technology,
Gr Noida

Ajeet Bhartee
Assistant Prof.
Department of Computer Science
Galgotia's college of
Engineering & Technology,
Gr Noida

ABSTRACT
Today's new technologies which allow mobile phone and handheld device to access the internet have made wireless transaction possible.

Cryptography is the technique in which file is converted in unreadable format. In this file of unreadable format is send, after sending, receiving the file use some algorithms to decrypt the file and read the original data.

Main factor to secure the medium is algorithms and use key size in their algorithms.RSA is the traditional method which provide secure medium. in most of the online transmission field. But here use RSA algorithms with ECC. Which provide more secure medium for transmission

General Terms
Cryptography

Keywords
Cryptography, encryption, decryption, RSA, ECC, transmission

1. INTRODUCTION
Mobile commerce, known as m-commerce, is discussed with the use , application, integration of WTT(wireless telecommunication technique).

In 1960, the proliferation of computer and communication system, brought with demand from the private sector for means to protect information in digital form.

Work of feistel at IBM in early 1970's and culminating in 1977 with the adoption as a US federal information processing standard for encrypting unclassified information , DES , the DATA ENCRYPTION STANDARD.

1976 diffie Hellman published new direction of cryptography

In 1978 rivest, Shamir, Adelman discovered the first practical public key, encryption and signature scheme, now referred to as RSA.

In 1991 the first international standard for digital signature (ISO/IEC 9796) was adopted, it is based on RSA public key scheme.

1994 the us government adopted the digital standard, a mechanism based on the ElGamal public key scheme,

Mobile commerce (3G) technologies was first introduced in JAPAN 2001 and then spread in Europe and USA in 2002.

And continuously day by day work on this field for proper security in this field.

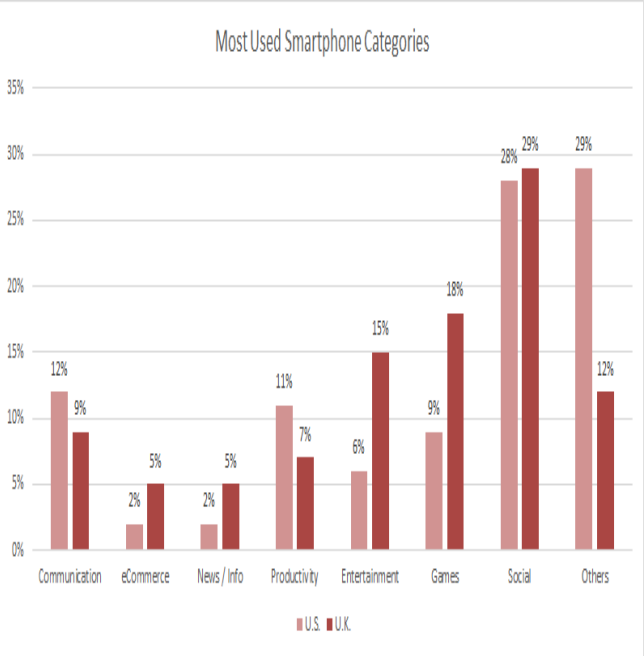


Fig-1

2. M-COMMERCE SECURITY CONCERN
M-COMMERCE needs several layer of security

i) Device security

ii) Language security

iii) Wireless security

iv) Cryptography security

1. Device Security
Design of mobile device there are number of high quality security features-

a) A build in password mechanism which will lock after several mistyped attempts

b) An industry approved, tamper-proof smart card known as SIM (subscriber identification module)

2. Language Security-
Java execution is feasible for PDA, smart phones, laptop and other platform. Server side java technology, java-2 enterprise editions (J2EE) platform.

3. Wireless Security-

I) Wap Security

II) Pki/Wpki

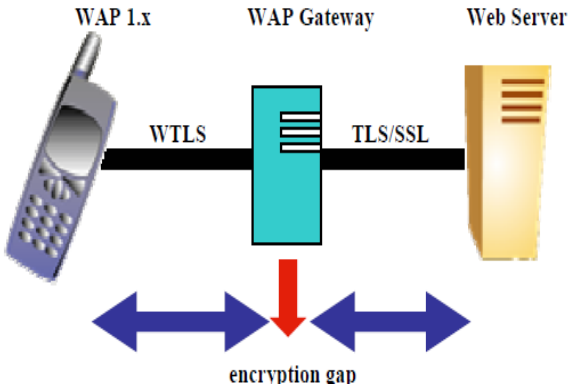


Fig-2

1. **Wap Security**

M-commerce where internet moves data from one device to other device. WAP enabled phones can access interactive service such as information and interactive entertainment**.**

WAP 1.x security uses the wireless transport layer security protocol (WTLS). Is equivalent to SSL (secure socket layer) and it provides authentication, encryption and integrity service.

WTLS support some algorithms like diffie-Hellman, RC5, SHA-1 .it also support some trusted method like DES and 3DES.

2. PKI-PKI

Trusted service enable the secure transfer of information and support a wide variety m-commerce application, PKI must ensure.

i) Confidentiality achieved by cryptography

ii) Authentication achieved by digital certificate

iii) Integrity achieved by digital signature

iv) Non-repudiation achieved by digital signature

PKI consist of fallowing component

i) Certificate authority

ii) Registration authority

iii) Certificate holders

iv) Verification

v) Repositories

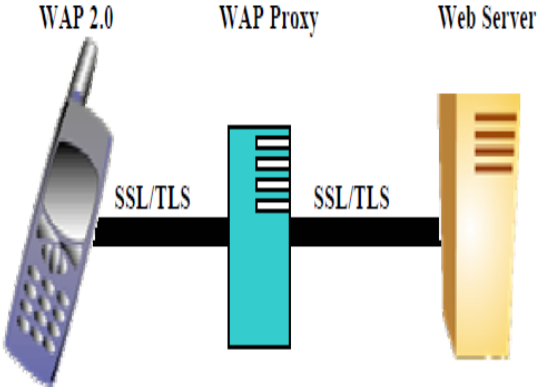


Fig-3

3. RSA ALGORTHIMS

In cryptography, RSA is an algorithm for public-key cryptography which was given by Rivest, Shamir and Adelman. According to Mathematically. The RSA algorithm is based on the mathematical part that is easy to find and multiple two large prime numbers together, but it is extremely difficult to factor their product. There are some important steps are involved in a RSA algorithm to solve a problem as given below:

Step 1: Assume two large prime numbers p & q.

Step 2: Compute: N = p*q Where N is the factor of two large prime number.

Step 3: Select an Encryption key (E) such that it is not a factor of (p-1)*(q-1)

I.e. Ø (n) = (p-1)*(q-1)

For calculating encryption exponents E, should be 1< E < Ø (n) such that

Gcd (E, Ø (n) =1 The main purpose of calculating gcd is that E & Ø(n) should

Be relative prime.

Where Ø (n) is the Euler Totient Function & E is the Encryption Key.

Step 4: Select the Decryption key (D),

Which satisfy the Equation D*E mod (p-1)*(q-1) = 1

Step 5: For Encryption:

Cipher Text= (Plain Text)E mod N CT = (PT) E mod N Or CT=ME mod N

Step 6: For Decryption: Plain Text= (Cipher Text)E mod N PT= (CT) E mod N

4. ECC ALGORITHMS

Elliptic Curve Cryptography (ECC) is emerging as an attractive public-key cryptosystem for mobile/wireless environments. Compared to traditional cryptosystems like RSA, ECC offers equivalent security with smaller key sizes, which results in faster computation; lower power consumption, as well as memory and bandwidth savings. This is especially useful for mobile devices which are typically limited in terms of their CPU, power and network connectivity. However, the true impact of any public-key cryptosystem can only be evaluated in the context of a security protocol. This paper presents a first estimate of the

performance improvements that can be expected in SSL (Secure Socket Layer), the dominant security protocol on the Web today, by adding ECC support.

For any cryptographic technique, there is an analogue for Elliptic Curve. One of these systems is Diffie – Hellman key exchange system. This paper proposed methods to encrypt and decrypt the message, and we will encrypt and decrypt the message by using the Diffie–Hellman Exchanging key. And this is a secrete point in the proposed methods (M1) and (M2). In the first method (M1), the sender compute the multiplication between the coordinates of the key in the encryption algorithm, and the receiver compute the multiplication between the coordinates of the key in the decryption algorithm. In the second method (M2), we support the system more security of the first method, because the sender compute the exponentiation function between the coordinates of the key in the encryption algorithm (use fast exponentiation method), and the receiver compute the inverse of the exponentiation function between the coordinates of the key in the decryption algorithm. The rapid progress in wireless mobile commerce.

Comparison between Key size of ECC and RSA.And also discuss public key cryptography mathematical problem and used algorithms.

Table-1

ECC KEY SIZE COMPARED TO RSA		
ECC KEY SIZE (bits)	Traditional RSA key size (bits)	Key –size ratio
109	512	1:5
131	768	1:6
163	1024	1:6
283	3072	1:11
409	7680	1:19
571	15360	1:27

Table-2

THREE MAJOR INDUSTRY –STANDARD PKC		
PKC	MATHEMATICAL PROBLEM	ALGORITHM
INTEGAR FACTORISATION	GIVEN A NUMBER n, FIND ITS PRIME FACTORS	RSA , ROBIN-WILLIAMS
DISCRETE LOGARITHM	GIVEN A PRIME n, AND NUMBER g AND h , FIND x SUCH THAT h=g^x mod n	ElGamal , Diffie-hellman , DSA
Ec discrete logarithms	Given an elliptic curve E and point P and Q on E , find x that Q =xP	EC-DIFFIE-HELLMAN , ECDSA

5. OBJECTIVES

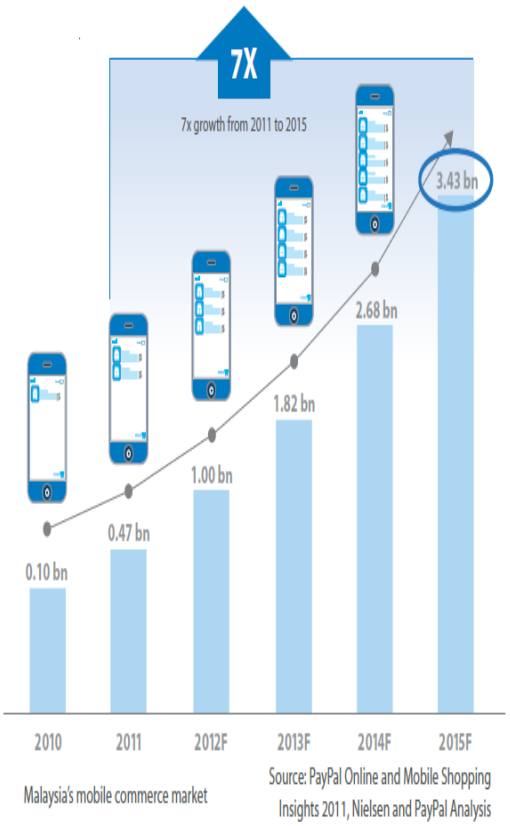
The objectives of the proposed algorithms are to provide more security during m-commerce operation.

In this mechanism system provide the server client mechanism in which the file uploaded on the server side can be downloaded by client who is successfully register on the system.

Server finds that requested client is authorised and permit to access the file. Previous way to secure the algorithms with single algorithm but here in this new work secure with tow algorithms.

6. CONCLUSION

Cryptographic support is an important mechanism of securing important data. In this work, we introduce combined approach of two well-known and secured algorithms RSA and ECC. This algorithm is simple and fast enough for most applications. RSA is already in use in most of the application globally, we add the more secured technique call elliptical curve cryptography to enhance its security. In future, we are interested to extend the proposed system for every possible format of files by which everyone is capable to use this system for secure data transmission and sharing of various files through this secure channel.



7. REFERENCES

[1] William Stallings: Cryptography and Network Security Principles and Practice, 5th Edition

[2] M. Junaid Arshad and M. Abrar "Securing DNS Using Elliptical Curve Cryptography: An Overview"

[3] Ram Ratan Ahirwal, Manoj Ahke, "Elliptic Curve Diffie-Hellman Key Exchange Algorithm for Securing

Hypertext Information on Wide Area Network", IJCSIT volume 4 (2) 2013

[4] S. Maria Celestin Vigila1, K. Muneeswaran2, "Elliptic Curve based Key Generation for Symmetric Encryption", IEEE 2011

[5] Vishwa gupta, 2. Gajendra Singh ,3 .Ravindra Gupta, "Advance cryptography algorithm for improving data security" IJARCSSE 2012

[6] G.V.S. Raju and Rehan Akbani, Department of Computer Science The University of Texas at San Antonio. San Antonio, TX 78249-0669 "Elliptic Curve Cryptosystem and its Applications"

[7] "Visa Mobile 3D Secure Specification for Mcommerce Security".

[8] Ram Ratan Ahirwal, Manoj Ahke, "Elliptic Curve Diffie-Hellman Key Exchange Algorithm for Securing Hypertext Information on Wide Area Network ", IJCSIT volume 4 (2) 2013

[9] S. Maria Celestin Vigila1, K. Muneeswaran2, "Elliptic Curve based Key Generation for Symmetric Encryption", IEEE 2011

[10] Batra, D. S., & Juneja, D. (2013, February). MCommerce in India: Emerging Issues. International Journal of Advanced Research in IT and Engineering, 2(2), 54-65.

[11] Y. Jing, G.-J. Ahn, Z. Zhao, and H. Hu, "Riskmon: Continuous and automated risk assessment of mobile applications," in Proc. of the 4th ACM Conference on Data and Application Security and Privacy (CODASPY'14), San Antonio, Texas, USA. ACM, March 2014, pp. 99–110.