A Secure Approach for SMS in GSM Network

Neetesh Saxena
Department of Computer Science & Engineering
Indian Institute of Technology, Indore, India
neetesh.saxena@gmail.com

Narendra S. Chaudhari
Department of Computer Science & Engineering
Indian Institute of Technology, Indore, India
narendra@iiti.ac.in

ABSTRACT
The Short Message Service (SMS) is one of very popular kind of superior and well-tried services with a global availability in GSM networks. This paper deals with an SMS security for mobile communication. The transmission of an SMS in GSM network is not secure; therefore it is desirable to secure SMS by additional encryption. A proposed approach, based on encryption and digital signature efficiently embeds the confidentiality, integrity, authentication, and non-repudiation in the SMS messages. In the next part, there is the description of design and implementation of the application, which encrypts SMS by DES, Triple DES, AES and Blowfish algorithms and finally signs SMS by DSA or RSA algorithm respectively. At the end, we described attacks on secured SMS and future extension of the application.

Categories and Subject Descriptors
C.1.3 Cellular architecture, D.3.2 Java, J2ME

General Terms
Security, Algorithms

Keywords
RSA, DSA, AES, DES, block cipher, asymmetric encryption

1. INTRODUCTION
Mobile phones are part of our daily life. Nowadays, mobile phones provide not only communication services, but also many multimedia and other functions [22]. Mobile phones contain private or personal data. This data is saved in a form of phone contacts, SMS, notices in a calendar, photos etc. Protection of the information depends also on a concrete user. The user should prevent against alienation of her/his mobile phone. If the mobile phone is in wrong hands, most of the information is available without a great effort (received SMS) [23]. User registers the theft of the mobile phone almost immediately, but tapping never. The SMS tapping is possible in GSM network at some places. There could be used the encryption for securing of SMS. Encryption is most often realized through some user encryption applications [2]. Sending an SMS is cheap, fast and simple. The mobile communications has experienced a great acceptance among the human societies. The SMS is the most popular data bearer/service within GSM, IS-95, CDMA2000, and other cellular networks.

CUBE 2012, September 3–5, 2012, Pune, Maharashtra, India. Copyright 2012 ACM 978-1-4503-1185-4/12/09…$10.00.

It is a store-and-forward, easy to use, popular, and low cost service. While it is mainly used for the personal communications, it has also been used in applications where the other party is an information system [1]. Various security services must be in any secure network like authentication, confidentiality, integrity, non-repudiation and availability of message. These services can be understood as:

Authentication means that correct identity is known to communicating partner;

Confidentiality means certain message information is kept secure from unauthorized party;

Integrity means message is unaltered during the communication;

Non-repudiation means the origin of a message cannot deny having sent the message;

Availability means the normal service provision in face of all kinds of attacks.

There are various attacks have found in the security of SMS in GSM network. Some of these attacks and their solutions have been discussed below.

Man-in-the-Middle Attack

In this attack, the attacker intercepts network transmissions between two hosts. The attacker then masquerades as one of the hosts, often inserting additional transmissions into the network dialogue.

(Solution: Encryption is the best defense against man-in-the-middle attacks)

Replay Attack

Replay attack occurs when a third party captures a message in transmission and replays it at a later time. By capturing the correct messages, an intruder may be able to gain access to a secure medium which are normally encrypted and unreadable.

(Solution: Pass back and forth a one time unique number or nonce)

Message disclosure

Disclosure of sensitive data can result in loss or damage, such as identity theft, lawsuits, loss of business, or regulatory fines. Any data that contains sensitive information must be protected from unauthorized users.

(Solution: Use encryption to protect sensitive data that is contained in a message)

Repudiation Attack

Repudiation attacks are an attempt to mislead or deny of sending or receiving messages.

(Solution: Use Digital Signature to provide non-repudiation)

In table1, we can easily see that plain text SMS is a weak encryption method. In this research work, a methodology is proposed and implemented to make it more secure while transmit the SMS over the network which is having confidential and important information.

Table1: GSM Technologies

Telecom Standard	Data Bearer	Mode of Transaction	Security
GSM	Plain Text SMS	SMS / J2ME	Weak Encryption
GSM	USSD / Application SMS	SMS / J2ME	Secure Channel
GSM	GPRS / WAP	J2ME / Browser	Secure Channel

2. LITERATURE SURVEY

In the literature, many authors have used different encryption techniques to provide confidentiality to SMS transmitted messages. Some of these works are presented in this section. In a study by Mary Agoyi and Devrim Seral [1] large key size algorithms are not suitable for SMS encryption due to small memory and low computational power of mobile phones. This has put Elliptic curve at an advantage over the RSA and ELGamal in SMS encryption. In the paper of Alfredo De Santis, Aniello Castiglione and Umberto Ferraro Petrillo [2] the results seem to show that RSA and DSA cryptosystems perform generally better than ECDSA, except when using very large keys. Nassim Khozooyi, Maryam Tahajod and Peyman khozooyi [3] are discussed the security of mobile network protocol along with information security for governmental transactions. A new public key-based solution for secure SMS messaging (SSMS) is introduced by M. Toorani and A. Beheshti Shirazi [4]. It efficiently combines encryption and digital signature and uses public keys for a secure key establishment to be used for encrypting the short messages via a symmetric encryption. Since it deploys elliptic curves and a symmetric encryption algorithm, it has great computational advantages over the previously proposed public key solutions while simultaneously providing the most feasible security services.

In a study of D. Lisonek and M. Drahansky [5] the application for securing of SMS has been designed and implemented, which prevents tapping and also substituting. In the paper of C. Narendiran, S. Albert Rabara and N. Rajendran [6] an end-to-end security framework using PKI for mobile banking is proposed. The security framework solution allows us to provide strong customer authentication and non-repudiation by employing public-key cryptography for customer certificates and digital signatures. It is observed that the AES algorithm utilized less computation time and memory for encrypting the user's data. The AES model shows greater performance than the 3DES and RSA model that uses Public Key Infrastructure. Mahmoud Reza Hashemi and Elahe Soroush [7] proposed a secure m-payment protocol for mobile devices. In the paper of Mohsen Toorani, Ali Asghar and Beheshti Shirazi [8], the security of the GSM network is evaluated, and a complete and brief review of its security problems is presented. Some practical solutions to improve the security of currently available 2G networks are also proposed. It became clear that encryption algorithm in GSM network A5/2 provided almost no security, and A5/1 could be attacked with practical complexity by a variety of techniques [9] [10] [14].

3. PROPOSED APPROACH

Figure1 represents the basic architecture of GSM network. As we, know that the encryption in GSM is previously managed by A5/1 and A5/2 algorithms. These algorithms do not provide end-to-end security. The privacy of most GSM phone conversations is previously protected by A5/1 and A5/2 stream ciphers, which were repeatedly shown to be cryptographically weak by many researchers.

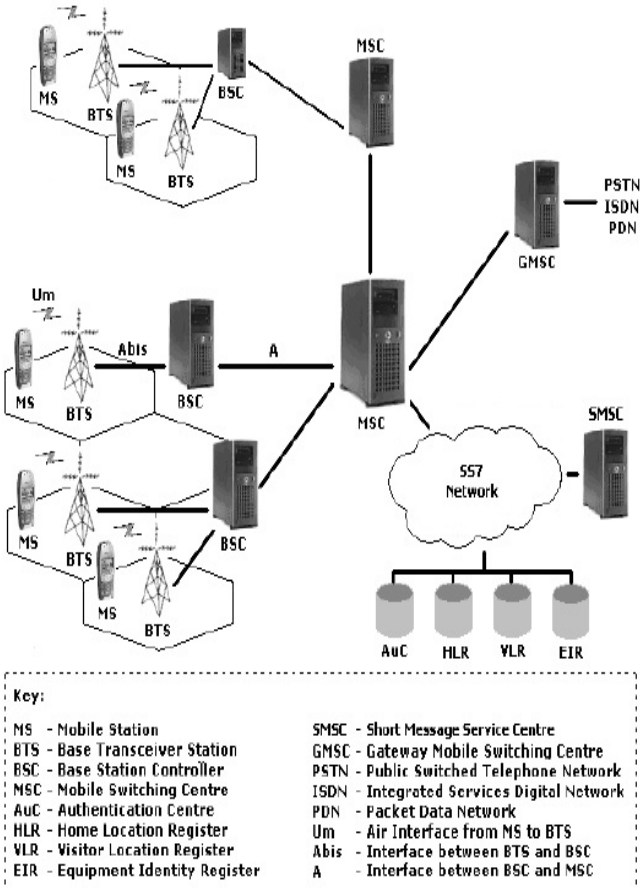

Figure 1. GSM Architecture

In 3GPP, they have replaced by a new A5/3 block cipher called KASUMI. But, now various attacks have been proved on it and KASUMI has been proved vulnerable. The existence of better related key attacks on the full KASUMI was already shown in [19] [20].So, there is a need to propose a secure system which can provide end-to-end security because none of A5/1, A5/2 and KASUMI provides end-to-end security.

The efficiency of a system for guaranteeing secure SMS messages is heavily influenced by the same ingredients which govern its own security, in other words, the cryptosystems and the security parameters it uses. The user should be given the possibility to choose to trade part of the security of a system with shorter response times, and vice-versa. Moreover, such a customization should be allowed on a per-message basis, because the same user might need to send messages, even to the same recipient, with different levels of security. So, we propose a system which could provide proper security by encrypting the message first then applying digital signature over the encrypted message. This system supports some of the most used digital signature schemes (i.e. RSA and DSA [3]). Here, SMS encrypt, sign and sends to receiver with

key using DES (Data Encryption Standard) or AES (Advance Encryption Standard), DSA (Digital Signature Algorithm) and RSA respectively.

4. SYMMETRIC KEY ALGORITHMS

Symmetric-key algorithms are a class of algorithms for cryptography that use trivially related, often identical, cryptographic keys for both decryption and encryption [11].

Data Encryption Standard

It is based on a symmetric-key algorithm that uses a 56-bits key. DES is now considered to be insecure for many applications. This is chiefly due to the 56-bits key size being too small; in January, 1999, distributed.net and the Electronic Frontier Foundation collaborated to publicly break a DES key in 22 hours and 15 minutes [15]. The algorithm is believed to be practically secure in the form of Triple DES, although there are theoretical attacks. In recent years, the cipher has been superseded by the Advanced Encryption Standard (AES) [7].

4.2 Triple-DES

Triple DES uses a key bundle which comprises three DES keys, K1, K2 and K3, each of 56 bits. Each triple encryption encrypts one block of 64 bits of data.

Encryption algorithm is:

Cipher text = EK_3 (DK_2 (EK_1 (Plain text)))

Decryption is the reverse:

Plain text = DK_1 (EK_2 (DK_3 (Cipher text)))

The standards define three keying options:

Keying option 1: All three keys are independent.
Keying option 2: K_1 and K_2 are independent, and $K_3 = K_1$.
Keying option 3: All three keys are identical, i.e. $K_1 = K_2 = K_3$.

Keying option-1 is the strongest, with 3 * 56 = 168 independent key bits.

Keying option-2 provides less security, with 2 * 56 = 112 key bits. This option is stronger than simply DES encrypting twice, e.g. with K1 and K2, because it protects against meet-in-the-middle attacks.

Keying option-3 is no better than DES, with only 56-bits key. This option provides backward compatibility with DES, because the first and second DES operations simply cancel out. However, even this more powerful version of DES may not be strong enough to protect data for very much longer. The DES algorithm itself has become obsolete and is in need of replacement. Triple DES is simply another mode of DES operation. It takes three 56-bits keys, for an overall key length of 168 bits. Attacks on two-key triple-DES have been proposed by Merkle and Hellman and Van Oorschot [16].

4.3 Advanced Encryption Standard

The standard comprises three block ciphers, AES-128, AES-192 and AES-256, adopted from a larger collection originally published as Rijndael. Each AES cipher has a 128-bit block size, with key sizes of 128, 192 and 256 bits, respectively. As of 2009, AES was one of the most popular algorithms used in symmetric key cryptography [12].

4.4 Blowfish

Blowfish algorithm uses 64 bits block plain text with variable size key length. Key varies from 32 bits to 448 bits. A reflection attack on blowfish has been found in 2007 [17].

5 DSA SIGNATURE SCHEME

The DSA provides the capability to generate and verify signatures. Signature generation makes use of a private key to generate a digital signature [21]. Anyone can verify the signature of a user by employing that user's public key. Signature generation can be performed only by the possessor of the user's private key [13]. Hash function is used in the signature generation process to obtain a condensed version of data, called a message digest. The message digest is then input to the DSA to generate the digital signature. The digital signature is sent to the intended verifier along with the signed data. The verifier of the message and signature verifies the signature by using the sender's public key [23]. Figure2 shows that same hash function must also be used in the verification process.

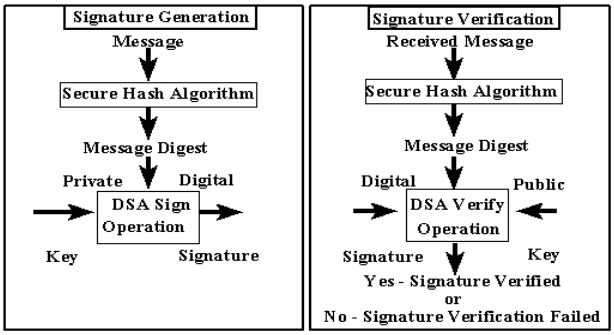

Figure 2. DSA signature generation and verification

For signature generation and verification, the data which is referred to as a message, M is reduced by means of the Secure Hash Algorithm (SHA). The DSA signature scheme consists of DSA = (DSA.key, DSA.gen, DSA.ver).

6 IMPLEMENTATION & RESULTS

We have used J2ME wireless toolkit for the implementation of SMS security. We have implemented DES, Triple-DES, AES and Blowfish algorithms for the purpose of encryption and decryption.

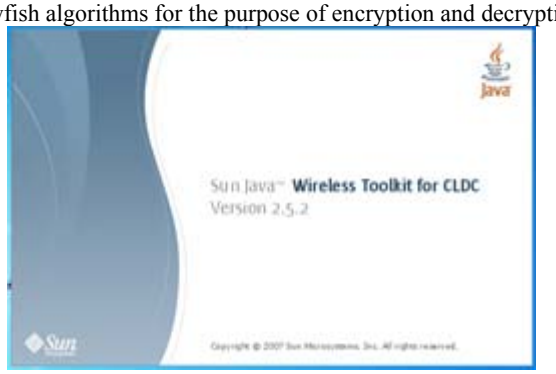

Figure 3. Starting J2ME Wireless Toolkit 2.5.2

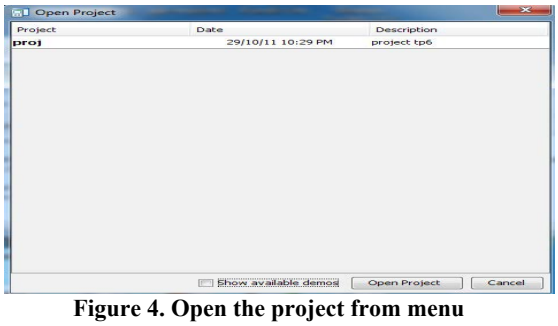

Figure 4. Open the project from menu

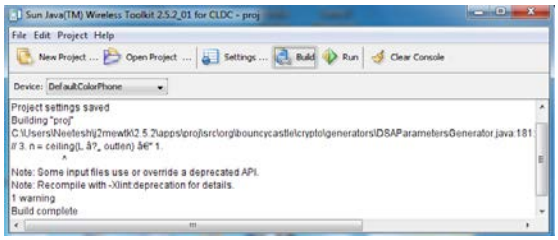

Figure 5. Compile the java code

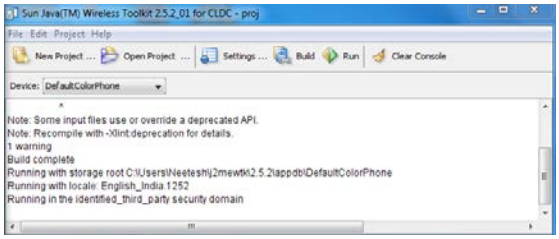

Figure 6. Run the code

Out of these algorithms AES gives the best result and takes minimum time to encrypt the text and the structure of AES is most complex out of these algorithms. Figures 3, 4, 5 and 6 show the basic code execution steps. Figures 7 to 12 show the process of DES encryption and decryption. Similarly, we have implemented all other algorithms in wireless toolkit. The results show that AES algorithm is the best algorithm for encryption and decryption and is unbreakable till now.

Figure 7. Menu for sending SMS

A nonce is used to make communication between sender and receiver. This will also prevent the system from replay attack. A random number is transmitted every time a communication takes place between sender and receiver.

Figure 8. Entering message to send

Figure 9. Sending SMS from one mobile to other mobile

Figure 10. Enter text for Encryption and select DES for encryption/decryption

Figure 11. Select encryption from menu and encrypted text

Figure13 and 14 shows the implementation of different algorithms with different data size. The results observed from these figures show that AES takes less time to encrypt and decrypt data as compare to other algorithms.

Table2 and table3 shows DSA and RSA digital signature generation and verification with different data sizes. As results show both the algorithm take almost same time but the structure of DSA is more difficult to vulnerable, so we choose DSA for signature purpose.

Figure 12. Select decryption from menu and decrypt the cipher text

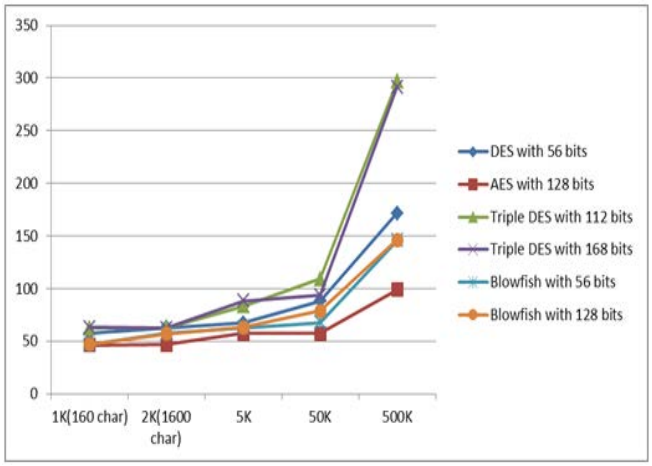

Figure 13. Encryption- Size vs. Time

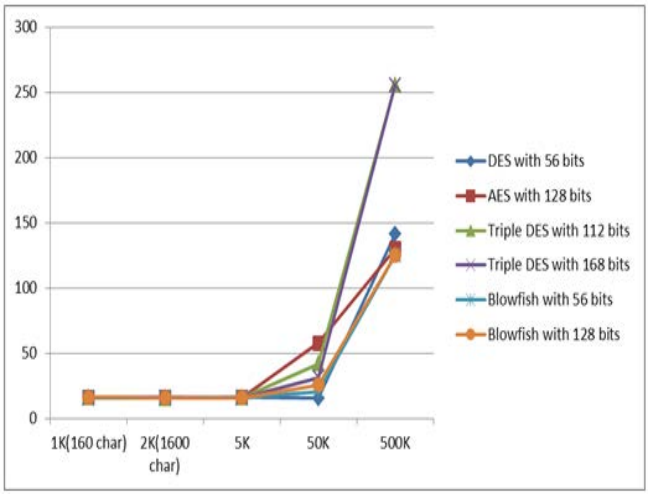

Figure 14. Decryption- Size vs. Time

Table2: Signature generation of DSA and RSA

Size	DSA with SHA1 Time (in millisec)	RSA with SHA1 Time (in millisec)
1K	15	16
2K	15	16
5K	15	16
50K	16	15
500K	16	16

Table3: Signature verification of DSA and RSA

Size	DSA with SHA1 Time (in millisec)	RSA with SHA1 Time (in millisec)
1K	16	16
2K	15	15
5K	20	16
50K	15	15
500K	16	16

7 CONCLUSION & FUTURE EXTENSION

The application for securing of SMS has been designed and implemented. This approach prevents the system from various attacks man-in-the-middle attack, replay attack, message

disclosure and repudiation attack. Out of these implemented algorithms AES is the best one and which is completely unbreakable till now. DSA is selected as a suitable algorithm for digital signature as it is based on discrete logarithm problem. Using the same value twice (even while keeping k secret), using a predictable value, or leaking even a few bits of k in each of several signatures, is enough to break DSA [18]. So, there is a future need of finding better algorithm for digital signature like elliptic curve based digital signature (also needs improvement because it also been proved vulnerable) or based on some harder problems. These points are under the consideration of research work for SMS security. There is a need to develop an algorithm which is much harder to break. In the future, the application could also provide MMS securing.

8 ACKNOWLEDGMENTS

Authors want to thank IIT Indore for their support in this research work. Reviewers of this paper are also thankful who gave suggestions and comments to make better quality research paper.

9 REFERENCES

[1] Agoyi Mary, Seral Devrim. 2010. SMS Security: An Asymmetric Encryption Approach. *Sixth International Conference on Wireless and Mobile Communications.* IEEE 2010, 448-452.

[2] Santis Alfredo De, Castiglione Aniello and Petrillo Umberto Ferraro. 2010. An Extensible Framework for Efficient Secure SMS. *International Conference on Complex, Intelligent and Software Intensive Systems.* IEEE 2010, 843-850.

[3] Khozooyi Nassim, Tahajod Maryam, khozooyi Peyman. 2009. Security in Mobile Governmental Transactions. *2009 Second International Conference on Computer and Electrical Engineering*. IEEE 2009, 168-172.

[4] Toorani M. and Shirazi A. Beheshti. 2008. SSMS - A secure SMS messaging protocol for the m-payment systems. in *IEEE Symposium on Computers and Communications*. IEEE July 2008, 700–705.

[5] Lisonek D., Drahansky M. 2008. SMS Encryption for Mobile Communication. in *International Conference on Security Technology*. IEEE Dec 2008, SECTECH ’08*,* 198–201.

[6] Narendiran C., Rabara S. Albert, Rajendran N. 2008. Performance Evaluation on End-to-End Security Architecture for Mobile Banking System. 978-1-4244-2829-8/08/$25.00, IEEE 2008.

[7] Hashemi Mahmoud Reza, Soroush Elahe. 2006. A Secure m-Payment Protocol for Mobile Devices. *IEEE CCECE/CCGEI, Ottawa*. May 2006, 294-297.

[8] Toorani Mohsen, Shirazi Ali Asghar Beheshti. 2008. Solutions to the GSM Security Weaknesses. *the Second International Conference on Next Generation Mobile Applications, Services, and Technologies.* IEEE 2008, 576-581.

[9] Barkan Elad and Biham Eli. 2006. Conditional Estimators: an Effective Attack on A5/1. *in proceedings of SAC 2005.* Springer 2006, Lecture Notes in Computer Science 3897, 1-19.

[10] Biryukov Alex, Shamir Adi and Wagner David. 2001. Real Time Cryptanalysis of A5/1 on a PC. in *proceedings of Fast Software Encryption 2000*. Springer 2001, Lecture Notes in Computer Science 1978, 1-18.

[11] Stallings W. 2006. Cryptography and network security. *Prentice Hall*. New Jersey, United State.

[12] Garza-Saldana J. J. and Diaz-Perez A. 2008. State of security for SMS on mobile devices. *Proceedings of the Electronics, Robotics and Automotive Mechanics Conference,* 110 -115.

[13] Sidek Salman Firdaus bin Haji. 2010. The Development of the Short Messaging Service (SMS) Application for the School Usage. 978-1-4244-6716-7/10/$26.00, IEEE 2010, 1382-1386.

[14] Ekdahl Patrik and Johansson Thomas. 2003. Another Attack on A5/1. *IEEE Transactions on Information Theory*. vol. 49, no. 1, 284–289.

[15] Web http://en.wikipedia.org/wiki/Data_Encryption_Standard

[16] Web http://www.rsa.com/rsalabs/node.asp?id=2231

[17] Gonzalez Tom. 2007. A Reflection Attack on Blowfish. *Journal of Latex Class Files.* vol. 6, no. 1, January 2007, 1-3.

[18] http://en.wikipedia.org/wiki/Digital_Signature_Algorithm

[19] Biham Eli, Dunkelman Orr, and Keller Nathan. 2005. A Related-Key Rectangle Attack on the Full KASUMI. *Advances in Cryptology, proceedings of ASIACRYPT 2005.* Springer 2005, Lecture Notes in Computer Science 3788, 443–461.

[20] Kim Jongsung, Hong Seokhie, Preneel Bart, Biham Eli, Orr Dunkelman, and Keller Nathan. 2009. Related Key Boomerang and Rectangle Attacks.

[21] Xuan Zuguang, Du Zhenjun, Chen Rong. 2009. Comparison Research on Digital Signature Algorithms in Mobile Web Services. *International Conference on Management and Service Science.* IEEE 2009, MASS '09, 1-4.

[22] Saxena Neetesh and Payal Ashish. 2011. Enhancing Security System of Short Message Service for M-Commerce in GSM. *International Journal of Computer Science & Engineering Technology (IJCSET).* ISSN: 2229-3345, vol. 2, no. 4, April 2011, 126-133.

[23] Saxena Neetesh, Chaudhari Narendra S. 2011. A Secure Digital Signature Approach for SMS Security. *International journal of Computer Application (IJCA).* Special issues on IP Multimedia Communications, published by Foundation of Computer Science. ISBN: 978-93-80864-99-3, Oct. 2011, New York, USA, 98-102.