Volume: 05, Issue: 02, Pages:1873-1882 (2013) ISSN : 0975-0290

SMS Security in Mobile Devices: A Survey

Muhammad Waseem Khan
Department of Computer Science, COMSATS Institute of Information Technology, Wah Cantt
Email: muhammad.wasim1@gmail.com

ABSTRACT

The Short Message Service (SMS) is one of the frequently used mobile services with universal availability in all GSM networks. The current SMS hasn't achieved secure transmission of plaintext between different mobile phone devices. SMS doesn't have its own build-in mechanism to secure the transmitted data because security isn't considered as a priority application for mobile devices. Many SMS security schemes have been proposed by the researchers. This survey presents the existing schemes used to secure SMS message communication. State of the art SMS security solutions for mobile devices is presented from the period 2006-2013. Literature research of those security schemes is conducted and presented in this survey. The effect of each security scheme on mobile device's performance is also observed. Finally, a general summary of all security schemes with their limitations is presented.

Keywords – **Cryptography, One-time-key Pad, PKI, Short message service, SMS security**

Date of Submission: June 01, 2013 Date of Acceptance: August 12, 2013

1. INTRODUCTION

Short message service (SMS) is a wireless text messaging service that enables the mobile subscribers to transmit text messages among each other. The length of SMS message is 160 characters having no pictures /graphics in it. Global System for Mobile Communication (GSM) is used as a mean of sending SMS messages. After the SMS message is sent by the user, SMS Center (SMSC) is used to store the SMS messages in order to forward them to the target mobile device. SMSC uses Store-and-forward technique to store messages in order to forward to the target device. If the (Home Location Register) HLR of target mobile device is active, then SMSC will transfer the SMS message to target mobile device. SMSC will receive the verification message that confirms the delivery of SMS message to target device [1]. Un-encrypted SMS messages are stored in SMSC; therefore, SMSC staff can view and modify the content of SMS message. Many SMSCs can also keep the copy of SMS message for billing and auditing purposes. Therefore, it becomes easy for attackers to view SMS messages through SMSC [2]. After attacking SMSC, attacker can read the SMS messages, example of such an attack in recent years is the interception of English football captain, David Backham's SMS messages sent to his personal assistant, Rebecca loos and published in the tabloid [3]. mmO2, European phone operator has dismissed its two employees on intercepting and providing SMS copies to their friends [4].

Several Cryptography methods have been used to reduce the SMS security threats and provide enough security to mobile devices. But these encryption techniques can't perform their activity in a complete manner since it affects the performance of mobile devices in terms of power and battery life constraints [5]. Symmetric Cryptography is the type of encryption used to provide end-to-end security to SMS messages. It is also good for mobile devices due to their limited resources, i.e., limited power/energy, in-sufficient memory and less processing power [6]. It uses the shared secret key between two parties in order to protect SMS message communication. Key distribution mechanism remains in-secure, since if an attacker intercepts the key distribution process and intercepting the key, he/she can easily modify the SMS message contents. Therefore, Key distribution is quite difficult and insecure in symmetric key cryptography. DES and AES are the examples of symmetric key cryptography [7].

The key distribution problem is solved by Asymmetric cryptography by using pair of keys (i.e. private and public) for communication. Sender is using public key for communication while private key is used in order to decrypt the message. It doesn't offer authentication facility; therefore man-in-the-middle attack is common in public key cryptography. Public key infrastructure (PKI) is then used to improve the deficiency of public key cryptography [8], [9]. Although Asymmetric encryption is strong and key distribution is also very easy in it, but, it is avoided because of its computational overhead [10].

Nevertheless, mobile devices have improved their memory capacity as well as their performance. Energy efficiency and battery technology is also improved in order to extend the operational time of mobile devices. Besides of these developments, it is still a research question that whether symmetric and asymmetric encryption can fully provide their advantages to secure mobile SMS messages.

This survey focuses on the use of different encryption techniques to secure SMS messages. The performance of different encryption schemes, i.e., symmetric encryption, asymmetric encryption and One-Time-Pad (OTP) encryption on modern mobile devices is evaluated and presented. The effect of encryption schemes on the performance of mobile devices and SMS message is also discussed. For this purpose, literature review of latest security mechanisms used for mobile SMS messages is conducted. The existing security schemes used for SMS message is studied and compared based on their security characteristics. The literature review of current security mechanisms used for SMS messages is conducted from

Volume: 05, Issue: 02, Pages:1873-1882 (2013) ISSN : 0975-0290

the last decade. The most common encryption techniques are discussed and evaluated in second section and conclusion is presented at the end.

2. OVERVIEW OF SMS SECURITY ALGORITHMS

2.1 DES

Data Encryption Standard (DES) is considered as most commonly used symmetric encryption algorithm. DES apply 56-bit key to any 64-bit data block using Fiestel approach. It involves 16 rounds. DES security has become weak, because of many attacks that make it insecure [11].

Hao Zhao, Sead Muftic [12] implemented a new secure mobile wallet application using J2ME for convenience and security of financial mobile transactions performed by the subscribers. AES and DES are used as an encryption methods and SHA-1,2 are used to generate hashes/keys for authentication purpose. Separate authentication module, i.e., PIV is implemented as a separate java card applet to provide authentication service to all subscribers.

Harb [13] has used symmetric and asymmetric cryptography to develop secure mobile payment application model. It is suitable for online payment/ transactions; provides security with minimum cryptography keys and less encryption operations. SMS is used as a transport channel in order to send transactions to payer. 3DES session key is used to secure SMS communication b/w customer and bank. J2ME application generates encrypted SMS having payer's confirmation and sends it to payer's bank. Payer's bank will decrypt SMS and send payee's mobile number to PG.

D.B. Ojha [14] has found that many attacks affect the security of DES algorithm. They evaluated different attacks on DES i.e., brute force attack, meet-in-the middle attack and used Linear and differential cryptanalysis to increase efficiency of DES. The proposed approach used single 64-bit key for encryption/decryption in DES. It behaves like a One-time pad for each block. It is found that their technique improves the security and efficiency of DES against many attacks, e.g., meet-in-the middle attack etc.

2.2 AES

Advance Encryption Standard (AES) is a symmetric encryption scheme established as a DES successor. AES is a block cipher with block length of 128 bits, and key size of 128,192, and 256 bits. The round transformation in AES is composed of byte substitution, shift rows, mix columns and add round key steps. AES has been broken by Brute-force attack and many algebraic attacks [15].

Johnny Li-Chang Lo [16] proposed a new protocol, i.e., SMSSec to secure end-to-end SMS communication and guarantee the integrity of message content in mobile commerce. Two separate handshakes, i.e., first and nth handshake are utilized to use symmetric and asymmetric encryption techniques respectively. RSA and AES are used for encryption whereas HMAC is used for authentication and keys generation. SMS efficiency is measured by sending a number of different SMS messages between different mobile devices. Many issues have taken place for 1st handshake e.g., short length SMS. uses of AES encryption for such SMS is not suitable. It is found that nth handshake is more efficient since it uses two SMS messages, whereas 1st handshake takes three messages. After handshakes, encrypted communication is done using one SMS message.

Hassan Mathkour [17] proposed a new system, i.e., Secret Short Message Service (SSMS) to secure SMS messages transmission on mobile network. Their system can also protect the private data saved on mobile phone. AES-Rijndeal is used to perform encryption. Secret key is embedded in cipher text using hash. It is used to encrypt SMS message. Message decryption also uses the same secret key. Encrypted secret key is used for encryption and decryption. Bouncy-Castle J2ME cryptographic library is used for encryption with SHA-1.

K. Singh [18] developed a new peer-to-peer Android application to secure the SMS-based communication between users. Deffie-Hellman key exchange mechanism is used to exchanging keys at both sides i.e., sender and receiver. AES (Advance encryption standard) is used to encrypt and decrypt messages at sender and receiver. After it, SMS is being sent to the receiver. Receiver will receive the message and decrypt it using AES. Built-in Java libraries are used for AES encryption and decryption with 128 bit key.

2.3 BlowFish

It is a symmetric block cipher that is used to encrypt and secure the data. The key size of Blow Fish ranges from 32 bits to 448 bits. It is license-free and free to use for all users. It uses Fiestel cipher and S-boxes with XOR operation in all 16 rounds. The problem of Blow Fish algorithm is that it has weak keys. Blow Fish remained successful against many attacks but extra computational effort is required against dictionary attacks [19].

Aditee Gautam [20] proposed a block based transformation algorithm in order to transfer and encrypt images in the form of blocks without losing any information. It will reproduce the original image without losing any information. The transformation process consists of dividing image into blocks to create a new image. This image is passed on to Blow-fish encryption algorithm in order to perform encryption.

Neetesh Saxena [21] proposed a new approach to provide SMS security using encryption and digital signatures. Firstly, message is encrypted then digital signature is applied on the encrypted message. DES, AES, DSA, and RSA are used respectively in order to encrypt SMS

Volume: 05, Issue: 02, Pages:1873-1882 (2013) ISSN : 0975-0290

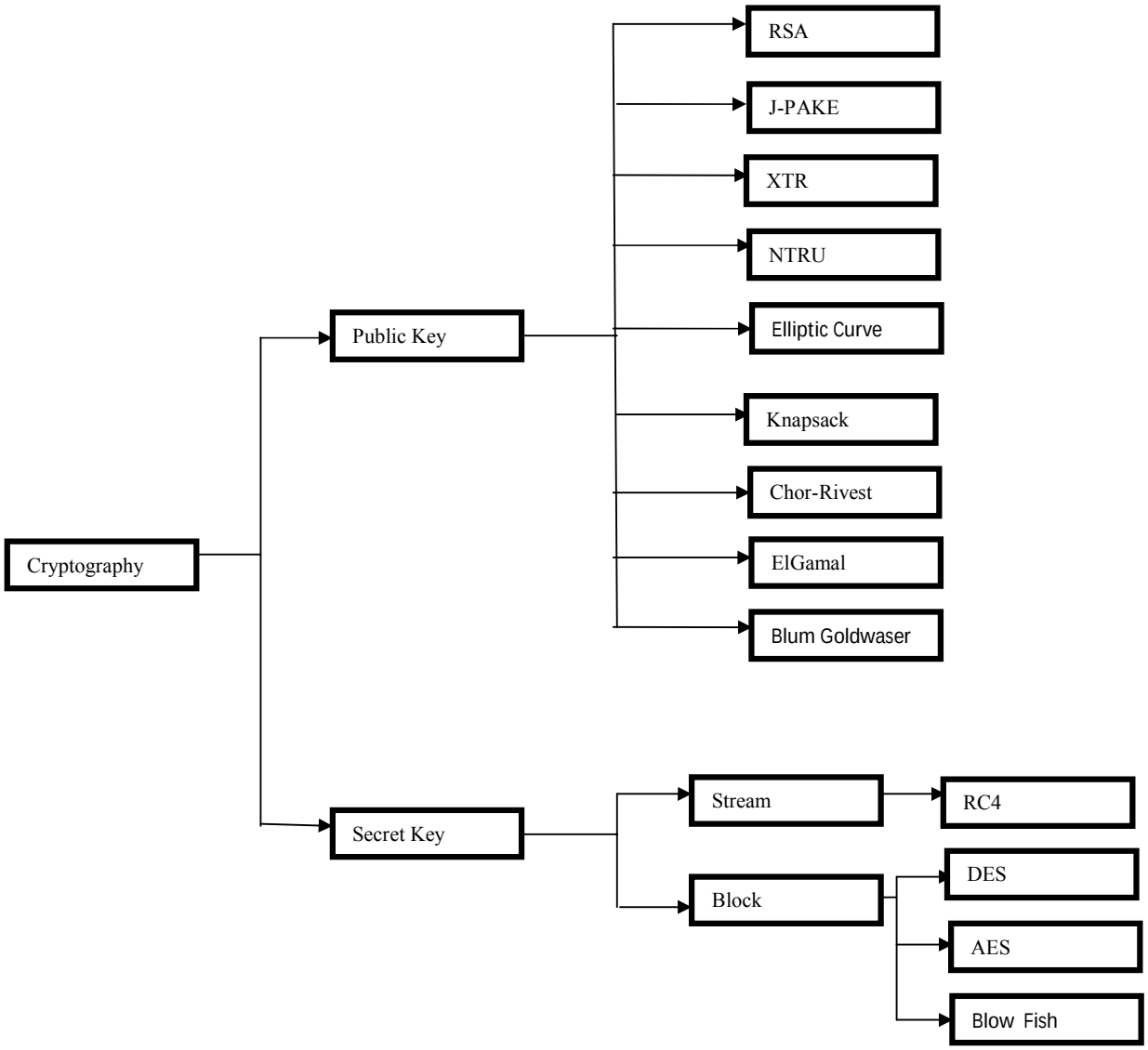

Fig 1.0 Overview of the SMS Security Algorithms

message. Signature generation uses hash function to get message digest. DSA signature method is used to verify signatures. DES, Triple-DES, AES and Blowfish algorithms are implemented and AES is found to take less encryption/decryption time.

2.4 RSA

Rivest-Shamir-Adleman (RSA) is one of the most commonly used public key encryption scheme used to encrypt blocks of data. RSA uses encryption keys of variable sizes. The key is derived from the product of two prime numbers. Attacker can't get the prime number of keys which makes it more secure to use. Modular exponentiation operation is used in RSA for encryption. Many attacks remain successful against RSA including chosen plain-text attack and chosen cipher-text attacks [22], [23].

Marko Hassinen [24] has used RSA algorithm to encrypt SMS messages used in mobile commerce, whereas keys are generated using SHA-1. Private keys are restricted to mobile devices. Authentication Server will then generate certificates for public keys. Lightweight Directory Access Protocol (LDAP) database is used to store/retrieve those certificates. These certificates are further used by mobile user to exchange encrypted SMS messages.

Er. Kumar Saurabh [25] proposed a new method for node's authentication in wireless sensor networks using RSA. RSA algorithm is applied into source node, intermediate node, and destination node. Proposed algorithm generates private and public keys. Then cipher-text is created, which is encrypted using public key. Private Key is sent to the receiver. After encryption, packet is sent to intermediate node, which sends it to the destination node. Destination node will finally decrypt it using private key. Analysis of scheme is conducted in

Volume: 05, Issue: 02, Pages:1873-1882 (2013) ISSN : 0975-0290

Matlab, and results shows that technique is effective in terms of energy efficiency and data transfer.

David Lisoněk [26] proposed an application to encrypt SMS messages using asymmetric RSA cipher. OAEP padding scheme is used to avoid RSA from dictionary attacks. Private keys are stored in the application, whereas public keys are stored in mobile's memory. Symbian OS is used as a programming environment since it requires less computational power. Key generation operation is tested on Nokia N80 by subtracting the actual start time of key generation from its final time. Analysis of several attacks on application is also conducted at the end.

Alfredo De Santis [27] proposed a secure extensible and efficient SMS (SEESMS) application framework which allows two mobile peers to exchange encrypted SMS message in an efficient manner by selecting their level of security. ECIES and RSA are used for encryption. RSA, DSA, and ECDSA signatures are also used to validate contacts. After being registered with SEESMS on mobile, keys are exchanged b/w users to transmit secure SMS using HMAC. Users will then select energy efficient cryptosystem, encrypt SMS using it, and send to the receiver. Comparison of RSA, DSA, and ECDSA is conducted on the basis of energy efficiency on N95 mobile. RSA and DSA are found better than ECDSA.

Neetesh Saxena [28] has analyzed and compares different digital signature methods, i.e., DSA, RSA, and ECDSA using Java. The experiments are conducted on PC to check encryption performance of all three algorithms. Results of RSA, DSA, and ECDSA are shown on the basis of their key generation execution time, signature generation, and signature verification time. It is found that SHA-1 provides better security and ECDSA is better than DSA in signature generation and verification. Results have shown that proposed ECDSA performs better than simple ECDSA.

2.5 Elliptic Curve

Elliptic curve cryptography (ECC) is a new method of public key cryptography. It is based on the algebraic structure of elliptic curves over finite fields. It has a smaller key size of 256 bit. It provides same security as RSA with this smaller key size, whereas RSA requires 3072-bit public key to achieve same security. Key size of ECC is twice of its security parameter [29].

Mary Agoyi [30] has presented an evaluation of RSA, ELGamal, and Elliptic Curve encryption techniques on the basis of their encryption/decryption time. After testing application on ARM9 processor mobile phone, it is found that key generation time of elliptic curve is less as compared to other two schemes. Encryption time of ELGamal is found to be larger whereas decryption time of all schemes is almost equal. Finally, Elliptic Curve is suggested as most cost effective algorithm since it uses small key size to offers high security as compare to RSA and ELGamal.

Basar Kasim [31] proposed a new Elliptic Curve Cryptography (ECC) based GSM security protocol. Deffie-Hellman is used to produce share secret keys. Authentication and Key distribution is conducted in a new VLR area of mobile device. Shared Deffie-Hellman key is used in this process. Correct signed response and encryption process is based on correct ECDH secret key. Shared secret key is also used in end-to-end mobile user security protocol. ECC is good in speed and efficiency. It ensures that user's private parameters are secure in SIM card.

2.6 ElGamal

ElGamal is a public key encryption algorithm based on Deffie-Hellman key exchange mechanism. It is currently used in GNU privacy guard software, and PGP. ElGamal encryption consists of three steps, i.e., key generation, encryption, and decryption. Security of ElGamal depends on the computation of discrete logs. The only demerit of ElGamal is that the length of cipher text is same as plain text but one plain text can generate different cipher texts each time it is encrypted by ElGamal. It is mostly used in hybrid cryptosystems. Brute force attack and meet-in-the middle attack try to make ElGamal insecure [32].

Myungsun Kim [33] used El-Gamal encryption scheme to decompose extension fields. It is also used to decompose the public key using El-Gamal Encryption method. It helps to reduce multiple cipher-texts without losing any information. El-Gamal encryption scheme consists of Key-generation, Encryption, and decryption. Private and public keys are generated in Key-gen step. Encoding and encryption of plaintext is done in next step. Finally, shared secret key is defined for receiver and message is decrypted using that shared key.

2.7 Blum Goldwasser

It is an asymmetric and probabilistic key encryption algorithm with a fixed size cipher text. It uses XOR based stream cipher and Blum Blum Shub (BBS) pseudo-random number generator to generate keys. It uses integer factorization for key generation process. It is also very efficient in storage since cipher text's size remain constant for any message. It consists of key generation, message encryption, and message decryption. XOR and BBS are used in encryption/decryption process. It is found that it is more efficient than RSA [34].

Aldrin W. Wanambisi [35] developed a new encryption mechanism, i.e., Probabilistic Data Encryption Scheme (PDES). It combines the security of Blum-Goldwasser and probabilistic scheme with efficiency of deterministic scheme. They used Quadratic-Residue generator as a pseudorandom number generator. Key-generation, Encryption, and decryption processes used Blum-Goldwasser algorithm. Statistical analysis of scheme is conducted and it is found that if the numbers of bits are very small then cipher text will become vulnerable to attacks.

2.8 KnapSack

Knapsack encryption is also known as first practical asymmetric encryption scheme. It uses Merkle-Hellman knapsack encryption scheme since other schemes are

Volume: 05, Issue: 02, Pages:1873-1882 (2013) ISSN : 0975-0290

proven to be insecure. It is based on subset-sum problem in mathematics. Two keys, i.e., private and public are required for communication. It is one-way, i.e., public key is used for encryption, whereas private key is used for decryption. Keys are generated using prime numbers, and extended Euclidean algorithm is used in order to decrypt messages. Many attacks including Shamir, Brickell, and Odlyzko broke it and make it insecure [36].

Baocang Wang [37] proposed a new probabilistic knapsack based public key encryption system, whereas cipher text is nonlinear to plaintext. It consists of key generation, encryption, and decryption. Deffie-hellman key exchange mechanism is used in order to generate keys. Encryption algorithm choose index vector in order to perform encryption. Decryption is performed after it. Modular multiplication is used in encryption/decryption. Security analysis is conducted using brute force attack, low density attack, and various other attacks on the system.

2.9 Chor-Rivest

It is a public key encryption algorithm like knapsack systems. It also uses the concept of subset sum problems. It is found that it take longest time to break because of efficient usage of finite fields. It uses abstract algebra in its encryption process, which make it stronger. Firstly, it creates a finite field, and computes discrete logarithms, then generates private and public keys. It doesn't use modular multiplication to solve an easy subset-sum problem. Public key is found to be very large in this scheme.

Serge Vaudenay[38] proposed a technique to break Chore-rivest cryptosystem. It is found that it takes a longer time to break. It produces the private and public keys with the help of discrete logarithms, and random integer. Knapsack based encryption method is used for encryption. Schnorr-Horner attack is considered, and Lenstra's conjectures is solved which is a problem for above attack. It is helpful in making discrete logarithmic problem quite easy.

2.10 NTRU

NTRU encryption scheme is a lattice-based public key cryptosystem which offers high speed key creation, encryption, and decryption. It is very famous in electronics industry. Polynomials are used in order to generate key pair. Modular operation is used to encrypt messages using encryption keys. Brute Force attack and meet in-the-middle attacks are solved by NTRU. Lattice reduction and chosen cipher text attacks have broken the NTRU. It is still secure to many attacks but there is a tradeoff between performance and security which make it vulnerable [39].

Sameer Hasan Al-Bakri [40] proposed a P2P public key cryptography in order to secure mobile communication. It provide authentication, confidentiality, and integrity needed for mobile devices. NTRU is used for public key cryptography. It performs key generation, encryption, and decryption. It is found that NTRU provide same security as compared to RSA. Key exchange is done using deffie-hellman mechanism. Encryption is then performed using AES-Rijnadeal algorithm because it holds less NTRU keys. Encrypted messages are then exchange between mobile users.

2.11 J-PAKE

Password authenticated key exchange by juggling (J-PAKE) is a password authenticated key agreement protocol. It doesn't require any public key infrastructure and allows two devices to start communication based on their shared passwords. It executes in two rounds, in first round two parties verify zero-knowledge proofs, and in second round, keys are generated using hash function. It avoids off-line and on-line dictionary attacks.

Feng Hao[41] has found that problem of develop secure communication between two parties without PKI is still unsolved. They proposed Password authentication key exchange by juggling (J-PAKE). It is able to done mutual authentication in two steps. Firstly, two parties will exchange public keys; secondly, they encrypt the shared password using juggling method by juggling the public keys. Juggling technique will solve the PAKE problem. It protects from offline dictionary attacks. It also protects the users from cracking their password.

2.12 XTR

ECSTR (XTR) is a new algorithm used for public key encryption. It uses the field trace to represent elements of a subgroup of a multiplicative group of a finite field. It solves the discrete logarithm related problems to secure encryption process. It uses XTR subgroup which consists of many arithmetic operations. The applications of XTR are Deffie-Hellman key agreement and ElGamal Encryption.

Arjen K. Lenstra proposed a new XTR based public key system in order to reduce communication and computational overhead without affecting the security. XTR-DH, XTR-ElGamal, and XTR-NR signature scheme is presented in the paper. XTR is able to solve discrete logarithm related problems. Finite field and subgroup size is selected in order to provide efficient security. After it subgroup selection is conducted. XTR is currently using in Deffie-Hellman key agreement and ElGamal encryption. [42]

Ashok Kumar Nanda [43] proposed XTR-NR signature algorithm to increase security, speed, and reliability of SMS message. Encryption is performed on data block having two parts of equal length, cryptographic check function (CCF) is used to append digital signature with SMS message. After encoding, message is transfer on noisy channel, at receiver end, firstly channel decoding is performed, segmentation of message into two parts is done, and finally it gets SID with feedback of two blocks. Correction is performed using feedback in order to correct decoding process.

Volume: 05, Issue: 02, Pages:1873-1882 (2013) ISSN : 0975-0290

Table 1. General Summary

Sr#	Technique Name	Advantages	Limitations
1.	**RSA** [22],[25]	• It provides Strong Security • It is easy to use • It kepts Non-repudiation • It uses Strong Random Number Generation	• It has slow speed • It becomes the victim of Impersonation • Encrypted data size is very Large
2.	**J-PakE** [42],[60]	• It has Zero Knowledge proof of password • Key Exchange mechanism is authenticated • It provides Explicit key confirmation • It provides resistance to Off-line dictionary attack • It kept the property of Forward secrecy	• It is Computationally expensive
3.	**XTR** [43],[59]	• Key generation/selection is very fast • It has Low Computational cost • The Encryption/Decryption is Fast in XTR. • It has Small Key size • It offers Strong security • It provides Fast signature verification • Parameter generation is also easy and fast	• The Size of P^6 scales sub-exponential • Public key size of XTR is greater than ECC • It is Vulnerable to Side channel attacks
4.	**NTRU** [53],[41],[55]	• It Uses less Resources (e.g., battery, CPU etc) • It is Smallest public key cryptosystem • It is Ideal for embedded device • It is 200x times faster than ECC and RSA • It uses Less memory • String security	• Decryption process in NTRU is slow than DES
5.	**Elliptic Curve** [29],[32],[31]	• It has Strong shorter keys • It has Low CPU Consumption • It uses Less Memory • consume less storage space	• It involves Complicated Group Operations • It need pre-computed tables
6.	**Knapsack** [36],[37],[57]	• It is Simple • It is One-way, i.e., public key is only used for encryption. • It uses Trap-door function • It is Transparent • It has a Good Speed	• It is Polynomial time breakable • It is Less Secure • It is Easily breakable
7.	**Chor-Rivest** [38],[39]	• It has Easy implementation • It is Difficult to break	• It has Large size public keys • It has Long key generation time • It has Slow Decryption process
8.	**BlumGoldwasser** [34],[35]	• It is Semantically secure • It uses Storage apace Efficiently • It provides Efficient Computation • It is Efficient for Large cipher texts	• It is Vulnerable to cipher attacks • It is Computationally insecure • Computation is Expensive

Volume: 05, Issue: 02, Pages:1873-1882 (2013) ISSN : 0975-0290

9.	**ElGamal** [32],[33]	• It is Randomized Cryptosystem • It has Smaller key sizes • It uses Semantic security • It has the property of Non-malleability • It provides Fast Signature Generation • It offers Fast key generation • It uses Efficient Exponentiation • It provides Hardware compaction	• It has Large message expansion • Signature verification is expensive • It has Expensive group parameter generation
10.	**Blow Fish** [19],[29],[57], [58]	• It has Good Key Strength • It has Good Speed • It is Unpatented • It is Licence-free • It has Efficient hardware implementation • It is Freely available • It has Fast execution time • It is Energy-Efficient	• It is In-sufficient for Large files • It uses Variable-Length Key • It has Long Initialization time • It has Complicated Encryption function • It is Time Consuming • It posses Key Variation
11.	**AES** [15],[19],[17], [57], [58]	• It is Highly Efficient • It is Less Complex • It is Highly Secure • It has Good Speed • It has Low Resource Consumption • It has Low RAM requirement	• It Requires more processing • It uses More Rounds of communication • It has Complex Configuration • It is Time Consuming
12.	**DES** [11],[19],[17], [56], [58]	• It uses Single Key both for encryption and decryption • It is More Confidential • It is Useful for Authentication • It provides MAC authentication • It has Good Speed	• It has Short Length Key • Keys can be Easily broken • It has Weak Substitution Tables • It is Unsecure • It is Vulnerable to Brute-force attack • It is Key-dependent

Other SMS Security Algorithms

Marko Hassinen [44] proposed an application to send encrypted SMS messages using quasi-group encryption method. Application can encrypt full length SMS message of 160 characters using 16 rounds of encryption. It contains Java midlet classes to implement encryption in Nokia and Siemens mobiles. Nokia application can receive and decrypt the SMS message, but Siemens application has to store SMS in the mobile's inbox from where application can encrypt/decrypt the message. Results show that application requires less mobile memory and limited power requirements.

N.J Croft and M.S Olivier [45] proposed 'Approximated One-Time Pad' to secure SMS communication in GSM environment. 'One-time pad' fulfills all the requirements of a typical encryption algorithm. However, a random pad computation, i.e., a random key generation is required both at MS (Mobile Station) and GSM network in order to encrypt SMS message. Encryption of the message is done by XORing each of the seven data segments of message with the approximated one-time pad. This will generate a 160-bit block of cipher text.

Xinhua Zhang [46] presented a mobile e-commerce system using J2ME. Java servlet programming (JSP) with XML is used to process client's requests and sends back the response to them. E-commerce system is divided into application, business logic, and data layers. Four features are considered in order to realize three layers for developed application, i.e., control flow, interface display, connection with server, and encapsulation with resolution of XML message format.

Jongseok Choi and Howon Kim [47] have found two issues related to SMS security, i.e., national laboratories are monitoring the messages of selected users, and, SMS can't use two-way communication because these will double the cost. A common public key cryptography for SMS security is presented to solve the above two issues. SMS-gateway is used as third party tool to send/receive messages among mobile devices. They claim that attacker can't get the gateway's secret and decryption keys in order to extract the plain text of message.

Mazen Tawfik [48] has found that low performance and weak encryption are two problems of Pretty Good Privacy (PGP) algorithm. They proposed a new cryptographic system based on chaotic encryption system in order to make PGP more secure. It consumed less time as compared to other encryption algorithms. Padding is not use in this system. Analysis of performance is conducted in form of encryption/decryption time using C#.

Saurabh Samanta [49] has found that Short Message Peer-to-Peer protocol, which is an application layer protocol is

Volume: 05, Issue: 02, Pages:1873-1882 (2013) ISSN : 0975-0290

used to send computer generated SMS messages over TCP/IP connection is not secure and it causes loss of revenue. Author has proposed a secure SMPP protocol and developed a client application to connect to server using Transport Layer Security (TLS). In experiments, it is found that a small overhead performance cost is inducted to send messages using secure SMPP.

Nenad Gligoric [50] proposed a new hybrid solution for M2M communication over SMS, i.e., application layer security with compression. It will provide security as well as reduce the size of data. Compression is performed using GZIP [51],[52]. Finally SMS is sent to the receiver. Experiments are conducted between android mobile devices in GSM network. It is found that proposed secure framework has no effect on SMS delivery time of M2M communication over SMS.

Hatem Hamad [53] proposed a new method to encrypt MMS messages using a new secret key to secure data b/w two mobile devices. Key is generated from dynamic tolerance distance (DTD), and velocity of mobile device. Statistical analysis, key sensitivity analysis, and key space analysis experiments are performed on the proposed algorithm using dataset of cameramen image, monaliza image, and plain text. It is found that key is strong enough for encryption/ decryption process.

Joy Bose [54] provides a new method to encrypt SMS messages using accelerometer, gyroscope, and multi-touch GPS sensors. Symmetric key cryptography is used to encrypt the SMS message data. The key will be in the form of gestures made by user or it can be sensor readings, e.g., location. Encoding and decoding is performed on the basis of input gestures. Neural network is used to train the input gestures in order to use as a key for encryption/decryption process. Authors have also used XOR function to encrypt data with gestures as a key. Finally, implementation is performed on Android mobile phone.

CONCLUSION

This paper reviews the latest security schemes used for SMS message security in modern mobile devices. Performance of mobile devices depends on encryption time of a security scheme used for SMS. It is found that key generation and encryption time is increases with key size of security algorithm. Therefore, large key size algorithms, i.e., DES, AES RSA, ElGamal, and BlowFish are not suitable for SMS encryption due to low computational power of mobile devices. Elliptic Curve algorithm is therefore useful for SMS encryption since it provides high security with smaller key size. Performance analysis of all these schemes will be considered as a future work.

ACKNOWLEDGEMENTS

I acknowledge COMSATS Institute of Information Technology-Pakistan for providing me support for this work.

REFERENCES

[1] J. Brown, B. Shipman, and R. Vetter, SMS: The short message service, Computer, 40, 2007, 106-110.

[2] A. Rafat. (2006). The SMS Privacy Problem. Available: http://www.textually.org/textually/archives/2004/04/003489.htm

[3] A. G. Breed. (2006). Ubiquitous message technology can be powerful tool for good or ill. Available: http://www.tmcnet.com/usubmit/2006/10/17/1985881.htm

[4] N. Jones. (2006). Don't Use SMS for Confidential Communication, Gartner. Available: http://www.gartner.com/DisplayDocument?doc_cd=111720

[5] A. Grillo, A. Lentini, G. Me, and G. F. Italiano, Transaction oriented text messaging with Trusted-SMS, Proc. Computer Security Applications Conference, 2008, 485-494.

[6] A. J. Nicholson, I. E. Smith, J. Hughes, and B. D. Noble, Lokey: Leveraging the sms network in decentralized, end-to-end trust establishment, in Pervasive Computing, (Springer, 2006) 202-219.

[7] D. Lisonek and M. Drahansky, Sms encryption for mobile communication, Proc. Security Technology, 2008. SECTECH'08. International Conference on, 2008, 198-201.

[8] N. B. Anuar, L. N. Kuen, O. Zakaria, A. Gani, and A. W. A. Wahab, GSM mobile SMS/MMS using public key infrastructure: m-PKI, WSEAS Transactions on Computers, 7, 2008, 1219-1229.

[9] M. Sharif, T. Faiz, and M. Raza, Time signatures-an implementation of Keystroke and click patterns for practical and secure authentication, Proc. Third International Conference on Digital Information Management, 2008. ICDIM 2008, 559-562.

[10] M. Raza, M. Iqbal, M. Sharif, and W. Haider, A Survey of Password Attacks and Comparative Analysis on Methods for Secure Authentication, World Applied Sciences Journal, 19, 2012, 439-444,.

[11] F. I. P. S. Publication, Data Encryption Standard, 1993.

[12] H. Zhao and S. Muftic, Design and implementation of a mobile transactions client system: Secure UICC mobile wallet, International Journal for Information Security Research, vol. 1, 2011, 113-120.

[13] H. Harb, H. Farahat, and M. Ezz, SecureSMSPay: secure SMS mobile payment model, Proc. 2nd International Conference on Anti-counterfeiting, Security and Identification, 2008. ASID, 2008, 11-17.

[14] D. Ojha, R. Singh, A. Sharma, A. Mishra, and S. Garg, An Innovative Approach to Enhance the Security of Data Encryption Scheme,

Volume: 05, Issue: 02, Pages:1873-1882 (2013) ISSN : 0975-0290

International Journal of Computer Theory and Engineering, vol. 2, 2010, 1793-8201.

[15] N.-F. Standard, Announcing the Advanced Encryption Standard (AES), Federal Information Processing Standards Publication, vol. 197, 2001.

[16] J. L.-C. Lo, J. Bishop, and J. H. Eloff, SMSSec: an end-to-end protocol for secure SMS, Computers & Security, vol. 27, 2008, 154-167.

[17] H. Mathkour, G. Assassa, A. Al-Muharib, and A. Juma'h, A Secured Cryptographic Messaging System Proc. International Conference on Machine Learning and Computing (ICMLC), 2009.

[18] A. Singh, S. Maheshwari, S. Verma, and R. Dekar, Peer to Peer Secure Communication in Mobile Environment: A Novel Approach, International Journal of Computer Applications, vol. 52, 2012 24-29.

[19] J. Thakur and N. Kumar, DES, AES and Blowfish: Symmetric Key Cryptography Algorithms Simulation Based Performance Analysis, International Journal of Emerging Technology and Advanced Engineering, 1(2), 2011, 6-12.

[20] A. Gautam, M. Panwar, and D. P. Gupta, A New Image Encryption Approach Using Block Based Transformation Algorithm, International Journal Of Advanced Engineering Sciences And Technologies, 2010, 090-096.

[21] N. Saxena and N. S. Chaudhari, A secure approach for SMS in GSM network, Proc. CUBE International Information Technology Conference, 2012, 59-64.

[22] S. Sharma, J. S. Yadav, and P. Sharma, Modified RSA Public Key Cryptosystem Using Short Range Natural Number Algorithm, International Journal, vol. 2, 2012.

[23] Farrukh Saleem, Muhammad Sharif, Aman Ullah Khan, An Efficient and Secure Method for Public Key Cryptosystems, National Conference on Information Technology: Present Practices and Challenges, Asia-Pacific Institute of Management, New Delhi, India, August 31 - September 1, 2007.

[24] M. Hassinen, Java based public key infrastructure for sms messaging, Proc. 2nd International Conference on Information and Communication Technologies, 2006. ICTTA'06., 2006, 88-93.

[25] S. Singh and E. K. Saurabh, Providing Security in Data Aggregation using RSA algorithm, International Journal of Computers & Technology, vol. 3, 2012, 60-65.

[26] D. Lisonek and M. Drahansky, Sms encryption for mobile communication, Proc. International Conference on Security Technology, 2008. SECTECH'08., 2008, 198-201.

[27] A. De Santis, A. Castiglione, G. Cattaneo, M. Cembalo, F. Petagna, and U. F. Petrillo, An extensible framework for efficient secure SMS, Proc. International Conference on Complex, Intelligent and Software Intensive Systems (CISIS), 2010, 843-850.

[28] N. Saxena and N. S. Chaudhari, Secure encryption with digital signature approach for Short Message Service, Proc. World Congress on Information and Communication Technologies (WICT), 2012, 803-806.

[29] G. S. I. Blake, and N. Smart, Ed., Advances in Elliptic Curve Cryptography (London Mathematical Society,Cambridge University Press 2005).

[30] M. Agoyi and D. Seral, SMS security: an asymmetric encryption approach, Proc. 6th International Conference on Wireless and Mobile Communications (ICWMC), 2010, 448-452.

[31] B. Kasim and L. Ertaul, GSM SECURITY II, 2005.

[32] K. Rabah, Elliptic curve elgamal encryption and signature schemes, Information Technology Journal, vol. 4, 2005, 299-306.

[33] M. Kim, J. Kim, and J. H. Cheon, Compress Multiple Ciphertexts using ElGamal Encryption Schemes, J. Korean Math. Soc, vol. 50, 2013, 361-377.

[34] M. Blum and S. Goldwasser, An efficient probabilistic public-key encryption scheme which hides all partial information, in Advances in Cryptology, 1985, 289-299.

[35] A. W. Wanambisi, C. Maende, G. M. Muketha, and S. Aywa, A Probabilistic Data Encryption scheme (PDES), Journal of Natural Sciences Research, vol. 3, 2013, 21-26.

[36] A. Agarwal, Encrypting Messages using the Merkle-Hellman Knapsack Cryptosystem, IJCSNS, vol. 11, 2011, p. 12.

[37] B. Wang, Q. Wu, and Y. Hu, A knapsack-based probabilistic encryption scheme, Information Sciences, vol. 177, 2007, 3981-3994.

[38] S. Vaudenay, Cryptanalysis of the Chor-Rivest cryptosystem, Advances in Cryptology—CRYPTO'98, 1998, 243-256.

[39] H. Sakshaug, Security Analysis of the NTRUEncrypt Public Key Encryption Scheme, Department of Mathematical Sciences, Norwegian University of Science and Technology, 2007.

[40] S. H. Al-Bakri, M. M. Kiah, A. Zaidan, B. Zaidan, and G. M. Alam, Securing peer-to-peer mobile communications using public key cryptography, New security strategy, International Journal of the Physical Sciences, vol. 6, 2011, 930-938.

[41] F. Hao and P. Y. Ryan, Password authenticated key exchange by juggling: Springer, 2011.

[42] A. K. Lenstra and E. R. Verheul, The XTR public key system, in Advances in Cryptology—CRYPTO 2000, 1-19.

[43] A. K. Nanda and L. K. Awasthi, Joint Channel Coding and Cryptography for SMS, Proc.

Volume: 05, Issue: 02, Pages:1873-1882 (2013) ISSN : 0975-0290

International Siberian Conference on Control and Communications (SIBCON), 2011, 51-55.

[44] M. Hassinen and S. Markovski, Secure SMS messaging using Quasigroup encryption and Java SMS API, vol. 3, 2003, 18,.

[45] N. J. Croft and M. S. Olivier, Using an approximated one-time pad to secure short messaging service (SMS), Proc. Southern African Telecommunication Networks and Applications Conference. South Africa, 2005.

[46] X. Zhang, Design of mobile electronic commerce system based on J2ME, Proc. International Conference on Electronic Computer Technology, 2009, 706-709.

[47] J. Choi and H. Kim, A Novel Approach for SMS Security, International Journal of Security and Its Applications, vol. 6, 2012, 373-378.

[48] M. T. Mohammed, A. E. Rohiem, A. El-moghazy, and A. Ghalwash, Chaotic Encryption Based PGP Protocol, 2013.

[49] S. Samanta, R. Mohandas, and A. R. Pais, Secure Short Message Peer-to-Peer Protocol, International Journal of Electronic Commerce, vol. 3, 2012.

[50] N. Gligoric, T. Dimcic, D. Drajic, S. Krco, and N. Chu, Application-layer security mechanism for M2M communication over SMS, Proc. Telecommunications Forum (TELFOR), 2012, 5-8.

[51] Q. Naeem, M. Sharif, and M. Raza, "Improving audio data quality and compression," in Emerging Technologies, 2008. ICET 2008. 4th International Conference on, 2008, pp. 332-337.

[52] Rana Muhammad Nazim, Muhammad Sharif, Mudassar Raza, Aman Ullah Khan, Layered Compression Technique (LCT) Based on Entropy or Dictionary Methods, The First International Conference on Computer, Control & Communication (IC4), organized by Pakistan Navy Engineering College (PNEC), a constituent college of National University of Sciences & Technology (NUST), in collaboration with IEEE Karachi Sector, Higher Education Commission (HEC) and Pakistan Council of Scientific and Industrial Research (PCSIR), November, 2007 at PNEC, Karachi, Pakistan, 12-13

[53] H. Hamad and S. El Kourd, Key strength with encryption and dynamic location of mobile phone, Proc. 6th International Conference on Sciences of Electronics, Technologies of Information and Telecommunications (SETIT), 2012, 468-473.

[54] J. Bose and T. Arif, Encryption in mobile devices using sensors, Proc. Sensors Applications Symposium (SAS), IEEE, 2013, 55-60.

[55] S. Sharma, J. S. Yadav, and P. Sharma, Modified RSA Public Key Cryptosystem Using Short Range Natural Number Algorithm, International Journal, vol. 2, 2012.

[56] R. Kaur and V. Banga, Image Security using Encryption based Algorithm, Proc. International Conference on Trends in Electrical, Electronics and Power Engineering (ICTEEP'2012) 15-16.

[57] M. Kiah and M. Laiha, A novel peer-to-peer SMS security solution using a hybrid technique of NTRU and AES-Rijndael, Scientific Research and Essays, vol. 2, 2010, 3455-3466.

[58] M. Agrawal and P. Mishra, A comparative survey on symmetric key encryption techniques, International Journal on Computer Science and Engineering (IJCSE), vol. 4, 2012, 877-882.

[59] M. S. Lee, Improved cryptanalysis of a knapsack-based probabilistic encryption scheme, Information Sciences, 2012.

[60] S. P. Singh and R. Maini, Comparison of data encryption algorithms, International Journal of Computer Science and Communication, vol. 2, 2011, 125-127.

[61] A. K. Nanda and L. K. Awasthi, XTR Cryptosystem for SMS Security, International Journal of Engineering and Technology, IJET, 4(6), 2012, 1793-8244

[62] J. Katz, R. Ostrovsky, and M. Yung, Efficient password-authenticated key exchange using human-memorable passwords, in Advances in Cryptology—EUROCRYPT 2001,(Springer, 2001), 475-494.