Cryptography on Android Message Applications – A Review

Nishika
MTech Student, CSE
PDM College of Engineering
Bahadurgarh, India
ngulia5101989@gmail.com

Rahul Kumar Yadav
AP, CSE
PDM College of Engineering
Bahadurgarh, India
rahul_engg@pdm.ac.in

***Abstract*— Short Message Service (SMS) is a text messaging service component of phone, web, or mobile communication systems, using standardized communications protocols that allow the exchange of short text messages between fixed line or mobile phone devices. Security of SMS's is still an open challenging task. Various Cryptographic algorithms have been applied to secure the mobile SMS. The success of any cryptography technique depends on various factors like complexity, time, memory requirement, cost etc. In this paper we survey the most common and widely used SMS Encryption techniques. Each has its own advantages and disadvantages. Recent trends on Cryptography on android message applications have also been discussed. The latest cryptographic algorithm is based on lookup table and dynamic key which is easy to implement and to use and improve the efficiency. In this paper, an improvement in lookup table and dynamic algorithm is proposed. Rather than using the Static Lookup Table, Dynamic Lookup Table may be used which will improve the overall efficiency.**

Keywords*- *SMS, AES, DES, Blowfish, RSA, 3DES, LZW.

I. Introduction

Communication is a better way to exchange the feelings, ideas and expression. It is the activity of conveying information through the exchange of thoughts, messages, or information, as by speech, signals, writing, or behavior. Communication involves a sender and a receiver conveying information through a communication channel. Sender and receiver are the most important part of communication. There are various methods for communication [1]. Verbal communication includes text messages, presentations and discussions. Non Verbal communication includes gestures and eye-contact.

SMS Message Service (SMS) is a textual form of communication which is of precise length. It falls under the category of verbal communication [1]. SMS's are very much in use. So it is must to secure SMS's. There are various methods to secure SMS. One of them is cryptography.

Cryptography has always been an important task. The main goal of every cryptographic activity is Data Security (e.g. "hiding messages from unauthorized eyes"). Cryptography encodes messages in such a way, that only the sender and the receiver can understand it. Today, cryptography has its place not only in the army, but also in the civilian sector. With the upcoming mainframe computers in the seventies and with the personal computers in the eighties, cryptography has become available to everyone. Nowadays an ordinary PC can produce codes of such complexity, that the most powerful supercomputer, using the best available attack algorithms, would not break it in millions of years. Cryptography is used to secure telephone, internet, and email communication and to protect software and other digital property. First thing that is really needed in order to do cryptography (e.g. encryption, decryption) is a cryptographic algorithm. There are algorithms that could be used by hand. Today, many cryptographic algorithms are available like RSA, DES, 3DES, Blowfish, AES are just the names of a few. Cryptographic algorithms, also called Ciphers are classified as either symmetric or asymmetric.

A. Symmetric Ciphers

Classical (symmetric) algorithms, such as DES, are based on a common secret key for both, encryption and decryption. This is the reason why this scheme is also called "Secret-Key". Their strengths include especially fast encryption/decryption

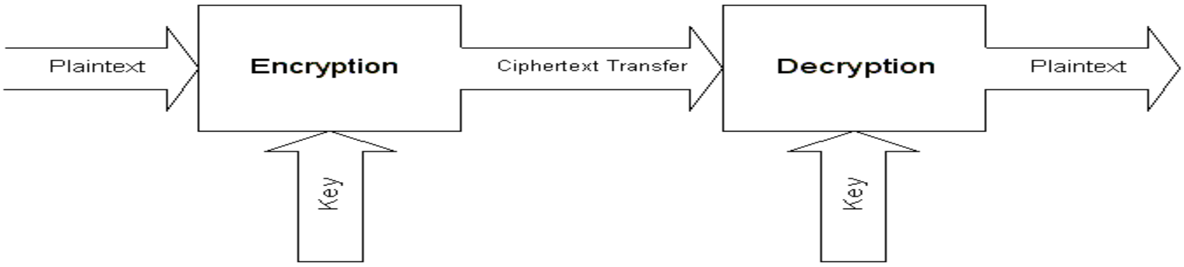

Figure 1. Symmetric Ciphers

B. Asymmetric Ciphers

Such a scheme is also called a “Public-Key”-Scheme, because the encryption key is made public. This way, a complete stranger can use the encryption key to encrypt a message, but only someone with the corresponding decryption key can decrypt the message. The encryption key is called the Public Key, and the decryption key is called the Private Key.

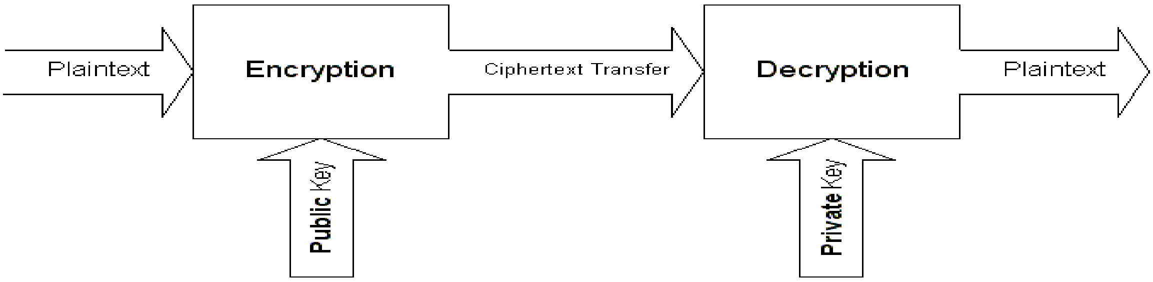

Figure 2. Asymmetric Ciphers

II. LITERATURE SURVEY

In year 2008, David Lisonek et al., [20] proposed an algorithm to send message through GSM using an asymmetric Rivest, Shamir and Adleman (RSA) cipher. This application prevents taping and substituting techniques to secure SMS. It is achieved by storing the public key in a certificate which can be signed by the certification authority.

In year 2008, S. H. Shah Newaz et al., [19] proposed scheme for the enhancement of SMS security system for GSM users. SafeSMS has two methods for encrypting via Quasigroup and Blowfish Thereby, incorporating digital signature over cipher which is converted so by existing encryption schemes is made compatible to GSM security infrastructure. Encryption can be done with the existing GSM encryption algorithm, called A8. Then the encrypted message will create hash and finally it will be digitally signed. Thus, signed encrypted message will be transmitted.

In year 2008, Marko Hassinen [18] provided application solution named “Safe SMS”, using java for achieving confidentiality, integrity and authentication in SMS without any additional hardware for ensuring message is not tempered and authenticates sender.

In year 2009, Ch. Rupa et al., [17] proposed accost effective scheme which uses a concept called Cheating Text. The original message is embedded in a meaningful text cheating text. Here, index table called (Real Message Index File) RIF file is hashed and sent to the receiver along with the cheating text in which the original message is embedded. Authentication is achieved by verifying the hash value of the plain text.

In Year 2010, Machigar Ongtang [16] performed a work, “Porscha: Policy Oriented Secure Content Handling in Android”. In this paper, Author explores the requirements and enforcement of digital rights management (DRM) policy on smart phones. An analysis of the Android market shows that DRM services should ensure: a) protected content is accessible only by authorized phones b) content is only accessible by provider-endorsed applications, and c) access is regulated by contextual constraints, e.g., used for a limited time, a maximum number of viewings, etc.

In 2010, Mary Agoyi et al., [15] evaluated encryption and decryption time for three algorithms RSA, Elliptic-curve and EIGamal to which plain text of different sizes is provided based on results one is chosen for further encryption. Their performance evaluation in securing SMS shows thet key generation, encryption and decryption time increases with an increase in the key size: Large key size algorithms are not suitable for SMS encryption due to small memory and low computational power of mobile phones.

In Year 2011, Mark H. Goadrich [13] performed a work, “Smart Smartphone Development: iOS versus Android”. In a remarkably short timeframe, developing apps for smartphones has gone from an arcane curiosity to an essential skill set. In this paper, Author will compare the two, and address the question: which should faculty teach?

In Year 2011, Nathaniel Husted [12] performed a work, “Smartphone Security Limitations: Conflicting Traditions”. Presented paper looks at these fundamental limitations and how they relate to the challenge of reconciling governance practices in use on general purpose computers and mobile phones. Author also provides certain policy guidelines and platform architecture suggestions that will help create a more secure smart phone platform.

In year 2011, Na Qi Jink Pan Qun Ding [12] did improvements on RSA algorithm because the SMSC will filter out the characters which are out of prescribed limit, thus the cipher text can’t reach the destination. Thus, they also used FPGA based on high speed processing tools to implement the RSA algorithms and apply it in mobile phone short message encryption system.

In Year 2012, Rohan Rayarikar [10] performed a work, “SMS Encryption using AES Algorithm on Android". Author has developed an application on Android platform which allows the user to encrypt the messages before it is transmitted over the network. Author has used the Advanced Encryption Standards algorithm for encryption and decryption of the data. This application can run on any device which works on Android platform. This application provides a secure, fast, and strong encryption of the data.

In Year 2012, Manisha Madhwani[1] performed a work, “Cryptography on Android Message Application Using Look up Table and Dynamic Key (Cama)”. In this paper Author propose an efficient algorithm for cryptography which is based on static Look Up table and Dynamic Key. Symmetric encryption and decryption is used in this algorithm. The proposed algorithm is more secure and simple to implement. This application makes use of built in android Intents and SMS Manager to send and receive messages

In year 2012, Mohsen Toorani et al., [2] provided the introduction of new Secure SMS Messaging Protocol (SSMS) for the Mobile-Payment systems. It being an application-layer protocol is intended for GSM users as a secure bearer in the mobile payment systems. It uses elliptic curve-based public key solution which uses public key as secret key for symmetric encryption.

In Year 2012, Bhaskar Sarma [3] performed a work, “Android Permissions: A Perspective Combining Risks and Benefits”. In this paper, Author investigate the feasibility of using both the permissions an app requests, the category of the app, and what permissions are requested by other apps in the same category to better inform users whether the risks of installing an app is commensurate with its expected benefit. Author proposes several risk signals that and evaluate them using two datasets, one consists of 158,062 Android apps from the Android Market, and another consists of 121 malicious apps. Author demonstrates the effectiveness of presented proposal through extensive data analysis.

In Year 2012, Adrienne Porter Felt [4] performed a work, “Android Permissions: User Attention, Comprehension, and Behaviour”. Author performed two usability studies: an Internet survey of 308 Android users and a laboratory study wherein Author interviewed and observed 25 Android users. Author present recommendations for improving user attention and comprehension, as well as identify open challenges.

In Year 2012, Liu Yang [5] performed a work, “Short Paper: Enhancing Users’ Comprehension of Android Permissions”. In this paper, Author proposes to help Android users better understand application permissions through crowd sourcing. In Presented approach, collections of users of the same application use Presented tool to help each other on permission understanding by sharing their permission reviews. Author demonstrates the feasibility of Presented approach by implementing a proof-of-concept of Presented design.

In Year 2012, Xuetao Wei [6] performed a work, “Permission Evolution in the Android Ecosystem”. In this paper, Author presents arguably the first long-term study that is centred on both permission evolution and usage, of the entire Android ecosystem (platform, third-party apps, and pre-installed apps). First, Author study the Android platform to see how the set of permissions has evolved; Author find that this set tends to grow, and the growth is not aimed towards providing finer-grained permissions but rather towards offering access to new hardware features; a particular concern is that the set of Dangerous permissions is increasing. Second, Author study Android third-party and pre-installed apps to examine whether they follow the principle of least privilege.

In Year 2012, David Barrera [7] performed a work, “Understanding and Improving App Installation Security Mechanisms through Empirical Analysis of Android”. Author provides a detailed analysis of two largely unexplored aspects of the security decisions made by the Android operating system during the app installation process: update integrity and UID assignment. To inform Presented analysis, Author collect a dataset of Android application metadata and extract features from these binaries to gain a better understanding of how developers interact with the security mechanisms invoked during installation.

In Year 2012, Kathy Wain Yee Au [8] performed a work, "PScout: Analyzing the Android Permission Specification". In this paper, Author perform an analysis of the permission system of the Android smartphone OS in an attempt to begin answering some of these questions. Because the documentation of Android's permission system is incomplete and because Author wanted to be able to analyze several versions of Android, Author developed PScout, a tool that extracts the permission specification from the Android OS source code using static analysis.

In Year 2012, Sung Ryul Kim [9] performed a work, "A Hybrid Design of Online Execution Class and Encryption-based Copyright Protection for Android Apps". This paper combines two of the proposed techniques, namely the Online Execution Class and Encryption-based Copyright Protection with a smooth scaling between the two techniques. Author will show that this scaling provides better protection than any one of the techniques can provide by itself.

III. DISCUSSION

Although many SMS Encryption techniques are available but some of them as discussed above are quite popular among practitioners. A number of result analyses have been performed using the above mentioned techniques along with different significant outcomes. Some are discussed as below:

DES (Data Encryption Standard), was the first encryption standard to be published by NIST (National Institute of Standards and Technology). It was designed by IBM based on their Lucifer cipher. DES became a standard in 1974 (www.tropsoft.com). DES uses a 56 bit key, and maps 64 bit input block into a 64 bit output block. The key actually looks like a 64 bit quantity, but one bit in each of the 8 octets is used for odd parity on each octet. There are many attacks and methods recorded till now those exploit the weaknesses of DES, which made it an insecure block cipher [22].

In 3DES memory required for implementation is the highest means it is the slowest algorithm. This is the main drawback of 3DES. It is having a sufficient value of avalanche effect. Several internet-based applications have adopted triple DES. But because of various drawbacks it is not a reasonable candidate for long term use [21].

(Elminaam et. al., 2010) presented a comparison of AES, DES, 3DES, RC2, Blowfish and RC6. They used different settings for each algorithm such as different sizes of data blocks, different data types, battery power consumption, different key size and finally encryption/decryption speed. They concluded that in case of changing packet size Blowfish showed better performance than other algorithms followed by RC6 [22].

Blowfish is a symmetric block cipher that can be effectively used for encryption and safeguarding of data. It takes a variable-length key, from 32 bits to 448 bits, making it ideal for securing data. Blowfish was designed in 1993 by Bruce Schneier as a fast, free alternative to existing encryption algorithms. Blowfish is unpatented and license-free, and is available free for all uses. Though it suffers from weak keys problem, no attack is known to be successful against it (Bruce, 1996) (Nadeem, 2005) [22].

Manisha Madhwani proposed an efficient algorithm for cryptography which is based on static Look Up table and Dynamic Key. Symmetric encryption and decryption is used in this algorithm. The proposed algorithm is more secure and simple to implement. This application makes use of built in android Intents and SMS Manager to send and receive messages. In computer science, a lookup table is an array that replaces runtime computation with a simpler array indexing operation. The savings in terms of processing time can be significant, since retrieving a value from memory is often faster than undergoing an 'expensive' computation or input/output operation. [23]

It is realized that the security is most essential for mobile users and network operators to avoid different threats at different levels. The transmission of an SMS in GSM network is not secure at all. Existing system uses very complicated algorithms to perform encryption. Therefore it is desirable to secure SMS for business purposes by additional encryption. So an efficient algorithm is needed which is easy to implement and to understand.

IV. CONCLUSION

The security of text becomes major issue especially in case of mobile banking; message carrying any military information; M-Commerce etc. First DES was developed but many attacks and methods recorded till now which exploit the weaknesses of DES, and made it an insecure algorithm. After that AES was developed which is found to be very complex for Android Message Application. All these algorithms are asymmetric ciphers which are very difficult to implement because two different keys need to be generated for both encryption and decryption. The latest algorithm cryptography on Android Message Applications was proposed by Manisha Madhwani which is based on Static Lookup table and Dynamic key. It uses symmetric key encryption and decryption. This application makes use of built in android Intents and SMS manager to send and receive messages. The decrypted message is received at the receivers end. In addition to this, Dynamic Lookup table may be used rather than Static Lookup table. The Dynamic Lookup table followed by LZW compression will require less memory as no need to store ASCII values corresponding to all characters and due to compression, the size of actual communication text will also be reduced. The values corresponding to SMS will be fetched at runtime.

ACKNOWLEDGMENT

I would like to thank almighty and my family for their constant support during this work. I would also like to thank my Guide Mr. Rahul Kumar Yadav for his support and encouragement to complete our work.

REFERENCES

[1] Manisha Madhwani, “Cryptography On Android Message Application using Look Up Table and Dynamic Key (Cama)”, IOSR Journal of Computer Engineering (IOSRJCE) ISSN: 2278-0661, ISBN: 2278-8727 Volume 6, Issue 2 (Sep-Oct.2012), PP 54-59

[2] M. Toorani and A. A. Behesti, SSMS – A Secure SMS Messaging Protocol for the M-Payment Systems, IEEE Symposium on Computers and Communications, 2012, 700-705

[3] Bhaskar Sarma, “Android Permissions: A Perspective Combining Risks and Benefits”, SACMAT’12, June 20–22, 2012, Newark, New Jersey, USA. ACM 978-1-4503-1295-0/12/06 (pp 13-22)

[4] Adrienne Porter Felt, “Android Permissions: User Attention, Comprehension, and Behavior”, Symposium on Usable Privacy and Security (SOUPS) 2012, July 11-13,2012, Washington, DC, USA

[5] Liu Yang, “Short Paper: Enhancing Users’ Comprehension of Android Permissions”, SPSM’12, October 19, 2012, Raleigh, North Carolina, USA. ACM 978-1-4503-1666-8/12/10 (pp 21-26)

[6] Xuetao Wei, “Permission Evolution in the Android Ecosystem”, ACSAC ’12 Dec. 3-7, 2012, Orlando, Florida USA ACM 978-1-4503-1312-4/12/12 (pp 31-40)

[7] David Barrera, “Understanding and Improving App Installation Security Mechanisms through Empirical Analysis of Android”, SPSM’12, October 19, 2012, Raleigh, North Carolina, USA. ACM 978-1-4503-1666-8/12/10 (pp 81-92)

[8] Kathy Wain Yee Au, “PScout: Analyzing the Android Permission Specification”, CCS’12, October 16–18, 2012, Raleigh, North Carolina, USA. ACM 978-1-4503-1651-4/12/10 (pp 217-228)

[9] Roland Schloglhofer, “Secure and Usable Authentication on Mobile Devices”, MoMM2012, 3-5 December, 2012, Bali, Indonesia. ACM 978-1-4503-1307-0/12/12 (pp 257-262)

[10] Sung Ryul Kim, “A Hybrid Design of Online Execution Class and Encryption-based Copyright Protection for Android Apps”, RACS’12, October 23-26, 2012, San Antonio, TX, USA. ACM 978-1-4503-1492-3/12/10 (pp 342-343)

[11] Rohan Rayarikar, “SMS Encryption using AES Algorithm on Android”, International Journal of Computer Applications (0975 – 8887) Volume 50– No.19, July 2012 (pp 12-17)

[12] Na Qi Jink Pan Qun Ding, The Implementation of FPGA-based RSA Public-Key Application and Its Application in Mobile -Phone SMS Encryption System, IEEE International Conference on Instrumentation, Measurement, Computer, Communication and Control, 2011, 700-703.

[13] Nathaniel Husted, “Smartphone Security Limitations: Conflicting Traditions”, GTIP ’11 Dec. 6, 2011, Orlando, Florida USA ACM 978-1-4503-1082-6/11/12 (pp 5-12)

[14] Mark H. Goadrich, “Smart Smartphone Development: iOS versus Android”, SIGCSE’11, March 9–12, 2011, Dallas, Texas, USA. ACM 978-1-4503-0500-6/11/03 (pp 607-612)

[15] Mary Agoyi and Devrim Seral, SMS Security: An Asymmetric Encyrption Approach, IEEE International Conference on Wireless and Mobile Communication, 2010, 448-452.

[16] Machigar Ongtang, “Porscha: Policy Oriented Secure Content Handling in Android”, ACSAC ’10 Dec. 6-10, 2010, Austin, Texas USA ACM 978-1-4503-0133-6/10/12 (pp 221-230)

[17] Ch. Rupa and P.S. Avadhani, Message Encryption Scheme Using Cheating Text, IEEE International Conference on Information Technology, 2009, 470-474.

[18] Marko Hassinen, SafeSMS- End-to-End Encrption for SMS Messages, IEEE International Conference on Telecommunications, 2008, 359-365.

[19] S. Jahan, M. M, Hussain, M. R. Amin and S. H. Shah Newaz, A Proposal for Enhancing the Security System of Short Message Service in GSM, IEEE International Conference on Anti-counterfeiting Security and Identification, 2008, 235-240.

[20] David Lisonek and Martin Drahansky, SMS Encryption for Mobile Communication, IEEE International Conference on Security Technology, 2008, 198-201.

[21] Himani Agrawal and Monisha Sharma, Implementation and analysis of various symmetric cryptosystems, Indian Journal of Science and Technology, Vol. 3 No. 12 (Dec 2010) ISSN: 0974- 6846

[22] Jawahar Thakur and Nagesh Kumar, DES, AES and Blowfish: Symmetric Key Cryptography Algorithms Simulation Based Performance Analysis, International Journal of Emerging Technology and Advanced Engineering, (ISSN 2250-2459, Volume 1, Issue 2, December 2011)

[23] http//en.wikipedia.org/wiki/lookup_table#cite_ref-1

AUTHORS PROFILE

Nishika, received her BTech Degree in Information Technology from MD University, India. Currently, she is an MTech student in Computer Science and Engineering, PDM College of Engineering, Bahadurgarh, India. Her research interests include Network Security and Software Engineering.

Rahul Kumar Yadav, working as Assistant Professor in Computer Science and Engineering, PDM College of Engineering, Bahadurgarh, India. His research interests are Software Engineering and Security.