International Journal of Information, Control and Computer Sciences
ISSN: 2517-9942
Vol:12, No:10, 2018

A Comparative Analysis of Asymmetric Encryption Schemes on Android Messaging Service

Mabrouka Alghernai, Fatma Karkouri

***Abstract*—**Today, Short Message Service (SMS) is an important means of communication. SMS is not only used in informal environment for communication and transaction, but it is also used in formal environments such as institutions, organizations, companies, and business world as a tool for communication and transactions. Therefore, there is a need to secure the information that is being transmitted through this medium to ensure security of information both in transit and at rest. But, encryption has been identified as a means to provide security to SMS messages in transit and at rest. Several past researches have proposed and developed several encryption algorithms for SMS and Information Security. This research aims at comparing the performance of common Asymmetric encryption algorithms on SMS security. The research employs the use of three algorithms, namely RSA, McEliece, and RABIN. Several experiments were performed on SMS of various sizes on android mobile device. The experimental results show that each of the three techniques has different key generation, encryption, and decryption times. The efficiency of an algorithm is determined by the time that it takes for encryption, decryption, and key generation. The best algorithm can be chosen based on the least time required for encryption. The obtained results show the least time when McEliece size 4096 is used. RABIN size 4096 gives most time for encryption and so it is the least effective algorithm when considering encryption. Also, the research shows that McEliece size 2048 has the least time for key generation, and hence, it is the best algorithm as relating to key generation. The result of the algorithms also shows that RSA size 1024 is the most preferable algorithm in terms of decryption as it gives the least time for decryption.

***Keywords*—**SMS, RSA, McEliece, RABIN.

I. Introduction

SHORT message service commonly known as SMS is a form of text messaging communication type. SMS is a service of sending short messages, which consist of up to 160 characters between mobile devices. SMS is a type of communication, which involves personal, official, business, and social messaging [1]. The protocol type used in SMS system is a standardized communication protocol that allows fixed line or mobile devices to exchange short text messages [2].

SMS is associated with mobile communication. SMS is transmitted through the GSM architecture. Transmission of SMS is in plain text. The GSM, through which the SMS is transmitted, uses A5/A3 encryption algorithm, which has a 64-bit binary code. This encryption algorithm has proven to be vulnerable and has been cracked, leaving SMS contents to the threats of exposure as there are several security risks during transmission [3].

Transmission of SMS is usually through the Short Message Service Centre (SMSC). SMSCs are owned and run by Third party telecommunication operators. Third party telecommunication operators are responsible for routing and delivering of SMS message between the senders and the receivers. When a user wants to send an SMS, he/she types a message using his/her mobile device and sends it to the intended receiver. After the message is sent, before the recipient receives the message, a store-and-forward message mechanism is applied, where the message is initially delivered to the SMSC and stored temporarily in the database of the service provider. After the store and forward mechanism, the message is forwarded to the recipient's phone. The problem here is that the mobile operators have access to the information stored in SMSC. SMS stored in the SMSC is prone to confidentiality issues as it can be viewed or modified by the SMSC operators [4].

SMS Message transmission is very sensitive especially when it involves some very important information and critical data that are highly confidential, any form of interception on it by an unauthorized person can be very destructive, leading to a loss of integrity and confidentiality of the message.

Encryption can be used to solve security issues related to transmission of information; this research aims at evaluating the three most used asymmetric encryption algorithms in SMS security to help to improve the security of SMS.

II. Literature Review

A. GSM Evolution

Global system for Mobile communication (GSM) which was formerly Group special mobile is a digital phone device, which was first developed with the primary purpose of solving the fragmentation issue of the first cellular system. It is the first cellular system to specify digital modulation and network layer architectures [5]. GSM operates on several frequency bands, some of which are 900 MHz frequency (GSM 900), 1800 MHz frequency (GSM 1800), 2100 MHz frequency. Since the introduction of GSM to Europe in 1991, it has gained wide usage across the globe and has become the most common cellular standard [6].

The official birth of GSM happened in 1989, as the Special Mobile Group was tasked by the European Initiative to develop a cellular telephony system for European states, for which the GSM standard was finalized in 1990 [6]. GSM

Mabroka Alghernini is with the Higher Institute Of Sciences and Technolog, Aljofra – Sokna, Libya (phone: 218912508554; e-mail: kokyrbab1@gmail.com).

Fatma A. Karkouri is with the Higher Institute of Refrigeration and Air Conditioning Sokna, Libya (phone: +218913395819; e-mail: f_sokna@ yahoo.com).

service started in 1991. During the period of 1990 to 1997, GSM specifications with different functionalities and features were released; the GSM phase1, GSM phase 2+, R97, R98, R99, Rel-4, Rel-5, Rel-6, Rel-7, Rel-8 and Rel-9. In December 1998, the Third Generation mobile system was developed through a collaborative project of European Telecommunications Standard Institute (ETSI), Association of Radio Industries and Business, Japan (ARIB), Telecommunications Technology Committee, Japan (TTC), Alliance for Telecommunications Industry solutions, North America (ATIS) and China Communication Standard Association (CCSA) [7].

The GSM phase 1 system design operated on 900 MHz frequency band supported multiple data services up to 9.6 kbits/s. The device also supported full rate speech codec at 13 kbits/s. The GSM phase 2 supported 1800 MHz frequency band. GSM phase 2+ had the SIM application toolkit function, which provided the framework for application like banking and weather residing on the SIM. The phase release 97 contained General packet radio service that allowed packet switched data connections. It supported security mechanism for SIM application toolkit. The release 5 made improvement to GSM/UTRAN networking. The release 7 supported mobile station antenna performance mechanisms [7].

B. GSM Architecture

There are several sub-systems involved in GSM architecture, the GSM architecture network is made up of several elements that are interrelated, as they operate together to construct the entire system of the GSM. Subsystems of the GSM architecture play a role in interacting with GSM operations to establish interactions with the other network architecture. Therefore, one elementary function of the GSM network architecture is to interact with components of network elements [8].

There is a constant development in the innovation of the GSM systems in order to meet up with the dynamic environment and the vast changes occurring in the technology sector and the world at large, but still, the GSM architecture network is primarily being maintained. The four major parts that make up the GSM specifications of the network system of the GSM architecture are Mobile Station (MS), Network and Switching Subsystem (NSS), Base-Station Subsystem (BSS), Operation and Support Subsystem (OSS) [9]. These four major elements, that make up the network operations, interact with one another, where the user of the system has no previous knowledge and understanding of these elements differences within the GSM system.

C. Mobile Messaging

In the current age, there are many new ways of communicating electronically [10]. In a research by Duggan (2015) [11], his survey showed that 36% of smart phones owners use messaging software to meet specific needs. These messaging apps, such as WhatsApp, iMessage, Facebook to mention a few, allow users to communicate through texts without the use of SMS. The result in his research showed that different communication tools for messaging have become popular for private and official purposes.

D. SMS and SMS Transmission

SMS system type of communication first started in the United Kingdom (UK) in the year 1992, when it was tested and showed its success that was the first of that kind, afterwards SMS was adopted as a major means of communication even within the private, public, and governmental systems. This application in the mobile device (SMS) was found to be efficient because it is cheap in cost, and it could be used to communicate to several recipients with the same time. It has shown also its effectiveness because it was fast, of a good quality, reasonable and sensible [12].

There could be interception of private messages by unauthorized users who want to access the information in a message. Therefore, there is an urgent need for securing this communication platform. There are numerous security challenges and attacks that could exploit the SMS transmission. SMS can easily be intercepted, so hackers are developing new techniques of attacking and stealing information through SMS. Some challenges that give access to unauthorized users are unencrypted SMS and erroneous sending of SMS to the wrong or unauthorized persons [13].

SMS is transmitted on the service providers network, through the message centers, the originating message finds the message center of the receiving network and drops the message in that network, which is then transmitted to the recipient subscriber in the home network [14]. Fig. 2 gives an illustration on how the SMS is transmitted over SMSC.

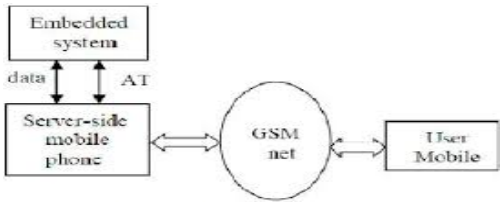

Fig. 1 Protocol of secure transmission of SMS

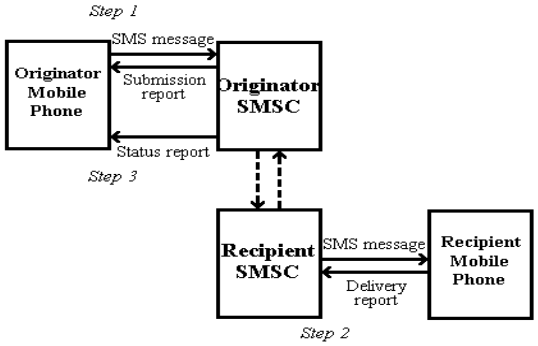

Fig. 2 SMS transmission through SMSC

SMS cannot fully have confidential and integrity traits because the messaging system is not reliable as they are transferred in plain text also known to be the original

message, then transferred within the channel that is secured by some network operators so the messages could be stored temporary on the database [15], and so, it is necessary to supply secure communication between users as shown in Fig. 1.

Most SMS are transmitted over the GSM which uses the A5/A3 algorithm of 64-bit binary code that has been cracked by experts, showing that it is no longer secured or reliable because the SMS is at risk of being exposed during transmission, the SMS is usually written as plaintext, then transferred in the same plaintext form through such insecure channels [3].

Fig. 3 shows how message is intercepted by unauthorized persons over the network, so then the message is lured to be directed to the attacker instead of the authentic receiver.

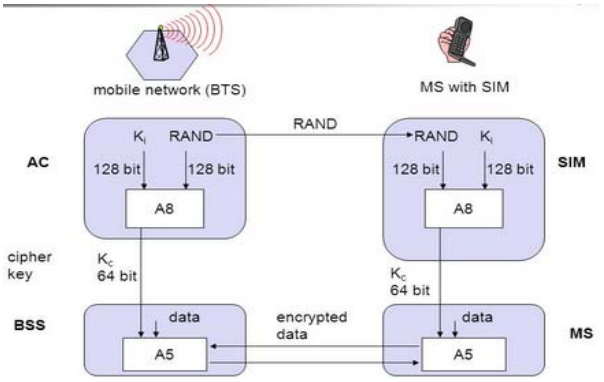

Fig. 3 GSM key generation and encryption

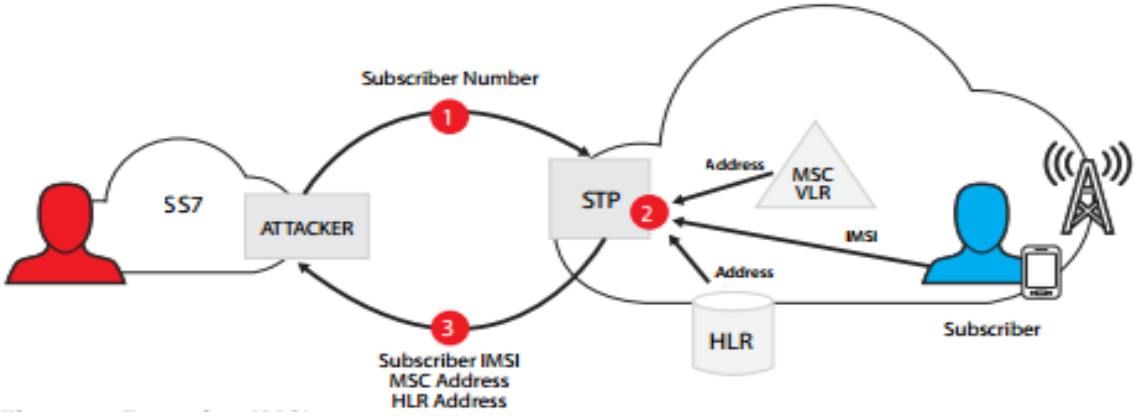

Fig. 4 SMS interception

E. Security Issue in GSM

GSM architecture enables us to understand how mobile communication functions when using wireless of mobile that has become very familiar and well known in this line system, using this communication type, information is being transferred from one entity to other entities regardless of the place and location, when the connection is available, the information can be transferred easily. During transfer of information, lots of security issues could arise leading to challenges of interception by unauthorized party to be involved in the information sharing.

The GSM system is highly vulnerable due to the growth of mobility involved by its users, hence there is high level of interception, access, eaves dropping by unauthorized persons, parties, entities and software, compared to the old communication system that uses the wired system. The old system has less vulnerability, therefore there is a need to innovate a system to improve the security of the GSM network considering the type of information being transmitted using this medium, bank information, personal information, business information and so on, they are highly confidential, critical, sensitive and important information that needs to be protected from unauthorized parties, instead so many experts have proven how insecure this mobile system is as its architecture can easily be pierced [16].

F. Security Issue in SMS

For information to be secured, the information must have a high level of integrity and confidentiality, without disrupting its availability. In the SMS security challenges, the mobile device which is used to transmit the message could be a subject or an object of attack, in the sense that when it is an object of attack [17], the mobile device is the entity that is targeted to be attacked, meaning that the security codes on the mobile device are broken, then the SMS can be accessed and viewed. Moreover, when it is a subject of attack, it means that the mobile device is an active instrument used to lunch attacks on other devices in order to access the SMS information. Therefore, the sender performs encryption on the message so that it becomes unreadable to someone else other than the receiver, whereas the receiver performs the decryption process on the message with the aid of the generated secret key.

III. Cryptograpgy

In this section, more enlightenment on the general concept of cryptography is given. This includes the encryption process, decryption process, key generation process. The three algorithms used for this research which are RSA, McEliece

and Rabin are defined with mathematical function.

Cryptography is the method employed through code writings so that information that is being transmitted can be secured. When the methods of cryptography and cryptanalysis are being combined, it is known as cryptology which is the science of the encryption process. As a way of understanding what cryptanalysis means, it is a process of retrieving the initials of the original message after it has been encrypted, without necessarily knowing or understanding the algorithm used for the encryption, this method of cryptanalysis involves both encryption and decryption [18]. Encryption means encoding a message from the plain text, so that unauthorized persons cannot make a meaning out of the information.

Encryption is a means of securing the information and enhancing its protection, with the symmetric or asymmetric methods used to carry out this action, while the decrypting process is decoding the encoded message back to a plain text form or a readable form. This is possible if the authorized persons have the required secret keys generated to complete the process [19].

The cryptographic algorithms are majorly divided into two categories, known as symmetric and asymmetric cryptography, and in today's system of encrypting. There could be a combination of both methods, known as the hybrid because it uses both the asymmetric and symmetric algorithms, in which they are distinguished by the key types used in the encryption process and the decryption process. The key types are private and public keys, the asymmetric algorithm uses both the private and public key types while the symmetric algorithm uses only the public key [20].

A. Asymmetric Cryptography

This encryption type is known as the public-key type of encryption, it uses two related keys, where one of the keys is used to encode the information and the other one to decode the information. For instance, if key A is used to encrypt the message, then key B has to be used to decrypt the message, here one of the keys serves as a private key while the other one as a public key in order to acquire a high value. The advantage is that the challenge of key sharing is eliminated, but then the time involved is consuming, hence reduces the efficiency of the method. It makes use of the RSA algorithm method [21].

B. Symmetric Cryptography

The cryptography of symmetric encryption with the aid of a generated secret key to encode the information, and the same secret key is needed to decode the information. This method is known to be very efficient because of the little time involved in the process but the disadvantage involved here is the problem of key sharing because both the sender and receiver of the message must have the generated secret key and safely used so that it is not being compromised or exposed to unauthorized persons, because if the key is compromised by a third party who is not authorized to view the information, the information loses its confidentiality and integrity. The most known example of symmetric encryption is the DES which means Data Encryption Standard. It has a size of 64 block of bit, with key of 56 bit and the cryptosystem is accepted for use by the federal standards for encrypting non-classified information by the NIST body in the year 1976. The DES was later upgraded to a more advance standard called the 3DES to enhance the security level to be more than that of the DES, then later developed Advanced Encryption Standard (AES), this later replaced the DES and 3DES because of its advancement nature [22].

C. Hybrid Cryptography

This method of cryptography implies the combination of both symmetric and asymmetric methods except the use of digital certificates, but then the asymmetric method is used more frequently than the symmetric method so as to create the hybrid effect. The method of exchanging key here is using the Diffie-Hellman method in order to provide foundation for later development of the encryption needing the public key.

D. Encryption Key Size

Keys are required in coding information for security purposes, therefore when using ciphered text, the key size to be used must be determined because it is very important, as it shows the strength applied in the encrypting process. It is not about secrecy of the encryption algorithm that enhances the security level of the information, but it is secured when some or all of the variable elements are secured by the secret key(s).

E. RSA Cryptosystem

The RSA cryptosystem is derived from the names of Rivest, Shamir and Adleman. It is an important method commonly used in the public key type of cryptography. The encryption process involves the use of a public key and decrypting with a private key. The RSA cryptosystem by far is the most important and commonly used cipher method of encrypting and it came into existence in the year 1978 [23].

RSA cryptosystem involves making a choice of two prime numbers that are large in size, like numbers *a* and *b*; hence we can calculate their products and their total number, as illustrated in (1)

$$n = p \times q$$
$$\varphi(n) = (p-1) \times (q-1) \quad (1)$$

We select an integer f, which satisfies (2), where *gcd* stands for the greatest common divisor

$$f < \varphi(n)$$
$$\gcd(\varphi(n), f) = 1 \quad (2)$$

An integer *d* is then calculated using (3).

$$d = f^{-1} mod \varphi(n) \quad (3)$$

The public key is $\{f, n\}$, and the private key is $\{d, n\}$. To encrypt an information, say M, we then convert the plaintext to cipher text as shown in (4).

$$C = M^6 mod\ n \quad (4)$$

To decrypt the cipher text back to plain text, (5) is then used to produce the information M.

$$M = C^d mod\ n \quad (5)$$

F. McEliece Cryptosystem

The McEliece encryption scheme was developed in the year 1978. It uses the public-key encryption scheme which started based on error-correcting codes. The concept of this algorithm is due to the need to decode the Goppa codes but was not available for the general linear code.

In this cryptosystem of McEliece algorithm, the Goppa codes are used to make the performance by using three types of operations which include plaintext encryption, decryption of the cipher text and that of the key generation.

The determination of the Goppa code is consistent in the key generation. The nature of the Goppa code is linear, therefore the $k \times n$generator matrix can be used to generate it, when denoted by G making a random choice of nonsingular$k\times$ k matrix S with an$\times$ n permutation matrix P, we therefore make a computation for the public key

$$k \times n \quad (6)$$

The generator matrix is

$$\hat{G} = SGP \quad (7)$$

On the other hand, the secret key is given as

$$sk = (\Gamma(l, g), S, P) \quad (8)$$

This secret key is as the result of the output produced by the key generation, and then, the public key is as given in (9)

$$pk = \left(n, t, \hat{G}\right) \quad (9)$$

When encrypting the SMS information from its plaintext, the public generator matrix is being used to encrypt the message M, which is

$$C = M\hat{G} \quad (10)$$

Then, the vector E which is an error vector having *n* length and *t* weight is then randomly chosen so as to add to the code word as the cipher text

$$C = \widehat{C \oplus E} \quad (11)$$

To decrypt the cipher text back to plain text, the outcome is

$$\hat{C}P^{-1} \quad (12)$$

This must be initially computed, having the code word which contains an error that is

$$MSG \oplus EP^{-1} \quad (13)$$

Therefore, we use the algorithm to decode the encrypted message so as to have the secret code obtained, then multiplied by $G_Y - 1$ on the right side, such that $GG_Y - 1 = I_k$ is the $k \times k$ identity matrix, in order to find $\widehat{M} = MS$ Our final step is to compute $M = \widehat{M}S^{-1}$ to have back the message to its plain text format.

G.RABIN Cryptosystem

The scheme of RABIN encryption was first proposed in the year 1980 in order for it to be a resolution to the challenge of number determination, by its prime or composite number type, hence this algorithm was developed and employed to suggest solutions for the techniques of the probabilistic [24].

The scheme of RABIN creates both private and public keys that are required for the encrypting and decrypting of the process. The process of generating the private and public keys involves the creation of two large prime numbers. Let us say *p* and q of about the same size. The value of n is computed as given in (14)

$$.n = p \times q \quad (14)$$

(p, q) is the private key and *n* is the public key.

To encrypts a message M. The encryption which is done by obtaining the public key n, represent the message as an integer m as given in (15)

$$m = \{0,1,2 \ldots\ldots, n-1, n-2\} \quad (15)$$

The cipher text is computed as given in (16)

$$C = M^2\, mod\ n \quad (16)$$

For decryption, choose a and b, such that

$$ap + b_2 = 1 \quad (17)$$

Compute

$$r = C^{\frac{p+1}{4}} (mod\ p) \quad (18)$$

$$s = C^{(q+1)/4} (mod\ q) \quad (19)$$

$$x = (aps + bqr) mod\ n \quad (20)$$

$$y = (ap - bqr) mod\ n \quad (21)$$

The four square roots of $c\ mod\ n$ are x, -x mod n, y and –y mod n

The message is any of the four square roosts.

The cipher text is generated through the encryption to protect the message, then sent to the receiver Bob, who then decrypts the message with the theorem of the Chinese reminder so as to obtain the four square roots m_1 m_2 $m_3$and m_4 having equal probability involved [25].

The advantage of using the RABIN algorithm technique to

encrypt the information is the high level of security. It provides against attackers and hackers, and also the advantage of time management, because it is very fast as it has just singular squaring modular. The disadvantage of the RABIN technique is the lack of the ability to be deterministic because the receiver of the message must choose from the equally four likely possibilities that are the outcomes, also the technique has a slow speed at decryption which can be related to the RSA algorithm. Lastly, the RABIN algorithm is vulnerable to the attacks of the RSA encryption scheme [25].

IV. Performance Analysis

In this section, explanations are given on the development of the software, the programs used and how the results turn out to resolve the security challenges faced in SMS, providing solutions adequately, the functions that the software provides will be illustrated here, with hands-on experiments with the aid of diagrams, showing the encryption and decryption processes, the time used and how it varies depending on the key size used for the algorithm.

A. Summary and Evaluation of the Algorithms

TABLEI
SUMMARY AND EVALUATION OF THE ALGORITHMS

RSA	McEliece	RABIN
Integer factorized problem	Linear code decoding problem	Integer factorization problem square roots modulo composite.
No attack possible in reasonable computation time	Relatively fast encryption and decryption	Secure against attack by passive adversary Extremely fast encryption due to single modular squaring
Susceptible to brute force, side channel and mathematical attacks To ensure long-term security, modulus of at least 2048-bits is recommended.	Very large size of the public key	Not deterministic Slower decryption speed but comparable to RSA Susceptible to RSA attacks

V. Experimental Result

The relationships existing in the whole process will be illustrated here with the aid of the screen shots as seen in Figs. 4 and 5. The android phones are used for testing. The key generation process, encryption process, decryption process, application source codes, are involved to achieve the objectives of this research. Initializing the process from the settings of the mobile devices, we will view how the SMS are being sent using the different programming languages of RSA, RABIN and McEliece, testing each of these algorithms and calculating the time that they take to generate the secret keys, the size used for the key, and revealing how it affects the efficiency of encrypting and decrypting the messages so as to free the three major aspect of security challenge of the SMS system, which are the confidentiality, integrity, and authentication .

The asymmetric and symmetric methods of cryptography are used in different levels, depending on what is intended to be achieved, for instance, to resolve confidentiality security challenge, the symmetric method can be employed but to resolve both confidentiality and integrity security issues, hybrid cryptography, asymmetric cryptography or digital signature methods can be utilized [20].

The research focuses on android mobile devices; therefore, we shall be carrying out the practical testing on an android device of Samsung grand neo of model S6, using android version 5.2.1 at a speed level of 1.5 GHz, RAM size 4.5 GB and total internal memory of 12.0 GB to demonstrate the key generation, time for encryption, and decryption.

Fig. 4 summarizes the three methods of RSA, RABIN, and McEliece implemented on the android device at the same time. RSA is being implemented from the settings to carry out the encryption process and categorized according to different sizes, ranging from key size 1024, 2048, and 4096. Mceliece method is used with different key levels 1024, 2048, and 4096, and which of these sizes is more effective and efficient. RABIN at different size levels of 1024, 2048, and 4096, being implemented on the android device to view how the process will be effectively carried out. Fig. 4 demonstrates how the message is being initialized, the recipient(s) to whom the message is to be sent is/are selected, and then the message is composed and encrypted with the secret key generated.

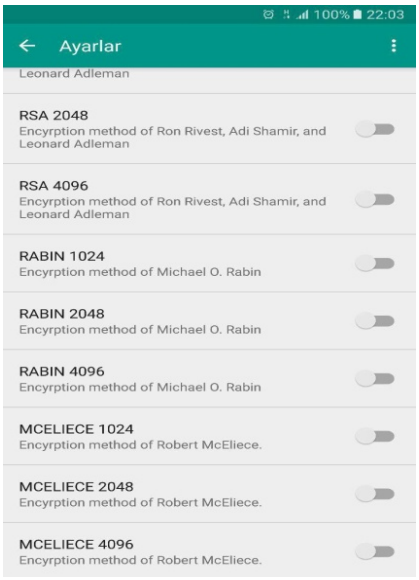

Fig. 5 RSA and RABIN and McEliece implemented on the android device

Fig. 6 shows the encrypted message from the sender to the recipient in an unreadable form so that unauthorized persons cannot read the information.

Fig. 7 shows message from the receiver, sending back a reply in an encrypted format so that it is protected from unauthorized persons, the message can therefore be viewed when unlocked with a secret key.

Fig. 8 shows the graphical user interfaced from the message options.

Time for Encryption, Decryption and Key Generation

Calculating the time involved in encryption, decryption and key generation is very important and it determines how efficient or effective the process is, the algorithm for the process is created and the time is calculated in nanoseconds carefully considering the bytes sizes. Having this information will help the programmer to decide on which of the algorithm is best needed for encryption in terms of time taking, or which one takes the least time to decrypt and which one has the best timing when it comes to key generation. Now, depending on the situation and the need for securing a message, the best option that best suits the situation will be applied.

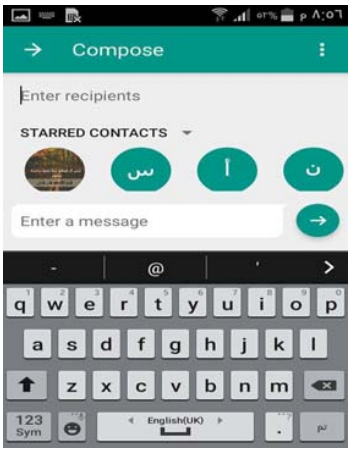

Fig. 6 Initializing composition of the SMS

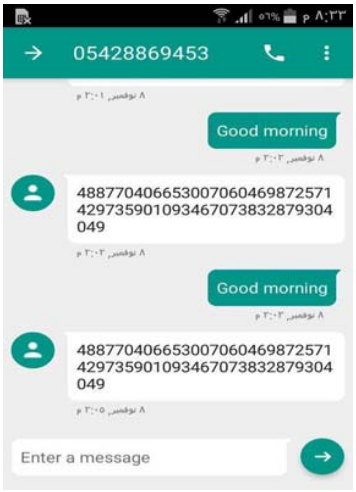

Fig. 7 Encrypted messages from the sender

Fig. 10 illustrates RSA algorithm with the size of 2048 takes the time of 1277.00 to generate a secret key needed to encrypt the message, this is the most time taken from the above illustration while the least time taken is using the algorithm MCELIECE size 2048 which takes the time of 623.17.

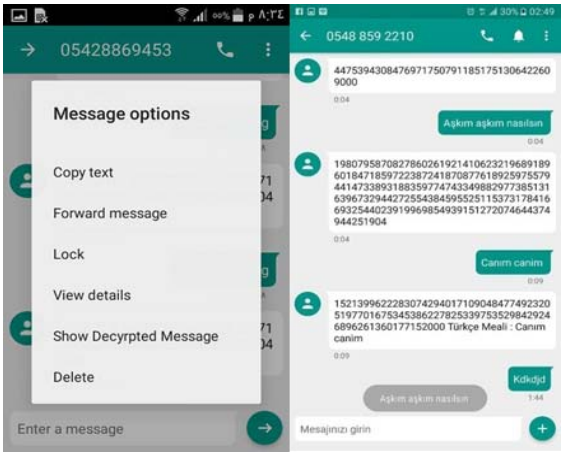

Fig. 8 Decrypting action taken on encrypted SMS and encrypted messages as reply from receiver

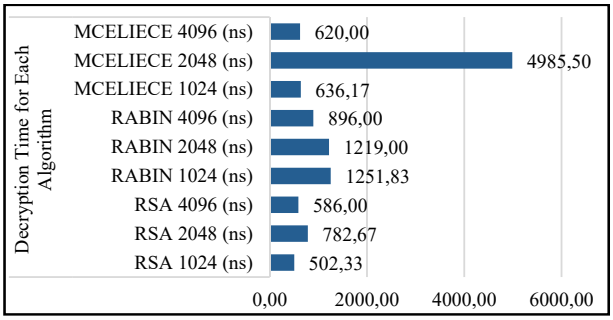

Fig. 9 Decryption time for each algorithm

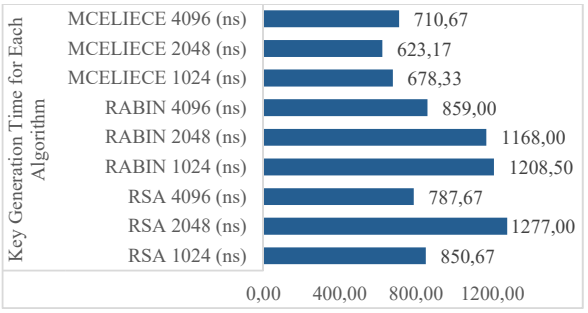

Fig. 10 Time taken to generate key at encryption

Fig. 11 illustrates RSA algorithm with the size of 2048 which takes 1277.00 of time to generate a secret key needed to encrypt the message; this is the longest time taken from the above illustration while the least time taken is using the algorithm McEliece size 2048 which takes 623.17 of time.

Fig. 9 illustrates the time taken during message encryption; the best time which is the least time required is when algorithm McEliece size 4096 is used, followed by McEliece size 2048 and then McEliece 1024. The worst time experienced which requires more time to encrypt a message is when the algorithm RABIN size 4096 is used, followed by RSA 4096 then RABIN 2048. Therefore, the programmer having this information can choose the best option for

algorithm that is most efficient and effective.

Table II illustrates the time taken during message encryption; the best time which is the least time required is when algorithm McEliece size 4096 is used, followed by McEliece size 2048 and then McEliece 1024. The worst time experienced which requires more time to encrypt a message is when the algorithm RABIN size 4096 is used, followed by RSA 4096 then RABIN 2048. Therefore, the programmer having this information can choose the best option for algorithm that is most efficient and effective.

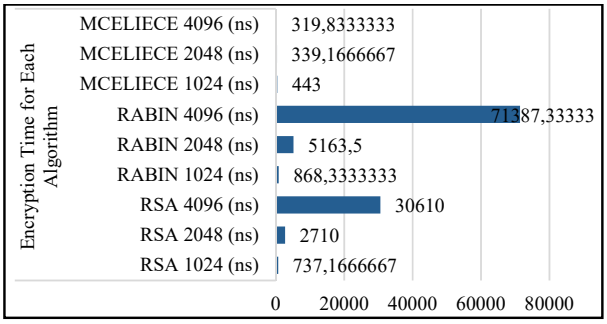

Fig. 11 Time taken for key generation at encryption

TABLE II
KEY GENERATION TIME FOR EACH ALGORITHM

Plaintext in bytes	RSA 1024 (ns)	RSA 2048 (ns)	RSA 4096 (ns)	RABIN 1024 (ns)	RABIN 2048 (ns)	RABIN 4096 (ns)	MCELIECE 1024 (ns)	MCELIECE 2048 (ns)	MCELIECE 4096 (ns)
13	955	896	517	1454	1759	586	227	201	289
22	477	1110	164	1135	1056	437	576	857	744
29	1159	1234	367	1049	1023	1271	1171	837	1096
41	1513	2221	1642	2228	893	277	592	624	1041
50	440	681	803	661	587	457	613	225	976
60	560	1520	1233	724	1690	2126	891	995	118
Key Gene. Avg.	**850.67**	**1277.00**	**787.67**	**1208.50**	**1168.00**	**859.00**	**678.33**	**623.17**	**710.67**

TABLE III
KEY GENERATION TIME FOR ALGORITHM

Plaintext in bytes	RSA 1024 (ns)	RSA 2048 (ns)	RSA 4096 (ns)	RABIN 1024 (ns)	RABIN 2048 (ns)	RABIN 4096 (ns)	MCELIECE 1024 (ns)	MCELIEC E 2048 (ns)	MCELIEC E 4096 (ns)
13	611	6635	6487	716	4101	41374	560	429	333
22	983	2894	24624	900	3641	45812	335	257	279
29	458	3532	41258	864	5414	163673	655	287	345
41	727	891	49240	1104	1206	17592	399	273	280
50	1025	1925	29465	1307	1061	30389	370	426	322
60	619	383	32586	319	15558	129484	339	363	360
Encryption Avg.	**737.17**	**2710.00**	**30610.00**	**868.33**	**5163.50**	**71387.33**	**443.00**	**339.17**	**319.83**

TABLE IV
KEY GENERATION TIME FOR ALGORITHM

Plaintext and Cipher text Length									
Plaintext in bytes	RSA 1024 (ns)	RSA 2048 (ns)	RSA 4096 (ns)	RABIN 1024 (ns)	RABIN 2048 (ns)	RABIN 4096 (ns)	MCELIECE 1024 (ns)	MCELIECE 2048 (ns)	MCELIECE 4096 (ns)
13	93	93	93	62	62	62	617	617	617
22	158	158	158	105	105	105	616	616	616
29	208	208	208	139	139	139	616	616	616
41	295	295	295	197	197	197	618	618	618
50	360	360	360	240	240	240	617	617	617
60	616	616	616	288	288	288	618	617	618

Table III shows the decryption time of the algorithm, where the best average decryption time is when the RSA algorithm is in use with the least size of 1024, and the algorithm with the maximum average time of 4985.50 ns is McEliece at 2048 size.

Table IV gives information on time taken to actually encrypt a message, changing it from its plaintext format to a ciphered text format, depending on the size of the plaintext in bytes, the time taken is also determined, from the above table, the algorithm sizes makes too much difference, for instance, RSA algorithm of sizes 1024, 2048 and 4096 all used the time 93 for plaintext of 13 bytes, but then the higher the bytes sizes are the more time required to convert a plaintext into a cipher text.

VII. CONCLUSION

This paper employed the use of Java and Blue Stack assisted software tool to build an Android mobile application for SMS Encryption. RSA, Rabin, and McEliece Encryption techniques which were adopted to encrypt the plain text and converting it into ciphered text before it is being transmitted to the network. Our solutions focus more on using the Asymmetric Encryption based on RSA, RABIN, and McEliece encryption technique over the symmetric

encryption. It is preferable to use the asymmetric encryption technique because its key is not distributed through a third party and it provides more security as compared to symmetric key encryption.

REFERENCES

[1] Agoyi, M., and Seral, D. (2010). SMS security: an asymmetric encryption approach. In Wireless and Mobile Communications (ICWMC), 6th International Conference on IEEE, 448-452.
[2] Saxena, N., and Chaudhari, N. S. (2011). A secure digital signature approach for SMS security. International journal of Computer Application (IJCA), ISBN, 978-93.
[3] Heshem A. El Zouka (2015). Providing end-to-end secure communications in GSM networks. International Journal of Network Security and Its Applications (IJNSA) Vol. 7
[4] Medani, A., Gani, A., Zakaria, O., Zaidan, A. A., and Zaidan, B. B. (2011). Review of mobile short message service security issues and techniques towards the solution. Scientific Research and Essays, 6(6), 1147-1165.
[5] Gu, G., and Peng, G. (2010). The survey of GSM wireless communication system. 2010 International Conference on Computer and Information Application. 121-124.
[6] Oancea, C. D. (2011). GSM infrastructure used for data transmission. 7th International Symposium Advanced Topics In Electrical Engineering (ATEE) 1-4.
[7] Saily, M., Sebire, G., and Riddington, E. (Eds.). (2011). GSM/EDGE: Evolution and performance.
[8] Penttinen J. T. J (2015). The telecommunication handbook: Engineering guidelines for fixed mobile and satellite systems. Wiley-Blackwell 281-289.
[9] Sahin M. E, Nilufr A. S & Karan Yasin (2013), Selective radiation measurement for safety evaluation of base stations. Turkey, Gazi University Journal of science 26(1) 73-83.
[10] Rakestraw, T. L., Eunni, R. and Kasuganti, R. R. (2013). The mobile apps industry: A case study. Journal of Business Cases and Applications.
[11] Duggan, M. (2015). Mobile messaging and social media 2015. Retrieved January 30, 2017, from http://www.pewinternet.org/2015/08/19/mobile-messaging-and-social-media-2015/.
[12] Khan, M. W. (2013). SMS Security in Mobile Devices: A Survey. *International Journal of Advanced Networking and Applications*, *5*(2), 1873.
[13] Markovski, Smile, Aleksandra Kuzmanovska, and Milivoj Simeonovski. "A protocol for secure sms communication for android os." In ICT Innovations 2011, pp. 171-178. Springer Berlin Heidelberg, 2012.
[14] Arreymbi, J. (2011). Investigating Issues in Mobile Network in Security. Journal of Modern Applied Science, 2(6), 3-10.
[15] Rayarikar, Rahin, Sadiku and Marmor T (2012). SMS encryption using AES Algorithm onandroid IJCA 50.19.
[16] Raheem A., (2014). An Investigation into Authentication Security of GSM Algorithm for Mobile Banking.
[17] Rautkar, S. D., and Prasad, D. P. S. (2015). An overview of real time secure SMS transmission. International Journal of Advanced Research in Computer and Communication Engineering, 4(1).
[18] Bruen, Aiden A. and Forcinito, Mario A. (2011) .Cryptography, Information Theory, and Error-Correction: A Handbook for the 21st Century. 21-29.
[19] Menezes, A. J., VanOorshot, P. C. and Vanstone, S. A. (2010). Applied Cryptography.
[20] Kumar, Y., Munjal, R., & Sharma, H. (2011). Comparison of symmetric and asymmetric cryptography with existing vulnerabilities and countermeasures. International Journal of Computer Science and Management Studies, 11(03).
[21] Gaithuru, J. N., Bakhtiari, M., Salleh, M., and Muteb, A. M. (2015). A comprehensive literature review of asymmetric key cryptography algorithms for establishment of the existing gap. In Software Engineering Conference (MySEC), 236-244 IEEE.
[22] Nath, A., Ghosh, S., and Mallick, M. A. (2010). Symmetric Key Cryptography Using Random Key Generator. In Security and Management, 234-242.
[23] Sindhu UL (2016), "Implementation of secured SMS for end to end communication using RSA algorithm", International Journal of Multidisciplinary Research.
[24] Kessler, G.C., (2012). "Introduction to Cryptography".
[25] Elia, M., Piva, M., & Schipani, D. (2015). The RABIN cryptosystem.