MNK Publication

International Journal of Latest Research in Science and Technology **ISSN (Online):2278-5299**
Volume 4, Issue 1: Page No.47-55, January-February 2015
https://www.mnkpublication.com/journal/ijlrst/index.php

SECURITY ASSURANCE FRAMEWORK FOR SMS USING CASCADED ENCRYPTION ALGORITHM

[1]Reynaldo E. Castillo, [2]Gerald T. Cayabyab,[3]Bartolome T. Tanguilig III
[1]Technological Institute of the Philippines, Quezon City, Philippines
[2] Technological Institute of the Philippines, Quezon City, Philippines
[3] Technological Institute of the Philippines, Quezon City, Philippines

Abstract*-*Security assurance in any telecommunication lines is a necessity. It is everyone's desire to maintain secrecy of any information sent thru both unsecured and secured telecommunication lines. Short Message Service (SMS) has turned into an extension and has been an important part in the life of its user. Payment, mobile banking, important reminders such as stocks and news alerts, traffic updates, weather information and business related information are being catered thru SMS. Problems of privacy and imitations are the core issues dealt in the study. In order to prolong the secrecy of any information, an implementation of an improved cryptology scheme was designed. The study used a cascaded encryption process designed for sending SMS thru any communication line. The strength of the algorithm using the framework focused on designing a secured encryption process and adapting AES (Advance Encryption Standard) encryption with two more encryption layers. It discussed impact of the framework upon encryption process. This paper defined possible parameters which are focused on threat and risk analyses and prevention, technical and architectural requirements. The combined scheme provides further authenticity, security, privacy protections. During transmission or while in storage, security is still a significant concern to electronic information frameworks against coincidental or unlawful obliteration or modification. Cascaded encryption algorithm is one of the ways to ensure information security to which intended parties are able to read and access the confidential information. Aside from the cipher key used in the algorithm is of 128 bits, the approach had utilized two more layers for more confusion. Therefore, to the get the plaintext and cipher key an attacker has to check 2128*n possibilities where n is the number of substitutions and fold-shifting processes which are practically almost impossible.

Keywords–AES; Encryption; Decryption; Plain Text; Cipher Text; SMS; Information Privacy and Security; ODD-EVEN Substitution; Folded-Shifting Method

I. INTRODUCTION

Exchange of feelings, ideas and expression is generally known to be communication. It is the movement of passing on data through the exchange of thoughts, messages, or information, as by speech, signals, writing, or behaviour [1]. Sender and receiver are involved in conveying information through a communication channel. Sender and receiver are the most important parts of communication. There are various methods for communication [2]. Verbal communication includes text messages, presentations and discussions. Non-Verbal communication includes gestures and eye-contact.

Mobile phones are one of the most common devices use to communicate with other people. With the fast expansion of innovation and with spread of smart phones, the security of Short Message Service (SMS) has become a necessity and plays a very important role. For the need of the individuals about the security of these short messages in mobile phones, most analysts gave their endeavours in examining the encryption strategy and concentrated on its application in telecommunication devices such as mobile phones [3].Personal information and other private data are being communicated through text messages this is because the delivery of these information is faster and cheaper. These data are stored in a form of SMS, notices in a calendar, phone contacts, photos and the like. As SMS is presently broadly utilized as business apparatus, its security has turned into a real sympathy toward business organizations and clients. There are a lot of cases about information that are being stolen and/or disclosed to unintended receiver. Tapping applications are in the business sector today. These applications re-send received and sent SMS to an attacker's number. The application is hidden after installation. This application can be even uninstalled remotely when the mobile phone receives an SMS in proper configuration [18]. With this, there is a need to further guarantee individual data security, and deal with individuals' protection well in the crowd. There is a need for multilayered security assurance framework for SMS encryption in order to prolong and ensure information secrecy in a secured or unsecured medium of communication. The secrecy of these information does not depend alone to the user. Although service providers give their own mechanism on protecting and hiding information sent via SMS to other people, it is still visible, in the part of the service provider, to read or somehow disclose some or even all information in that communication line.

The mobile phone should always be protected by the user from alienation of others. Likewise, medium of communication must also be secured in order to prolong the secrecy of any information sent via SMS. On the off chance that the data that are on the cellular phone is in wrong hands, most or even the greater part of the data can be effectively revealed and can be utilized for perpetrating wrongdoings. In any case, private data is powerless against potential gatecrashers who may intercept and extract or alter the contents of information during transmission or while in storage [4] [5] [6]. Secured communication channel is hard to

Publication History

Manuscript Received	:	*20 February 2015*
Manuscript Accepted	:	*25 February 2015*
Revision Received	:	*24 February 2015*
Manuscript Published	:	*28 February 2015*

accomplish or there is insignificant dependence of network-wide services [7]. As information traverses an unsecured channel, it is now powerless to eavesdropping, illegal retrieval, and intended modification [8]. Tapping an SMS can be done by an attacker in different places. SMS tapping from radio broadcast, when SMS is sent or received from a mobile phone to base transceiver station (BTS) [9]. Tapping is easily given to the attacker has an access to the BTS or other parts of the SMS network. Moreover, the telecommunication administrator can simply read all sent SMSs. Despite the fact that it would likely be relatively complex to hack into the telecommunication administrator frameworks from an outer source to acquire the information or data contained within an SMS, thus finding of staff's special privileges to look at the SMS messages and influencing them to uncover the information is very much easy[9]. Hacking into a mobile phone's communication line is very much possible.

Guarding data and data frameworks from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction will be on computer security or IT security area. Keeping protection in anybody's personal communication is something everyone's need. With this, encryption is the key. Encryption is any form of coding, ciphering, or secret writing [10], and a practical means to achieve information secrecy [11]. If smartphones and tablet PCs are not adequately protected against mobile device security threats, the competitive edge and other benefits of mobility might be lost. While the market is on rapid growth of development, IT organizations identify security as one of their greatest concerns about extending mobility. Chains of successful attacks to the initial security of SMSs were documented years before and until at present there are still a lot of problems about information secrecy [19]. Therefore, various encryption techniques are used.

The need for an end to end SMS encryption is really [12] important in order to ensure a secure medium for communication. Likewise, encrypted message normally get bigger than the first message prompting extreme charges in sending SMS encrypted message. Aside from further strengthening security and data integrity, the study also aims to develop encryption method that will produce minimal additional keys which will not lead to minimum payments. Various algorithms for encryption and decryption adds additional keys in order to hide the real size of the plain text which means additional cost for the part of the user. Out of the entire group of algorithms, Advance Encryption System (AES) is the most preferred one. The reason is that AES requires very low RAM space and it's very fast. On Pentium Pro processors AES encryption requires only 18 clock cycles/byte equivalent to throughput of about 11Mib/s for 200MHz processor [13]. This is the reason why the study had chosen to utilize AES algorithm. The disadvantage of this model is the need for exchange of encryption keys via a secured/unsecured communication [17].

Furthermore, the study focused on developing a cascaded encryption method in producing the cipher text and the adapting XORed result of the last 64 bit of sender plus 64 bit of receiver SIM numbers in Advance Encryption Algorithm for secrete key generation, verification and validation. In this study, keys used for encryption and decryption processes will be computed using the current active SIM number on the device. This means that keys will not be sent via any other communication medium.

II. REVIEW OF RELATED LITERATURE

David Celdran wrote in a thought-provoking essay stated that in under 10 years the utilization of the Short Message Service (SMS) – or text messaging – on the nation's cellular telephone system has changed the individual and political lives of the residents of the Philippines. The qualities of integration, rate, cost adequacy, portability and secrecy of content informing and its flexibility to Filipino society has made SMS the most well-known type of private communication technology in the country[27].

The security of text messages becomes major issue especially in case of mobile banking; message carrying any military information; M-Commerce etc. First and foremost DES was produced yet numerous attacks and strategies recorded until now which abuse the shortcomings of DES, and made it an unstable calculation. Then AES was created which is discovered to be extremely unpredictable for Android Message Application. This algorithm produces keys and texts which are extremely hard to execute on the grounds that two separate keys need to be produced for both encryption and decryption. The most recent algorithm for cryptography on Android Message Applications was proposed by Manisha Madhwani which is taking into account Static Lookup table and Dynamic key. It utilizes symmetric key encryption and decryption. This application makes utilization of implicit android Intents and SMS administrator to send and get 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. [26].

According to Racherla and Saha, implementing security in wireless systems is a difficult and challenging task to the fact that mobility of users and network components and the fact that the wireless medium is susceptible interception and fraud. In their study [13] they had discussed the problems in implementing security in wireless systems and explored possible security problems and methods to improve security in wireless systems. In line with this, the study formulated more secured scheme in SMS encryption. A cascaded encryption technique will be integrated in the prolonging the secrecy of the text message.

When selecting the encryption algorithm, both efficient software and hardware implementations were taken into consideration. In the paper Approaches for the AES written by Xinmiao Zhang and Keshab K. Parhi addresses efficient hardware implementation approaches for the AES algorithm. They had stated that compared to software implementations, hardware implementations provide more physical security as well as higher speed. Different applications of the AES algorithm may require different speed/area trade-offs. Some applications, such as smart cards and cellular phones, require small area [14]. In the study, the entire encryption and decryption process will consider machine capacity in order to ensure shorter acceptable time response and information reliability.

In the study of Rayarikar, Upadhyay and Pimpale, they had focused on the development of an application on Android platform which allows the user to encrypt the messages before it is transmitted over the network. In their study, AES algorithm is being utilized alone for encryption and decryption of the text messages and at the same time, key generation is automatic [15]. In line with this, the study utilized AES for encryption and decryption as its last layer together with other 2 encryption processes which will result to further security. Also, the study has a verification and validation scheme before the decryption process starts. The application will check first the active SIM number which is on the device. Thru this, the key which is to be used on the decryption process will be verified and validated before decryption process start. This means that keys will never be sent via mobile networks.

A protocol for secure SMS message exchange to a vending machine was developed in the study of Hassinen and Hypponen. They had provided strong authentication of communicating parties, non-repudiation, and confidentiality. A program that implements this protocol was developed and tested in a partly simulated environment. In this protocol, strong user authentication is performed in order to initiate a bank transfer. [16] The proposed study attempts to implement security to end to end SMS users.

III.SMS TRANSMISSION

Typically, a message is being transmitted thru a telecommunication provider from the source to the recipient and passed on to several stations before reaching the intended recipient (See Fig. 1).

1. Base Transceiver Station (BTS)

The BTS is a telecoms base used to encourage wireless communication between subscriber's gadget and telecoms system administrator [29]. As a feature of a telecommunication network, a BTS has technologies for the encryption and decryption of communications, spectrum filtering equipment, antennas and transceivers (TRX) to name a few. A BTS typically has multiple transceivers that allow it to serve many of the cell's different frequencies and sectors [30] Likewise, secrecy of the message sent via a telecommunication line is not possible among the personnel working within the system. Tapping or disclosing the message content is still possible most especially if the personnel has his/her own agenda.

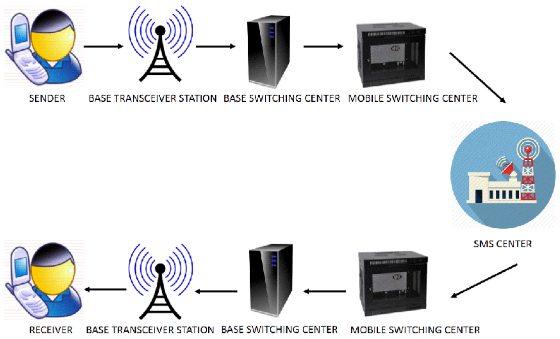


Fig. 1Telecommunication Line Model

2. Base Switching Controller (BSC)

In telecommunication, [31] a parent base switching/station controller (BSC) controls all BTSs via the base station control function (BCF) - either a different unit or incorporated with the TRX for minimized base stations. The BCF gives an association with the system administration framework (NMS) and deals with the handset's operational states.

3. Mobile Switching Center (MSC)

A mobile switching center (MSC) is [32] the centerpiece of a network switching subsystem (NSS). The MSC is mostly associated with communications switching functions, such as call set-up, release, and routing. On the other hand, it additionally performs a large group of different obligations, including steering SMS messages, telephone calls, fax, and administration charging and also interfacing with different systems, for example, people in general exchanged phone system (PSTN).

The MSC is organized so base stations unite with it, while it associate with the PSTN. Since mobile phones connect with these base stations, all types of communication, whether between two mobile phones or between a phone and a landline phone, go through the MSC.

4. SMS Center (SMSC)

When SMS is transmitted from a cell phone, the message will be received by mobile carrier's SMS Center (SMSC), do destination finding, and then send it to destination devices (mobile phone). Hence wrong selection of the destination device is possible while during the processing of sending the message.

SMSC is SMS service center which is mounted on mobile carrier core networks. Alongside as SMS forwarding, SMSC also acts as temporary storage for SMS messages. So, if the target cell phone is not active, SMS will store the message and then deliver it after the destination cell phone is active. As additional, SMSC also report the sender whether the SMS sending is success or not. However SMSC cannot store the SMS message forever since the storage capacity is not unlimited.

This is how the SMS works in general. During the SMS delivering, sender cell phone and SMSC is dynamically communicating. So, if the non-active destination cell phones become active, SMSC directly notifies the sender cell phone and tell that the SMS delivering is success [33].

The encryption process was incorporated prior to sending the message in any communication line. Thus, the message being transported before entering into the medium is already encrypted and safe for any alienation. The man in the middle who has direct manipulation the content of the message being sent thru a network prevent or at least lessen disclosure of the message . In addition, messages stored as plain messages before they will successfully delivered will also be secured from any unintended personnel.

IV.THREATS AND ATTACKS

SMS has become an extension and had played a very import role in the life of its users. In telecommunication line, only the airway traffic in the middle of the mobile station and base transceiver station is optionally encrypted with a weak and broken stream cipher which is A5 encryption process.

With this, the authentication is one-sided and also open to attackers. Likewise, identifying security threats is an important part in the process of information security.

4.1 SMS Threats and Attacks

Among known attacks on SMS are as follows [22] [23]:

1. Man-in-middle Attack: This is the system that verifies clients. The client does not authenticate network so the attacker can utilize a false BTS with the same mobile system code as the subscriber's legitimate network to impersonate himself and perform a man-in-the-middle attack.

2. Replay Attack: The attacker can abuse the transmitted messages between the user and system to perform the replay attacks.

3. Message Disclosure: Messages could be intercepted and snooped during transmission since encryption is not applied to short message transmission by default. In addition, before they are successfully delivered to the intended recipient, SMS messages are stored as plain text by the SMSC. These messages could be viewed by operators in the SMSC who have access to the messaging system.

4. Spamming: While utilizing SMS as a legitimate to advertising channel, numerous individuals have had the inconvenience of getting SMS spam. The accessibility of mass SMS broadcasting utilities makes it simple for virtually everybody to convey mass SMS messages.

5. Denial of Service (DoS) Attacks: DoS attacks are made conceivable by sending repetitive messages to a target mobile phone, making the victim’s mobile phone inaccessible.

6. SMS Phone Crashes: Some defenseless cell telephones may crash on the off chance that they get a specific kind of distorted short message. When a malformed message is received, the infected phone becomes inoperable.

7. SMS Viruses: The potential of viruses being spread through SMS is becoming greater. There have been no reports of viruses being attached to short messages, but as mobile phones are getting more powerful and programmable.

8. SMS Phishing: Similar to an Internet phishing attack using email, attackers are attempting to fool mobile phone users with bogus text messages. SMS phishing is a combination of SMS and phishing.

4.2 A5 Threats and Attacks

As of this moment, A5 encryption process is currently adopted by communication lines. There are numerous concrete algorithms which hide underneath the name "A5". Which algorithm is utilized relies on upon the provider, who, in turn, is controlled by local protocols and what it could allow from the GSM consortium. Likewise, a dynamic attacker with a fake base station can conceivably compel a cellphone to utilize an alternate variation, different from what it would have utilized something else, and there are relatively few telephones which would alarm the users about it and even less subscriber who would think about it [34].

- A5/0 means "no encryption". Information is sent as plain text. In a few nations, this is only allowed mode.
- A5/1 is the old "strong" algorithm, utilized in Europe and North America.
- A5/2 is the old "weak" algorithm, technically meant for "those countries who are good friends but that users do not totally trust nonetheless".
- A5/3 is the newer algorithm for GPRS/UMTS.

4.2.1 Mobile Telecommunication System Implementation

KASUMI is a name given to A5/3 block cipher. It provides acceptable security. It has a few issues which would make it "academically broken", but none really usable in practice [34].

A5/2 is indeed weak security protocol. The attack needs a portion of a second, subject to a pre-computation which takes less than an hour on a PC and needs a few gigabytes of storage. There are technical informations, mostly because the GSM protocol itself is complex, but one can assume that the A5/2 layer is delicate. [34]

A5/1 is stronger, but not very strong. It utilizes a 64-bit key, but the algorithm structure is weaker and permits an attack with complexity about 242.7 elementary operations. There have been number research study which talks about this complexity, mostly by doing pre-computation and waiting for the algorithm internal state to reach a specific structure; although these research studies advertise slightly lower complexity figures which is around 240, they have problems which make them difficult to apply, such as requiring thousands of known plaintext bits. With only 64 known plaintext bits, the raw complexity is 242.7 [34].

The measure of the inside condition of A5/1, and the way A5/1 is applied to encrypt data, also make it vulnerable to time-memory trade-offs, for example, rainbow tables. This assumes that the attacker ran once a truly massive computation, and stored terabytes of data; afterwards, the online phase of the attack can be quite fast. Details very-quite a bit, depending on how much storage space you have, how much CPU power is accessible for the online phase, and to what extent that the users are prepared to sit tight for the outcome. [34]

V. SECURITY REQUIREMENTS

Every security system must provide a bundle of security function that can guarantee the secrecy of the system. These functions are usually referred to as the goal of security system [24] [25] [28].

1. Authentication: This is the step of figuring out if somebody or something is, truth be told, who or what it is declared to be. This imply that before sending and receiving the information utilizing the structure, the receiver and sender character ought to be checked.

2. Data Integrity: Data integrity refers to keeping up and guaranteeing the precision and consistency of information over its whole life-cycle, and is a critical perspective to the outline, execution and utilization of any framework which stores, forms, or recovers information.

3. Service Reliability and Availability: Percentage of time a computer system is available for use. Since secure frameworks typically get attacked by intruders, which may influence their accessibility and sort of administrations to their users, such system ought to give an approach to concede their users the quality of service they anticipate.

4. Accountability: is the requirement that actions of an entity may be traced uniquely to that entity.

5. Non-repudiation: It is the confirmation that somebody can't deny something. Regularly, non-repudiation refers to the capacity to guarantee that a party to an agreement or a communication cannot deny the realness from securing their

signature on a document or the sending of a message that they started.

6. Secrecy or Confidentiality: It is a set of standards that bounds access or places restrictions on definite types of information. Generally, this feature shows how the majority of subscriber identify a sure system. It implies that just the verified individuals have the capacity to translate the message content and nobody else.

VI. CONCEPTUAL FRAMEWORK

To further strengthen security, the study used the idea of encrypting encrypted message one or more times where the user can specify either double or triple encryption using any combination of encryption algorithms. Multiple-encryption is performed on each block, before moving on to the next block, as opposed to encrypting all the data and then encrypting the resulting cypher text.

In the study, the encryption and decryption process will go thru three levels without compromising the length of the text message, which is a consideration for the users' part, and use the sender and receiver SIM number information in generating the private key for the AES algorithm.

6.1 Odd-Even Substitution

Odd-Even Substitution is a process on which the length of the messages is the consideration for the encryption process. To identify the length of the message, use the SIZE () function. The message will be converted to an 8-bit binary format based on the ASCII Table. After conversion, the generated binary numbers will be divided in to blocks. Messages having length of 1 to 80 charters or 8 to 640 bits will be divided by 32 bits per block and messages having length from 81 to 160 character or 648 to 1280 bits will be divided by 64 bit per block. After determining the number of blocks, each block will now go through separate encryption process.

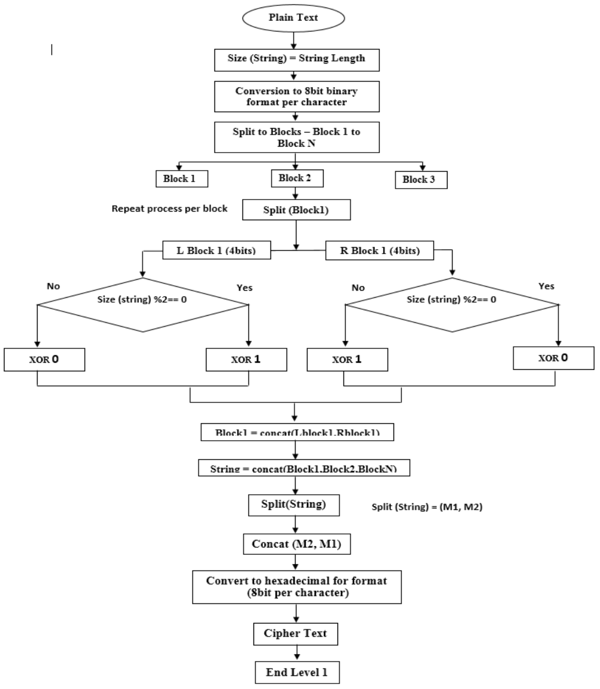

Plain Text
Size (String) = String Length
Conversion to 8bit binary format per character
Split to Blocks – Block 1 to Block N
Block 1
Block 2
Block 3
Repeat process per block
Split (Block1)
L Block 1 (4bits)
R Block 1 (4bits)
No
Yes
Size (string) %2== 0
No
Yes
Size (string) %2== 0
XOR 0
XOR 1
XOR 1
XOR 0
Block1 = concat(Lblock1.Rblock1)
String = concat(Block1.Block2.BlockN)
Split(String)
Split (String) = (M1, M2)
Concat (M2, M1)
Convert to hexadecimal for format (8bit per character)
Cipher Text
End Level 1

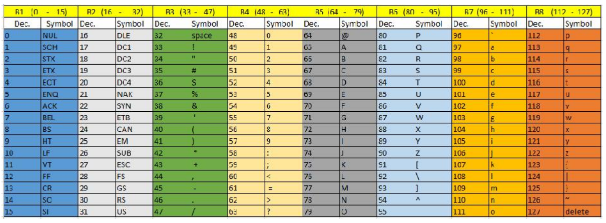
Fig. 2 ODD-EVEN Encryption Process

The next process will be dividing each block to halves. After doing this, XORing the bits per block will be based on the total number of block. If the number of blocks is odd, left half will be XORed with 0 and right half will be XORed with 1. If the number of block is even, left half will be XORed with 1 and right half will be XORed with 0. Then, all blocks will be concatenated to each other starting from Block 1 to Block N. The combined blocks will be divided into half, M1 and M2. M1 will be swapped with M2 using the CONCAT (M2, M1) function. After doing this, combined binary string will be converted to hexadecimal format. This is the cipher text produced in the first level of encryption process. This hexadecimal result will be the cypher text which is to be used on the next level of encryption process (see Fig. 2).

6.2 Folded Shifting Method

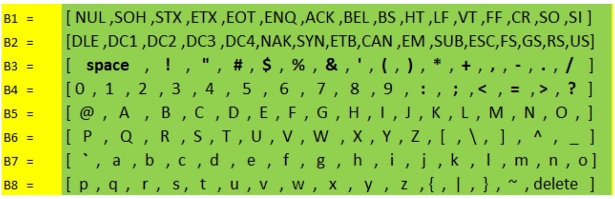
After using the ODD-EVEN substitution, the resulting value which is on hexadecimal format will undergo another encryption process. Folded Shifting Method is applied on a set of lists, folded and shifted, to which the new value of the cipher text will be derived. Figure 3 shows a conversion table which hexadecimal values are stored in an array from index zero (0) to index one hundred twenty seven (127). The entire list will be folded into 8 buckets from B1 to B8. The arrangement (index number) of character in Figure 4 is based on the decimal format per once converted. All possible key characters are included in this array of data. For shifting process, the study used the computation which is the summation of receiver's number / 11, in integer format, (decryption, user number / 11) to identify the number of shifting per bucket.

This process was used to ensure that the different cipher text will be sent to two or more users even if the plain text is the same. In the shifting process, the computed value will be used to place the n number of elements into the last part of the list. The behavior acts the same ways like a queue as an element is being transferred to the rear of the list. Using the index number, each character will be replaced by its corresponding key on Figure 4 using the current index number. The process will produce different set of arrangement because of the computation being utilized in the shifting process. Once the process is over (see Fig. 5), the cipher text being produced will undergo thru a string compression process utilizing the Run Length Encoding by Arturo San Emeterio Campos. After compression, the resulting value will go to the last encryption process.



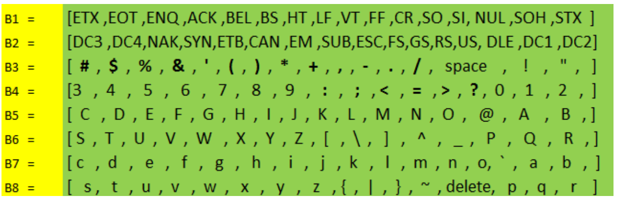
B1 (0 - 15)		B2 (16 - 32)		B3 (33 - 47)		B4 (48 - 63)		B5 (64 - 79)		B6 (80 - 95)		B7 (96 - 111)		B8 (112 - 127)	
Dec.	Symbol	Dec.	Symbol	Dec.	Symbol	Dec.	Symbol	Dec.	Symbol	Dec.	Symbol	Dec.	Symbol	Dec.	Symbol
0	NUL	16	DLE	32	space	48	0	64	@	80	P	96	`	112	p
1	SCH	17	DC1	33	!	49	1	65	A	81	Q	97	a	113	q
2	STX	18	DC2	34	"	50	2	66	B	82	R	98	b	114	r
3	ETX	19	DC3	35	#	51	3	67	C	83	S	99	c	115	s
4	ECT	20	DC4	36	$	52	4	68	D	84	T	100	d	116	t
5	ENQ	21	NAK	37	%	53	5	69	E	85	U	101	e	117	u
6	ACK	22	SYN	38	&	54	6	70	F	86	V	102	f	118	v
7	BEL	23	ETB	39	'	55	7	71	G	87	W	103	g	119	w
8	BS	24	CAN	40	(	56	8	72	H	88	X	104	h	120	x
9	HT	25	EM	41	)	57	9	73	I	89	Y	105	i	121	y
10	LF	26	SUB	42	*	58	:	74	J	90	Z	106	j	122	z
11	VT	27	ESC	43	+	59	;	75	K	91	[	107	k	123	{
12	FF	28	FS	44	,	60	<	76	L	92	\	108	l	124	|
13	CR	29	GS	45	-	61	=	77	M	93	]	109	m	125	}
14	SC	30	RS	46	.	62	>	78	N	94	^	110	n	126	~
15	SI	31	US	47	/	63	?	79	O	95		111	o	127	delete

Fig. 3 Original Substitution



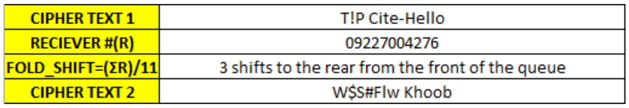
B1 =	[NUL ,SOH ,STX ,ETX ,EOT ,ENQ ,ACK ,BEL ,BS ,HT ,LF ,VT ,FF ,CR ,SO ,SI]
B2 =	[DLE ,DC1 ,DC2 ,DC3 ,DC4,NAK,SYN,ETB,CAN ,EM ,SUB,ESC,FS,GS,RS,US]
B3 =	[space , ! , " , # , $, % , & , ' , (,) , * , + , , , - , . , /]
B4 =	[0 , 1 , 2 , 3 , 4 , 5 , 6 , 7 , 8 , 9 , : , ; ,< , = ,> , ?]
B5 =	[@ , A , B , C , D , E , F , G , H , I , J , K , L , M , N , O ,]
B6 =	[P , Q , R , S , T , U , V , W , X , Y , Z , [, \ ,] , ^ , _]
B7 =	[` , a , b , c , d , e , f , g , h , i , j , k , l , m , n , o]
B8 =	[p , q , r , s, t , u , v , w , x , y , z ,{ , | , } , ~ , delete]

Fig. 4 List View Per Bucket



B1 =	[ETX ,EOT ,ENQ ,ACK ,BEL ,BS ,HT ,LF ,VT ,FF ,CR ,SO ,SI, NUL ,SOH ,STX]
B2 =	[DC3 ,DC4,NAK,SYN,ETB,CAN ,EM ,SUB,ESC,FS,GS,RS,US, DLE ,DC1 ,DC2]
B3 =	[# , $, % , & , ' , (,) , * , + , , , - , . , / , space , ! , " ,]
B4 =	[3 , 4 , 5 , 6 , 7 , 8 , 9 , : , ; ,< , = ,> , ?, 0 , 1 , 2 ,]
B5 =	[C , D , E , F , G , H , I , J , K , L , M , N , O , @ , A , B ,]
B6 =	[S , T , U , V , W , X , Y , Z , [, \ ,] , ^ , _ , P , Q , R ,]
B7 =	[c , d , e , f , g , h , i , j , k , l , m , n , o, ` , a , b ,]
B8 =	[s, t , u , v , w , x , y , z ,{ , | , } , ~ , delete, p , q , r]

Fig. 5 List View Folded and Shifted After Calculation



CIPHER TEXT 1	T!P Cite-Hello
RECIEVER #(R)	09227004276
FOLD_SHIFT=(ΣR)/11	3 shifts to the rear from the front of the queue
CIPHER TEXT 2	W$S#Flw Khoob

Fig. 6 Final Substitution Sample Output

6.3 Adaptation of XORed Result of the Combined 64 bit of Sender-Receiver SIM Numbers in Advance Encryption System Algorithm

AES algorithm is one of the most common and prominent among available encryption algorithms because of its encryption complexity yet machine friendly mechanism. In the study, the whole process of AES algorithm will be adapted. The enhancement will be on the generation of the 128 bit keys use for encryption and decryption process (see Fig. 7). The key will be derived from the last 4 digits of the sender's and receiver's phone number which will form an eight (8) digit number. The sender's SIM number will be automatically identified by the application and will be combined to the receiver's number. These will be converted to 64 bit Binary Number based on ASCII format. The result will then be XORed to one another. After achieving the XORed result, the result itself will be appended to itself to produce a 128 bit key needed for the AES process.

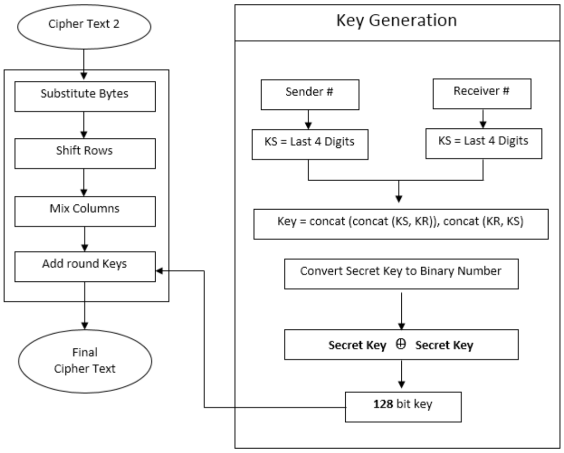


Fig. 7 AES Algorithm With Key Formulation Scheme

Aside from the key generation upon the encryption process, another good thing about the proposed study is the secret key computation for decryption process which is not sent via any other medium. In order to decrypt the cypher text another computation will be done. Thus on the decryption process, the process will validate, verify and use the current active SIM number which is on the device which is the receiver's SIM number. Then these numbers will be combined with the sender's number and will undergo on the same process done on the key generation on the encryption process resulting to a newly computed key out of the current active SIM number on the device.

VII. SYSTEM ARCHITECTURE

Fig. 8 shows the whole system architecture of the study. The plain text created by the sender user was secured using the cascaded approach for encryption process. In the proposed study, the cipher text was sent alone on any mobile network. Secret keys used for decryption were not sent to any mobile network. All keys were recomputed once decryption process was initiated.

Once the receiver got the cipher text, the application now need to identify the current active number on the mobile phone in order to proceed on the computation of the key. After the computation, the cipher text go through the inverse process of each encryption process in order to obtain the plain text. If the user reply on the sender, the whole process will take place again. In this case, the receiver will now be the new sender and the sender will now be the new receiver.

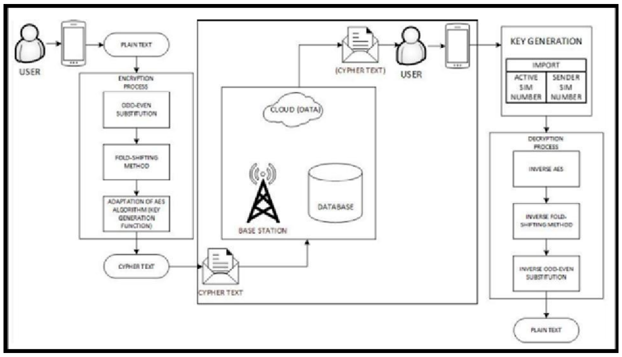


Fig. 8 System Architecture

Despite the fact that the encryption and decryption utilize the same process, the key transforming is performed in opposite order within the decryption process and the cipher text as the input. Development of decryption process is very important to make sure that the cascaded encryption algorithm can decrypt the cipher text back to its original form.

VIII. EVALUATION AND ANALYSIS

The multi-layered encryption process is divided into three layers. The first layer, Odd-Even Substitution, has the following pseudo code.

```
LEVEL 1: ODD-EVEN SUBSTITUTION                    (1)
INPUT: String plaintext
OUTPUT: String ciphertext (LEVEL 1)
size ← length(plaintext)
for i ← 0 to size -1
        c[i] ← convertAscii(plaintext[i])
div ← 4 // 32 bits
```

```
if size > 80 then
        div ← 8
count ← [size/dive]  // integer format // block count
for i ← 0 to count -1
        j ← 0
        k ← i*div
        while j<div and k+j< size
                b[i] ←b[i] ∪ c[k+j]
                j ← j+1
for i ← n to count – 1
        for j ← n to length(b[i])
                lblock ← split(b[i][j],1)
                rblock ← split(b[i][j],2)
                if i%2 = 0 then
                        lblock ← lblock XOR 0
                        rblock ← rblock XOR 1
                else
lblock ← lblock XOR 1
                        rblock ← rblock XOR 0
                b[i][j] ← concat(lblock, rblock)
        m ← m ∪ b[i]
m1 ← split(m,1)
m2 ← split(m,2)
m ← concat(m2,m1)
for i ← 0 to length(m) -1
        m[i] ← hex(m[i])
return m
```

From Level 1 encryption process, the output will undergo another encryption layer which will further strengthen and hide the plain text. The next layer, Fold-Shifting Method, used the receiver's phone number. Thus, this method will ensure that each message being sent to several number of recipient will have different message even if the plain text are all the same.

LEVEL 2: FOLD-SHIFTING METHOD (2)

INPUT: String ciphertext (from LEVEL 1), int number
OUTPUT: String ciphertext2 (from LEVEL 2)

```
copy ← number
while copy > 0
        sum ← sum + copy % 2
        copy ← copy/10
shift ← sum/11
for i ← 0 to 7
        row ← i *15
        for j ← 0 to 14
        bucket[i] ← bucket[i] ∪
asciiChar((row+j+shift+)%15)
for i ← 0 to length(ciphertext1)-1
        curr ← ascii(ciphertext1[i])
        m ← concat(m,butcket[curr/15][curr%15])
return m
```

On the last level of the cascaded encryption, the cipher text from the second level had been encryption once again utilizing the AES algorithm. The study adopted the encryption AES process. In this layer, generation of private key is based on the users' phone numbers (sender and receiver for encryption, receiver and sender for decryption). This is to ensure that no private key will be shared to a communication line.

LEVEL 3: AES KEY GENERATION (128 bits) (3)

INPUT: intsender_no, intreceiver_no
OUTPUT: 128 bit key

```
scopy ← sender_no
rcopy ← receiver_no
for i ← 0 to 3
        sdigits ← concat(sdigits, scopy%10)
        rdigits ← concat(rdigits, rcopy%10)
        scopy ← scopy/10
        rcopy ← rcopy/10
sbin ← convertbin(scopy)
rbin ← convertbin(rcopy)
key1 ← concat(sbin, rbin)
key2 ← concat(rbin, sbin)
key3 ← key1 XOR key2
key3 ← concat(key3, key3)
return key3
```

Using BlueJ, a JAVA application development tool, the pseudo code entry per layer was transformed to a java program. This was done to ensure that the processes proposed in this study is possible to be implemented on a real communication line setup.

IX. RESULT AND DISCUSSION

In the proposed multi-layered encryption process, the study simulated the SMS privacy and security enhancement and experienced a successful end to end operation. The designed cascaded encryption technique was able to encrypt and decrypt text message.

The following results were gathered thru program simulation:

```
PLAIN TEXT                                              (4)
LENGTH: 118
Hi Rey. I need to talk to you later. My bank account number
is 000111101111. Please meet me later at TIP 2 PM. Thanks.

SENDER:         09348769912
RECIPIENT:      09227094299

LEVEL1                                                  (5)
LENGTH: 118
#gv#222222222222##Tgggvg#gggv#gg#ggvgv#gv#TET#2#
TE##Tggggv#Eg#Tgv##E#gggg#vg#vggg#vg#vgv#ggvgv##
Ev#gggg#ggggvgv#gvgggv

LEVEL2                                                  (6)
LENGTH: 118
'kz'666666666666"Xkkkzk'kkkz'kk'kkzkz'kz'XIX'6'XI"Xkkkk
z'Ik'Xkz"I'kkkk'zk'zkkk'zk'zkz'kkzkz"Iz'kkkk'kkkkzkz'kzkkkz

COMPRESSION                                             (7)
LENGTH: 97
'kz'1262'X3kzk'3kz'2k'2kzkz'kz'XIX'6'XI2'X4kz'Ik'Xkz2'I'4k'
zk'z3k'zk'zkz'2kzkz2'Iz'4k'4kzkz'kz3kz
```

LEVEL3 (8)
LENGTH: 156

TClsyz14FP4g4QDqb1rfl8jRBFcLF1mbT5VI5sisvYy5Zq/FdB3cLs7lF+f7Um6zBUpZG+FepyPw
CCQJie/W0tb9ZeZb/z0pyAMcfDcNCxlyh8skTxPXGx4eDNtUywyAPanMA/KPuATWu959u6oDGQ==

Fig. 9 shows the simulation result for the running time. The cascaded technique was tested in different input sizes (from a small number (1) of character to highest (160)) on a single and regular message. The size is directly proportional to the running time behavior of the cascaded encryption process.

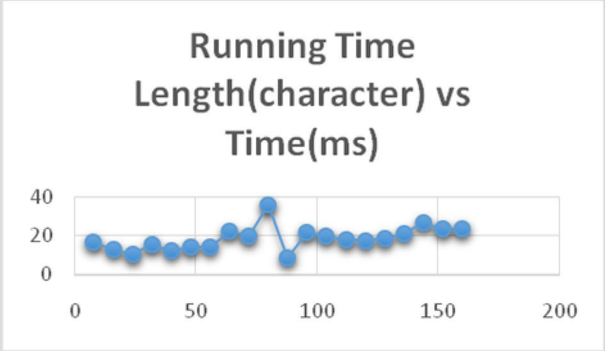


Fig. 9 Cascaded Encryption Algorithm-Running Time

Theoretically, Level 1 can be represented in $f(n) \in O(n2)$. Level 2 has $f(m,n) \in O(m + n2)$. Level 3 can be represented as $f(l,m,n) \in O(l+m+n3)$.

X. SUMMARY AND CONCLUSION

To conclude, the study is motivated by the fact of ensuring privacy and security, but solution cost was also taken into account vigorously. Several relevant works were analyzed for gathering knowledge to accomplish this research. This is an application layer protocol and low cost approach in context of computational and implementation scenario. For any SMS service, this approach can be used to ensure privacy and security. However, the operators and handset /mobile stations providers need to be aligned with this approach and cumulative understanding can ensure secured messaging with high privacy.

XI. FUTURE WORKS

For further algorithm implementation, the study is also looking forward for possibilities that the algorithm can also be applied and implemented in different environments not only in SMS communication lines but also on email, documents, social media and other transactional data for privacy and security purposes. For further enhancement, the security framework may also be compared to other encryption algorithms.

ACKNOWLEDGMENT

The researchers would like to express their sincere appreciation and deep gratitude to all participants in this work.

REFERENCES

[1] Nishika and R. Yadav,"Cryptography on Android Message Applications – A Review", Nishika et.al / International Journal on Computer Science and Engineering (IJCSE)

[2] M. 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

[3] J. Pan, Q. Ding and N. Qi , "The Research of Chaos-based SMS Encryption in Mobile Phone", 2012 Second International Conference on Instrumentation & Measurement, Computer, Communication and Control.

[4] B. Lewis, "Making Smart Cards work in the enterprise", SANS Institute InfoSec Reading Room, SANS Institute 2002,http://www.sans.org/reading_room/whitepapers/authentication/making-smart-cards-work-enterprise_138 [retrieved: April, 2011].

[5] T. Diament, H. Lee, A. Keromytis, and M. Yung," The efficient dual receiver cryptosystem and its application", International Journal of Network Security, Vol. 13, pp. 135-151, November 2010.

[6] W. Zibideh and M. Matalgah, "Modified-DES encryption algorithm with improved BER performance in wireless communication", 2011 IEEE Radio and Wireless Symposium (RWS), pp. 219-224, Phoenix, AZ, January 2011, in press.

[7] P. Rakers, L. Connell, T. Collins, and D. Russel, "Secure contactless smartcard ASIC with DPA protection", IEEE Journal of Solid-State Circuits, Vol. 36, Issue 3, pp. 559-565, 2001.

[8] O. Grabbe, "The DES algorithm illustrated", Laissez Faire City Times, Vol. 2, No. 28. (http://www.doc88.com/p-281792313650.html) [retrieved: April, 2011].

[9] D. Lisoněk, M. Drahanský,"SMS Encryption for Mobile Communication", 2008 International Conference on Security Technology

[10] L. Gilman, "Encryption of data", Encyclopedia of Espionage, Intelligence, and Security. (http://www.faqs.org/espionage/Ec- Ep/Encrption -of-Data.html) retrieved: April, 2011].

[11] D. Coppersmith, "The data encryption standard (DES) and its strength against attacks", IBM Journal of Research and Development, Vol. 38, Issue. 3, pp. 243-250, May 1994.

[12] PriyankaPimpale, Rohan Rayarikar and SanketUpadhyay, "Modifications to AES Algorithm for Complex Encryption", IJCSNS International Journal of Computer Science and Network Security, VOL.11 No.10, October 2011.

[13] G. Racherla and D. Saha, "Security and Privacy Issues in Wireless and Mobile Computing, IEEE 2000

[14] X. Zhang and K. Parhi Approaches for the AES,IEEE 2002

[15] R.Rayarikar,S. Upadhyay and P. Pimpale,"SMS Encryption using AES Algorithm on Android", International Journal of Computer Applications (0975 – 8887) Volume 50– No.19, July 2012

[16] Hassinen and Hypponen,"Strong Mobile Authentication". IEEE 2005

[17] O.Žitovský,Šifrováníkomunikacemobilníchzařízenípomocí Java ME (Communication Encryption of Mobile Devices

using Java ME), Master thesis, Masaryk University Faculty of Informatics, Brno, 2007Hassinen and Hypponen,"Strong Mobile Authentication". IEEE 2005

[18] http://www.spyphones.biz/index.php?categoryID=83

[19] GOOGLE2008,WIKIPEDIA.COM,http://en.wikipedia.org /wiki/A5/1

[20] http://developer.android.com/about/index.html

[21] http://developer.android.com/sdk/index.html?hl=sk

[22] Mohsen Toorani, Ali AsgharBeheshtiShirazi, "Solutions to the GSM Security Weaknesses", the Second International Conference on Next Generation Mobile Applications, Services, and Technologies, 2008 IEEE, pp. 576-581.

[23] NeeteshSaxena and Ashish payal, "Enhancing Security System of Short Message Service for M-Commerce in GSM", International Journal of Computer Science & Engineering Technology (IJCSET), ISSN: 2229-3345 Vol. 2 No. 4, April 2011, pp. 126-133.

[24] Al Tamimi, A., Peromance Analysis of Data Encryption Algorithms.

[25] Savola,R.,"Software Security Assurance Telecommunication Systems", 2009 IEEE.

[26] Nishika et.al, "Cryptography on Android Message Applications – A Review", International Journal on Computer Science and Engineering, Vol. 5 No. 05 May 2013.

[27] David Celdran: The Philippines – SMS and Citizenship

[28] Pourali, A., "The Presentation of an Ideal Safe SMS based model in mobile electronic commerce using Encryption hybrid algorithms AES and ECCC", 2014 IEEE.

[29] http://www.esru.strath.ac.uk/EandE/Web_sites/10-11/Mobile_mast/bts.htm

[30] http://www.techopedia.com/definition/2927/base-transceiver-station-bts

[31] http://www.techopedia.com/definition/2927/base-transceiver-station-bts

[32] http://www.techopedia.com/definition/8448/mobile-switching-center-msc

[33] http://nutsmumbai.co.in/wp-content/uploads/2013/06/SMS-Encryption-using-AES-Algorithm-on-Android-Paper-2012.pdf

[34] http://security.stackexchange.com/questions/11493/how-hard-is-it-to-intercept-sms-two-factor-authentication

[35] R.T. Marler and J.S. Arora, "Survey of multi-objective optimization methods for engineering," Struct. Multidisc. Optim. 26, pp. 369–395, 2004.

[36] M. A. M. Belal, M. K. Hasan, I. A. Nusair and N. M. Badra, 2012, "Applying Integer Linear Modeling to solve Time-Cost Tradeoff Problems in Construction Projects,"Journal of Al Azhar University Engineering Sector, Cairo, Vol. 7, No. 24, pp. 753-760, July 2012.