Journal of Engineering and Applied Sciences 12 (21): 5384-5387, 2017
ISSN: 1816-949X

Toward Trust and More Characters of Arabic Short Message Service using Encryption

Ameer Kadhim Hadi
Department of Information Networks, University of Babylon, 51001 Hilla, Babylon, Iraq

Abstract: SMS is an abbreviation for Short Message Service. It is frequently referred to as SMS messaging or "texting" as well. SMS is a technique by which text can be sent to a mobile phone via. other mobile phone, smart phone or tablets with GSM service. There are three problems in Arabic SMS first, Arabic language has cost twice more than another Latinas SMS (English), since, it has only 70 characters per one SMS while the Latinas SMS has 170/1 SMS. Second, most of the cell phone services providers are out of the country that use their services, the providers may be show the content of the SMS in additional to the probability of going the SMS to wrong side (number) accidentally. Third, the phone service sometimes be very bad since network overload especially in some events related to all people or some of them. So, the recipient will receive "some of the text is missing". This study proposes a system depends on the encryption to solve the above problems. The system applied on many types of smart phones and the experiments show that the proposed system was able to decrease the cost of the Arabic SMS to the half rate and it also succeed to increase the safety and the security of the Arabic SMS in addition to improve the services of the phone and decrease probability of receiving "some of the text is missing".

Key words: Short message service, secure Arabic SMS, increase characters per one Arabic SMS, abbreviation, probability, system

INTRODUCTION

Mobile SMS is one of most popular communication methods among people. It provides a low cost if it compare with phone call. In Iraq Arabic SMS is used by different levels of population. The standard SMS can include only 1120 bit. Arabic SMS messages similar to other language like Chinese, Korean and Japanese which use 16 bits to represent one characters. So, these languages are restricted to 70 characters per one SMS (1120/16 = 70). While Latin languages like English, French, use GSM encoding which equates to 7 bits per character; limiting 1 SMS to at most 160 characters (1120/7 = 160).

One of Arabic SMS uses is to send sensitive information like military or something related the security. So, if any attacker get this SMS as clear Arabic in the middle or the SMS send to wrong number then it will exposure and cause big threats. The operator of mobile network can see the content of SMS and this problem since, many operators are out of Iraq and not owned by the government. This study proposed a solving to the low characters per one Arabic SMS and for the security of it by using the encryption and convert Arabic SMS to English SMS before send it using an end to end encryption algorithm.

This study explored many literature and previous research. Abdullah (2009) suggested a RSA and Hoffman compression to encrypt the Arabic SMS and the study concluded that the proposed research need processing which may consume more power from the battery. Agoyi and Seral (2010) proposed an asymmetric encryption approach for English SMS for provide high security and secure channel of communication. Researchers compared RSA and Elliptic curve techniques in English SMS messages for many sizes to compute encryption time. A new method used in Nanda and Awasti for coding and cryptography of SMS. An extended approach for SMS security using authentication functions was suggested by Saxena *et al.* (2012). The SMS depend on one-time passwords showed with all possible attacks and defense by Mulliner *et al.* (2013). Many efforts explored in SMS where the researchers used the encryption of 3D-AES which is type of block cipher on Android and SMS application as by Ariffi *et al.* (2013). Classical encryption used by Fahrianto *et al.* (2014) encrypted SMS text in English language using Caesar cipher and Vigenere algorithm. Yuan *et al.* (2015) showed SMS encryption method as an android application with using chaos to make the encryption strong and hard to cryptanalysis while (Wael and Hassene, 2016) applied encryption algorithm based only on hyper chaotic system and not only chaos. Another method of encryption SMS showed by Siahaan (2016) where researchers suggested using Vernam encryption for compress English SMS and make it more secure. Finally, Kamel and George (2016) shown amodel for SMS secure exchange over mobile network.

MATERIALS AND METHODS

This study will explore the algorithms and methods are used to convert Arabic SMS to English SMS. English SMS has 170/1 SMS while Arabic SMS has only 70 characters per one. This study use to algorithms one for encrypt Arabic SMS and second for decrypt it.

Design of the propsed methods: The design of the proposed system contains from 2 phases encryption and decryption as shown in Fig. 1.

Sender should encrypt the Arabic SMS using secret key and the proposed encryption algorithm which convert it to English characters then send it over mobile phone network to the receiver. The receiver will decrypt the encrypted Arabic SMS (English SMS) using the same secret key and decryption algorithm.

Encryption method: The encryption algorithm depends on main goal of convert Arabic characters to English characters to provide more characters per one Arabic SMS. The proposed algorithm convert each Arabic to English one and keep the number and special characters as they in both side. Table 1 show the conversion method using encryption dictionary.

Encryption algorithem: This study will explore the algorithm that use to encrypt the Arabic SMS.

Algorithm encryption of Arabic SMS:

```
Input: Arabic SMS(AS) and key
Output: Encrypted Arabic SMS (EAS)
Begin:
EAS←Key
For I = 1 to length of AS
EAS =EAS+ replace AS (I) with correspond English
Character as in encryption dictionary
End for
Send EAS to the receiver phone
END algorithm
```

Decryption method: After the sender send the encrypted Arabic SMS over the mobile phone network to specific number of receiver, the decryption start on the receiver side. The receiver must input the same key to get the Arabic SMS. In this phase the encryption dictionary will use in reverse way. Algorithm decryption Arabic SMS shows all process as in algorithm.

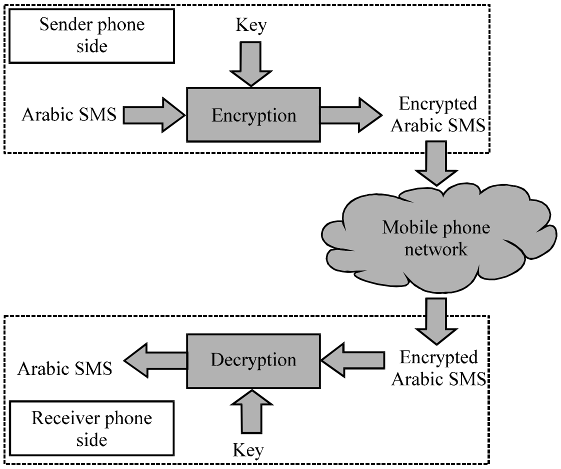


Fig. 1: General design of the proposed method

Table 1: Encryption dictionary

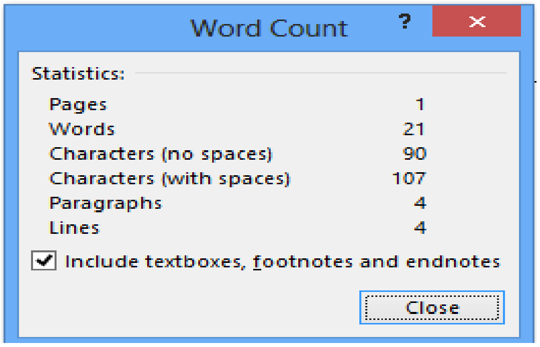
Arabic characters	Encrypted Arabic characters	Arabic characters	Encrypted Arabic characters
ذ	A	ا	B
ر	C	ب	D
ع	E	ت	F
غ	G	ث	H
ف	I	ح	J
ق	K	خ	L
و	M	ج	N
م	O	س	P
ك	Q	ش	R
ى	S	ص	T
ؤ	U	ض	V
ه	W	ط	X
د	Y	ظ	Z
ذ	a	ئ	y
ل	b	ن	k
ؤ	c	ء	t
ي	d	ة	e

Algorithm decryption of Arabic SMS:

```
Input: Encrypted Arabic SMS (EAS) and receiver key
Output: Arabic SMS (AS)
Begin
Key←Extracted the key from encrypted Arabic SMS
Counter←1
Lable 1: Input receiver key
IF key equal to receiver key then
{For I = 1 to length of (EAS)-Length of (key)
    AS = AS+replace EAS (I) with correspond Arabic
    Character as in encryption dictionary
    End for
    Display EAS}
    Else
    {Counter = Counter+1
    If Counter not equal 3 then goto Lable 1
   Write "Not Authorized"}
End If
End algorithm
```

RESULTS AND DISCUSSION

This study shows the results of experiments and examples during use the proposed methods on Arabic SMS.



Statistics:

Pages	1
Words	21
Characters (no spaces)	90
Characters (with spaces)	107
Paragraphs	4
Lines	4

☑ Include textboxes, footnotes and endnotes

Fig. 2: Statistics of Arabic SMS

Example of encrypt Arabic SMS: Lets, take this Arabic SMS; The translation mean:

“Hi Sami,
Could you please bring the lectures of Mathematics to my home at 4 p.m.?
Thank you
Ameer”

The summary of Arabic SMS is shown in Fig. 2. There are 107 in this Arabic SMS, Each 60 characters will cost 250 IQD to send them. So this SMS need 500 IQD to send it without the proposed method. The encryption for this Arabic SMS key “BJft”:

OUJDB PBOd
WbOOQk Bk FNbD OEQ
BbOJBVUBFBbLBTeDOBYeBbCdVdBFBbfDdFkBEkYBbPBEe 4
OPBtB?RQUBBqBOdVBJft”

The encrypted Arabic SMS contains 107 plus 4 characters for key so the total is 111 English characters. Each 170 characters will cost only 250 IQD, so, the sending of encrypted Arabic SMS will cost only 250 IQD and not 500 IQD.

Example of dycription: This phase will work on receiver side, the receiver input the key, the proposed system will extract the key from the encrypted Arabic SMS then it will validate with entered key. If the key is valid then the system will reverse the encryption and output the plain Arabic SMS. Wrong key will give the receiver only 3 chance to try again else the SMS will not decrypt.

CONCLUSION

The results of testing the proposed system showed increasing in the characters of Arabic SMS. This advantage implies to decrease the cost of it. Since, sending 156 Arabic characters for only 250 IDQ is cheaper than send only 70 characters for same price. This method showed that sending SMS to unauthorized receiver keep it from exposure since, the unauthorized receiver get the SMS as encrypted. Finally, the proposed method has showed a good impact on the mobile networks that come from converteach Arabic character with 16 bit to English character with 7 bit of physical representation provide a compression in the size of whole Arabic SMS andas a result the overload on the mobile network will decrease.

ACKNOWLEDGEMENTS

This study was partially funded by College of Information Technology, University of Babylon. We are thankful to our colleagues who provided skills that greatly helped the research, even they might not come to an agreement with the academic style of writing which provided in this study. We have to show our thanks to computer center for attachment their treasures of knowledge and tools with us through the working of this work. We are also immensely grateful to writing and research center in IT college for their remarks on an earlier styles of the manuscript, although any mistakes are our own and should not tarnish the standings of this appreciated side.

REFERENCES

Abdullah, A.A., 2009. Enhancing cost and security of Arabic SMS messages over mobile phone network. Raf. J. Comp. Math., 6: 111-127.

Agoyi, M. and D. Seral, 2010. SMS security: An asymmetric encryption approach. Proceedings of the 6th International Conference on Wireless and Mobile Communications (ICWMC), September 20-25, 2010, IEEE, Valencia, Spain, ISBN:978-1-4244-8021-0, pp: 448-452.

Ariffi, S., R. Mahmod, R. Rahmat and N.A. Idris, 2013. SMS encryption using 3D-AES block cipher on Android message application. Proceedings of the International Conference on Advanced Computer Science Applications and Technologies (ACSAT), December 23-24, 2013, IEEE, Kuching, Malaysia, ISBN:978-1-4799-2759-3, pp: 310-314.

Fahrianto, F., S.U. Masruroh and N.Z. Ando, 2014. Encrypted SMS application on Android with combination of caesar cipher and vigenere algorithm. Proceedings of the 2014 International Conference on Cyber and IT Service Management (CITSM), November 3-6, 2014, IEEE, South Tangerang, Indonesia, ISBN:978-1-4799-7973-8, pp: 31-33.

Kamel, M.B.M. and L.E. George, 2016. Secure model for SMS exchange over GSM. Intl. J. Comput. Network Inf. Secur., 1: 1-8.

Mulliner, C., R. Borgaonkar, P. Stewin and J.P. Seifert, 2013. SMS-based one-time passwords: Attacks and defense. Proceedings of the International Conference on Detection of Intrusions and Malware and Vulnerability Assessment, July 18-19, 2013, Springer, Berlin, Germany, pp: 150-159.

Saxena, N., N.S. Chaudhari and G.L. Prajapati, 2012. An extended approach for SMS security using authentication functions. Proceedings of the 7th IEEE Conference on Industrial Electronics and Applications (ICIEA), July 18-20, 2012, IEEE, Singapore, ISBN:978-1-4577-2118-2, pp: 663-668.

Siahaan, A.P.U., 2016. Securing short message service using Vernam Cipher in Android operating system. IOSR. J. Mob. Comput. Appl., 3: 11-16.

Wael, A. and S. Hassene, 2016. A new SMS encryption algorithm based on hyperchaotic system. Proceedings of the 2nd International Conference on Advanced Technologies for Signal and Image Processing (ATSIP), March 21-23, 2016, IEEE, Monastir, Tunisia, ISBN:978-1-4673-8527-5, pp: 57-62.

Yuan, F., G.Y. Wang and B.Z. Cai, 2015. Android SMS encryption system based on chaos. Proceedings of the IEEE 16th International Conference on Communication Technology (ICCT), October 18-20, 2015, IEEE, Hangzhou, China, ISBN:978-1-4673-7004-2, pp: 856-862.