Real Implantation for SMS Encryption–Based on Android Message Application

Monther H. M. Al-Bsool
Department of Information Technology, AL-Balqa' Applied University/
AL-Huson College, PO box 50, Al-Huson, Irbid – Jordan

Abstract
Short Message Service (SMS) is a very popular way for mobile phone and portable device users to send and receive simple text messages. Unfortunately, SMS does not offer a secure environment for confidential data during transmission. This paper deals with an SMS encryption for mobile communication on Android message application. The transmission of an SMS in mobile communication is not secure. Therefore, we have implemented three of block cipher symmetric cryptography algorithms (i.e. AES algorithm, DES, and 3-DES) and compared between three of them in terms of encryption and decryption delay time. This provides a guideline for the choice of the most suitable cryptography algorithm for mobile communication on Android message application. From our experiment tests, the DES encryption algorithm has low encryption delay time in different message sizes (i.e. 32, 64,128,256,512, and 1024) bit.

Keywords: SMS, Mobile Application, Android, Encryption

1. Introduction

Nowadays, SMS is more and more common among mobile phone users. SMS is a text messaging service component of mobile phone, web, or mobile communication systems, using standardized communications protocols that allow the exchange of short text messages between fixed line or mobile phone devices. Users can used SMS to send or receive from a single person, or several persons, personal messages, email notifications, information services [1], school activity alerts, notification from teacher, job dispatches, and also stock alerts. However, the security issue [1-3] of SMS's is still an open challenging task. SMS is now a very common communication tool. The security protection of SMS messages is not yet that sophisticated and difficult to implement in practice. The confidentiality and integrity mechanisms are only specified as optional security measures that can be made available, but they are not mandatory requirements for SMS system implementation [3]. In this paper, we have implemented three of block cipher symmetric cryptography algorithms (i.e. AES algorithm, DES, and 3-DES) and compared between three of them in terms of encryption and decryption delay time. This provides a guideline for the choice of the most suitable cryptography algorithm for mobile communication on Android message application.

2. Short Message Services (SMS)

As mentioned earlier in the previous section, SMS provides a convenient means for people to communicate with each other using text messages (i.e. mobile devices). Each message can contain at most 140 bytes of data, the equivalent of up to 160 English characters, or 70 Chinese characters. Solutions for e-Marketers are available to deliver bulk SMS messages to a large group of people, instead of sending SMS messages one by one manually [4]. There are many of software tools are used to collect phone numbers from imported text files or contact information stored in mobile phones [5]. The overview of the SMS transmission (SMS user equipment) is shown in Figure 1.

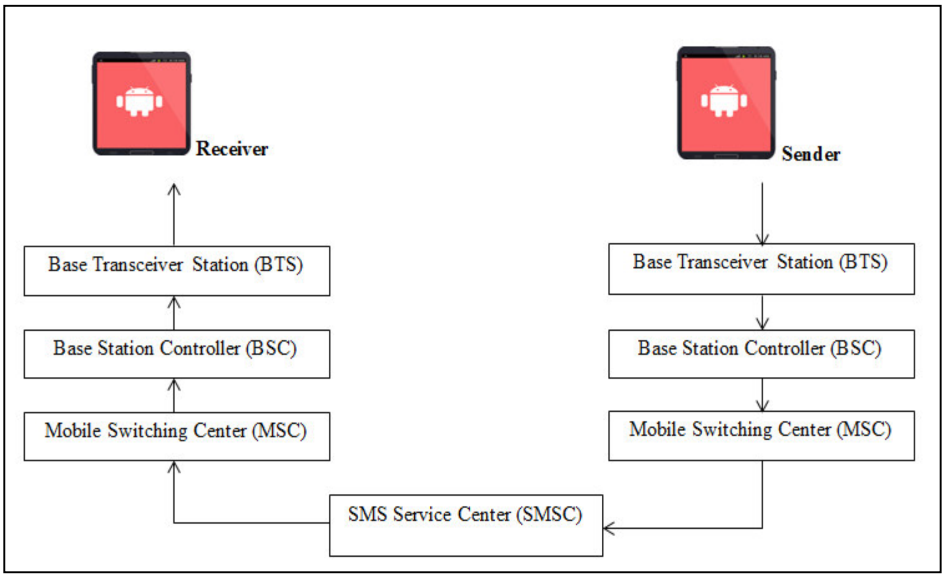

Receiver
Sender
Base Transceiver Station (BTS)
Base Station Controller (BSC)
Mobile Switching Center (MSC)
Base Transceiver Station (BTS)
Base Station Controller (BSC)
Mobile Switching Center (MSC)
SMS Service Center (SMSC)

Figure 1. SMS Transmission

2.1 SMS User Equipment

As mentioned earlier, SMS provides a convenient means for people to communicate with each other using text messages using computing devices (i.e. mobile devices). As well as SMS can also work on other computing devices such as PC, Laptop, or Tablet PC as long as they can accept SIM Card [4][5].

2.1.1 Base Transceiver Station (BTS)

A base transceiver station (BTS) is a piece of network equipment that facilitates wireless communication between a device and network. BTS consists of antennas that relay radio messages, transceivers, duplexers, amplifiers and some of equipment which is used for encryption and decryption the text messages [4].

2.1.2 Base Station Controller (BSC)

A base station controller (BSC) is a critical mobile network component that controls one or Baser Transceiver Stations (BTS), the main function of the BSC is radio network management. To make it clear, A BSC works with a mobile switching center (MSC) to provide full mobile telephony and fulfill the requirements capacity [4].

2.1.3 Mobile Switching Center (MSC)

A mobile switching center (MSC) is mostly associated with communications switching functions, such as call set-up, release, and routing. However, it also performs a host of other duties (i.e. routing SMS messages, conference calls, fax, and service billing), as well as interfacing with other networks (i.e. PSTN) [2- 4].

2.1.4 SMS Service Center (SMSC)

A Short Message Service Centre (SMSC) usually owned and run by a telecommunication operator which is responsible for the routing and delivery of SMS. When a SMS message is delivered to the SMSC, a store-and-forward message mechanism is implemented, whereby the message is temporarily stored for routing checking path, then forwarded to the recipient's phone when the recipient device is available (i.e. same as E-mail messages processes) [4]. The sub-functions of SMSC notify the sender whether the SMS delivering is success or not to the destination (Receiver Mobile phone) [5].

3. Encryption Algorithms

Cryptography encryption algorithms can be classified into two major types. Symmetric key encryption cryptography algorithm and Asymmetric key encryption cryptography algorithm as shown in Figure 2. Both of these types can be summarized as follows:

- Asymmetric Key Encryption Cryptography Algorithm

In asymmetric cryptography (i.e. double secret key), two different keys are used for encryption and decryption (i.e. public and private keys). The public key is announced and shared for all terminals on the network. Anyone who wants to encrypt the plaintext should know the public key of receiver. Only an authorized person can decrypt the cipher text through his own private key which means the private key is not be shared with anyone. Symmetric encryption algorithm compared with Asymmetric encryption algorithm runs faster. Also the memory requirement is lesser than the asymmetric one. In other words, Symmetric encryption algorithm is better than Asymmetric encryption algorithms in terms of execution delay time [9-10].

- Symmetric Key Encryption Cryptography Algorithm

In symmetric cryptography (i.e. Secret key cryptography) a single key used for encryption and decryption process at sender and receiver side respectively which is means the key must be known to both the sender and the receiver. The key plays a very important role in symmetric key encryption cryptography since the security directly depends on the nature of the key (i.e. the key length). There are a several symmetric key encryption algorithms such as DES, 3-DES, AES, RC4, RC6, and BLOWFISH [6] [9]. More details about some of symmetric key encryption cryptography algorithms are in the following sub-sections.

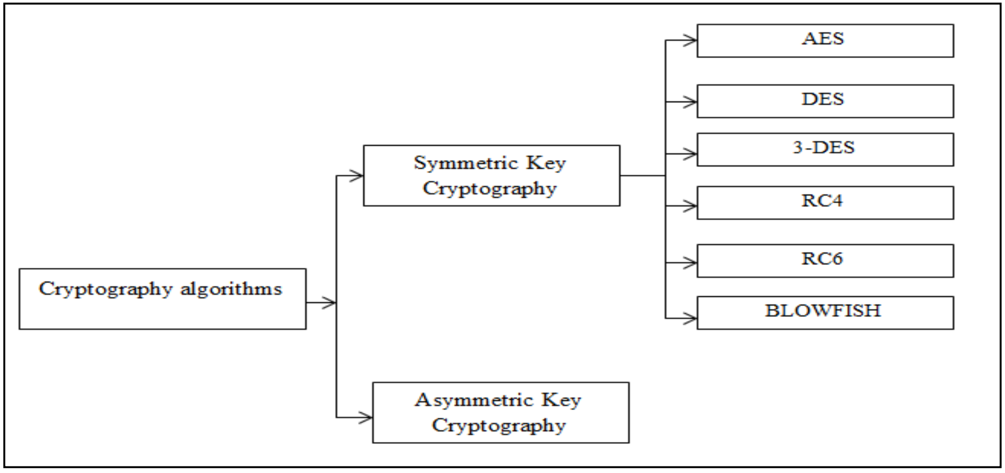


Figure 2. Classification of Cryptography Algorithms

3.1 DES

The Data Encryption Standard (DES) is a block cipher, meaning a cryptographic key and algorithm are applied to a block of data simultaneously rather than one bit at a time. To encrypt a plaintext message, DES groups the plaintext into 64-bit blocks. Each block is encrypted using the secret key into a 64-bit ciphetext by means of permutation and substitution. AES process involves 16 rounds and can run in four different modes, encrypting blocks individually or making each cipher block dependent on all the previous blocks. Decryption is simply the inverse of encryption, following the same steps but reversing the order in which the keys are applied.

3.2 AES

The Advanced Encryption Standard (AES, Rijndael algorithm) is a block cipher text the block size can be 128(AES -128), 192(AES -192) and 256 (AES -256) bits key lengths [8][9]. AES is based on round function, and different combinations of the algorithm are structured by repeating these round function different times. Each round function contains a parallel four steps, byte substitution, row shifting, column mixing and key addition, the data is passed through 10 rounds or 12 rounds or 14 rounds, and each step has its own particular functionality [6].

3.3 3-DES

3-Data Encryption Standard (3-DES) which applies the Data Encryption Standard (DES) cipher algorithm three times to each data block. The key size is increased in 3-DES to ensure additional security through encryption capabilities. Each block contains 64 bits of data. Three keys are referred to as bundle keys with 56 bits per key for each time [6].

4. Design and Implementation

The SMS encryption application works with SMS on Android platform, which the SMS is encrypted in the first step at sender side, digitally signed in the second step and sent in the last step (i.e. Receiver side) which involves of reversing all that has happened in the encryption process (i.e. Sender side) as shown in Figure 3.

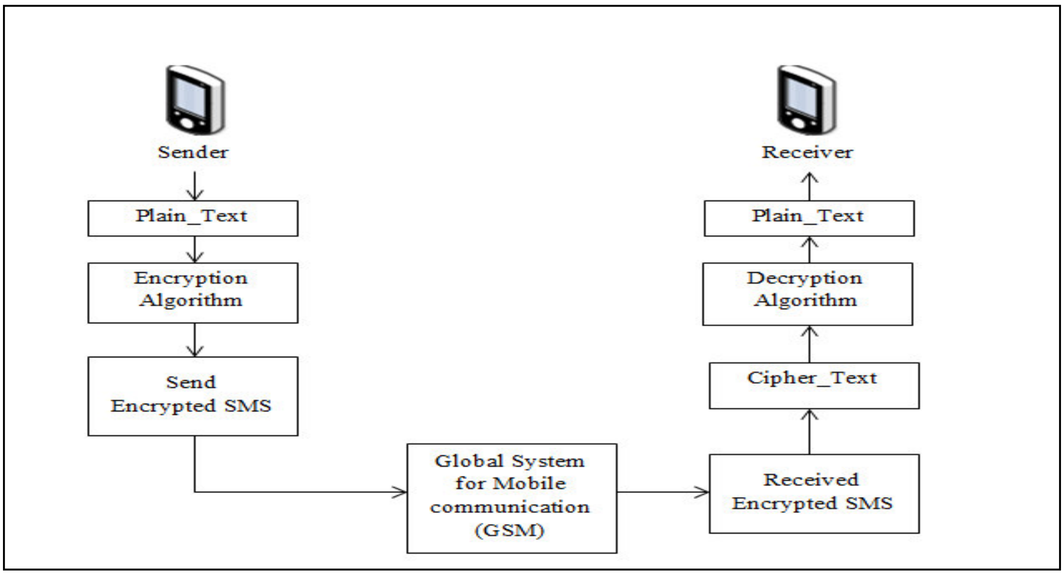
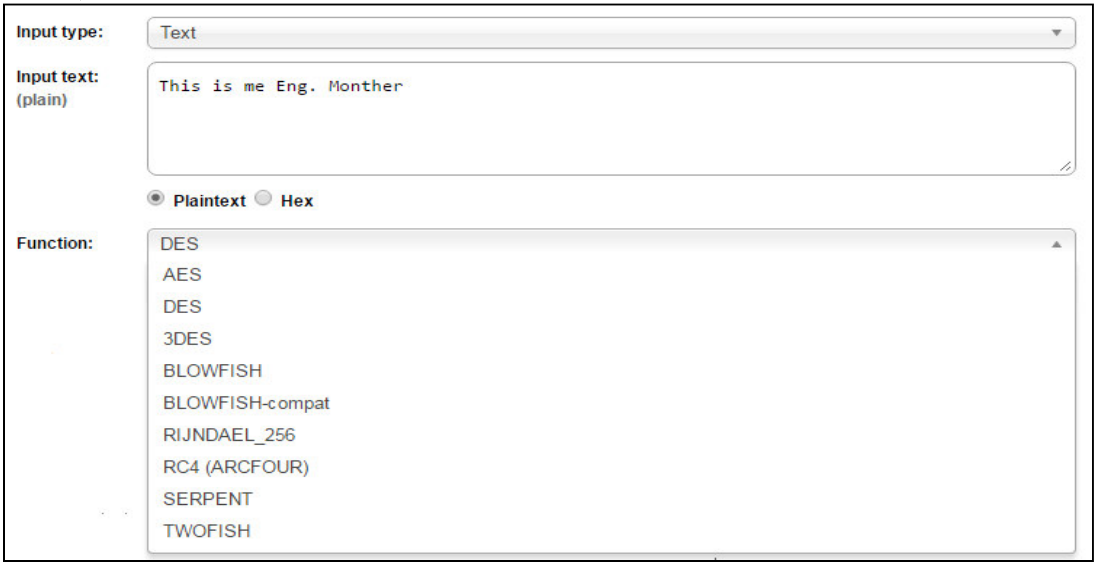


Figure 3. SMS Encryption and Decryption

As mentioned earlier, this application was tested on Android OS, v4.1.2 (Jelly Bean), Cortex-A5 processor mobile phone running at 1 GHz speed with dual SIM option, and 2 GB internal Memory and 512 MB RAM. The performance data were collected by applying a set of random SMS message (i.e. Plaintext) with a different size on the mobile phone to get the encryption delay time for three of block cipher symmetric cryptography algorithms (i.e. AES algorithm, DES, and 3-DES).

5. Application Snapshots

Some of the important snapshots of our Android SMS encryption application are shown in the Figure 4, 5, 6 and 7 respectively.



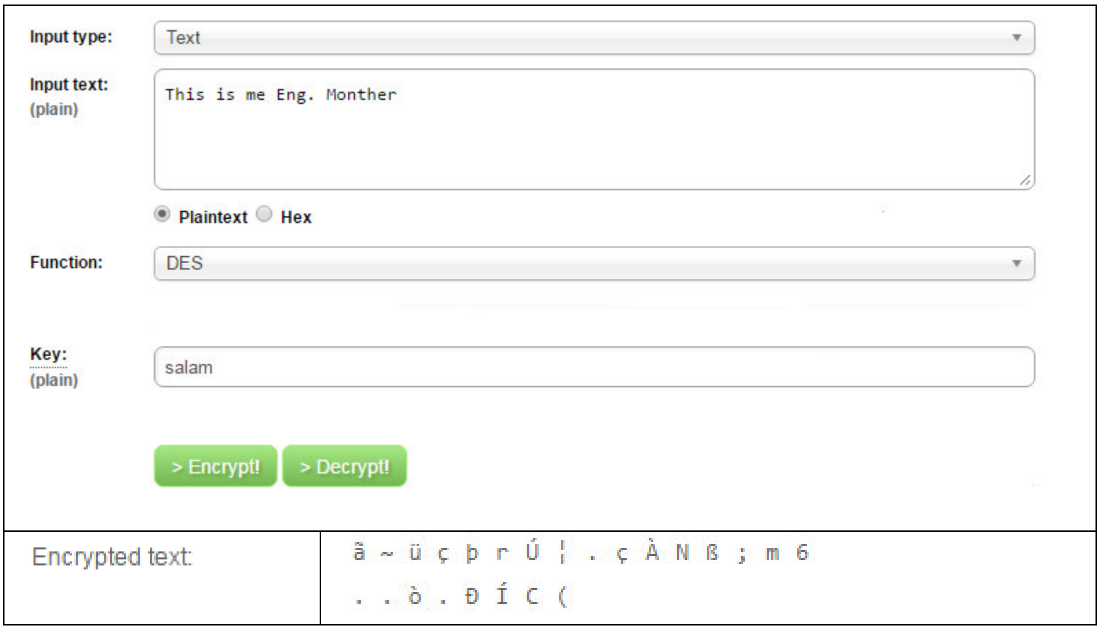
Input type: Text

Input text: (plain) This is me Eng. Monther

● Plaintext ○ Hex

Function: DES

Figure 4. Select SMS Encryption Algorithm from Options



Input type: Text

Input text: (plain) This is me Eng. Monther

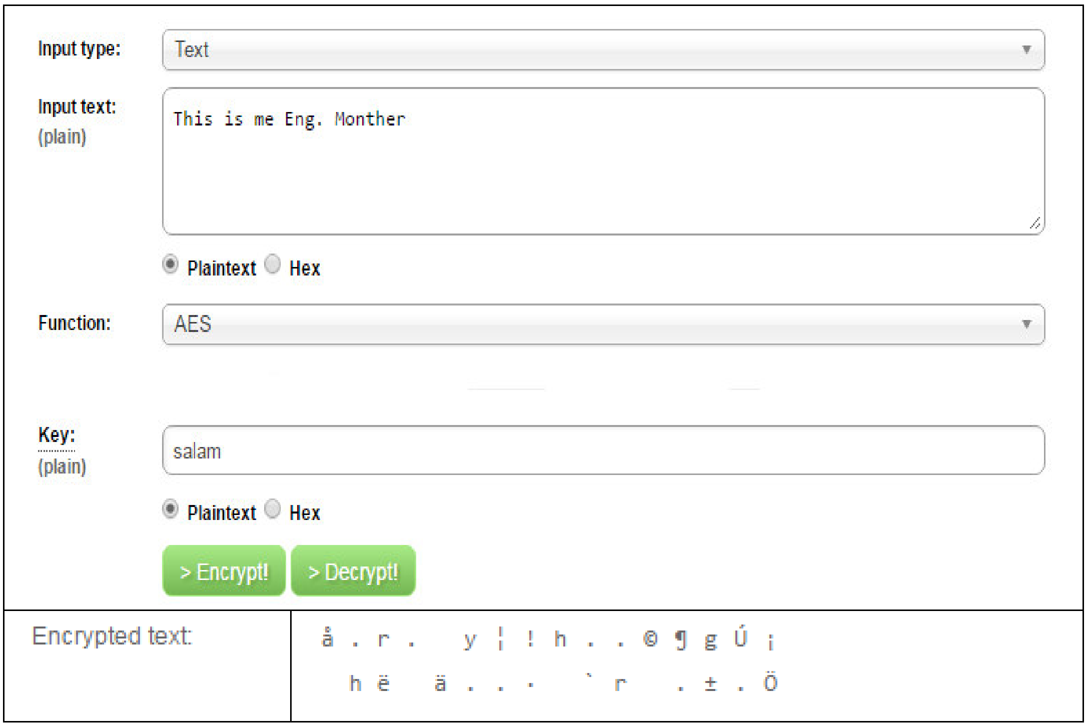
● Plaintext ○ Hex

Function: DES

Key: (plain) salam

Encrypted text: ã ~ ü ç þ r Ú ¦ . ç À N ß ; m 6
. . ò . Đ Í C (

Figure 5. Encryption SMS using DES Algorithm



Input type: Text

Input text: (plain) This is me Eng. Monther

● Plaintext ○ Hex

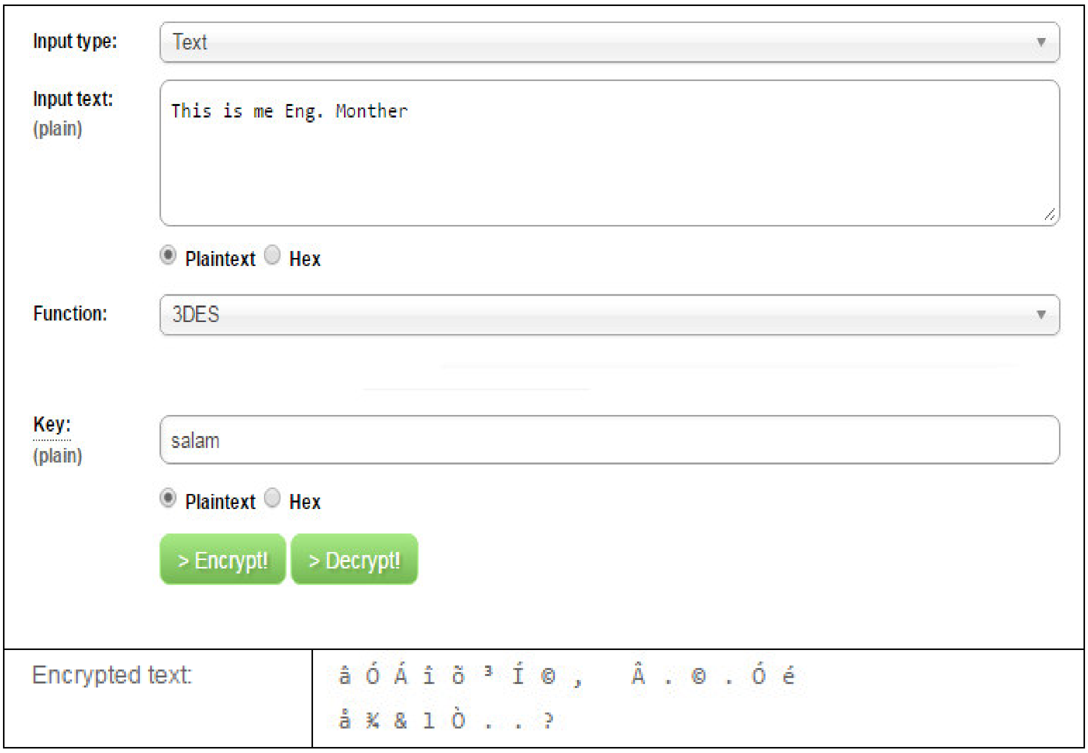
Function: AES

Key: (plain) salam

● Plaintext ○ Hex

Encrypted text: å . r . y ¦ ! h . . © ¶ g Ú ¡
h ë ä . . · ` r . ± . Ö

Figure 6. Encryption SMS using AES Algorithm



Input type: Text

Input text: (plain)
This is me Eng. Monther

● Plaintext ○ Hex

Function: 3DES

Key: (plain)
salam

● Plaintext ○ Hex

Encrypted text: â Ó Á î ö ³ Í © ,   Â . © . Ó é
å ¾ & 1 Ò . . ?

Figure 7. Encryption SMS using 3-DES Algorithm

6. Results and Discussion

Encryption delay time is the time taken to convert the SMS plaintext (i.e. Original SMS) into cipher text (i.e. Encrypted SMS). For each key size of same algorithm, random SMS message of different bit sizes was encrypted. Based on our experimental test, we have calculated the delay time introduced by each cryptographic encryption algorithm (i.e. AES, DES, and 3-DES) as shown in the Table 1.

Table 1. Encryption delay time for AES, DES, and 3-DES (millisecond)

Plain_text size	AES	DES	3-DES
32-bit	42	21	110
64-bit	72	33	180
128-bit	141	68	282
256-bit	292	182	438
512-bit	407	307	811
1024-bit	873	510	1492

It is clear from Table 1, that encryption delay time and the plaintext (i.e. SMS) size are related. Increase the plaintext size which increase the encryption delay time. To make it clear, Figure 8 shows the line charts of the encryption delay time (millisecond) for each of the SMS encryption algorithm (i.e. AES, DES, and 3-DES).

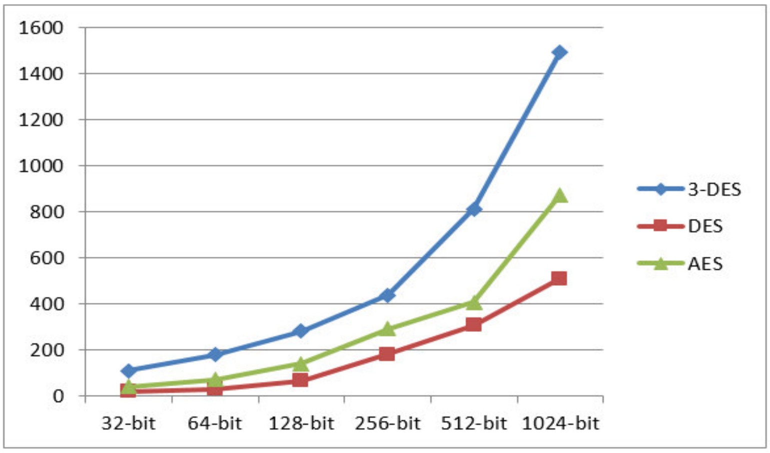


Figure 8. Delay time for SMS Encryption Algorithms

It is clear from Figure 8 DES encryption algorithm has low encryption time in different message size (i.e. 32, 64,128,256,512, and 1024) bit compared with AED, and 3-DES.

7. Conclusion

Using SMS for communication and information exchange, care should be taken when sensitive information is transmitted using SMS through unsecure channel. The users should be aware that SMS messages might be subject to interception from un-authorized access. In this paper, the application of SMS encryption for some of block cipher cryptographic encryption algorithms (i.e. AES, DES, 3-DES) on android application has been designed and implemented. The SMS encryption application is running in the mobile phone which does not require any additional encryption devices. The experimental test showed that the encryption algorithms (i.e. AES, DES, and 3-DES) are suitable and easy to implement in mobile device. As well as, the experimental test showed that the DES has low encryption delay time when applied to in different message size (i.e. 32, 64,128,256,512, and 1024) bit.

8. Acknowledgement

The authors would like to thank all the people who have supported this work, special thanks to Dr. Obaida M. Al-Hazaimeh.

References

[1] Harb, Hany, Hassan Farahat, and Mohamed Ezz. "SecureSMSPay: secure SMS mobile payment model." In *Anti-counterfeiting, Security and Identification, 2008. ASID 2008. 2nd International Conference on*, pp. 11-17. IEEE, 2008.

[2] Lisoněk, David, and Martin Drahansky. "Sms encryption for mobile communication." In *Security Technology, 2008. SECTECH'08. International Conference on*, pp. 198-201. IEEE, 2008.

[3] Rayarikar, Rohan, Sanket Upadhyay, and Priyanka Pimpale. "SMS Encryption using AES Algorithm on Android." *International Journal of Computer Applications* 50, no. 19 (2012).

[4] Ariffi, Suriyani, Ramlan Mahmod, Ratini Rahmat, and Nuzul Annisa Idris. "SMS Encryption Using 3D-AES Block Cipher on Android Message Application." In *Advanced Computer Science Applications and Technologies (ACSAT), 2013 International Conference on*, pp. 310-314. IEEE, 2013.

[5] Hassinen, Marko. "SafeSMS-end-to-end encryption for SMS." In*Telecommunications, 2005. ConTEL 2005. Proceedings of the 8th International Conference on*, vol. 2, pp. 359-365. IEEE, 2005.

[6] Al-Hazaimeh, Obaida Mohammad Awad. "a new approach for complex Encrypting and decrypting data." *International Journal of Computer Networks & Communications* 5, no. 2 (2013): 95.

[7] Al-Hazaimeh, Obaida. "Increase the security level for real-time application using new key management solution." *International Journal of Computer Science Issues* 9, no. 3 (2012).

[8] Al-Qasrawi, Isra Sitan, and Obaida Mohammed Al-Hazaimeh. "A PAIR-WISE KEY ESTABLISHMENT SCHEME FOR AD HOC NETWORKS."*International Journal of Computer Networks & Communications* 5, no. 2 (2013): 125.

[9] Al-Hazaimeh, Obaida Mohammad Awad. "Design of a New Block Cipher Algorithm." *Network and Complex Systems* 3 (2013): 1-6.

[10] Al-hazaimeh, Obaida M. "A novel encryption scheme for digital image-based on one dimensional logistic map." *Computer and Information Science* 7, no. 4 (2014): 65.