IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 18, Issue 6, Ver. II (Nov. - Dec. 2016), PP 54-58
www.iosrjournals.org

SMS EncryptionUsing One-Time Pad Cipher

Muhammad Iqbal[1], Muhammad Akbar Syahbana Pane[2],
Andysah Putera Utama Siahaan[3]
Faculty of Computer Science
[1,3]Universitas Pembangunan Panca Budi
[2]Universiti Malaysia Perlis
[1,3]Jl. Jend. Gatot Subroto Km. 4,5 Sei Sikambing, 20122, Medan, Sumatera Utara, Indonesia
[2]02600 Arau, Perlis, Malaysia

***Abstract**: The content of the SMS is very crucial. It consists of an imperative information. Unknown participants can not retrieve it. To protect the SMS content, the sender must provide the unique character before it is completely sent. The cryptography technique is needed. The plaintext has to be encrypted before transmitted. The one-time pad method can be applied to the plaintext. The one-time pad is one of the easiest cryptography methods. It turns the plaintext into the ciphertext by doing XOR operation to every character. It generates the new ASCII as the cipher character.*
***Keywords**: One-Time Pad, Cryptography, Security*

I. Introduction

A cell phone is one result of the development of communications technology [1][2]. There are some communications services that can be used on mobile phones, such as telephone service, video call, SMS, and MMS. Short Message Service (SMS) or short message is a function of communication that is widely used by mobile phone users. One reason the SMS became one of the most important services and necessary because SMS is easy to use and costs incurred for sending SMS is relatively inexpensive [8]. But along with the increasing number of mobile phones that use the SMS service is not offset by a factor of security that existed at the service. Many mobile phone users are not aware that SMS does not guarantee the integrity and security of the message. In communicating through SMS, messages sent information can be stolen by others. The weakness is caused due to an SMS using a universal coding standard; SMS is built with a system language program language similar to programs such as computer hardware, and mobile phones can translate all the data in a specific frequency that is open (in the air).

One SMS security process that can be used in the process of storing or sending SMS is to perform the cryptographic process [8]. A cryptographic process is usually done by scrambling the data so that the original file is not easy to read or hijacked by certain circles are not interested. Many algorithms or methods that could be used for the cryptographic process. Methods Vernam Cipher is one of the manifold symmetric key algorithm key used to perform encryption and decryption using the same key. In the process of encryption, Vernam Cipher algorithm uses way cipher stream cipher which is derived from the XOR between bit plaintext and the bit key, whereas for the binary permutation is done by reversing the binary code for each character. In this report will be discussed in the program applications that can perform cryptographic process to a file where the cryptographic process comprising encryption and decryption using the Vernam Cipher.

II. Theories

A. Cryptography

As The word cryptography is derived from the Greek, "Kryptos" meaning hidden and "graphein" which means writing. So the word cryptography can be interpreted in the form of the phrase "hidden writing." According to the Request for Comments (RFC), cryptography is the science of mathematics dealing with the transformation of data to make meaning it can not be understood (to hide its meaning), to prevent it from changing without permission or prevent it from unauthorized use [3][4][5]. If the transformation can be restored, cryptography can also be interpreted as a process of converting encrypted data back into a form that can be understood. That is, cryptography can be defined as the process to protect data in the broadest sense.

Menezes, Oorschot, and Vanstone (1996) states that cryptography is a study of mathematical techniques related to aspects of information security are like confidentiality, data integrity, authentication and entity data authentication. Authenticity means not only the provision of information security but rather a set of techniques.

In general, the encryption and decryption operations can be described mathematically as follows:

EK (M) = C (Encryption Process)
DK (C) = M (Decryption Process)

At the time of the encryption process we encrypt a message M with a key K and C. While the message is generated in the decryption process, message C is described by using a key K so that the resulting message M is the same as the previous message [6][7].Thus the security of a message depends on the key or keys that are used and does not depend on the algorithm used. So the algorithms used they can be published and analyzed, as well as products that use these algorithms can be mass produced. It does not matter if someone knows the algorithm that we use. As long as he does not know the key used, he still can not read the message.

B. One Time Pad

One Time Pad included in a group of symmetric cryptography. It contains a row of characters randomly generated keys. This cipher is implemented through a key consisting of a set of random characters that are not repetitive. At One Time Pad, each letter key is used once for a single message and not reused. The length of the key character streams equal to the length of the message [8].One Time Pad was found in 1917 by Major Joseph Mauborgne. Cipher is included into the group of cryptographic algorithms symmetry. One Time Pad (pad = paper notebooks) contain rows of characters randomly generated keys. Originally, the fruit of the one-time pad is a tape (tape) which contain rows of key characters. One pad is used only once (one time) only to encrypt the message after the pad has been used demolished so as not to be reused for other encrypting messages. Rules encryption used the same as in Vigenere Cipher. The sender uses each character key to encrypt the plaintext characters [8].

Encryption can be described as the sum of the plaintext characters with a one-time pad key character:

$$C = (P \oplus K) \qquad (1)$$

Where:

P : plaintext characters
K : key characters
C : ciphertext characters

Once the sender encrypts the message with the one-time pad, the sender destroyed the one-time pad. The recipients of the message using the same one-time pad to decrypt the ciphertext characters into characters plaintext by the equation:

$$P = (C \oplus K) \qquad (2)$$

An algorithm is said to be safe, if not there is no way to find her plaintext. Until now, only the algorithm One Time Pad (OTP) which otherwise could not be solved though given unlimited resources.Encryption on the principle of the algorithm is to combine each character in the plaintext with the characters on the keys. Therefore, the key length must be at least equal to the length of the plaintext. In theory, it is impossible to decrypt ciphertext without knowing the key. For if the key used was incorrect, erroneous results will be obtained as well, or not plaintext should be. Then each key can only be used for one message. The key collection should be done randomly so in the unpredictable opponent, and the number of key characters must be as many as the number of characters of the message.

III. Interface Design

This section describes the interface design of the SMS encryption. The following figure illustrate the function of the interface respectively.

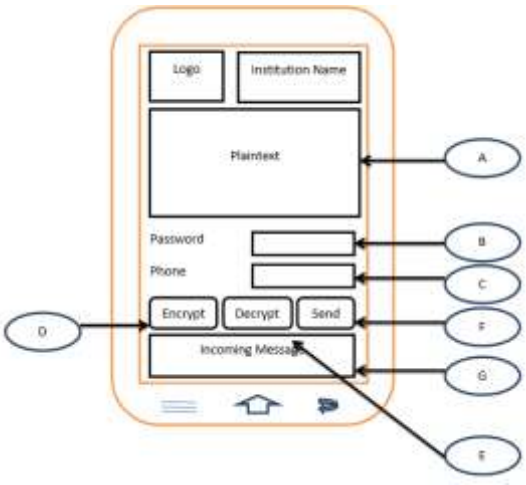

Fig. 1 SMS Interface Design

Where:
A : Message Box
B : Password Box
C : Phone Number
D : Encrypt Button
E : Decrypt Button
F : Send Button
G : Incoming Message List

IV. Result and Discussion

In a research analysis algorithm is an algorithm Vernam Cipher Key symmetric manifold where the keys used in encryption and decryption are the same keys. For encryption, algorithm it uses the stream cipher that is derived from the XOR between bit plaintext with bits Key. In this algorithm, the plaintext is converted into ASCII code and then XOR operation performed on the key that has been converted into ASCII code anyway.

A. Encryption

Let's take a look at the previous example. Tabel 1 is some of the plaintext ASCII code.
Plaintext = AKBAR

Table 1. Plaintext ASCII code

	P1	P2	P3	P4	P5
Plaintext	A	K	B	A	R
ASCII	65	75	66	65	82
Binary	1000001	1001011	1000010	1000001	1010010

If the number of key bits fewer than the number of plaintexts, the key will be looping in the one-time cipher algorithm because the number of bits in the key must be equal to the number of bits of plaintext.

Table 2. Key ASCII code

	KV1	KV2	KV3	KV4	KV5
Key	1	2	3	1	2
ASCII	49	50	51	49	50
Biner	110001	110010	110011	110001	110010

Table 2 is the code of the key. The key is repeated until the length of the plaintext is met.
The encryption calculation:

$$CT[1] = PT[1] \oplus K[1] = 65 \oplus 49 = 112$$

$$CT[2] = PT[2] \oplus K[2] = 75 \oplus 50 = 121$$

$$CT[3] = PT[3] \oplus K[3] = 66 \oplus 51 = 113$$

$$CT[4] = PT[4] \oplus K[4] = 65 \oplus 49 = 112$$

$$CT[5] = PT[5] \oplus K[5] = 82 \oplus 50 = 96$$

After the above calculation, the ciphertext is obtained. There are several characters are illegible. It shows on the screen. The ASCII 0 – 31 are usually unprinted. They are marked as or any other character. The ASCII 32 – 127 are printed and primarily used. The ASCII 128 – 255 are the extended characters that show like symbols. Table 3 shows the result after being encrypted [8].

Table 3. Ciphertext ASCII code

	CV1	CV2	CV3	CV4	CV5
Ciphertext	P	Y	q	p	`
ASCII	112	121	113	112	96
Biner	1110000	1111001	1110001	1110000	1100000

B. Decryption

To perform the decryption process, first, do the xor operation using the same formula. At this stage of the method, the ciphertext is decrypted with a key early on when to do the encryption, where the key initial plan writer is 12312.

Table 4. Decryption process

(*ciphertext* xor *key*)	ASCII	*Plaintext*
01110000 xor 00110001 = 01000001	65	A
01111001 xor 00110010 = 01001011	75	K
01110001 xor 00110011 = 01000010	66	B
01110000 xor 00110001 = 01000001	65	A
01100000 xor 00110010 = 01010010	82	R

Table 4 show the calculation of the decryption process. The ciphertext is converted back into the plaintext by using the key provided earlier. The ASCII generated is similar with the first declared.

The decryption calculation:

PT[1] = CT[1] ⊕ K[1]
= 112 ⊕49
= 65

PT[2] = CT[2] ⊕ K[2]
= 121 ⊕50
= 75

PT[3] = CT[3] ⊕ K[3]
= 113 ⊕51
= 66

PT[4] = CT[4] ⊕ K[4]
= 112 ⊕49
= 65

PT[5] = CT[5] ⊕ K[5]
= 96 ⊕50
= 82

V. Conclusion

The conclusion that can be drawn from the manufacture of security applications SMS with Vernam cipher algorithms and cipher feedback is the use of encryption on a message; then the message is confidential can be kept confidential from the parties who are not interested. Messages can only be read by someone who has authority. Between the sender and the recipient must agree in advance a password that will be used to expedite the process of sending and receiving SMS.

VI. Future Scope

In this study, certainly not free of shortcomings, and may be enhanced by subsequent researchers. To further enhance this application the author gives some suggestions, among others, these applications can be added security features, making it more awake their privacy. Encryption and decryption process in this method can be combined with other methods so that the security level is reached. Online authentication is better applied to the next security techniques to ensure the key integrity.

References

[1]. Forouzan, Cryptography and Network Security, McGraw-Hill, 2006.

[2]. Z. Ghadialy, "The SS7 Flaws that Allows Hackers to Snoop on Your Calls and SMS," The 3G4G Blog, 29 12 2014. [Online]. Available: http://blog.3g4g.co.uk/2014/12/the-ss7-flaws-that-allows-hackers-to.html. [Diakses 15 7 2016].

[3]. H. M. E. Bakry, A. E. T. E. Deen dan A. H. E. Tengy, "Implementation of a Hybrid Encryption Scheme for SMS / Multimedia Messages on AndroidI," *International Journal of Computer Applications,* vol. 85, no. 2, pp. 1-5, 2014.

[4]. S. Jha dan U. Dutta, "Review on SMS Encryption using MNTRU Algorithms on Android," *International Journal of Computer Science and Information Technologies,* vol. 6, no. 4, pp. 3855-3858, 2015.

[5]. A. P. U. Siahaan, "RC4 Technique in Visual Cryptography RGB Image Encryption," *International Journal of Computer Science and Engineering,* vol. 3, no. 7, pp. 1-6, 2016.

[6]. A. P. U. Siahaan, "Three-Pass Protocol Concept in Hill Cipher Encryption Technique," *International Journal of Science and Research,* vol. 5, no. 3, 2016.

[7]. R. Rayarikar, S. Upadhyay dan P. Pimpale, "SMS Encryption using AES Algorithm on Android," *International Journal of Computer Applications,* vol. 50, no. 19, pp. 12-17, 2012.

[8]. A. P. U. Siahaan, "Securing Short Message ServiceUsing Vernam Cipher in Android Operating System," *IOSR Journal of Mobile Computing & Application,* vol. 3, no. 4, pp. 11-16, 2016.