International Journal of Informatics and Computer Science (The IJICS)
Vol 2 No 1, March 2018
ISSN 2548-8384 (online)
ISSN 2548-8449 (print)
Page: 20-25

Implementation of Base64 Algorithm for Securing SMS on Smartphones

Ros Minarni

Department of Computer Science STMIK Budi Darma, North Sumatra, Indonesia

Abstract –In this study the authors used the base64 algorithm, the Base64 algorithm is one algorithm for encoding and decoding a data using the ASCII format, which is based on 64 base numbers or can be said to be one of the methods used to encode (encode) binary data. The results obtained from the ROSMINARNI text message example were encoded with base64 into Uk9TTUlOQVJOSQ, the application of the Base64 algorithm to secure sms messages was done by creating a cryptographic application with the help of the Java Android programming language, the process of securing SMS messages using the Base64 algorithm can run well and produce difficult ciphertext known by ordinary people.

Keywords – SMS, Security, Base64 Algorithm

1 INTRODUCTION

Many features provided by Android as a mobile phone operating system (cellphone) such as video playback, push mail, accessing internet services and so on. However, the features used on other ordinary cellphones such as Short Message Service (SMS), calls and Multimedia Message Service (MMS) can still be used on these android devices. One that is still widely used is SMS. SMS services that use the default mobile SMS application are still widely used by everyone, and are not a safe path for exchanging information, especially if important or confidential information such as passwords, pin numbers, or company secrets that may not be known by people who are not entitled.

SMS was originally designed for communication where the message sent is plaintext. Plaintext data like this can be intercepted on the road by anyone who has access to the SMS system. Short Message Service Center (SMSC) of the operator is one of the parties that can retrieve this data, although in each agreement there is a clause about data confidentiality, but the plaintext data that is sent and the file is stored in various places both on the operator's server and the content providers carry a large potential danger. Weaknesses are because SMS uses universal coding standards, SMS is built with a program language system that is similar to hardware programming languages such as computers and mobile phones that can translate all data in certain frequencies that are open (in the air) that are very vulnerable to threats such as eavesdropping on non-parties responsible [9]. The ease of exchanging information via SMS is misused by several parties. Some people try to steal information that is not their right.

One example of a 2007 SMS wiretapping case that happened to a journalist named Metta Dharma Saputra who was not a criminal, terrorist, and narcotics dealer (according to Number 36 of 1999 concerning Telecommunications and Government Regulation Number 52 of 2000) turned out to be tapped, that means that something similar can happen to anyone. This will certainly be very dangerous for users, especially for those who often send important and confidential data and information via SMS. Important or confidential information in question is information that is positive.

One of the important things in communication using a computer is ensuring the confidentiality of data. The information which is the result of the processing of data has a different value for each person. Often information becomes very valuable, and not everyone is allowed to know it. But there are always those who try to find out information in ways that are not supposed to even damage it. They often do this either online (connected to the network) or off-line (not connected to the network).

Based on the above facts, there needs to be information security both during storage and sending information. To do this there is a method which is commonly called data encoding. In this research, the author will try to implement a branch of mathematics called "Cryptography" (cryptography). With cryptography, data can be transformed into incomprehensible codes called encryption, and return them back to the original data called data decryption.

2 THEORY

2.1 Cryptography

ISSN 2548-8384 (online)
ISSN 2548-8449 (print)
Page: 20-25

Cryptography (Cryptography) comes from the Greek language, "Cryptos" means "secret" (secret) and "graphein" meaning "writing" (writing). So, cryptography means "secret writing" (secret writing). Cryptography is the science and art of maintaining message security. (Cryptography is the art and the experience of keeping messages secure). According to Kromodimoeljo [1]. In his book explains, data or information that can be read and understood its meaning is called plaintext. The encrypted plaintext is called ciphertext. Ciphertext must be transformed back into the original plaintext so that the message received can be read [1].

2.2 Base64 Algorithm

Base64 transformation is an algorithm for Encoding and Decoding a data into ASCII format, which is based on 64 base numbers or can be said to be one of the methods used to encode (encode) binary data. The characters produced in this Base64 transformation consist of A..Z, a..z and 0..9, and are added with the last two symbols which are + and/and one character equal to (=) used for adjustments and fulfill binary data or the term referred to as pad fillers. The symbol character that will be generated will depend on the algorithm that is running [7].

Cryptography Transformation Base64 is widely used in the internet world as a data format media for sending data, this is because the results of Base64 are in the form of Plaintext, so this data will be much easier to send, compared to binary data formats [7]. In Base64 Encoding can be grouped and divided into several criteria listed and can be seen in table 1.

Table 1. Encoding Base64

Index	Value	Index	Value	Index	Value	Index	Value	Index	Value
0	A	14	O	28	C	42	Q	56	4
1	B	15	P	29	D	43	R	57	5
2	C	16	Q	30	E	44	S	58	6
3	D	17	R	31	F	45	T	59	7
4	E	18	S	31	G	46	U	60	8
5	F	19	T	33	H	47	V	61	9
6	G	20	U	34	I	48	W	62	+
7	H	21	V	35	J	49	X	63	-
8	I	22	W	36	K	50	Y		
9	J	23	X	37	L	51	Z		
10	K	24	Y	38	M	52	0		
11	L	25	Z	39	N	53	1		
12	M	26	A	40	O	54	2		
13	N	27	B	41	P	55	3		

The Base64 encoding technique is actually simple, if there is one (string) bytes to be encoded into Base64 then the method is:
1. Break the string bytes to per-3 bytes.
2. Combine 3 bytes into 24 bits. With a note of 1 bytes = 8 bits, so 3 x 8 = 24 bits.
3. Then the 24 bits that are stored are buffered (broken up) broken into 6 bits, then it will produce 4 fractions.
4. Each fraction is converted to a decimal value, where the maximum value of 6 bits is 63.
5. Finally, make the decimal values into an index to select the constituent characters from base64 and the maximum is 63 or index to 64 and so on until the end of the string bytes that we want to convert. If it turns out that in the encoding process there are remaining dividers, then add as a fulfillment of the remaining characters = Then sometimes on base64 one or two characters will appear = ().

3 RESULT AND DISCUSSION

Base64 algorithm is an algorithm used to encode and decode both images and plain text, Base64 algorithm is different from other cryptographic algorithms that make changes and combine the results of encryption that has been processed, Base64 algorithm does not combine the results of the process but change a value to other value forms without combining the results and not requiring keys. The form of testing Base64 algorithm on SMS message security can be seen in the following example:

Text message = ROSMINARNI = 82 79 83 77 73 78 65 82 78 73

ISSN 2548-8384 (online)
ISSN 2548-8449 (print)
Page: 20-25

Bit = 01010010 01001111 01010011 01001101 01001001 01001110 01000001 01010010 01001110 01001001

the next step is to change the value into several blocks with the provisions of the Base64 index (table 1).

The Base64 index table above is used as the basis for changes to the binary values of the hexadecimal change images, here are the steps for the Base64 encoding process that I designed.

1. Input

Letter = ROSMINARNI
ASCII = 82 79 83 77 73 78 65 82 78 73
Bit = 0101001001001111010100110100110101001001010011100 1
000001 010100100100111001001001
Index = 20 36 61 19 19 20 37 14 16 21 9 14 18 16

2. Process

Bit = 010100 100100 111101 010011 010011 010100 100101 001110 010000 010101 001001 001110 010010 000001

The resulting bit is then converted into a 6-bit form, the following is a table that changes the process to 6 bits

Table 2. Binary 6 Bit

No	Binary 6 Bit	Decimal
1	010100	20
2	100100	36
3	111101	61
4	010011	19
5	010011	19
6	010100	20
7	100101	37
8	001110	14
9	010000	16
10	010101	21
11	001001	9
12	001110	14
13	010010	18
14	010000	16

From the above table, the decimal value of 20 36 61 19 19 20 37 14 16 21 9 14 18 16 is obtained.

3. Output

The decimal value 20 36 61 19 19 20 37 14 16 21 9 14 18 16 is then converted to ASCII in accordance with table 1 which is the Base64 algorithm index

Table 3. Output Base64 Bit

No	Decimal	Index Value
1	20	U
2	36	k
3	61	9
4	19	T
5	19	T
6	20	U
7	37	l
8	14	O
9	16	Q
10	21	V
11	9	J

ISSN 2548-8384 (online)
ISSN 2548-8449 (print)
Page: 20-25

12	14	O
13	18	S
14	16	Q

From table 3 we get the Uk9TTUlOQVJOSQ encoding results, so the ROSMINARNI messages are encoded with Base64 to Uk9TTUUOQVJOSQ

4. The description process

For the description / decoding process not much different from the encoding process, the encoding results are then converted into decimal form based on the Base64 index table and continued by changing to the 6-bit binary form which is then combined into an 8-bit binary.
Results of encoding = Uk9TTUlOQVJOSQ
Decimal = 20 36 61 19 19 20 37 14 16 21 9 14 18 16
Binary 6 Bit = 0101000 100100 111101 010011 010011 010100 100101 001110 010000 010101 001001 001110 010010 010000
Then the 6 Bit binary is combined into 8 Bit
Binary 8 Bit = 01010010 01001111 01010011 01001101 01001001 01001110 01001111 01001110 01001001

Then the 8-bit binary results have been completed, then the text will return to the beginning, namely ROSMINARNI.

4 CONCLUSION

Based on the discussion of the previous chapters that have been carried out, the following conclusions can be drawn:

1. The process of securing SMS messages using the Base64 algorithm can work well and produce ciphertext that is difficult for ordinary people to know.
2. The application of the Base64 algorithm to secure SMS messages is done by creating a cryptographic application with the help of the Java Android programming language
3. The message security system depends on the key used, in this study the key is used in strings and the author adds a hashing function that is part of the cryptographic library of the Java cryptography class.

REFERENCES

[1] S. Kromodimoeljo, TEORI & APLIKASI KRIPTOGRAFI, Jakarta: SPK IT Consulting, 2010.
[2] A. Kadir, From Zero To A Pro: Pemrograman Aplikasi Android+cd, Jogyakarta: Penerbit Andi, 2014.
[3] Yosua P. W. Simaremare, Perancangan Object Oriente Software Menggunakan UML, Penerbit Andi, 2013, Yogyakarta
[4] Haviluddin, "Memahami Penggunaan UML (Unified Modelling Language)," Jurnal Informatika Mulawarman, vol. 6, no. 1, pp. 1-15, 2011.
[5] F. W. C, A. P Rahanglar and F. D. Pretes, "Penerapan Algoritma Gabungan RC4 dan BASE64 Pada Sistem Keamanan E-Commerce," in Seminar Nasional Aplikasi Teknologi Informasi, Yogyakarta, 2012.
[6] R. V. Imbar and E. Tirta, "Analisa, Perancangan dan Implementasi Sistem Informasi Penjualan Pelumas Studi Kasus : Perusahaan "PT. Pro Roll International"," Jurnal Informatika, vol. 3, no. 1, pp. 119-149, 2007.
[7] A. P. Nugraha and E. Gunadhi, "PENERAPAN KRIPTOGRAFI BASE64 UNTUK KEAMANAN URL (UNIFORM RESOURCE LOCATOR) WEBSITE DARI SERANGAN SQL INJECTION," Jurnal Algoritma Sekolah Tinggi Teknologi Garut , vol. 13, no. 1, pp. 491-498, 2016.
[8] M. Hidayatulloh and E. Insannudin, "ENKRIPSI DAN DEKRIPSI MENGGUNAKAN VIGENERE CIPHER ASCII JAVA," Jurnal Informatika, vol. 3, no. 2, pp. 18-25, 2015.
[9] H. Abdurachman and E. Gunadhi, "KEAMANAN KOMUNIKASI DATA SMS PADA ANDROID DENGAN MENGGUNAKAN APLIKASI KRIPTOGRAPI ADVANCE ENCRYPTION STANDARD (AES)," Jurnal Algoritma, vol. 1, no. 1, pp. 1-6, 2015.
[10] T. W. W and A. Sanjaya, "STUDI SISTEM KEAMANAN KOMPUTER," Jurnal Artificial, vol. 2, no. 2, pp. 70-77, 2008.
[11] M. Afrina and A. Ibrahim, "Pengembangan Sistem Informasi SMS Gateway Dalam Meningkatkan Layanan Komunikasi Sekitar Akademika Fakultas Ilmu Komputer Unsri," Jurnal Sistem Informasi, vol. 7, no. 2, pp. 852-864, 2015.