Building Informatics, Technology and Science (BITS), Vol 1, No 1, Juni 2019
ISSN 2684-8910 (media cetak)
Hal 28-33

Implementasi Algoritma Base64 untuk Mengamakan SMS pada Smartphone

Ros Minarni

Program Studi Teknik Informatika, STMIK Budi Darma, Medan, Indonesia
Email: rosminarni313@gmail.com *)

Abstrak

Suatu fasilitas yang disediakan ponsel untuk melakukan pengiriman data berupa pesan singkat atau sering disebut SMS. SMS yang dikirimkan tidak dapat dijamin integritas dan keamanannya. Hal tersebut dikarenakan pesan yang dikirim akan disimpan di SMSC (Short Massage Service Center), tempat dimana SMS disimpan sebelum dikirim ke tujuan. Hal-hal tersebut dapat sangat merugikan jika informasi yang dicuri atau disadap adalah informasi yang bersifat penting atau rahasia. Sehingga diperlukan suatu penerapan algoritma enkripsi untuk mencegah penyadapan terhadap pesan SMS. Oleh karena itu, diperlukan algoritma untuk mengamankannya, salah satunya dengan menggunakan algoritma base64. Algoritma Base64 merupakan salah satu algoritma untuk Encoding dan Decoding suatu data dengan menggunakan format ASCII, yang didasarkan pada bilangan dasar 64 atau bisa dikatakan sebagai salah satu metode yang digunakan untuk melakukan encoding (penyandian) terhadap data binary. Hasil yang didapat dari contoh pesan teks ROSMINARNI diencoding dengan base64 menjadi Uk9TTUlOQVJOSQ, Penerapan algoritma Base64 untuk mengamankan pesan sms dilakukan dengan membuat sebuah aplikasi kriptografi dengan bantuan bahasa pemrograman Java Android, Proses pengamanan pesan SMS menggunakan algoritma Base64 dapat berjalan dengan baik dan menghasilkan *ciphertext* yang susah diketahui oleh orang awam.

Kata Kunci: SMS, Keamanan, Algoritma, Base64, Smartphone

Abstract

A facility provided by cellphones to send data in the form of short messages or often called SMS. SMS integrity and security cannot be sent. This is because messages sent will be stored in the SMSC (Short Massage Service Center), the place where the SMS is stored before being sent to the destination. These things can be very detrimental if the information stolen or tapped is information that is important or confidential. So we need an application of encryption algorithms to prevent tapping on SMS messages. Therefore, an algorithm is needed to secure it, one of them is using the base64 algorithm. The base64 algorithm is one of the algorithms for encoding and decoding data using ASCII format, which is based on basic numbers 64 or can be said as one of the methods used to encode binary data. The results obtained from the example of ROSMINARNI text messages are encoded with base64 to be Uk9TTUlOQVJOSQ, Application of Base64 algorithm to secure SMS messages is done by creating a cryptographic application with the help of the Java Java programming language. known by lay people.

Keywords: SMS, Security, Algorithm, Base64, Smartphone

1. PENDAHULUAN

Banyak fitur-fitur yang disediakan oleh Android sebagai sistem operasi telepon selular (ponsel) seperti pemutaran video, push mail, mengakses layanan internet dan sebagainya. Akan tetapi, fitur-fitur yang digunakan pada ponsel biasa lainnya yaitu seperti *Short Message Service* (SMS), *call* dan *Multimedia Message Service* (MMS) masih dapat digunakan pada perangkat android tersebut. Salah satu yang masih banyak digunakan yaitu SMS. Layanan SMS yang menggunakan aplikasi SMS bawaan ponsel masih banyak digunakan oleh setiap orang, dan bukan merupakan jalur yang aman dalam pertukaran informasi, terlebih jika informasi yang sifatnya penting atau rahasia seperti password, nomor pin, atau rahasia perusahaan yang tidak boleh diketahui oleh orang yang tidak berhak.

SMS pada awalnya dirancang untuk komunikasi dimana pesan yang dikirimkan adalah *plaintext.* Data *plaintext* seperti ini dapat dicegat di jalan oleh siapa saja yang memiliki akses ke sistem SMS. *Short Message Service Center* (SMSC) milik operator merupakan salah satu pihak yang dapat mengambil data ini, walaupun dalam setiap perjanjian terdapat klausul tentang kerahasiaan data, akan tetapi data *plaintext* yang terkirim dan berkasnya tersimpan di berbagai tempat baik di *server* milik operator maupun milik *content provider* membawa satu potensi bahaya yang besar. Kelemahan itu dikarenakan SMS menggunakan standar pengkodingan yang universal, SMS dibangun dengan sistem bahasa program yang sejenis dengan bahasa program *hardware* seperti komputer dan telepon selular dapat menerjemahkan semua data dalam frekuensi tertentu yang terbuka (di udara) yang sangat rentan akan ancaman seperti penyadapan pihak yang tak bertanggung jawab[9].

Salah satu hal yang penting dalam komunikasi menggunakan komputer adalah menjamin kerahasiaan data. Informasi yang merupakan hasil pengolahan dari data, mempunyai nilai yang berbeda bagi setiap orang. Seringkali sebuah informasi menjadi sangat berharga, dan tidak semua orang diperkenankan untuk mengetahuinya. Namun selalu saja ada pihak yang berusaha untuk mengetahui informasi dengan cara-cara yang tidak semestinya bahkan bermaksud untuk merusaknya.

Dalam penelitian ini penulis akan mencoba mengimplementasikan suatu cabang ilmu matematika yang disebut dengan "*Cryptography*" (kriptografi). Dengan kriptografi, data dapat diubah menjadi sandi-sandi yang tidak dimengerti yang disebut enkripsi, serta mengembalikannya kembali ke data semula yang disebut dekripsi data**.** Dalam penyusunan penelitian ini penulis akan menggunakan algoritma Base64, algoritma base64 merupakan algoritma encoding dan decoding yang bisa digunakan untuk pesan teks.

2. METODE PENELITIAN

2.1 Kriptografi

Kriptografi (Cryptography) berasal dari bahasa Yunani yaitu "*Cryptos*" artinya "*secret*" (rahasia) dan "*graphein*" artinya "*writing*" (tulisan). Jadi, kriptografi berarti "*secret writing*" (tulisan rahasia). Kriptografi adalah ilmu dan seni untuk menjaga keamanan pesan. (*Cryptography is the art and sience of keeping message secure*). Menurut Kromodimoeljo[1]. Dalam bukunya menjelaskan, data atau informasi yang dapat dibaca dan dimengerti maknanya disebut *plaintext*. *Plaintext* yang tersandi disebut *ciphertext*. *Ciphertext* harus dapat ditransformasikan kembali menjadi plaintext semula agar pesan yang diterima bisa dibaca[1].

2.2 Algoritma Base64

Transformasi Base64 merupakan salah satu algoritma untuk Encoding dan Decoding suatu data ke dalam format ASCII, yang didasarkan pada bilangan dasar 64 atau bisa dikatakan sebagai salah satu metoda yang digunakan untuk melakukan encoding (penyandian) terhadap data binary. Karakter yang dihasilkan pada transformasi Base64 ini terdiri dari A..Z, a..z dan 0..9, serta ditambah dengan dua karakter terakhir yang bersimbol yaitu + dan / serta satu buah karakter sama dengan (=) yang digunakan untuk penyesuaian dan menggenapkan data binary atau istilahnya disebut sebagai pengisi pad. Karakter simbol yang akan dihasilkan akan tergantung dari proses algoritma yang berjalan[7].

Kriptografi Transformasi Base64 banyak digunakan di dunia internet sebagai media data format untuk mengirimkan data, ini dikarenakan hasil dari Base64 berupa *Plaintext*, maka data ini akan jauh lebih mudah dikirim, dibandingkan dengan format data yang berupa binary[7].

3. ANALISA DAN PEMBAHASAN

Algoritma Base64 merupakan algoritma yang digunakan untuk melakukan proses *encoding* dan *decoding* baik pada citra maupun teks biasa, algoritma Base64 ini berbeda dengan algoritma kriptografi lainnya yang melakukan pengubahan dan menggabungkan hasil enkripsi yang sudah di proses, algoritma Base64 tidak menggabungkan hasil prosesnya tetapi mengubah suatu nilai ke bentuk nilai lainnya tanpa menggabungkan hasilnya dan tidak memerlukan kunci. Bentuk pengujian algoritma Base64 pada keamanan pesan SMS dapat dilihat pada contoh berikut:

3.1 Tahapan Enkripsi

Pesan SMS = ROSMINARNI = 82 79 83 77 73 78 65 82 78 73
Bit = 01010010 01001111 01010011 01001101 01001001 01001110 01000001 01010010 01001110 01001001

langkah berikutnya adalah mengubah nilai menjadi beberapa blok dengan ketentuan index Base64 sebagai berikut:

Tabel 1. Index Algoritma 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		

Tabel index Base64 diatas digunakan sebagai dasar perubahan untuk nilai binari dari gambar hasil perubahan hexadesimal, berikut adalah langkah proses encoding Base64 yang penulis rancang.

1. Input
   Huruf = ROSMINARNI

Building Informatics, Technology and Science (BITS), Vol 1, No 1, Juni 2019
ISSN 2684-8910 (media cetak)
Hal 28-33

ASCII = 82 79 83 77 73 78 65 82 78 73
Bit = 010100100100111101010011010011010100100101001110010000 01010010010011100100 1001
Index = 20 36 61 19 19 20 37 14 16 21 9 14 18 16

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

Hasil bit tersebut kemudian diubah kedalam bentuk 6 bit, berikut adalah tabel proses pengubah menjadi 6 bit

Tabel 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

Dari tabel diatas didapat nilai decimal 20 36 61 19 19 20 37 14 16 21 9 14 18 16.

3. Output
nilai decimal 20 36 61 19 19 20 37 14 16 21 9 14 18 16 kemudian dirubah kedalam bentuk ASCII sesuai dengan tabel 3.1 yang merupakan index algoritma Base64

Tabel 3. Output Base64

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
12	14	O
13	18	S
14	16	Q

Dari tabel 3 didapat hasil encoding **Uk9TTUlOQVJOSQ**, jadi pesan ROSMINARNI diencoding dengan Base64 menjadi **Uk9TTUlOQVJOSQ**

3.2 Tahapan Deskripsi

Untuk proses deskripsi / decoding tidak jauh berbeda dengan proses encoding, hasil encoding kemudian di rubah kedalam bentuk decimal berdasarkan tabel index Base64 dan dilanjutkan dengan mengubah ke bentuk binari 6 bit yang kemudian digabung menjadi binari 8 bit.

Building Informatics, Technology and Science (BITS), Vol 1, No 1, Juni 2019
ISSN 2684-8910 (media cetak)
Hal 28-33

Hasil 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

Lalu digabung binary 6 Bit nya menjadi 8 Bit
Binary 8 Bit = 01010010 01001111 01010011 01001101 01001001 01001110 01001111 01001110 01001001

Kemudian hasil binary 8 bit telah selesai, maka hasil teks akan balik ke semula yaitu ROSMINARNI

4. IMPLEMENTASI

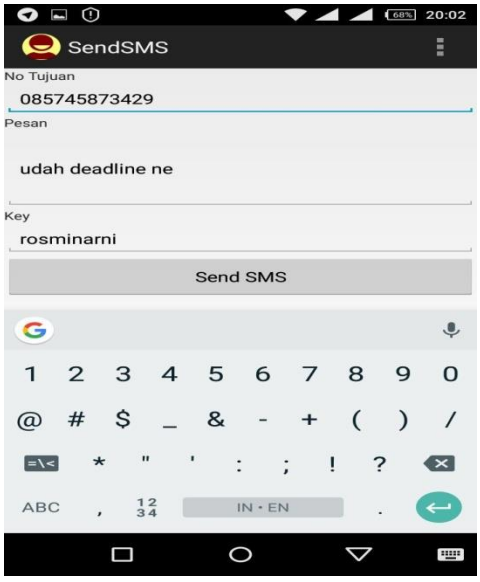
Sistem ini agar dapat berjalan tidak lepas dari *Software* yang jelas mendukung *Hardware* diatas perangkat lunak seperti Sistem Operasi dan Program Aplikasi seperti berikut

1. Sistem Operasi Windows 7 Ultimate
2. Microsoft Office 2010
3. Eclipse

Tampilan pertama program begitu dijalankan adalah seperti gambar dibawah ini.

Gambar 1. Form Utama

Gambar 1 merupakan form utama merupakan yang penulis rancang, pada gambar di atas tampak informasi tombol Kirim SMS dan Baca SMS, untuk langkah awal penulis menguji kirim SMS, berikut tampilannya



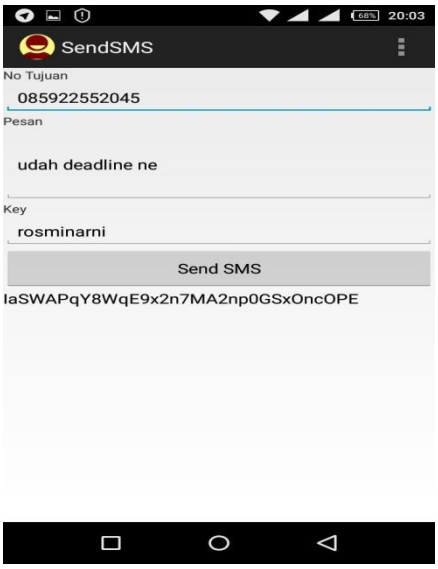
Gambar 2. Proses Pengiriman SMS

Gambar 2 merupakan form yang digunakan untuk melakukan pengiriman SMS, pada proses pengiriman SMS ada beberapa hal yang harus diperhatikan diantaranya adalah sebagai berikut:

1. No Tujuan, pada bagian ini pengguna smartphone harus memasukkan no HP tujuan penerima
2. Pesan, pada bagian ini pengguna *smartphone* memasukkan pesan SMS yang akan dikirimkan dan di enkripsi
3. *Key*, pada bagian ini pengguna *smartphone* memasukkan kunci yang digunakan sebagai proses enkripsi dan dekripsi.

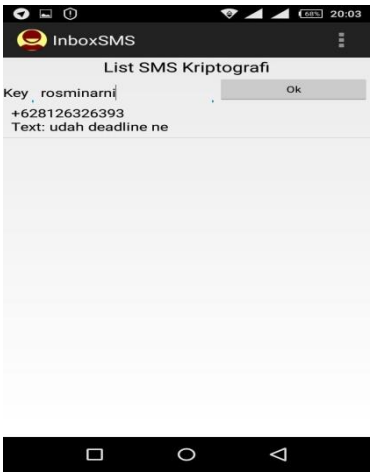
Building Informatics, Technology and Science (BITS), Vol 1, No 1, Juni 2019
ISSN 2684-8910 (media cetak)
Hal 28-33

Setelah selesai semua informasi dimasukkan berikutnya adalah menekan tombol Send SMS maka akan tampil *ciphertext* seperti berikut:



Gambar 3. Kirim SMS

Pada gambar 3 tampak informasi *ciphertext* dibagian bawa tombol Send SMS, *ciphertext* tersebut yang dikirim kepada nomor penerima, berikut adalah tampilan ketika proses dekripsi diterima di hp penerima SMS.



Gambar 4. Hasil Dekripsi

5. KESIMPULAN

Berdasarkan pembahasan dari bab-bab sebelumnya yang telah dilakukan maka dapat diambil beberapa kesimpulan sebagai berikut:

1. Proses pengamanan pesan SMS menggunakan algoritma Base64 dapat berjalan dengan baik dan menghasilkan *ciphertext* yang susah diketahui oleh orang awam.
2. Penerapan algoritma Base64 untuk mengamankan pesan sms dilakukan dengan membuat sebuah aplikasi kriptografi dengan bantuan bahasa pemrograman Java Android
3. Sistem keamanan pesan tergantung kepada kunci yang digunakan, pada penelitian ini kunci yang digunakan dalam string dan penulis menambahkan fungsi hashing yang merupakan bagian library kriptografi dari *class cryptography Java.*

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.