Implementasi Algoritma Mars Pada Pengamanan SMS

Nurainun Sinaga*, Muhammad Syahrizal

Prodi Teknik Informatika, STMIK Budi Darma, Medan, Indonesia

Email: ¹*nurainunsinaga@gmail.com, ²syahrizal83.budidarma@gmail.com

Email Penulis Korespondensi: nurainunsinaga@gmail.com

Submitted 08-05-2020; Accepted 01-06-2020; Published 14-06-2020

Abstrak

SMS (Short Message Service) merupakan sebuah revolusi teknologi komunikasi yang populer. Perkembangan teknologi komputerisasi ini sudah sangat meningkat. SMS sangat rentan terhadap penyadapan maupun pencurian data oleh pihak-pihak yang tidak bertanggung jawab. Demi menjaga keamanan SMS dapat dilakukan dengan pemanfaatan teknik kriptografi. Teknik kriptografi dapat menyandikan SMS dengan mengenkripsikannya ke dalam bentuk sandi-sandi yang tidak dipahami. Algoritma Mars adalah algoritma yang menggunakan kunci 128 bit dan proses enkripsinya terdiri dari 32 round. Algoritma simetri ini akan menghasilkan tingkat keamanan yang lebih tinggi terhadap citra usg karena dapat menyandikannya ke bentuk sandi dengan proses yang cukup rumit sehingga akan mempersulit kriptanalisis untuk mengakses citra tersebut. Penelitian ini akan menggunakan Algoritma Mars untuk proses enkripsi dan dekripsinya, sehingga dalam prosesnya perlu melalui beberapa tahap yang panjang agar dapat menghasilkan cipher akhirnya. Penelitian ini menguraikan proses pengamanan SMS dengan menyandikannya berdasarkan algoritma Mars, dalam bentuk sandi yang sulit dipahami dan dimengerti oleh orang lain. Hal ini dilakukan sebagai upaya untuk meminimalisir tindakan-tindakan penyalahgunaan SMS.

Kata Kunci: Kriptografi, Pengamanan, SMS, Mars.

Abstract

SMS (Short Message Service) is a popular communication technology revolution. The development of computerized technology has been very advanced. SMS is very vulnerable to data theft or theft by irresponsible parties. For the sake of maintaining the security of SMS can be done by using cryptographic techniques. Cryptographic techniques can encode text messages by encrypting them into passwords that are not understood. Mars algorithm is an algorithm that uses a 128-bit key and the encryption process consists of 32 rounds. This symmetry algorithm will produce a higher level of security for the ultrasound image because it can encode it into a form of cipher with a process that is complex enough so that it will be difficult for cryptanalysts to access the image. This research will use the Mars algorithm for the encryption and decryption process, so the process needs to go through several long stages in order to produce the final cipher. This study describes the process of securing SMS by encoding it based on the Mars algorithm, in the form of a password that is difficult for others to understand and understand. This is done as an effort to minimize acts of misuse of SMS.

Keywords: Cryptography, Security, SMS, Mars.

1. PENDAHULUAN

Teknik kriptografi merupakan salah satu teknik pengamanan data dengan melakukan proses penyandian terhadap data yang ingin diamankan sehingga makna asli dari data tidak lagi dapat dimengerti. Kriptografi merupakan salah satu teknik yang dapat digunakan dalam menjaga dan mengamankan informasi yang sangat penting untuk dijaga agar informasi tersebut tetap utuh dan terjamin pada saat di distribusikan dari suatu tempat ke tempat lain [1]. Perkembangan teknologi komputerisasi saat ini sudah sangat meningkat bagi pengguna komputer. Semakin tinggi teknologi komputer semakin tinggi tingkat ancaman keamanan bagi pengguna komputer. Pengguna perlu untuk menyimpan data berupa file yang berisi informasi. Salah satunya adalah SMS (*Short Message Service*) merupakan sebuah revolusi teknologi komunikasi yang sangat populer. Dengan menggunakan SMS seseorang dapat saling bertukar pesan dengan orang lain [2].

Algoritma MARS (*Multivariate Adaptive Regression Splines*) adalah salah satu kandidat AES (*Advanced Encryption Standard*) yang masuk dalam 5 besar pada AES *Competition*. Algoritma ini adalah *shared-key cipher block* dengan ukuran blok 128 bit dan ukuran kunci bervariasi antara 128 sampai 448 bit. Sebelum enkripsi blok dimulai, tiap blok dibagi menjadi empat word data yang tiap word terdiri dari 32 data. Keseluruhan operasi internal terjadi pada tiap satu word data. Langkah utama dari metode ini adalah proses ekspansi kunci, proses enkripsi, dan proses deskripsi [3].

Berdasarkan penelitian sebelumnya yang dilakukan oleh Fettiana, menyatakan bahwa aplikasi ini digunakan untuk mengamankan atau menyembunyikan pesan asli dari pihak ketiga yang ingin mengetahui isi pesan pengirim. Terdapat empat menu yaitu tulis pesan (*write*) yang digunakan untuk menulis pesan text asli (*plaintext*) dan mengubahnya menjadi pesan dalam bentuk tersembunyi (*ciphertext*) dengan memasukkan kunci rahasia sebelum menenkripsi pesan singkat tersebut, kotak masuk (*inbox*) digunakan untuk melihat daftar pesan singkat yang masuk serta mengubahnya kembali menjadi pesan text asli menggunakan kata kunci yang sama pada saat pesan singkat dikirim sehingga pesan dapat dibaca dan dimengerti, info berisi informasi tentang penggunaan aplikasi EnkripsiDes SMS dan keluar (*exit*) yaitu untuk keluar dari program aplikasi [2].

Penelitian selanjutnya yang dilakukan oleh N. Sinaga, S. Aini, S. Gulo juga menyatakan dalam penelitiannya, Kriptografi adalah ilmu yang membahas mengenai penyandian, pengamanan, dan penyamaran pesan yang memiliki tujuan untuk menghindari pengambilan pesan secara tidak sah [4].

2. METODE PENELITIAN

2.1 Kriptografi

Kriptografi (*cryptography*) berasal dari bahasa Yunani, yaitu dari kata *cypto* dan *graphia* yang berarti penulisan rahasia. Kriptografi adalah ilmu ataupun seni yang mempelajari bagaimana membuat suatu pesan yang dikirim oleh pengirim dapat disampaikan kepada penerima dengan aman. Kriptografi juga merupakan studi terhadap teknik matematis yang terkait dengan aspek keamanan suatu sistem informasi seperti kerahasiaan, integritas data, autentikasi dan ketiadaan penyangkalan[1].

2.2 SMS(Short message Service)

SMS adalah suatu fasilitas untuk mengirim dan menerima suatu pesan singkat berupa teks melalui perangkat nirkabel, yaitu perangkat komunikasi telepon selular, dalam hal ini perangkat nirkabel yang digunakan adalah telepon seluler. SMS merupakan salah satu sarana komunikasi antara semua orang di dunia. SMS sangat populer di Eropa, Asia dan Australia. Teknologi ini banyak dipilih karena selain praktis, biaya yang harus dikeluarkan untuk mengirimkan satu SMS cukup terjangkau[2].

2.3 Algoritma Mars

Algoritma MARS (*Multivariate Adaptive Regression Splines*) adalah salah satu kandidat AES (*Advanced Encryption Standard*) yang masuk dalam 5 besar pada AES *Competition*. Algoritma ini adalah *shared-key cipher block* dengan ukuran blok 128 bit dan ukuran kunci bervariasi antara 128 sampai 448 bit. Sebelum enkripsi blok dimulai, tiap blok dibagi menjadi empat word data yang tiap word terdiri dari 32 data. Keseluruhan operasi internal terjadi pada tiap satu word data. Langkah utama dari metode ini adalah proses ekspansi kunci, proses enkripsi, dan proses deskripsi[3].

Multivariate Adaptive Regression Splines (MARS) merupakan metode dengan pendekatan regresi nonparametrik yang pertama kali diperkenalkan oleh Friedman pada tahun 1991. Model MARS berguna untuk mengatasi permasalahan data berdimensi tinggi dan menghasilkan prediksi variabel respon yang akurat, dan menghasilkan model kontinu dalam *knot* berdasarkan nilai *Generalized Cross Validation* (GCV) terkecil. Permasalahan berdimensi tinggi adalah suatu permasalahan dengan jumlah variabel yang banyak serta ukuran sampel yang besar sehingga memerlukan perhitungan yang rumit. Data berdimensi tinggi yang dimaksud adalah data dengan ukuran $3 \leq v \leq 20$, dimana v adalah banyak variabel prediktor dan sampel data yang berukuran $50 \leq N \leq 1000$, dimana N untuk ukuran sampel (Friedman, 1991). Notasi yang digunakan dalam *chipper* adalah :

1. $D[]$ adalah suatu array dari 4 32 bit data word. Array ini berisikan *plaintext* dan pada akhir proses enkripsi berisikan *chipertext*.
2. $K[]$ adalah array untuk *expended key*, terdiri dari 40 32 bit.
3. $S[]$ adalah array yang berisikan *S-box*, terdiri dari 512 bit word.

Perluasan kunci berfungsi untuk membangkitkan sub kunci dari kunci yang diberikan yakni $K[]$ terdiri dari n 32 bit dan diperluas menjadi 40 32 bit sub kunci $K[]$. Tahapan yang dilakukan pada perluasan kunci adalah:

1. Kunci disimpan pada variabel sementara $T[]$ yang diset menjadi :
 $T[0 \dots n-1] = K[0 \dots n-1]$, $T[n] = n$, $T[n+1 \dots 14] = 0$
2. Kemudian diikuti dengan proses sebagai berikut :
 - a. Transformasikan $T[]$ dengan persamaan linier sebagai berikut :
 Untuk $i = 0 \dots 14$, $T[i] = T[i] \oplus ((T[i-7 \bmod 15] \oplus T[i-2 \bmod 15]) \lll 3) \oplus (4i+j)$ Dimana : j merupakan jumlah iterasi
 - b. Lakukan 4 iterasi tipe-1 *feistel network* sebagai berikut :
 Untuk $i = 0 \dots 14$, $T[i] = (T[i] \oplus S[\text{low 9 bits dari } T[i-1 \bmod 15]]) \lll 9$
 - c. Ambil 10 word data dari $T[]$ ke $K[]$:
 $K[10j + 1] = T[4i \bmod 15]$, $i = 0 \dots 9$

Terakhir, nilai $K_5, K_7 \dots K_{35}$ diubah dengan ketentuan j digunakan untuk menampung dua bit terendah dari $K[i]$, w menampung $K[i]$ yang dua bit terendahnya diubah menjadi 1. Bit mask ke l akan diset menjadi 1 jika ml terdapat 10 bit 1 atau bit 0 yang berurutan. r digunakan untuk menyimpan lima bit terendah dari $K[i-1]$, lalu $B[]$ (tabel $B[] = \{0xa4a8d57b, 0x5b5d193b, 0xc8a8309b, 0x73f9a978\}$) dirotasikan sebanyak r posisi ke kiri yang hasilnya ditampung dalam p . Terakhir p di-XOR-kan dengan w dibawah kontrol M dan disimpan di dalam K .

3. HASIL DAN PEMBAHASAN

Pengamanan informasi merupakan suatu pengamanan dalam bentuk penyandian pesan atau informasi itu sendiri, agar informasi tersebut tidak dapat dicuri oleh pihak-pihak yang tidak berkepentingan. Pengembangan ilmu teknologi jaman sekarang menemukan berbagai cara untuk dapat mencuri informasi yang telah dirahasiakan. Seiring dengan itu, dibutuhkan suatu pengamanan yang lebih kuat seperti melakukan penyandian pesan. Penyandian pesan atau informasi ini diharapkan mampu memperkuat pengamanan informasi melalui media seperti pengamanan SMS.

Pada proses pengamanan pesan sms memastikan bahwa *user* (pengguna) dan orang yang berkomunikasi dengan *user* saja yang dapat membaca apa yang dikirimkan. Pesan-pesan yang akan diamankan (enkripsi) dengan kunci dan hanya penerima dan *user* saja yang memiliki kunci special yang diperlukan untuk membuka dan membaca pesan yang dikirimkan. Untuk membuka pesan yang telah dikirim si penerima pesan harus melakukan proses dekripsi dan penggunaan kunci yang telah ditentukan oleh *user* (pengguna) sehingga pesan tersebut dapat dibaca oleh si penerima pesan.

Algoritma untuk menghasilkan kunci untuk proses enkripsi dan dekripsi terdiri dari enam langkah. Enam tahap ini akan menghasilkan sebuah angka yang merupakan salah satu bagian aliran kunci. Langkah utama dari metode ini adalah proses ekspansi kunci, proses enkripsi, dan proses dekripsi. Adapun struktur *cipher* dari algoritma Mars antara lain :

1. *forward mixing*
2. *cryptography core*
3. *backward mixing*

Notasi yang digunakan dalam *cipher* antara lain :

1. $D[]$ adalah sebuah *array* untuk 4 word 32-bit data. Inisial D berisi *plaintext* dan pada akhir proses enkripsi berisi *ciphertext*.
2. $K[]$ adalah *array* untuk *expanded key*, terdiri dari 40 word 32 bit
3. $S[]$ adalah sebuah S-box, terdiri dari 512 word 32-bit

Sampel penerapan metode mars pada pengamanan pesan SMS yaitu:

Plaintext : TEMBAKKAN DIA

Key : BUDIDARM

***Plaintext :**

Char	T	E	M	B	A	K	A	N	D
Des	84	69	77	66	65	75	65	78	68
Bin	01010100	01000101	01001101	01000010	01000001	01001011	01000001	01001110	01000100
Char	I	A							
Des	73	65							
Bin	01001001	01000001							

***Key :**

Char	B	U	D	I	D	A	R	M
Des	66	85	68	73	68	65	82	77
Bin	01000010	01010101	01000100	01001001	01000100	01010000	01010010	01001101

Proses pembangkitan kunci karena ada 16 putaran, maka dibutuhkan kunci internal sebanyak 16 buah, yaitu K_1 , K_2 , ..., K_{16} . Kunci-kunci internal ini dapat dibangkitkan sebelum proses enkripsi atau bersamaan dengan proses enkripsi. Kunci internal dibangkitkan dari kunci eksternal yang diberikan oleh pengguna. Kunci eksternal panjangnya 64 bit atau 8 karakter. Lakukan Permutation Compression (PC-1) terhadap biner kunci sesuai dengan tabel PC-1. Hal ini dilakukan untuk mengkompresikan 64 bit kunci eksternal menjadi 56 bit.

Tabel 1. Permutation Compression (PC-1)

57	49	41	33	25	17	9
1	58	50	42	34	26	18
10	2	59	51	43	35	27
19	11	3	60	52	44	36
63	55	47	39	31	23	15
7	62	54	45	38	30	22
14	6	61	53	45	37	29
21	13	5	20	20	12	4

Cara melakukan nya cari bit pada posisi ke-57 dan pindahkan pada posisi ke-1, cari bit ke 49 dan pindah kan pada posisi ke-2 cari posisi ke 41 dean pindah kan pada posisi ke-3, dan seterusnya. Gabungkan semua biner kunci kemudian lakukan Permutasi Compresi-1 (PC-1) untuk mendapatkan 56 bit pra kunci

***Biner Kunci:**

0100001001010101010001000100100101000100010100000101001001001101

***Hasil PC-1**

11000000001111110100000010000010000111010110100010000010

Hasil PC-1 di bagi menjadi 2 kelompok yang terdiri dari C_0 dan D_0 yang masing-masing terdiri dari 28 bit:

$C_0 = 1100000000111111010000001000$

$D_0 = 001000011101011010001000010$

Proses Generate key (Pembangkitan Kunci) left shift operation sebanyak 16 iterasi :

Tabel 2. Generate key (Pembangkit Kunci)

Putaran	Jumlah Putaran	C_0	D_0
		1100000000111111010000001000	0010000111010110100010000010
1	1	1000000001111110100000010001	0100001110101101000100000100
2	1	0000000011111101000000100011	1000011101011010001000001000
3	2	0000001111110100000010001100	0001110101101000100000100010
4	2	0000111111010000001000110000	0111010110100010000010001000

Putaran	Jumlah Putaran	C ₀	D ₀
5	2	0011111101000000100011000000	1101011010001000001000100001
6	2	1111110100000010001100000000	0101101000100000100010000111
7	2	1111010000001000110000000011	0110100010000010001000011101
8	2	11010000001000110000000011 11	1010001000001000100001110101
9	1	1010000001000110000000011111	0100010000010001000011101011
10	2	1000000100011000000001111110	0001000001000100001110101101
11	2	0000010001100000000111111010	0100000100010000111010110100
12	2	0001000110000000011111101000	0000010001000011101011010001
13	2	0100011000000001111110100 000	0001000100001110101101000100
14	2	000110000000011 11110100 00001	0100010000111010110100010000
15	2	0110000000011 11110100 0000100	0001000011101011010001000001
16	1	1100000000011 11110100 00001000	0010 00011101 01101000 10000010

Proses generate key(pembangkit kunci) penggabungan kembali C₀ & D₀ hasil left shift operation dan lakukan PC-2. Cara melakukan nya cari bit pada posisi ke-57 dan pindahkan pada posisi ke-1, cari bit ke 49 dan pindah kan pada posisi ke-2 cari posisi ke 41 dean pindah kan pada posisi ke-3, dan seterusnya.

Tabel 3. Permutation Commpression (PC-2)

14	17	11	24	1	5
3	28	15	6	21	10
23	19	12	4	26	8
16	7	27	20	13	2
41	52	31	37	47	55
30	40	51	45	33	48
44	49	39	56	34	53
46	42	50	36	29	32

Setelah di lakukan Generate key maka di hasilkan kunci internal untuk proses Enkripsi :

Tabel 4. Kunci Internal

Round	Biner Kunci
K[1]	111110010100100100000010100100011010 000101000
K[2]	1010000100011010001010100010010000000011000110
K[3]	101000010011001011010000100001001110001010000101
K[4]	000101000101111001010000100001001110001010000101
K[5]	010001100110000100010000001100100000000110001011
K[6]	10001110010001010100110100001100110000110001011
K[7]	10001100100010101001101000001100110000110001011
K[8]	0100101101000001000010110111101000100001010000

Proses Enkripsi

Langkah pertama

P [1] = 01010100 00000000 00000000 00000000 00000000

K[1] = 11111001 01001001 00000010 10010010 00011010 00010100 Xor

C[1] = 10100101 01001001 00000010 10010010 00011010 00010100

Lakukan sampai Langkah kedelapan

P [8] = 01001110 00000000 00000000 00000000 00000000

K[8] = 00101001 10000001 10101011 01100000 11000001 00011010 Xor

C[8] = 01100111 10000001 10101011 01100000 11000001 00011010

Plaintext = ¥ ä ì V ç Å space g

Proses Deskripsi

Untuk mendapatkan hasil plaintext dari proses dekripsi ini maka di lakukan langkah seperti pada proses enkripsi :

Langkah pertama

C[1] = 10100101 01001001 00000010 10010010 00011010 00010100

K[1] = 11111001 01001001 00000010 10010010 00011010 00010100 Xor

P[1] = 01011100 00000000 00000000 00000000 00000000 00000000

Lakukan sampai Langkah kedelapan

C[8] = 01100111 0110011110101011 01100000 11000001 00011010

K[8] = 00101001 10000001 10101011 0110000110000001 00011010 Xor

P[8] = 01001110 00000000 00000000 00000000 00000000

Dan sekarang biner plaint nya adalah diambil dari hasil P1 yang telah di ubah ke dalam kode ascii, maka di hasil kan :
Plaintext = TEMBAKKAN.

4. KESIMPULAN

Berdasarkan uraian pembahasan dari penelitian yang telah dilakukan, maka dapat diperoleh kesimpulan sebagai berikut:

1. Algoritma mars dapat mengamankan pesan dengan aman sampai pada tujuan saat pengiriman pesan. Informasi yang dikirimkan tidak dapat disadap atau dibaca oleh pihak lain tanpa memiliki kunci khusus.
2. Penerapan algoritma mars memiliki penyandian, pengamanan, dan penyamaran pesan sms yang memiliki tujuan untuk menghindari pengambilan pesan secara tidak sah

REFERENCES

- [1] J. Computech, "SISTEM PENGKODEAN DATA PADA FILE TEKS," vol. 1, no. 2, pp. 105–118, 2007.
- [2] G. P. R. S. Fettiana, Elvina, "Pembuatan Algoritma Enkripsi Des Sms Berbasis Mobile," vol. VI, no. 2, pp. 151–166, 2015.
- [3] M. Silalahi et al., "Perancangan Program Aplikasi Kriptografi," vol. 5, no. 1, pp. 14–19, 2007.
- [4] N. Sinaga, S. Aini, and B. Gulo, "Penerapan Algoritma Skipjack Untuk Menyandikan Short Message Service," no. 1, pp. 33–46, 2018.
- [5] E. Setyaningsih, Kriptografi & implementasinya menggunakan MATLAB, 1st ed. Yogyakarta: Andipublisher, 2015.
- [6] Munir rinaldi, Kriptografi. Informatika bandung, 2006.
- [7] Sadikin Rifki, Kriptografi untuk keamanan jaringan. 2012.
- [8] G. G. Maulana, "Pembelajaran Dasar Algoritma Dan Pemrograman Menggunakan El-Goritma Berbasis Web," J. Tek. Mesin, vol. 06, no. 2, pp. 69–73, 2017.
- [9] C. Algoritma, "Ketepatan Klasifikasi Status Pemberian Air Susu Ibu (ASI) Menggunakan Multivariate Adaptive Regression Splines (MARS) dan," vol. 5, pp. 229–238, 2016.
- [10] D. Sartika, "PENGEMBANGAN PERANGKAT LUNAK PENYEMBUNYIAN PESAN," vol. 7, no. 1, pp. 1–6, 2016.
- [11] A. R. ; D. Alvianto, "Pengaman Pengiriman Pesan Via SMS dengan Algoritma RSA Berbasis Android," J. SAINS dan SENI ITS, vol. 4, no. 1, pp. 1–5, 2015.
- [12] A. Kadir, Pengenalan sistem informasi. Yogyakarta: Andipublisher, 2008.
- [13] S. Dharwiyanti and R. S. Wahono, "Pengantar Unified Modeling LAnguage (UML)," IlmuKomputer.com, pp. 1–13, 2003.