TIN: Terapan Informatika Nusantara
Vol 2, No 1, Juni 2021, Hal 29-34
ISSN 2722-7987 (Media Online)
Website https://ejurnal.seminar-id.com/index.php/tin

Implementasi Algoritma Skipjack Untuk Mengamankan Audio

Rahmadani Harahap

Program Studi Teknik Informatika, Universitas Budi Darma, Medan, Indonesia
Email : rahmahrp1995@gmail.com

Abstrak−Salah satu hal yang penting untuk menjamin kerahasiaan data atau informasi adalah enkripsi. Enkripsi menggunakan suatu algoritma yang dapat mengkodekan semuaa aliran data (stream) bit dari sebuah pesan, skipjack merupakan algoritma elektronik codebook 64-bit parameter yang digunakan untuk enkripsi adalah 80-bit kunci, dan mempunyai 32 putaran untuk proses enkripsi dan dekripsi. Algoritma ini dapat digunakan pada salah satu dari empat modus ditetapkan dalam FIPS 81 untuk digunakan dalam data Encryption Standart (DES).Algoritma yang akan digunakan untuk kriptografi dikatakan aman bila meenuhi tiga kriteria. Ketiga kriteria tersebut adalah persamaan matematis yang digunakan hartus kompleks, sehingga algoritma sulit dipecahkan secara analitik, biaya yang digunakan untuk memecahkan chipertext melampaui nilai informasi, dan waktu yang diperlukan untuk memecahkan chipertext melampaui lamanya waktu informasi.Kekuatan algoritma enkripsi apapun tergantung pada kemampuan untuk menahan serangan yang ditujukan untuk menentukan key atau uncrypted communication. Secara garis besar ada dua jenis serangan, yaitu brute-force dan shortcut. Oleh karena itu pada makalah ini akan dibahas sejauhh mana algoritma skipjack menjamin keamanan suatu informasi yang disembunyikan.

Kata Kunci: Skipjack; Audio

Abstract−One of the important things to ensure the confidentiality of data or information is encryption. Encryption uses an algorithm that can encode all bit streams of a message, skipjack is a 64-bit electronic codebook algorithm. The parameters used for encryption are 80-bit keys, and have 32 rounds for the encryption and decryption process. This algorithm can be used in one of the four modes specified in FIPS 81 for use in the Data Encryption Standard (DES). The algorithm that will be used for cryptography is said to be safe if it meets three criteria. The three criteria are the mathematical equations used must be complex, so that the algorithm is difficult to solve analytically, the cost used to solve the ciphertext exceeds the value of the information, and the time required to decipher the ciphertext exceeds the length of the information time. The strength of any encryption algorithm depends on its ability to withstand attacks. which is intended to determine the key or uncrypted communication. Broadly speaking, there are two types of attacks, namely brute-force and shortcuts. Therefore, in this paper we will discuss the extent to which the skipjack algorithm guarantees the security of hidden information.

Keywords: Skipjack; Audio

1. PENDAHULUAN

Kemajuan dan perkembangan teknologi saat ini telah berpengaruh pada semua aspek kehidupan manusia, tidak terkecuali dalam hal telekomunikasi. adanya sarana seperti internet, komunikasi jarak jauh dapat dilakukan dengan cepat dan mudah. Namun disisi lain, ternyata internet tidak terlalu aman karena internet adalah sarana umum yang dapat dipergunakan oleh siapapun sehingga sangat rawan terhadap penyadap informasi oleh pihak-pihak yang tidak berhak mengetahui informasi tersebut. Karena pengguna internet begitu luas seperti bisnis, perdagangan, bank, industri. Salah satu cara yang dapat digunakan untuk pengaman informasi adalah dengan cara menggunakan sistem kriptografi.

Data atau informasi tersebut dapat berupa teks, citra/gambar, audio, dan video. Dengan adanya kemajuan teknologi informatika, data atau informasi dapat disajikan dalam bentuk digital. Akan tetapi, bentuk penyimpanan seperti ini sangat rentan dari aspek keamanannya. Data dapat dengan mudah diganti, dan dimanipulasi sehingga dapat memungkinkan terjadinya penyadapan audio. Audio adalah suara atau bunyi yang dihasilkan oleh getaran suatu benda, agar dapat tertangkap oleh telinga manusia getaran tersebut harus kuat minimal 20 kali/detik suara yaitu suatu getaran yang dihasilkan oleh gesekan, pantulan dan lain-lain, antara benda-benda. Sedangkan gelombang yaitu suatu getaran yang terdiri dari amplitude dan juga waktu, suara dibangun oleh periode, apabila tidak berarti itu bukan suara.

Audio merupakan salah satu elemen yang penting, karena ikut berperan dalam membangun sebuah sistem komunikasi dalam bentuk suara, suatu sinyal elektrik yang membawa unsur-unsur bunyi didalamnya. Audio itu terbentuk melalui beberapa tahap diantaranya, tahap pengambilan atau penangkapan suara, sambungan transmisi yang membawa bunyi, amplifer dan lain-lain. Algoritma *skipjack* merupakan salah satu dari algoritma kriptografi yang dapat digunakan dalam mengamankan data rahasia yang dikembangkan pada tahun 1987. *Skipjack* merupakan representasi dari *family of encryption algorithms* sebagai dari algoritma tipe 1 yang dikembangkan Badan Keamanan Nasional Amerika Serikat. Berdasarkan penelitian terlebih dahulu yang dilakukan oleh suprianto mengatakan spesifikasi dari sebuah algoritma yang baik dan tahan terhadap setiap jenis serangan adalah mempunyai struktur yang sederhana serta tidak rumit dan algoritma *skipjack* termasuk dalam jenis ini.

Berdasarkan permasalahan tersebut, maka diperlukan suatu pengamatan informasi dalam bentuk rekaman audio suara format MP3 dengan menggunakan kriptografi. Kriptografi dapat mengubah informasi dengan proses enkripsi dari bentuk semula ke bentuk yang tidak dapat diketahui serta dimengerti oleh semua orang kecuali si pembuat keamanan. Kriptografi membantu dalam peningkatan keamanan informasi dengan mengubah informasi asli (plaintext) menjadi informasi dalam bentuk yang telah diamankan atau tersandi (chipertext) dengan menggunakan kunci yang hanya diketahui oleh phak penerima dan pengirim saja. Kriptografi mampu memberikan pengamanan informasi dalam bentuk apapun dengan menggunakan suatu algoritma untuk menjaga kerahasiaan suatu informasi.

TIN: Terapan Informatika Nusantara
Vol 2, No 1, Juni 2021, Hal 29-34
ISSN 2722-7987 (Media Online)
Website https://ejurnal.seminar-id.com/index.php/tin

Salah satu solusi untuk menyelesaikan masalah diatas adalah melakukan proses penyandian (enkripsi dan dekripsi) terhadap audio yang akan digunakan. Enkripsi dilakukan untuk mengubah data asli menjadi data rahasia, sedangkan dekripsi dilakukan oleh penerimauntuk mengetahui isi data asli dengan cara mengubah data rahasia menjadi data asli. Proses ini disebut dengan teknik kriptografi dimana selama proses pengiriman data, data yang harus bersifat rahasia dan data aslinya hanya diketahui oleh pengirim dan penerima dengan menggunakan kunci rahasia

2. METODOLOGI PENELITIAN

2.1 Kriptografi

Kriptografi adalah ilmuyang mempelajari teknik matematis yang berhubungan dengan aspek keamanan aspek keamanan informasi seperti kenyakinan, integritas data, autentikasi entitas dalam keaslian data[2]. matematis yang berhubungan dengan aspek keamanan informasi seperti tingkat kenyakinan, integritas data, autentikasi entitas dan autentikasi keaslian data. Seni didefenisikan dengan akta sejarah bahwa setiap orang mempunyai cara masing-masing untuk mengamankan data, sehingga pesan memiliki nilai estetika tersendiri yang berhubungan dengan seni dan kebudayaan, jika diperhatikan secara mendalam grafi di kriptografi memiliki makna sebuah seni. Keamanan pada data, kehandalan keamanan tergantung dan cara masing-masing dalam memahami penting dari data tersebut, dalam menjaga kerahasiaan data, kriptografi mentransformasikan data jelas (plaintext) kedalam bentuk data sandi (chipertext) yang tidak dapat dikenali proses pengambilan sebuah chipertext ke plaintext diebut deskripsi

2.2 Algoritma Skipjack

Algoritma skipjack merupakan salah satu dari algoritma kriptografi yang dapat digunakan dalam mengamankan data rahasia yang dikembangkpada tahun 1987. Skipjack merupakan representasi dari *family of encryption algoritms* sebagai bagian dari algoritma tipe yang dikembangkan Badan Keamanan Nasional AmerikaSerikat. Berdasarkan penelitian terdahulu yang dilakukan oleh Suprianto mengatakan spesifikasi dari sebuah algoritma yang baik dan tahan terhadap setiap jenis serangan adalah mempunyai struktur yang sederhana serta tidak rumit dan algoritma skipjack termasuk dalam jenis ini [4]

Terdapat dua tipe putaran dalam skipjack cipher yang disebut dengan stepping rule[4]. Kedua tipe tersebut adalah :

Tipe A :

1. Upablok W1 dienkripsi dengan fungsi G adalah empat putaran Fiestel cipher biasa.
2. Hasil enkripsinya dan nomor putaran yang bertambah dari satu sampai dengan 32, di XOR dengan upablok W4.
3. Setiap upablok dirotasi W1 ke W2, W2 ke W3, W3 ke W4, dan W4 ke W1.

Tipe B :

1. Upablok W2 di-xor dengan W1 dan nomor putaran.
2. W1 dienkripsi dengan fungsi permutasi G.
3. Setiap upablok dirotasi W1 ke W2, W2 ke W3, W3 ke W4, dan W4 ke W1.

Putaran ke-32 *fiestel*tak seimbang pada algoritma *skipjack* terdiri dari delapan putaran tipe A dan delapan putaran tipe B. ubah- kunci pada masing-masing putaran menggunakan fungsi *fiestel*pada fungsi permutasi G. permutasi *fiestel* pada permutasi G melakukan penerimaan input 8 bit dan kemudian di XOR dengan upa kunci. Hasil tersebut disubsitusi berdasarkan table *lookup* atau yang disebut table F [2]

Tabel 1. *fiestel table* (*F-table*) *skipjack*

	x0	x1	x2	x3	x4	x5	x6	x7	x8	x9	xA	xB	xC	xD	xE	xF
0x	a3	d7	09	83	f8	48	f6	f4	b3	21	15	78	99	b1	af	f9
1x	e7	2d	4d	8a	ce	4c	ca	2e	52	95	d9	1e	4e	38	44	28
2x	0a	df	02	a0	17	f1	60	68	12	b7	7a	c3	e9	fa	3d	53
3x	96	84	6b	ba	f2	63	9a	19	7c	ae	e5	f5	f7	16	6a	a2
4x	39	b6	7b	0f	c1	93	81	1b	ee	b4	1a	ea	d0	91	2f	b8
5x	55	b9	da	85	3f	41	bf	e0	5a	58	80	5f	66	0b	d8	90
6x	35	d5	c0	a7	33	06	65	69	45	00	94	56	6d	98	9b	76
7x	97	fc	b2	c2	b0	fe	db	20	e1	eb	d6	e4	dd	47	4a	1d
8x	42	ed	9e	6e	49	3c	cd	43	27	d2	07	d4	de	c7	67	18
9x	89	cb	30	1f	8d	c6	8f	aa	c8	74	dc	c9	5d	5c	31	a4
Ax	70	88	61	2c	9f	0d	2b	87	50	82	54	64	26	7d	03	40
Bx	34	4b	1c	73	d1	c4	fd	3b	cc	fb	7f	ab	e6	3e	5b	a5
Cx	ad	04	23	9c	14	51	22	f0	29	79	71	7e	ff	8c	0e	e2
Dx	0c	ef	bc	72	75	6f	37	a1	ec	d3	8e	62	8b	86	10	e8
Ex	08	77	11	be	92	4f	24	c5	32	36	9d	cf	f3	a6	bb	ac
Fx	5e	6c	a9	13	57	25	b5	e3	bd	a8	3a	01	05	59	2a	46

Kunci pada algoritma skipjack memiliki ukuran panjang 80 bit, kemudian dikelola dengan sederhana yaitu mengelompokkan biner kunci menjadi 10 kelompok atau subkunci (CV0, CV1, CV2,……, CV9) yang masing-masing terdiri dari 8 bit. Kelompok-kelompok bit kunci ini adalah yang digunakan dalam prosesenkripsi maupun dekripsi.

TIN: Terapan Informatika Nusantara
Vol 2, No 1, Juni 2021, Hal 29-34
ISSN 2722-7987 (Media Online)
Website https://ejurnal.seminar-id.com/index.php/tin

2.3 Permutasi G

Permutasi G yang merupakan 4 round dari struktur *feistel* adalah fungsi permutasi pada algoritma skipjack. Table subtitusi byte yang fixed merupakan fungsi round, yang dinamakan *f- Table*. Masing-masing rond dari permutasi G juga memasukkan sebuah *cryptonavariable* (CV). Permutasi G dilakukan pada dekripsi di awal setiap rule yakni A dan rule B. proses permutasi G yang disebut dengan permutasi G-1 yang dilakukan diawal setiap rule A-1 dan rule B-2 sebagai masukan (*input*) untuk melakukan proses permutasi adalah seperempat bagian dari blok plaintext atau pun blok ciphertext dalam bentuk heksadesimal yang berukuran 16 bit. Berikut ini adalah langkah-langkah dari permutasi G dan permutasi G-1:

1. Permutasi G, G (Word =||g1 || g2) =g5 || g6 dimana g1 adalah adalah *byte* pertama dari Word (*high byte*) dan g2 byte kedua dari Word (*low byte*) dan sebagai hasilnya (*output*) adalah gabungan antara g5 dengan g6. Untuk g3, g4, g5, dan g6, rumus yang berlaku adalah formula gi = F(gi-1⊕CV 4k+i-3) ⊕gi-2. Dimana 3⊕ I ⊕ 6 (i awal =3), k pada proses enkrpsi putaran pertama adalah 0,F merupakan table subtitusi atau F-table, dan cv 4k+i-3 adalah *cryptovariable* dengan indeks (4k+i-3) dalam *cryptovariable schedule*. Sesuai dengan rumus
   gi = F(gi-1⊕cv4k+i-3) ⊕gi-2 maka :
   g3= F(g2⊕cv4k)⊕g1
   g4 =F(g3⊕cv4k+1)⊕g2
   g5 = F(g4⊕cv4k+2)⊕g3
   g6 = F(g4⊕cv4k+3)⊕g4
2. Permutasi G-1, G-1 (word = g5 || g6) =g1 || g2 dimana g5 adalah byte kedua dari word (*low byte*) dan sebagai hasilnya (*output*) adalah gabungan antara g1 dengan g2. Untuk g4, g3, g2, g1, rumus yang berlaku adalah sebagai berikut:
   Gi-2 = F(gi-1⊕cv4 (k-1) + i -3) ⊕gi
   Dimana 3⊕ i ⊕ 6, (i awal = 6), k pada proses dekripsi putaran pertama adalah 32, F merupakan table substitusi atau *F- table*, dan cv4(k-1)+i-3 adalah *cryptovariable* dengan indeks (4 (k-1)+i-3) dalam *cryptovariable schedule*. Sesuai dengan rumus gi-2 = F(gi-1⊕cv4(k -1) + I – 3) ⊕ gi, maka:
   g4 = F (g5 ⊕ cv4 (k – 1) + 3) ⊕ g6
   g3 = F (g4 ⊕ cv4 (k – 1) + 2) ⊕ g5
   g2 = F (g3 ⊕ cv4 (k – 1) + 1) ⊕ g4
   g1 = F (g2 ⊕ cv4 (k – 1) + 1) ⊕g3

2.4 Audio

Audio adalah suara/bunyi yang dihasilkan oleh getaran suatu benda. Agar dapat tertangkap telinga manusia, getaran tersebut harus cukup kuat yaitu minimal 20 kali perdetik. Jika kurang dari jumlah itu, teliga manusia tidak akan mendengarnya sebgai suatu bunyi

3. HASIL DAN PEMBAHASAN

Berikut ini akan diimplementasikan pengamanan audio berdasarkan prosedur algoritma skipjack.

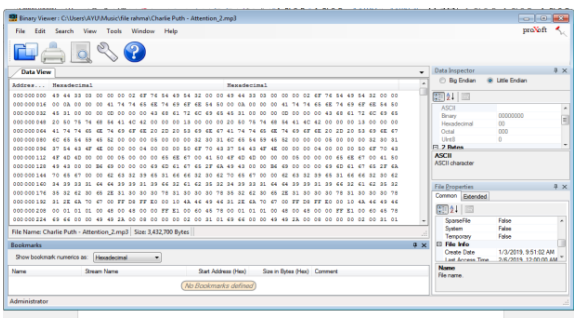
a. Proses pengolahan kunci
   Kunci = RAHMADANIH
   Bentuk heksadesimal = 52 41 48 4D 41 44 41 4E 49 48

Masing-masig kunci akan dibagi menjadi 8 bit dan dikelompokkan menjadi 10 sub kunci sebagai berikut.

Cv[0] = 52 cv[1] = 41 cv[2] = 48 cv[3] = 4D cv[4] = 41
Cv[5] = 44 cv[6] = 41 cv[7] = 4E cv[8] =49 cv[9] = 48

3.1 Proses Enkripsi Algoritma *Skipjack*

Berikut ini merupakan audio suara MP3 yang telah dikonversialkan terlebih dahulu kedalam bilangan decimal dengan menggunakan aplikasi



Gambar 2. Nilai Hasil heksadesimal dari audio

TIN: Terapan Informatika Nusantara
Vol 2, No 1, Juni 2021, Hal 29-34
ISSN 2722-7987 (Media Online)
Website https://ejurnal.seminar-id.com/index.php/tin

Maka dilakukan proses pembagian atau dibagi terlebih dahulu sebelum dienkripsikan.
Planinteks 1 = 42 44 33 03 00 0A 00 00
Kunci = RAHMADANIH
Cv[0] = 52 cv[1] = 41 cv[2] = 48 cv[3] = 4D cv[4] = 41
Cv[5] = 44 cv[6] = 41 cv[7] = 4E cv[8] = 49 cv[9] = 48
Ubah plainteks menjadi 4 bagian (W1, W2, W3, W4)
W1 (0) = 4244 W2 (0) = 3303
W3 (0) = 000A W4 (0) = 0000

Putaran ke-1 (Rule A, K = 0; (counter = 1)
g1 = Mid (W1 (0) , 1,2) = 42
g2 = Mid (W1 (0) , 3,2) = 44
g3 = F (g2 ⊕ cv [(4 * k) mod 10]) ⊕ g1
= F (g2 ⊕ cv [(4 * 0) mod 10]) ⊕ g1
= F (g2 ⊕ cv [(0 *) mod 10]) ⊕ g1
= F (g2 ⊕ cv [0] mod 10]) ⊕ g1
= F (44 ⊕ 52)⊕ 42
g2 = 44 = 01000100
cv[0]= 52 = 01010010 ⊕
00010110
00010110 = F (16) ⊕ 42
F (16) = CA⊕ 42
CA = 11001010
42 = 01000010⊕
g3 = 10001000 (88)
g4 = F (g3 ⊕ cv [(4 * k) + 1 mod 10]) ⊕ g2
= F (g3 ⊕ cv [(4 * 0) + 1 mod 10]) ⊕ g2
= F (g3 ⊕ cv [(0 + 1) mod 10]) ⊕ g2
= F (g3 ⊕ cv [1] ⊕ g2
= F (88 ⊕ 41) ⊕ g2
g3 = 88 = 10001000
cv[1] = 41 = 01000001
11001001
11001001= F(C9) = 79
F(C9) = 79
79 = 01111001
44 = 01000100 ⊕
g4= 00111101
g5 = F (g4 ⊕ cv [(4 * k) + 2 mod 10]) ⊕ g3
= F (3D ⊕ cv [(4 * 0) + 2 mod 10]) ⊕ 88
= F (3D ⊕ 48) ⊕ 88
3D = 00111101
48 = 01001000 ⊕
01110101
F (75) ⊕ 88
F E ⊕ 88
FE = 11111110
88 = 10001000 ⊕
01111010
g5 = 76
g6 =C8
g (W1(0) = g5 + g6 =76C8
W1(1) = G (W1(0)) ⊕ W4 (0) ⊕ counter 1
G(W1(0)) = 76C8 = 0111011011001000
W4(0) = 0000 = 0000000000000000⊕
0011010000110011
Counter = 1 = 0000000000000001⊕
0111011011001001 (76C9)
W2(1)= G(W1(0)) = 76C8
W3(1) = W2(0) = 3303
W4(1) = W3(0) = 000A

TIN: Terapan Informatika Nusantara
Vol 2, No 1, Juni 2021, Hal 29-34
ISSN 2722-7987 (Media Online)
Website https://ejurnal.seminar-id.com/index.php/tin

K = 1 ; counter = 2
Ciphertext = W1(2) + W2(2) + W3(2) + W4(2) = 76C9 76C8 3303 000A

3.2 Proses deskripsi Algoritma *Skipjack*

Untuk mengembalikan cipherteks kebentuk plainteks (karakter awal maka dilakukan permutasi G-1 terlebih dahulu. Permutasi G-1 merupakan kebailikan dari permutasi G. permutasi G-1 diperlukan dalam proses dekripsi.
Cipherteks 1 : DIC6 E45 E92 8783
Kunci : RAHMADANIH
Cv[0] = 52 cv[1] = 41 cv[2] = 48 cv[3] = 4D cv[4] = 41
Cv[5] = 44 cv[6] = 41 cv[7] = 4E cv[8] =49 cv[9] = 48
Ubah Plainteks menjadi 4 bagian (W1, W2, W3, W4)
W1(0) = DIC6 W2 (0) = E45
W3(0) = E92 W4 (0) = 8783

Putaran ke-1 (Rule B-1, k = 32, counter = 32)
G-1 (32)) = G-1 (E45)
g5 = E
g6 = 45
g4 = F(g5 ⊕ cv[((4*(k - 1) + 3) mod 10) ⊕ g6
cv [((4*(32-1) + 3) mod 10] = cv[7] = 4E
5g = E = 00001110
Cv[7] = 4E = 01001110 ⊕
~~01000000~~
F(01000000) = F (40) = 39
F(40) = 39 =00111001
g6 = 45=01000101⊕
~~g4= 01111100 (7C)~~
g3 = F(g5 ⊕ cv[((4*k-1) + 2) mod 10) ⊕ g5
cv [((4*32-1) + 2) mod 10] = cv [6] = 41
g4 = 7C = 01111100
cv[6] = 41= 01000001⊕
~~00111100 (3C)~~
F(00111100) = F (3C)= F7
F(3C) = F7 =11110111
g5=E= 00001110⊕
~~g3 = 11111001(F9)~~
g2 = F(g3⊕ cv[((4*k-1) + 1) mod 10) ⊕ g4
cv [((4*32-1) + 1) mod 10] = cv [5] = 44
g3 = F9 = 11111001
cv[5] = 44= 01000100⊕
~~10111101 (BD)~~
F(10111101) = F (BD) = 3E
F(BD) = 3E = 00111110
g4=7C = 01111100 ⊕
~~g2 = 01000010 (42)~~
W3(29)= W4 (30) = EA42
W4(29) = W1 (30)= F18D
K =29; counter = 29
Ciphertext = W1(29) + W2(29) + W3(29)+ W4(29) = B8FE 3488 EA42 F18D
Untuk mendapatkan nilai plainteks maka dilakukan perputaran sebanyak 32 kali sehingga mengasilkan nilai 42 44 33 03 00 0A 00 00

4. KESIMPULAN

Berdasarkan pembahasan di atas, dapat disimpulkan proses enkripsi dan deskripsi algoritma skipjack sebanyak 32 putaran artinya algoritma pertama diputar dan diulang sebanyak 32kali untuk mendapatkan hasil pengamanan dengan mengubah audio MP3 ke dalam bentuk heksadesimal terlebih dahulu, lalu menyelesaikan dengan rule A dan rule B. bilangan heksadesimal audio dan kunci diperoleh, diubah kebilangan biner terlebih dahulu lalu melakukan proses XOR. Algoritma skipjack mmberikan pengamanan yang kuat sehingga audiotersebut tidak akan tersebar kepada orang yang tidak memiliki hak.

REFERENCES

[1] D. lamhot sitorus M.kom, *algoritma dan pemograman*. 2015.
[2] Harun Mukhtar, *kriptografi untuk keamanan data*. DEEPUBLISH, 2018.
[3] universitas amikom Dony Ariyus, *pengantar ilmu kriptografi: teori Analisis dan implementasi*. C.V ANDI OFFSET, 2008.
[4] B. G. Nurainun sinaga, Syarifah Aini, "penerapan algoritma skipjack untuk menyandikan short message service," 2018.
[5] B. Soeherman and M. Pinontoan, "Designing Information System," 2008.
[6] H. M. Jogianto, *Analisis dan Desain Sistem Informasi*. 2007.
[7] A. Ramadhan, *visual basic 6*. PT Eles media Komputiando, 2004.