Seminar Nasional Teknologi Komputer & Sains (SAINTEKS)
SAINTEKS 2019
ISBN: 978-602-52720-1-1
Januari 2019
Hal: 910 - 915

Pengamanan Audio Menggunakan Algoritma RC4+

Zakiyah Khoiriah Siregar, Aprillya Ulva, Zubaidah

Prodi Teknik Informatika STMIK Budi Darma, Medan, Indonesia
Jalan Sisingamangaraja No. 338, Medan, Indonesia

Abstrak

Pengamanan file berupa audio, video maupun data teks pada perkembangan teknologi saat ini sangat penting dilakukan. Salah satu media yang sering digunakan dalam berkomunikasi adalah audio. Media komunikasi saati ini telah banyak yang memfasilitasi penggunaan audio untuk menyampikan informasi baik yang bersifat penting atau rahasia. Namun, aspek pengamanan terhadap audio tersebut haruslah diutamakan agar tidak dapat disalahgunakan oleh orang lain untuk kepentingan tertentu. Salah satu teknik yang dapat digunakan untuk meminimalisir tindak-tindakan penyalahgunaan tersebut adalah mengimplementasikan teknik kriptografi. Teknik kriprografi bekerja berdasarkan algoritma yang adalah, salah satunya adalah algoritma RC4+ yang merupakan pengembangan dari algoritma RC4. Penelitian ini, menguraikan bagaimana pemanfaatan algoritma RC4+ untuk mengamankan audio berformat WAV dengan tujuan dapat meminimalisir tindakan-tindakan pihak lain terhadap audio yang didistribusikan.

Kata Kunci: Kriptografi, Algoritma RC4+, Audio, WAV

1. PENDAHULUAN

Permasalahan keamanan data penting atau rahasia merupakan salah satu masalah yang sering terjadi di era digitalisasi yang berkembang pesat saat ini. Pemanfaatan audio sebagai salah satu media dalam dalam berkomunikasi menjadi salah satu sasaran dari permasalahan tersebut. Saat ini pemanfaatan audio dalam menyampaikan informasi berupa pesan baik rahasia atau tidak sangatlah pesat. Saat ini banyak aplikasi komunikasi yang telah menyediakan fitur komunikasi menggunakan media audio, sehingga sangat memudahkan proses komunikasi. Sejalan dengan perkembangan fitur komunikasi tersebut, maka permasalahan penyadapan, pencurian dan penyalahgunaan terhadap audio yang didistribusikan juga sering terjadi hingga saat ini sehingga sehingga sering merugikan pemilik informasi dalam bentuk audio.

Teknik kriptografi dapat dimanfaatkan sebagai salah satu solusi untuk mengatasi permasalahan keamanan pada audio, sehingga dapat meminimalisir tindakan-tindakan penyalahgunaan yang dapat dilakukan oleh pihak tertentu. Penerapan salah satu algoritma dari teknik kriptografi untuk mengamankan data yang ditransmisikan melalui media komunikasi sangat cukup baik untuk dilakukan saat ini untuk mengatasi hal-hal yang tidak diinginkan, sehingga informasi penting atau rahasia dapat terjaga dengan baik[1]. Algoritma RC4+ adalah salah satu algoritma kriptografi yang bekerja dengan *stream cipher*. Algoritma ini merupakan pengembangan dari algoritma RC4 yang memiliki kelebihan dalam pengacakan kunci yang digunakan baik pada proses enkripsi maupun dekripsi[2][3].

Audio yang berformat WAV merupakan salah satu format audio yang baik digunakan dalam berkomunikasi. Pengamanan audio berformat WAV berdasarkan algoritma RC4+ menjadi salah satu upaya untuk meminimalisir tindakan penyalahgunaan yang dilakukan oleh pihak lain yang tidak diberi hak akses. Audio asli akan disandikan terlebih dahulu berdasarkan algoritma RC4+ sehingga dihasilkan *cipher* audio. *Cipher* audio yang dihasilkan inilah yang akan didistribusikan kepada penerima.

Tabel 1. Penelitian Terkait

No	Penulis	Judul	Kesimpulan
1	Kristoforus Jawa Bendi dan Titus Andika Rizki	Sistem Kriptografi DES pada Media Audio [4]	Berdasarkan penelitian terdahulu dapat disimpulkan bahwa teknik kriptografi dapat mengamankan komunikasi dalam bentuk audio, sehingga informasi yang ada di dalam audio dapat terjaga dengan baik
2	Fengky Fernando, Siswanto, dan Eko Suryana	Aplikasi Kriptografi untuk Mengamankan File Audio Video Menggunakan Visual Basic .NET [5]	Berdasarkan penelitian terdahulu dapat disimpulkan bahwa penerapan teknik kriptografi dapat mengoptimalkan keamanan file audio dan audio dengan baik.
3	Muhammad Reza Vahlevi	Implementasi Algoritma RC4+ dan Rabin-Williams dalam Skema Hybrid Cryptosystem dalam Pengamanan File Gambar pada Aplikasi Instant Messaging Berbasis Android [6]	Berdasarkan penelitian terdahulu dapat disimpulkan bahwa algoritma RC4+ mampu meningkatkan ketahanan gambar karena kunci yang dihasilkan cukup acak dan sulit dipecahkan

2. METODOLOGI PENELITIAN

2.1 Kriptografi

Kriptografi merupakan suatu ilmu yang mempelajari bagaimana cara menjaga keamanan sebuah file ataupun data agar pesan tetap aman saat dikirimkan tanpa mengalami gangguan dari pihak ketiga. Kriptografi juga bisa disebut sebagai alat pengaman data dengan menyandikan data yang akan diamankan[7]. Kriptografi terdiri dari dua proses yakni enkripsi dan

ISBN: 978-602-52720-1-1
Januari 2019
Hal: 910 - 915

deskripsi. Proses enkripsi merupakan proses yang mengubah *plain* menjadi *chiper* dengan menggunakan kunci tertentu, sehingga informasi sulit diketahui, sedangkan proses deskripsi merupakan proses mengubah *chiper* menjadi *plain*. Penerapan teknik kriptografi harus mewujudkan prinsip pembingungan (konfusi) dan difusi (peleburan) sehingga informasi asli yang terkandung dalamdata asli dapat terjaga dengan baik[8].

2.2 Algoritma RC4+

Algoritma RC4+ merupakan salah satu algoritma kunci simetris dalam bentuk *stream cipher*. Saat ini model untuk desain *stream cipher* sangat diperlukan dalam berbagai aplikasi pengamanan[2]. Sandi atau kunci pada algoritma RC4+ dapat lebih kuat dengan menambahkan beberapa operasi yang dikembangkan dari struktur seperti RC4. Fitur tambahan yang menjadi keunggulan algoritma ini adalah proses pergeseran bit data pada proses pembangkitan kunci, sedangkan proses *Key Scheduling Algorithm* (KSA) dan *Pseudo Random Generation Algorithm* (PRGA) pada algoritma ini hampir sama dengan RC4[3],[6].

Pseudocode untuk *proses Key Schedulling Algorithm* (KSA) :

```
F or i = 0 to 255
      S[i] := i
endfor

j := 0
for i from 0 to 255
      j := (j + S[i] + key[i mod keylength]) mod 256
      swap values of S[i] and S[j]
      j :=j
endfor
```

Pseudocode untuk proses *Pseudo Random Generation Algorithm* (PRGA) :

```
i=0; j=0
For i = 0 to LengthOfPlain-1
      i := i + 1
      a := S[i]
      j := (j + a) mod 256
      Swap S[i] and S[j]
      b := S[j]; S[i] := b; S[j] := a
      c := S[i<<5 ⊕ j>>3] + S[j<<5 ⊕ i>>3]
      z :=(S[a+b] + S[c⊕0xAA]) ⊕ S[j+b]
endFor
```

i dan j adalah indeks array 8-bit, << pergeseran ke kiri dan >> pergeseran ke kanan, ⊕ adalah eksklusif OR. Formulasi proses enkripsi dan dekripsi pada algoritma RC4+ ini [2],[3],[6], adalah sebagai berikut:

Proses Enkripsi :

$$Ci = Pi \oplus Ki \quad (1)$$

Proses Dekripsi :

$$Pi = Ci \oplus Ki \quad (2)$$

2.3 Audio

Audio adalah sebuah fisik yang dihasilkan oleh getaran suatu benda yang berupa sinyal analog dengan amplitude yang perubahannya secara kontiniu terhadap satuan waktu yang disebut dengan frekuensi. Audio berformat WAV merupakan format audio yang menjadi standar microsoft dan IBM untuk personal computer (PC), biasanya menggunakan coding PCM (*Pulse Code Modulation*). Format audio WAV dapat tersimpan seluruhnya ke dalam media penyimpanan karena tidak mengalami proses kompresi pada saat tersimpan. Umumnya file audio berformat WAV ini jarang sekali digunakan di internet karena ukurannya yang relatif besar namun memiliki konstruksi dan hasil yang lebih baik[9]. Sama hal dengan dokumen yang berupa gambar dan teks, file suara juga dapat dimodifikasikan sehingga mengandung informasi yang dapat tersembunyi.

3. ANALISA DAN PEMBAHASAN

3.1 Analisa

Permasalahan penyadapan yang sering terjadi pada jalur distribusi pesan saat ini sangat sering terjadi, terutama informas-informasi yang sifatnya rahasia. Masalah tersebut terjadi karena minimnya tindakan pengamanan terhadap data yang didistribusikan. Prosedur penerapan teknik kriptografi untuk mengamankan file audio hampir sama dengan prosedur penerpannya pada jenis data lain seperti teks dan gambar. Sebelum audio dienkripsi atau didekripsi, maka terlebih dahulu data dari audio harus dirubah menjadi nilai, umumnya berupa nilai hexa desimal. Perlu diperhatikan bahwa tidak semua data yang dimiliki oleh sebuah file audio harus disandikan.

Ada beberapa bagian data yang tidak boleh disandikan untuk menjaga tetap terpeliharanya informasi yang ada di dalam sebuah audio. Bagian tersebut meliputi bagian *chunk* dan *sub chunk (ID dan Size), audio format, num channel, sample*

ISBN: 978-602-52720-1-1
Januari 2019
Hal: 910 - 915

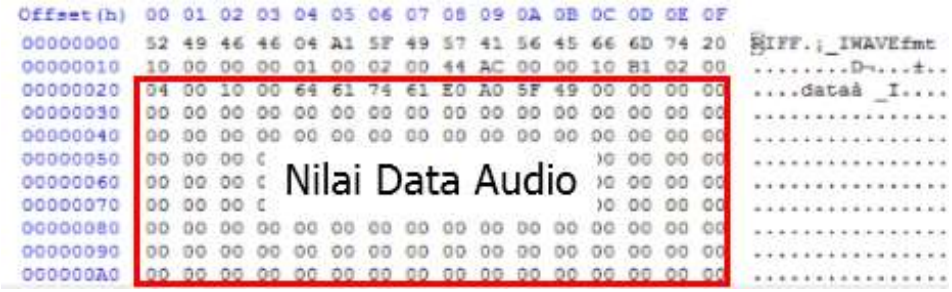
rate, byte rate, block align, bit per sample. Bagian data pada audio merupakan bagian yang dapat dimanipulasi atau dienkripsi dan didekripsi berdasarkan algoritma teknik kriptografi.

Algoritma RC4+ melakukan proses pembangkitan kunci dengan mengacak nilai-nilai data dari sebuah audio, kemudian melakukan proses pergeseran bit. Kunci yang dibangkitkan berjumlah sama seperti jumlah data dari sebuah file audio. Skema pengamanan audio berdasarkan algoritmaRC4+ disajikan pada gambar berikut.

Gambar 1. Skema Pengamanan Audio Berdasarkan Algoritma RC4+

3.2 Pembahasan

Sebelum proses enkripsi maupun dekripsi nilai-nilai data audio dilakukan, audio yang akan diamankan ditransofrmasikan dalam bentuk nilai hexa desimal, sehingga dapat dipisahkan informasi dan data dari audio, kemudian algoritma RC4+ akan melakukan proses pembangkitan nilai-nilai kunci berdasarkan nilai kunci awal yang diinput oleh pengguna. Proses pembentukan kunci meliputi proses KSA dan PRGA, sehingga dihasilkan nilai-nilai kunci yang baru dan sangat acak.



Gambar 2. Nilai-nilai Informasi dan Data Audio

Nilai yang berada dalam kotak merah adalah nilai data audio yang dapat dienkripsi atau dekripsi berdasarkan algoritma RC4+, sedangkan nilai-nilai yang berada pada baris pertama dan kedua adalah nilai informasi dari audio.
Bila diasumsikan nilai kunci awal yang digunakan dalam implementasi ini adalah STMIK, maka akan dilakukan proses KSA dan PRGA.
Proses KSA :

Tabel 2. Tabel S-Box

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
:	:	:	:	:	:	:	:	:	:	:	:	:	:	:	:
:	:	:	:	:	:	:	:	:	:	:	:	:	:	:	:
:	:	:	:	:	:	:	:	:	:	:	:	:	:	:	:
240	241	242	243	244	245	246	247	248	249	250	251	252	253	254	255

Tabel 3. Karakter kunci dibuat dalam bentuk array :

Index 0	Index 1	Index 2	Index 3	Index 4
S	T	M	I	K

Kemudian proses swap isi Tabel sesuai dengan *pseudocode*
Nilai mulai dari 0 hingga 255
Pada saat nilai i=0, maka
j= (j + S[i] + Key [i mod keylength]) Mod 256
j=(0+ S [0] + Key [0 mod 5]) mod 256
j=(0+0+Key [0]) Mod 256
j=(0 + 0 + 83) Mod 256
j=83 Mod 256
j=83

ISBN: 978-602-52720-1-1
Januari 2019
Hal: 910 - 915

Nilai S[i] Swap dengan Nilai S[j]
Nilai S [0] ditukar (swap) dengan Nilai S [83]

Maka:
S[0]=83 dan S [83]=0
Lakukan proses swap hingga i = 255

Setelah proses permutasi ini dilakukan hingga nilai i=255, maka dapat menyebabkan nilai array S-Box dapat di tukar secara berulang atau lebih dari satu kali. Hasil proses permutasi Tabel S-Box keseluruhan adalah:

Tabel 4. Hasil Permutasi S-Box

83	21	109	67	223	62	219	233	128	41	123	163	83	2	139	61
137	37	149	86	170	184	146	131	229	64	125	107	232	251	84	120
161	149	242	129	242	96	209	196	199	15	176	121	165	38	161	81
:	:	:	:	:	:	:	:	:	:	:	:	:	:	:	:
:	:	:	:	:	:	:	:	:	:	:	:	:	:	:	:
220	17	18	108	155	211	183	65	114	166	227	34	91	145	202	12
80	142	201	7	78	151	218	26	93	169	247	63	132	204	29	112

Setelah dihasilkan tabel S-BOX yang telah dipermutasikan, maka selanjutnya adalah melakukan proses PRGA berdasarkan pseudocode-nya. Proses PRGA dilakukan sejumlah nilai data audio yang akan dienkripsi. Bila dimisalkan nilai hexa desimal audio yang akan disandikan adalah 04 00 10 00 64 61 74 61 E0, berarti proses PRGA akan dilakukan sebanyak 9 iterasi untuk menghasilkan 9 buah nilai kunci baru.

Tabel 5. Transformasi Nilai Data Audio dari Hexa ke Decimal

Hexa	04	00	10	00	64	61	74	61	E0
Deximal	4	0	16	0	100	97	116	97	224

Mencari nilai i, a dan j :
Nilai i dan j dimulai dari 0
i = (i+j) Mod 256 →(0+1) Mod 256=1
a = S[i] →S [i]=21
j = (j+a) Mod 256 →(0+21) Mod 256=21
j = j → Nilai j selanjutnya adalah nilai j terakhir

Tukarkan nilai i, a dan j
b = S[i] →S [21] =184
S [i] = b →S [1] = 184
S [j] = a →S [21] = 21

Selanjutnya adalah menghitung nilai c dan z, dimana nilai i dan j adalah :
i = 1 dan j = 21
S [i] = b →S [1] = 184
S [j] = a →S [21] = 21

sehingga nilai c dan z adalah :

$$c = (S[((i<<5) \oplus (j>>3)) \bmod 2560 + S[((j<<5) \oplus (i>>3)) \bmod 256]) \bmod 256$$
$$= (S[((1<<5) \oplus (21>>3)) \text{ MOD } 256) + S[((21<<5) \oplus (1>>3)) \bmod 256]) \bmod 256$$
$$= (S[(32 \oplus 2) \bmod 256] + S[(160 \oplus 0) \bmod 256]) \bmod 256$$
$$= (S[34 \bmod 256] + S[160 \bmod 256]) \bmod 256$$
$$= (S[34] + S[160] \bmod 256$$
$$= (242 + 141) \bmod 256$$
$$= 383 \bmod 256$$
$$c = 127$$

Berdasarkan proses sebelumnya telah ditetapkan nilai i dan j adalah :
i = 1 dan j = 21

ISBN: 978-602-52720-1-1
Januari 2019
Hal: 910 - 915

a = S [i] →S [1]=21
j = (j+a) mod 256 →(0+21)mod 256=21
S [i] = b →S [1]=184
S [j] = a →S [21]=21
Nilai c = 127

Selanjutnya mencari nilai z :
c = ((S[a+b] mod 256 + S [((c ⊕ 00AA) mod 2560)] ⊕ S[((j+b) mod 256]) mod 256
= ((S[21+184] mod 256 + S [((127 ⊕ 170) mod 2560)] ⊕ S[((21 + 184) mod 256]) mod 256
= ((S[205 mod 256 + S [((127 ⊕ 170) mod 256)]) ⊕ S[205 mod 256]) mod 256
= ((S[205] + S [((213 mod 256)]) ⊕ S [205 mod256]) mod 256
= ((S[205] + S[213]) ⊕ S [205]) mod 256
= ((8 + 216) ⊕ 8) mod 256
= (224 ⊕ 8) mod 256
= 232 mod 256
z = 232
nilai z merupakan nilai kunci (K) yang digunakan untuk melakukan proses enkripsi atau dekripsi nilai data audio pada index pertama. Proses PRGA ini dilakukan sebanyak nilai data audio asli (sembilan iterasi).

Setelah didapatkan seluruh nilai kunci, maka proses enkripsi dilakukan berdasarkan persamaan 1.
Nilai Audio adalah 04 00 10 00 64 61 74 61 E0
P_{audio} [0] = 4 → 00000100
K [0] = 232 → 11101000 ⊕
C_{audio}[0] = 236 → 11101100 → dalam nilai desimal = EC
Setelah seluruh nilai-nilai data audio dienkripsi, maka diperoleh nilai cipher audio yang kemudian dipetakan menjadi file audio terenkripsi.

Offset (h)	00	01	02	03	04	05	06	07	08
00000000	EC	49	46	46	B4	9A	48	29	57
00000010	10	00	00	00	01	00	02	00	44
00000020	04	00	10	00	64	61	74	61	90
00000030	05	06	51	08	DA	05	CE	07	AE
00000040	49	05	3F	06	11	05	B6	05	D6
00000050	59	04	19	04	18	04	8C	03	D6

Gambar 3. Nilai-nilai Cipher Audio

Proses dekripsi dilakukan dengan cara yang sama seperti proses enkripsi. Penerima audio melakukan proses KSA dan PRGA untuk membangkitkan kunci yang baru berdasarkan kunci awal yang telah disepakati, kemudian melakukan proses XOR antara nilai-nilai data *cipher* audio dengan nilai kunci hasil PRGA. Nilai-nilai tersebut akan petakan menjadi audio baru yang sama seperti *plain* audio.

4. KESIMPULAN

Berdasarkan uraian analisa dan pembahasan dalam penelitian ini, maka disimpulkan bahwa proses pengulangan nilai kunci yang sama dari hasil PRGA algoritma RC4+ sangat jarang terjadi, sehingga kunci baru yang dihasilkan benar-benar acak. Jumlah kunci yang dibangkitkan berbanding lurus dengan jumlah nilai *plain*, sehingga memerlukan waktu lama. *Cipher audio* yang diihasilkan dari implementasi algoritma RC4+ dapat menyembunyikan pola *plain audio*, sehingga dapat meminimalisir tindakan penyalahgunaan audio oleh pihak lain.

REFERENCES

[1] M. Diana and T. Zebua, "Optimalisasi Beaufort Cipher Menggunakan Pembangkit Kunci RC4 Dalam Penyandian SMS," *J. Sains Komput. Inform.*, vol. 2, no. 1, pp. 12–22, 2018.
[2] F. Akbar, H. Mawengkang, and S. Efendi, "Comparative analysis of RC4 + algorithm , RC4 NGG algorithm and RC4 GGHN algorithm on image file security," *2nd Nommensen Int. Conf. Technol. Eng.*, pp. 1–7, 2018.
[3] M. A. Budiman, Amalia, and N. I. Chayanie, "An Implementation of RC4+Algorithm and Zig-zag Algorithm in a Super Encryption Scheme for Text Security," *J. Phys. Conf. Ser.*, vol. 978, no. 1, 2018.
[4] K. Jawa Bendi and T. Andika Rizki, "Sistem Kriptografi DES pada Media Audio," in *Seminar Nasional Teknologi Terapan SV UGM*, 2016, pp. 640–644.
[5] F. Fernando, Siswanto, and E. Suryana, "Aplikasi Kriptografi untuk Mengamankan File Audio Video Menggunakan Visual Basic .NET," *J. Media Infotama*, vol. 10, no. 1, pp. 27–34, 2014.
[6] M. Reza Vahlevi, "Implementasi Algoritma RC4+ dan Rabin-Williams dalam Skema Hybrid Cryptosystem dalam Pengamanan File Gambar pada Aplikasi Instant Messaging Berbasis Android," Universitas Sumatera Utara, 2018.
[7] M. A. Wijaya, W. Kurniawan, and A. Kusyanti, "Perancangan dan Implementasi Algoritma Enkripsi Idea pada Perangkat Kriptografi Berbasis

ISBN: 978-602-52720-1-1
Januari 2019
Hal: 910 - 915

FPGA," vol. 2, no. 12, pp. 6973–6981, 2018.
[8] T. Zebua, "Encoding the Record Database of Computer Based Test Exam Based on Spritz Algorithm," *Lontar Komput. J. Ilm. Teknol. Inf.*, vol. 9, no. 1, p. 52-62, 2018.
[9] R. N. F and N. W. H, "Aplikasi Keamanan File Audio Wav (Waveform) Dengan," *J. Nas. Inform. dan Teknol. Jar.*, vol. 1, no. 2, pp. 113–119, 2017.