Seminar Nasional Teknologi Komputer & Sains (SAINTEKS)
SAINTEKS 2019
ISBN: 978-602-52720-1-1
Januari 2019
Hal: 894 - 897

# Penerapan Metode IDEA Untuk Mengamankan File Audio

**Joslin Nababan, Limcia Hutajulu, Marjadi Hebert Harianja**

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

**Abstrak**

Keamanan data sangat berperan penting dalam proses pendistribusian data terutama data yang bersifat rahasia dan penting. Hal ini dilakukan untuk menjaga kerahasiaan serta keutuhan data yang akan diterima. Salah satu jenis data yang perlu diamankan adalh file audio, karena sama halnya dengan jenis data lainnya audio juga bisa dimodifikasi sehingga dapat mengandung informasi yang tersembunyi. Audio merupakan media digital yang banyak digunakan dalam penyampaian pesan. Dengan bantuan koneksi internet, pertukaran informasi melalui audio semakin cepat. Bila audio yang akan dikirim merupakan informasi yang sangat penting,maka perlu dilakukan teknik pengamanan data. Salah satu metode yang dapat digunakan adalah dengan metode IDEA (*International Data Encryption Algorithm*). Algoritma IDEA merupakan algoritma dalam kriptografi yang memberikan keamanan tinggi, dimana proses penyelesaian dilakukan dengan proses pembentukan kunci, proses enkripsi serta proses dekripsi. Diterapkannya proses pengamanan terhadap data data, maka akan menyulitkan pihak lain yang tidak berkepentingan untuk mengetahui isi data rahasia tersebut.

**Kata Kunci:** Kriptografi, IDEA, Audio, Informasi, Block Cipher

## 1. PENDAHULUAN

Perkembangan teknologi terutama dibidang komunikasi dan informasi,terutama dalam distribusi informasi melalui internet saat ini sangat berkembang sangat pesat. Namun hal tersebut tidak semua memberikan dampak yang positif bagi pengguna. Internet sebagai media yang sering digunakan sebagai pertukaran informasi memiliki jalur yang tidak terlalu aman,dikarenakan hak akses yang mudah dan secara bebas digunakan oleh siapapun,sehingga mempermudah seseorang dalam melakukan penyadapan informasi/pesan,baik itu dalam bentuk pesan teks, gambar maupun audio [1].

Salah satu jenis file yang sering digunakan dalam penyampaian pesan adalah audio. Seperti halnya pada dokumen yang berupa teks maupun gambar, file suara juga dapat dimodifikasi oleh pihak pihak yang tidak bertanggungjawab, sehingga kemungkinan mengandung informasi yang berbeda dengan informasi sebenarnya. Bila audio yang dimodifikasi merupakan pesan penting, tentu akan merugikan pihak tertentu. Dengan demikian audio membutuhkan teknik pengamanan yang baik[2].

Kriptografi merupakan suatu ilmu yang mempelajari bagaimana cara agar menjaga data atau pesan tetap aman saat dikirimkan tanpa mengalami gangguan dari pihak ketiga. Kriptografi memiliki berbagai metode yang dapat digunakan mengamankan data, yang memiliki teknik pengkodean yang rumit sehigga informasi tidak dapat diketahui oleh pihak lain[3]. Salah satu metode yang dianggap sebagai algoritma *block cipher* teraman dalam kriptografi adalah metode IDEA*(International Data Encryption Algorithm*).

Metode IDEA pertama kali diperkenalkan oleh Xuejia Lai dan James Massey pada tahun 1990 dengan nama PES (*Proposed Encryption Standard)*, namun pada tahun 1992, namanya diganti menjadi IDEA yang dirancang untuk menggantikan metode DES (*Data Encryption Standard*). Metode IDEA beroperasi pada block *plaintext* 64-bit dan panjang kuncinya 128 bit, dimana proses penyelesaiannya dilakukan dengan tiga proses,yaitu proses pembangkitan kunci, proses enkripsi dan proses dekripsi[4]. Pemanfaatan algoritma IDEA untuk mengamankan audio diharapkan mampu meningkatkan keamanan dalam pertukaran informasi, sehingga pesan dalam bentuk audio yang didistribusikan terjaga kerahasiaan dan keutuhannya.

**Tabel 1.** Penelitian Terkait

| No | Penulis | Judul | Kesimpulan |
|---|---|---|---|
| 1 | Kristoforus Jawa Bendi dan Titus Andika Rizki | Sistem Kriptografi DES pada Media Audio[5] | Berdasarkan penelitian terdahulu dapat disimpulkan bahwa perlunya penerapan teknik kriptografi untuk mengamankan komunikasi dalam bentuk audio, sehingga informasi yang ada di dalam audio dapat terjaga dengan baik |
| 2 | Muhammad Adi Wijaya,Wijaya Kurniawan dan Ari Kusyanti | Perancangan dan Implementasi Algoritma Enkripsi Idea pada Perangkat Kriptografi Berbasis FPGA[6] | Berdasarkan penelitian terdahulu dapat disimpulkan bahwa keamanan data berdasarkan algoritma IDEA cukup baik serta tidak berpengaruh pada waktu yang dibutuhkan. |
| 3 | Tri Andriyanto dan D.L. Crispina Pardede | Studi dan Perbandingan Algoritma IDEA dan Algoritma Blowfish [7] | Berdasarkan penelitian terdahulu dapat disimpulkan bahwa algorima IDEA dapat digunakan untuk mengamankan jenis audio. |

## 2. METODOLOGI PENELITIAN

### 2.1 Kriptografi

Kriptografi merupakan suatu ilmu yang mempelajari bagaimana cara agar menjaga data atau pesan tetap aman saat dikirimkan tanpa mengalami gangguan dari pihak ketiga. Kriptografi juga dapat diartikan sebagai teknik pengamanan data

ISBN: 978-602-52720-1-1
Januari 2019
Hal: 894 - 897

dengan menyandikan data yang akan diamankan (merubah data menjadi menjadi sandi tertentu[8]. Kriptografi terdiri dari dua proses utama, yakni proses enkripsi dan proses dekripsi. Proses enkripsi merupakan proses mengubah *plaintext* menjadi *ciphertext* dengan menggunakan kunci tertentu,sehingga informasi sulit diketahui, sedangkan proses dekripsi merupakan proses mengubah ciphertext menjadi *plaintext*[9][10].

### 2.2 Metode IDEA

Metode *International Data Encryption Algorithm* (IDEA) pertama kali diperkenalkan oleh Xuejia Lai dan James Massey pada tahun 1990, dengan nama PES (*Proposed Encryption Standard*). Kemudian sang penemu memperkuat algoritma hasil pengubahan dengan nama IPES (*Improved proposed Encryption Algorithm*). Tahun 1992, IPES diubah lagi dengan nama IDEA, yang dirancang sebagai pengganti metode DES (*Data Encryption Standard*)[4], [6], [7].

Kelebihan Metode IDEA

1. Algoritma ini menyediakan keamanan yang cukup tinggi yang tidak didasarkan atas kerahasiaan algoritmanya akan tetapi lebih ditekankan pada keamanan/kerahasiaan kunci yang digunakan.
2. Dapat dengan mudah untuk dipahami secara penuh.
3. Algoritma ini dapat digunakan dan dimengerti oleh semua orang.
4. Algoritma ini sangat layak untuk digunakan sebagai keamanan dalam bidang aplikasi.
5. Dapat diterapkan dalam bentuk komponen elektronik (chip) secara ekonomis atau relatif murah.
6. Dapat digunakan secara efisien.
7. Algoritma ini memungkinkan untuk disebar luaskan ke seluruh dunia.
8. Menyediakan kemanan tingkat tinggi karena algoritma ini tidak berdasarkan penjagaan terhadap kerahasiaan kunci yang dilakukan oleh pemakai.
9. Sudah dilindungi hak paten untuk mencegah pembajakan dan kejahatan.

Kelemahan Metode IDEA

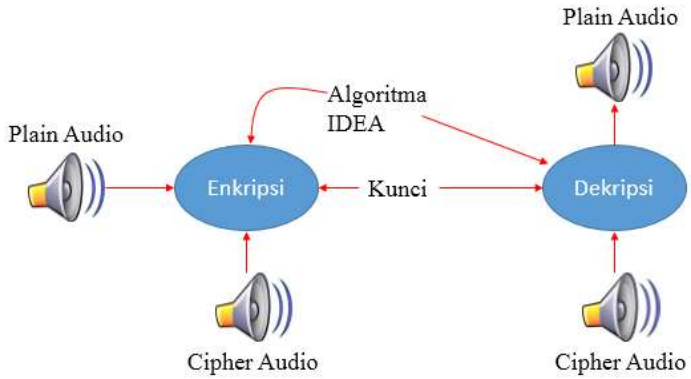
1. Key schedule yang sangat sederhana membuat IDEA memiliki kunci yang lemah.
2. Keamanan IDEA masih memiliki kelemahan karena panjang block yang relative kecil(64 bit).

### 2.3 Audio

Salah satu media digital yang dapat digunakan dalam penyampaian pesan dalam bentuk auditif adalah audio. Audio banyak digunakan dalam pentampaian pesan karena mudah dalam penggunaannya dan pengaksesannya. Berbagai macam file audio,yaitu WAV, WMA, MP3, FLAC, MP4 dan AMR[3]. Sama halnya seperti dokumen yang berupa gambar dan teks, file suara juga dapat dimodifikasi sehingga mengandung informasi yang dapat tersembunyi. Modifikasi dilakukan agar orang yang tidak berkepentingan tidak mudah untuk menghapusnya, sehingga tidak dapat merusak signal asli.

## 3. ANALISA DAN PEMBAHASAN

Permasalahan yang dibahas dalam penelitian ini adalah pengamanan file audio sehingga file audio hanya akan diketahui oleh orang-orang yang berkepentingan. Pada penelitian ini pengamanan file dilakukan menggunakan algoritma IDEA. Adapun teknik penyelesaian dalam metode IDEA adalah dengan melakukan proses pembentukan kunci,proses enkripsi dan proses dekripsi. Implementasi algoritma IDEA untuk mengamankan audio dapat diilustrasikan pada gambar di bawah ini :




**Gambar 1.** Ilustrasi Proses Pengamanan Audio Berdasarkan Metode IDEA

### 3.1 Proses Pembentukan Kunci

Proses pembentukan kunci dimulai dengan membagi 128 bit kunci menjadi 8 buah 16 bit subkunci, subkunci pertama untuk algoritma dengan 6 subkunci pertama untuk putaran pertama, dan dua subkunci terakhir untuk putaran ke dua. Algoritma IDEA menggunakan 52 subkunci dengan 6 buah subkunci untuk 8 putaran dan 4 subkunci lagi untuk tranformasi *output*.

Subkunci yang digunakan untuk proses enkripsi pada algoritma IDEA adalah :

**Tabel 2.** Sub Kunci Proses Enkripsi

| Putaran | Kunci |
|---|---|
| Putaran ke-1 | $K_1$, $K_2$, $K_3$, $K_4$, $K_5$, $K_6$ |

ISBN: 978-602-52720-1-1
Januari 2019
Hal: 894 - 897

| | |
|---|---|
| Putaran ke-2 | $K_7$, $K_8$, $K_9$, $K_{10}$, $K_{11}$, $K_{12}$ |
| Putaran ke-3 | $K_{13}$, $K_{14}$, $K_{15}$, $K_{16}$, $K_{17}$, $K_{18}$ |
| Putaran ke-4 | $K_{19}$, $K_{20}$, $K_{21}$, $K_{22}$, $K_{23}$, $K_{24}$ |
| Putaran ke-5 | $K_{25}$, $K_{26}$, $K_{27}$, $K_{28}$, $K_{29}$, $K_{30}$ |
| Putaran ke-6 | $K_{31}$, $K_{32}$, $K_{33}$, $K_{34}$, $K_{35}$, $K_{36}$ |
| Putaran ke-7 | $K_{37}$, $K_{38}$, $K_{39}$, $K_{40}$, $K_{41}$, $K_{42}$ |
| Putaran ke-8 | $K_{43}$, $K_{44}$, $K_{45}$, $K_{46}$, $K_{47}$, $K_{48}$ |
| Transformasi Output | $K_{49}$, $K_{50}$, $K_{51}$, $K_{52}$ |

Subkunci yang digunakan untuk dekripsi :

**Tabel 3.** Sub K unci Proses Dekripsi

| Putaran | Kunci |
|---|---|
| Putaran ke-1 | $(K_{49})^{-1}$, $-K_{50}$, $-K_{51}$, $(K_{52})^{-1}$, $K_{47}$, $K_{48}$ |
| Putaran ke-2 | $(K_{43})^{-1}$, $-K_{44}$, $-K_{45}$, $(K_{46})^{-1}$, $K_{41}$, $K_{42}$ |
| Putaran ke-3 | $(K_{37})^{-1}$, $-K_{38}$, $-K_{39}$, $(K_{40})^{-1}$, $K_{35}$, $K_{36}$ |
| Putaran ke-4 | $(K_{31})^{-1}$, $-K_{32}$, $-K_{33}$, $(K_{34})^{-1}$, $K_{29}$, $K_{30}$ |
| Putaran ke-5 | $(K_{25})^{-1}$, $-K_{26}$, $-K_{27}$, $(K_{28})^{-1}$, $K_{23}$, $K_{24}$ |
| Putaran ke-6 | $(K_{19})^{-1}$, $-K_{20}$, $-K_{21}$, $(K_{22})^{-1}$, $K_{17}$, $K_{18}$ |
| Putaran ke-7 | $(K_{13})^{-1}$, $-K_{14}$, $-K_{15}$, $(K_{16})^{-1}$, $K_{11}$, $K_{12}$ |
| Putaran ke-8 | $(K_7)^{-1}$, $-K_8$, $-K_9$, $(K_{10})^{-1}$, $K_5$, $K_6$ |
| Transformasi Output | $(K_1)^{-1}$, $-K_2$, $-K_3$, $(K_4)^{-1}$ |

### 3.2 Proses Enkripsi

Pada proses enkripsi,terdapat tiga operasi yang berbeda untuk pasangan sub blok 16 bit yang digunakan

1. XORdua sublok 16 bit perbit
2. Penjumlahan integer modulo ($2^{16}$+1)dua sub blok 16 bit
3. Perkalian modulo ($2^{16}$+1) dua sub blok 16 bit

Blok pesan 64 bit,dibagi menjadi 4 sub blok 16 bit, $Y_1$, $Y_2$, $Y_3$, $Y_4$. Keempat sub blok ditransformasikan menjadi sub blok 16 bit, yaitu blok 16-bit, $Y_1$, $Y_2$, $Y_3$, $Y_4$ sebagai pesan rahasia 64-bit Y = ($Y_1$, $Y_2$, $Y_3$, $Y_4$) yang berada dibawah kendali 52 sub blok kunci 16-bit yang dibentuk dari dari blok kunci 128 bit. Keempat sub-blok 16-bit, $Y_1$, $Y_2$, $Y_3$, $Y_4$, digunakan sebagai masukan untuk putaran pertama dari algoritma IDEA. Dalam setiap putaran dilakukan operasi XOR, penjumlahan, perkalian antara dua sub-blok 16-bit dan diikuti pertukaran antara sub-blok 16-bit putaran kedua dan ketiga. Pada setiap putaran dilakukan operasi-operasi sebagai berikut :

1. Perkalian $X_1$ dengan sub-kunci pertama
2. Penjumlahan $X_2$ dengan sub-kunci kedua
3. Pejumlahan $X_3$ dengan sub kunci ketiga
4. Perkalian $X_4$ dengan sub kunci keempat
5. Operasi XOR hasil langkah 1) dan 3)
6. Operasi XOR hasil angkah 2) dan 4)
7. Perkalian hasil langkah 5) dengan sub-kunci kelima
8. Penjumlahan hasil langkah 6) dengan langkah 7)
9. Perkalian hasil langkah 8) dengan sub-kunci keenam
10. Penjumlahan hasil langah 7) dengan 9)
11. Operasi XOR hasil langkah 1) dan 9)
12. Operasi XOR hasil langkah 3) dan 9)
13. Operasi XOR hasil langkah 2) dan 10)
14. Operasi XOR hasil langkah 4) dan 10)

Setelah putaran kedelapan terdapat transformasi keluaran, yaitu :

1. Perkalian $X_1$ dengan sub-kunci pertama
2. Penjumlahan $X_2$ dengan sub-kuci ketiga
3. Penjumlahan $X_3$ dengan sub-kunci kedua
4. Perkalian $X_4$ dengan sub-kunci keempat

### 3.3 Proses Dekripsi

Proses dekripsi menggunakan algoritma yang sama dengan proses enkripsi. Subkey pada pada proses dekripsi terbalik dengan *subkey* pada proses enkripsi. Selain itu, proses dekripsi memiliki 52 buah subkunci yang digunakan, masing masing merupakan hasil turunan 52 buah subkunci enkripsi.

ISBN: 978-602-52720-1-1
Januari 2019
Hal: 894 - 897

## 4. KESIMPULAN

Berdasarkan analisan dan pembahasan penelitian ini, maka disimpulkan bahwa metode IDEA dapat digunakan untuk meningkarkan keamanan file audio yang memiliki proses utama meliputi proses pembentukan kunci, proses enkripsi dan proses dekripsi. Pengamanan file audio berdasarkan algoritma IDEA menghasilkan sandi-sandi dalam bentuk audio yang mampu menyembunyikan dan merahasiakan audio asli.

## REFERENCES

[1] F. Teknologi and I. Universitas, "PENGEMBANGAN APLIKASI KRIPTOGRAFI FILE DOKUMEN , AUDIO DAN GAMBAR DENGAN ALGORITMA DES," vol. VIII, no. 2, pp. 185–190, 2016.
[2] J. I. Polinema, R. Byte, and P. Encoding, "PENGEMBANGAN SISTEM KEAMANAN INFORMASI MENGGUNAKAN METODE KRIPTOGRAFI 3DES DAN STEGANOGRAFI RANDOM BYTE POSITION ENCODING PADA," pp. 109–116, 2016.
[3] U. S. Utara, U. S. Utara, and U. S. Utara, "Pengamanan File Audio Dengan Menggunakan Algoritma Rivest Shamir Adleman dan Metode Modified Least Significant Bit Red Channel," 2018.
[4] P. Informatika, B. Darma, and L. B. Masalah, "PENERAPAN METODE IDEA PADA PERANCANGAN APLIKASI," no. November, pp. 152–156, 2013.
[5] K. Jawa Bendi and T. Andika Rizki, "Sistem Kriptografi DES pada Media Audio," in *Seminar Nasional Teknologi Terapan SV UGM*, 2016, pp. 640–644.
[6] M. Adi Wijaya, W. Kurniawan, and A. Kusyanti, "Perancangan dan Implementasi Algoritma Enkripsi Idea pada Perangkat Kriptografi Berbasis FPGA," *J. Pengemb. Teknol. Inf. dan Ilmu Komput.*, vol. 2, no. 12, pp. 6973–6981, 2018.
[7] T. Andriyanto and D. L. C. Pardede, "STUDI DAN PERBANDINGAN ALGORITMA IDEA DAN ALGORITMA BLOWFISH," in *Seminar Ilmiah Nasional Komputer dan Sistem Intelijen (KOMMIT 2008)*, 2008, pp. 182–189.
[8] M. A. Wijaya, W. Kurniawan, and A. Kusyanti, "Perancangan dan Implementasi Algoritma Enkripsi Idea pada Perangkat Kriptografi Berbasis FPGA," vol. 2, no. 12, pp. 6973–6981, 2018.
[9] L. Penjualan and H. Berbasis, "IMPLEMENTASI METODE KRIPTOGRAFI IDEA pada PRIORITY DEALER untuk LAYANAN PEMESANAN dan LAPORAN PENJUALAN HAMDPHONE BERBASIS WEB," pp. 1–7.
[10] 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.