KLIK (Kajian Ilmiah Informatika & Komputer), Vol. 1 No. 1, Agustus 2020
e-ISSN 2723-3898 (Media Online)
Hal 1-5

Perancangan Aplikasi Keamanan Pesan Audio Dengan Metode CAST-256

Elprida Hutahaean

Teknik Informatika, Universitas Budi Darma, Medan, Indonesia
Email: elfridahutahaean51@gmail.com

Abstrak

Kriptografi adalah ilmu ataupun seni yang mempelajari bagaimana membuat suatu pesan yang dikirim oleh pengirim dapat disampaikan kepada penerima dengan aman. Kriptografi merupakan bagian dari suatu cabang ilmu matematika yang disebut kriptologi (cryptologi). Kriptografi bertujuan menjaga kerahasiaan informasi yang terkandung dalam data sehingga informasi tersebut tidak dapat diketahui oleh pihak yang tidak sah. Perancang algoritma kriptografi disebut kriptografer. Hal tersebut membuat informasi menjadi suatu hal kursial yang harus dijaga kerahasiaan ny.salah satu cara dalam bertukar informasi adalah dengan menggunakan pesan elektronik. Metode Cast merupakan algoritma block chiper yang telah digunakan dalam berbagai produk seperti contoh pgp.Metode Cast sebagai kunci simetri. File audio merupakan suara sampel suara, setiap fraksi n satu detik, sampel suara disimpan sebagai informasi digital dalam dit dan byte.Audio adalah bahan mengandung pesan dalam bentuk auditif(pita suara atau piringan suara), yanga dapat merancang pikiran, perasaan, perhatian, dan kemauan siswa sehingga terjadi proses belajar mengajar.Audio adalah fenomena fisik yang dihasilkan oleh getaran suatu benda yang berupa sinya analog dengan amplitude yang berubah secara continiu terhadap satuan waktu yang disebut frekuensi

Kata Kunci: Kriptografi, Metode cast, File audio.

Abstract

Cryptography is the science or art of learning how to make a message sent by the sender safely delivered to the recipient. Cryptography is part of a branch of mathematics called cryptology (cryptology). Cryptography aims to maintain the confidentiality of information contained in data so that information can not be known by unauthorized parties. The designer of a cryptographic algorithm is called a cryptographer. This makes information a material that must be kept confidential. One way to exchange information is to use electronic messages. The Cast method is a block cipher algorithm that has been used in various products such as the pgp example. The Cast method is the key to symmetry. Audio files are sound samples of sound, every fraction n one second, sound samples are stored as digital information in dit and bytes. Audio is material containing messages in auditive form (vocal cords or voice plates), which can design thoughts, feelings, concerns, and student's will so that the learning process occurs. Audio is a physical phenomenon produced by the vibration of an object in the form of an analog signal with an amplitude that changes continuously with respect to a unit of time called frequency

Keywords: Cryptography, Cast method, Audio file..

1. PENDAHULUAN

Teknologi juga terus menerus berupaya memenuhi kebutuhan masyarakat akan informasi yang dapat diakses dengan mudah dan cepat terutama dalam hal berkomunikasi. Komunikasi dapat mengandung sebuah informasi yang bersifat rahasia maka keamanan informasi menjadi faktor utama yang harus dipenuhi agar terhindar dari pihak-pihak yang tidak bertanggung jawab. Salah satu komunikasi yang bersifat rahasia dapat berupa pesan audio. Penyampaian komunikasi menggunakan pesan audio bersifat rahasia sering dihack oleh pihak yang tidak bertanggung jawab, maka dari itu diperlukan pengembangan sistem berupa aplikasi yang dapat mengamankan pesan audio bersifat rahasia untuk menghindari pihak-pihak yang tidak bertanggung jawab[1]. Kriptografi adalah ilmu yang mempelajari teknik teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasian , integritas data serta orientakasi. Masalah keamanan dan kerahasiaan data merupakan suatu hal yang sangat penting terutama didalam menghadapi persaingan bisnis[2]. Data yang bersifat perlu dibuatkan sistem penyimpanan dan pengirimanannya agar tidak terbaca atau diubah oleh orang orang yang tidak bertangug jawab baik dengan file teks tersebut dikirim melalui media internet. Untuk menyimpan data tersebut agar benar benar ama tentunya dilakukan sistem pengamanan yang baik, yang bebas dari jangkauan orang yang tidak berhak, baik bebas jangkauan secara fisik maupun sistem .Metode *CAST-256* disebut juga dengan *CAST6* dirancang oleh *Carlisle Adams, Howard Heys, Stafford Tavares, dan Michael Wiener*. Arsitektur *CAST-256* dibangun berdasarkan *CAST-128. CAST-256* dengan *CAST-128* antara lain pada fungsi perputaran yang digunakan, *S-Box,* serta tiap putaran menggunakan sepasang subkey yaitu subkey *5-bit Kr* sebagai *rotation key* dan *32-bit Km* sebagai masking *key*[3]. Untuk melakukan pengembangan sistem dalam melakukan pengamanan pesan *audio* pada penelitian ini penulis merancang aplikasi keaman pesan *audio* dengan penerapan metode *CAST-256* menggunakan *software visual basic net 2008*. Hasil dari penelitian ini diharapkan dapat menjadi alternative untuk membantu dalam membuat suatu keamanan pesan *audio* yang bersifat rahasia agar terhindar dari pihak yang tidak bertanggungjawab.

2. METODE PENELITIAN

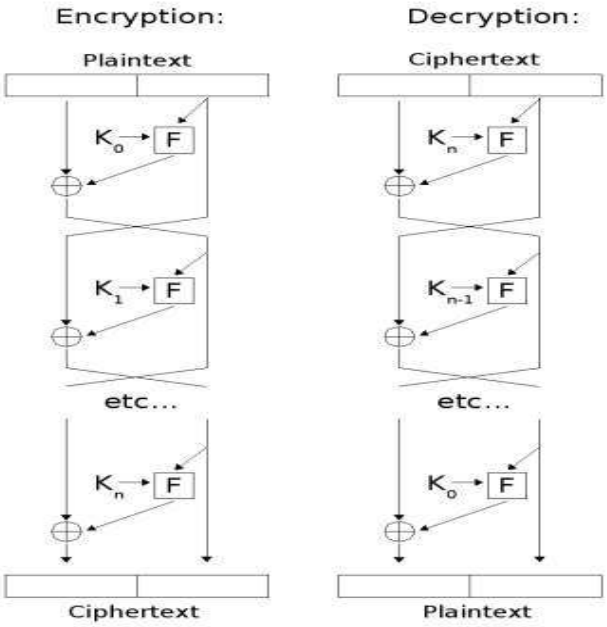
2.1 Kriptografi

Kriptografi (cryptography) berasal dari Bahasa Yunani, yaitu cryptos 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 merupakan bagian dari suatu cabang ilmu matematika yang disebut kriptologi (cryptology). Kriptografi bertujuan menjaga kerahasian informasi yang terkandung dalam data sehingga informasi tersebut tidak dapat diketahui oleh pihak yang tidak sah. Perancang algoritma kriptografi disebut kriptografer. Kriptanalisis (cryptanalysis) adalah suatu ilmu dan seni membuka (breaking) ciphertext menjadi plaintext tanpa mengetahui kunci yang

digunakan. Pelaku kriptanalisis disebut kriptanalis (cryptanalyst). Kriptanalis merupakan lawan kriptografer. Persamaan kriptanalis dan kriptografer adalah bahwa kedua sama-sama menerjemhkan ciphertext menjadi plaintext [4].

2.2 Metode *CAST-256*

Metode *CAST-256* dirancang oleh *Carlisle Adams, Howard Heys, Stafford Tavares,* dan *Michael Wiener*. Arsitektur metode *CAST-256* dibangun berdasarkan *CAST-128*[5]. Metode*CAST-256* adalah sebuah cipher simetri yang didesain berdasarkan prosedur mendesain *CAST*. Algoritma ini merupakan ektensi dari *CAST-128* dan telah didaftarkan sebagai salah satu kandidat untuk *NIST Advanced Encryption Standard (AES)*. Dalam mendesain algoritma *CAST-256* ini, *Howard Heys* dan *Michael Wiener* juga turut berkontribusi. *CAST-256* menggunakan komponen-komponen yangs ama dengan *CAST-128*, termasuk *S-boxes* (yang diadaptasi dari *block* berukuran 128 *bit*). Panjang kunci yang dapat diterima adalah 128, 160, 224, atau 256 *bit*. *CAST-256* menggunakan 48 putaran (*round*) yang sering disebut sebagai 12 "*quad-rounds*"[6].
Keamanan kerahasiaan suatu pesan tergantung pada keamanan kerahasiaan dari kunci itu sendiri.



Gambar 1. Feistel Cipher

Selanjutnya dilakukan proses enkripsi sebanyak 16putaran dan perhitungan untuk blok kanan dan kiri padaputaran ke I adalah sebagai berikut.

$$L_i = R_i - 1 \quad (1)$$

$$R_i = L_i - 1\ ^{f(R_{i-1}, K_{Li}, Kri)} \quad (2)$$

Dan tahapan terakhir adalah menukarkan blok final (telah dienkripsi sebanyak 16 putaran) L16 dan R16kemudian mengkonkatenasi hasil cipherteks pada blokkanan dan blok kiri. Berikut merupakan skema enkripsi dengan metode CAST[7].
CAST-256 didesain untuk mengijinkan adanyavariansi ukuran kunci dari 40 bit hingga 128 bit.Spesifikasi ukuran kunci adalah:

1. Untuk ukuran kunci yang masih berada pada *range*80 bit ke bawah, melibatkan 12 putaran prosesenkripsi.
2. Untuk ukuran kunci yang lebih banyak dari 80 bit,menggunakan 16 putaran penuh proses enkripsi.
3. Dan untuk ukuran kunci kurang dari 128 bit, kuncitersebut di-*padding*dengan *zero bytes* (pada posisi*rightmost* atau *least significant*).

2.3 File Audio

File audio merupakan sampel suara, setiap fraksi n dalam satu detik, sampel suara diambil dan disimpan sebagai informasi digital dalam *bit* dan *byte Tay Vaughan*[8].*Audio* adalah bahan yang mengandung pesan dalam bentuk *auditif* (pita suara atau piringan suara), yang dapat merangsang pikiran, perasaan, perhatian dan kemauan siswa sehingga terjadi proses belajar mengajar[9].Audio adalah fenomena fisik yang dihasilkan oleh getaran suatu benda yang berupa sinyal *analog* dengan *amplitude* yang berubah secara kontiniu terhadap satuan waktu yang disebut frekuensi.

3. ANALISA DAN PEMBAHASAN

Analisa terdapat suatu algoritma dapat bertujuan untuk melihat faktor efesiensi dan efektifitas dari algoritma yang sedang dianalisa , dapat dilakukan dengan melihat sisi waktu tempu dari suatu algoritma,proses atatu langkah langkah atau satuan waktu yang ditempuh dari suatu algoritma dalam menyelesaikan suatu masalah.kriptografi merupakan metode dengan menyandikan file teks menjadi yang sulit atau bahkan tidak dipahami melalui proses enkripsi, untuk memperoleh kembali informasi yang dapat dengan proses enkripsi, untuk memperoleh kembali informasih yang asli dan dapat dilakukan dengan proses enkripsi yang tentunya dapat digunakan dengan kunci yang benar, Untuk melindungi file teks darinpihak pihak yang tidak berkepintangan tersebut maka diperlukan enkripsi dan denkripsi agar dapat dilakukan dengan baik, dibutuhan suatu algoritma untuk endkripsi dan dekripsi .Algoritma yang digunakan dalam pengamanan file teks adalah Algoritma CAST.

Teknik kriptografi dengan menggunakan metode CAST-256 adalah teknik yang paling sederhana, pendekatan yang sederhana untuk menyisipkan informasi di dalam suatu audio.Modifikasi metode CAST-256 ini dilakukan dengan cara menysipkan

Pesan dan audio yang akan disisipkan dirubah menjadi bilangan biner berikut ini uraian proses perubahan. Untuk pengujian pesan yang disembunyikan dimanfaatkan pesan sebagia sampel seperti yang dijelaskan pada analisis kebutuhan data. Proses perubahan biner pada tabel berikut ini.

Tabel 1. Perubahan data pesan ke biner

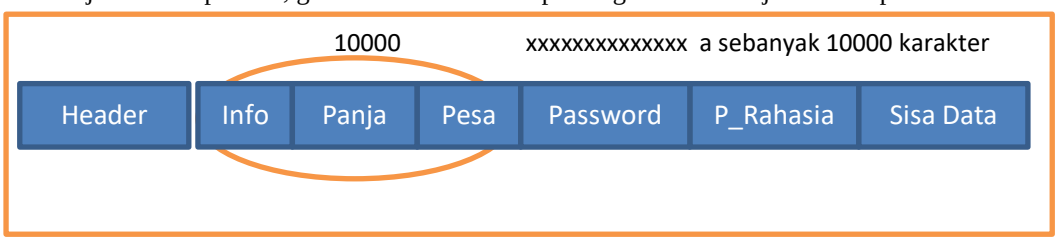
Text	Asci	Biner
F	83	01010011
R	04	01010100
I	77	01001101
D	73	01001001
A	75	01001011
H	66	01000010
U	85	01010101
T	68	01000100
A	73	01001001
H	68	01000100
A	65	01000000
E	82	01010010
A	77	01001101
N	65	01000000

Konversi data audio dengan ekstensi wav ke bilangan biner dengan bantuan aplikasi tertentu dan dihasilkan nilai ascii berikut ini.

Tabel 2. Konversi Audia WAV ke biner

ASCII	Biner	ASCII	Biner	ASCII	Biner	ASCII	Biner	ASCII	Biner
002	00000010	248	11111000	000	00000000	250	11111010	250	11111010
135	10000111	235	11101011	060	00111100	233	11101001	232	11101000
250	11111010	002	00000010	249	11111001	000	00000000	000	00000000
029	00011101	000	00000000	229	11100101	009	00001001	009	00001001
003	00000011	248	11111000	000	00000000	251	11111011	251	11111011
253	11111101	154	10011010	064	01000000	179	10110011	179	10110011
249	11111001	001	00000001	250	11111010	255	11111111	252	11111100
140	10001100	059	00111011	064	01000000	064	01000000	167	10100111
003	00000011	248	11111000	001	00000001	001	00000001	254	11111110
210	11010010	201	11001001	178	10110010	178	10110010	239	11101111

1. Membagi file wav menjadi beberapa blok, gambar berikut adalah pembagian wav menjadi beberapa blok



Gambar 2. Pembagian Blok

Blok pertama adalah header dari file wav, panjangnya yaitu 56 byte, pada bagian ini

Bedasarkan pembagian blok diatas maka blok pertama header tidak dapat dilakukan Modifikasi CAST karena akan merusak file wav ataupun file lagu tidak bisa dimainkan. Blok kedua adalah blok data wav. Blok data wav ini kemudian dibagi-bagi menjadi empat bagian bagian pertama untuk menyimpan informasi panjang karakter pesan, bagian kedua untuk menyisipkan password, bagian ketiga untuk menyisipkan pesan rahasia dan bagian ke empat adalah sisa data file wav yang tidak diubah. Untuk memperjelas maka dilakukan pembagian terhadap BIT. Dari gambar diatas maka blok header pada bit berikut ini :

Header = 00000010

Isi = **10000111 11111010 00011101 00000011**11111101 11111001 10001100 00000011 **11010010 11111000 11101011 00000010** 00000000 11111000 10011010 00000001 **00111011 11111000 11001001 00000000** 11111011 11111011 01000000 10110011 **10110011 11111010 11111111 11111100** 01000000 01000000 10100111 00000001 **00000001 11111110 11111010 11111010** 11101001 11101000 00000000 00000000 00001001 00001001 10110010

Sisa Data = 10110010

2. Melakukan Penyisipan

Proses penyisipan dilakukan dengan setiap bit nya dengan konsep CAST, namun dengan modifikasi maka dilakukan proses penyisipan dengan CAST + 1 , CAST 2 dan CAST+ 3

Data 1 : S dengan nilai Bit 01010011

Modifikasi dengan memanfaatkan CAST + 1 sehinga menghasilkan data berikut ini :

Penampung Pesan yang akan disisipkan	Hasil Perubahan Bit Penyisipan
10000111 11111010	10000**1**01 11111**1**0
00011101 00000011	00011**1**01 00000**1**1
11111101 11111001	11111**1**01 11111**1**01
10001100 00000011	10001**1**10 00000**1**1

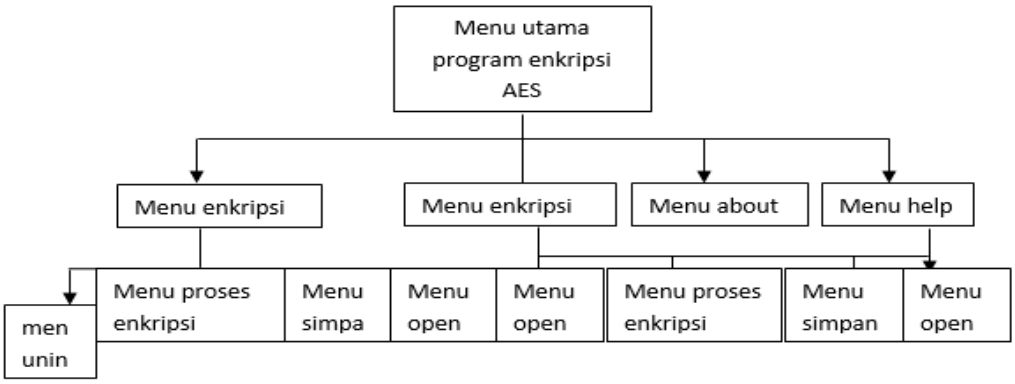
Sampai pada modifikasi dengan CAST + 3 dengan menempatkan pesan bit pada posisi ke 5, berikut ini adalah proses pembentukan Modifikasi CAST.

Penampung Pesan yang akan disisipkan	Hasil Setelah disisipkan
00111011 11111000	0011**0**011 1111**1**000
11001001 00000000	1100**1**001 0000**1**000
11111011 11111011	1111**0**011 1111**0**011
01000000 10110011	0100**0**000 1011**1**011

Shinggan di daptkan hasil pesan audio yang diaman kan dengan metode cast-256 yaitu 0011**0**011 1111**1**000 1100**1**001 0000**1**000 1111**0**011 1111**0**011 0100**0**000 1011**1**011.

Rancangan ini dibuat untuk memudahkan proses perancangnan aplikasih kripto sistem *Advance Encrptyon Standard* yang akan dibuat menggunakan algoritma enkripsi yaitu:

1. Menu enkripsi :new enkripsi (prose), Save (simpan), Open (Buka file yang diiginkan) dan meu utama.
2. Menu Dekripsi ysng terbagi menjadi New,Dekripsi (proses), save(simpan), Open (buka file yang diinginkan),dan menu utama.
3. Menu About : yang menjelaskan mengenai program aplikasih.
4. Menu Help :yang menjelaskan fungsi fungsi setiap event pada aplikasih



Gambar 3. Diagram hirakik

Skenario utama :

1. Pengiriman dan penerima sepakat untu melakukan pengiriman file teks secara aman mengunakan algoritma CAST 128
2. Penerimaan melakuka pembuatan kunci dan dihasilkan kunci umu dan kunci rahasia.

3. Kunci umu diberikan kepada sipengirim, melalui kunci tersebut sipengirim melakukan enkripsi dan terhadap file teks yang terinkripsi dan selajut ny hasil file tersebut dikirim ke sipenerima.
4. File tesk tersebut didekripsikan oleh sipenerima menggunak kunci rahasia yang telah dibuat sebelum ny.
5. Activity Diagram Pengembalian Teks

Activity diagram adalah ineraksi antara sistem dengan user dalam melakukan Pengembalian Teks dari wav.

4. KESIMPULAN

Setelah menyelesaikan pembahasan mengenai perancangan aplikasi keamanan pesan audio dengan metode cast-256 maka dapat diambil kesimpulan sebagai berikut:

1. Sistem keamanan data menggunakan aplikasi kriptografi dibuat untuk mengamankan file audio yang dibangun menggunakan bahasa pemograman Visual basic.
2. Berdasarkan hasil evaluasi yang telah penulis lakukan terhadap pengamanan file audio mengunakan metode Cast-256 berbasis visual basic mudah digunakan, dan membantu untuk meyelesaikan dalam mengamankan file audio bersifat rahasia..

REFERENCES

[1] Al Bahra Bin Ladjamudin, Analisis dan Desain Sistem Informasi. Tangerang: Graha Ilmu, 2005.
[2] Kusrini, Konsep dan Aplikasi Sistem Pendukung Keputusan. Yogyakarta: Andi, 2007.
[3] Dkk. Riswaya, "Aplikasi Pinjaman Pembayaran Secara Kredit Pada Bank Yudha Bhakti," vol. Vol. 8, 2016.
[4] Dkk. Rahmat Tullah, "Perancangan Aplikasi Kriptografi File Dengan Metode Algoritma Advanced Encryption Standard (AES," JURNAL SISFOTEK GLOBAL, vol. Vol. 6, 2016.
[5] Budi Utama dan Bayu Sunanda, "Perancangan perangkat lunak bantu untuk memahami kriptografi metode cast-128".
[6] Nabila As'ad, "Studi Analisis Algoritma CAST dan Implementasinya dalam PGP," MAKALAH IF3058 KRIPTOGRAFI TAHUN, 2010.
[7] Andrik Purwasito, "Analisis Pesan," The Messenger, vol. Volume 9, Januari 2017.
[8] Dkk. Rendra Warsita, "Rancang Bangun Aplikasi Kompresi Audio Berbasis Android Menggunakan Algoritma Huffman".
[9] Dkk. Frenky Fernando, "Aplikasi kriptografi untuk mengamankan file audio video menggunakan visual basic.net," Jurnal Media Infotama , vol. Vol. 10, Februari 2014.
[10] Heri Santoso dan M. Fakhriza, "Perancangan aplikasi keamanan file audio format wav (waveform) menggunakan algoritma RSA," Jurnal Ilmu Komputer dan Informatika, vol. Volume: 02, April 2018.
[11] Menggunakan UML, Informatika, Bandung, 2011 Herlawati Widodo Pudjo Prabowo,.