IMPLEMENTASI KRIPTOGRAFI HIBRID DENGAN ALGORITMA ELGAMAL DAN ALGORITMA ONETIME PAD(OTP) DALAM PENGAMANAN FILE AUDIO BERBASIS DESKTOP

Sri Melvani Hardi [(1)], Daniel Hamonangan [(2)], Muhammad Zarlis [(3)]
Program Studi S-1 Ilmu Komputer, Fasilkom-TI USU
Jalan Universitas N0.9 Kampus Universitas Sumatera Utara Medan 20155
E-mail : vani.hardi@usu.ac.id[(1)]
danchamp.siregar27@gmail.com[(2)]
m.zarlis@usu.ac.id[(3)]

Abstrak

Audio merupakan salah satu cara untuk menyampaikan informasi. Bertukar informasi audio dapat dilakukan dengan mudah pada saat ini. Namun hal ini menyebabkan informasi audio yang bersifat pribadi ataupun rahasia menjadi tidak aman. Maka dari itu diciptakanlah sebuah sistem pada desktop yang mampu mengamankan file audio dengan menggunakan algoritma One-Time Pad dan algoritma ElGamal. Algoritma One-Time Pad merupakan algoritma yang sangat aman dalam mengamankan data audio namun memiliki kerentanan didalam kebocoran informasi kunci maka dibutuhkan algoritma ElGamal yang dapat mencegah kebocoran informasi kunci. Berdasarkan pengujian didapatkan hasil bahwa cepat lambatnya waktu proses enkripsi dan proses dekripsi, dipengaruhi oleh ukuran data file audio .Semakin besar data file audio tersebut maka semakin lambat waktu proses yang dilakukan. Hasil dari sistem ini berupa file audio yang terenkripsi, file kunci OTP terenkripsi yang dapat mengamankan data.

Kata Kunci: *Kriptografi Audio, Kriptografi Wav File, One-Time Pad, ElGamal.*

1. PENDAHULUAN

Media audio adalah media yang digunakan untuk menyampaikan pesan yang hanya dapat dimengerti oleh indera pendengaran. Pesan atau informasi yang akan disampaikan dituangkan kedalam lambang-lambang auditif yang berupa kata-kata, musik, ataupun sound effect (Riyana, 2009). Media audio dipakai karena mudah dalam

DOI: https://doi.org/10.29103/techsi.v10i2.903

penggunaannya begitu juga dalam pengakasesannya. Dengan kecanggihan teknologi pada saat ini siapa pun dapat mengakses berbagai macam file audio.

Namun hal ini menyebabkan semakin tidak aman dalam bertukar informasi audio terutama audio yang bersifat rahasia ataupun pribadi yang tidak ingin diketahui orang lain. Maka dari itu perlu dilakukan pengamanan file audio sebelum audio tersebut dikirim untuk menghindari tindak kejahatan terhadap pesan audio yang dikirim.

Salah satu cara untuk menjaga keamanan dan kerahasiaan data suatu file audio adalah menggunakan kriptografi. Kriptografi adalah ilmu dan seni untuk mengamankan dokumen dengan teknik enkripsi sehingga dokumen yang diamankan tidak dapat di mengerti oleh orang lain yang tidak berkepentingan [2].

Ramadayanti (2008) meneliti tentang Analisa algoritma Vernam (OTP). Beliau menyimpulkan bahwa algoritma OTP tidak terpecahkan karena ciphertext yang seluruhnya acak didapatkan dari penjumlahan barisan kunci acak ditambah dengan plaintext yang tidak acak dan jika mendekripsikan cipherteksnya dengan beberapa kunci berbeda dapat menghasilkan plaintext yang bermakna, Namun algoritma ini juga memiliki kelemahan didalam pendistribusian kunci, pertukaran kunci yang terjadi antara pihak pengirim pesan dan penerima pesan merupakan titik rentan dalam metode enkripsi ini, karena kebocoran kunci dapat terjadi pada saat pertukaran informasi.

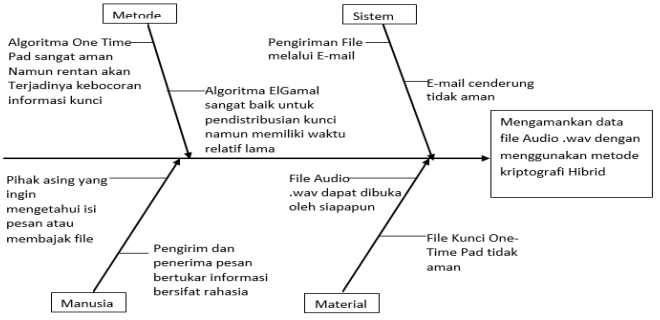
Riyanto (2007) meneliti tentang pengamanan pesan rahasia menggunakan algoritma kriptografi ElGamal atas grup penggandaan Zp*. Beliau menyimpul- kan bahwa algoritma kriptografi asimetris seperti algoritma kriptografi ElGamal, sangat baik untuk mengatasi masalah pada pendistribusian kunci.

Berdasarkan hasil penelitian diatas penulis hendak melakukan penelitian dengan mengkombinasikan algoritma One-Time Pad dan algoritma ElGamal untuk meningkatkan keamanan pada file audio, dengan judul "Implementasi Kriptografi Hibrid dengan Algoritma ElGamal dan Algoritma One-Time Pad dalam pengamanan file audio berbasis dekstop".

DOI: https://doi.org/10.29103/techsi.v10i2.903

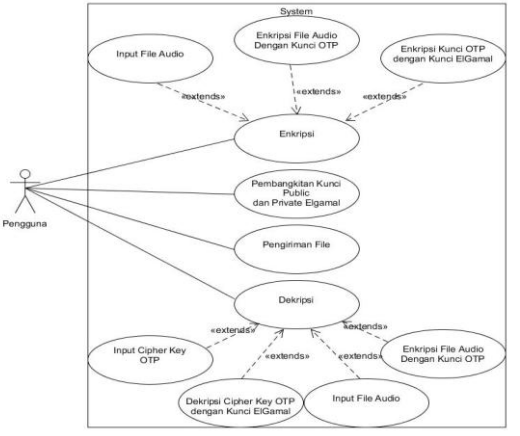
2. METODE PENELITIAN

Masalah dalam penelitian ini ditunjukan pada gambar 1 dibawah ini



Gambar 2.1. Diagram Ishikawa

Rancangan use case diagram pada penelitian ini ditunjukan pada gambar 2

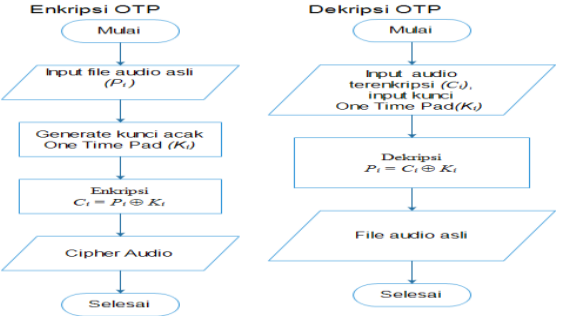


Gambar 2.2Use Case Diagram

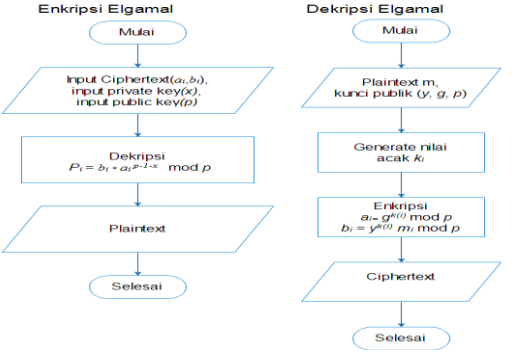
Flowchart merupakan diagram yang menggunakan simbol-simbol untuk menggambarkan urutan langkah kerja secara berurutan dan sistematis.

Berikut adalah flowchart enkripsi dan dekripsi pada sistem yang dapat dilihat pada gambar 3 dan gambar 4.′

DOI: https://doi.org/10.29103/techsi.v10i2.903



Gambar 2.3.*Flowchart* Enkripsi Dekripsi OTP



Gambar 2.4 *Flowchart* Enkripsi Dekripsi ElGamal

3. HASIL DAN PEMBAHASAN

3.1 Implementasi Sistem

Pada sistem yang dibangun ini terdapat beberapa tab page, yaitu : tabpage Beranda, tabpage Panduan, tabpage Enkripsi Audio, tabpage Pembangkit Kunci, tabpage Enkripsi Kunci OTP, tabpage Dekripsi Kunci OTP, tabpage Dekripsi Audio, tabpage Kirim File.

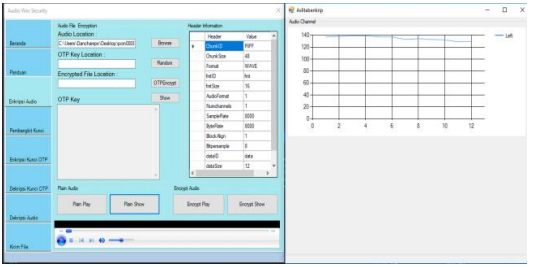
3.2 Diskusi Sistem

1. Diskusi Enkripsi Algoritma One-Time Pad(OTP):

a)pembacaan file audio

Diskusi yang dilakukan pada sistem ini adalah mengenkripsi dan mendekripsi *file audio* .wav 8-bit *mono channel* yang berukuran 56 byte yang dapat dilihat pada gambar 8.

DOI: https://doi.org/10.29103/techsi.v10i2.903



Gambar 3.1*Plainaudio*

Dari gambar 5 dapat dilihat contoh data *fileaudio* yang diinputkan di tampilkan dalam bentuk *chart*. Data *fileaudio* yang telah diuji ditunjukan dalam bentuk bilangan integer yang dapat dilihat pada tabel 1

Tabel 1 Hasil pembacaan data *plainaudio*

Index	Nilai
1	137
2	138
3	139
4	139
5	137
6	137
7	133
8	134
9	133
10	132
11	129
12	129

b) Pembangkitan Kunci One-Time Pad(OTP)

Adapun proses pembangkitan kunci *One-Time Pad* dibangkitkan secara acak sepanjang data *plainaudio*. Berikut merupakan hasil pembangkitan kunci pada tabel 2

Tabel 2 Hasil Pembangkitan Kunci OTP.

Index	Nilai
1	72
2	82
3	21
4	94
5	220
6	3
7	77
8	98
9	226
10	90
11	80
12	101

DOI: https://doi.org/10.29103/techsi.v10i2.903

c) Diskusi enkripsi file audio dengan One-Time Pad

Hasil enkripsi ini didapat dari proses perhitungan algoritma One-Time Pad yaitu (Ci=Pi ⊕Ki).

Contoh Proses enkripsi pada indeks 1:

-Pengirim mengambil data pesan audio (P1) = 137.

-Pengirim mengambil nilai Kunci One-Time Pad (K1) = 72.

-Pengirim melakukan proses enkripsi:

-(C1) = 137 ⊕72

-(C1) = 193

Hasil enkripsi perhitungan selengkapnya dapat dilihat pada tabel 3

Tabel 3 Hasil Enkripsi data plainaudio

Indeks	Data *Audio* Asli (P_i)	Kunci *One-Time Pad*(K_i)	*Audio* Terenkripsi $C_i=P_i \oplus K_i$
1	137	72	193
2	138	82	216
3	139	21	158
4	139	94	213
5	137	220	85
6	137	3	138
7	133	77	200
8	134	98	228
9	133	226	103
10	132	90	222
11	129	80	209
12	129	101	228

2. Diskusi Enkripsi Algoritma ElGamal

Dimulai dengan menerima kunci public yang dikirim oleh penerima. Kemudian membaca isi file kunci One-Time Pad yang nilainya dijelaskan pada tabel 2. Dilakukanlah proses enkripsi ElGamal menjadi kedalam dua block yaitu block ai dan block bi.

Berikut contoh perhitungan manual algoritma ElGamal :

-Pengirim pesan menerima kunci public p=257371, g=208475, y=91879.

-Pengirim pencacah pesan pada audio seperti pada table 2.

-Pengirim pesan memilih bilangan k secara acak yang relatif prima dengan p k1 =99821.

-Pengirim akan mengenkripsi pesan pada indeks 1 m1 = 72.

-Pengirim melakukan proses enkripsi menjadi block a1 dan block b1.

- a1 = gk mod p
- a1 = 20847599821 mod 257371
- a1 = 72053
- b1 = yk m mod p

DOI: https://doi.org/10.29103/techsi.v10i2.903

- b1 = 9187999821 * 72 mod 257371
- b1 = 103963

Maka dari hasil perhitungan manual didapatkanlah hasil dari enkripsi algoritma ElGamal yaitu a1 = 72053 dan b1 = 103963 dan pesan inilah yang akan dikirim kepada penerima pesan. Untuk proses perhitungan manual selengkapnya dapat dilihat pada tabel 4

Tabel 4 Hasil Perhitungan Enkripsi Algoritma El**Gamal**

Index(*i*)	Plaintext (*m*)	k_i	Ciphertext 1 (a_i) $a_i = g^k \bmod p$	Ciphertext 2 (b_i) $b_i = y^k m \bmod p$.
1	72	99821	72053	103963
2	82	257261	43609	107278
3	21	61183	162542	113545
4	94	199909	31160	246981
5	220	84557	132010	97326
6	3	218291	61502	95328
7	77	41533	88884	150684
8	98	225311	119421	234456
9	226	118813	252156	55086
10	90	215959	89930	110908

3. Diskusi Dekripsi Algoritma ElGamal

Pada algoritma *ElGamal* proses dekripsi dilakukan dengan menggabungkan $blocka_i$ dan $blockb_i$ menjadi pesan asli kembali m_i denganmenggunakan kunci *private* yang telah dibangkitkan dan bilangan prima *p* yang terdapat pada kunci *public*. Setelah itu dilakukan proses dekripsi dengan menggunakan algoritma *ElGamal*. Berikut contoh perhitungan manual proses dekripsi algoritma *ElGamal* pada indeks 1 :

-Penerima mengambil nilai kunci *private* yang telah dibangkitkan x = 130285.

-Penerima mengambil nilai bilangan prima pada kunci *publicp* = 257371.

-Penerima mengambil nilai $blocka_1$ = 72053.

-Penerima mengambil nilai $blockb_1$ = 103963.

-Penerima menghitung nilai pesan dengan algoritma *ElGamal*.

-$m_i = b / a^x \bmod p$

DOI: https://doi.org/10.29103/techsi.v10i2.903

- m_1 = 103963 / $72053^{130285} \bmod 257371$
- m_1 = 72

Hasil perhitungan manual algoritma *ElGamal* secara keseluruhan dapat dilihat pada tabel 5.

Tabel 5 Hasil Perhitungan Dekripsi Algoritma *ElGamal.*

Index(i)	Ciphertext1 (a_i)	Ciphertext2 (b_i)	Dekripsi (m) $m_i = b/a^x \bmod p$
1	72053	103963	72
2	43609	107278	82
3	162542	113545	21
4	31160	246981	94
5	132010	97326	220
6	61502	95328	3
7	88884	150684	77
8	119421	234456	98
9	252156	55086	226
10	89930	110908	90
11	188408	86840	80
12	92304	21453	101

4. Diskusi Dekripsi Algoritma One-Time Pad

Setelah didapatkan *file* kunci OTP yang telah didekripsi, maka penerima pesan dapat melakukan proses dekripsi terhadap *fileaudio* yang terenkripsi. Pada proses dekripsi *fileaudio* yang terenkripsi penerima pesan menginputkan *fileaudio* yang akan didekripsi, kemudian menginputkan *file* kunci OTP yang telah didekripsi. Proses dekripsi dilakukan dengan cara melakukan perhitungan XOR terhadap *file audio* yang terenkripsi dan *file* kunci OTP yang akan menghasilkan *file audio* asli. Berikut contoh perhitungan manual proses dekripsi algoritma *One-Time Pad* pada indeks 1 :

-Penerima mengambil nilai cipher*audio*C_1 = 193.

-Penerima mengambil nilai kunci OTP K_1= 72.

-Penerima melakukan proses dekripsi menggunakan $P_i=C_i \oplus K_i$.

-(P_1) = 137 $\oplus$72

-(P_1) = 193

DOI: https://doi.org/10.29103/techsi.v10i2.903

Perhitungan manual proses dekripsi algoritma *One-Time Pad* secara keseluruhan dapat dilihat pada tabel 6.

Tabel 6 Hasil Perhitungan Dekripsi *FileAudio.*

Indeks *i*	Kunci *One-Time Pad* (K_i)	*Audio* Terenkripsi (C_i)	Data *Audio* Asli ($P_i = C_i \oplus K_i$)
1	72	193	137
2	82	216	138
3	21	158	139
4	94	213	139
5	220	85	137
6	3	138	137
7	77	200	133
8	98	228	134
9	226	103	133
10	90	222	132
11	80	209	129
12	101	228	129

5. Diskusi Algoritma Terhadap Waktu Proses

Salah satu parameter Diskusi dalam penitian ini adalah Diskusi terhadap waktu proses enkripsi dan proses dekripsi.

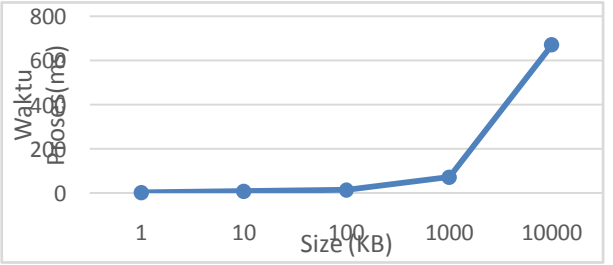
a) Diskusi Enkripsi file audio dengan algoritma OTP

Hubungan waktu proses enkripsi file audio terhadap ukuran suatu file audio dapat dilihat pada tabel 7 dan gambar 6

Tabel 7 Hasil Diskusi Waktu Proses Enkripsi *Audio*

Besar *File*(KB)	Waktu Proses (ms)			
	Percobaan 1	Percobaan 2	Percobaan 3	Rata-rata
±1	2	2	2	2
±10	9	9	9	9
±100	14	14	14	14
±1000	72	72	72	72
±10000	670	670	673	671

DOI: https://doi.org/10.29103/techsi.v10i2.903



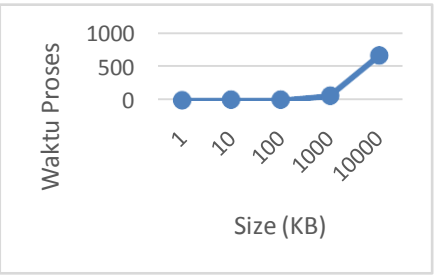
Gambar 3.2 *Chart* Waktu Proses Enkripsi Algoritma *OTP*

b) Diskusi Dekripsi file audio dengan algoritma OTP

Hubungan waktu proses enkripsi file audio terhadap ukuran suatu file audio dapat dilihat pada tabel 8 dan gambar 11.

Tabel 8 HasilDiskusi Waktu Proses Dekripsi *FileAudio*

Besar *File*(KB)	Waktu Proses (ms)			
	Percobaan 1	Percobaan 2	Percobaan 3	Rata-rata
±1	2	2	2	2
±10	9	9	9	9
±100	14	14	14	14
±1000	72	72	72	72
±10000	670	668	674	670.6



Gambar 7*Chart* Waktu Proses Dekripsi Algoritma *OTP*

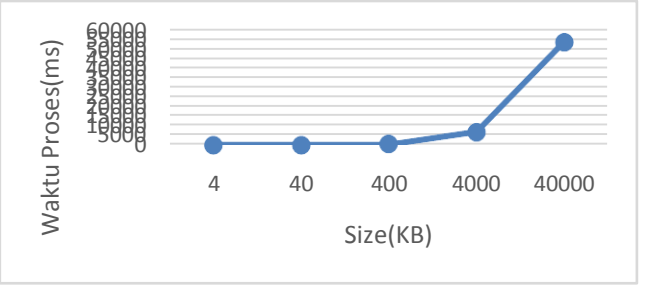
c)Diskusi Enkripsi File Kunci OTP dengan Algoritma ElGamal

Hubungan waktu proses enkripsi file kunci OTP terhadap ukuran suatu file audio dapat dilihat pada tabel 9 dan gambar 8

DOI: https://doi.org/10.29103/techsi.v10i2.903

Tabel 9 HasilDiskusi Waktu Proses Enkripsi *File* Kunci OTP.

Besar *File* Kunci OTP(KB)	Waktu Proses (ms)			
	Percobaan 1	Percobaan 2	Percobaan 3	Rata-rata
±4	21	21	21	21
±40	74	74	74	74
±400	678	675	678	677
±4000	6614	6595	6595	6601.3
±40000	53751	54201	53118	53690



Gambar 3.3 *Chart* Waktu Proses Enkripsi Algoritma *ElGamal.*

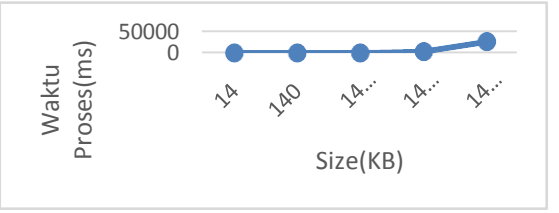
d)Diskusi Dekripsi File Kunci OTP dengan Algoritma ElGamal

Hubungan waktu proses enkripsi file kunci OTP terhadap ukuran suatu file audio dapat dilihat pada tabel 10 dan gambar 9.

Tabel 10 HasilDiskusi Waktu Proses Dekripsi *File* Kunci OTP.

Besar *File* kunci	Waktu Proses (ms)			
	Percobaan 1	Percobaan 2	Percobaan 3	Rata-rata
±14	8	8	8	8
±140	45	45	45	45
±1400	344	344	344	344
±14000	2828	2807	2796	2810.3
±140000	25409	25483	25514	25468

DOI: https://doi.org/10.29103/techsi.v10i2.903



Gambar 3.4 *Chart* Waktu Proses Dekripsi Algoritma *ElGamal*.

4. KESIMPULAN

1. Implementasi kriptografi hibrid dari kedua algoritma berhasil diterapkan dan hasil diskusi pada sistem didapatkan bahwa file audio yang telah mengalami proses enkripsi dan proses dekripsi dengan algoritma One-Time Pad memiliki isi informasi yang sama dengan file audio yang asli.
2. Hasil diskusi pada sistem didapatkan bahwa pengkombinasian algoritma ElGamal dan One-Time Pad tidak efisien dikarenakan file kunci OTP terenkripsi memiliki ukuran data yang lebih besar dibanding file audio yang terenkripsi yang artinya pengiriman file kunci dan file audio serta proses enkripsi dan proses dekripsi akan membutuhkan waktu yang sangat lama.

DAFTAR PUSTAKA

Iqbal, M & Pane, M. A. S. 2016. SMS Encryption Using One-Time Pad Cipher. *IOSR Journal of Computer Engineering (IOSR-JCE)* Volume 18, No. 6: 54-58.

Ramadayanti, A. L. 2008. Analisa algoritma Vernam (OTP). Skripsi. Universitas Sriwijaya.

Riyanto, M. Z. 2007. Pengamanan Pesan Rahasia Menggunakan Algoritma ElGamal Atas Grup Pergandaan Z_p^*. Skripsi. Universitas Gadjah Mada.

Rolf, O. 2011. *Contemporary Cryptography.* 2nd Edition. Artech House: Norwood.

Salomon, D. 2007. *Data Compression: The Complete Reference.* 4th Edition.Springer- Verlag: London.

Zelvina, A., Efendi, S. & Arisandi, D. 2012. Perancangan Aplikasi Pembelajaran Kriptografi Kunci Publik ElGamal Untuk Mahasiswa. *Jurnal Dunia Teknologi Informasi* Volume 1, No. 1: 56-62.

DOI: https://doi.org/10.29103/techsi.v10i2.903