LAMPIRAN A
ALGORITMA AES – 128

AES (Advanced Encryption Standard)

Algoritma AES diperoleh melalui kompetisi yang dilakukan pada tahun 1997 oleh NIST (*National Institute of Standard and Technology*) untuk mencari standar algoritma enkripsi yang dapat dipergunakan dalam berbagai aplikasi. Proses seleksi ini amat ketat dan membutuhkan waktu yang cukup lama. Pada akhirnya, tanggal 2 Oktober 2000 terpilihlah algoritma Rijndael yang dibuat oleh Rijmen dan Daemen dari Belgia sebagai standar algoritma enkripsi yang biasa disebut AES. Meskipun masih baru, algoritma ini sudah dipergunakan pada berbagai aplikasi, salah satunya adalah untuk penyandian *password*. Penggunaan algoritma ini sudah sering dilihat pada perangkat lunak untuk kompresi data. Dalam perangkat lunak tersebut, salah satu metode yang digunakan untuk mengenkripsi *password* adalah dengan algoritma AES.

Garis besar algoritma Rijndael yang beroperasi pada blok 128-bit adalah sebagai berikut:

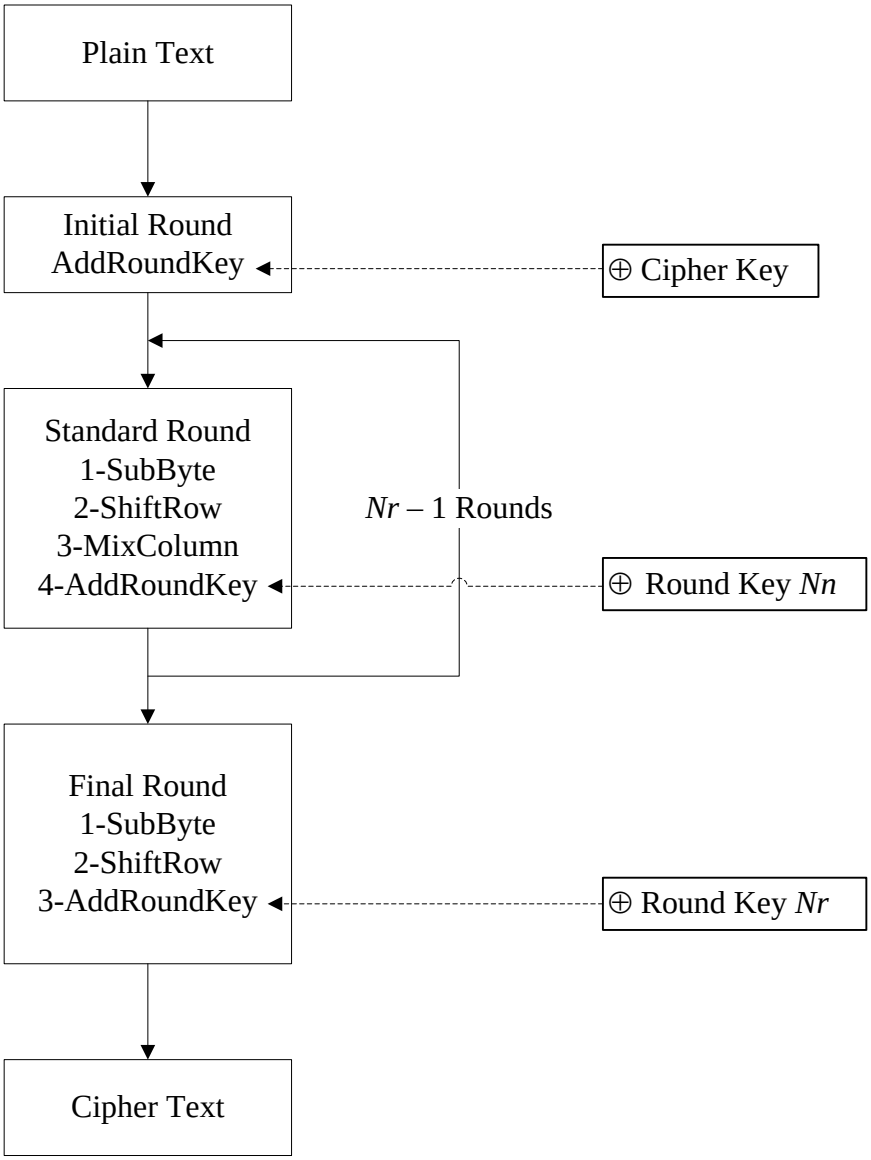
1. *AddRoundKey* : melakukan X-or antara *state* awal *(plainteks)* dengan *cipher key*. Tahap ini disebut juga *initial round*.
2. Putaran sebanyak Nr – 1 kali. Proses yang dilakukan pada setiap putaran adalah:
    a. *SubByte* : substitusi *byte* dengan menggunakan tabel substitusi (S-box).
    b. ShiftRow : pergeseran baris-baris *array* state secara *wrapping*.
    c. *MixColumn* : mengacak data pada masing-masing kolom *array state*.
    d. *AddRoundKey* : melakukan operasi X-or antara *state* sekarang dengan *round key*.
3. *Final round* : proses untuk putaran terakhir:
    a. *SubByte.*
    b. *ShiftRow.*
    c. *AddRoundKey.*

Algoritma Rijndael mempunyai 3 parameter yaitu :

1. *Plainteks* adalah *array* yang berukuran 16 *byte*, yang berisi data masukan.
2. *Cipherteks* adalah *array* yang berukuran 16 *byte*, yang berisi hasil enkripsi.

3. *Key* adalah *array* yang berukuran 16 byte, yang berisi kunci *ciphering* (disebut juga *cipher key*).

Blok diagram proses enkripsi AES dapat dilihat pada Gambar 2.1. Dengan Nr merupakan banyaknya putaran yang dilakukan dan Nn adalah putaran ke-n.



Gambar 1. Blok diagram Enkripsi AES

Rijndael mendukuang panjang kunci 128 bit sampai 256 bit. Panjang kunci dan ukuran blok dapat dipilih secara independen, dan setiap blok dienkripsi sejumlah

putaran tertentu. Jumlah putaran yang digunakan algoritma AES – 128 dapat dilihat pada Tabel 2.1.

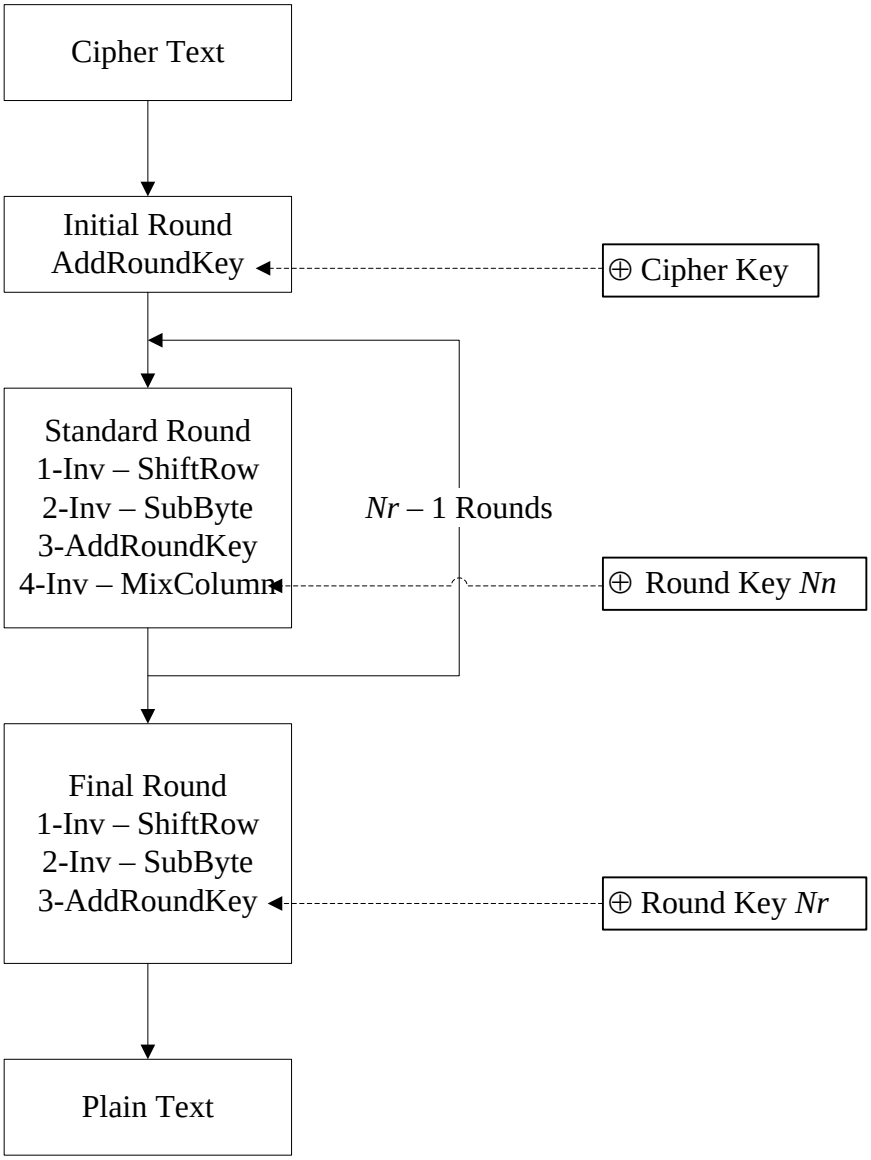
Tabel 1. Jumlah Putaran Pengoperasian AES – 128

Type	Panjang Kunci	Ukuran Blok	Jumlah Putaran
AES-128	128 bit	128 bit	10
AES-192	192 bit	128 bit	12
AES-256	256 bit	128 bit	14

Sedangkan algoritma dekripsi teorema AES – 128 yang beroperasi pada blok 128-bit adalah sebagai berikut :

1. *AddRoundKey* : melakukan X-or antara *state* awal (*cipherteks*) dengan *cipher key*. Tahap ini disebut juga *initial round*.
2. Putaran sebanyak Nr – 1 kali. Proses yang dilakukan pada setiap putaran adalah :
   a. *InvShiftRow* : pergeseran baris-baris *array* state secara *wrapping*.
   a. *InvSubByte* : substitusi *byte* dengan menggunakan tabel substitusi *Inverse* S-box.
   b. *AddRoundKey* : melakukan operasi X-or antara *state* sekarang dengan *round key*.
   c. *InvMixColumn* : mengacak data pada masing-masing kolom *array state*.
3. *Final round* : proses untuk putaran terakhir:
   a. *InvShiftRow*.
   b. *Inv SubByte*.
   c. *AddRoundKey*

Blok diagram algoritma dekripsi AES – 128 dapat dilihat pada Gambar 2.2. Untuk selanjutnya akan dijelaskan setiap iterasi tahapan *rounds* dari algoritma enkripsi dan dekripsi AES – 128.



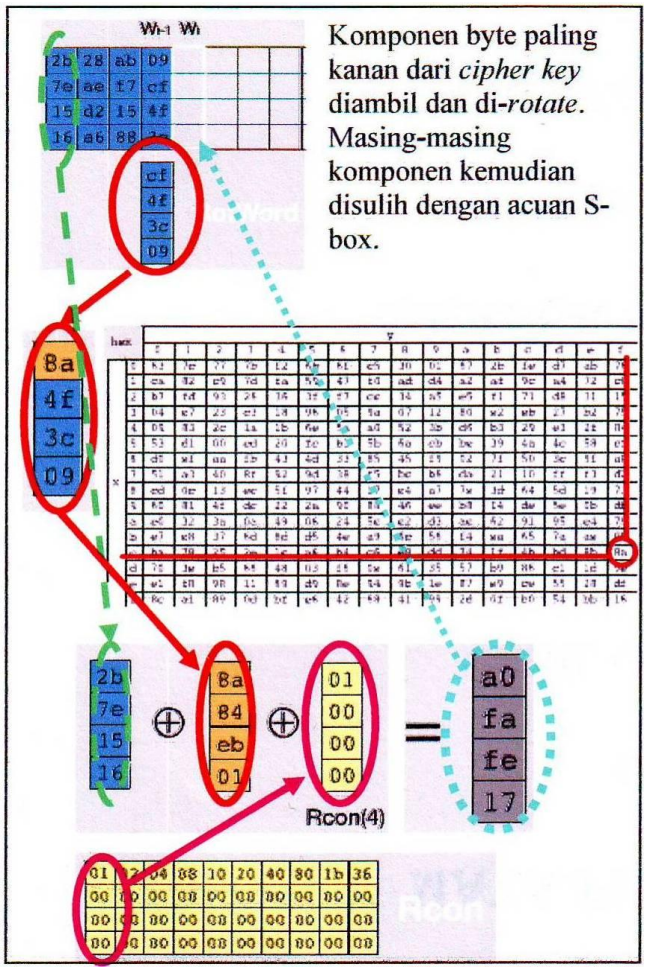
Gambar 2. Blok Diagram Dekripsi AES – 128

Prosedur *Key Expansion*

Ekspansi *cipher key* digunakan untuk membentuk *round key* yang akan digunakan pada langkah-langkah enkripsi dan dekripsi. Ekspansi kunci ini memiliki tahapan khusus yang dikenal sebagai *Rijndael's key schedule*.

Iterasi tahapan AddR*oundKey* pada algoritma AES – 128 diulang sebanyak sebelas kali. Oleh karenanya, terdapat sepuluh kali *round key* yang dibutuhkan dalam satu kali enkripsi *state*. Melalui *key schedule* tersebut, *key* yang menjadi

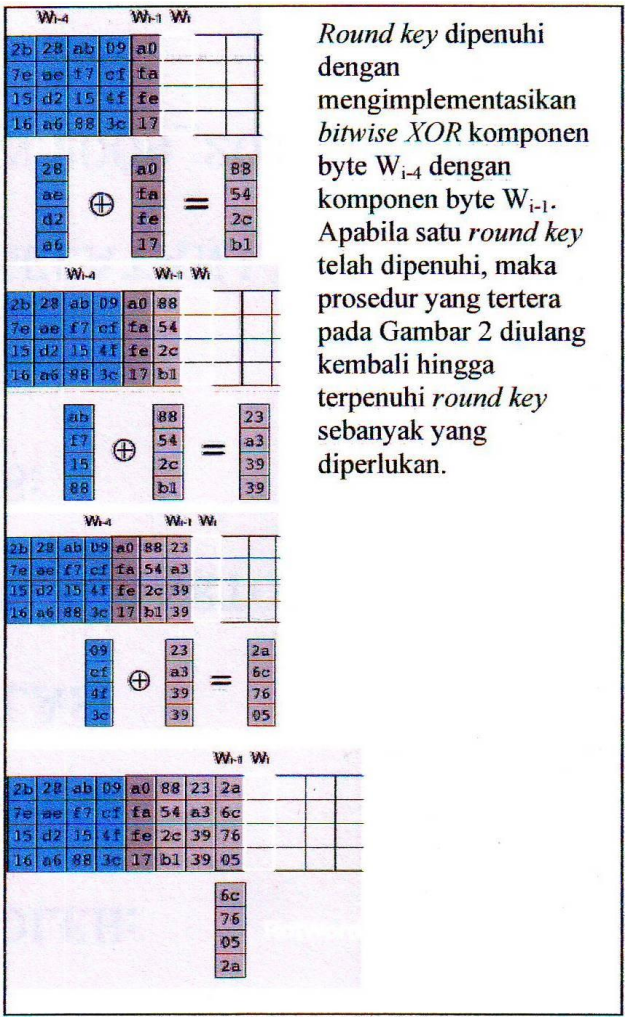
parameter masukan akan diekspansi menjadi beberapa *round key*. Ilustrasi tahapan *key schedule* dapat dilihat pada Gambar 2.3 da 2.4.



Gambar 3. Ilustrasi Prosedur *rijndael's key schedule*

AddRoundkey

Tahapan *AddRoundKey* pada algoritma enkripsi AES sesungguhnya hanyalah operasi X-or terhadap komponen *byte plaintext* dengan acuan *cipher key* (W) yang dihasilkan pada prosedur *key schedule*. Masing-masing komponen *byte* diubah ke dalam bentuk biner untuk kemudian dioperasikan masing – masing bit dengan fungsi logika X-or. Bilangan biner yang terbentuk kemudian dikonversi lagi menjadi komponen *byte* yang mewakili.



Gambar 4. Lanjutan Ilustrasi Prosedur *rijndael's key schedule*

Transformasi Subtitusi *Byte*

Dalam operasi ini, setiap *byte* yang akan dienkripsi disubtitusikan dengan nilai *byte* lain dengan menggunakan *S-box*. Tabel S-box yang dimaksud dapat dilihat pada Gambar 2.5. AES – 128 merupakan algoritma simetri, yang berarti tabel subtitusi yang dibutuhkan untuk enkripsi berbeda dengan dekripsi. Tabel S-box *invers* dapat dilihat pada Gambar 2.6

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

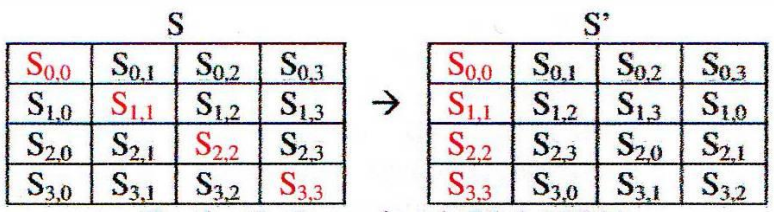
Gambar 5. S-box

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

Gamabr 6. S-box *Inverse*

<u>Transformasi Pergeseran Baris</u>

Pada operasi ini, *byte-byte* (128 bit) pada setiap baris digeser secara memutar dengan pergeseran yang berbeda dari tiap-tiap baris sesuai aturan. Baris ke-satu tidak akan mengalami proses pergeseran, sedangkan untuk baris ke-dua di geser satu kali ke kiri. Baris ketiga digeser ke kiri sebanyak dua kali dan baris ke-empat digeser ke kiri sebanyak tiga kali. Untuk lebih jelasnya, proses tersebut dapat dilihat pada Gambar 2.7



Gambar 7. Operasi Pada Blok 128-bit

Pada algoritma enkripsi akan dilakukan pergeseran ke arah kiri, tetapi pada algoritma dekripsi pergeseran dilakukan ke arah kanan.

Transformasi Pencampuran Kolom

Transformasi ini mengoperasikan blok pada masing-masing kolomnya. Setiap kolom akan dilakukan perkalian dengan matriks sesuai persamaan (2.1)

$$\begin{bmatrix} s'_{0,c} \\ s'_{1,c} \\ s'_{2,c} \\ s'_{3,c} \end{bmatrix} = \begin{bmatrix} 02\ 03\ 01\ 01 \\ 01\ 02\ 03\ 01 \\ 01\ 01\ 02\ 03 \\ 03\ 01\ 01\ 02 \end{bmatrix} \begin{bmatrix} s_{o,c} \\ s_{1,c} \\ s_{2,c} \\ s_{3,c} \end{bmatrix} \quad (2.1)$$

Dengan *c* adalah letak kolom, sehingga hasilnya adalah sebagai berikut :

$$s'0,c = (\{02\} \bullet s0,c) \oplus (\{03\} \bullet s1,c) \oplus s2,c \oplus s3,c \quad (2.2)$$

$$s'0,c = s0,c \oplus (\{02\} \bullet s1,c) \oplus (\{03\} \bullet s2,c) \oplus s3,c \quad (2.3)$$

$$s'0,c = s0,c \oplus s1,c \oplus (\{02\} \bullet s2,c) \oplus (\{03\} \bullet s3,c) \quad (2.4)$$

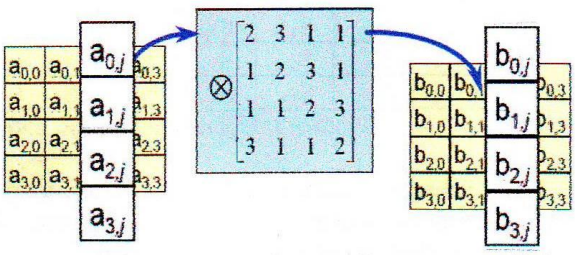
$$s'0,c = (\{03\} \bullet s0,c) \oplus s1,c \oplus s2,c \oplus (\{02\} \bullet s3,c) \quad (2.5)$$

Jika hasil perkalian memiliki lebih dari 8 bit, bit yang lebih tidak begitu saja dibuang. Hasil tersebut dilakukan operasi X-or dengan 100011011. Sebagai

contoh, perkalian 11001010 dengan 11 dengan GF$\left(2^8\right)$ akan berlangsung sebagai berikut :

11001010
11
---------- *
11001010
11001010
---------- xor
101011110
100011011
---------- xor
1000101

Nilai 1000101 merupakan hasil dari perkalian tersebut. Ilustrasi pencampuran kolom dapat dilihat pada Gambar 2.8.



Gambar 8. Ilustrasi Transformasi Percampuran Kolom

Operasi transformasi ini tidak digunakan dalam putaran terakhir, baik untuk enkripsi maupun dekripsi. Pada proses dekripsi pencampuran kolom dilakukan dengan cara melakukan perkalian dengan matriks dibawah ini :

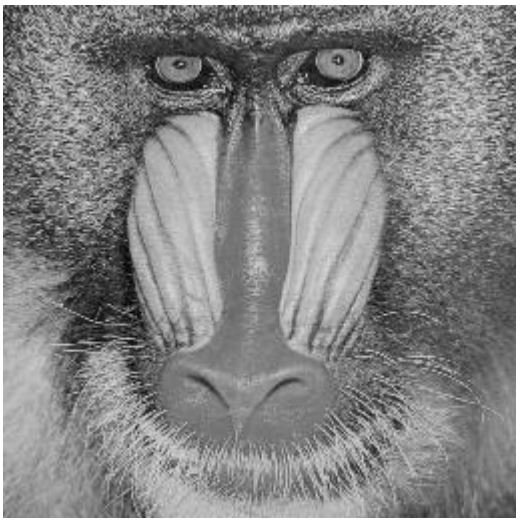
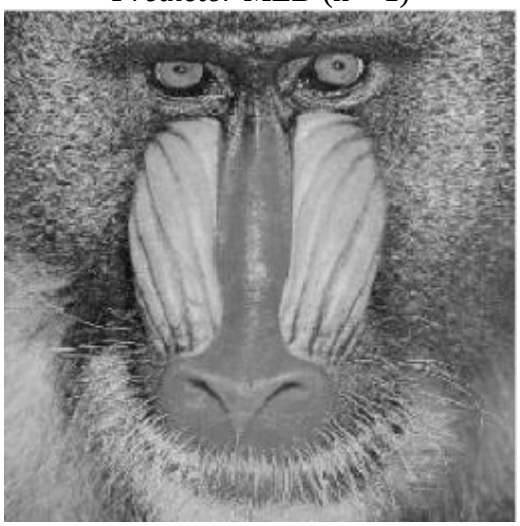
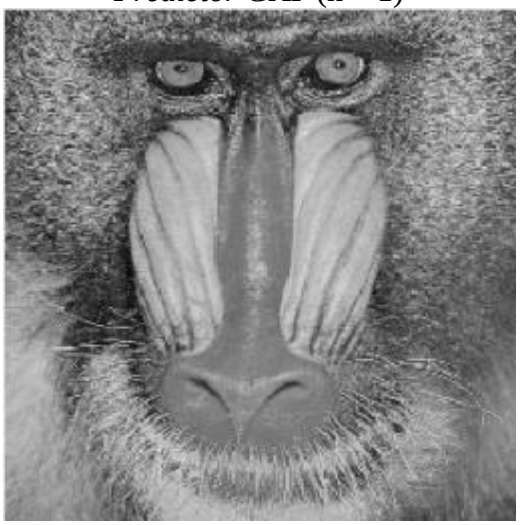
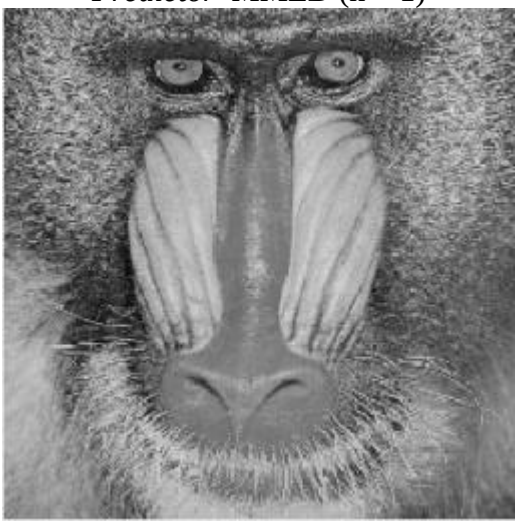
0e 0b 0d 09
09 0e 0b 0d
0d 09 0e 0b
0b 0d 09 0e

LAMPIRAN B
DATA PENGAMATAN HASIL PERCOBAAN

DATA PENGAMATAN PERCOBAAN PERTAMA

Stego – Image (*Host – Image* dan Data Rahasia Berupa Citra Bercorak)

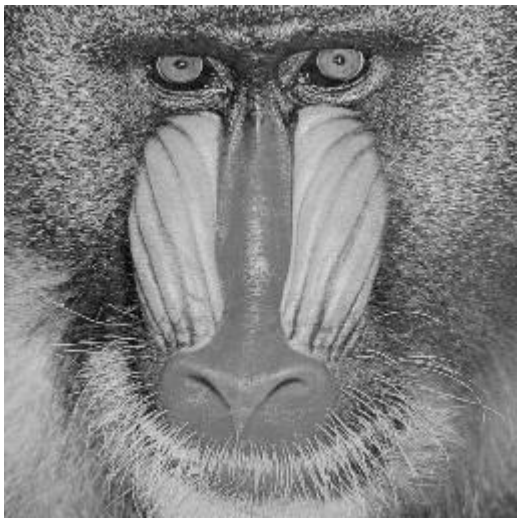
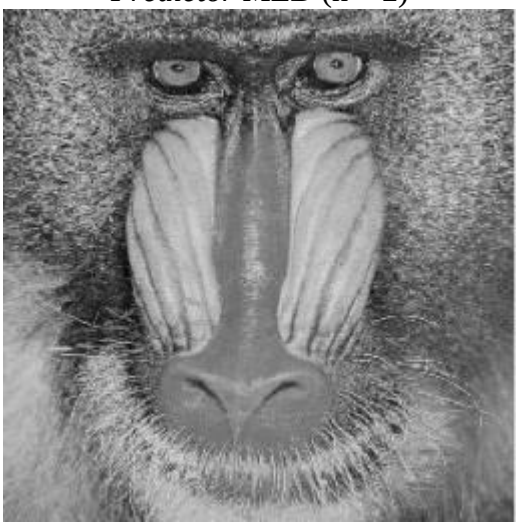
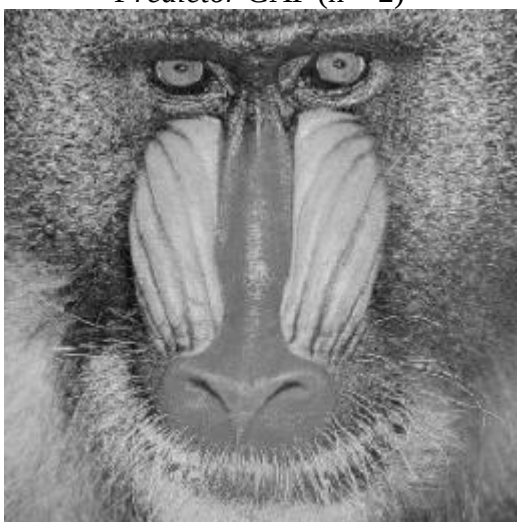
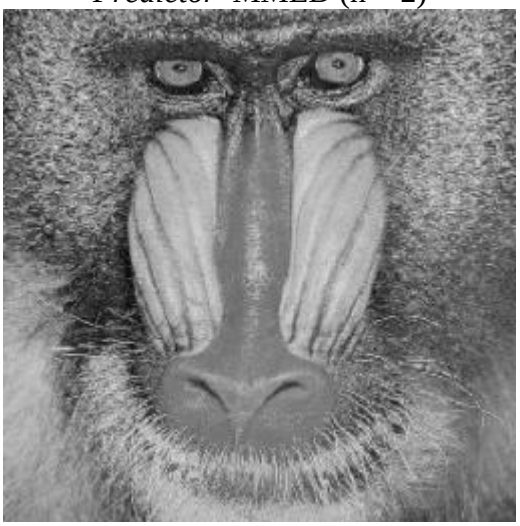
Host – Image Asli Lena 256 X 256 Pixel 	*Stego – Image* Lena Menggunakan *Predictor* MED (h = 1) 
Stego – Image Lena Menggunakan *Predictor* GAP (h = 1) 	*Stego – Image* Lena Menggunakan *Predictor* MMED (h = 1) 

Host – Image Asli Madrill 256 X 256 Pixel 	*Stego – Image* Madrill Menggunakan *Predictor* MED (h = 1) 
Stego – Image Madrill Menggunakan *Predictor* GAP (h = 1) 	*Stego – Image* Madrill Menggunakan *Predictor* MMED (h = 1) 

Host – Image Asli Zelda 256 X 256 Pixel 	*Stego – Image* Zelda Menggunakan *Predictor* MED (h = 1) 
Stego – Image Zelda Menggunakan *Predictor* GAP (h = 1) 	*Stego – Image* Zelda Menggunakan *Predictor* MMED (h = 1) 

Host – Image Asli Boat 256 X 256 Pixel 	*Stego – Image* Boat Menggunakan *Predictor* MED (h = 1) 
Stego – Image Boat Menggunakan *Predictor* GAP (h = 1) 	*Stego – Image* Boat Menggunakan *Predictor* MMED (h = 1) 

Host – Image Asli Lena 256 X 256 Pixel 	*Stego – Image* Lena Menggunakan *Predictor* MED (h = 2) 
Stego – Image Lena Menggunakan *Predictor* GAP (h = 2) 	*Stego – Image* Lena Menggunakan *Predictor* MMED (h = 2) 

Host – Image Asli Madrill 256 X 256 Pixel 	*Stego – Image* Madrill Menggunakan *Predictor* MED (h = 2) 
Stego – Image Madrill Menggunakan *Predictor* GAP (h = 2) 	*Stego – Image* Madrill Menggunakan *Predictor* MMED (h = 2) 

Host – *Image* Asli Zelda 256 X 256 Pixel 	*Stego* – *Image* Zelda Menggunakan *Predictor* MED (h = 2) 
Stego – *Image* Zelda Menggunakan *Predictor* GAP (h = 2) 	*Stego* – *Image* Zelda Menggunakan *Predictor* MMED (h = 2) 

Host – *Image* Asli Boat 256 X 256 Pixel 	*Stego* – *Image* Boat Menggunakan *Predictor* MED (h = 2) 
Stego – *Image* Boat Menggunakan *Predictor* GAP (h = 2) 	*Stego* – *Image* Boat Menggunakan *Predictor* MMED (h = 2) 

Citra Rahasia Bercorak Hasil Ekstraksi *Stego – Image* (*Host – Image* dan Data Rahasia Berupa Citra Bercorak)

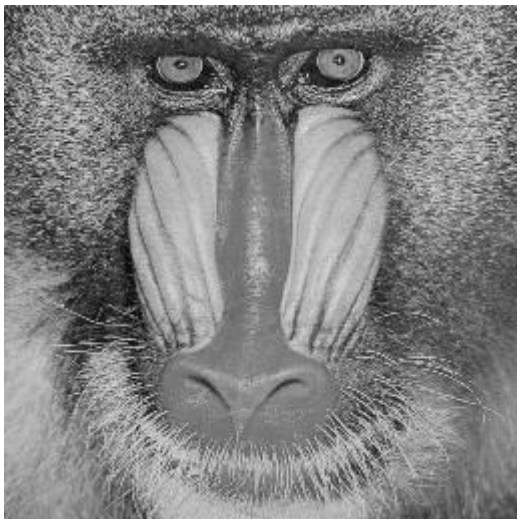
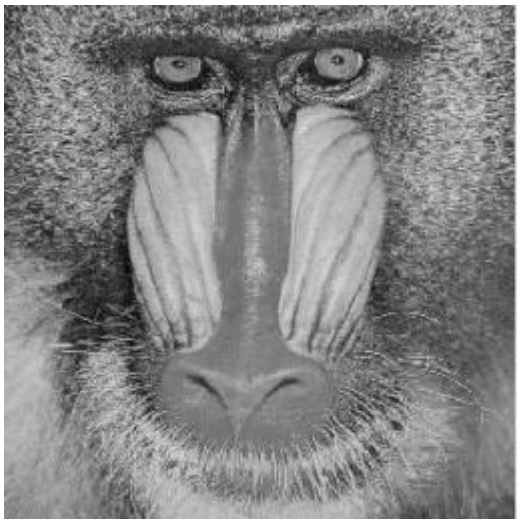
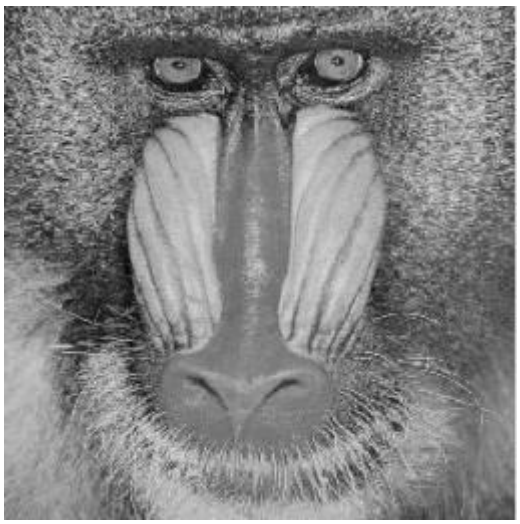
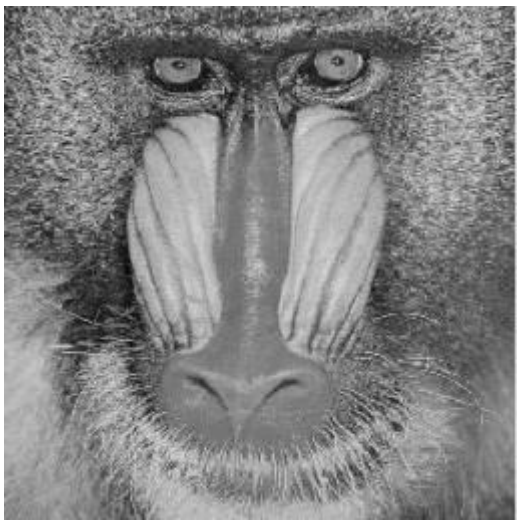
Secret – Image Pada *Stego – Image* Lena Menggunakan *Predictor* MED (h = 1) 	*Secret – Image* Pada *Stego – Image* Zelda Menggunakan *Predictor* MED (h = 1) 
Secret – Image Pada *Stego – Image* Lena Menggunakan *Predictor* GAP (h = 1) 	*Secret – Image* Pada *Stego – Image* Zelda Menggunakan *Predictor* GAP (h = 1) 
Secret – Image Pada *Stego – Image* Lena Menggunakan *Predictor* MMED (h = 1) 	*Secret – Image* Pada *Stego – Image* Zelda Menggunakan *Predictor* MMED (h = 1) 
Secret – Image Pada *Stego – Image* Mandrill Menggunakan *Predictor* MED (h = 1) 	*Secret – Image* Pada *Stego – Image* Boat Menggunakan *Predictor* MED (h = 1) 
Secret – Image Pada *Stego – Image* Mandrill Menggunakan *Predictor* GAP (h = 1) 	*Secret – Image* Pada *Stego – Image* Boat Menggunakan *Predictor* GAP (h = 1) 
Secret – Image Pada *Stego – Image* Mandrill Menggunakan *Predictor* MMED (h = 1) 	*Secret – Image* Pada *Stego – Image* Boat Menggunakan *Predictor* MMED (h = 1) 

Secret – Image Pada *Stego – Image* Lena Menggunakan *Predictor* MED (h = 2) 	*Secret – Image* Pada *Stego – Image* Zelda Menggunakan *Predictor* MED (h = 2) 
Secret – Image Pada *Stego – Image* Lena Menggunakan *Predictor* GAP (h = 2) 	*Secret – Image* Pada *Stego – Image* Zelda Menggunakan *Predictor* GAP (h = 2) 
Secret – Image Pada *Stego – Image* Lena Menggunakan *Predictor* MMED (h = 2) 	*Secret – Image* Pada *Stego – Image* Zelda Menggunakan *Predictor* MMED (h = 2) 
Secret – Image Pada *Stego – Image* Mandrill Menggunakan *Predictor* MED (h = 2) 	*Secret – Image* Pada *Stego – Image* Boat Menggunakan *Predictor* MED (h = 2) 
Secret – Image Pada *Stego – Image* Mandrill Menggunakan *Predictor* GAP (h = 2) 	*Secret – Image* Pada *Stego – Image* Boat Menggunakan *Predictor* GAP (h = 2) 
Secret – Image Pada *Stego – Image* Mandrill Menggunakan *Predictor* MMED (h = 2) 	*Secret – Image* Pada *Stego – Image* Boat Menggunakan *Predictor* MMED (h = 2) 

DATA PENGAMATAN PERCOBAAN KE-DUA

Stego – Image (*Host – Image* Berupa Citra Bercorak dan Data Rahasia Berupa Teks Rahasia 8192 *byte*) (h=1)

Host – Image Asli Lena 256 X 256 Pixel 	*Stego – Image* Lena Menggunakan *Predictor* MED 
Stego – Image Lena Menggunakan *Predictor* GAP 	*Stego – Image* Lena Menggunakan *Predictor* MMED 

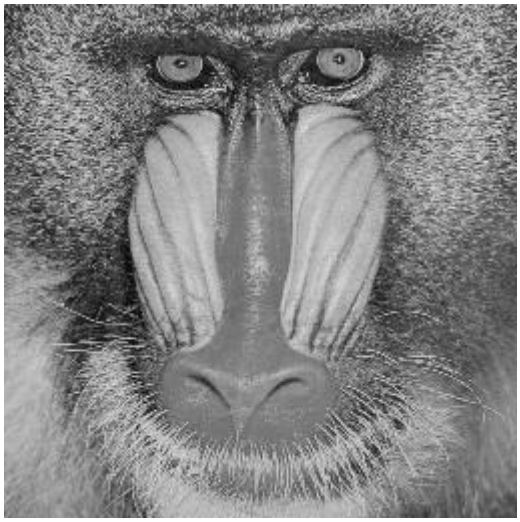
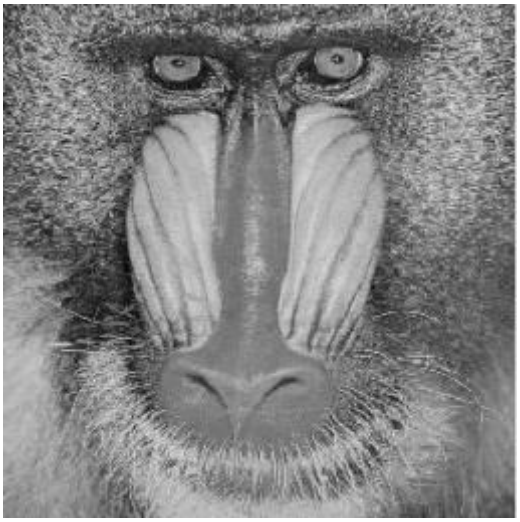
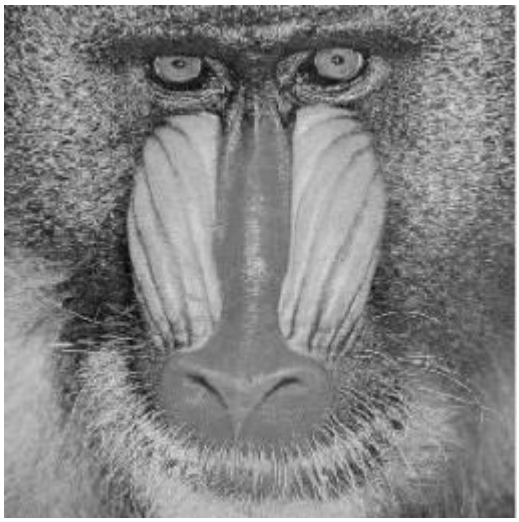
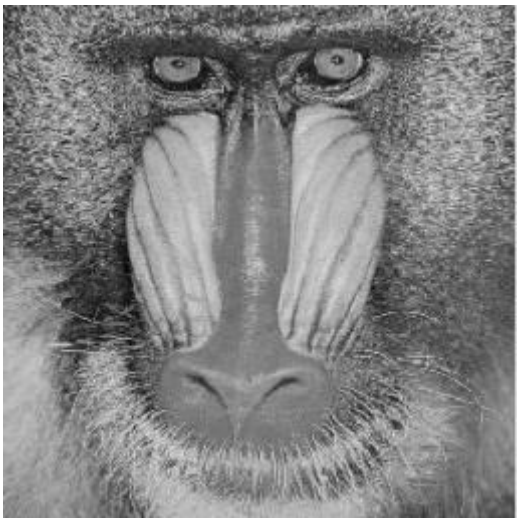
Host – Image Asli Mandrill 256 X 256 Pixel 	*Stego – Image* Mandrill Menggunakan *Predictor* MED 
Stego – Image Mandrill Menggunakan *Predictor* GAP 	*Stego – Image* Mandrill Menggunakan *Predictor* MMED 

Host – Image Asli Zelda 256 X 256 Pixel 	*Stego – Image* Zelda Menggunakan *Predictor* MED 
Stego – Image Zelda Menggunakan *Predictor* GAP 	*Stego – Image* Zelda Menggunakan *Predictor* MMED 

Host – Image Asli Boat 256 X 256 Pixel 	*Stego – Image* Boat Menggunakan *Predictor* MED 
Stego – Image Boat Menggunakan *Predictor* GAP 	*Stego – Image* Boat Menggunakan *Predictor* MMED 

Stego – Image (*Host – Image* Berupa Citra Bercorak dan Data Rahasia Berupa Teks Rahasia 16384 *byte*) (h=2)

Host – Image Asli Lena 256 X 256 Pixel 	*Stego – Image* Lena Menggunakan *Predictor* MED 
Stego – Image Lena Menggunakan *Predictor* GAP 	*Stego – Image* Lena Menggunakan *Predictor* MMED 

Host – Image Asli Mandrill 256 X 256 Pixel 	*Stego – Image* Mandrill Menggunakan *Predictor* MED 
Stego – Image Mandrill Menggunakan *Predictor* GAP 	*Stego – Image* Mandrill Menggunakan *Predictor* MMED 

Host – Image Asli Zelda 256 X 256 Pixel 	*Stego – Image* Zelda Menggunakan *Predictor* MED 
Stego – Image Zelda Menggunakan *Predictor* GAP 	*Stego – Image* Zelda Menggunakan *Predictor* MMED 

Host – *Image* Asli Boat 256 X 256 Pixel 	*Stego* – *Image* Boat Menggunakan *Predictor* MED 
Stego – *Image* Boat Menggunakan *Predictor* GAP 	*Stego* – *Image* Boat Menggunakan *Predictor* MMED 

DATA PENGAMATAN UNTUK TEKS RAHASIA MASUKAN MAKSIMUM

Teks Rahasia 8192 *byte* Asli Yang Akan Disispkan Pada Setiap *Host – Image* Bercorak (h = 1)

Kriptografi adalah ilmu sekaligus seni untuk menjaga kerahasiaan pesan dengan cara menyamarkannya menjadi bentuk tersandi yang tidak mempunyai makna. Bentuk tersandi ini hanya dapat dibaca oleh pihak yang berhak membacanya. Pesan yang akan dirahasiakan sebelum disamarkan disebut plaintext, sedangkan pesan setelah disamarkan disebut chipertext. Proses penyamaran plaintext ke chipertext disebut enkripsi, sedangkan pengembalian chiperteks menjadi plainteks semula disebut dekripsi.Kriptografi telah lama digunakan oleh tentara Sparta di Yunani sekitar tahun 400 SM. Mereka menggunakan alat yang disebut scytale. Alat ini terbuat dari daun papirus yang dililitkan pada batang silinder. Pesan yang akan dikirim ditulis horizontal. Setelah ditulis, daun dilepaskan dari batang kemudian dikirimkan ke penerima. Penerima dapat membaca pesan tersebut setelah melilitkan kembali daun tersebut pada batang silinder dengan ukuran diameter yang sama. Teknik ini dikenal dengan nama transposisi chiper yang merupakan metode enkripsi tertua. Pada zaman Romawi kuno, Julius Caesar juga menggunakan kriptografi untuk mengirimkan pesannya. Pesan yang ia kirimkan ditulis dengan mengganti alfabet dengan alfabet lain dengan kunci tertentu. Sang penerima tentu saja telah diberi tahu kunci tersebut. Cara menyandikannya adalah dengan mengganti semua susunan alfabet dengan alfabet yang posisinya berada setelah alfabet tersebut tergantung kunci. Sebagai contoh, Julius Caesar mengganti huruf a, b, dan c menjadi d, e, dan f. Pada perang dunia kedua, Jerman menggunakan mesin untuk mengrenkripsi pesan yang dikirimkan Hitler ke tentaranya yang bernama mesin enigma. Jerman meyakini kode-kode enkripsi dari mesin tersebut tidak dapat dipecahkan karena memiliki sekitar 15 milyar kemungkinan untuk mendekripsikannya. Kenyataannya sekutu mampu mendekripsikannya sehingga mesin tersebut beberapa kali memgalami perubahan.Fungsi hash sering disebut sebagai fungsi satu arah(one-way function). Fungsi ini mengubah suatu masukan menjadi keluaran, tetapi keluaran tersebut tidak dapat dikembalikan menjadi bentuk semula. Salah satu manfaatnya adalah penggunaan sidik jari (fingerprint). Sidik jari digunakan sebagai identitas pengirim pesan. Fungsi lain adalah untuk kompresi dan message digest. Contoh algoritma fungsi ini adalah MD-5 dan SHA.Pada algoritma ini, digunakan dua buah kunci yang berhubungan yang disebut dengan kunci umum dan kunci pribadi. Kunci umum dapat dipublikasikan sehingga pesan dapat dienkripsikan tetapi tidak dapat didekripsikan dengan kunci tersebut. Kunci pribadi hanya boleh digunakan oleh pihak yang berhak untuk mendekripsikan pesan yang terenkripsi. Algoritma yang menggunakan kunci umum dan publik ini antara lain : Digital Signature Algorithm (DSA), Rivest-Shamir-Adleman (RSA), Diffie-Hellman (DH), dan sebegainya.Algoritma ini menggunakan kunci yang sama untuk mengenkripsi dan mendekripsi data. Untuk mendekripsikan data, penerima menggunakan kunci yang sama dengan kunci yang digunakan pengirim untuk mengenkripsi data. Contoh dari algoritma ini adalah Data Encryption Standard (DES), International Data Encryption Algorithm (IDEA), Advanced Encryption Standard (AES), dan sebagainya. Dalam makalah ini, algoritma AES akan dibahas lebih lanjut.Steganografi adalah seni dan ilmu menulis atau menyembunyikan pesan tersembunyi dengan suatu cara sehingga selain si pengirim dan si penerima, tidak ada seorangpun yang mengetahui atau menyadari bahwa ada suatu pesan rahasia. Sebaliknya, kriptografi menyamarkan arti dari suatu pesan, tapi tidak menyembunyikan bahwa ada suatu pesan. Metode ini termasuk tinta yang tidak tampak, microdots, pengaturan kata, tanda tangan digital, jalur tersembunyi dan komunikasi spektrum lebar. Tujuan dari steganografi adalah merahasiakan atau menyembunyikan keberadaan dari sebuah pesan tersembunyi atau sebuah informasi. Dalam prakteknya kebanyakan diselesaikan dengan membuat perubahan tipis terhadap data digital lain yang isinya tidak akan menarik perhatian dari penyerang potensial, sebagai contoh sebuah gambar yang terlihat tidak berbahaya.Perubahan ini bergantung pada kunci (sama pada kriptografi) dan pesan untuk disembunyikan. Orang yang menerima gambar kemudian dapat menyimpulkan informasi

terselubung dengan cara mengganti kunci yang benar ke dalam algoritma yang digunakan.Kelebihan steganografi daripada kriptografi adalah pesan-pesannya tidak menarik perhatian orang lain. Pesan-pesan berkode dalam kriptografi yang tidak disembunyikan, walaupun tidak dapat dipecahkan, akan menimbulkan kecurigaan. Seringkali, steganografi dan kriptografi digunakan secara bersamaan untuk menjamin keamanan pesan rahasianya.Kebanyakan algoritma steganografi menggunakan sebuah kombinasi dari beberapa teknik pencitraan untuk melakukan sebuah tugas dalam penyelubungan pesan rahasia dalam sebuah selubung file. Sebuah program steganografi dibutuhkan untuk melakukan hal-hal berikut (baik implisit melalui suatu perkiraan maupun eksplisit melalui sebuah perhitungan), menemukan kelebihan bits dalam selubung file yang dapat digunakan untuk menyelubungi pesan rahasia didalamnya, memilih beberapa diantaranya untuk digunakan dalam menyelubungiDengan perkembangan teknologi komputer saat ini, pertukaran informasi dari suatu pihak ke pihak lain sangatlah diperlukan. Informasi yang dipertukarkan itu biasanya tidak ingin diketahui oleh pihak-pihak lain, terutama oleh pihak yang bertentangan dengan pihak yang bertukar informasi ataupun pihak yang baik sengaja maupun tidak sengaja dapat memanfaatkan informasi tersebut. Jika keamanan pertukaran informasi ini tidak dapat dijaga, maka pihak - pihak lain dapat memanfaatkan informasi tanpa izin dari pemilik informasi. Hal tersebut sangat merugikan pihak-pihak yang berhak atas informasi tersebut.Ancaman keamanan terhadap informasi dapat berupa berbagai bentuk. Bentuk ancaman tersebut dapat berupa interupsi, intersepsi, modifikasi, dan fabrikasi. Ancaman interupsi dapat mengganggu ketersediaan data. Data yang ada dapat dihapus sehingga pihak yang membutuhkan informasi tersebut tidak dapat menemukan datanya. Ancaman intersepsi merupakan ancaman terhadap kerahasiaan data. Informasi yang ada disadap dan dipergunakan oleh pihak yang tidak berhak sehingga merugikan pengguna data yang sah. Ancaman modifikasi mengakibatkan kesalahan dalam penerimaan informasi sehingga informasi yang diterima tidak sesuai dengan keinginan penerima maupun pengirimnya. Ancaman fabrikasi merupakan ancaman terhadap integritas karena informasi yang berhasil dicuri oleh pihak yang tidak berhak dipalsukan, lalu dikirimkan kepada penerima seolah-olah berasal dari pengirim yang sah.Untuk mengatasi ancaman-ancaman tersebut, diperlukan suatu cara agar informasi tersebut tidak dapat diketahui oleh pihak lain. Salah satu caranya adalah dengan menggunakan kriptografi. Kriptografi sudah dikenal sejak ribuan tahun yang lalu, Kriptografi terus-menerus dikembangkan hingga saat ini. Pengembangannya dilakukan oleh berbagai pihak dari berbagai negara, Karena banyaknya jumlah algoritma yang digunakan, diperlukanlah standar algoritma sehingga dapat dipergunakan dalam berbagai aplikasi. NIST (National Institute of Standard and Technology) mempublikasikan suatu algoritma pengenkripsian data baru untuk menggantikan algoritma DES (Data Encryption Standard) yang memiliki beberapa kelemahan. Algorima baru ini dinamakan AES (Advanced Encryption Standard) atau Rijndael. Algoritma ini diperoleh melalui kompetisi yang dilakukan pada tahun 1997. Proses seleksi ini amat ketat dan membutuhkan waktu yang cukup lama. Pada akhirnya, pada tanggal 2 Oktober 2000 terpilihlah algoritma Rijndael yang dibuat oleh Rijmen dan Daemen dari Belgia. Algoritma ini tepilih sebagai AES. Meskipun masih baru, algoritma ini sudah dipergunakan pada berbagai aplikasi, salah satunya adalah untuk penyandian password. Penggunaan algoritma ini sudah sering dilihat pada perangkat lunak untuk kompresi data. Dalam perangkat lunak tersebut, salah satu metode yang digunakan untuk mengenkripsi password adalah dengan algoritma AES.Pembentukan kode Huffman dapat dilakukan dengan membuat pohon biner. Sebuah simpul (node) dalam pohon xxxxxxxxxxxxxxxxxx

Teks Rahasia 8192 *byte* Yang Diekstrak dari *Stego* – *Image* Lena Menggunakan *Predictor* MED (h=1)

Kriptografi adalah ilmu sekaligus seni untuk menjaga kerahasiaan pesan dengan cara menyamarkannya menjadi bentuk tersandi yang tidak mempunyai makna. Bentuk tersandi ini hanya dapat dibaca oleh pihak yang berhak membacanya. Pesan yang akan dirahasiakan sebelum disamarkan disebut plaintext, sedangkan pesan setelah disamarkan disebut chipertext. Proses penyamaran plaintext ke chipertext disebut enkripsi, sedangkan pengembalian chiperteks menjadi plainteks semula disebut dekripsi.Kriptografi telah lama digunakan oleh tentara Sparta di Yunani

sekitar tahun 400 SM. Mereka menggunakan alat yang disebut scytale. Alat ini terbuat dari daun papirus yang dililitkan pada batang silinder. Pesan yang akan dikirim ditulis horizontal. Setelah ditulis, daun dilepaskan dari batang kemudian dikirimkan ke penerima. Penerima dapat membaca pesan tersebut setelah melilitkan kembali daun tersebut pada batang silinder dengan ukuran diameter yang sama. Teknik ini dikenal dengan nama transposisi chiper yang merupakan metode enkripsi tertua. Pada zaman Romawi kuno, Julius Caesar juga menggunakan kriptografi untuk mengirimkan pesannya. Pesan yang ia kirimkan ditulis dengan mengganti alfabet dengan alfabet lain dengan kunci tertentu. Sang penerima tentu saja telah diberi tahu kunci tersebut. Cara menyandikannya adalah dengan mengganti semua susunan alfabet dengan alfabet yang posisinya berada setelah alfabet tersebut tergantung kunci. Sebagai contoh, Julius Caesar mengganti huruf a, b, dan c menjadi d, e, dan f. Pada perang dunia kedua, Jerman menggunakan mesin untuk mengrenkripsi pesan yang dikirimkan Hitler ke tentaranya yang bernama mesin enigma. Jerman meyakini kode-kode enkripsi dari mesin tersebut tidak dapat dipecahkan karena memiliki sekitar 15 milyar kemungkinan untuk mendekripsikannya. Kenyataannya sekutu mampu mendekripsikannya sehingga mesin tersebut beberapa kali memgalami perubahan.Fungsi hash sering disebut sebagai fungsi satu arah(one-way function). Fungsi ini mengubah suatu masukan menjadi keluaran, tetapi keluaran tersebut tidak dapat dikembalikan menjadi bentuk semula. Salah satu manfaatnya adalah penggunaan sidik jari (fingerprint). Sidik jari digunakan sebagai identitas pengirim pesan. Fungsi lain adalah untuk kompresi dan message digest. Contoh algoritma fungsi ini adalah MD-5 dan SHA.Pada algoritma ini, digunakan dua buah kunci yang berhubungan yang disebut dengan kunci umum dan kunci pribadi. Kunci umum dapat dipublikasikan sehingga pesan dapat dienkripsikan tetapi tidak dapat didekripsikan dengan kunci tersebut. Kunci pribadi hanya boleh digunakan oleh pihak yang berhak untuk mendekripsikan pesan yang terenkripsi. Algoritma yang menggunakan kunci umum dan publik ini antara lain : Digital Signature Algorithm (DSA), Rivest-Shamir-Adleman (RSA), Diffie-Hellman (DH), dan sebegainya.Algoritma ini menggunakan kunci yang sama untuk mengenkripsi dan mendekripsi data. Untuk mendekripsikan data, penerima menggunakan kunci yang sama dengan kunci yang digunakan pengirim untuk mengenkripsi data. Contoh dari algoritma ini adalah Data Encryption Standard (DES), International Data Encryption Algorithm (IDEA), Advanced Encryption Standard (AES), dan sebagainya. Dalam makalah ini, algoritma AES akan dibahas lebih lanjut.Steganografi adalah seni dan ilmu menulis atau menyembunyikan pesan tersembunyi dengan suatu cara sehingga selain si pengirim dan si penerima, tidak ada seorangpun yang mengetahui atau menyadari bahwa ada suatu pesan rahasia. Sebaliknya, kriptografi menyamarkan arti dari suatu pesan, tapi tidak menyembunyikan bahwa ada suatu pesan. Metode ini termasuk tinta yang tidak tampak, microdots, pengaturan kata, tanda tangan digital, jalur tersembunyi dan komunikasi spektrum lebar. Tujuan dari steganografi adalah merahasiakan atau menyembunyikan keberadaan dari sebuah pesan tersembunyi atau sebuah informasi. Dalam prakteknya kebanyakan diselesaikan dengan membuat perubahan tipis terhadap data digital lain yang isinya tidak akan menarik perhatian dari penyerang potensial, sebagai contoh sebuah gambar yang terlihat tidak berbahaya.Perubahan ini bergantung pada kunci (sama pada kriptografi) dan pesan untuk disembunyikan. Orang yang menerima gambar kemudian dapat menyimpulkan informasi terselubung dengan cara mengganti kunci yang benar ke dalam algoritma yang digunakan.Kelebihan steganografi daripada kriptografi adalah pesan-pesannya tidak menarik perhatian orang lain. Pesan-pesan berkode dalam kriptografi yang tidak disembunyikan, walaupun tidak dapat dipecahkan, akan menimbulkan kecurigaan. Seringkali, steganografi dan kriptografi digunakan secara bersamaan untuk menjamin keamanan pesan rahasianya.Kebanyakan algoritma steganografi menggunakan sebuah kombinasi dari beberapa teknik pencitraan untuk melakukan sebuah tugas dalam penyelubungan pesan rahasia dalam sebuah selubung file. Sebuah program steganografi dibutuhkan untuk melakukan hal-hal berikut (baik implisit melalui suatu perkiraan maupun eksplisit melalui sebuah perhitungan), menemukan kelebihan bits dalam selubung file yang dapat digunakan untuk menyelubungi pesan rahasia didalamnya, memilih beberapa diantaranya untuk digunakan dalam menyelubungiDengan perkembangan teknologi komputer saat ini, pertukaran informasi dari suatu pihak ke pihak lain sangatlah diperlukan. Informasi yang dipertukarkan itu biasanya tidak ingin diketahui oleh pihak-pihak lain, terutama oleh pihak yang bertentangan dengan pihak yang bertukar informasi ataupun pihak yang baik sengaja maupun tidak

sengaja dapat memanfaatkan informasi tersebut. Jika keamanan pertukaran informasi ini tidak dapat dijaga, maka pihak - pihak lain dapat memanfaatkan informasi tanpa izin dari pemilik informasi. Hal tersebut sangat merugikan pihak-pihak yang berhak atas informasi tersebut.Ancaman keamanan terhadap informasi dapat berupa berbagai bentuk. Bentuk ancaman tersebut dapat berupa interupsi, intersepsi, modifikasi, dan fabrikasi. Ancaman interupsi dapat mengganggu ketersediaan data. Data yang ada dapat dihapus sehingga pihak yang membutuhkan informasi tersebut tidak dapat menemukan datanya. Ancaman intersepsi merupakan ancaman terhadap kerahasiaan data. Informasi yang ada disadap dan dipergunakan oleh pihak yang tidak berhak sehingga merugikan pengguna data yang sah. Ancaman modifikasi mengakibatkan kesalahan dalam penerimaan informasi sehingga informasi yang diterima tidak sesuai dengan keinginan penerima maupun pengirimnya. Ancaman fabrikasi merupakan ancaman terhadap integritas karena informasi yang berhasil dicuri oleh pihak yang tidak berhak dipalsukan, lalu dikirimkan kepada penerima seolah-olah berasal dari pengirim yang sah.Untuk mengatasi ancaman-ancaman tersebut, diperlukan suatu cara agar informasi tersebut tidak dapat diketahui oleh pihak lain. Salah satu caranya adalah dengan menggunakan kriptografi. Kriptografi sudah dikenal sejak ribuan tahun yang lalu, Kriptografi terus-menerus dikembangkan hingga saat ini. Pengembangannya dilakukan oleh berbagai pihak dari berbagai negara, Karena banyaknya jumlah algoritma yang digunakan, diperlukanlah standar algoritma sehingga dapat dipergunakan dalam berbagai aplikasi. NIST (National Institute of Standard and Technology) mempublikasikan suatu algoritma pengenkripsian data baru untuk menggantikan algoritma DES (Data Encryption Standard) yang memiliki beberapa kelemahan. Algorima baru ini dinamakan AES (Advanced Encryption Standard) atau Rijndael. Algoritma ini diperoleh melalui kompetisi yang dilakukan pada tahun 1997. Proses seleksi ini amat ketat dan membutuhkan waktu yang cukup lama. Pada akhirnya, pada tanggal 2 Oktober 2000 terpilihlah algoritma Rijndael yang dibuat oleh Rijmen dan Daemen dari Belgia. Algoritma ini tepilih sebagai AES. Meskipun masih baru, algoritma ini sudah dipergunakan pada berbagai aplikasi, salah satunya adalah untuk penyandian password. Penggunaan algoritma ini sudah sering dilihat pada perangkat lunak untuk kompresi data. Dalam perangkat lunak tersebut, salah satu metode yang digunakan untuk mengenkripsi password adalah dengan algoritma AES.Pembentukan kode Huffman dapat dilakukan dengan membuat pohon biner. Sebuah simpul (node) dalam pohon xxxxxxxxxxxxxxxxxx

Teks Rahasia 8192 *byte* Yang Diekstrak dari *Stego – Image* Lena Menggunakan *Predictor* GAP (h=1)

Kriptografi adalah ilmu sekaligus seni untuk menjaga kerahasiaan pesan dengan cara menyamarkannya menjadi bentuk tersandi yang tidak mempunyai makna. Bentuk tersandi ini hanya dapat dibaca oleh pihak yang berhak membacanya. Pesan yang akan dirahasiakan sebelum disamarkan disebut plaintext, sedangkan pesan setelah disamarkan disebut chipertext. Proses penyamaran plaintext ke chipertext disebut enkripsi, sedangkan pengembalian chiperteks menjadi plainteks semula disebut dekripsi.Kriptografi telah lama digunakan oleh tentara Sparta di Yunani sekitar tahun 400 SM. Mereka menggunakan alat yang disebut scytale. Alat ini terbuat dari daun papirus yang dililitkan pada batang silinder. Pesan yang akan dikirim ditulis horizontal. Setelah ditulis, daun dilepaskan dari batang kemudian dikirimkan ke penerima. Penerima dapat membaca pesan tersebut setelah melilitkan kembali daun tersebut pada batang silinder dengan ukuran diameter yang sama. Teknik ini dikenal dengan nama transposisi chiper yang merupakan metode enkripsi tertua. Pada zaman Romawi kuno, Julius Caesar juga menggunakan kriptografi untuk mengirimkan pesannya. Pesan yang ia kirimkan ditulis dengan mengganti alfabet dengan alfabet lain dengan kunci tertentu. Sang penerima tentu saja telah diberi tahu kunci tersebut. Cara menyandikannya adalah dengan mengganti semua susunan alfabet dengan alfabet yang posisinya berada setelah alfabet tersebut tergantung kunci. Sebagai contoh, Julius Caesar mengganti huruf a, b, dan c menjadi d, e, dan f. Pada perang dunia kedua, Jerman menggunakan mesin untuk mengrenkripsi pesan yang dikirimkan Hitler ke tentaranya yang bernama mesin enigma. Jerman meyakini kode-kode enkripsi dari mesin tersebut tidak dapat dipecahkan karena memiliki sekitar 15 milyar kemungkinan untuk mendekripsikannya. Kenyataannya sekutu mampu

mendekripsikannya sehingga mesin tersebut beberapa kali memgalami perubahan.Fungsi hash sering disebut sebagai fungsi satu arah(one-way function). Fungsi ini mengubah suatu masukan menjadi keluaran, tetapi keluaran tersebut tidak dapat dikembalikan menjadi bentuk semula. Salah satu manfaatnya adalah penggunaan sidik jari (fingerprint). Sidik jari digunakan sebagai identitas pengirim pesan. Fungsi lain adalah untuk kompresi dan message digest. Contoh algoritma fungsi ini adalah MD-5 dan SHA.Pada algoritma ini, digunakan dua buah kunci yang berhubungan yang disebut dengan kunci umum dan kunci pribadi. Kunci umum dapat dipublikasikan sehingga pesan dapat dienkripsikan tetapi tidak dapat didekripsikan dengan kunci tersebut. Kunci pribadi hanya boleh digunakan oleh pihak yang berhak untuk mendekripsikan pesan yang terenkripsi. Algoritma yang menggunakan kunci umum dan publik ini antara lain : Digital Signature Algorithm (DSA), Rivest-Shamir-Adleman (RSA), Diffie-Hellman (DH), dan sebegainya.Algoritma ini menggunakan kunci yang sama untuk mengenkripsi dan mendekripsi data. Untuk mendekripsikan data, penerima menggunakan kunci yang sama dengan kunci yang digunakan pengirim untuk mengenkripsi data. Contoh dari algoritma ini adalah Data Encryption Standard (DES), International Data Encryption Algorithm (IDEA), Advanced Encryption Standard (AES), dan sebagainya. Dalam makalah ini, algoritma AES akan dibahas lebih lanjut.Steganografi adalah seni dan ilmu menulis atau menyembunyikan pesan tersembunyi dengan suatu cara sehingga selain si pengirim dan si penerima, tidak ada seorangpun yang mengetahui atau menyadari bahwa ada suatu pesan rahasia. Sebaliknya, kriptografi menyamarkan arti dari suatu pesan, tapi tidak menyembunyikan bahwa ada suatu pesan. Metode ini termasuk tinta yang tidak tampak, microdots, pengaturan kata, tanda tangan digital, jalur tersembunyi dan komunikasi spektrum lebar. Tujuan dari steganografi adalah merahasiakan atau menyembunyikan keberadaan dari sebuah pesan tersembunyi atau sebuah informasi. Dalam prakteknya kebanyakan diselesaikan dengan membuat perubahan tipis terhadap data digital lain yang isinya tidak akan menarik perhatian dari penyerang potensial, sebagai contoh sebuah gambar yang terlihat tidak berbahaya.Perubahan ini bergantung pada kunci (sama pada kriptografi) dan pesan untuk disembunyikan. Orang yang menerima gambar kemudian dapat menyimpulkan informasi terselubung dengan cara mengganti kunci yang benar ke dalam algoritma yang digunakan.Kelebihan steganografi daripada kriptografi adalah pesan-pesannya tidak menarik perhatian orang lain. Pesan-pesan berkode dalam kriptografi yang tidak disembunyikan, walaupun tidak dapat dipecahkan, akan menimbulkan kecurigaan. Seringkali, steganografi dan kriptografi digunakan secara bersamaan untuk menjamin keamanan pesan rahasianya.Kebanyakan algoritma steganografi menggunakan sebuah kombinasi dari beberapa teknik pencitraan untuk melakukan sebuah tugas dalam penyelubungan pesan rahasia dalam sebuah selubung file. Sebuah program steganografi dibutuhkan untuk melakukan hal-hal berikut (baik implisit melalui suatu perkiraan maupun eksplisit melalui sebuah perhitungan), menemukan kelebihan bits dalam selubung file yang dapat digunakan untuk menyelubungi pesan rahasia didalamnya, memilih beberapa diantaranya untuk digunakan dalam menyelubungiDengan perkembangan teknologi komputer saat ini, pertukaran informasi dari suatu pihak ke pihak lain sangatlah diperlukan. Informasi yang dipertukarkan itu biasanya tidak ingin diketahui oleh pihak-pihak lain, terutama oleh pihak yang bertentangan dengan pihak yang bertukar informasi ataupun pihak yang baik sengaja maupun tidak sengaja dapat memanfaatkan informasi tersebut. Jika keamanan pertukaran informasi ini tidak dapat dijaga, maka pihak - pihak lain dapat memanfaatkan informasi tanpa izin dari pemilik informasi. Hal tersebut sangat merugikan pihak-pihak yang berhak atas informasi tersebut.Ancaman keamanan terhadap informasi dapat berupa berbagai bentuk. Bentuk ancaman tersebut dapat berupa interupsi, intersepsi, modifikasi, dan fabrikasi. Ancaman interupsi dapat mengganggu ketersediaan data. Data yang ada dapat dihapus sehingga pihak yang membutuhkan informasi tersebut tidak dapat menemukan datanya. Ancaman intersepsi merupakan ancaman terhadap kerahasiaan data. Informasi yang ada disadap dan dipergunakan oleh pihak yang tidak berhak sehingga merugikan pengguna data yang sah. Ancaman modifikasi mengakibatkan kesalahan dalam penerimaan informasi sehingga informasi yang diterima tidak sesuai dengan keinginan penerima maupun pengirimnya. Ancaman fabrikasi merupakan ancaman terhadap integritas karena informasi yang berhasil dicuri oleh pihak yang tidak berhak dipalsukan, lalu dikirimkan kepada penerima seolah-olah berasal dari pengirim yang sah.Untuk mengatasi ancaman-ancaman tersebut, diperlukan suatu cara agar informasi tersebut tidak dapat diketahui

oleh pihak lain. Salah satu caranya adalah dengan menggunakan kriptografi. Kriptografi sudah dikenal sejak ribuan tahun yang lalu, Kriptografi terus-menerus dikembangkan hingga saat ini. Pengembangannya dilakukan oleh berbagai pihak dari berbagai negara, Karena banyaknya jumlah algoritma yang digunakan, diperlukanlah standar algoritma sehingga dapat dipergunakan dalam berbagai aplikasi. NIST (National Institute of Standard and Technology) mempublikasikan suatu algoritma pengenkripsian data baru untuk menggantikan algoritma DES (Data Encryption Standard) yang memiliki beberapa kelemahan. Algorima baru ini dinamakan AES (Advanced Encryption Standard) atau Rijndael. Algoritma ini diperoleh melalui kompetisi yang dilakukan pada tahun 1997. Proses seleksi ini amat ketat dan membutuhkan waktu yang cukup lama. Pada akhirnya, pada tanggal 2 Oktober 2000 terpilihlah algoritma Rijndael yang dibuat oleh Rijmen dan Daemen dari Belgia. Algoritma ini tepilih sebagai AES. Meskipun masih baru, algoritma ini sudah dipergunakan pada berbagai aplikasi, salah satunya adalah untuk penyandian password. Penggunaan algoritma ini sudah sering dilihat pada perangkat lunak untuk kompresi data. Dalam perangkat lunak tersebut, salah satu metode yang digunakan untuk mengenkripsi password adalah dengan algoritma AES.Pembentukan kode Huffman dapat dilakukan dengan membuat pohon biner. Sebuah simpul (node) dalam pohon xxxxxxxxxxxxxxxxxx

Teks Rahasia 16384 *byte* Asli Yang Akan Disispkan Pada Setiap *Host – Image*

Kriptografi adalah ilmu sekaligus seni untuk menjaga kerahasiaan pesan dengan cara menyamarkannya menjadi bentuk tersandi yang tidak mempunyai makna. Bentuk tersandi ini hanya dapat dibaca oleh pihak yang berhak membacanya. Pesan yang akan dirahasiakan sebelum disamarkan disebut plaintext, sedangkan pesan setelah disamarkan disebut chipertext. Proses penyamaran plaintext ke chipertext disebut enkripsi, sedangkan pengembalian chiperteks menjadi plainteks semula disebut dekripsi.Kriptografi telah lama digunakan oleh tentara Sparta di Yunani sekitar tahun 400 SM. Mereka menggunakan alat yang disebut scytale. Alat ini terbuat dari daun papirus yang dililitkan pada batang silinder. Pesan yang akan dikirim ditulis horizontal. Setelah ditulis, daun dilepaskan dari batang kemudian dikirimkan ke penerima. Penerima dapat membaca pesan tersebut setelah melilitkan kembali daun tersebut pada batang silinder dengan ukuran diameter yang sama. Teknik ini dikenal dengan nama transposisi chiper yang merupakan metode enkripsi tertua. Pada zaman Romawi kuno, Julius Caesar juga menggunakan kriptografi untuk mengirimkan pesannya. Pesan yang ia kirimkan ditulis dengan mengganti alfabet dengan alfabet lain dengan kunci tertentu. Sang penerima tentu saja telah diberi tahu kunci tersebut. Cara menyandikannya adalah dengan mengganti semua susunan alfabet dengan alfabet yang posisinya berada setelah alfabet tersebut tergantung kunci. Sebagai contoh, Julius Caesar mengganti huruf a, b, dan c menjadi d, e, dan f. Pada perang dunia kedua, Jerman menggunakan mesin untuk mengrenkripsi pesan yang dikirimkan Hitler ke tentaranya yang bernama mesin enigma. Jerman meyakini kode-kode enkripsi dari mesin tersebut tidak dapat dipecahkan karena memiliki sekitar 15 milyar kemungkinan untuk mendekripsikannya. Kenyataannya sekutu mampu mendekripsikannya sehingga mesin tersebut beberapa kali memgalami perubahan.Fungsi hash sering disebut sebagai fungsi satu arah(one-way function). Fungsi ini mengubah suatu masukan menjadi keluaran, tetapi keluaran tersebut tidak dapat dikembalikan menjadi bentuk semula. Salah satu manfaatnya adalah penggunaan sidik jari (fingerprint). Sidik jari digunakan sebagai identitas pengirim pesan. Fungsi lain adalah untuk kompresi dan message digest. Contoh algoritma fungsi ini adalah MD-5 dan SHA.Pada algoritma ini, digunakan dua buah kunci yang berhubungan yang disebut dengan kunci umum dan kunci pribadi. Kunci umum dapat dipublikasikan sehingga pesan dapat dienkripsikan tetapi tidak dapat didekripsikan dengan kunci tersebut. Kunci pribadi hanya boleh digunakan oleh pihak yang berhak untuk mendekripsikan pesan yang terenkripsi. Algoritma yang menggunakan kunci umum dan publik ini antara lain : Digital Signature Algorithm (DSA), Rivest-Shamir-Adleman (RSA), Diffie-Hellman (DH), dan sebegainya.Algoritma ini menggunakan kunci yang sama untuk mengenkripsi dan mendekripsi data. Untuk mendekripsikan data, penerima menggunakan kunci yang sama dengan kunci yang digunakan pengirim untuk mengenkripsi data. Contoh dari algoritma ini adalah Data Encryption Standard (DES), International Data Encryption Algorithm (IDEA), Advanced Encryption Standard (AES), dan

sebagainya. Dalam makalah ini, algoritma AES akan dibahas lebih lanjut.Steganografi adalah seni dan ilmu menulis atau menyembunyikan pesan tersembunyi dengan suatu cara sehingga selain si pengirim dan si penerima, tidak ada seorangpun yang mengetahui atau menyadari bahwa ada suatu pesan rahasia. Sebaliknya, kriptografi menyamarkan arti dari suatu pesan, tapi tidak menyembunyikan bahwa ada suatu pesan. Metode ini termasuk tinta yang tidak tampak, microdots, pengaturan kata, tanda tangan digital, jalur tersembunyi dan komunikasi spektrum lebar. Tujuan dari steganografi adalah merahasiakan atau menyembunyikan keberadaan dari sebuah pesan tersembunyi atau sebuah informasi. Dalam prakteknya kebanyakan diselesaikan dengan membuat perubahan tipis terhadap data digital lain yang isinya tidak akan menarik perhatian dari penyerang potensial, sebagai contoh sebuah gambar yang terlihat tidak berbahaya.Perubahan ini bergantung pada kunci (sama pada kriptografi) dan pesan untuk disembunyikan. Orang yang menerima gambar kemudian dapat menyimpulkan informasi terselubung dengan cara mengganti kunci yang benar ke dalam algoritma yang digunakan.Kelebihan steganografi daripada kriptografi adalah pesan-pesannya tidak menarik perhatian orang lain. Pesan-pesan berkode dalam kriptografi yang tidak disembunyikan, walaupun tidak dapat dipecahkan, akan menimbulkan kecurigaan. Seringkali, steganografi dan kriptografi digunakan secara bersamaan untuk menjamin keamanan pesan rahasianya.Kebanyakan algoritma steganografi menggunakan sebuah kombinasi dari beberapa teknik pencitraan untuk melakukan sebuah tugas dalam penyelubungan pesan rahasia dalam sebuah selubung file. Sebuah program steganografi dibutuhkan untuk melakukan hal-hal berikut (baik implisit melalui suatu perkiraan maupun eksplisit melalui sebuah perhitungan), menemukan kelebihan bits dalam selubung file yang dapat digunakan untuk menyelubungi pesan rahasia didalamnya, memilih beberapa diantaranya untuk digunakan dalam menyelubungiDengan perkembangan teknologi komputer saat ini, pertukaran informasi dari suatu pihak ke pihak lain sangatlah diperlukan. Informasi yang dipertukarkan itu biasanya tidak ingin diketahui oleh pihak-pihak lain, terutama oleh pihak yang bertentangan dengan pihak yang bertukar informasi ataupun pihak yang baik sengaja maupun tidak sengaja dapat memanfaatkan informasi tersebut. Jika keamanan pertukaran informasi ini tidak dapat dijaga, maka pihak - pihak lain dapat memanfaatkan informasi tanpa izin dari pemilik informasi. Hal tersebut sangat merugikan pihak-pihak yang berhak atas informasi tersebut.Ancaman keamanan terhadap informasi dapat berupa berbagai bentuk. Bentuk ancaman tersebut dapat berupa interupsi, intersepsi, modifikasi, dan fabrikasi. Ancaman interupsi dapat mengganggu ketersediaan data. Data yang ada dapat dihapus sehingga pihak yang membutuhkan informasi tersebut tidak dapat menemukan datanya. Ancaman intersepsi merupakan ancaman terhadap kerahasiaan data. Informasi yang ada disadap dan dipergunakan oleh pihak yang tidak berhak sehingga merugikan pengguna data yang sah. Ancaman modifikasi mengakibatkan kesalahan dalam penerimaan informasi sehingga informasi yang diterima tidak sesuai dengan keinginan penerima maupun pengirimnya. Ancaman fabrikasi merupakan ancaman terhadap integritas karena informasi yang berhasil dicuri oleh pihak yang tidak berhak dipalsukan, lalu dikirimkan kepada penerima seolah-olah berasal dari pengirim yang sah.Untuk mengatasi ancaman-ancaman tersebut, diperlukan suatu cara agar informasi tersebut tidak dapat diketahui oleh pihak lain. Salah satu caranya adalah dengan menggunakan kriptografi. Kriptografi sudah dikenal sejak ribuan tahun yang lalu, Kriptografi terus-menerus dikembangkan hingga saat ini. Pengembangannya dilakukan oleh berbagai pihak dari berbagai negara, Karena banyaknya jumlah algoritma yang digunakan, diperlukanlah standar algoritma sehingga dapat dipergunakan dalam berbagai aplikasi. NIST (National Institute of Standard and Technology) mempublikasikan suatu algoritma pengenkripsian data baru untuk menggantikan algoritma DES (Data Encryption Standard) yang memiliki beberapa kelemahan. Algorima baru ini dinamakan AES (Advanced Encryption Standard) atau Rijndael. Algoritma ini diperoleh melalui kompetisi yang dilakukan pada tahun 1997. Proses seleksi ini amat ketat dan membutuhkan waktu yang cukup lama. Pada akhirnya, pada tanggal 2 Oktober 2000 terpilihlah algoritma Rijndael yang dibuat oleh Rijmen dan Daemen dari Belgia. Algoritma ini tepilih sebagai AES. Meskipun masih baru, algoritma ini sudah dipergunakan pada berbagai aplikasi, salah satunya adalah untuk penyandian password. Penggunaan algoritma ini sudah sering dilihat pada perangkat lunak untuk kompresi data. Dalam perangkat lunak tersebut, salah satu metode yang digunakan untuk mengenkripsi password adalah dengan algoritma AES.Pembentukan kode Huffman dapat dilakukan dengan membuat pohon

biner. Sebuah simpul (node) dalam pohon xxxxxxxxxxxxxxxxxxKriptografi adalah ilmu sekaligus seni untuk menjaga kerahasiaan pesan dengan cara menyamarkannya menjadi bentuk tersandi yang tidak mempunyai makna. Bentuk tersandi ini hanya dapat dibaca oleh pihak yang berhak membacanya. Pesan yang akan dirahasiakan sebelum disamarkan disebut plaintext, sedangkan pesan setelah disamarkan disebut chipertext. Proses penyamaran plaintext ke chipertext disebut enkripsi, sedangkan pengembalian chiperteks menjadi plainteks semula disebut dekripsi.Kriptografi telah lama digunakan oleh tentara Sparta di Yunani sekitar tahun 400 SM. Mereka menggunakan alat yang disebut scytale. Alat ini terbuat dari daun papirus yang dililitkan pada batang silinder. Pesan yang akan dikirim ditulis horizontal. Setelah ditulis, daun dilepaskan dari batang kemudian dikirimkan ke penerima. Penerima dapat membaca pesan tersebut setelah melilitkan kembali daun tersebut pada batang silinder dengan ukuran diameter yang sama. Teknik ini dikenal dengan nama transposisi chiper yang merupakan metode enkripsi tertua. Pada zaman Romawi kuno, Julius Caesar juga menggunakan kriptografi untuk mengirimkan pesannya. Pesan yang ia kirimkan ditulis dengan mengganti alfabet dengan alfabet lain dengan kunci tertentu. Sang penerima tentu saja telah diberi tahu kunci tersebut. Cara menyandikannya adalah dengan mengganti semua susunan alfabet dengan alfabet yang posisinya berada setelah alfabet tersebut tergantung kunci. Sebagai contoh, Julius Caesar mengganti huruf a, b, dan c menjadi d, e, dan f. Pada perang dunia kedua, Jerman menggunakan mesin untuk mengrenkripsi pesan yang dikirimkan Hitler ke tentaranya yang bernama mesin enigma. Jerman meyakini kode-kode enkripsi dari mesin tersebut tidak dapat dipecahkan karena memiliki sekitar 15 milyar kemungkinan untuk mendekripsikannya. Kenyataannya sekutu mampu mendekripsikannya sehingga mesin tersebut beberapa kali memgalami perubahan.Fungsi hash sering disebut sebagai fungsi satu arah(one-way function). Fungsi ini mengubah suatu masukan menjadi keluaran, tetapi keluaran tersebut tidak dapat dikembalikan menjadi bentuk semula. Salah satu manfaatnya adalah penggunaan sidik jari (fingerprint). Sidik jari digunakan sebagai identitas pengirim pesan. Fungsi lain adalah untuk kompresi dan message digest. Contoh algoritma fungsi ini adalah MD-5 dan SHA.Pada algoritma ini, digunakan dua buah kunci yang berhubungan yang disebut dengan kunci umum dan kunci pribadi. Kunci umum dapat dipublikasikan sehingga pesan dapat dienkripsikan tetapi tidak dapat didekripsikan dengan kunci tersebut. Kunci pribadi hanya boleh digunakan oleh pihak yang berhak untuk mendekripsikan pesan yang terenkripsi. Algoritma yang menggunakan kunci umum dan publik ini antara lain : Digital Signature Algorithm (DSA), Rivest-Shamir-Adleman (RSA), Diffie-Hellman (DH), dan sebegainya.Algoritma ini menggunakan kunci yang sama untuk mengenkripsi dan mendekripsi data. Untuk mendekripsikan data, penerima menggunakan kunci yang sama dengan kunci yang digunakan pengirim untuk mengenkripsi data. Contoh dari algoritma ini adalah Data Encryption Standard (DES), International Data Encryption Algorithm (IDEA), Advanced Encryption Standard (AES), dan sebagainya. Dalam makalah ini, algoritma AES akan dibahas lebih lanjut.Steganografi adalah seni dan ilmu menulis atau menyembunyikan pesan tersembunyi dengan suatu cara sehingga selain si pengirim dan si penerima, tidak ada seorangpun yang mengetahui atau menyadari bahwa ada suatu pesan rahasia. Sebaliknya, kriptografi menyamarkan arti dari suatu pesan, tapi tidak menyembunyikan bahwa ada suatu pesan. Metode ini termasuk tinta yang tidak tampak, microdots, pengaturan kata, tanda tangan digital, jalur tersembunyi dan komunikasi spektrum lebar. Tujuan dari steganografi adalah merahasiakan atau menyembunyikan keberadaan dari sebuah pesan tersembunyi atau sebuah informasi. Dalam prakteknya kebanyakan diselesaikan dengan membuat perubahan tipis terhadap data digital lain yang isinya tidak akan menarik perhatian dari penyerang potensial, sebagai contoh sebuah gambar yang terlihat tidak berbahaya.Perubahan ini bergantung pada kunci (sama pada kriptografi) dan pesan untuk disembunyikan. Orang yang menerima gambar kemudian dapat menyimpulkan informasi terselubung dengan cara mengganti kunci yang benar ke dalam algoritma yang digunakan.Kelebihan steganografi daripada kriptografi adalah pesan-pesannya tidak menarik perhatian orang lain. Pesan-pesan berkode dalam kriptografi yang tidak disembunyikan, walaupun tidak dapat dipecahkan, akan menimbulkan kecurigaan. Seringkali, steganografi dan kriptografi digunakan secara bersamaan untuk menjamin keamanan pesan rahasianya.Kebanyakan algoritma steganografi menggunakan sebuah kombinasi dari beberapa teknik pencitraan untuk melakukan sebuah tugas dalam penyelubungan pesan rahasia dalam sebuah selubung file. Sebuah program steganografi dibutuhkan untuk melakukan hal-hal berikut (baik implisit melalui suatu perkiraan

maupun eksplisit melalui sebuah perhitungan), menemukan kelebihan bits dalam selubung file yang dapat digunakan untuk menyelubungi pesan rahasia didalamnya, memilih beberapa diantaranya untuk digunakan dalam menyelubungiDengan perkembangan teknologi komputer saat ini, pertukaran informasi dari suatu pihak ke pihak lain sangatlah diperlukan. Informasi yang dipertukarkan itu biasanya tidak ingin diketahui oleh pihak-pihak lain, terutama oleh pihak yang bertentangan dengan pihak yang bertukar informasi ataupun pihak yang baik sengaja maupun tidak sengaja dapat memanfaatkan informasi tersebut. Jika keamanan pertukaran informasi ini tidak dapat dijaga, maka pihak - pihak lain dapat memanfaatkan informasi tanpa izin dari pemilik informasi. Hal tersebut sangat merugikan pihak-pihak yang berhak atas informasi tersebut.Ancaman keamanan terhadap informasi dapat berupa berbagai bentuk. Bentuk ancaman tersebut dapat berupa interupsi, intersepsi, modifikasi, dan fabrikasi. Ancaman interupsi dapat mengganggu ketersediaan data. Data yang ada dapat dihapus sehingga pihak yang membutuhkan informasi tersebut tidak dapat menemukan datanya. Ancaman intersepsi merupakan ancaman terhadap kerahasiaan data. Informasi yang ada disadap dan dipergunakan oleh pihak yang tidak berhak sehingga merugikan pengguna data yang sah. Ancaman modifikasi mengakibatkan kesalahan dalam penerimaan informasi sehingga informasi yang diterima tidak sesuai dengan keinginan penerima maupun pengirimnya. Ancaman fabrikasi merupakan ancaman terhadap integritas karena informasi yang berhasil dicuri oleh pihak yang tidak berhak dipalsukan, lalu dikirimkan kepada penerima seolah-olah berasal dari pengirim yang sah.Untuk mengatasi ancaman-ancaman tersebut, diperlukan suatu cara agar informasi tersebut tidak dapat diketahui oleh pihak lain. Salah satu caranya adalah dengan menggunakan kriptografi. Kriptografi sudah dikenal sejak ribuan tahun yang lalu, Kriptografi terus-menerus dikembangkan hingga saat ini. Pengembangannya dilakukan oleh berbagai pihak dari berbagai negara, Karena banyaknya jumlah algoritma yang digunakan, diperlukanlah standar algoritma sehingga dapat dipergunakan dalam berbagai aplikasi. NIST (National Institute of Standard and Technology) mempublikasikan suatu algoritma pengenkripsian data baru untuk menggantikan algoritma DES (Data Encryption Standard) yang memiliki beberapa kelemahan. Algorima baru ini dinamakan AES (Advanced Encryption Standard) atau Rijndael. Algoritma ini diperoleh melalui kompetisi yang dilakukan pada tahun 1997. Proses seleksi ini amat ketat dan membutuhkan waktu yang cukup lama. Pada akhirnya, pada tanggal 2 Oktober 2000 terpilihlah algoritma Rijndael yang dibuat oleh Rijmen dan Daemen dari Belgia. Algoritma ini tepilih sebagai AES. Meskipun masih baru, algoritma ini sudah dipergunakan pada berbagai aplikasi, salah satunya adalah untuk penyandian password. Penggunaan algoritma ini sudah sering dilihat pada perangkat lunak untuk kompresi data. Dalam perangkat lunak tersebut, salah satu metode yang digunakan untuk mengenkripsi password adalah dengan algoritma AES.Pembentukan kode Huffman dapat dilakukan dengan membuat pohon biner. Sebuah simpul (node) dalam pohon xxxxxxxxxxxxxxxxxx

Teks Rahasia 16384 *byte* Yang Diekstrak dari *Stego* – *Image* Lena Menggunakan *Predictor* MED (h=2)

Kriptografi adalah ilmu sekaligus seni untuk menjaga kerahasiaan pesan dengan cara menyamarkannya menjadi bentuk tersandi yang tidak mempunyai makna. Bentuk tersandi ini hanya dapat dibaca oleh pihak yang berhak membacanya. Pesan yang akan dirahasiakan sebelum disamarkan disebut plaintext, sedangkan pesan setelah disamarkan disebut chipertext. Proses penyamaran plaintext ke chipertext disebut enkripsi, sedangkan pengembalian chiperteks menjadi plainteks semula disebut dekripsi.Kriptografi telah lama digunakan oleh tentara Sparta di Yunani sekitar tahun 400 SM. Mereka menggunakan alat yang disebut scytale. Alat ini terbuat dari daun papirus yang dililitkan pada batang silinder. Pesan yang akan dikirim ditulis horizontal. Setelah ditulis, daun dilepaskan dari batang kemudian dikirimkan ke penerima. Penerima dapat membaca pesan tersebut setelah melilitkan kembali daun tersebut pada batang silinder dengan ukuran diameter yang sama. Teknik ini dikenal dengan nama transposisi chiper yang merupakan metode enkripsi tertua. Pada zaman Romawi kuno, Julius Caesar juga menggunakan kriptografi untuk mengirimkan pesannya. Pesan yang ia kirimkan ditulis dengan mengganti alfabet dengan alfabet lain dengan kunci tertentu. Sang penerima tentu saja telah diberi tahu kunci tersebut. Cara

menyandikannya adalah dengan mengganti semua susunan alfabet dengan alfabet yang posisinya berada setelah alfabet tersebut tergantung kunci. Sebagai contoh, Julius Caesar mengganti huruf a, b, dan c menjadi d, e, dan f. Pada perang dunia kedua, Jerman menggunakan mesin untuk mengrenkripsi pesan yang dikirimkan Hitler ke tentaranya yang bernama mesin enigma. Jerman meyakini kode-kode enkripsi dari mesin tersebut tidak dapat dipecahkan karena memiliki sekitar 15 milyar kemungkinan untuk mendekripsikannya. Kenyataannya sekutu mampu mendekripsikannya sehingga mesin tersebut beberapa kali memgalami perubahan.Fungsi hash sering disebut sebagai fungsi satu arah(one-way function). Fungsi ini mengubah suatu masukan menjadi keluaran, tetapi keluaran tersebut tidak dapat dikembalikan menjadi bentuk semula. Salah satu manfaatnya adalah penggunaan sidik jari (fingerprint). Sidik jari digunakan sebagai identitas pengirim pesan. Fungsi lain adalah untuk kompresi dan message digest. Contoh algoritma fungsi ini adalah MD-5 dan SHA.Pada algoritma ini, digunakan dua buah kunci yang berhubungan yang disebut dengan kunci umum dan kunci pribadi. Kunci umum dapat dipublikasikan sehingga pesan dapat dienkripsikan tetapi tidak dapat didekripsikan dengan kunci tersebut. Kunci pribadi hanya boleh digunakan oleh pihak yang berhak untuk mendekripsikan pesan yang terenkripsi. Algoritma yang menggunakan kunci umum dan publik ini antara lain : Digital Signature Algorithm (DSA), Rivest-Shamir-Adleman (RSA), Diffie-Hellman (DH), dan sebegainya.Algoritma ini menggunakan kunci yang sama untuk mengenkripsi dan mendekripsi data. Untuk mendekripsikan data, penerima menggunakan kunci yang sama dengan kunci yang digunakan pengirim untuk mengenkripsi data. Contoh dari algoritma ini adalah Data Encryption Standard (DES), International Data Encryption Algorithm (IDEA), Advanced Encryption Standard (AES), dan sebagainya. Dalam makalah ini, algoritma AES akan dibahas lebih lanjut.Steganografi adalah seni dan ilmu menulis atau menyembunyikan pesan tersembunyi dengan suatu cara sehingga selain si pengirim dan si penerima, tidak ada seorangpun yang mengetahui atau menyadari bahwa ada suatu pesan rahasia. Sebaliknya, kriptografi menyamarkan arti dari suatu pesan, tapi tidak menyembunyikan bahwa ada suatu pesan. Metode ini termasuk tinta yang tidak tampak, microdots, pengaturan kata, tanda tangan digital, jalur tersembunyi dan komunikasi spektrum lebar. Tujuan dari steganografi adalah merahasiakan atau menyembunyikan keberadaan dari sebuah pesan tersembunyi atau sebuah informasi. Dalam prakteknya kebanyakan diselesaikan dengan membuat perubahan tipis terhadap data digital lain yang isinya tidak akan menarik perhatian dari penyerang potensial, sebagai contoh sebuah gambar yang terlihat tidak berbahaya.Perubahan ini bergantung pada kunci (sama pada kriptografi) dan pesan untuk disembunyikan. Orang yang menerima gambar kemudian dapat menyimpulkan informasi terselubung dengan cara mengganti kunci yang benar ke dalam algoritma yang digunakan.Kelebihan steganografi daripada kriptografi adalah pesan-pesannya tidak menarik perhatian orang lain. Pesan-pesan berkode dalam kriptografi yang tidak disembunyikan, walaupun tidak dapat dipecahkan, akan menimbulkan kecurigaan. Seringkali, steganografi dan kriptografi digunakan secara bersamaan untuk menjamin keamanan pesan rahasianya.Kebanyakan algoritma steganografi menggunakan sebuah kombinasi dari beberapa teknik pencitraan untuk melakukan sebuah tugas dalam penyelubungan pesan rahasia dalam sebuah selubung file. Sebuah program steganografi dibutuhkan untuk melakukan hal-hal berikut (baik implisit melalui suatu perkiraan maupun eksplisit melalui sebuah perhitungan), menemukan kelebihan bits dalam selubung file yang dapat digunakan untuk menyelubungi pesan rahasia didalamnya, memilih beberapa diantaranya untuk digunakan dalam menyelubungiDengan perkembangan teknologi komputer saat ini, pertukaran informasi dari suatu pihak ke pihak lain sangatlah diperlukan. Informasi yang dipertukarkan itu biasanya tidak ingin diketahui oleh pihak-pihak lain, terutama oleh pihak yang bertentangan dengan pihak yang bertukar informasi ataupun pihak yang baik sengaja maupun tidak sengaja dapat memanfaatkan informasi tersebut. Jika keamanan pertukaran informasi ini tidak dapat dijaga, maka pihak - pihak lain dapat memanfaatkan informasi tanpa izin dari pemilik informasi. Hal tersebut sangat merugikan pihak-pihak yang berhak atas informasi tersebut.Ancaman keamanan terhadap informasi dapat berupa berbagai bentuk. Bentuk ancaman tersebut dapat berupa interupsi, intersepsi, modifikasi, dan fabrikasi. Ancaman interupsi dapat mengganggu ketersediaan data. Data yang ada dapat dihapus sehingga pihak yang membutuhkan informasi tersebut tidak dapat menemukan datanya. Ancaman intersepsi merupakan ancaman terhadap kerahasiaan data. Informasi yang ada disadap dan dipergunakan oleh pihak yang tidak

berhak sehingga merugikan pengguna data yang sah. Ancaman modifikasi mengakibatkan kesalahan dalam penerimaan informasi sehingga informasi yang diterima tidak sesuai dengan keinginan penerima maupun pengirimnya. Ancaman fabrikasi merupakan ancaman terhadap integritas karena informasi yang berhasil dicuri oleh pihak yang tidak berhak dipalsukan, lalu dikirimkan kepada penerima seolah-olah berasal dari pengirim yang sah.Untuk mengatasi ancaman-ancaman tersebut, diperlukan suatu cara agar informasi tersebut tidak dapat diketahui oleh pihak lain. Salah satu caranya adalah dengan menggunakan kriptografi. Kriptografi sudah dikenal sejak ribuan tahun yang lalu, Kriptografi terus-menerus dikembangkan hingga saat ini. Pengembangannya dilakukan oleh berbagai pihak dari berbagai negara, Karena banyaknya jumlah algoritma yang digunakan, diperlukanlah standar algoritma sehingga dapat dipergunakan dalam berbagai aplikasi. NIST (National Institute of Standard and Technology) mempublikasikan suatu algoritma pengenkripsian data baru untuk menggantikan algoritma DES (Data Encryption Standard) yang memiliki beberapa kelemahan. Algorima baru ini dinamakan AES (Advanced Encryption Standard) atau Rijndael. Algoritma ini diperoleh melalui kompetisi yang dilakukan pada tahun 1997. Proses seleksi ini amat ketat dan membutuhkan waktu yang cukup lama. Pada akhirnya, pada tanggal 2 Oktober 2000 terpilihlah algoritma Rijndael yang dibuat oleh Rijmen dan Daemen dari Belgia. Algoritma ini tepilih sebagai AES. Meskipun masih baru, algoritma ini sudah dipergunakan pada berbagai aplikasi, salah satunya adalah untuk penyandian password. Penggunaan algoritma ini sudah sering dilihat pada perangkat lunak untuk kompresi data. Dalam perangkat lunak tersebut, salah satu metode yang digunakan untuk mengenkripsi password adalah dengan algoritma AES.Pembentukan kode Huffman dapat dilakukan dengan membuat pohon biner. Sebuah simpul (node) dalam pohon xxxxxxxxxxxxxxxxxxKriptografi adalah ilmu sekaligus seni untuk menjaga kerahasiaan pesan dengan cara menyamarkannya menjadi bentuk tersandi yang tidak mempunyai makna. Bentuk tersandi ini hanya dapat dibaca oleh pihak yang berhak membacanya. Pesan yang akan dirahasiakan sebelum disamarkan disebut plaintext, sedangkan pesan setelah disamarkan disebut chipertext. Proses penyamaran plaintext ke chipertext disebut enkripsi, sedangkan pengembalian chiperteks menjadi plainteks semula disebut dekripsi.Kriptografi telah lama digunakan oleh tentara Sparta di Yunani sekitar tahun 400 SM. Mereka menggunakan alat yang disebut scytale. Alat ini terbuat dari daun papirus yang dililitkan pada batang silinder. Pesan yang akan dikirim ditulis horizontal. Setelah ditulis, daun dilepaskan dari batang kemudian dikirimkan ke penerima. Penerima dapat membaca pesan tersebut setelah melilitkan kembali daun tersebut pada batang silinder dengan ukuran diameter yang sama. Teknik ini dikenal dengan nama transposisi chiper yang merupakan metode enkripsi tertua. Pada zaman Romawi kuno, Julius Caesar juga menggunakan kriptografi untuk mengirimkan pesannya. Pesan yang ia kirimkan ditulis dengan mengganti alfabet dengan alfabet lain dengan kunci tertentu. Sang penerima tentu saja telah diberi tahu kunci tersebut. Cara menyandikannya adalah dengan mengganti semua susunan alfabet dengan alfabet yang posisinya berada setelah alfabet tersebut tergantung kunci. Sebagai contoh, Julius Caesar mengganti huruf a, b, dan c menjadi d, e, dan f. Pada perang dunia kedua, Jerman menggunakan mesin untuk mengrenkripsi pesan yang dikirimkan Hitler ke tentaranya yang bernama mesin enigma. Jerman meyakini kode-kode enkripsi dari mesin tersebut tidak dapat dipecahkan karena memiliki sekitar 15 milyar kemungkinan untuk mendekripsikannya. Kenyataannya sekutu mampu mendekripsikannya sehingga mesin tersebut beberapa kali memgalami perubahan.Fungsi hash sering disebut sebagai fungsi satu arah(one-way function). Fungsi ini mengubah suatu masukan menjadi keluaran, tetapi keluaran tersebut tidak dapat dikembalikan menjadi bentuk semula. Salah satu manfaatnya adalah penggunaan sidik jari (fingerprint). Sidik jari digunakan sebagai identitas pengirim pesan. Fungsi lain adalah untuk kompresi dan message digest. Contoh algoritma fungsi ini adalah MD-5 dan SHA.Pada algoritma ini, digunakan dua buah kunci yang berhubungan yang disebut dengan kunci umum dan kunci pribadi. Kunci umum dapat dipublikasikan sehingga pesan dapat dienkripsikan tetapi tidak dapat didekripsikan dengan kunci tersebut. Kunci pribadi hanya boleh digunakan oleh pihak yang berhak untuk mendekripsikan pesan yang terenkripsi. Algoritma yang menggunakan kunci umum dan publik ini antara lain : Digital Signature Algorithm (DSA), Rivest-Shamir-Adleman (RSA), Diffie-Hellman (DH), dan sebegainya.Algoritma ini menggunakan kunci yang sama untuk mengenkripsi dan mendekripsi data. Untuk mendekripsikan data, penerima menggunakan kunci yang sama dengan kunci yang digunakan pengirim untuk mengenkripsi data. Contoh dari algoritma ini adalah

Data Encryption Standard (DES), International Data Encryption Algorithm (IDEA), Advanced Encryption Standard (AES), dan sebagainya. Dalam makalah ini, algoritma AES akan dibahas lebih lanjut.Steganografi adalah seni dan ilmu menulis atau menyembunyikan pesan tersembunyi dengan suatu cara sehingga selain si pengirim dan si penerima, tidak ada seorangpun yang mengetahui atau menyadari bahwa ada suatu pesan rahasia. Sebaliknya, kriptografi menyamarkan arti dari suatu pesan, tapi tidak menyembunyikan bahwa ada suatu pesan. Metode ini termasuk tinta yang tidak tampak, microdots, pengaturan kata, tanda tangan digital, jalur tersembunyi dan komunikasi spektrum lebar. Tujuan dari steganografi adalah merahasiakan atau menyembunyikan keberadaan dari sebuah pesan tersembunyi atau sebuah informasi. Dalam prakteknya kebanyakan diselesaikan dengan membuat perubahan tipis terhadap data digital lain yang isinya tidak akan menarik perhatian dari penyerang potensial, sebagai contoh sebuah gambar yang terlihat tidak berbahaya.Perubahan ini bergantung pada kunci (sama pada kriptografi) dan pesan untuk disembunyikan. Orang yang menerima gambar kemudian dapat menyimpulkan informasi terselubung dengan cara mengganti kunci yang benar ke dalam algoritma yang digunakan.Kelebihan steganografi daripada kriptografi adalah pesan-pesannya tidak menarik perhatian orang lain. Pesan-pesan berkode dalam kriptografi yang tidak disembunyikan, walaupun tidak dapat dipecahkan, akan menimbulkan kecurigaan. Seringkali, steganografi dan kriptografi digunakan secara bersamaan untuk menjamin keamanan pesan rahasianya.Kebanyakan algoritma steganografi menggunakan sebuah kombinasi dari beberapa teknik pencitraan untuk melakukan sebuah tugas dalam penyelubungan pesan rahasia dalam sebuah selubung file. Sebuah program steganografi dibutuhkan untuk melakukan hal-hal berikut (baik implisit melalui suatu perkiraan maupun eksplisit melalui sebuah perhitungan), menemukan kelebihan bits dalam selubung file yang dapat digunakan untuk menyelubungi pesan rahasia didalamnya, memilih beberapa diantaranya untuk digunakan dalam menyelubungiDengan perkembangan teknologi komputer saat ini, pertukaran informasi dari suatu pihak ke pihak lain sangatlah diperlukan. Informasi yang dipertukarkan itu biasanya tidak ingin diketahui oleh pihak-pihak lain, terutama oleh pihak yang bertentangan dengan pihak yang bertukar informasi ataupun pihak yang baik sengaja maupun tidak sengaja dapat memanfaatkan informasi tersebut. Jika keamanan pertukaran informasi ini tidak dapat dijaga, maka pihak - pihak lain dapat memanfaatkan informasi tanpa izin dari pemilik informasi. Hal tersebut sangat merugikan pihak-pihak yang berhak atas informasi tersebut.Ancaman keamanan terhadap informasi dapat berupa berbagai bentuk. Bentuk ancaman tersebut dapat berupa interupsi, intersepsi, modifikasi, dan fabrikasi. Ancaman interupsi dapat mengganggu ketersediaan data. Data yang ada dapat dihapus sehingga pihak yang membutuhkan informasi tersebut tidak dapat menemukan datanya. Ancaman intersepsi merupakan ancaman terhadap kerahasiaan data. Informasi yang ada disadap dan dipergunakan oleh pihak yang tidak berhak sehingga merugikan pengguna data yang sah. Ancaman modifikasi mengakibatkan kesalahan dalam penerimaan informasi sehingga informasi yang diterima tidak sesuai dengan keinginan penerima maupun pengirimnya. Ancaman fabrikasi merupakan ancaman terhadap integritas karena informasi yang berhasil dicuri oleh pihak yang tidak berhak dipalsukan, lalu dikirimkan kepada penerima seolah-olah berasal dari pengirim yang sah.Untuk mengatasi ancaman-ancaman tersebut, diperlukan suatu cara agar informasi tersebut tidak dapat diketahui oleh pihak lain. Salah satu caranya adalah dengan menggunakan kriptografi. Kriptografi sudah dikenal sejak ribuan tahun yang lalu, Kriptografi terus-menerus dikembangkan hingga saat ini. Pengembangannya dilakukan oleh berbagai pihak dari berbagai negara, Karena banyaknya jumlah algoritma yang digunakan, diperlukanlah standar algoritma sehingga dapat dipergunakan dalam berbagai aplikasi. NIST (National Institute of Standard and Technology) mempublikasikan suatu algoritma pengenkripsian data baru untuk menggantikan algoritma DES (Data Encryption Standard) yang memiliki beberapa kelemahan. Algorima baru ini dinamakan AES (Advanced Encryption Standard) atau Rijndael. Algoritma ini diperoleh melalui kompetisi yang dilakukan pada tahun 1997. Proses seleksi ini amat ketat dan membutuhkan waktu yang cukup lama. Pada akhirnya, pada tanggal 2 Oktober 2000 terpilihlah algoritma Rijndael yang dibuat oleh Rijmen dan Daemen dari Belgia. Algoritma ini tepilih sebagai AES. Meskipun masih baru, algoritma ini sudah dipergunakan pada berbagai aplikasi, salah satunya adalah untuk penyandian password. Penggunaan algoritma ini sudah sering dilihat pada perangkat lunak untuk kompresi data. Dalam perangkat lunak tersebut, salah satu metode yang digunakan untuk mengenkripsi password adalah

dengan algoritma AES.Pembentukan kode Huffman dapat dilakukan dengan membuat pohon biner. Sebuah simpul (node) dalam pohon xxxxxxxxxxxxxxxxxx

Teks Rahasia 16384 *byte* Yang Diekstrak dari *Stego – Image* Lena Menggunakan *Predictor* GAP (h=2)

Kriptografi adalah ilmu sekaligus seni untuk menjaga kerahasiaan pesan dengan cara menyamarkannya menjadi bentuk tersandi yang tidak mempunyai makna. Bentuk tersandi ini hanya dapat dibaca oleh pihak yang berhak membacanya. Pesan yang akan dirahasiakan sebelum disamarkan disebut plaintext, sedangkan pesan setelah disamarkan disebut chipertext. Proses penyamaran plaintext ke chipertext disebut enkripsi, sedangkan pengembalian chiperteks menjadi plainteks semula disebut dekripsi.Kriptografi telah lama digunakan oleh tentara Sparta di Yunani sekitar tahun 400 SM. Mereka menggunakan alat yang disebut scytale. Alat ini terbuat dari daun papirus yang dililitkan pada batang silinder. Pesan yang akan dikirim ditulis horizontal. Setelah ditulis, daun dilepaskan dari batang kemudian dikirimkan ke penerima. Penerima dapat membaca pesan tersebut setelah melilitkan kembali daun tersebut pada batang silinder dengan ukuran diameter yang sama. Teknik ini dikenal dengan nama transposisi chiper yang merupakan metode enkripsi tertua. Pada zaman Romawi kuno, Julius Caesar juga menggunakan kriptografi untuk mengirimkan pesannya. Pesan yang ia kirimkan ditulis dengan mengganti alfabet dengan alfabet lain dengan kunci tertentu. Sang penerima tentu saja telah diberi tahu kunci tersebut. Cara menyandikannya adalah dengan mengganti semua susunan alfabet dengan alfabet yang posisinya berada setelah alfabet tersebut tergantung kunci. Sebagai contoh, Julius Caesar mengganti huruf a, b, dan c menjadi d, e, dan f. Pada perang dunia kedua, Jerman menggunakan mesin untuk mengrenkripsi pesan yang dikirimkan Hitler ke tentaranya yang bernama mesin enigma. Jerman meyakini kode-kode enkripsi dari mesin tersebut tidak dapat dipecahkan karena memiliki sekitar 15 milyar kemungkinan untuk mendekripsikannya. Kenyataannya sekutu mampu mendekripsikannya sehingga mesin tersebut beberapa kali memgalami perubahan.Fungsi hash sering disebut sebagai fungsi satu arah(one-way function). Fungsi ini mengubah suatu masukan menjadi keluaran, tetapi keluaran tersebut tidak dapat dikembalikan menjadi bentuk semula. Salah satu manfaatnya adalah penggunaan sidik jari (fingerprint). Sidik jari digunakan sebagai identitas pengirim pesan. Fungsi lain adalah untuk kompresi dan message digest. Contoh algoritma fungsi ini adalah MD-5 dan SHA.Pada algoritma ini, digunakan dua buah kunci yang berhubungan yang disebut dengan kunci umum dan kunci pribadi. Kunci umum dapat dipublikasikan sehingga pesan dapat dienkripsikan tetapi tidak dapat didekripsikan dengan kunci tersebut. Kunci pribadi hanya boleh digunakan oleh pihak yang berhak untuk mendekripsikan pesan yang terenkripsi. Algoritma yang menggunakan kunci umum dan publik ini antara lain : Digital Signature Algorithm (DSA), Rivest-Shamir-Adleman (RSA), Diffie-Hellman (DH), dan sebegainya.Algoritma ini menggunakan kunci yang sama untuk mengenkripsi dan mendekripsi data. Untuk mendekripsikan data, penerima menggunakan kunci yang sama dengan kunci yang digunakan pengirim untuk mengenkripsi data. Contoh dari algoritma ini adalah Data Encryption Standard (DES), International Data Encryption Algorithm (IDEA), Advanced Encryption Standard (AES), dan sebagainya. Dalam makalah ini, algoritma AES akan dibahas lebih lanjut.Steganografi adalah seni dan ilmu menulis atau menyembunyikan pesan tersembunyi dengan suatu cara sehingga selain si pengirim dan si penerima, tidak ada seorangpun yang mengetahui atau menyadari bahwa ada suatu pesan rahasia. Sebaliknya, kriptografi menyamarkan arti dari suatu pesan, tapi tidak menyembunyikan bahwa ada suatu pesan. Metode ini termasuk tinta yang tidak tampak, microdots, pengaturan kata, tanda tangan digital, jalur tersembunyi dan komunikasi spektrum lebar. Tujuan dari steganografi adalah merahasiakan atau menyembunyikan keberadaan dari sebuah pesan tersembunyi atau sebuah informasi. Dalam prakteknya kebanyakan diselesaikan dengan membuat perubahan tipis terhadap data digital lain yang isinya tidak akan menarik perhatian dari penyerang potensial, sebagai contoh sebuah gambar yang terlihat tidak berbahaya.Perubahan ini bergantung pada kunci (sama pada kriptografi) dan pesan untuk disembunyikan. Orang yang menerima gambar kemudian dapat menyimpulkan informasi terselubung dengan cara mengganti kunci yang benar ke dalam algoritma yang

digunakan.Kelebihan steganografi daripada kriptografi adalah pesan-pesannya tidak menarik perhatian orang lain. Pesan-pesan berkode dalam kriptografi yang tidak disembunyikan, walaupun tidak dapat dipecahkan, akan menimbulkan kecurigaan. Seringkali, steganografi dan kriptografi digunakan secara bersamaan untuk menjamin keamanan pesan rahasianya.Kebanyakan algoritma steganografi menggunakan sebuah kombinasi dari beberapa teknik pencitraan untuk melakukan sebuah tugas dalam penyelubungan pesan rahasia dalam sebuah selubung file. Sebuah program steganografi dibutuhkan untuk melakukan hal-hal berikut (baik implisit melalui suatu perkiraan maupun eksplisit melalui sebuah perhitungan), menemukan kelebihan bits dalam selubung file yang dapat digunakan untuk menyelubungi pesan rahasia didalamnya, memilih beberapa diantaranya untuk digunakan dalam menyelubungiDengan perkembangan teknologi komputer saat ini, pertukaran informasi dari suatu pihak ke pihak lain sangatlah diperlukan. Informasi yang dipertukarkan itu biasanya tidak ingin diketahui oleh pihak-pihak lain, terutama oleh pihak yang bertentangan dengan pihak yang bertukar informasi ataupun pihak yang baik sengaja maupun tidak sengaja dapat memanfaatkan informasi tersebut. Jika keamanan pertukaran informasi ini tidak dapat dijaga, maka pihak - pihak lain dapat memanfaatkan informasi tanpa izin dari pemilik informasi. Hal tersebut sangat merugikan pihak-pihak yang berhak atas informasi tersebut.Ancaman keamanan terhadap informasi dapat berupa berbagai bentuk. Bentuk ancaman tersebut dapat berupa interupsi, intersepsi, modifikasi, dan fabrikasi. Ancaman interupsi dapat mengganggu ketersediaan data. Data yang ada dapat dihapus sehingga pihak yang membutuhkan informasi tersebut tidak dapat menemukan datanya. Ancaman intersepsi merupakan ancaman terhadap kerahasiaan data. Informasi yang ada disadap dan dipergunakan oleh pihak yang tidak berhak sehingga merugikan pengguna data yang sah. Ancaman modifikasi mengakibatkan kesalahan dalam penerimaan informasi sehingga informasi yang diterima tidak sesuai dengan keinginan penerima maupun pengirimnya. Ancaman fabrikasi merupakan ancaman terhadap integritas karena informasi yang berhasil dicuri oleh pihak yang tidak berhak dipalsukan, lalu dikirimkan kepada penerima seolah-olah berasal dari pengirim yang sah.Untuk mengatasi ancaman-ancaman tersebut, diperlukan suatu cara agar informasi tersebut tidak dapat diketahui oleh pihak lain. Salah satu caranya adalah dengan menggunakan kriptografi. Kriptografi sudah dikenal sejak ribuan tahun yang lalu, Kriptografi terus-menerus dikembangkan hingga saat ini. Pengembangannya dilakukan oleh berbagai pihak dari berbagai negara, Karena banyaknya jumlah algoritma yang digunakan, diperlukanlah standar algoritma sehingga dapat dipergunakan dalam berbagai aplikasi. NIST (National Institute of Standard and Technology) mempublikasikan suatu algoritma pengenkripsian data baru untuk menggantikan algoritma DES (Data Encryption Standard) yang memiliki beberapa kelemahan. Algorima baru ini dinamakan AES (Advanced Encryption Standard) atau Rijndael. Algoritma ini diperoleh melalui kompetisi yang dilakukan pada tahun 1997. Proses seleksi ini amat ketat dan membutuhkan waktu yang cukup lama. Pada akhirnya, pada tanggal 2 Oktober 2000 terpilihlah algoritma Rijndael yang dibuat oleh Rijmen dan Daemen dari Belgia. Algoritma ini tepilih sebagai AES. Meskipun masih baru, algoritma ini sudah dipergunakan pada berbagai aplikasi, salah satunya adalah untuk penyandian password. Penggunaan algoritma ini sudah sering dilihat pada perangkat lunak untuk kompresi data. Dalam perangkat lunak tersebut, salah satu metode yang digunakan untuk mengenkripsi password adalah dengan algoritma AES.Pembentukan kode Huffman dapat dilakukan dengan membuat pohon biner. Sebuah simpul (node) dalam pohon xxxxxxxxxxxxxxxxxxKriptografi adalah ilmu sekaligus seni untuk menjaga kerahasiaan pesan dengan cara menyamarkannya menjadi bentuk tersandi yang tidak mempunyai makna. Bentuk tersandi ini hanya dapat dibaca oleh pihak yang berhak membacanya. Pesan yang akan dirahasiakan sebelum disamarkan disebut plaintext, sedangkan pesan setelah disamarkan disebut chipertext. Proses penyamaran plaintext ke chipertext disebut enkripsi, sedangkan pengembalian chiperteks menjadi plainteks semula disebut dekripsi.Kriptografi telah lama digunakan oleh tentara Sparta di Yunani sekitar tahun 400 SM. Mereka menggunakan alat yang disebut scytale. Alat ini terbuat dari daun papirus yang dililitkan pada batang silinder. Pesan yang akan dikirim ditulis horizontal. Setelah ditulis, daun dilepaskan dari batang kemudian dikirimkan ke penerima. Penerima dapat membaca pesan tersebut setelah melilitkan kembali daun tersebut pada batang silinder dengan ukuran diameter yang sama. Teknik ini dikenal dengan nama transposisi chiper yang merupakan metode enkripsi tertua. Pada zaman Romawi kuno, Julius Caesar juga menggunakan kriptografi untuk mengirimkan pesannya. Pesan

yang ia kirimkan ditulis dengan mengganti alfabet dengan alfabet lain dengan kunci tertentu. Sang penerima tentu saja telah diberi tahu kunci tersebut. Cara menyandikannya adalah dengan mengganti semua susunan alfabet dengan alfabet yang posisinya berada setelah alfabet tersebut tergantung kunci. Sebagai contoh, Julius Caesar mengganti huruf a, b, dan c menjadi d, e, dan f. Pada perang dunia kedua, Jerman menggunakan mesin untuk mengrenkripsi pesan yang dikirimkan Hitler ke tentaranya yang bernama mesin enigma. Jerman meyakini kode-kode enkripsi dari mesin tersebut tidak dapat dipecahkan karena memiliki sekitar 15 milyar kemungkinan untuk mendekripsikannya. Kenyataannya sekutu mampu mendekripsikannya sehingga mesin tersebut beberapa kali memgalami perubahan.Fungsi hash sering disebut sebagai fungsi satu arah(one-way function). Fungsi ini mengubah suatu masukan menjadi keluaran, tetapi keluaran tersebut tidak dapat dikembalikan menjadi bentuk semula. Salah satu manfaatnya adalah penggunaan sidik jari (fingerprint). Sidik jari digunakan sebagai identitas pengirim pesan. Fungsi lain adalah untuk kompresi dan message digest. Contoh algoritma fungsi ini adalah MD-5 dan SHA.Pada algoritma ini, digunakan dua buah kunci yang berhubungan yang disebut dengan kunci umum dan kunci pribadi. Kunci umum dapat dipublikasikan sehingga pesan dapat dienkripsikan tetapi tidak dapat didekripsikan dengan kunci tersebut. Kunci pribadi hanya boleh digunakan oleh pihak yang berhak untuk mendekripsikan pesan yang terenkripsi. Algoritma yang menggunakan kunci umum dan publik ini antara lain : Digital Signature Algorithm (DSA), Rivest-Shamir-Adleman (RSA), Diffie-Hellman (DH), dan sebegainya.Algoritma ini menggunakan kunci yang sama untuk mengenkripsi dan mendekripsi data. Untuk mendekripsikan data, penerima menggunakan kunci yang sama dengan kunci yang digunakan pengirim untuk mengenkripsi data. Contoh dari algoritma ini adalah Data Encryption Standard (DES), International Data Encryption Algorithm (IDEA), Advanced Encryption Standard (AES), dan sebagainya. Dalam makalah ini, algoritma AES akan dibahas lebih lanjut.Steganografi adalah seni dan ilmu menulis atau menyembunyikan pesan tersembunyi dengan suatu cara sehingga selain si pengirim dan si penerima, tidak ada seorangpun yang mengetahui atau menyadari bahwa ada suatu pesan rahasia. Sebaliknya, kriptografi menyamarkan arti dari suatu pesan, tapi tidak menyembunyikan bahwa ada suatu pesan. Metode ini termasuk tinta yang tidak tampak, microdots, pengaturan kata, tanda tangan digital, jalur tersembunyi dan komunikasi spektrum lebar. Tujuan dari steganografi adalah merahasiakan atau menyembunyikan keberadaan dari sebuah pesan tersembunyi atau sebuah informasi. Dalam prakteknya kebanyakan diselesaikan dengan membuat perubahan tipis terhadap data digital lain yang isinya tidak akan menarik perhatian dari penyerang potensial, sebagai contoh sebuah gambar yang terlihat tidak berbahaya.Perubahan ini bergantung pada kunci (sama pada kriptografi) dan pesan untuk disembunyikan. Orang yang menerima gambar kemudian dapat menyimpulkan informasi terselubung dengan cara mengganti kunci yang benar ke dalam algoritma yang digunakan.Kelebihan steganografi daripada kriptografi adalah pesan-pesannya tidak menarik perhatian orang lain. Pesan-pesan berkode dalam kriptografi yang tidak disembunyikan, walaupun tidak dapat dipecahkan, akan menimbulkan kecurigaan. Seringkali, steganografi dan kriptografi digunakan secara bersamaan untuk menjamin keamanan pesan rahasianya.Kebanyakan algoritma steganografi menggunakan sebuah kombinasi dari beberapa teknik pencitraan untuk melakukan sebuah tugas dalam penyelubungan pesan rahasia dalam sebuah selubung file. Sebuah program steganografi dibutuhkan untuk melakukan hal-hal berikut (baik implisit melalui suatu perkiraan maupun eksplisit melalui sebuah perhitungan), menemukan kelebihan bits dalam selubung file yang dapat digunakan untuk menyelubungi pesan rahasia didalamnya, memilih beberapa diantaranya untuk digunakan dalam menyelubungiDengan perkembangan teknologi komputer saat ini, pertukaran informasi dari suatu pihak ke pihak lain sangatlah diperlukan. Informasi yang dipertukarkan itu biasanya tidak ingin diketahui oleh pihak-pihak lain, terutama oleh pihak yang bertentangan dengan pihak yang bertukar informasi ataupun pihak yang baik sengaja maupun tidak sengaja dapat memanfaatkan informasi tersebut. Jika keamanan pertukaran informasi ini tidak dapat dijaga, maka pihak - pihak lain dapat memanfaatkan informasi tanpa izin dari pemilik informasi. Hal tersebut sangat merugikan pihak-pihak yang berhak atas informasi tersebut.Ancaman keamanan terhadap informasi dapat berupa berbagai bentuk. Bentuk ancaman tersebut dapat berupa interupsi, intersepsi, modifikasi, dan fabrikasi. Ancaman interupsi dapat mengganggu ketersediaan data. Data yang ada dapat dihapus sehingga pihak yang membutuhkan informasi tersebut tidak dapat menemukan datanya. Ancaman intersepsi merupakan ancaman

terhadap kerahasiaan data. Informasi yang ada disadap dan dipergunakan oleh pihak yang tidak berhak sehingga merugikan pengguna data yang sah. Ancaman modifikasi mengakibatkan kesalahan dalam penerimaan informasi sehingga informasi yang diterima tidak sesuai dengan keinginan penerima maupun pengirimnya. Ancaman fabrikasi merupakan ancaman terhadap integritas karena informasi yang berhasil dicuri oleh pihak yang tidak berhak dipalsukan, lalu dikirimkan kepada penerima seolah-olah berasal dari pengirim yang sah.Untuk mengatasi ancaman-ancaman tersebut, diperlukan suatu cara agar informasi tersebut tidak dapat diketahui oleh pihak lain. Salah satu caranya adalah dengan menggunakan kriptografi. Kriptografi sudah dikenal sejak ribuan tahun yang lalu, Kriptografi terus-menerus dikembangkan hingga saat ini. Pengembangannya dilakukan oleh berbagai pihak dari berbagai negara, Karena banyaknya jumlah algoritma yang digunakan, diperlukanlah standar algoritma sehingga dapat dipergunakan dalam berbagai aplikasi. NIST (National Institute of Standard and Technology) mempublikasikan suatu algoritma pengenkripsian data baru untuk menggantikan algoritma DES (Data Encryption Standard) yang memiliki beberapa kelemahan. Algorima baru ini dinamakan AES (Advanced Encryption Standard) atau Rijndael. Algoritma ini diperoleh melalui kompetisi yang dilakukan pada tahun 1997. Proses seleksi ini amat ketat dan membutuhkan waktu yang cukup lama. Pada akhirnya, pada tanggal 2 Oktober 2000 terpilihlah algoritma Rijndael yang dibuat oleh Rijmen dan Daemen dari Belgia. Algoritma ini tepilih sebagai AES. Meskipun masih baru, algoritma ini sudah dipergunakan pada berbagai aplikasi, salah satunya adalah untuk penyandian password. Penggunaan algoritma ini sudah sering dilihat pada perangkat lunak untuk kompresi data. Dalam perangkat lunak tersebut, salah satu metode yang digunakan untuk mengenkripsi password adalah dengan algoritma AES.Pembentukan kode Huffman dapat dilakukan dengan membuat pohon biner. Sebuah simpul (node) dalam pohon xxxxxxxxxxxxxxxxxx

DATA PENGAMATAN PERCOBAN KE-TIGA

Teks Rahasia 8192 *byte* Asli Yang Akan Disispkan Pada Setiap *Host – Image* Polos Abu-abu (h = 1)

Kriptografi adalah ilmu sekaligus seni untuk menjaga kerahasiaan pesan dengan cara menyamarkannya menjadi bentuk tersandi yang tidak mempunyai makna. Bentuk tersandi ini hanya dapat dibaca oleh pihak yang berhak membacanya. Pesan yang akan dirahasiakan sebelum disamarkan disebut plaintext, sedangkan pesan setelah disamarkan disebut chipertext. Proses penyamaran plaintext ke chipertext disebut enkripsi, sedangkan pengembalian chiperteks menjadi plainteks semula disebut dekripsi.Kriptografi telah lama digunakan oleh tentara Sparta di Yunani sekitar tahun 400 SM. Mereka menggunakan alat yang disebut scytale. Alat ini terbuat dari daun papirus yang dililitkan pada batang silinder. Pesan yang akan dikirim ditulis horizontal. Setelah ditulis, daun dilepaskan dari batang kemudian dikirimkan ke penerima. Penerima dapat membaca pesan tersebut setelah melilitkan kembali daun tersebut pada batang silinder dengan ukuran diameter yang sama. Teknik ini dikenal dengan nama transposisi chiper yang merupakan metode enkripsi tertua. Pada zaman Romawi kuno, Julius Caesar juga menggunakan kriptografi untuk mengirimkan pesannya. Pesan yang ia kirimkan ditulis dengan mengganti alfabet dengan alfabet lain dengan kunci tertentu. Sang penerima tentu saja telah diberi tahu kunci tersebut. Cara menyandikannya adalah dengan mengganti semua susunan alfabet dengan alfabet yang posisinya berada setelah alfabet tersebut tergantung kunci. Sebagai contoh, Julius Caesar mengganti huruf a, b, dan c menjadi d, e, dan f. Pada perang dunia kedua, Jerman menggunakan mesin untuk mengrenkripsi pesan yang dikirimkan Hitler ke tentaranya yang bernama mesin enigma. Jerman meyakini kode-kode enkripsi dari mesin tersebut tidak dapat dipecahkan karena memiliki sekitar 15 milyar kemungkinan untuk mendekripsikannya. Kenyataannya sekutu mampu mendekripsikannya sehingga mesin tersebut beberapa kali memgalami perubahan.Fungsi hash sering disebut sebagai fungsi satu arah(one-way function). Fungsi ini mengubah suatu masukan menjadi keluaran, tetapi keluaran tersebut tidak dapat dikembalikan menjadi bentuk semula. Salah satu manfaatnya adalah penggunaan sidik jari (fingerprint). Sidik jari digunakan sebagai identitas pengirim pesan. Fungsi lain adalah untuk kompresi dan message digest. Contoh algoritma fungsi ini adalah MD-5 dan SHA.Pada algoritma ini, digunakan dua buah kunci yang berhubungan yang disebut dengan kunci umum dan kunci pribadi. Kunci umum dapat dipublikasikan sehingga pesan dapat dienkripsikan tetapi tidak dapat didekripsikan dengan kunci tersebut. Kunci pribadi hanya boleh digunakan oleh pihak yang berhak untuk mendekripsikan pesan yang terenkripsi. Algoritma yang menggunakan kunci umum dan publik ini antara lain : Digital Signature Algorithm (DSA), Rivest-Shamir-Adleman (RSA), Diffie-Hellman (DH), dan sebegainya.Algoritma ini menggunakan kunci yang sama untuk mengenkripsi dan mendekripsi data. Untuk mendekripsikan data, penerima menggunakan kunci yang sama dengan kunci yang digunakan pengirim untuk mengenkripsi data. Contoh dari algoritma ini adalah Data Encryption Standard (DES), International Data Encryption Algorithm (IDEA), Advanced Encryption Standard (AES), dan sebagainya. Dalam makalah ini, algoritma AES akan dibahas lebih lanjut.Steganografi adalah seni dan ilmu menulis atau menyembunyikan pesan tersembunyi dengan suatu cara sehingga selain si pengirim dan si penerima, tidak ada seorangpun yang mengetahui atau menyadari bahwa ada suatu pesan rahasia. Sebaliknya, kriptografi menyamarkan arti dari suatu pesan, tapi tidak menyembunyikan bahwa ada suatu pesan. Metode ini termasuk tinta yang tidak tampak, microdots, pengaturan kata, tanda tangan digital, jalur tersembunyi dan komunikasi spektrum lebar. Tujuan dari steganografi adalah merahasiakan atau menyembunyikan keberadaan dari

sebuah pesan tersembunyi atau sebuah informasi. Dalam prakteknya kebanyakan diselesaikan dengan membuat perubahan tipis terhadap data digital lain yang isinya tidak akan menarik perhatian dari penyerang potensial, sebagai contoh sebuah gambar yang terlihat tidak berbahaya.Perubahan ini bergantung pada kunci (sama pada kriptografi) dan pesan untuk disembunyikan. Orang yang menerima gambar kemudian dapat menyimpulkan informasi terselubung dengan cara mengganti kunci yang benar ke dalam algoritma yang digunakan.Kelebihan steganografi daripada kriptografi adalah pesan-pesannya tidak menarik perhatian orang lain. Pesan-pesan berkode dalam kriptografi yang tidak disembunyikan, walaupun tidak dapat dipecahkan, akan menimbulkan kecurigaan. Seringkali, steganografi dan kriptografi digunakan secara bersamaan untuk menjamin keamanan pesan rahasianya.Kebanyakan algoritma steganografi menggunakan sebuah kombinasi dari beberapa teknik pencitraan untuk melakukan sebuah tugas dalam penyelubungan pesan rahasia dalam sebuah selubung file. Sebuah program steganografi dibutuhkan untuk melakukan hal-hal berikut (baik implisit melalui suatu perkiraan maupun eksplisit melalui sebuah perhitungan), menemukan kelebihan bits dalam selubung file yang dapat digunakan untuk menyelubungi pesan rahasia didalamnya, memilih beberapa diantaranya untuk digunakan dalam menyelubungiDengan perkembangan teknologi komputer saat ini, pertukaran informasi dari suatu pihak ke pihak lain sangatlah diperlukan. Informasi yang dipertukarkan itu biasanya tidak ingin diketahui oleh pihak-pihak lain, terutama oleh pihak yang bertentangan dengan pihak yang bertukar informasi ataupun pihak yang baik sengaja maupun tidak sengaja dapat memanfaatkan informasi tersebut. Jika keamanan pertukaran informasi ini tidak dapat dijaga, maka pihak - pihak lain dapat memanfaatkan informasi tanpa izin dari pemilik informasi. Hal tersebut sangat merugikan pihak-pihak yang berhak atas informasi tersebut.Ancaman keamanan terhadap informasi dapat berupa berbagai bentuk. Bentuk ancaman tersebut dapat berupa interupsi, intersepsi, modifikasi, dan fabrikasi. Ancaman interupsi dapat mengganggu ketersediaan data. Data yang ada dapat dihapus sehingga pihak yang membutuhkan informasi tersebut tidak dapat menemukan datanya. Ancaman intersepsi merupakan ancaman terhadap kerahasiaan data. Informasi yang ada disadap dan dipergunakan oleh pihak yang tidak berhak sehingga merugikan pengguna data yang sah. Ancaman modifikasi mengakibatkan kesalahan dalam penerimaan informasi sehingga informasi yang diterima tidak sesuai dengan keinginan penerima maupun pengirimnya. Ancaman fabrikasi merupakan ancaman terhadap integritas karena informasi yang berhasil dicuri oleh pihak yang tidak berhak dipalsukan, lalu dikirimkan kepada penerima seolah-olah berasal dari pengirim yang sah.Untuk mengatasi ancaman-ancaman tersebut, diperlukan suatu cara agar informasi tersebut tidak dapat diketahui oleh pihak lain. Salah satu caranya adalah dengan menggunakan kriptografi. Kriptografi sudah dikenal sejak ribuan tahun yang lalu, Kriptografi terus-menerus dikembangkan hingga saat ini. Pengembangannya dilakukan oleh berbagai pihak dari berbagai negara, Karena banyaknya jumlah algoritma yang digunakan, diperlukanlah standar algoritma sehingga dapat dipergunakan dalam berbagai aplikasi. NIST (National Institute of Standard and Technology) mempublikasikan suatu algoritma pengenkripsian data baru untuk menggantikan algoritma DES (Data Encryption Standard) yang memiliki beberapa kelemahan. Algorima baru ini dinamakan AES (Advanced Encryption Standard) atau Rijndael. Algoritma ini diperoleh melalui kompetisi yang dilakukan pada tahun 1997. Proses seleksi ini amat ketat dan membutuhkan waktu yang cukup lama. Pada akhirnya, pada tanggal 2 Oktober 2000 terpilihlah algoritma Rijndael yang dibuat oleh Rijmen dan Daemen dari Belgia. Algoritma ini tepilih sebagai AES. Meskipun masih baru, algoritma ini sudah dipergunakan pada berbagai aplikasi, salah satunya adalah untuk penyandian password. Penggunaan algoritma ini sudah sering dilihat pada perangkat lunak untuk kompresi data. Dalam perangkat lunak tersebut, salah satu metode yang digunakan untuk mengenkripsi password adalah dengan algoritma AES.Pembentukan kode Huffman dapat dilakukan dengan membuat pohon biner. Sebuah simpul (node) dalam pohon xxxxxxxxxxxxxxxxxx

Teks Rahasia 8192 *byte* Yang Diekstrak dari *Stego – Image* Polos Abu-abu Menggunakan *Predictor* MED (h=1)

Kriptografi adalah ilmu sekaligus seni untuk menjaga kerahasiaan pesan dengan cara menyamarkannya menjadi bentuk tersandi yang tidak mempunyai makna. Bentuk tersandi ini hanya dapat dibaca oleh pihak yang berhak membacanya. Pesan yang akan dirahasiakan sebelum disamarkan disebut plaintext, sedangkan pesan setelah disamarkan disebut chipertext. Proses penyamaran plaintext ke chipertext disebut enkripsi, sedangkan pengembalian chiperteks menjadi plainteks semula disebut dekripsi.Kriptografi telah lama digunakan oleh tentara Sparta di Yunani sekitar tahun 400 SM. Mereka menggunakan alat yang disebut scytale. Alat ini terbuat dari daun papirus yang dililitkan pada batang silinder. Pesan yang akan dikirim ditulis horizontal. Setelah ditulis, daun dilepaskan dari batang kemudian dikirimkan ke penerima. Penerima dapat membaca pesan tersebut setelah melilitkan kembali daun tersebut pada batang silinder dengan ukuran diameter yang sama. Teknik ini dikenal dengan nama transposisi chiper yang merupakan metode enkripsi tertua. Pada zaman Romawi kuno, Julius Caesar juga menggunakan kriptografi untuk mengirimkan pesannya. Pesan yang ia kirimkan ditulis dengan mengganti alfabet dengan alfabet lain dengan kunci tertentu. Sang penerima tentu saja telah diberi tahu kunci tersebut. Cara menyandikannya adalah dengan mengganti semua susunan alfabet dengan alfabet yang posisinya berada setelah alfabet tersebut tergantung kunci. Sebagai contoh, Julius Caesar mengganti huruf a, b, dan c menjadi d, e, dan f. Pada perang dunia kedua, Jerman menggunakan mesin untuk mengrenkripsi pesan yang dikirimkan Hitler ke tentaranya yang bernama mesin enigma. Jerman meyakini kode-kode enkripsi dari mesin tersebut tidak dapat dipecahkan karena memiliki sekitar 15 milyar kemungkinan untuk mendekripsikannya. Kenyataannya sekutu mampu mendekripsikannya sehingga mesin tersebut beberapa kali memgalami perubahan.Fungsi hash sering disebut sebagai fungsi satu arah(one-way function). Fungsi ini mengubah suatu masukan menjadi keluaran, tetapi keluaran tersebut tidak dapat dikembalikan menjadi bentuk semula. Salah satu manfaatnya adalah penggunaan sidik jari (fingerprint). Sidik jari digunakan sebagai identitas pengirim pesan. Fungsi lain adalah untuk kompresi dan message digest. Contoh algoritma fungsi ini adalah MD-5 dan SHA.Pada algoritma ini, digunakan dua buah kunci yang berhubungan yang disebut dengan kunci umum dan kunci pribadi. Kunci umum dapat dipublikasikan sehingga pesan dapat dienkripsikan tetapi tidak dapat didekripsikan dengan kunci tersebut. Kunci pribadi hanya boleh digunakan oleh pihak yang berhak untuk mendekripsikan pesan yang terenkripsi. Algoritma yang menggunakan kunci umum dan publik ini antara lain : Digital Signature Algorithm (DSA), Rivest-Shamir-Adleman (RSA), Diffie-Hellman (DH), dan sebegainya.Algoritma ini menggunakan kunci yang sama untuk mengenkripsi dan mendekripsi data. Untuk mendekripsikan data, penerima menggunakan kunci yang sama dengan kunci yang digunakan pengirim untuk mengenkripsi data. Contoh dari algoritma ini adalah Data Encryption Standard (DES), International Data Encryption Algorithm (IDEA), Advanced Encryption Standard (AES), dan sebagainya. Dalam makalah ini, algoritma AES akan dibahas lebih lanjut.Steganografi adalah seni dan ilmu menulis atau menyembunyikan pesan tersembunyi dengan suatu cara sehingga selain si pengirim dan si penerima, tidak ada seorangpun yang mengetahui atau menyadari bahwa ada suatu pesan rahasia. Sebaliknya, kriptografi menyamarkan arti dari suatu pesan, tapi tidak menyembunyikan bahwa ada suatu pesan. Metode ini termasuk tinta yang tidak tampak, microdots, pengaturan kata, tanda tangan digital, jalur tersembunyi dan komunikasi spektrum lebar. Tujuan dari steganografi adalah merahasiakan atau menyembunyikan keberadaan dari sebuah pesan tersembunyi atau sebuah informasi. Dalam prakteknya kebanyakan diselesaikan dengan membuat perubahan tipis terhadap data digital lain yang isinya tidak akan menarik perhatian dari penyerang potensial, sebagai contoh sebuah gambar yang terlihat tidak berbahaya.Perubahan ini bergantung pada kunci (sama pada kriptografi) dan pesan untuk disembunyikan. Orang yang menerima gambar kemudian dapat menyimpulkan informasi terselubung dengan cara mengganti kunci yang benar ke dalam algoritma yang digunakan.Kelebihan steganografi daripada kriptografi adalah pesan-pesannya tidak menarik perhatian orang lain. Pesan-pesan berkode dalam kriptografi yang tidak disembunyikan, walaupun tidak dapat dipecahkan, akan menimbulkan kecurigaan. Seringkali, steganografi dan kriptografi digunakan secara bersamaan untuk menjamin keamanan pesan rahasianya.Kebanyakan algoritma steganografi menggunakan sebuah kombinasi dari beberapa teknik pencitraan untuk melakukan sebuah tugas dalam penyelubungan pesan rahasia dalam sebuah selubung file. Sebuah program steganografi dibutuhkan untuk melakukan hal-hal berikut (baik implisit melalui suatu perkiraan

maupun eksplisit melalui sebuah perhitungan), menemukan kelebihan bits dalam selubung file yang dapat digunakan untuk menyelubungi pesan rahasia didalamnya, memilih beberapa diantaranya untuk digunakan dalam menyelubungiDengan perkembangan teknologi komputer saat ini, pertukaran informasi dari suatu pihak ke pihak lain sangatlah diperlukan. Informasi yang dipertukarkan itu biasanya tidak ingin diketahui oleh pihak-pihak lain, terutama oleh pihak yang bertentangan dengan pihak yang bertukar informasi ataupun pihak yang baik sengaja maupun tidak sengaja dapat memanfaatkan informasi tersebut. Jika keamanan pertukaran informasi ini tidak dapat dijaga, maka pihak - pihak lain dapat memanfaatkan informasi tanpa izin dari pemilik informasi. Hal tersebut sangat merugikan pihak-pihak yang berhak atas informasi tersebut.Ancaman keamanan terhadap informasi dapat berupa berbagai bentuk. Bentuk ancaman tersebut dapat berupa interupsi, intersepsi, modifikasi, dan fabrikasi. Ancaman interupsi dapat mengganggu ketersediaan data. Data yang ada dapat dihapus sehingga pihak yang membutuhkan informasi tersebut tidak dapat menemukan datanya. Ancaman intersepsi merupakan ancaman terhadap kerahasiaan data. Informasi yang ada disadap dan dipergunakan oleh pihak yang tidak berhak sehingga merugikan pengguna data yang sah. Ancaman modifikasi mengakibatkan kesalahan dalam penerimaan informasi sehingga informasi yang diterima tidak sesuai dengan keinginan penerima maupun pengirimnya. Ancaman fabrikasi merupakan ancaman terhadap integritas karena informasi yang berhasil dicuri oleh pihak yang tidak berhak dipalsukan, lalu dikirimkan kepada penerima seolah-olah berasal dari pengirim yang sah.Untuk mengatasi ancaman-ancaman tersebut, diperlukan suatu cara agar informasi tersebut tidak dapat diketahui oleh pihak lain. Salah satu caranya adalah dengan menggunakan kriptografi. Kriptografi sudah dikenal sejak ribuan tahun yang lalu, Kriptografi terus-menerus dikembangkan hingga saat ini. Pengembangannya dilakukan oleh berbagai pihak dari berbagai negara, Karena banyaknya jumlah algoritma yang digunakan, diperlukanlah standar algoritma sehingga dapat dipergunakan dalam berbagai aplikasi. NIST (National Institute of Standard and Technology) mempublikasikan suatu algoritma pengenkripsian data baru untuk menggantikan algoritma DES (Data Encryption Standard) yang memiliki beberapa kelemahan. Algorima baru ini dinamakan AES (Advanced Encryption Standard) atau Rijndael. Algoritma ini diperoleh melalui kompetisi yang dilakukan pada tahun 1997. Proses seleksi ini amat ketat dan membutuhkan waktu yang cukup lama. Pada akhirnya, pada tanggal 2 Oktober 2000 terpilihlah algoritma Rijndael yang dibuat oleh Rijmen dan Daemen dari Belgia. Algoritma ini tepilih sebagai AES. Meskipun masih baru, algoritma ini sudah dipergunakan pada berbagai aplikasi, salah satunya adalah untuk penyandian password. Penggunaan algoritma ini sudah sering dilihat pada perangkat lunak untuk kompresi data. Dalam perangkat lunak tersebut, salah satu metode yang digunakan untuk mengenkripsi password adalah dengan algoritma AES.Pembentukan kode Huffman dapat dilakukan dengan membuat pohon biner. Sebuah simpul (node) dalam pohon xxxxxxxxxxxxxxxxxx

Teks Rahasia 16384 *byte* Asli Yang Akan Disispkan Pada Setiap *Host – Image* Polos Abu-abu (h=2)

Kriptografi adalah ilmu sekaligus seni untuk menjaga kerahasiaan pesan dengan cara menyamarkannya menjadi bentuk tersandi yang tidak mempunyai makna. Bentuk tersandi ini hanya dapat dibaca oleh pihak yang berhak membacanya. Pesan yang akan dirahasiakan sebelum disamarkan disebut plaintext, sedangkan pesan setelah disamarkan disebut chipertext. Proses penyamaran plaintext ke chipertext disebut enkripsi, sedangkan pengembalian chiperteks menjadi plainteks semula disebut dekripsi.Kriptografi telah lama digunakan oleh tentara Sparta di Yunani sekitar tahun 400 SM. Mereka menggunakan alat yang disebut scytale. Alat ini terbuat dari daun papirus yang dililitkan pada batang silinder. Pesan yang akan dikirim ditulis horizontal. Setelah ditulis, daun dilepaskan dari batang kemudian dikirimkan ke penerima. Penerima dapat membaca pesan tersebut setelah melilitkan kembali daun tersebut pada batang silinder dengan ukuran diameter yang sama. Teknik ini dikenal dengan nama transposisi chiper yang merupakan metode enkripsi tertua. Pada zaman Romawi kuno, Julius Caesar juga menggunakan kriptografi untuk mengirimkan pesannya. Pesan yang ia kirimkan ditulis dengan mengganti alfabet dengan alfabet lain dengan kunci tertentu. Sang penerima tentu saja telah diberi tahu kunci tersebut. Cara

menyandikannya adalah dengan mengganti semua susunan alfabet dengan alfabet yang posisinya berada setelah alfabet tersebut tergantung kunci. Sebagai contoh, Julius Caesar mengganti huruf a, b, dan c menjadi d, e, dan f. Pada perang dunia kedua, Jerman menggunakan mesin untuk mengrenkripsi pesan yang dikirimkan Hitler ke tentaranya yang bernama mesin enigma. Jerman meyakini kode-kode enkripsi dari mesin tersebut tidak dapat dipecahkan karena memiliki sekitar 15 milyar kemungkinan untuk mendekripsikannya. Kenyataannya sekutu mampu mendekripsikannya sehingga mesin tersebut beberapa kali memgalami perubahan.Fungsi hash sering disebut sebagai fungsi satu arah(one-way function). Fungsi ini mengubah suatu masukan menjadi keluaran, tetapi keluaran tersebut tidak dapat dikembalikan menjadi bentuk semula. Salah satu manfaatnya adalah penggunaan sidik jari (fingerprint). Sidik jari digunakan sebagai identitas pengirim pesan. Fungsi lain adalah untuk kompresi dan message digest. Contoh algoritma fungsi ini adalah MD-5 dan SHA.Pada algoritma ini, digunakan dua buah kunci yang berhubungan yang disebut dengan kunci umum dan kunci pribadi. Kunci umum dapat dipublikasikan sehingga pesan dapat dienkripsikan tetapi tidak dapat didekripsikan dengan kunci tersebut. Kunci pribadi hanya boleh digunakan oleh pihak yang berhak untuk mendekripsikan pesan yang terenkripsi. Algoritma yang menggunakan kunci umum dan publik ini antara lain : Digital Signature Algorithm (DSA), Rivest-Shamir-Adleman (RSA), Diffie-Hellman (DH), dan sebegainya.Algoritma ini menggunakan kunci yang sama untuk mengenkripsi dan mendekripsi data. Untuk mendekripsikan data, penerima menggunakan kunci yang sama dengan kunci yang digunakan pengirim untuk mengenkripsi data. Contoh dari algoritma ini adalah Data Encryption Standard (DES), International Data Encryption Algorithm (IDEA), Advanced Encryption Standard (AES), dan sebagainya. Dalam makalah ini, algoritma AES akan dibahas lebih lanjut.Steganografi adalah seni dan ilmu menulis atau menyembunyikan pesan tersembunyi dengan suatu cara sehingga selain si pengirim dan si penerima, tidak ada seorangpun yang mengetahui atau menyadari bahwa ada suatu pesan rahasia. Sebaliknya, kriptografi menyamarkan arti dari suatu pesan, tapi tidak menyembunyikan bahwa ada suatu pesan. Metode ini termasuk tinta yang tidak tampak, microdots, pengaturan kata, tanda tangan digital, jalur tersembunyi dan komunikasi spektrum lebar. Tujuan dari steganografi adalah merahasiakan atau menyembunyikan keberadaan dari sebuah pesan tersembunyi atau sebuah informasi. Dalam prakteknya kebanyakan diselesaikan dengan membuat perubahan tipis terhadap data digital lain yang isinya tidak akan menarik perhatian dari penyerang potensial, sebagai contoh sebuah gambar yang terlihat tidak berbahaya.Perubahan ini bergantung pada kunci (sama pada kriptografi) dan pesan untuk disembunyikan. Orang yang menerima gambar kemudian dapat menyimpulkan informasi terselubung dengan cara mengganti kunci yang benar ke dalam algoritma yang digunakan.Kelebihan steganografi daripada kriptografi adalah pesan-pesannya tidak menarik perhatian orang lain. Pesan-pesan berkode dalam kriptografi yang tidak disembunyikan, walaupun tidak dapat dipecahkan, akan menimbulkan kecurigaan. Seringkali, steganografi dan kriptografi digunakan secara bersamaan untuk menjamin keamanan pesan rahasianya.Kebanyakan algoritma steganografi menggunakan sebuah kombinasi dari beberapa teknik pencitraan untuk melakukan sebuah tugas dalam penyelubungan pesan rahasia dalam sebuah selubung file. Sebuah program steganografi dibutuhkan untuk melakukan hal-hal berikut (baik implisit melalui suatu perkiraan maupun eksplisit melalui sebuah perhitungan), menemukan kelebihan bits dalam selubung file yang dapat digunakan untuk menyelubungi pesan rahasia didalamnya, memilih beberapa diantaranya untuk digunakan dalam menyelubungiDengan perkembangan teknologi komputer saat ini, pertukaran informasi dari suatu pihak ke pihak lain sangatlah diperlukan. Informasi yang dipertukarkan itu biasanya tidak ingin diketahui oleh pihak-pihak lain, terutama oleh pihak yang bertentangan dengan pihak yang bertukar informasi ataupun pihak yang baik sengaja maupun tidak sengaja dapat memanfaatkan informasi tersebut. Jika keamanan pertukaran informasi ini tidak dapat dijaga, maka pihak - pihak lain dapat memanfaatkan informasi tanpa izin dari pemilik informasi. Hal tersebut sangat merugikan pihak-pihak yang berhak atas informasi tersebut.Ancaman keamanan terhadap informasi dapat berupa berbagai bentuk. Bentuk ancaman tersebut dapat berupa interupsi, intersepsi, modifikasi, dan fabrikasi. Ancaman interupsi dapat mengganggu ketersediaan data. Data yang ada dapat dihapus sehingga pihak yang membutuhkan informasi tersebut tidak dapat menemukan datanya. Ancaman intersepsi merupakan ancaman terhadap kerahasiaan data. Informasi yang ada disadap dan dipergunakan oleh pihak yang tidak

berhak sehingga merugikan pengguna data yang sah. Ancaman modifikasi mengakibatkan kesalahan dalam penerimaan informasi sehingga informasi yang diterima tidak sesuai dengan keinginan penerima maupun pengirimnya. Ancaman fabrikasi merupakan ancaman terhadap integritas karena informasi yang berhasil dicuri oleh pihak yang tidak berhak dipalsukan, lalu dikirimkan kepada penerima seolah-olah berasal dari pengirim yang sah.Untuk mengatasi ancaman-ancaman tersebut, diperlukan suatu cara agar informasi tersebut tidak dapat diketahui oleh pihak lain. Salah satu caranya adalah dengan menggunakan kriptografi. Kriptografi sudah dikenal sejak ribuan tahun yang lalu, Kriptografi terus-menerus dikembangkan hingga saat ini. Pengembangannya dilakukan oleh berbagai pihak dari berbagai negara, Karena banyaknya jumlah algoritma yang digunakan, diperlukanlah standar algoritma sehingga dapat dipergunakan dalam berbagai aplikasi. NIST (National Institute of Standard and Technology) mempublikasikan suatu algoritma pengenkripsian data baru untuk menggantikan algoritma DES (Data Encryption Standard) yang memiliki beberapa kelemahan. Algorima baru ini dinamakan AES (Advanced Encryption Standard) atau Rijndael. Algoritma ini diperoleh melalui kompetisi yang dilakukan pada tahun 1997. Proses seleksi ini amat ketat dan membutuhkan waktu yang cukup lama. Pada akhirnya, pada tanggal 2 Oktober 2000 terpilihlah algoritma Rijndael yang dibuat oleh Rijmen dan Daemen dari Belgia. Algoritma ini tepilih sebagai AES. Meskipun masih baru, algoritma ini sudah dipergunakan pada berbagai aplikasi, salah satunya adalah untuk penyandian password. Penggunaan algoritma ini sudah sering dilihat pada perangkat lunak untuk kompresi data. Dalam perangkat lunak tersebut, salah satu metode yang digunakan untuk mengenkripsi password adalah dengan algoritma AES.Pembentukan kode Huffman dapat dilakukan dengan membuat pohon biner. Sebuah simpul (node) dalam pohon xxxxxxxxxxxxxxxxxxKriptografi adalah ilmu sekaligus seni untuk menjaga kerahasiaan pesan dengan cara menyamarkannya menjadi bentuk tersandi yang tidak mempunyai makna. Bentuk tersandi ini hanya dapat dibaca oleh pihak yang berhak membacanya. Pesan yang akan dirahasiakan sebelum disamarkan disebut plaintext, sedangkan pesan setelah disamarkan disebut chipertext. Proses penyamaran plaintext ke chipertext disebut enkripsi, sedangkan pengembalian chiperteks menjadi plainteks semula disebut dekripsi.Kriptografi telah lama digunakan oleh tentara Sparta di Yunani sekitar tahun 400 SM. Mereka menggunakan alat yang disebut scytale. Alat ini terbuat dari daun papirus yang dililitkan pada batang silinder. Pesan yang akan dikirim ditulis horizontal. Setelah ditulis, daun dilepaskan dari batang kemudian dikirimkan ke penerima. Penerima dapat membaca pesan tersebut setelah melilitkan kembali daun tersebut pada batang silinder dengan ukuran diameter yang sama. Teknik ini dikenal dengan nama transposisi chiper yang merupakan metode enkripsi tertua. Pada zaman Romawi kuno, Julius Caesar juga menggunakan kriptografi untuk mengirimkan pesannya. Pesan yang ia kirimkan ditulis dengan mengganti alfabet dengan alfabet lain dengan kunci tertentu. Sang penerima tentu saja telah diberi tahu kunci tersebut. Cara menyandikannya adalah dengan mengganti semua susunan alfabet dengan alfabet yang posisinya berada setelah alfabet tersebut tergantung kunci. Sebagai contoh, Julius Caesar mengganti huruf a, b, dan c menjadi d, e, dan f. Pada perang dunia kedua, Jerman menggunakan mesin untuk mengrenkripsi pesan yang dikirimkan Hitler ke tentaranya yang bernama mesin enigma. Jerman meyakini kode-kode enkripsi dari mesin tersebut tidak dapat dipecahkan karena memiliki sekitar 15 milyar kemungkinan untuk mendekripsikannya. Kenyataannya sekutu mampu mendekripsikannya sehingga mesin tersebut beberapa kali memgalami perubahan.Fungsi hash sering disebut sebagai fungsi satu arah(one-way function). Fungsi ini mengubah suatu masukan menjadi keluaran, tetapi keluaran tersebut tidak dapat dikembalikan menjadi bentuk semula. Salah satu manfaatnya adalah penggunaan sidik jari (fingerprint). Sidik jari digunakan sebagai identitas pengirim pesan. Fungsi lain adalah untuk kompresi dan message digest. Contoh algoritma fungsi ini adalah MD-5 dan SHA.Pada algoritma ini, digunakan dua buah kunci yang berhubungan yang disebut dengan kunci umum dan kunci pribadi. Kunci umum dapat dipublikasikan sehingga pesan dapat dienkripsikan tetapi tidak dapat didekripsikan dengan kunci tersebut. Kunci pribadi hanya boleh digunakan oleh pihak yang berhak untuk mendekripsikan pesan yang terenkripsi. Algoritma yang menggunakan kunci umum dan publik ini antara lain : Digital Signature Algorithm (DSA), Rivest-Shamir-Adleman (RSA), Diffie-Hellman (DH), dan sebegainya.Algoritma ini menggunakan kunci yang sama untuk mengenkripsi dan mendekripsi data. Untuk mendekripsikan data, penerima menggunakan kunci yang sama dengan kunci yang digunakan pengirim untuk mengenkripsi data. Contoh dari algoritma ini adalah

Data Encryption Standard (DES), International Data Encryption Algorithm (IDEA), Advanced Encryption Standard (AES), dan sebagainya. Dalam makalah ini, algoritma AES akan dibahas lebih lanjut.Steganografi adalah seni dan ilmu menulis atau menyembunyikan pesan tersembunyi dengan suatu cara sehingga selain si pengirim dan si penerima, tidak ada seorangpun yang mengetahui atau menyadari bahwa ada suatu pesan rahasia. Sebaliknya, kriptografi menyamarkan arti dari suatu pesan, tapi tidak menyembunyikan bahwa ada suatu pesan. Metode ini termasuk tinta yang tidak tampak, microdots, pengaturan kata, tanda tangan digital, jalur tersembunyi dan komunikasi spektrum lebar. Tujuan dari steganografi adalah merahasiakan atau menyembunyikan keberadaan dari sebuah pesan tersembunyi atau sebuah informasi. Dalam prakteknya kebanyakan diselesaikan dengan membuat perubahan tipis terhadap data digital lain yang isinya tidak akan menarik perhatian dari penyerang potensial, sebagai contoh sebuah gambar yang terlihat tidak berbahaya.Perubahan ini bergantung pada kunci (sama pada kriptografi) dan pesan untuk disembunyikan. Orang yang menerima gambar kemudian dapat menyimpulkan informasi terselubung dengan cara mengganti kunci yang benar ke dalam algoritma yang digunakan.Kelebihan steganografi daripada kriptografi adalah pesan-pesannya tidak menarik perhatian orang lain. Pesan-pesan berkode dalam kriptografi yang tidak disembunyikan, walaupun tidak dapat dipecahkan, akan menimbulkan kecurigaan. Seringkali, steganografi dan kriptografi digunakan secara bersamaan untuk menjamin keamanan pesan rahasianya.Kebanyakan algoritma steganografi menggunakan sebuah kombinasi dari beberapa teknik pencitraan untuk melakukan sebuah tugas dalam penyelubungan pesan rahasia dalam sebuah selubung file. Sebuah program steganografi dibutuhkan untuk melakukan hal-hal berikut (baik implisit melalui suatu perkiraan maupun eksplisit melalui sebuah perhitungan), menemukan kelebihan bits dalam selubung file yang dapat digunakan untuk menyelubungi pesan rahasia didalamnya, memilih beberapa diantaranya untuk digunakan dalam menyelubungiDengan perkembangan teknologi komputer saat ini, pertukaran informasi dari suatu pihak ke pihak lain sangatlah diperlukan. Informasi yang dipertukarkan itu biasanya tidak ingin diketahui oleh pihak-pihak lain, terutama oleh pihak yang bertentangan dengan pihak yang bertukar informasi ataupun pihak yang baik sengaja maupun tidak sengaja dapat memanfaatkan informasi tersebut. Jika keamanan pertukaran informasi ini tidak dapat dijaga, maka pihak - pihak lain dapat memanfaatkan informasi tanpa izin dari pemilik informasi. Hal tersebut sangat merugikan pihak-pihak yang berhak atas informasi tersebut.Ancaman keamanan terhadap informasi dapat berupa berbagai bentuk. Bentuk ancaman tersebut dapat berupa interupsi, intersepsi, modifikasi, dan fabrikasi. Ancaman interupsi dapat mengganggu ketersediaan data. Data yang ada dapat dihapus sehingga pihak yang membutuhkan informasi tersebut tidak dapat menemukan datanya. Ancaman intersepsi merupakan ancaman terhadap kerahasiaan data. Informasi yang ada disadap dan dipergunakan oleh pihak yang tidak berhak sehingga merugikan pengguna data yang sah. Ancaman modifikasi mengakibatkan kesalahan dalam penerimaan informasi sehingga informasi yang diterima tidak sesuai dengan keinginan penerima maupun pengirimnya. Ancaman fabrikasi merupakan ancaman terhadap integritas karena informasi yang berhasil dicuri oleh pihak yang tidak berhak dipalsukan, lalu dikirimkan kepada penerima seolah-olah berasal dari pengirim yang sah.Untuk mengatasi ancaman-ancaman tersebut, diperlukan suatu cara agar informasi tersebut tidak dapat diketahui oleh pihak lain. Salah satu caranya adalah dengan menggunakan kriptografi. Kriptografi sudah dikenal sejak ribuan tahun yang lalu, Kriptografi terus-menerus dikembangkan hingga saat ini. Pengembangannya dilakukan oleh berbagai pihak dari berbagai negara, Karena banyaknya jumlah algoritma yang digunakan, diperlukanlah standar algoritma sehingga dapat dipergunakan dalam berbagai aplikasi. NIST (National Institute of Standard and Technology) mempublikasikan suatu algoritma pengenkripsian data baru untuk menggantikan algoritma DES (Data Encryption Standard) yang memiliki beberapa kelemahan. Algorima baru ini dinamakan AES (Advanced Encryption Standard) atau Rijndael. Algoritma ini diperoleh melalui kompetisi yang dilakukan pada tahun 1997. Proses seleksi ini amat ketat dan membutuhkan waktu yang cukup lama. Pada akhirnya, pada tanggal 2 Oktober 2000 terpilihlah algoritma Rijndael yang dibuat oleh Rijmen dan Daemen dari Belgia. Algoritma ini tepilih sebagai AES. Meskipun masih baru, algoritma ini sudah dipergunakan pada berbagai aplikasi, salah satunya adalah untuk penyandian password. Penggunaan algoritma ini sudah sering dilihat pada perangkat lunak untuk kompresi data. Dalam perangkat lunak tersebut, salah satu metode yang digunakan untuk mengenkripsi password adalah

dengan algoritma AES.Pembentukan kode Huffman dapat dilakukan dengan membuat pohon biner. Sebuah simpul (node) dalam pohon xxxxxxxxxxxxxxxxxx

Teks Rahasia 16384 *byte* Yang Diekstrak dari *Stego – Image* Polos Abu-abu Menggunakan *Predictor* MED (h=2)

Kriptografi adalah ilmu sekaligus seni untuk menjaga kerahasiaan pesan dengan cara menyamarkannya menjadi bentuk tersandi yang tidak mempunyai makna. Bentuk tersandi ini hanya dapat dibaca oleh pihak yang berhak membacanya. Pesan yang akan dirahasiakan sebelum disamarkan disebut plaintext, sedangkan pesan setelah disamarkan disebut chipertext. Proses penyamaran plaintext ke chipertext disebut enkripsi, sedangkan pengembalian chiperteks menjadi plainteks semula disebut dekripsi.Kriptografi telah lama digunakan oleh tentara Sparta di Yunani sekitar tahun 400 SM. Mereka menggunakan alat yang disebut scytale. Alat ini terbuat dari daun papirus yang dililitkan pada batang silinder. Pesan yang akan dikirim ditulis horizontal. Setelah ditulis, daun dilepaskan dari batang kemudian dikirimkan ke penerima. Penerima dapat membaca pesan tersebut setelah melilitkan kembali daun tersebut pada batang silinder dengan ukuran diameter yang sama. Teknik ini dikenal dengan nama transposisi chiper yang merupakan metode enkripsi tertua. Pada zaman Romawi kuno, Julius Caesar juga menggunakan kriptografi untuk mengirimkan pesannya. Pesan yang ia kirimkan ditulis dengan mengganti alfabet dengan alfabet lain dengan kunci tertentu. Sang penerima tentu saja telah diberi tahu kunci tersebut. Cara menyandikannya adalah dengan mengganti semua susunan alfabet dengan alfabet yang posisinya berada setelah alfabet tersebut tergantung kunci. Sebagai contoh, Julius Caesar mengganti huruf a, b, dan c menjadi d, e, dan f. Pada perang dunia kedua, Jerman menggunakan mesin untuk mengrenkripsi pesan yang dikirimkan Hitler ke tentaranya yang bernama mesin enigma. Jerman meyakini kode-kode enkripsi dari mesin tersebut tidak dapat dipecahkan karena memiliki sekitar 15 milyar kemungkinan untuk mendekripsikannya. Kenyataannya sekutu mampu mendekripsikannya sehingga mesin tersebut beberapa kali memgalami perubahan.Fungsi hash sering disebut sebagai fungsi satu arah(one-way function). Fungsi ini mengubah suatu masukan menjadi keluaran, tetapi keluaran tersebut tidak dapat dikembalikan menjadi bentuk semula. Salah satu manfaatnya adalah penggunaan sidik jari (fingerprint). Sidik jari digunakan sebagai identitas pengirim pesan. Fungsi lain adalah untuk kompresi dan message digest. Contoh algoritma fungsi ini adalah MD-5 dan SHA.Pada algoritma ini, digunakan dua buah kunci yang berhubungan yang disebut dengan kunci umum dan kunci pribadi. Kunci umum dapat dipublikasikan sehingga pesan dapat dienkripsikan tetapi tidak dapat didekripsikan dengan kunci tersebut. Kunci pribadi hanya boleh digunakan oleh pihak yang berhak untuk mendekripsikan pesan yang terenkripsi. Algoritma yang menggunakan kunci umum dan publik ini antara lain : Digital Signature Algorithm (DSA), Rivest-Shamir-Adleman (RSA), Diffie-Hellman (DH), dan sebegainya.Algoritma ini menggunakan kunci yang sama untuk mengenkripsi dan mendekripsi data. Untuk mendekripsikan data, penerima menggunakan kunci yang sama dengan kunci yang digunakan pengirim untuk mengenkripsi data. Contoh dari algoritma ini adalah Data Encryption Standard (DES), International Data Encryption Algorithm (IDEA), Advanced Encryption Standard (AES), dan sebagainya. Dalam makalah ini, algoritma AES akan dibahas lebih lanjut.Steganografi adalah seni dan ilmu menulis atau menyembunyikan pesan tersembunyi dengan suatu cara sehingga selain si pengirim dan si penerima, tidak ada seorangpun yang mengetahui atau menyadari bahwa ada suatu pesan rahasia. Sebaliknya, kriptografi menyamarkan arti dari suatu pesan, tapi tidak menyembunyikan bahwa ada suatu pesan. Metode ini termasuk tinta yang tidak tampak, microdots, pengaturan kata, tanda tangan digital, jalur tersembunyi dan komunikasi spektrum lebar. Tujuan dari steganografi adalah merahasiakan atau menyembunyikan keberadaan dari sebuah pesan tersembunyi atau sebuah informasi. Dalam prakteknya kebanyakan diselesaikan dengan membuat perubahan tipis terhadap data digital lain yang isinya tidak akan menarik perhatian dari penyerang potensial, sebagai contoh sebuah gambar yang terlihat tidak berbahaya.Perubahan ini bergantung pada kunci (sama pada kriptografi) dan pesan untuk disembunyikan. Orang yang menerima gambar kemudian dapat menyimpulkan informasi terselubung dengan cara mengganti kunci yang benar ke dalam algoritma yang

digunakan.Kelebihan steganografi daripada kriptografi adalah pesan-pesannya tidak menarik perhatian orang lain. Pesan-pesan berkode dalam kriptografi yang tidak disembunyikan, walaupun tidak dapat dipecahkan, akan menimbulkan kecurigaan. Seringkali, steganografi dan kriptografi digunakan secara bersamaan untuk menjamin keamanan pesan rahasianya.Kebanyakan algoritma steganografi menggunakan sebuah kombinasi dari beberapa teknik pencitraan untuk melakukan sebuah tugas dalam penyelubungan pesan rahasia dalam sebuah selubung file. Sebuah program steganografi dibutuhkan untuk melakukan hal-hal berikut (baik implisit melalui suatu perkiraan maupun eksplisit melalui sebuah perhitungan), menemukan kelebihan bits dalam selubung file yang dapat digunakan untuk menyelubungi pesan rahasia didalamnya, memilih beberapa diantaranya untuk digunakan dalam menyelubungiDengan perkembangan teknologi komputer saat ini, pertukaran informasi dari suatu pihak ke pihak lain sangatlah diperlukan. Informasi yang dipertukarkan itu biasanya tidak ingin diketahui oleh pihak-pihak lain, terutama oleh pihak yang bertentangan dengan pihak yang bertukar informasi ataupun pihak yang baik sengaja maupun tidak sengaja dapat memanfaatkan informasi tersebut. Jika keamanan pertukaran informasi ini tidak dapat dijaga, maka pihak - pihak lain dapat memanfaatkan informasi tanpa izin dari pemilik informasi. Hal tersebut sangat merugikan pihak-pihak yang berhak atas informasi tersebut.Ancaman keamanan terhadap informasi dapat berupa berbagai bentuk. Bentuk ancaman tersebut dapat berupa interupsi, intersepsi, modifikasi, dan fabrikasi. Ancaman interupsi dapat mengganggu ketersediaan data. Data yang ada dapat dihapus sehingga pihak yang membutuhkan informasi tersebut tidak dapat menemukan datanya. Ancaman intersepsi merupakan ancaman terhadap kerahasiaan data. Informasi yang ada disadap dan dipergunakan oleh pihak yang tidak berhak sehingga merugikan pengguna data yang sah. Ancaman modifikasi mengakibatkan kesalahan dalam penerimaan informasi sehingga informasi yang diterima tidak sesuai dengan keinginan penerima maupun pengirimnya. Ancaman fabrikasi merupakan ancaman terhadap integritas karena informasi yang berhasil dicuri oleh pihak yang tidak berhak dipalsukan, lalu dikirimkan kepada penerima seolah-olah berasal dari pengirim yang sah.Untuk mengatasi ancaman-ancaman tersebut, diperlukan suatu cara agar informasi tersebut tidak dapat diketahui oleh pihak lain. Salah satu caranya adalah dengan menggunakan kriptografi. Kriptografi sudah dikenal sejak ribuan tahun yang lalu, Kriptografi terus-menerus dikembangkan hingga saat ini. Pengembangannya dilakukan oleh berbagai pihak dari berbagai negara, Karena banyaknya jumlah algoritma yang digunakan, diperlukanlah standar algoritma sehingga dapat dipergunakan dalam berbagai aplikasi. NIST (National Institute of Standard and Technology) mempublikasikan suatu algoritma pengenkripsian data baru untuk menggantikan algoritma DES (Data Encryption Standard) yang memiliki beberapa kelemahan. Algorima baru ini dinamakan AES (Advanced Encryption Standard) atau Rijndael. Algoritma ini diperoleh melalui kompetisi yang dilakukan pada tahun 1997. Proses seleksi ini amat ketat dan membutuhkan waktu yang cukup lama. Pada akhirnya, pada tanggal 2 Oktober 2000 terpilihlah algoritma Rijndael yang dibuat oleh Rijmen dan Daemen dari Belgia. Algoritma ini tepilih sebagai AES. Meskipun masih baru, algoritma ini sudah dipergunakan pada berbagai aplikasi, salah satunya adalah untuk penyandian password. Penggunaan algoritma ini sudah sering dilihat pada perangkat lunak untuk kompresi data. Dalam perangkat lunak tersebut, salah satu metode yang digunakan untuk mengenkripsi password adalah dengan algoritma AES.Pembentukan kode Huffman dapat dilakukan dengan membuat pohon biner. Sebuah simpul (node) dalam pohon xxxxxxxxxxxxxxxxxxKriptografi adalah ilmu sekaligus seni untuk menjaga kerahasiaan pesan dengan cara menyamarkannya menjadi bentuk tersandi yang tidak mempunyai makna. Bentuk tersandi ini hanya dapat dibaca oleh pihak yang berhak membacanya. Pesan yang akan dirahasiakan sebelum disamarkan disebut plaintext, sedangkan pesan setelah disamarkan disebut chipertext. Proses penyamaran plaintext ke chipertext disebut enkripsi, sedangkan pengembalian chiperteks menjadi plainteks semula disebut dekripsi.Kriptografi telah lama digunakan oleh tentara Sparta di Yunani sekitar tahun 400 SM. Mereka menggunakan alat yang disebut scytale. Alat ini terbuat dari daun papirus yang dililitkan pada batang silinder. Pesan yang akan dikirim ditulis horizontal. Setelah ditulis, daun dilepaskan dari batang kemudian dikirimkan ke penerima. Penerima dapat membaca pesan tersebut setelah melilitkan kembali daun tersebut pada batang silinder dengan ukuran diameter yang sama. Teknik ini dikenal dengan nama transposisi chiper yang merupakan metode enkripsi tertua. Pada zaman Romawi kuno, Julius Caesar juga menggunakan kriptografi untuk mengirimkan pesannya. Pesan

yang ia kirimkan ditulis dengan mengganti alfabet dengan alfabet lain dengan kunci tertentu. Sang penerima tentu saja telah diberi tahu kunci tersebut. Cara menyandikannya adalah dengan mengganti semua susunan alfabet dengan alfabet yang posisinya berada setelah alfabet tersebut tergantung kunci. Sebagai contoh, Julius Caesar mengganti huruf a, b, dan c menjadi d, e, dan f. Pada perang dunia kedua, Jerman menggunakan mesin untuk mengrenkripsi pesan yang dikirimkan Hitler ke tentaranya yang bernama mesin enigma. Jerman meyakini kode-kode enkripsi dari mesin tersebut tidak dapat dipecahkan karena memiliki sekitar 15 milyar kemungkinan untuk mendekripsikannya. Kenyataannya sekutu mampu mendekripsikannya sehingga mesin tersebut beberapa kali memgalami perubahan.Fungsi hash sering disebut sebagai fungsi satu arah(one-way function). Fungsi ini mengubah suatu masukan menjadi keluaran, tetapi keluaran tersebut tidak dapat dikembalikan menjadi bentuk semula. Salah satu manfaatnya adalah penggunaan sidik jari (fingerprint). Sidik jari digunakan sebagai identitas pengirim pesan. Fungsi lain adalah untuk kompresi dan message digest. Contoh algoritma fungsi ini adalah MD-5 dan SHA.Pada algoritma ini, digunakan dua buah kunci yang berhubungan yang disebut dengan kunci umum dan kunci pribadi. Kunci umum dapat dipublikasikan sehingga pesan dapat dienkripsikan tetapi tidak dapat didekripsikan dengan kunci tersebut. Kunci pribadi hanya boleh digunakan oleh pihak yang berhak untuk mendekripsikan pesan yang terenkripsi. Algoritma yang menggunakan kunci umum dan publik ini antara lain : Digital Signature Algorithm (DSA), Rivest-Shamir-Adleman (RSA), Diffie-Hellman (DH), dan sebegainya.Algoritma ini menggunakan kunci yang sama untuk mengenkripsi dan mendekripsi data. Untuk mendekripsikan data, penerima menggunakan kunci yang sama dengan kunci yang digunakan pengirim untuk mengenkripsi data. Contoh dari algoritma ini adalah Data Encryption Standard (DES), International Data Encryption Algorithm (IDEA), Advanced Encryption Standard (AES), dan sebagainya. Dalam makalah ini, algoritma AES akan dibahas lebih lanjut.Steganografi adalah seni dan ilmu menulis atau menyembunyikan pesan tersembunyi dengan suatu cara sehingga selain si pengirim dan si penerima, tidak ada seorangpun yang mengetahui atau menyadari bahwa ada suatu pesan rahasia. Sebaliknya, kriptografi menyamarkan arti dari suatu pesan, tapi tidak menyembunyikan bahwa ada suatu pesan. Metode ini termasuk tinta yang tidak tampak, microdots, pengaturan kata, tanda tangan digital, jalur tersembunyi dan komunikasi spektrum lebar. Tujuan dari steganografi adalah merahasiakan atau menyembunyikan keberadaan dari sebuah pesan tersembunyi atau sebuah informasi. Dalam prakteknya kebanyakan diselesaikan dengan membuat perubahan tipis terhadap data digital lain yang isinya tidak akan menarik perhatian dari penyerang potensial, sebagai contoh sebuah gambar yang terlihat tidak berbahaya.Perubahan ini bergantung pada kunci (sama pada kriptografi) dan pesan untuk disembunyikan. Orang yang menerima gambar kemudian dapat menyimpulkan informasi terselubung dengan cara mengganti kunci yang benar ke dalam algoritma yang digunakan.Kelebihan steganografi daripada kriptografi adalah pesan-pesannya tidak menarik perhatian orang lain. Pesan-pesan berkode dalam kriptografi yang tidak disembunyikan, walaupun tidak dapat dipecahkan, akan menimbulkan kecurigaan. Seringkali, steganografi dan kriptografi digunakan secara bersamaan untuk menjamin keamanan pesan rahasianya.Kebanyakan algoritma steganografi menggunakan sebuah kombinasi dari beberapa teknik pencitraan untuk melakukan sebuah tugas dalam penyelubungan pesan rahasia dalam sebuah selubung file. Sebuah program steganografi dibutuhkan untuk melakukan hal-hal berikut (baik implisit melalui suatu perkiraan maupun eksplisit melalui sebuah perhitungan), menemukan kelebihan bits dalam selubung file yang dapat digunakan untuk menyelubungi pesan rahasia didalamnya, memilih beberapa diantaranya untuk digunakan dalam menyelubungiDengan perkembangan teknologi komputer saat ini, pertukaran informasi dari suatu pihak ke pihak lain sangatlah diperlukan. Informasi yang dipertukarkan itu biasanya tidak ingin diketahui oleh pihak-pihak lain, terutama oleh pihak yang bertentangan dengan pihak yang bertukar informasi ataupun pihak yang baik sengaja maupun tidak sengaja dapat memanfaatkan informasi tersebut. Jika keamanan pertukaran informasi ini tidak dapat dijaga, maka pihak - pihak lain dapat memanfaatkan informasi tanpa izin dari pemilik informasi. Hal tersebut sangat merugikan pihak-pihak yang berhak atas informasi tersebut.Ancaman keamanan terhadap informasi dapat berupa berbagai bentuk. Bentuk ancaman tersebut dapat berupa interupsi, intersepsi, modifikasi, dan fabrikasi. Ancaman interupsi dapat mengganggu ketersediaan data. Data yang ada dapat dihapus sehingga pihak yang membutuhkan informasi tersebut tidak dapat menemukan datanya. Ancaman intersepsi merupakan ancaman

terhadap kerahasiaan data. Informasi yang ada disadap dan dipergunakan oleh pihak yang tidak berhak sehingga merugikan pengguna data yang sah. Ancaman modifikasi mengakibatkan kesalahan dalam penerimaan informasi sehingga informasi yang diterima tidak sesuai dengan keinginan penerima maupun pengirimnya. Ancaman fabrikasi merupakan ancaman terhadap integritas karena informasi yang berhasil dicuri oleh pihak yang tidak berhak dipalsukan, lalu dikirimkan kepada penerima seolah-olah berasal dari pengirim yang sah.Untuk mengatasi ancaman-ancaman tersebut, diperlukan suatu cara agar informasi tersebut tidak dapat diketahui oleh pihak lain. Salah satu caranya adalah dengan menggunakan kriptografi. Kriptografi sudah dikenal sejak ribuan tahun yang lalu, Kriptografi terus-menerus dikembangkan hingga saat ini. Pengembangannya dilakukan oleh berbagai pihak dari berbagai negara, Karena banyaknya jumlah algoritma yang digunakan, diperlukanlah standar algoritma sehingga dapat dipergunakan dalam berbagai aplikasi. NIST (National Institute of Standard and Technology) mempublikasikan suatu algoritma pengenkripsian data baru untuk menggantikan algoritma DES (Data Encryption Standard) yang memiliki beberapa kelemahan. Algorima baru ini dinamakan AES (Advanced Encryption Standard) atau Rijndael. Algoritma ini diperoleh melalui kompetisi yang dilakukan pada tahun 1997. Proses seleksi ini amat ketat dan membutuhkan waktu yang cukup lama. Pada akhirnya, pada tanggal 2 Oktober 2000 terpilihlah algoritma Rijndael yang dibuat oleh Rijmen dan Daemen dari Belgia. Algoritma ini tepilih sebagai AES. Meskipun masih baru, algoritma ini sudah dipergunakan pada berbagai aplikasi, salah satunya adalah untuk penyandian password. Penggunaan algoritma ini sudah sering dilihat pada perangkat lunak untuk kompresi data. Dalam perangkat lunak tersebut, salah satu metode yang digunakan untuk mengenkripsi password adalah dengan algoritma AES.Pembentukan kode Huffman dapat dilakukan dengan membuat pohon biner. Sebuah simpul (node) dalam pohon xxxxxxxxxxxxxxxxxx