

REALISASI VISUAL KRIPTOGRAFI MENGGUNAKAN PENDEKATAN PERTUKARAN KUNCI DIFFIE-HELLMAN

Disusun oleh :

Antonius Fanthony (1122024)

Program Studi Teknik Elektro, Fakultas Teknik, Universitas Kristen Maranatha

Jl. Prof. Drg. Suria Sumantri, MPH. No. 65, Bandung, Jawa Barat, Indonesia

e-mail : Antonius.fanth@gmail.com

ABSTRAK

Di era modern ini banyak orang yang melakukan pertukaran data menggunakan gambar sebagai data yang akan ditukar. Dengan menggunakan rancangan kriptografi maka data yang dikirim dan diterima akan menjadi lebih aman dari orang asing yang akan mencoba melihat maupun mengambil data tersebut.

Pada Tugas Akhir ini, dibuat realisasi kriptografi visual menggunakan pendekatan pertukaran kunci Diffie-Hellman saat melakukan proses deskripsi dengan melakukan proses iterasi pada saat mencari nilai kunci rahasia dari masing-masing pengirim. Sedangkan dalam proses enkripsi menggunakan rumusan modulus pada rumusan dasar Diffie-Hellman.

Dari data pengamatan dan analisis penelitian yang sudah dilakukan pada pelaksanaan Tugas Akhir, dapat diambil beberapa kesimpulan bahwa pada saat pengujian menggunakan metoda SSIM(*Structural SIMilarity*) hasil gambar deskripsi baik dengan rentang nilai SSIM antara 0.7933 sampai dengan 0.9640.

Kata Kunci : Kriptografi, Kriptografi Visual, Diffie-Hellman, Pertukaran Kunci Diffie-Hellman

**THE REALIZATION OF VISUAL CRYPTOGRAPHY USING APPROACHING
DIFFIE-HELLMAN KEY EXCHANGE**

Composed by :

Antonius Fanthony (1122024)

*Department of Electrical Engineering, Faculty of Engineering,
Maranatha Christian University, Bandung, West Java, Indonesia*

e – mail : Antonius.fanth@gmail.com

ABSTRACT

This modern many people who exchange data using images as data to be exchanged. By using a cryptographic design data sent and received will be safer from the stranger who will try to see or retrieve the data.

In this Final Project, created The Realization of Visual Cryptography using Approaching Key Exchange Diffie-Hellman to be able to perform the process of decryption for sending image by doing iteration process when searching secret key from sender. While in encryption process use mod formula from Diffie-Hellman basic formula.

From the observation data and research analysis that has been done on the implementation of Final Project, it can be concluded that at the time of testing using SSIM (Structural SIMilarity) method is good with the range of values between 0.7933 to 0.9640.

Keywords: *Cryptography, Cryptography Visual, Diffie-Hellman, Key Exchange Diffie-Hellman*

DAFTAR ISI

ABSTRAK	i
<i>ABSTRACT</i>	ii
KATA PENGANTAR	iii
DAFTAR ISI	v
DAFTAR TABEL	vii
DAFTAR GAMBAR	viii
 BAB 1 PENDAHULUAN	
1. 1. Latar Belakang	1
1. 2. Perumusan Masalah	1
1. 3. Tujuan	2
1. 4. Pembatasan Masalah	2
1. 5. Sistematika Penulisan.....	2
 BAB 2 LANDASAN TEORI	
2. 1. Pengertian Citra <i>Digital</i>	3
2. 1. 1 Citra Berwarna	4
2. 2. <i>Cryptography</i>	4
2. 1. 1. <i>Cryptography</i> Simetris	4
2. 1. 2. <i>Cryptography</i> Asimetris	5
2. 1. 3. <i>Cryptography</i> Hybrid	5
2. 3. <i>Cryptography Visual</i>	6
2. 4. <i>Key exchange Diffie-Hellman</i>	7
2. 5. SSIM (<i>Structural Similarity</i>).....	9
 BAB 3 PERANCANGAN PERANGKAT LUNAK	
3. 1 Arsitektur Perancangan	11
3. 2 Diagram Alir	14
3. 2. 1 Diagram Alir Proses Enkripsi	14

3. 2. 2 Diagram Alir Proses Deskripsi.....	16
3. 3 Pengujian SSIM	18
 BAB 4 DATA PENGAMATAN DAN ANALISIS	
4. 1 Data Pengamatan	19
4. 2 Analisis Data	30
 BAB 5 SIMPULAN DAN SARAN	
5. 1. Simpulan	35
5. 2. Saran	35
DAFTAR REFRENSI	36
LAMPIRAN A <i>LISTING</i> PROGRAM ENKRIPSI.....	A - 1
LAMPIRAN B <i>LISTING</i> PROGRAM DESKRIPSI	B – 1
LAMPIRAN C <i>LISTING</i> PROGRAM PENGUJIAN SSIM	C–1
LAMPIRAN D <i>LISTING</i> TOOLBOX BIGMOD	D-1

DAFTAR TABEL

Tabel 4.1.1.	Percobaan Pertama Pertukaran Data Pertama	20
Tabel 4.1.2.	Percobaan Pertama Pertukaran Data Kedua	21
Tabel 4.1.3.	Percobaan Pertama Pertukaran Data Ketiga	22
Tabel 4.1.4.	Percobaan Kedua Pertukaran Data Pertama	23
Tabel 4.1.5.	Percobaan Kedua Pertukaran Data Kedua	24
Tabel 4.1.6.	Percobaan Kedua Pertukaran Data Ketiga	25
Tabel 4.1.7.	Percobaan Ketiga Pertukaran Data Pertama	26
Tabel 4.1.8.	Percobaan Ketiga Pertukaran Data Kedua	27
Tabel 4.1.9.	Percobaan Ketiga Pertukaran Data Ketiga	28
Tabel 4.1.10.	Contoh Percobaan Jika Salah Satu <i>Share</i> Yang Diterima	29
Tabel 4.2.1.	Hasil Pengujian Percobaan Pertama Dengan Metoda SSIM	31
Tabel 4.2.2.	Hasil Pengujian Percobaan Kedua Dengan Metoda SSIM	32
Tabel 4.2.3.	Hasil Pengujian Percobaan Ketiga Dengan Metoda SSIM	33

DAFTAR GAMBAR

Gambar 2.3.1. Contoh Model Dasar <i>Cryptography Visual</i>	6
Gambar 2.3.2. Contoh Model Kriptografi Visual Moni Naor dan Adi Shamir ...	7
Gambar 2.4.1. Model Dasar Kriptografi Diffie-Hellman Dengan Warna	8
Gambar 3.1.1. Diagram Blok Proses Enkripsi <i>Cryptography</i>	11
Gambar 3.1.2. Diagram Blok Proses Deskripsi <i>Cryptography</i>	12
Gambar 3.2.1. Diagram Alir Proses Enkripsi <i>Cryptography</i>	14
Gambar 3.3.1. Diagram Alir Proses Deskripsi <i>Cryptography</i>	16
Gambar 4.1.1. Contoh Perbandingan Hasil Matriks Citra Masukkan Dengan Hasil Deskripsi Dengan Nilai $q = 257$	29
Gambar 4.1.2. Gambar Perbandingan Hasil Matriks Hasil Deskripsi Dengan Citra Masukkan Dengan Nilai $q = 281$	30
Gambar 4.1.3. Gambar Perbandingan Hasil Matriks Hasil Deskripsi Dengan Citra Masukkan Dengan Nilai $q = 313$	30