PENGAMANAN PESAN MENGGUNAKAN *HYBRID* KRIPTOSISTEM *VIGENERE CIPHER* DAN *ADVANCED ENCRYPTION STANDARD* 128 DIPADUKAN DENGAN *PIXEL VALUE DIFFERENCING*

SKRIPSI

untuk memenuhi salah satu syarat mencapai derajat Sarjana
Program Studi Teknik Komputer

Diajukan oleh:

DIAH PINGKAN SARI

18.83.0326

Kepada

PROGRAM SARJANA
PROGRAM STUDI TEKNIK KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS AMIKOM YOGYAKARTA
YOGYAKARTA
2022

PENGAMANAN PESAN MENGGUNAKAN *HYBRID* KRIPTOSISTEM *VIGENERE CIPHER* DAN *ADVANCED ENCRYPTION STANDARD* 128 DIPADUKAN DENGAN *PIXEL VALUE DIFFERENCING*

SKRIPSI

untuk memenuhi salah satu syarat mencapai derajat Sarjana

Program Studi Teknik Komputer

Diajukan oleh:

DIAH PINGKAN SARI

18.83.0326

Kepada

PROGRAM SARJANA

PROGRAM STUDI TEKNIK KOMPUTER

FAKULTAS ILMU KOMPUTER

UNIVERSITAS AMIKOM YOGYAKARTA

YOGYAKARTA

2022

HALAMAN PERSETUJUAN

SKRIPSI

PENGAMANAN PESAN MENGGUNAKAN *HYBRID* KRIPTOSISTEM *VIGENERE CIPHER* DAN *ADVANCED ENCRYPTION STANDARD* 128 DIPADUKAN DENGAN *PIXEL VALUE DIFFERENCING*

yang disusun dan diajukan oleh

Diah Pingkan Sari

18.83.0326

Telah disetujui oleh Dosen Pembimbing Skripsi
pada tanggal 30 Mei 2022

Dosen Pembimbing,

Dony Ariyus, M.Kom.
NIK. 190302128

HALAMAN PENGESAHAN

SKRIPSI

PENGAMANAN PESAN MENGGUNAKAN *HYBRID* KRIPTOSISTEM *VIGENERE CIPHER* DAN *ADVANCED ENCRYPTION STANDARD* 128 DIPADUKAN DENGAN *PIXEL VALUE DIFFERENCING*

yang disusun dan diajukan oleh
Diah Pingkan Sari

18.83.0326

Telah dipertahankan di depan Dewan Penguji
pada tanggal 23 Juni 2022

Susunan Dewan Penguji

Nama Penguji	Tanda Tangan
Dony Ariyus, M.Kom. **NIK. 190302128**	
Subektiningsih, M.Kom. **NIK. 190302413**	
Wahyu Suketyastama Putra, S.T., M.Eng **NIK. 190302328**	

Skripsi ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana Komputer
Tanggal 7 Juli 2022

DEKAN FAKULTAS ILMU KOMPUTER

Hanif Al Fatta,S.Kom., M.Kom.
NIK. 190302096

HALAMAN PERNYATAAN KEASLIAN SKRIPSI

Yang bertandatangan di bawah ini,

Nama mahasiswa : Diah Pingkan Sari
NIM : 18.83.0326

Menyatakan bahwa Skripsi dengan judul berikut:

Pengamanan Pesan Menggunakan *Hybrid* Kriptosistem *Vigenere Cipher* dan *Advanced Encryption Standard* 128 Dipadukan Dengan *Pixel Value Differencing*

Dosen Pembimbing : Dony Ariyus, M.Kom.

1. Karya tulis ini adalah benar-benar ASLI dan BELUM PERNAH diajukan untuk mendapatkan gelar akademik, baik di Universitas AMIKOM Yogyakarta maupun di Perguruan Tinggi lainnya.
2. Karya tulis ini merupakan gagasan, rumusan dan penelitian SAYA sendiri, tanpa bantuan pihak lain kecuali arahan dari Dosen Pembimbing.
3. Dalam karya tulis ini tidak terdapat karya atau pendapat orang lain, kecuali secara tertulis dengan jelas dicantumkan sebagai acuan dalam naskah dengan disebutkan nama pengarang dan disebutkan dalam Daftar Pustaka pada karya tulis ini.
4. Perangkat lunak yang digunakan dalam penelitian ini sepenuhnya menjadi tanggung jawab SAYA, bukan tanggung jawab Universitas AMIKOM Yogyakarta.
5. Pernyataan ini SAYA buat dengan sesungguhnya, apabila di kemudian hari terdapat penyimpangan dan ketidakbenaran dalam pernyataan ini, maka SAYA bersedia menerima SANKSI AKADEMIK dengan pencabutan gelar yang sudah diperoleh, serta sanksi lainnya sesuai dengan norma yang berlaku di Perguruan Tinggi.

Yogyakarta, 23 Juni 2022

Yang Menyatakan,

Diah Pingkan Sari

HALAMAN MOTTO

"Dan Dia mendapatimu sebagai seorang yang bingung, lalu Dia memberikan petunjuk. Dan Dia mendapatimu sebagai seorang yang kekurangan, lalu Dia memberikan kecukupan."

~ QS Ad-Dhuha 7-8 ~

"Nak, seberat dan serumit apapun jalan kehidupanmu, jangan pernah sudi kehilangan mimpi-mimpi dan cita-citamu"

~ Romi Satria Wahono ~

HALAMAN PERSEMBAHAN

Puji syukur saya panjatkan ke hadirat Allah SWT yang telah memberikan kesehatan, rahmat dan karunia-Nya sehingga saya dapat diberikan kesempatan untuk menyelesaikan penyusunan skripsi ini dengan baik dan lancar. Tak lupa ucapan terima kasih saya haturkan kepada orang-orang tercinta yang telah memberikan do'a, dukungan, dan motivasinya sehingga membuat penulis semakin semangat untuk menyelesaikan skripsi ini dengan baik dan tepat waktu. Dengan bangga dan penuh rasa syukur, skripsi ini saya persembahkan untuk :

1. Ayah dan Ibu tercinta sebagai tanda bakti dan terima kasih, maka dengan ini saya persembahkan skripsi ini kepada ayah dan ibu karena telah memberikan do'a, dukungan, motivasi, dan kasih sayang yang tak terhingga. Terima kasih banyak saya ucapkan kepada keduanya ❤
2. Adik yang sangat saya sayangi, Candra Dewi Lestari yang telah menjadi penyemangat dan pembangkit *mood* dalam mengerjakan skripsi.
3. Dosen pembimbing skripsi saya bapak Dony Ariyus, M.Kom. Saya sangat berterima kasih atas bimbingannya selama ini dengan memberikan masukan dan saran yang membangun agar penelitian dan penulisan saya menjadi lebih baik lagi.
4. Bapak dan Ibu dosen Universitas AMIKOM Yogyakarta khususnya dari prodi Teknik Komputer yang telah membagikan ilmunya selama saya menempuh pendidikan di Universitas AMIKOM Yogyakarta.
5. Sahabat dan teman-teman saya yang telah memberikan semangat serta motivasinya kepada saya agar penulisan skripsi ini bisa diselesaikan dengan baik dan tepat waktu.
6. Serta berbagai pihak yang tidak dapat saya sebutkan satu per satu.

KATA PENGANTAR

Alhamdulillah, segala puji dan syukur penulis panjatkan ke hadirat Allah SWT karena atas ridho-Nya penulis dapat menyelesaikan penyusunan skripsi yang berjudul "**Pengamanan Pesan Menggunakan *Hybrid* Kriptosistem *Vigenere Cipher* dan *Advanced Encryption Standard* 128 Dipadukan dengan *Pixel Value Differencing***", untuk memenuhi salah satu persyaratan mencapai derajat Sarjana di Program Studi Teknik Komputer Fakultas Ilmu Komputer Universitas AMIKOM Yogyakarta. Penulis menyadari bahwa dalam proses penulisan ini mengalami banyak kendala dan hambatan. Namun berkat dukungan dan bimbingan dari berbagai pihak serta berkah dari Allah SWT, maka semua kendala tersebut dapat diatasi. Penulis mengucapkan terima kasih dan penghargaan setinggi-tingginya kepada semua pihak yang telah membantu dalam proses penyusunan skripsi ini kepada yang terhormat :

1. Allah SWT atas rahmat, hidayah, serta karunia-Nya kepada penulis sehingga dapat menyelesaikan penyusunan skripsi ini.
2. Prof. Dr. M. Suyanto, M.M. selaku Rektor Universitas AMIKOM Yogyakarta.
3. Hanif Al Fatta,S.Kom., M.Kom. selaku Dekan Fakultas Ilmu Komputer
4. Dony Ariyus, M.Kom. selaku Ketua Program Studi Teknik Komputer sekaligus dosen pembimbing yang telah memberikan arahan, saran dan motivasi agar penulis dapat menyelesaikan naskah skripsi ini dengan baik.
5. Bapak dan Ibu dosen yang telah memberikan ilmunya selama penulis menempuh pendidikan di Universitas AMIKOM Yogyakarta.
6. Serta semua pihak yang telah banyak membantu dalam proses penyusunan skripsi ini yang tidak dapat penulis sebutkan satu per satu.

Akhir kata, penulis mengharapkan skripsi ini dapat memberikan manfaat bagi penulis khususnya dan bagi pembaca pada umumnya.

Yogyakarta, 30 Mei 2022

Penulis

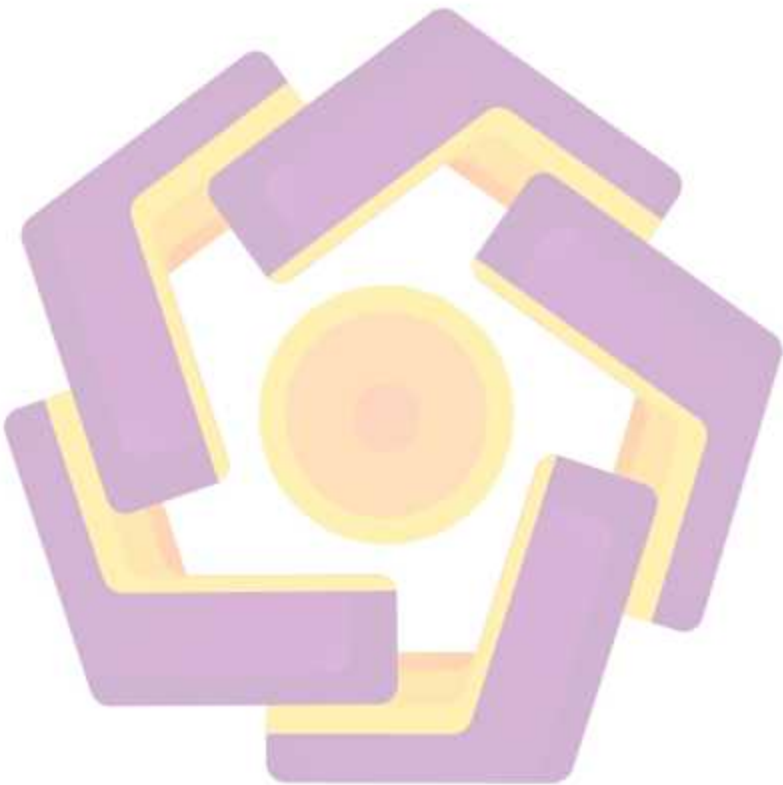
DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

DAFTAR PERSAMAAN

DAFTAR LAMPIRAN



DAFTAR LAMBANG DAN SINGKATAN

AES	: *Advanced Encryption Standard*
dB	: *Desibel*
mod	: *Modulo*
MSE	: *Mean Squared Error*
PNG	: *Portable Network Graphics*
PSNR	: *Peak Signal to Noise Ratio*
PVD	: *Pixel Value Differencing*
XOR	: *Exclusive OR*
$\oplus$	: *XOR*
ASCII	: *American Standard Code for Information Interchange*

DAFTAR ISTILAH

AES-128 bit	: Algoritma enkripsi dan dekripsi yang diterapkan untuk *hybrid* kriptosistem bersama dengan *Vigenere Cipher*
Algoritma	: Proses komputasi dan perhitungan yang terstruktur dan sistematis
Biner	: Bilangan yang tersusun dari dua angka yaitu 0 dan 1 yang digunakan untuk operasi logika
Case-sensitive	: Kepekaan terhadap penulisan karakter baik berupa huruf, angka, maupun simbol
Cipherteks	: Hasil dari proses enkripsi yang berupa kode rahasia
Cover-Image	: *File* gambar atau *image* yang digunakan untuk media penyembunyian pesan
Dekripsi	: Proses yang digunakan untuk menerjemahkan pesan dalam bentuk kode atau cipherteks agar mudah dipahami oleh penerimanya
Distorsi	: Perubahan atau penyimpangan pada *image* baik berupa warna, dimensi maupun bentuknya
Enkripsi	: Proses yang digunakan untuk mengubah pesan menjadi kode rahasia yang sulit dipahami atau cipherteks
Grayscale	: Citra digital yang memiliki nilai intensitas piksel keabuan
Heksadesimal	: Bilangan yang terdiri dari 16 basis
Plainteks	: Pesan yang dapat dibaca atau pahami maknanya
Piksel	: Elemen terkecil pada citra digital yang diukur dengan satuan *inch*
Pixel Value Differencing	: Teknik steganografi yang digunakan untuk menyembunyikan pesan ke dalam media *image*
Stego-Image	: *File* gambar atau *image* yang telah disisipi pesan
Vigenere Cipher	: Algoritma enkripsi dan dekripsi yang diterapkan untuk *hybrid* kriptosistem bersama dengan AES-128

INTISARI

Perkembangan teknologi pada era industri 4.0 membuat sebagian aktivitas dapat dilakukan secara digital. Salah satu keuntungan yang diperoleh yaitu dapat mendukung kemudahan proses komunikasi, terutama komunikasi jarak jauh yang dilakukan melalui media telepon, SMS, email, dan sebagainya. Melalui media tersebut, para pengguna dapat berbagi pesan dalam bentuk *text*, foto, video, audio, bahkan dapat melampirkan *file*. Disisi lain, kemajuan dalam bidang komunikasi tersebut juga memiliki beberapa ancaman keamanan, misalnya penyadapan jaringan melalui serangan *Man In The Middle* dengan teknik *sniffing* yang memiliki tujuan untuk mendapatkan data penting atau sensitif yang dibagikan melalui media komunikasi yang terhubung dengan jaringan yang sudah terinfeksi. Tindakan pencegahan yang dilakukan untuk mencegah kebocoran informasi dapat dilakukan dengan menerapkan kombinasi kriptografi atau disebut dengan *hybrid* kriptosistem dan memadukannya dengan teknik steganografi.

Penelitian ini menerapkan *hybrid* kripstosistem *Vigenere Cipher* dan *Advanced Encryption Standard* 128 bit (AES). Sedangkan teknik steganografi yang digunakan yaitu *Pixel Value Differencing* (PVD). Adapun mekanisme yang diterapkan yaitu melakukan *generate ciphertext* menggunakan *Vigenere Cipher* kemudian cipherteks tersebut dienkripsi menggunakan *Advanced Encryption Standard* 128 bit (AES). Hasil enkripsi tersebut kemudian dikonversi ke dalam format desimal untuk memudahkan proses penyisipan pesan ke dalam media *image* menggunanakan *Pixel Value Differencing* (PVD).

Dengan adanya kombinasi *hybrid* kriptosistem membuat pesan yang dienkripsi sulit didekripsi tanpa menggunakan kunci yang sesuai karena enkripsi dan dekripsi menggunakan algoritma AES bersifat *case-sentitive*. Steganografi menggunakan *Pixel Value Differencing* (PVD) menghasilkan nilai PSNR yang tinggi sebesar 93.38702 dB.

Kata kunci: *Vigenere Cipher*, *Advanced Encryption Standard* 128, *Pixel Value Differencing*, *Hybrid* Kriptosistem, Steganografi

ABSTRACT

Technological developments in the industrial era 4.0 make some activities can be done digitally. One of the advantages obtained is that it can support the convenience of the communication process, especially long-distance communication through telephone, SMS, email, and so on. Through this media, users can share messages in the form of text, photos, videos, audio, and even files. On the other hand, advances in the field of communication also have several security threats, for example, network eavesdropping through Man In The Middle attacks with sniffing techniques which have the aim of obtaining important or sensitive data that is shared through communications connected to infected networks. Preventive measures taken to prevent information leakage can be done by applying a combination of cryptography or what is called a hybrid cryptosystem and combining it with steganography.

This research applies a hybrid cryptosystem Vigenere Cipher and Advanced Encryption Standard 128 bit (AES). While the steganography technique used is Pixel Value Differencing (PVD). The mechanism applied is to produce ciphertext using Vigenere Cipher then the ciphertext is encrypted using the Advanced Encryption Standard 128 bit (AES). The encryption results are then converted into a lethal format to facilitate the process of inserting messages into image media using Pixel Value Differencing (PVD).

The combination of a hybrid cryptosystem makes encrypted messages difficult to decrypt without using the appropriate key because encryption and decryption using the AES algorithm are case-sensitive. Steganography using a Pixel Value Differencing (PVD) produces a high PSNR value of 93,38702 dB.

Keyword: *Vigenere Cipher, Pixel Value Differencing, Advanced Encryption Standard 128, Hybrid Cryptosystem, Steganography*