KEMENTERIAN RISET, TEKNOLOGI DAN PENDIDIKAN TINGGI
UNIVERSITAS SUMATERA UTARA
FAKULTAS ILMU KOMPUTER DAN TEKNOLOGI INFORMASI
Jalan Universitas No. 9A Kampus USU, Medan 20155
Tel/Fax: 061 8228048, e-mail: fasilkomti@usu.ac.id, laman: http://fasilkom-ti.usu.ac.id

FORM PENGAJUAN JUDUL

Foto Terbaru

Nama : Ihya Ainun Fikri

NIM : 161401021

Judul diajukan oleh* : ☐ Dosen
☐ Mahasiswa

Bidang Ilmu (tulis dua bidang) : Cryptography dan Kompresi Data

Uji Kelayakan Judul** : ◯ Diterima ◯ Ditolak

Hasil Uji Kelayakan Judul :

Calon Dosen Pembimbing I : M. Andri Budiman,ST.,M.Comp.Sc.,M.E.M
NIP : 197510082008011011
Calon Dosen Pembimbing II : Dian Rachmawati, S.Si, M.Kom
NIP : 198307232009122004

Paraf Calon Dosen Pembimbing I

Medan, ...

Ka. Laboratorium Penelitian,

** Centang salah satu atau keduanya*

*** Pilih salah satu*

(Dani Gunawan, S.T, M.T.)

NIP.198209152012121002

KEMENTERIAN RISET, TEKNOLOGI DAN PENDIDIKAN TINGGI
UNIVERSITAS SUMATERA UTARA
FAKULTAS ILMU KOMPUTER DAN TEKNOLOGI INFORMASI
Jalan Universitas No. 9A Kampus USU, Medan 20155
Tel/Fax: 061 8228048, e-mail: fasilkomti@usu.ac.id, laman: http://fasilkom-ti.usu.ac.id

RINGKASAN JUDUL YANG DIAJUKAN

*Semua kolom di bawah ini diisi oleh mahasiswa yang sudah mendapat judul

Judul / Topik Skripsi	Sistem Kripto-Kompresi dengan Algoritma Multi-Factor RSA dan Algoritma Levenstein Code
Latar Belakang dan Penelitian Terdahulu	Dewasa ini kemudahan dalam melakukan komunikasi jarak jauh sudah menjadi hal yang biasa, sebab itu keterikatan masyarakat dalam menggunakan internet sudah mendarah daging. Pengiriman pesan teks dengan pemanfaatan internet sangat memudahkan masyarakat dalam berkomunikasi jarak jauh, namun hal tersebut dapat menjadi sebuah masalah jika adanya pihak-pihak yang tidak berkepentingan memanfaatkan informasi yang dikirim. Dari itu keamanan teks yang terkirim telah menjadi faktor penting yang harus di perhatikan. Jaringan internet merupakan jaringan yang sangat rentan akan terjadinya penyadapan informasi. Oleh karena itu diperlukan sebuah solusi agar pesan yang terkirim tidak mudah dibaca oleh orang yang menyadap pesan tersebut. Salah satunya adalah dengan mengenkripsi pesan yang akan dikirim secara *end-to-end* sehingga pesan hanya bisa dibaca oleh pengirim dan penerima pesan dan yang berada di jaringan internet adalah pesan yang sudah terenkripsi. [1] Kriptografi adalah ilmu dan seni untuk menjaga kerahasiaan data yang berhubungan dengan aspek keamanan informasi. Hal ini bertujuan agar sebuah data yang disampaikan hanya dimengerti oleh orang yang berhak untuk mengetahuinya dan tidak ada pihak lain yang terlibat. Salah satu contoh dari ilmu kriptografi adalah algoritma kunci simetris dan kunci asimetris. Algoritma kunci simetris adalah algoritma yang menggunakan kunci yang sama untuk proses enkripsi dan deskripsi. Algoritma kunci asimetri adalah algoritma pengenkripsian dengan menggunakan kunci publik sebagai media pengenkripsi dan kunci privat sebagai media pendekripsiannya. [2] Untuk mengirim pesan terenkripsi tentunya penerima harus memiliki kunci untuk mendekripsikan pesan tersebut agar dapat dibaca. Karena tidak aman, jika pengirim juga mengirimkan kunci untuk mendekripsikannya, maka diperlukan algoritma yang menggunakan kunci yang berbeda untuk proses enkripsi dan dekripsinya yang biasa disebut algoritma asimetris atau algoritma kunci publik. Kunci yang digunakan untuk proses enkripsi disebut kunci publik (tidak rahasia) sedangkan kunci yang digunakan untuk proses dekripsi disebut kunci privat (rahasia). Di sini penulis menggunakan varian algoritma RSA yaitu algoritma Multi-Factor RSA. Pemilihan algoritma Multi-Factor RSA didasarkan pada kebutuhan aplikasi *instant messaging* yaitu memerlukan kombinasi kunci privat dan publik yang banyak mengingat banyaknya pengguna aplikasi yang tiap pengguna harus memiliki kombinasi kunci yang berbeda.[1] Pada algoritma Multi-Factor RSA tingkat kesulitan bergantung pada bilangan prima yang di bangkitkan dan akan menjadi kunci privat yang harus di

	jaga kerahasiaannya. Saat pembangkitan kunci diperlukannya paling sedikit 3 buah bilangan prima yang mana masing masing bilangan prima sekitar 341 bit. Namun penggunaan algoritma Multi-Factor RSA memiliki kelemahan yang sangat fatal, yaitu terdapat ukuran *file* yang terenkripsi dan ukuran *file* sebelum di enkripsi sangat signifikan. *File* yang terenkripsi didapati jauh lebih besar daripada *file* asli sehingga dibutuhkannya algoritma kompresi untuk memudahkan penerima dalam menerima *file* terenkripsi. Salah satu algoritma kompresi yang akan penulis gunakan pada penelitian ini adalah algoritma Levenstein Code. [3] Kompresi data adalah suatu proses untuk mengubah sebuah input data stream (stream sumber atau data mentah asli) ke dalam aliran data yang lain yang berupa output atau stream lainnya (data yang sudah terkompresi) yang memiliki ukuran yang lebih kecil (Salomon & Giovanni, 2010). [4] Ada beberapa faktor yang harus diperhatikan dalam kompresi data yaitu)Ratio of Compression, Compression Ratio, Redudancy, dan time process. Ada banyak algoritma yang dikembangkan untuk kompresi data, namun belum ada satupun algoritma yang baik untuk mengkompresi berbagai tipe *file* karena karakteristik atau struktur *file* yang berbeda-beda. [5]
Rumusan Masalah	Permasalah yang akan di bahas dalam penelitian ini adalah penggunaan algoritma Multi-Factor RSA menghasilkan *file* enkripsi yang memiliki ukuran *file* yang cukup signifikan dengan *file* aslinya. Dari permasalahan tersebut maka deperlukan adanya algoritma kompresi guna memperkecil ukuran *file* tersebut.
Metodologi	Tahapan-tahapan metodologi penelitian: 1. Studi Pustaka Pada tahap ini penulis berupaya mengumpulkan referensi terkait penelitian baik itu berupa buku, jurnal, artikel, situs internet, dan penelitian yang terkait dengan algortima kriptografi Multi-Factor RSA dan algoritma kompresi data Levenstein Code. Hal ini dilakukan agar memperoleh informasi dan data yang di perlukan dalam penulisan penelitian ini. 1. Analisa dan Perancangan Berdasarkan ruang lingkup penelitian, penulis akan merancang sebuah diagram alir (*flowchart)* dan ishikawa diagram (*fishbone*) yang dimana hal tersebut adalah hasil dari analisa terhadap hal – hal yang di butuhkan pada penelitian. 2. Implementasi Pada proses ini penelitian akan penulis implementasikan dalam bentuk system yang menggunakan Bahasa pemrograman c# dan di sesuaikan dengan alur diagram yang telah di rancang sebelumnya. 3. Pengujian Di tahap ini penulis akan menggunakan *file* teks yang berekstensi .DOCX yang kemudian akan di proses pada system yang telah di rancang sebelumnya.

KEMENTERIAN RISET, TEKNOLOGI DAN PENDIDIKAN TINGGI
UNIVERSITAS SUMATERA UTARA
FAKULTAS ILMU KOMPUTER DAN TEKNOLOGI INFORMASI
Jalan Universitas No. 9A Kampus USU, Medan 20155
Tel/Fax: 061 8228048, e-mail: fasilkomti@usu.ac.id, laman: http://fasilkom-ti.usu.ac.id

	4. Dokumentasi Pada tahap ini, penelitian akan didokumentasikan dalam bentuk skripsi. Mulai dari tahap analisa hingga sampai tahap pengujian akan di cantumkan agar dapat mengetahui hasil akhir pada penelitian.
Referensi	1. Bayati. 2017. *Implementasi Algoritma Affine Cipher, RSA-CRT dan Alternate Unary Code Dalam Pengamanan Dan Kompresi Teks.* Skripsi. Univeritas Sumatera Utara. 2. Panjaitan, Fredryk. 2018. *Implementasi Kriptografi Hybrid Algoritma RSA-CRT dan Playfair Cipher Dalam Pengamanan File Citra.* Skripsi. Universitas Sumatera Utara. 3. Boneh, Dan; Shacham, Hovav. 2002. *Fast Variants of RSA.* CryptoBytes. 4. Lili, Anggraini. 2016. *PERBANDINGAN ALGORITMA ELIAS DELTA CODES DENGAN ALGORITMA LEVENTEIN CODE DALAM KOMPRESI CITRA .GIF*. Skripsi. Universitas Sumatera Utara. 5. Simorangkir, Elsya Sabrina Asmta. 2017. *ANALISIS PERBANDINGAN ALGORITMA HUFFMANDAN ALGORITMA SEQUITURDALAM KOMPRESI DATA TEXT.* Skripsi. Universitas Sumatera Utara.

Medan, ...
Mahasiswa yang mengajukan,

(Ihya Ainun Fikri)

NIM. 161401021