STUDI KOMPARASI AL-GORITMA KEAMANAN DATA MENGGUNAKAN KRIPTOGRAFI VIGENERE CHIPER DAN RIVEST SHAMIR ADLEMAN (RSA)

Ii Sopiandi[1], **Abdul jabbar**[2]
[1,]*Program Stud iInformatika, Fakultas Teknik, Universitas Majalengka*
[2,]*Program Stud iInformatika, Fakultas Teknik, Universitas Majalengka*
Email: [1]*iisopiandi@unma.ac.id,* [2]*jabbarmuhammad20@gmail.com*

ABSTRACT

This study aims to compare empirically the cryptographic Vigenere Chiper and Rivest Shamir Adleman (RSA) using the Waterfall methodology based on this research in terms of Encryption and Decryption, in terms of time (seconds) to find out how long the encryption and decryption time is, the researchers prepare 10 (ten) TXT file types with different sizes and compared to the average amount of time obtained. Understanding Cryptography According to Experts Cryptography is the science and art of securely storing messages, data or information. Cryptography comes from the Greek word Crypto and Graphia which means secret writing. Cryptography is a science that studies writing in secret. Cryptography is part of a branch of mathematics called Cryptology.

Keyword:*: Kriptografi, Vigenere Chiper, Rivest Shamir Adleman (RSA),Kriptografi Asimetri ,Kriptografi Simetris..*

1. PENDAHULUAN

1.1. Latar Belakang

Kriptografi pada awalnya merupakan ilmu yang mempelajari penyembunyian pesan. Namun, seiring berkembangnya teknologi, kriptografi ini juga berkembang, perkembangan teknologi ini dapat dilihat dengan adanya internet yang menghubungkan komputer satu sama lain. Dengan adanya perkembangan ini kriptografi sangat dibutuhkan untuk keamanan data yang dikirim kepada komputer lain.

Dalam era digital, komunikasi melalui jaringan komputer memegang peranan penting. Melalui komunikasi elektronik, seseorang dapat melakukan transaksi atau komunikasi dengan sangat cepat dan praktis. Hal ini merupakan pengaruh dari perkembangan yang sangat signifikan dalam teknologi informasi, dimana bandwidth internet yang semakin besar dengan biaya akses yang semakin murah. Konsekuensinya adalah resiko dalam keamanan informasi semakin meningkat.

Kriptografi adalah ilmu yang bersandarkan pada teknik matematika untuk berurusan dengan keamanan informasi seperti kerahasiaan, keutuhan data dan autentikasi entitas. Ada empat tujuan utama dari kriptografi. Kerahasiaan (confidentiality) di mana kriptografi digunakan untuk menjaga isi dari informasi dari siapapun kecuali yang memiliki otoritas atau kunci rahasia untuk membuka informasi yang telah disandi. Kerahasiaan dijaga dengan melakukan enkripsi (penyandian). Keutuhan (integrity) yang berhubungan dengan penjagaan dari perubahan data secara tidak sah. Untuk menjaga integritas data, sistem harus memiliki kemampuan untuk mendeteksi manipulasi data oleh pihak-pihak yang tidak berhak. Fungsi kriptografi yang lain adalah autentikasi yang berhubungan dengan identifikasi atau pengenalan, baik secara kesatuan sistem maupun informasi itu sendiri. Dua pihak yang saling berkomunikasi harus saling memperkenalkan diri. Informasi yang dikirimkan melalui jaringan harus diautentikasi keaslian, isi datanya, waktu pengiriman, dan lain-lain. Non-repudiation adalah usaha untuk mencegah terjadinya penyangkalan terhadap pengiriman dengan kata lain, terciptanya suatu informasi oleh yang mengirimkan. Di dalam kriptografi terdapat dua Algoritma yang berbeda algoritma **Simetris** adalah "si penerima pesan harus diberitahu kunci dari pesan tersebut agar bisa mendekripsikan pesan yang terkirim" contoh nya Kriptografi

Vigenere Chiper dan algoritma **Asimetris** (*asymmetric algorithm*) "adalah suatu algoritma dimana kunci enkripsi yang digunakan tidak sama dengan kunci dekripsi. Pada algoritma ini menggunakan dua kunci yakni kunci publik (public key) dan kunci privat (private key)". Contohnya Kriptografi (RSA) Rivest Shamir Adleman.

Oleh karena itu perlunya implementasi keamanan Algoritma kriptografi khususnya keamanan data teks yang digunakan pada vignere chiper dan RSA, maka penulis terdorong untuk membuat judul mengambil judul " *Studi Komparasi Kriptografi Vignere Chiper dan Rivest Shamir Adleman (RSA)*"

Dari latar belakang diatas dapat didefinisikan salah satu masalah yaitu bagaimana Studi Komparasi algoritma kriptografi Vigenere Chiper dan Rivest

Shamir Adleman (RSA) untuk proses selisih waktu enkripsi dan pendekripsian

Dari hasil identifikasi masalah di atas, maka didapat sebuah perumusan masalahnya berdasarkan latar belakang, maka yang menjadi rumusan masalah pada penelitian ini adalah bagaimana membandingkan algoritma Vigenere Chiper dan Rivest Shamir Adleman (RSA) selisih waktu pengenkripsian dan pendekripsian pesan teks.

1.2. Tinjuan Pustaka

Kata kriptografi berasal dari bahasa Yunani, "*kryptós*" yang berarti tersembunyi dan "*gráphein*" yang berarti tulisan. Sehingga kata kriptografi dapat diartikan berupa frase "tulisan tersembunyi". Menurut *Request for Comments* (RFC), kriptografi merupakan ilmu matematika yang berhubungan dengan transformasi data untuk membuat artinya tidak dapat dipahami (untuk menyembunyikan maknanya), mencegahnya dari perubahan tanpa izin, atau mencegahnya dari penggunaan yang tidak sah. Jika transformasinya dapat dikembalikan, kriptografi juga bisa diartikan sebagai proses mengubah kembali data yang terenkripsi menjadi bentuk yang dapat dipahami. Artinya, kriptografi dapat diartikan sebagai proses untuk melindungi data dalam arti yang luas (Oppliger, 2005:30).

Jadi, secara umun dapat diartikan sebagai seni menulis atau memecahkan *cipher* (Talbot dan welsh, 2006).Menezes, Oorschot dan Vanstone (1996) menyatakan bahwa kriptografi adalah suatu studi teknik matematika yang berhubungan dengan aspek keamanan informasi seperi kerahasiaan, integritas data, otentikasi entitas dan otentikasi keaslian data. Kriptografi tidak hanya berarti penyediaan keamanan informasi, melainkan sebuah himpunan taknik-teknik.

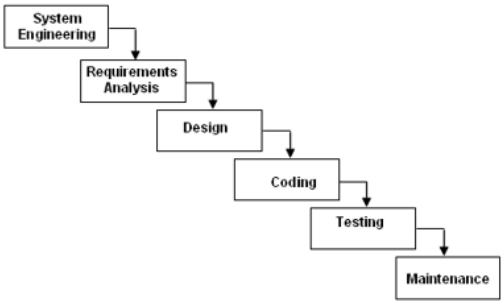
Pengembangan paling mengejutkan dalam sejarah kriptografi terjadi pada 1976 saat Diffie dan Hellman mempublikasikan *"New Directions in Cryptography"*. Tulisan ini memperkenalkan konsep revolusioner kriptografi kunci publik dan juga memberikan metode baru untuk pertukaran kunci, keamanan yang berdasar pada kekuatan masalah logaritma diskret. Meskipun Diffie dan Hellman tidak memiliki realisasi praktis pada ide enkripsi kunci publik saat itu, idenya sangat jelas dan menumbuhkan ketertarikan yang luas pada komunitas kriptografi.

Pada 1978 Rivest, Shamir dan Adleman menemukan rancangan enkripsi kunci publik yang sekarang disebut RSA. Rancangan RSA berdasar pada masalah faktorisasi bilangan yang sulit, dan menggiatkan kembali usaha untuk menemukan metode yang lebih efisien untuk pemfaktoran. Tahun 80-an terjadi peningkatan luas di area ini, sistem RSA masih aman. Sistem lain yang merupakan rancangan kunci publik ditemukan oleh Taher ElGamal pada tahun 1984. Rancangan ini berdasar pada masalah logaritma diskret.

Tujuan dari kriptografi Kerahasiaan (*confidentiality*) adalah layanan yang digunakan untuk menjaga isi informasi dari semua pihak kecuali pihak yang memiliki otoritas terhadap informasi. Ada beberapa pendekatan untuk menjaga kerahasiaan, dari pengamanan secara fisik hingga penggunaan algoritma matematika yang membuat data tidak dapat dipahami. Istilah lain yang senada dengan *confidentiality* adalah *secrecy* dan *privacy*. Integritas data adalah layanan penjagaan pengubahan data dari pihak yang tidak berwenang. Untuk menjaga integritas data, sistem harus memiliki kemampuan untuk mendeteksi manipulasi pesan oleh pihak-pihak yang tidak berhak, antara lain penyisipan, penghapusan, dan pensubsitusian data lain kedalam pesan yang sebenarnya. Di dalam kriptografi, layanan ini direalisasikan dengan menggunakan tanda-tangan digital (*digital signature*). Pesan yang telah ditandatangani menyiratkan bahwa pesan yang dikirim adalah asli. Otentikasi adalah layanan yang berhubungan dengan identifikasi, baik mengidentifikasi kebenaran pihak-pihak yang berkomunikasi (*user authentication* atau *entity authentication*) maupun mengidentifikasi kebenaran sumber pesan (*data origin authentication*). Dua pihak yang saling berkomunikasi harus dapat mengotentikasi satu sama lain sehingga ia dapat memastikan sumber pesan. Pesan yang dikirim melalui saluran komunikasi juga harus diotentikasi asalnya. Otentikasi sumber pesan secara implisit juga memberikan kepastian integritas data.

1.3. Metodologi Penelitian

Dalam hal metodologi penelitian menggunakan waterfall dan , hanya di kumpulkan berupa berkas berkas data saja yang di butuhkan seperti journal pendukung dan pengumpulan bahan-bahan data seperti di bawah ini :



Gambar 1 : Waterfall

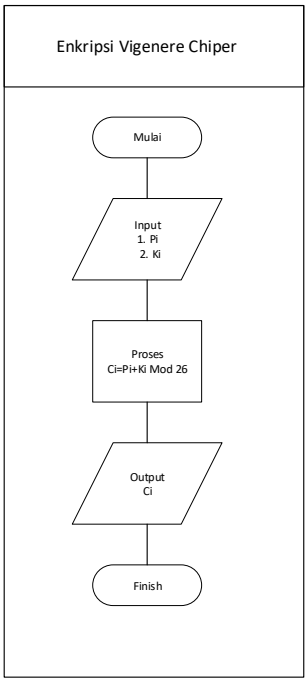
Tahapan analisis Studi Komparasi Kriptografi Vigenere Chiper dan Rivest Shamir Adleman (RSA) menggunakan metode waterfall berikut Tabel penjelasanya

No	Nama	Kegiatan
1	*System Engineering*	1. Analisis kebutuhan perangkat keras 2. Identifikasi masalah
2	*Requiremen Analysis*	1. Studi Literatur 2. Wawancara 3. Studi kepustakaan
3	*Design*	1. Pembuatan rumusan masalah 2. Pembuatan Rumus Enkripsi dan Dekripsi
4	*Coding*	1. Implementasi
5	*Testing*	1. Pengujian Sistem/program Enkripsi dan Dekripsi Vigenere Chiper dan Rivest Shamir adleman (RSA)
6	*Maintenance*	1. Perawatan Aplikasi

Berikut peralatan dan spesifikasi yang telah sesuaikan untuk kebutuhan penelitian ini :

1. Komputer (Pc)
   Hdd : 250GB
   Ram 2GB
   Proc: dual Core
   Monitor 14 Inc
2. Kebutuhan Software
   Office (Excel)
   Xampp
   PHP/Laravel

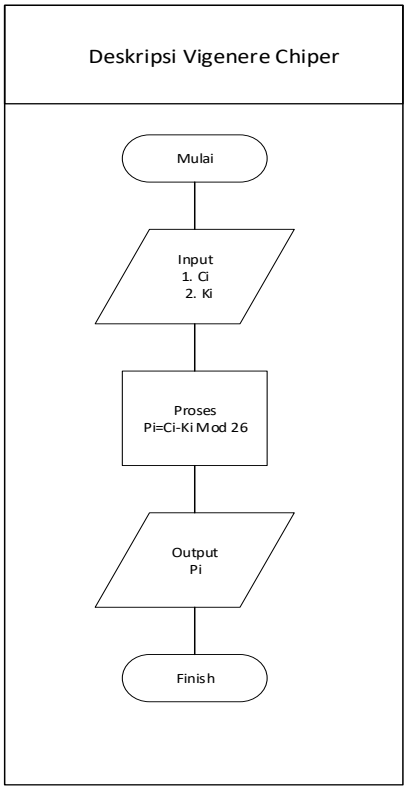
Berikut Flowchart yang sudah dibuat meliputi Enkripsi Vigenere Chiper, Dekripsi Vigenere Chiper, Enkripsi RSA dan Dekripsi RSA :



Gambar 2 : Flowchat Enkripsi Vigenere Chiper

Gambar Flowchart Enkripsi Vigenere Chiper ini terdapat Penjelasan Arti Simbol/Kata Ci : *Chipertext* merupakan hasil dari enkripsi tersebut. Ki : Kunci *Private* dimana kunci ini tidak boleh diketahui oleh orang lain dan Pi:*Plaintext* adalah karakter/huruf sebelum di enkripsi

Berikut Flowchart Dekripsi Vigenere Chiper yang sudah dibuat :

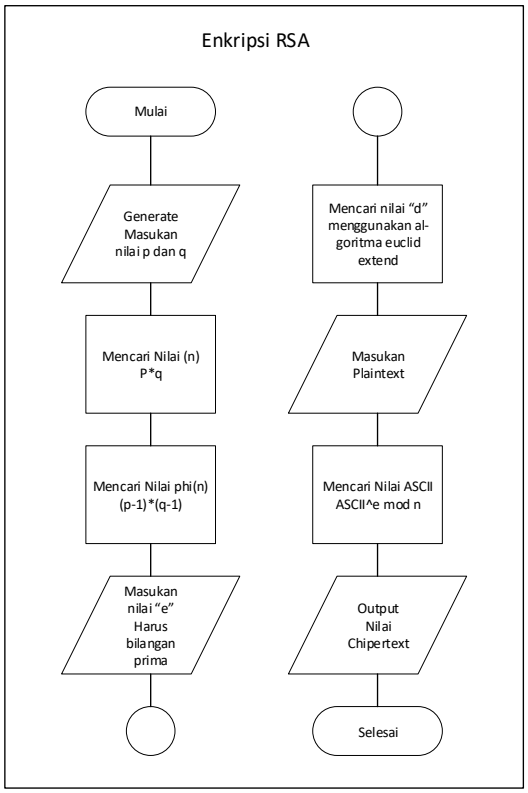


Gambar 3 : Flowchat Enkripsi Vigenere Chiper

Gambar Flowchart Enkripsi Vigenere Chiper ini terdapat Penjelasan Arti Simbol/Kata Ci : *Chipertext* merupakan hasil dari enkripsi tersebut. Ki : Kunci *Private* dimana kunci ini tidak boleh diketahui oleh orang lain dan Pi:*Plaintext* adalah karakter/huruf sebelum di enkripsi.

2. PEMBAHASAN

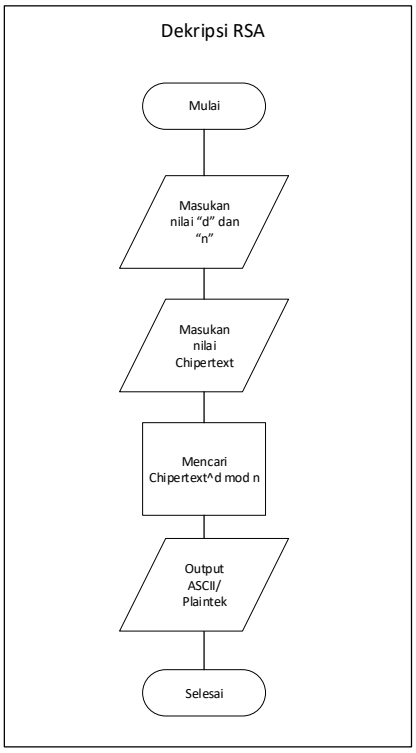
Berikut Flowchart Ekripsi yang sudah dibuat RSA :



Gambar 4 : Flowchart Enkripsi Rives Shamir Adleman(RSA)

Flowchart ini merupakan Enkripsi Rives Shamir Adlenan (RSA) berikut Penjelasannya Sebelum menggunakan ekripsi RSA, harus megenerate terlebih dahulu. Dengan mencari nilai P dan Q (harus Bilangan Prima) setelah menemukanya mencari nilai Phi(n) dengan rumus (p-1)*(q-1) lalu masukan nilai "e" bilangan prima dan untuk mencari nilai "d" harus menggunakan algoritma *Euclid Extend* dan menghasilkan ASCII^e Mod n Nilai ascii ini diperoleh dari Karakter/huruf yang akan di Enkripsikan

Berikut Dekripsi Rives Shamir Adlenan (RSA) yang sudah dibuat :



Gambar 5 : Flowchart Enkripsi Rives Shamir Adleman(RSA)

Gambar Flowchart Dekripsi ini memiliki tahap-tahap yaitu untuk menDekripsikanya pertama memasukan nilai "d" dan "n" yang sudah di cari sebelum mengenkripsikanya, Kedua masukan nilai Chipertext yang sudah di convert ke ASCII Ketiga mencari rumus Chipertext^d mod n yang sudah dicari sebelum enkripsi.

2.1. Langka-langkah Penggunaan enskripsi

Berikut langkah-langkah enkripsi dan dekripsi :

Enkripsi Vigenere Chiper

Masukan Nilai Pi dan Ki (Pi: Plaintext, Ki:Kunci *Private*)

Misal Pi = 9 (J)

Ki = 6 (G)

Ci=Pi + Ki Mod 26

Ci =((9 + 6) Mod 26)

Ci = 15 (P)

Dekripsi Vigenere Chiper

Masukan Nilai Ci dan Ki

Misal Ci=15

Ki=6

Pi=Ci - Ki Mod 26

Pi=15 - 6 Mod 26

Pi=9 (J)

Generate RSA

Mencari Nilai P dan Q

Misal P= 47 (Bil. Prima)

Q=71 (Bil. Prima)

Mencari (n)= P*Q

(n)=47*71

(n)=3337

3.Mencari phi(n)= (p-1)*(q-1)

(47-1)*(71-1)

46*70

Phi (n) = 3220

Masukan nilai e (bilangan

prima)

Misal e=79

Masukan nilai d, nilai ini hanya dapat melalui algoritma Euclid extend, Misal d = 1019 Jadi dapat diperoleh hasil :

Tabel. 1 Tabel Kunci RSA

K. Publik	e	n
	79	3337
K. Private	d	n
	1019	3337

Berikut table kunci yang sudah di generate berdasarkan bilangan yang sudah ditentukan

Berikut table Enkripsi RSA yang sudah di rumuskan dan di hitung berdasarkan nilai yang ada.

Tabel. 2. Enkripsi RSA

Plaintext	J	A	B	A	R
Nilai ASCII	74	65	66	65	82
Rumus	74^79 mod 3337	65^79 mod 3337	66^79 mod 3337	65^79 mod 3337	82^79 mod 3337
Chipertext	1294	541	795	541	274

Berikut table dekripsi yang sudh dibuat berdasarkan table di atas.

Tabel 3. Dekripsi RSA

Chipertext	1294	541	795	541	274
Rumus	1294^1019 mod 3337	541^1019 mod 3337	795^1019 mod 3337	541^1019 mod 3337	274^1019 mod 3337
Hasil / ASCII	74	65	66	65	82
Plaintext	J	A	B	A	R

3. KESIMPULAN

Berisi berbagai kesimpulan yang diambil berdasarkan penelitian yang telah dilakukan.Berisi pernyataan singkat tentang hasil yang disarikan dari pembahasan. Saran dapat dituliskan pada bagian paling akhir.

Pada judul ini akan dijelaskan mengenai hasil penelitian Perbandingan/Studi komparasi algoritma kriptografi Vigenere Chiper dan Rivest shamir Adleman dalam mengenkripsi dan dekripsi data teks di dalam dokumen dengan ekstensi file(.txt) dan berapa lama waktu yang dibutuhkan dua algoritma tersebut untuk mengenkripsi dan dekripsi data teks.

No	Nama Sampel	Ukuran Asli	VC			
			ENKRIPSI	Ukuran	DEKRIPSI	Ukuran
1	File01	1Kb	0.06248	1Kb	0.00123	1Kb
2	File02	5 Kb	0.004	5 Kb	0.00385	5 Kb
3	File03	15 Kb	0.01526	15 Kb	0.01593	15 Kb
4	File04	68 Kb	0.06097	68 Kb	0.06431	68 Kb
5	File05	119 Kb	0.11281	119 Kb	0.11514	119 Kb
6	File06	128 Kb	0.16037	128 Kb	0.12746	128 Kb
7	File07	144 Kb	0.13614	144 Kb	0.16893	144 Kb
8	File08	159 Kb	0.16153	159 Kb	0.24421	159 Kb
9	File09	179 Kb	0.21317	179 Kb	0.2368	179 Kb
10	File10	212 Kb	0.24548	212 Kb	0.26701	212 Kb
Rata –Rata			**0.117221**		**0.15497375**	

Gambar 6. Hasil Penelitian Vigenere Chiper

Hasil porcobaan dengan 10 File dengan ukuran berbeda beda, bisa disimpulkan untuk hasil rata-rata Enkripsi : 0.117221 dan rata-rata

dekripsi : 0.15497375 dengan menggunakan satu kata kuci yang sama “jabbar”.

Nama Sampel	RSA			
	ENKRIPSI	Ukuran	DESKRIPSI	Ukuran
File01	0,00577	1 kb	0,05216	5 kb
File02	0,02869	23 Kb	0,27393	5 Kb
File03	0,08652	15 Kb	0,79228	69Kb
File04	0,50394	68 Kb	4,96505	318 Kb
File05	0,73183	199 Kb	10,42074	516 Kb
File06	0,89405	128 kb	6.87102	606kb
File07	1,27688	144 kb	6,78434	679 kb
File08	1,49985	159 kb	7,59035	746 kb
File09	1,85582	179 kb	8,47661	824 kb
File10	2,3636	212 kb	9,79799	996 kb
	0,924695		**5,461494444**	

Gambar 7 : Hasil Penelitian RSA

Hasil porcobaan dengan 10 File dengan ukuran berbeda beda, bisa disimpulkan untuk hasil rata-rata Enkripsi : 0,924695 dan rata-rata dekripsi : 5,461494444 dengan menggunakan kunci publik n : 3337, e : 79 dan d : 1019

Dari hasil rumusan masalah diatas bisa disimpulkan bahwa pembandingan al-goritma vigenere chiper dan rivest shamir adleman (RSA) adalah sebagai berikut Algoritma vigenere chiper lebih cepat proses enkripsi dan dekripsi karena al-goritma tidak ada perubahan jumlah kata dan ukuran file. Al-Goritma Rivest Shamir Adleman (RSA) untuk waktu enkripsi lebih cepat dan waktu pendekripsian lebih lama karena ada perubahan 4 (empat) kali lebih banyak penambahan jumlah kata dan ukuran.

PUSTAKA

Ahmat Sayuti. dkk. Perbandingan Performa Algoritma Hill Cipher dengan Rsa dalam Proses Enkripsi dan Dekripsi Text. 2019.Palembang.

Andro Elif, Achmad wahid, 2015. Implentasi Algoritma kriptografi Rivest Shamir Adleman dan Vigenere Chiper pada gambar 8 bit. Semarang.

Zainal Arifin (2009), Studi Kasus Penggunaan Algoritma RSA Sebagai Algoritma Kriptografi yang Aman, Program Studi Ilmu Komputer, FMIPA Universitas Mulawarman.

Chin-Chen Chang (2001), A New Encryption Algorithm for Image Cryptosystems, Department of Computer Science and Information Engineering, National Chung Cheng University, Chaiyi, Taiwan.

Dyani Mustikarini (2012), Implementasi Dan Analisa Pengiriman Data Menggunakan Algoritma Kriptografi RSA Pada Sistem Eucalyptus Private Cloud IAAS, Fakultas Teknik Komputer, Departemen Teknik Elektro, Universitas Indonesia.

Didin Mukodim (2002), Tinjauan Tentang Enkripsi Dan Dekripsi Suatu Teknik Pengamanan Data Dengan Penyandian RSA, Universitas Gunadarma.

Gunawan Indra, 2018, Kombinasi Al-goritma Caesar chiper dan algoritma RS. Sumatra Utara

Prisyafandiafif Charifa (2013), Penerapan Vigenere Cipher Untuk Aksara Arab, Program tudi Teknik Informatika, Sekolah Teknik Elektro danInformatika, Institut Teknologi Bandung.

Rini Wati Lumbangaol (2013), Aplikasi Pengamanan Gambar Dengan Algoritma Rivest-Shamir Adleman (RSA), Jurusan Teknik Informatika, STMIK Budidarma Medan.

Ivan Wibowo (2009), Penerapan Algoritma Kriptografi Asimetris RSA Untuk Keamanan Data Di Oracle, Teknik Informatika, Universitas Kristen Duta Wacana. M. Yuli Andri (2009), Implementasi Algoritma Kriptografi DES, RSA, Dan Algoritma Kompresi LZW Pada Berkas Digital, Program Studi Ilmu Komputer Fakultas Matematika Dan Ilmu Pengetahuan Alam, Universitas Sumatera Utara.