# PENERAPAN SISTEM KRIPTOGRAFI ENKRIPSI JAMAK DAN TANDA TANGAN DIGITAL DALAM MENDUKUNG KEAMANAN INFORMASI

**Phie Chyan[1)]**
[1]Program Studi Teknik Informatika, Fakultas Teknologi Informasi, Universitas Atma Jaya Makassar
Alamat e-mail: phie_chyan@lecture.uajm.ac.id

***ABSTRACT***

*The use of cryptographic techniques and digital signatures is widely applied as a method to secure confidentiality and authenticity of data such as sending data over the internet network. on cryptographic, data that intent to be secret is disguised by changing the original data to unreadable format while the digital signature is used to check the authenticity of the message according to the source. Both of these techniques have weaknesses, but by combining these two techniques it will make confidential data more secure in secrecy and authenticity. The main discussion of this research is to create a data security application by combining cryptographic techniques and the use of digital signatures. The algorithm used is a Multi- encryption algorithm consisting of a combination of substitution and transposition algorithms and el gamal algorithm for document verification using digital signatures. The process that is done is to encrypt the message either typed directly into the application or from the text file that is loaded into the application. The results of this study are applications designed to meet information security needs, both protection against the confidentiality of information and protection against counterfeiting and changing unwanted information.*

***Keywords:*** *Cryphtograph, Multi-encryption, Digital Signature*

## 1. PENDAHULUAN

Dewasa ini, perkembangan ilmu dan teknologi telah merambah ke segala aspek kehidupan termasuk dalam aspek komunikasi, saat ini terdapat banyak medium dan metode dalam mengirim dan menerima pesan yang pada intinya memberi kemudahan bagi tiap orang untuk dapat berkomunikasi satu sama lain. Di balik segala kecanggihan dan kemudahan yang ditawarkan terdapat satu hal krusial yang kadang kurang diperhatikan oleh pelaku komunikasi yaitu keamanan informasi. Keamanan informasi mencakup bagaimana menjaga kerahasiaan pesan sehingga orang yang tidak berhak tidak dapat memahami pesan yang terkirim. Salah satu cara untuk mempertahankan kerahasiaan dari pesan tersebut adalah dengan menyandikan pesan yang dikirim menjadi kode-kode yang tidak dipahami, sehingga bila ada pihak ketiga yang tidak berhak mengakses informasi tersebut akan kesulitan menterjemahkan isi pesan yang sebenarnya. Namun, aspek keamanan informasi tidak hanya semata-mata bagaimana membuat pesan menjadi rahasia tapi juga bagaimana melindungi pesan dari perubahan yang tidak terotorisasi, menjaga keamanan pesan hanya dengan menyandikan pesan tidak menutup kemungkinan untuk pesan tersebut dimodifikasi oleh pihak ke tiga. Untuk memperkuat kerahasiaan serta keaslian dari pesan tersebut, maka dikembangkanlah tanda tangan digital. Dengan adanya tanda tangan digital penerima pesan akan percaya bahwa pesan yang dikirimkan masih otentik dari pengirim asilnya. Kedua aspek keamanan informasi diatas merupakan layanan yang disediakan oleh kriptografi (Rinaldi,2006 :2).

Kriptologi berasal dari bahasa Yunani, yang terdiri dari dua kata yaitu *cryptos* dan *graphein*. *Cryptos* berarti rahasia, dan *graphein* berarti tulisan. Sehingga menurut bahasa, kriptologi berarti tulisan rahasia. Sedangkan definisi kriptografi adalah suatu ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi, integritas suatu data, serta otentifikasi data (Menezes,1996: 4). Enkripsi adalah sebuah proses penyandian yang melakukan perubahan

sebuah kode (pesan) dari yang bisa dimengerti (*plaintext*) menjadi sebuah kode yang tidak bisa dimengerti (*ciphertext*). Sedangkan proses kebalikannya untuk mengubah *ciphertext* menjadi *plaintext* disebut dekripsi. Proses enkripsi dan dekripsi memerlukan suatu mekanisme dan kunci tertentu.

Kerahasiaan dan kekuatan dari suatu algoritma kriptografi modern ditentukan oleh kunci yang digunakan dalam proses enkripsi dan dekripsi pesan, bukan dari algoritmanya sendiri yang pada dasarnya sudah diketahui oleh publik. Hal ini menimbulkan tantangan tersendiri dalam mengamankan pesan yang dikirim, dengan menggunakan algoritma yang umum diketahui oleh publik, seorang kriptanalis dapat menggunakan berbagai macam metode untuk memecahkan kunci yang digunakan oleh pengirim pesan berdasarkan karakteristik suatu algoritma kriptografi yang telah diketahui. Metode *known plaintext attack*, metode statistik atau *exhaustive search* merupakan beberapa metode umum yang digunakan dan terbukti cukup efektif dalam menyerang sebagian besar jenis algoritma kriptografi. Salah satu cara untuk memperkuat algoritma kriptografi adalah dengan melakukan *multiple encryption* atau enkripsi jamak. Dengan metode ini suatu pesan akan dienkripsi lebih dari satu kali dengan menggunakan algoritma kriptografi yang berbeda.

Berdasarkan uraian dan latar belakang masalah diatas maka penulis mengangkat kasus tersebut untuk diteliti dan membangun suatu aplikasi yang dapat mendukung penerapan sistem kriptografi menggunakan enkripsi jamak dan tanda tangan digital untuk digunakan dalam proses pengiriman dan penerimaan pesan.

Penelitian ini bertujuan untuk:

1. Membangun aplikasi penyandian pesan menggunakan algoritma kriptografi berenkripsi jamak dan tanda tangan digital
2. Menguji tingkat keamanan algoritma kriptografi enkripsi jamak dengan teknik kriptanalis yang digunakan pada kriptografi enkripsi tunggal.

## 2. TINJAUAN PUSTAKA

### 2.1 Kriptografi

Kriptografi (*cryptography*) berasal dari Bahasa Yunani, yaitu *cryptos* yang berarti *secret* (rahasia), sedangkan *graphien* artinya *writing* (tulisan). Jadi secara asal bahasa kriptografi berarti *secret writing* (tulisan rahasia). Kriptografi memiliki beberapa definisi. Salah satu definisi kriptografi adalah ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan, integritas data, serta otentifikasi (Menezes, 1996 :4) .

Di dalam kriptografi, akan sering ditemukan berbagai istilah (terminologi). Adapun istilah-istilah yang kerap kali digunakan adalah sebagai berikut.

1. Pesan, *Plaintext*, dan *Ciphertext*

Pesan adalah data ataupun suatu informasi yang dapat dibaca dan dimengerti maknanya. Dan nama lain untuk pesan ialah *plaintext*, atau teks jelas. *Ciphertext* adalah suatu bentuk pesan yang bersandi. Disandikannya suatu pesan adalah agar pesan tersebut tidak dapat dimengerti oleh pihak lainnya.

Contoh plaintext

> Ketika saya berjalan – jalan di pantai, saya menemukan banyak sekali kepiting yang merangkak menuju ke laut. Mereka adalahn anak kepiting yang baru saja menetas dari dalam pasir.

Contoh Ciphertext

> Κετικα σαψα βερφαλαν □ φαλαν δι πανται, σα ψα μενεμυκαν βανψακ σεκαλι κεπιτινγ ψανγ με ρανγκακ μενυφυ κε λαυτ. Μερεκα αδαλαην ανα κ κεπιτινγ ψανγ βαρυ σαφα μενεταση δαρι δαλαμ πασιρ.

2. Pengirim dan Penerima

Suatu aktivitas komunikasi data, akan melibatkan pertukaran antara dua entitas, yakni pengirim dan penerima. Pengirim adalah entitas yang mengirim pesan kepada entitas lainnya. Sedangkan penerima adalah entitas yang menerima pesan. (Rinaldi, 2006 : 4). Suatu pengiriman pesan, pengirim tentu menginginkan pesan dapat dikirim secara aman. Untuk mengamankannya, pengirim biasanya akan menyandikan pesan yang dikirimkan tersebut.

3. Enkripsi dan Dekripsi

Suatu proses untuk menyandikan *plaintext* menjadi *ciphertext* disebut enkripsi (*encryption*). Sedangkan proses pengembalian dari *ciphertext* manjadi *plaintext* dinamakan dekripsi (*decription*) (Rinaldi, 2006 : 4). Enkripsi dan dekripsi merupakan suatu pesan yang memetakan elemen-elemen antara kedua himpunan tersebut. Misalkan *P* adalah himpunan *plaintext*, dan *C* adalah himpunan *ciphertext*, maka fungsi enkripsi *E* memetakan *P* ke *C*, ditulis $E(P) = C$. Dan fungsi dekripsi *D* memetakan *C* ke *P*, ditulis $D(C) = P$.

4. Cipher dan Kunci

Algoritma kriptografi disebut juga *cipher* yaitu aturan atau fungsi matematika yang digunakan untuk enkripsi dan dekripsi. Beberapa *cipher* memerlukan algoritma yang berbeda untuk enkripsi dan dekripsi (Stalling, 2005: 30).

Untuk menjaga kerahasiaan pengiriman pesan dalam kriptografi modern dibutuhkan kunci. Kunci (*key*) adalah parameter yang digunakan untuk mentransformasi proses pengenkripsian dan pendekripsian pesan. Biasanya, kunci berupa deretan bilangan maupun string. Dengan menggunakan kunci *K* maka proses enkripsi dan dekripsi dapat ditulis sebagai $EK(P) = C$ dan $DK(C) = P$, dan kedua fungsi tersebut memenuhi $DK(EK(P)) = P$.

5. Sistem Kriptografi Kunci Simetri dan Tak Simetri

Sistem kriptografi merupakan kumpulan yang terdiri dari *plaintext*, *ciphertext*, kunci, enkripsi serta dekripsi.(Stinson, 2006 :1) .

Berdasarkan kunci yang digunakan dalam proses enkripsi dan dekripsi, kriptografi dapat dibedakan menjadi kriptografi kunci simetri dan kriptografi kunci tak simetri. Kriptografi kunci tak simetri ini sering disebut dengan kriptografi kunci publik. Kriptografi kunci simetri, sering disingkat menjadi kriptografi simetri, kunci yang digunakan pada proses enkripsi dan dekripsi adalah sama. Oleh karena itu, sebelum saling berkomunikasi kedua belah pihak harus melakukan kesepakatan dalam menentukan kunci yang akan digunakan. Keamanan menggunakan sistem ini terletak pada kerahasiaan kunci yang akan digunakan. Sedangkan dalam sistem kriptografi kunci publik, kunci yang digunakan dalam proses enkripsi dan dekripsi berbeda. Sistem ini terdapat dua buah kunci, yaitu kunci publik dan kunci privat. Kunci publik digunakan untuk proses enkripsi, dan kunci privat digunakan untuk mendekripsikan pesan. Kunci publik bersifat tak rahasia, sedangkan kunci privat hanya boleh diketahui oleh penerima pesan.

### 2.1.1 Tujuan Kriptografi

Tujuan dari kriptografi adalah sebagai berikut.

1. Kerahasiaan Data (*confidentiality*), merupakan suatu layanan yang digunakan untuk menjaga isi dari informasi dari pihak pihak yang tak berhak untuk mendapatkannya.
2. Integritas Data (*data integrity*), merupakan suatu layanan dimana menjamin bahwa pesan masih asli, dan belum dimanipulasi oleh pihak - pihak yang tidak berhak. Realisasi layanan ini di dalam kriptografi, adalah dengan menggunakan tanda tangan digital.
3. Otentifikasi (*authentication*), merupakan suatu layanan yang berhubungan dengan identifikasi. Misalnya, mengidentifikasi suatu kebenaran pihak-pihak yang berkomunikasi (entitas) maupun mengidentifikasi kebenaran sumber pesan. Sama seperti poin (b), di dalam kriptografi, layanan ini diwujudkan dengan menggunakan tanda tangan.
4. Nirpenyangkalan (*non-repudiation*), merupakan suatu layanan untuk mencegah entitas yang saling berkomunikasi melakukan penyangkalan. Misalkan salah satu dari entitas menyangkal telah mengirim maupun menerima pesan.

### 2.1.2 Jenis Kriptografi

Dalam ilmu kriptografi suatu pesan yang akan dirahasiakan atau disandikan disebut dengan *plaintext*, sedangkan pesan yang telah disandikan sehingga tidak bermakna lagi yang bertujuan agar pesan

tidak dapat dibaca oleh pihak yang tidak berhak disebut *ciphertext*. Lalu dalam ilmu kriptografi terdapat istilah enkripsi dan deskripsi. Enkripsi adalah proses menyandikan *plaintext* menjadi *ciphertext*. Sedangkan proses mengembalikan *ciphertext* menjadi *plaintext* semula disebut sebagai dekripsi.

Secara umum berdasarkan penggunaan kuncinya, algoritma kriptografi dibagi menjadi dua bagian, yaitu :

1. Algoritma simetris

Algoritma ini sering juga disebut algoritma klasik karena memakai kunci yang sama untuk proses enkripsi dan deskripsinya. Algoritma simetri sudah ada lebih dari 4000 tahun yang lalu. Pengiriman pesan mengguanakan algoritma tersebut mengharuskan si penerima pesan untuk mengetahui kunci dari pesan tersebut agar bisa mendekripsi pesan yang dikirim. Keamanan dari pesan tersebut yang menggunakan algoritma itu tergantung pada kunci. Jika kunci tersebut diketahui oleh orang lain, maka orang lain tersebut bisa melakukan enkripsi dan dekripsi terhadap pesan tersebut. Algoritma yang memakai kunci simetri di antaranya adalah DES, RC2, RC4, RC5, RC6, AES, dan sebagainya

2. Algoritma Asimetris

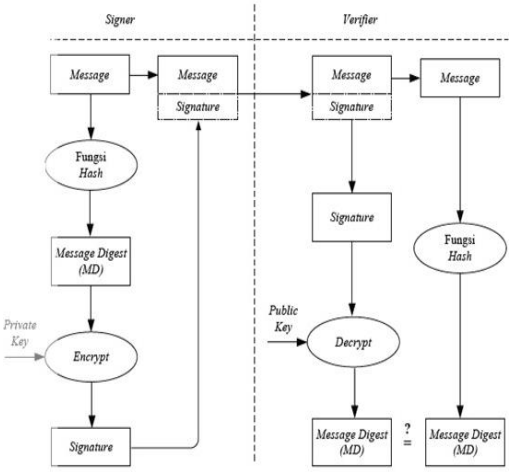
Algoritma asimetri sering juga disebut algoritma kunci publik. Artinya, kata kunci yang digunakan untuk melakukan enkripsi dan deskripsinya berbeda. Pada algoritma asimetri, kunci terbagi menjadi dua bagian yang saling terkait secara matematis:

a. Kunci umum (*public key*) adalah kunci yang boleh diketahui semua orang (dipublikasikan) dan tidak bersifat rahasia
b. Kunci pribadi (*private key*) adalah kunci yang dirahasiakan (hanya boleh diketahui oleh satu orang yang bersangkutan).

Kunci-kunci tersebut saling berhubungan satu dengan yang lainnya. Penggunaan kunci umum memungkinkan seseorang untuk bisa mengenkripsi pesan, tetapi tidak mendekripsinya. Hanya orang yang memiliki kunci pribadi yang mendekripsi pesan tersebut. Algoritma asimetris bisa mengirim pesan dengan lebih aman daripada algoritma simetris terutama karena tidak perlu mendistribusikan kunci pada saluran tidak aman seperti pada algoritma simetri. Algoritma yang memakai kunci umum di antaranya adalah DSA, RSA, DH, ECC, dan sebagainya

## 2.2 Teminologi Tanda Tangan Digital

Tandatangan digital tujuannya mirip dengan tandatangan yang dihasilkan tulisan tangan. Tujuannya untuk memberikan suatu alat yang digunakan oleh entitas untuk mengikat identitasnya menjadi satu bagian dari informasi (Menezes et al. 2010). Sistem kriptografi kunci-publik cocok untuk pemberian tandatangan digital menggunakan fungsi *hash* (Munir, 2005). Penandatanganan pesan dengan cara mengenkripsinya selalu memberikan dua fungsi yaitu kerahasiaan dan otentikasi. Pada beberapa kasus, yang dibutuhkan hanya otentikasi saja, sehingga tandatangan digitaldengan sistem kunci-publik ini dapat menyelesaikan masalah *non-repudiation*. Diagram tandatangan digital menggunakan fungsi *hash* ditunjukkan pada Gambar 1.




Gambar 1. Diagram tanda tangan digital menggunakan fungsi *hash* satu arah (Munir 2006).

Tandatangan digital yang termasuk ke dalam standar DSS, yaitu:

1. DSA

DSA tidak dapat digunakan untuk enkripsi,tetapi dikhususkan untuk tandatangan digital. Fungsi utama DSA adalah:

- Pembentukantanda tangan (*signature generation*).
- Pemeriksaan keabsahan tanda tangan (*signature verifying*).

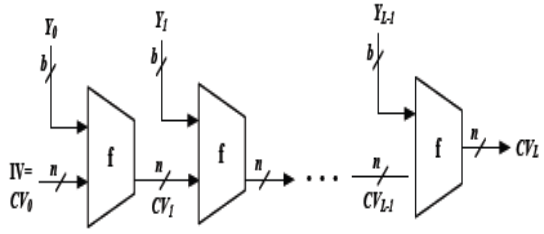
Tingkat keamanan DSA berdasarkan pada kemampuan komputasi dari logaritma diskret dalam subgrup urutan prima Zp*.

2. RSA

RSA melibatkan kunci publik dan kunci privat. Keamanan algoritme RSA terletak pada sulitnya memfaktorkan bilangan besar menjadi faktor-faktor prima. Pemfaktoran dilakukan untuk memperoleh kunci privat. Selama pemfaktoran bilangan besar menjadi faktor-faktor prima belum ditemukan, maka keamanan RSA tetap terjamin.

### 2.3 Fungsi Hash

Fungsi *hash* adalah fungsi yang menerima masukan *string* yang panjangnya sembarang dan mengonversinya menjadi *string* keluaran yang panjangnya tetap (Munir 2006). Keluaran fungsi *hash* disebut juga nilai *hash* atau pesan ringkas atau *message digest*(MD). Aplikasi fungsi *hash* antara lain untuk memverifikasi kesamaan salinan suatu arsip dengan arsip aslinya yang tersimpan di dalam sebuah *database* terpusat. Fungsi *hash* satu-arah (*One-way Hash*) adalah fungsi *hash* yang bekerja dalam satu arah, pesan yang sudah diubah menjadi MD tidak dapat dikembalikan lagi menjadi pesan semula.Struktur umum fungsi *hash* ditunjukkan pada Gambar 2.




Gambar 2. Struktur umum fungsi hash

Struktur pada gambar tersebut merupakan proses iterasi fungsi *hash*, yang ditemukan oleh Merkle, dan merupakan struktur fungsi *hash* yang banyak digunakan saat ini. Fungsi *hash* menerima sebuah masukan pesan dan membaginya ke sejumlah *L* blok dengan masing-masing blok panjangnya *b* bit (*Y0* sampai *YL-1*). Jika diperlukan, blok terakhir (*final block*) dapat digabungkan (*padded*) dengan sejumlah bit. Blok terakhir juga merupakan jumlah panjang masukan untuk fungsi *hash*. Algoritma *hash* melibatkan penggunaan iterasi fungsi kompresi, *f*, yang mengambil dua *input* (*n*-bit *input* dari langkah sebelumnya, yang disebut *chaining variabel* (*CV*), dan sebuah *b*-bit blok) dan menghasilkan *outputn*-bit. Pada awal proses *hashing*, *CV* yang memiliki nilai awal yang *specified* sebagai bagian dari algoritma. Nilai akhir dari *CV* adalah nilai *hash* atau MD (Stalling, 2005).

Fungsi *hash* terdiri atas beberapa jenis, pada penelitian ini digunakan hanya tiga contoh fungsi *hash* yaitu SHA-256, SHA-384 dan Tiger. Tiger dirancang oleh Ross Anderson dan Eli Biham pada tahun 1996. Tiger dirancang untuk dapat bekerja pada mesin 64 bit tapi dapat juga berkerja pada mesin 32 bit (Ismaliansyah 2006). Spesifikasi dari ketiga fungsi *hash* tersebut ditunjukkan pada Tabel1

Tabel 1. Spesifikasi fungsi *hash* SHA-256, SHA-384 dan Tiger

| Tipe hash | Spesifikasi Ukuran (bits) | | | |
|---|---|---|---|---|
| | Pesan | Blok | Word | MD |
| SHA-256 | $<2^{64}$ | 512 | 32 | 256 |
| SHA-384 | $<2^{128}$ | 1024 | 64 | 384 |
| TIGER | $<2^{64}$ | 512 | 64 | 192 |

## 3. METODOLOGI PENELITIAN

Untuk mencapai tujuan penelitian maka kegiatan penelitian dibagi dalam beberapa tahap yaitu 1) Studi literatur, 2) Pengumpulan data, 3) Perancangan Sistem, 4) Implementasi sistem aplikasi, dan 5) Analisis sistem dan evaluasi (chyan, 2018; chyan dan Marwi, 2014)

### 3.1 Studi Literatur

Studi literatur dilakukan untuk mendapatkan dasar teoritis dan juga metode analisis terkini agar diperoleh hasil yang sesuai dengan perkembangan dalam bidang ilmu teknologi informasi. Kegiatan yang dilakukan pada tahapan ini adalah mengumpulkan dan mempelajari artikel, jurnal dan referensi lain nya yang mutakhir berkaitan dengan kriptografi dan berbagai algoritma-algoritma kriptografi & modern termasuk didalamnya penggunaan tanda tangan digital dan fungsi hash.

### 3.2. Pengumpulan Data

Mengumpulkan data yang berkenaan dengan data pendukung dalam proses implementasi aplikasi penyandian dan tanda tangan digital yang akan dijalankan. Data yang dikumpulkan berupa berbagai algoritma kriptografi yang akan diterapkan dalam penyandian pesan.

### 3.3 Perancangan Sistem

Pada tahap ini dilakukan perancangan sistem aplikasi berbasis GUI yang digunakan sebagai *user interface*. Disini pesan yang disandikan dapat langsung diketik ke dalam interface maupun dalam bentuk file yang menjadi masukan bagi aplikasi. Kemudian pengguna dapat memilih jenis algoritma yang akan digunakan (dapat menggunakan enkripsi tunggal atau jamak). Hasil dari proses akan menampilkan pesan yang sudah terenkripsi dan dapat di output ke layar atau dalam file.

### 3.4 Implementasi Sistem Aplikasi

Pada tahap ini dilakukan implementasi secara keseluruhan dari desain sistem aplikasi yang dikembangkan**.**

## 4. HASIL DAN PEMBAHASAN

### 4.1 Kebutuhan Sistem

Kebutuhan sistem pada aplikasi enkripsi dan dekripsi email ini meliputi beberapa hal, diantaranya adalah:

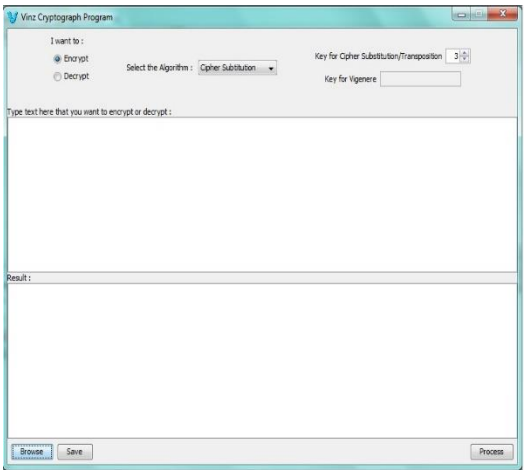
1. Komputer PC dengan spesifikasi standars
2. Netbeans 7.0, sebagai perangkat lunak dari aplikasi
3. Browser, dapat menggunakan Mozilla Firefox ataupun Google Chrome

### 4.2 Perancangan Sistem

Perancangan sistem perangkat lunak yang dibuat meliputi perancangan model perangkat lunak meliputi pembuatan antarmuka aplikasi dimana pengguna dapat mengekripsi dan mendekripsi pesan, serta memeriksa signature dari pesan yang diterima untuk memeriksa keaslian pesan.

### 4.3 Pengujian implementasi sistem

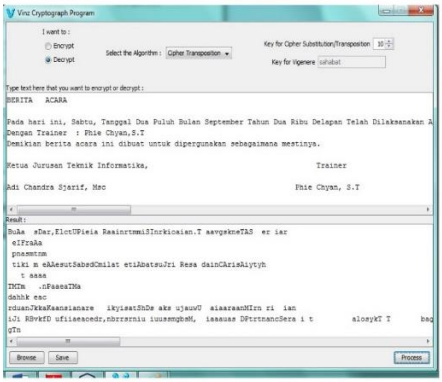
Langkah awal untuk menjalankan aplikasi enkripsi dan dekripsi pesan ini adalah membuka Netbeans 7.0. Tampilan awal dari program ini ditunjukkan pada Gambar 3




Gambar 3. Tampilan Menu Utama

#### 4.3.1 Enkripsi Pesan

Untuk melakukan proses mengenkripsi pesan, pengguna dapat langsung menulis pada text field yang disediakan dalam interface program atau dapat juga untuk mengenkripsi keseluruhan pesan pada sebuah file teks, hal ini dapat dilakukan dengan mengklik tombol browse untuk memuat isi teks yang terdapat pada file, setelah itu pengguna dapat memilih jenis algoritma yang digunakan, untuk menerapkan enkripsi jamak pengguna dapat memilih lebih dari 1 algoritma kriptografi untuk mengenkripsi pesan kemudian setelah itu klik tombol proses untuk memperoleh hasilnya yang ditampilkan pada text field, hasil yang ditampilkan dapat disimpan kembali pada file teks, proses enkripsi suatu pesan seperti terlihat pada gambar 4.

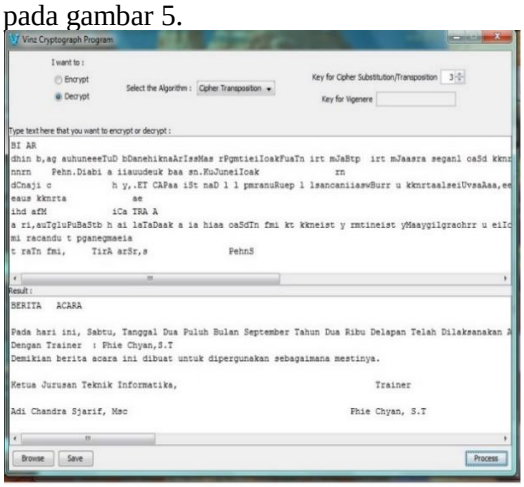



Gambar 4. Proses Enkripsi Pesan

#### 4.3.2 Dekripsi Pesan

Seperti halnya dalam proses enkripsi, pengguna dapat langsung menulis pada text

area yang disediakan dalam interface program atau untuk mendekripsi keseluruhan pesan pada sebuah file teks, hal ini dapat dilakukan dengan mengklik tombol browse untuk memuat isi teks yang terdapat pada file, setelah itu pengguna dapat memilih jenis algoritma yang digunakan, untuk menerapkan enkripsi jamak pengguna dapat memilih lebih dari 1 algoritma untuk mengdekripsi pesan kemudian setelah itu klik tombol proses untuk memperoleh hasilnya yang ditampilkan pada text field, hasil yang ditampilkan dan dapat disimpan kembali (ekspor) pada dokumen file teks. Proses dekripsi suatu pesan seperti terlihat pada gambar 5.




Gambar 5. Proses Dekripsi Pesan

### 4.3.3 Tanda Tangan Digital

Penerapan sistem kriptografi ElGamal pada tanda tangan digital terdapat pada proses pembentukan kunci, penandatanganan, serta verifikasi. Perhitungannya ketiga proses tersebut berdasar pada masalah logaritma diskret pada grup $\mathbb{Z}$p*. Proses pembuatan tanda tangan digital pada suatu dokumen dengan menggunakan algoritma ElGamal adalah sebagai berikut:

1. Pembentukan kunci yang dilakukan oleh pengirim pesan. Langkah-langkah pembentukan kunci meliputi:
   a. Pilih bilangan prima *p*.
   b. Pilih dua buah bilangan acak g dan *s*, dimana $s \in \{1,2,3,\dots,p-1\}$
   c. Hitung $v = g^s mod\ p$
   d. Publikasikan nilai *p*,,dan *v*. Namun nilai *s* dirahasiakan.

   Dari proses pembentukan kunci, diperoleh kunci publik (*p*,, *v*) dan kunci *a*.
2. Proses Penandatanganan. Proses penandatanganan dilakukan oleh pengirim pesan. Adapun langkah-langkah penandatanganan suatu dokumen adalah sebagai berikut.
   a. Menghitung nilai *hash* (*MD*) suatu dokumen dengan langkah sebagai berikut.
      1) Memotong pesan *m* menjadi blok-blok pesan, sehingga satu blok adalah satu karakter pesan.
      2) Mengkonversikan masing-masing karakter yang telah diperoleh ke dalam kode ASCII, sehingga diperoleh *plaintext* sebanyak *n* bilangan, yaitu *m1, m2 ..., mn.*
      3) Menjumlahkan *plaintext* yang telah dikonversi ke dalam kode ASCII. Lalu melakukan perhitungan berikut: $MD = [(m_1 + m_2 + \cdots + m_n) \mod 256] + 1$.
   b. Menghitung nilai kriptografis suatu dokumen. Langkah – langkah dalam menghitung nilai kriptografis adalah sebagai berikut.
      1) Memilih nilai *e*, yang relatif prima dengan *p*-1
      2) Menghitung: $R = g^e mod\ p$ dan $T = (MD - sR)e^{-1} mod\ (p-1)$. dan.
      3) Membubuhkan tanda tangan (*R*, *T*) pada dokumen. (*R*, *T*) inilah yang dinamakan nilai kriptografis (tanda tangan digital).
   c. Mengirimkan dokumen yang telah dibubuhi dengan tanda tangan digital.
3. Proses verifikasi tanda tangan digital. Pada proses verifikasi ini, dilakukan oleh pihak penerima pesan. Langkah – langkah dalam proses verifikasi tanda tangan adalah sebagai berikut.
   a. Menghitung nilai MD.
   b. Mengecek bahwa 1≤ R ≤ p-1 terpenuhi
   c. Menghitung $v^R R^T$ mod p.
   d. Dan diperiksa bahwa $v^R R^T \equiv g^{MD}$ mod p .

Jika perhitungan mod *p* terpenuhi, maka dokumen yang dikirimkan dikatakan masih asli atau berasal dari pengirim yang sebenarnya.

### 4.4 Hasil Uji Kriptanalisis

Dengan menggunakan salah satu metode kriptanalis yaitu *exhaustive key search*, didapatkan hasil pengujian yang dapat menggambarkan kekuatan algoritma kriptografi jamak dibandingkan dengan algoritma kriptografi tunggal, perbedaan dari algoritma kriptografi tunggal terhadap algoritma kriptografi jamak adalah dari panjang key yang digunakan, pada algoritma kriptografi jamak, *key* yang digunakan mempunyai ukuran bit yang lebih panjang sehingga dari tingkat keamanan yang dihasilkan jauh lebih tinggi, berikut pada tabel 2 memperlihatkan hasil pengujian menggunakan metode kriptanalis *exhaustive key search.*

Tabel 2 Hasil pengujian kriptanalis menggunakan exhaustive key search

| Ukuran kunci | Jumlah kemungkinan kunci | Lama waktu untuk $10^6$ percobaan per detik | Lama waktu untuk $10^{12}$ percobaan per detik |
|---|---|---|---|
| 16 bit | $2^{16} = 65536$ | 32.7 milidetik | 0.0327 mikrodetik |
| 32 bit | $2^{32} = 4.3 \times 10^9$ | 35.8 menit | 2.15 milidetik |
| 56 bit | $2^{56} = 7.2 \times 10^{16}$ | 1142 tahun | 10.01 jam |
| 128 bit | $2^{128} = 4.3 \times 10^{38}$ | $5.4 \times 10^{24}$ tahun | $5.4 \times 10^{18}$ tahun |

## 5. KESIMPULAN

Berdasarkan hasil penelitian dan pembahasan yang telah dilakukan, dapat diambil beberapa kesimpulan sebagai berikut.

1. Kerahasiaan pesan dapat dilindungi dengan menerapkan teknik kriptografi untuk mengenkripsi pesan menjadi bentuk yang tidak terbaca bagi orang yang tidak berhak untuk membacanya.
2. Algoritma kriptografi enkripsi jamak memberikan tingkat perlindungan yang lebih tinggi dari enkripsi tunggal karena menggunakan beberapa algoritma yang berbeda dalam proses enkripsi pesan yang bertingkat.

## 6. DAFTAR PUSTAKA


[1] Ismaliansyah MK., 2006. Kriptanalisis http://www.informatika.org/~rinaldi/Kriptografi/2006 2007/Makalah2/Makalah-057.pdf, [25 Mei 2013].

[2] Menezes A, Oorcshot. P, and Vanstone. S, 2010. Handbook of Applied Cryptography, Taylor & Francis publisher

[3] Munir, R, 2005. Penggunaan Tanda Tangan Digital Untuk Menjaga Integritas Berkas Perangkat Lunak, Prosiding Seminar Nasional: SNATI UII Yogyakarta, 18 Juni 2005 page 87-95

[4] Munir, R., 2006. Kriptografi, Penerbit informatika Bandung

[5] Rasyid MF. 2007. Tanda Tangan Digital Majemuk dengan Kunci Publik Tunggal dengan Algoritma RSA dan El Gamal. http://www.informatika.org/~rinaldi/Kriptografi/2007-2008/Makalah2/MakalahIF50542007-B-039.pdf, [25 Mei 2013].

[6] Chyan, P., 2018. Metode Modifikasi Histogram Untuk Peningkatan Kontras dan Kecerahan Citra. Journal Scientific and Applied of Informatics (JSAI), 1(3), pp.76-80.

[7] Chyan, P. and Marwi, H.C., 2014. Sistem Temu Balik Citra Menggunakan Ekstraksi Fitur Citra Dengan Klasifikasi Region Untuk Identifikasi Objek. TEMATIKA, Journal of Informatics and Information Systems, 2(2), pp.63-72.

[8] Stallings, Williams, 2005. Cryptography and Network Security Principles and Practices 4th edition. New Jersey: Pearson

[9] Stinson, D.R. 2006. Cryptography Theory and Practice. Florida: CRC Press