**ENKRIPSI TEKS MENGGUNAKAN TRANSPOSISI BINER DENGAN PENDEKATAN OCTAGRAM**

**PROPOSAL TUGAS AKHIR**



**Oleh:**

**AHMAD RAMLI**

**NIM. 17 615 023**

**KEMENTERIAN RISET TEKNOLOGI DAN PENDIDIKAN TINGGI**

**POLITEKNIK NEGERI SAMARINDA**

**JURUSAN TEKNOLOGI INFORMASI**

**PROGRAM STUDI TEKNIK INFORMATIKA**

**2019**

HALAMAN PERSETUJUAN

**ENKRIPSI TEKS MENGGUNAKAN TRANSPOSISI BINER DENGAN PENDEKATAN OCTAGRAM**



Nama Mahasiswa : Ahmad Ramli

NIM : 17 615 023

Jurusan : Teknologi Informasi

Program Studi : Teknik Informatika

Jenjang Studi : Diploma III

Dipromosikan oleh :

**Rihartanto, ST.,M.Si**

**NIP. 19711205 200312 1 001**

Kata Pengantar

Puji syukur alhamdulillah penulis panjatkan kehadirat Allah SWT yang telah melimpahkan rahmat-Nya serta hidayah-Nya sehingga penulis bisa menyelesaikan Proposal Tugas Akhir dengan judul Enkripsi Teks Menggunakan Transposisi Biner dengan Pendekatan *Octagram*.

Sholawat serta salam semoga selalu tercurahkan kepada Nabi Muhammad SAW beserta keluarga dan para sahabatnya hingga pada umatnya sampai akhir zaman.

Proposal Tugas Akhir ini disusun untuk memenuhi salah satu syarat dalam menyelesaikan jenjang pendidikan program Diploma III di Jurusan Teknologi Informasi, Politeknik Negeri Samarinda.

Dalam proses penyusunan Proposal Tugas Akhir ini, penulis mendapatkan banyak sekali bantuan, bimbingan serta dukungan dari berbagai pihak, sehingga dalam kesempatan ini penulis juga bermaksud menyampaikan rasa terima kasih kepada:

1. Kedua orang tua dan keluarga yang selalu memberi dukungan moral dan materi.
2. Ansar Rizal, ST., M.Kom. selaku Ketua Jurusan Teknologi Informasi Politeknik Negeri Samarinda
3. Rihartanto ST., M.Si selaku promotor yang telah membimbing hingga terselesaikannya proposal tugas akhir ini.
4. Staf dosen, staf teknisi, dan staf administrasi jurusan yang telah membantu dalam segala hal yang berkaitan dengan perkuliahan.
5. Semua sahabat dan rekan-rekan mahasiswa jurusan Teknologi Informasi yang ikut memberi saran dan masukan.
6. Serta semua pihak lain yang ikut terlibat dalam penyelsaian Proposal Tugas Akhir ini

Semoga Allah SWT memberi balasan yang setimpal kepada semuanya.

Penulis berharap skripsi yang telah disusun ini bisa memberikan sumbangsih untuk menambah pengetahuan para pembaca, dan akhir kata, dalam rangka perbaikan selanjutnya, penulis akan terbuka terhadap saran dan masukan dari semua pihak karena penulis menyadari skripsi yang telah disusun ini memiliki banyak sekali kekurangan.

Samarinda, 09 Desember 2019

Ahmad Ramli

DAFTAR ISI

[HALAMAN PERSETUJUAN i](#_Toc26791466)

[Kata Pengantar i](#_Toc26791467)

[DAFTAR ISI iii](#_Toc26791468)

[DAFTAR GAMBAR iv](#_Toc26791469)

[BAB I Pendahuluan 1](#_Toc26791470)

[1.1 Latar Belakang 1](#_Toc26791471)

[1.2 Rumusan Masalah 2](#_Toc26791472)

[1.3 Tujuan Penelitian 2](#_Toc26791473)

[1.4 Batasan Masalah 2](#_Toc26791474)

[1.5 Manfaat Penelitian 2](#_Toc26791475)

[BAB II TINJAUAN PUSTAKA 3](#_Toc26791476)

[2.1 Kajian Ilmiah 3](#_Toc26791477)

[2.2 Dasar Teori 5](#_Toc26791478)

[2.2.1 Informasi dan Data 5](#_Toc26791479)

[2.2.2 Kriptografi 6](#_Toc26791480)

[2.2.3 Octagram 9](#_Toc26791481)

[2.3 Mean Absolute Error (MAE) dan Mean Square Error (MSE) 11](#_Toc26791482)

[2.4 *Entropy* 12](#_Toc26791483)

[2.4.1 Menentukan Peluang Kemunculan 13](#_Toc26791484)

[2.4.2 Mencari *Entropy* 13](#_Toc26791485)

[BAB III METODE PENELITIAN 14](#_Toc26791486)

[3.1 Kerangka Konsep Penelitian 14](#_Toc26791487)

[3.2 Metodologi Penelitian 16](#_Toc26791488)

[3.2.1 Implementasi 17](#_Toc26791489)

[3.2.2 Pengujian 18](#_Toc26791490)

[3.2.3 Waktu dan Tempat Penelitian 18](#_Toc26791491)

[RENCANA JADWAL PENGERJAAN 19](#_Toc26791492)

[DATAR PUSTAKA 20](#_Toc26791493)

DAFTAR GAMBAR

|  |  |
| --- | --- |
| Gambar 2.1 Teknik Blocking…………………………………………………. | 7 |
| Gambar 2.2 Teknik Pemampatan…………………………………………….. | 8 |
| Gambar 2.3 Teknik Permutasi………………………………………………… | 9 |
| Gambar 2.4 Octagram Pada Masa Islam……………………………………. | 10 |
| Gambar 2.5 Heptagram, Octagram, dan Nonagram……………………….. | 11 |
| Gambar 3.1. Kerangka Konsep Penelitian…………………………...……… | 14 |
| Gambar 3.2. Teknik Permutasi ……………………………………………… | 15 |
| Gambar 3.3. Octagram…………………………........................................... | 16 |
| Gambar 3.4. Metodologi Penelitian…………………………………………... | 16 |

BAB I  
Pendahuluan

1.1 Latar Belakang

Blablabla…

1.2 Rumusan Masalah

Blablabla…

1.3 Tujuan Penelitian

Blablabla…

1.4 Batasan Masalah

Blablabla

1.5 Manfaat Penelitian

Blablbla.

BAB II  
TINJAUAN PUSTAKA

2.1 Kajian Ilmiah

Hasil penelitian yang telah dilakukan para peneliti dapat dijadikan dasar atau kajian untuk mempermudah dalam melakukan penelitian. Termasuk juga penelitian ini. Beberapa di antaranya adalah penelitian dengan judul Teknik Pemecahan Kunci Algoritma Rivest Shamir Adleman (RSA) dengan Metode Kraitchik. Peneliti mencari kunci privat algoritma RSA dengan memfaktorkan kunci publik n dengan Metode Kraitchik, kemdudian dilihat efisiensi waktu pemfaktorannya. Hasil penelitian memperlihatkan, bahwa semakin besar selisih antara factor kunci p dan q, maka semakin besar pula waktu pemfaktorannya. Pemfaktoran kunci publik (n) sebesar 19 digit (152 bit) dengan selisih factor kunci (p-q) = 22641980 membutuhkan waktu 93,6002 ms lebih cepat dibandingkan dengan panjang kunci 15 digit (120 bit) dengan selisih faktor kunci (p-q) = 23396206 yang membutuhkan waktu selama 5850,0103 ms. Faktor lain yang juga mempengaruhi adalah Gcd(p-1,q-1), panjang kunci dan faktor prima (p-1),(q-1). (Muchlis, Budiman, & Rachmawati, 2017)

Penelitian dengan judul Teknik Penyembunyian dan Enkripsi Pesan pada Citra Digital dengan Kombinasi Metode LSB dan RSA. Penelitian ini mengusulkan kombinasi teknik steganografi dan kriptografi menggunakan metode LSB – RSA. RSA merupakan teknik kriptografi yang populer dapat diterapkan pada citra digital. Nilai piksel citra digital hanya berkisar 0 sampai 255. Hal ini membuat kunci yang digunakan dalam RSA cukup terbatas sehingga kurang aman. Dalam penelitian ini diusulkan untuk mengkonversi nilai piksel citra menjadi 16 bit sehingga kunci yang digunakan dapat lebih bervariasi. Hasil eksperimen membuktikan adanya peningkatan keamanan serta nilai imperceptibility yang tetap terjaga. Hal ini dibuktikan dengan hasil PSNR 57.2258dB, MSE 0.1232dB. Metode ini juga tahan terhadap serangan salt and pepper. (Handoyo, Setiadi, Rachmawanto, Sari, & Susanto, 2018)

Dan penelitian dengan judul Mengukur Kecepatan Enkripsi dan Dekripsi Algoritma RSA pada Pengembangan Sistem Informasi Text Security. Objek penelitian ini adalah proses implementasi algoritma kriptografi RSA pada nilai parameter n dengan ukuran 1024 bit dan 2048 bit. Proses yang diamati adalah kompleksitas waktu yang dihasilkan oleh instruksi enkripsi dan dekripsi. Tahap-tahap yang dilakukan adalah studi pendahuluan, mengumpulkan data, menganalisis kebutuhan, pengembangan dan pengujian sistem informasi serta penarikan kesimpulan. Hasil pengujian menyatakan algoritma RSA 1024 bit memiliki rata-rata kecepatan enkripsi sebesar 352.488 nano second dan rata-rata kecepatan dekripsi sebesar 109.347.917 nano second, sedangkan pada algoritma RSA 2048 bit memiliki rata-rata kecepatan enkripsi sebesar 1.772.900 nano second dan rata-rata kecepatan dekripsi sebesar 775.282.334 nano second. (Wulansari, Alamsyah, Setyawan, & Susanto, 2016)

2.2 Dasar Teori

2.2.1 Kriptografi

Kriptografi berasal dari bahasa Yunani yaitu *“cryptos”* yang berarti rahasia dan *“graphein”* yang berarti tulisan. Dapat dikatakan kriptografi berarti suatu ilmu yang mempelajari penulisan secara rahasia dengan teknik matematika tertentu.

Kriptografi adalah ilmu mengenai teknik enkripsi dimana teks asli (plaintext) diubah menggunakan suatu kunci enkripsi menjadi teks acak yang sulit dibaca (ciphertext) oleh seseorang yang tidak memiliki kunci dekripsi. Probabilitas mendapat kembali naskah asli oleh seseorang yang tidak mempunyai kunci dekripsi dalam waktu yang tidak terlalu lama sangat kecil.

Kriptografi berdasarkan kunci yang digunakan, dapat dibagi menjadi simetris dan asimetris. Kriptografi dikatakan simetris jika kunci yang digunakan untuk menyandikan *plaintext* **sama** dengan kunci yang digunakan untuk memecahkan *ciphertext.* Sementara kriptografi dikatakan asimetris jika kunci yang digunakan untuk menyandikan *plaintext* **tidak sama** dengan kunci yang digunakan untuk memecahkan *ciphertext.*

Kelebihan kriptografi simetris adalah lebih mudah dibuat karena memanfaatkan kunci enkripsi dan dekripsi yang sama. Contoh kriptografi simetris adalah Caesar Cipher. Sementara keunggulan kriptografi asimetris lebih sulit untuk di pecahkan tanpa private key, sehingga keamanannya lebih terjaga. Contoh Kriptografi asimetris adalah RSA, DSA, danEIGamal.

Selain berdasarkan kunci yang digunakan, kriptografi juga dibagi menjadi lima berdasarkan tekniknya. Kelima teknik itu adalah:

* + - 1. Teknik Subtitusi (Algoritma Subtitusi)

Teknik subtitusi adalah teknik penyandian teks dengan cara mengganti huruf-huruf yang ada dengan huruf-huruf yang lain secara langsung dengan aturan tertentu. Contoh penerapan teknik ini adalah *Caesar Cipher.*

* + - 1. Teknik Blocking (Algoritma Blocking)

Teknik blocking adalah teknik penyandian dengan cara membagi huruf teks menjadi beberapa kolom, lalu membacanya dalam satu blok sesuai dengan ketentuan yang di tetapkan. contoh nya ditunjukan oleh Gambar 3.2 berikut.



Gambar 2.1 Teknik Blocking

* + - 1. Teknik Ekspansi (Algoritma Ekspansi)

Teknik ekspansi adalah teknik penyandian dengan memanjangkan *plaintext* dengan cara menambah huruf dengan aturan tertentu. Salah satu contohnya adalah dengan meletakkan huruf pertama kata di akhir kata dan jika huruf pertama dari kata dalam *plaintext* termasuk huruf konsonan, ditambahkan “i” dibelakang kata hasil enkripsi. Tetapi jika huruf dari kata dalam *plaintext* termasuk huruf vokal, ditambahkan “an” dibelakang kata hasil enkripsi. contohnya jika diberi *plaintext, “*teknologi informasi”. Maka hasil enkripsi nya adalah “eknologiti nformasiian”.

* + - 1. Teknik Pemampatan (Algoritma Pemampatan)

Teknik pemampatan adalah teknik penyandian dengan memampatkan isi teks. Hal ini dapat dilakukan dengan menghilangkan huruf tertentu pada susunan sesuai ketentuan, dan menyusunnya kembali di akhir hasil teks yang dimampatkan. Berikut adalah contoh teknik pemampatan.



Gambar 2.2 Teknik Pemampatan

* + - 1. Teknik Permutasi (Algoritma Permutasi)

Teknik permutasi atau transposisi adalah teknik penyandian teks dengan cara mengacak posisi susunan karakter dari teks tanpa mengubah identitas dari karakter dalam teks. Contohnya seperti gambar berikut.



Gambar 2.3Teknik Permutasi

Telah dibahas di atas, salah satu implementasi kriptografi asimetris adalah Rivest Shamir Adleman (RSA). Langkah-langkah untuk untuk membangkitkan kunci RSA adalah:

Menentukan nilai prima sebagai p dan q. Nilai kedua bilangan prima tersebut tidak boleh sama. Dan sebaiknya bilangan yang besar agar tingkat keamanannya juga meningkat.

Mencari nilai n dengan memanfaatkan persamaan 2.1.  
……………………………….……………………(2.1)

Mencari nilai ekuivalen dengan persamaan 2.2.

……………………………………(2.2)

Memilih bilangan prima secara random antara 1 sampai untuk mendapatkan kunci publik e.

Menghitung kunci private d dengan persamaan 2.3.

…………………………………………(2.3)

Pasangan kunci yaitu kunci publik (e,n) dan kunci private (d,n) telah dihasilkan.

* 1. Mean Absolute Error (MAE) dan Mean Square Error (MSE)

Mean Absolute Error (MAE) adalah rata-rata error dari peramalan dan hasil yang sebenarnya tanpa memperhatikan tanda positif atau negatif (absolut). Secara matematis MAE didefinisikan pada persamaan sebagai berikut :

(2.4)

Dimana:

*n* adalah jumlah data.

*fi* adalah nilai karakter hasil enkripsi.

*yi* adalah nilai karakter asli.

Nilai tengah galat kuadrat Mean Squared Error (MSE) adalah metode lain untuk mengevaluasi metode peramalan. Masing-masing kesalahan atau sisa dikuadratkan. Kemudian dijumlahkan dan ditambahkan dengan jumlah observasi. Pendekatan ini mengatur kesalahan peramalan yang besar karena kesalahan-kesalahan itu dikuadratkan. Metode itu menghasilkan kesalahan-kesalahan sedang yang kemungkinan lebih baik untuk kesalahan kecil, tetapi kadang menghasilkan perbedaan yang besar. Secara matematis MSE didefinisikan pada persamaan sebagai berikut :

(2.5)

Dimana:

*n* adalah jumlah data.

*fi* adalah nilai karakter hasil enkripsi.

*yi* adalah nilai karakter asli.

MSE memberikan bobot yang lebih besar jika dibandingkan dengan MAE, yakni nilai kuadratik dari *error*. Sebagai konsekuensinya, nilai *error* yang kecil akan semakin kecil dan nilai *error* yang besar akan semakin besar.

Dalam kasus klasifikasi biner, dimana hanya terdapat dua kelas dengan label kelas 0 dan 1, tidak ada perbedaan baik menggunakan MAE maupun MSE. Hal ini karena nilai *error* hanya mempunyai dua kemungkinan, 0 jika prediksi benar dan 1 jika prediksi kelas berbeda dengan kelas sebenarnya. Hasil kuadrat ataupun absolut dari *error* tersebut akan sama sehingga nilai MAE dan MSE pun akan identik.

BAB III  
METODE PENELITIAN

3.1 Kerangka Konsep Penelitian

Blablbla…

3.2 Metodologi Penelitian

Blablabla..

RENCANA JADWAL PENGERJAAN

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| NO | KEGIATAN | WAKTU | | | | | | | | | | | | | | | |
| Nov-19 | | | | DES 2019 | | | | Jan-20 | | | | Feb-20 | | | |
| 1 | 2 | 3 | 4 | 1 | 2 | 3 | 4 | 1 | 2 | 3 | 4 | 1 | 2 | 3 | 4 |
| 1 | Pembuatan Proposal |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 2 | Persetujuan Proposal |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 3 | Studi Literatul dan Pengambilan Data |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 4 | Perancangan |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 5 | Implementasi Enkripsi File Teks (.txt) |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 6 | Implementasi Dekripsi File Teks (.txt) |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 7 | Pengujian |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 8 | Seminar Hasil |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 9 | Pembuatan Laporan |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 10 | Sidang Akhir |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |

DATAR PUSTAKA

Handoyo, A. E., Setiadi, D. R. I. M., Rachmawanto, E. H., Sari, C. A., & Susanto, A. (2018). Teknik Penyembunyian dan Enkripsi Pesan pada Citra Digital dengan Kombinasi Metode LSB dan RSA. *Jurnal Teknologi Dan Sistem Komputer*, *6*(1), 37. https://doi.org/10.14710/jtsiskom.6.1.2018.37-43

Muchlis, B. S., Budiman, M. A., & Rachmawati, D. (2017). Teknik Pemecahan Kunci Algoritma Rivest Shamir Adleman (RSA) dengan Metode Kraitchik. *SinkrOn*, *2*(2), 49–64. Retrieved from http://jurnal.polgan.ac.id/index.php/sinkron/article/view/75

Wulansari, D., Alamsyah, Setyawan, F. A., & Susanto, H. (2016). Mengukur Kecepatan Enkripsi dan Dekripsi Algoritma RSA pada Pengembangan Sistem Informasi Text Security. *Seminar Nasional Ilmu Komputer (SNIK 2016)*, (Snik), 85–91.