**PEMBANGKITAN KUNCI PRIVAT PADA ENKRIPSI RSA MENGGUNAKAN INFORMASI PERANTI**

**PROPOSAL TUGAS AKHIR**



**Oleh:**

**YOGI ARIF WIDODO**

**NIM. 17 615 006**

**KEMENTERIAN RISET TEKNOLOGI DAN PENDIDIKAN TINGGI**

**POLITEKNIK NEGERI SAMARINDA**

**JURUSAN TEKNOLOGI INFORMASI**

**PROGRAM STUDI TEKNIK INFORMATIKA**

**2019**

HALAMAN PERSETUJUAN

**PEMBANGKITAN KUNCI PRIVAT PADA ENKRIPSI RSA MENGGUNAKAN INFORMASI PERANTI**



Nama Mahasiswa : Yogi Arif Widodo

NIM : 17 615 006

Jurusan : Teknologi Informasi

Program Studi : Teknik Informatika

Jenjang Studi : Diploma III

Dipromosikan oleh:

**Mulyanto, S.Kom., M.Cs**

**NIP. 19750213 200801 1 007**

Kata Pengantar

Puji syukur Alhamdulillah panjat-kan kehadirat Allah SWT yang telah melimpahkan rahmat-Nya serta hidayah-Nya sehingga mampu menyelesaikan Proposal Tugas Akhir dengan judul Pembangkitan Kunci Privat Pada Enkripsi RSA Menggunakan Infromasi Peranti.

Selawat 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, mendapatkan banyak sekali bantuan, bimbingan serta dukungan dari berbagai pihak, sehingga dalam kesempatan ini, 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. Mulyanto, S.Kom., M.Cs 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.

Harapan-nya tugas akhir yang telah disusun ini bisa memberikan sumbangsih untuk menambah pengetahuan, dan perbaikan selanjutnya, selalu terbuka terhadap saran dan masukan, karena menyadari tugas akhir yang telah disusun ini memiliki banyak sekali kekurangan.

Samarinda, 21 Desember 2019

Yogi Arif Widodo

DAFTAR ISI

[HALAMAN PERSETUJUAN i](#_Toc31862353)

[Kata Pengantar i](#_Toc31862354)

[DAFTAR ISI iii](#_Toc31862355)

[DAFTAR GAMBAR iv](#_Toc31862356)

[BAB I PENDAHULUAN 1](#_Toc31862357)

[1.1 Latar Belakang 1](#_Toc31862358)

[1.2 Rumusan Masalah 2](#_Toc31862359)

[1.3 Tujuan Penelitian 2](#_Toc31862360)

[1.4 Batasan Masalah 2](#_Toc31862361)

[1.5 Manfaat Penelitian 2](#_Toc31862362)

[BAB II TINJAUAN PUSTAKA 3](#_Toc31862363)

[2.1 Kajian Ilmiah 3](#_Toc31862364)

[2.2 Dasar Teori 5](#_Toc31862365)

[2.2.1 Kriptografi 5](#_Toc31862366)

[*2.2.2* Informasi Peranti 9](#_Toc31862367)

[2.3.1 Teori Bilangan ( Relatif Prima ) 10](#_Toc31862368)

[2.3.2 Entropy 10](#_Toc31862369)

[BAB III METODE PENELITIAN 11](#_Toc31862370)

[3.1 Kerangka Konsep Penelitian 11](#_Toc31862371)

[3.1.1 Kriptografi 12](#_Toc31862372)

[3.2 Metodologi Penelitian 13](#_Toc31862373)

[3.2.1 Riset Awal 14](#_Toc31862374)

[3.2.2 Tahapan Menentukan Bilangan Prima 14](#_Toc31862375)

[3.2.3 Tahapan Pembangkitan Kunci 16](#_Toc31862376)

[3.2.4 Pengujian 16](#_Toc31862377)

[3.2.5 Analisa Hasil 16](#_Toc31862378)

[3.2.6 Variabel Penelitian 17](#_Toc31862379)

[3.2.7 Waktu dan Tempat Penelitian 17](#_Toc31862380)

[RENCANA JADWAL PENGERJAAN 18](#_Toc31862381)

[DATAR PUSTAKA 19](#_Toc31862382)

DAFTAR GAMBAR

|  |  |
| --- | --- |
| Gambar 2.1 Teknik Blocking…………..…………………………...……. | 7 |
| Gambar 2.2 Teknik Pemampatan…………………………………...…….. | 8 |
| Gambar 2.3 Teknik Permutasi……………..…….………………...……… | 9 |
| Gambar 2.4 FlowChart Pembangkitan Kunci Algoritma RSA…....……… | 10 |
| Gambar 3.1. Diagram Alir Kerangka Konsep Penelitian……….………… | 12 |
| Gambar 3.2. Diagram Alir Metodologi Penelitian……………..……….… | 14 |
| Gambar 3.2.1 FlowChart Daur Ulang Pembangkitan Kunci....................... | 16 |
| Gambar 3.2.2 FlowChart Pembangkit Batas Atas Angka Prima................. | 17 |
| Gambar 3.2.3 FlowChart Hasil Pembangkit Semua Angka Prima............... | 17 |
| Gambar 3.2.4 FlowChart Terpilih-nya konstanta atau orde P dan Q……... | 16 |
| Gambar 3.2.5 FlowChart Pembangkitan Kunci dengan Informasi Peranti.. | 17 |

BAB I  
PENDAHULUAN

1.1 Latar Belakang

Keamanan informasi itu penting tergantung pada aspek data, terutama ketika menyangkut privasi seseorang yang tidak di otorisasi oleh pihak yang berwenang.

Selain menjadi ilmu mengamankan data, kriptografi adalah seni menjaga kerahasiaan data dengan mengubah-nya menjadi berbeda atau tidak bermakna dan dengan algoritma matematika, maka hanya dapat diselesaikan oleh orang yang memiliki kunci.

RSA (Rivest Shamir Adleman) merupakan teknik kriptografi moderen yang telah melewati batas paten selama 20 tahun, membuat-nya mudah di baca secara bebas. Sulit-nya memfaktorkan bilangan besar menjadi faktor – faktor prima (utama), serta perbedaan kunci dalam penyandian dan terjemahan, membuat RSA menjadi salah satu teknik yang sulit dipecahkan. Dengan pesatnya perkembangan teknologi atau se-iring waktu, perlu dilakukan sebuah trik atau modifikasi untuk tetap menjadikan RSA tetap terjaga dalam hal yang lebih spesifik.

Berdasarkan Aspek tersebut, maka pada penilitian ini melaksanakan “Pembangkitan Kunci Privat Pada Enkripsi RSA Menggunakan Informasi Peranti”.

1.2 Rumusan Masalah

Dalam melaksanakan penelitian, ada sejumlah masalah yang menjadi poin utama diskusi atau pembahasan, termasuk “Bagaimana Melakukan Pembangkitan Kunci Privat Pada Enkripsi RSA Sesuai Informasi Peranti”.

1.3 Tujuan Penelitian

Dari rumusan masalah, tujuan dari penelitian ini adalah:

1. Memanfaatkan informasi peranti dalam pembangkitan kunci privat
2. Memodifikasi Teknik pembangkitan kunci privat.

1.4 Batasan Masalah

Agar tidak terjadi kesalahan persepsi dan tidak meluasnya pokok bahasan, memerlukan batasan masalah sebagai berikut:

1. Informasi peranti menggunakan waktu dan persen baterai.
2. Waktu yang dipakai adalah sekarang
3. Zona waktu adalah **GMT -11:00** sampai **GMT +13:00**.
4. *PlainText* (m) dan *CipherText* (c) menggunakan ASCII (bukan tunggal karakter atau *null*) dengan *encoding* (UTF-8).
5. Panjang kunci adalah 7 *bit* (2 digit) sampai 14 bit (4 digit).

1.5 Manfaat Penelitian

Harapan penelitian yang dilaksanakan, dapat memberikan manfaat:

1. Kunci algoritma ter-integrasi dalam pembangkitan-nya.
2. Mengetahui algoritma RSA masih bertahan terhadap era perkembangan teknologi terbaru.

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 memfaktor-kan kunci publik n dengan Metode *Kraitchik*, kemudian dilihat efisiensi waktu pemfaktorannya. Hasil penelitian memperlihatkan, bahwa semakin besar selisih antara faktor kunci p dan q, maka semakin besar pula waktu pemfaktorannya. Pemfaktoran kunci publik (n) sebesar 19 digit (152 *bit*) dengan selisih faktor 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 memengaruhi 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 mngonversikan nilai piksel citra menjadi 16 bit sehingga kunci yang digunakan dapat lebih bervariasi. Hasil eksperimen membuktikan ada-nya 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* dan *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. Tahapan 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 data 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* adalah ekuivalen dengan kunci yang digunakan untuk memecahkan *ciphertext* (ini menjadikan kelebihan-nya)*.* Sementara kriptografi dikatakan asimetris jika kunci yang digunakan untuk menyandikan *plaintext* berbeda dengan kunci yang digunakan untuk memecahkan *ciphertext.*

Contoh kriptografi simetris adalah *Caesar* *Cipher*. Sementara keunggulan kriptografi asimetris lebih sulit untuk di pecahkan tanpa kunci privat, sehingga keamanannya lebih terjaga. Contoh Kriptografi asimetris adalah RSA, DSA, dan EIGamal.

Selain berdasarkan kunci yang digunakan, kriptografi dibagi menjadi 5 berdasarkan tekniknya. Kelima teknik itu adalah:

* + - 1. Teknik Substitusi (Algoritma Substitusi)

Teknik substitusi adalah teknik penyandian teks dengan cara mengganti huruf yang ada dengan 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*

(m), dengan menambah huruf sesuai aturan tertentu adalah cara-nya. Salah satu contohnya adalah dengan meletakkan huruf pertama kata di akhir kata dan jika huruf pertama dari kata dalam mtermasuk huruf konsonan, ditambahkan “i” dibelakang kata hasil enkripsi. Tetapi jika huruf dari kata dalam mtermasuk huruf vokal, ditambahkan “an” dibelakang kata hasil enkripsi. Contoh-nya jika diberi *m, “*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 2.3 Teknik 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 di anjurkan kembar (p = q). 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 privat d dengan persamaan 2.3.

…………………………………………… (2.3)

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



Gambar 2.4 FlowChart Pembangkitan Kunci Algoritma RSA

Untuk enkripsi dan Dekripsi

* + 1. Informasi Peranti

Informasi peranti adalah komponen perangkat lunak yang mengizinkan sebuah sistem komputer untuk berkomunikasi dengan sebuah perangkat keras. Data peranti memiliki cakupan luas, salah satu diantara-nya adalah:

1. Waktu (meliputi: 12 atau 24 jam format dan zona waktu).
2. Sinyal (terdiri dari jangkauan area, tegangan, arus dan lain-nya).
3. Suhu (skala: Celsius, Kelvin, Fahrenheit, dan Reamur).
4. Baterai (voltase, daya atau persen dan lain-nya).
   * 1. Teori Bilangan ( Relatif Prima )

Secara ringkas, relatif prima merupakan dua buah bilangan bulat a dan b dikatakan relatif prima jika GCD atau FPB (a, b) = 1, maka terdapat bilangan bulat m dan n sedemikian hingga ma + nb = 1. Disebut bilangan prima, jika pembaginya hanya 1 dan bilangan itu sendiri. Contoh angka 13 habis dibagi oleh 1 dan 13.

* + 1. Entropy

Entropy adalah suatu parameter untuk mengukur tingkat keberagaman dari kumpulan data. Jika nilai dari entropy semakin besar, maka tingkat keberagaman suatu kumpulan data semakin besar. Rumus untuk menghitung entropy sebagai berikut:

(2.4)

Dimana:

M = jumlah kelas klasifikasi

= jumlah proporsi sampel (peluang) untuk kelas i

Sedangkan rumus untuk entropy pada masing-masing variabel adalah:

(2.4)

Dimana:

A = Variabel.

v = nilai yang mungkin untuk variable A.

|Sv| = Jumlah sampel untuk nilai v.

|S| = Jumlah sampel untuk seluruh sampel data.

= Entropy untuk sampel yang memiliki nilai.

BAB III  
METODE PENELITIAN

3.1 Kerangka Konsep Penelitian

Kerangka konseptual penelitian (teori atau konsep ilmiah yang digunakan sebagai dasar penelitian) menjelaskan hubungan antara ruang lingkup penelitian dan ruang lingkup ilmu pengetahuan.

  
Gambar 3.1 Diagram Alir Kerangka Konsep Penelitian

* + 1. Kriptografi

Didalam kriptografi terdapat dua jenis algoritma berdasarkan kuncinya yaitu:

1. Algoritma Simetri
2. Algoritma Asimetri

Macam-macam Algoritma asimetri (Kriptografi Modern) di antaranya adalah:

1. *Diffle-Hellman (DH)*
2. *Elliptic Curve Cryptography (ECC)*
3. *Digital Signature Algorithm (DSA)*
4. *Rivest Shamir Adleman (RSA)*

Dari beberapa macam algoritma asimetri di atas yang digunakan adalah RSA dan jenis algoritma cipher adalah block. Proses pembangkitan kunci privat menggabungkan informasi peranti yaitu waktu dan baterai. Proses enkripsi dan dekripsi adalah jenis data teks.

3.2 Metodologi Penelitian



Gambar 3.2 Diagram Alir Metodologi Penelitian

3.2.1 Riset Awal

Sebelum melakukan penelitian terlebih dahulu mempelajari segala hal yang terkait dengan topik penelitian. Bagian utama yang perlu dipelajari adalah:

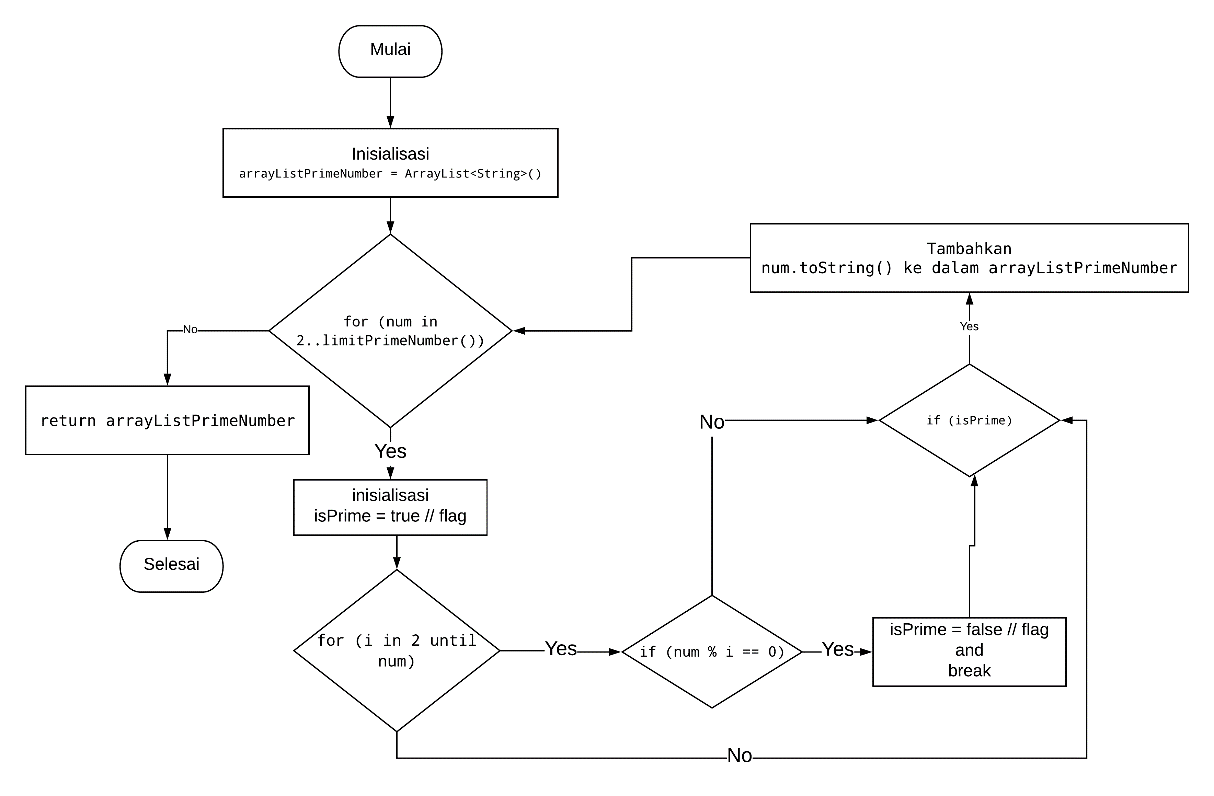
1. Konsep dasar Kriptografi
2. Algoritma *Rivest Shamir Adleman (RSA)*
3. Mengetahui penggunaan informasi peranti

3.2.2 Tahapan Menentukan Bilangan Prima

Berdasarkan riset awal yang dilakukan, Tahapan menentukan bilangan prima adalah langkah lanjutan dalam poin utama tujuan penelitian berdasarkan informasi peranti.



Gambar 3.2.2 FlowChart Pembangkit Batas Atas Angka Prima



Gambar 3.2.3 FlowChart Hasil Pembangkit Semua Angka Prima

Gambar 3.2.4 FlowChart Terpilih-nya konstanta atau orde P dan Q

3.2.3 Tahapan Pembangkitan Kunci



Gambar 3.2.5 FlowChart Pembangkitan Kunci dengan Informasi Peranti

3.2.4 Pengujian

Hasil kombinasi konstanta p dan q (orde), dalam pembangkitan kunci privat, di bandingkan dengan catatan nilai entropy semakin besar atau pola acak matrix.

3.2.5 Analisa Hasil

Hasil yang diperoleh dari pengujian kemudian dianalisa terutama pada proses terpilih-nya p dan q untuk pembangkitan kunci privat.

3.2.6 Variabel Penelitian

Fokus penelitian tugas akhir ini di tuangkan dalam variabel yaitu Modifikasi konstanta atau orde p dan q berdasarkan informasi peranti.

3.2.7 Waktu dan Tempat Penelitian

Penelitian dilaksanakan pada bulan Desember 2019 sampai bulan Februari 2020 di Politeknik Negeri Samarinda.

RENCANA JADWAL PENGERJAAN



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.