PEMBANGKITAN KUNCI PRIVATE PADA ENKRIPSI RSA MENGGUNAKAN INFORMASI DEVICE

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 PRIVATE PADA ENKRIPSI RSA MENGGUNAKAN INFORMASI DEVICE

Nama Mahasiswa	: Yogi Arif Widodo
NIM	: 17 615 006
Jurusan	: Teknologi Informasi
Program Studi	: Teknik Informatika
Jenjang Studi	: Diploma III

Dipromosikan oleh :

Rheo Malani, S.Kom. M.Kom

NIP. 19780823 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 Pembangkitan Kunci *Private* Pada Enkripsi RSA Menggunakan Infromasi *Device*

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. Rheo Malani, S.Kom. M.Kom 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, 21 Desember 2019

Yogi Arif Widodo

DAFTAR ISI

DAFTAR GAMBAR

BAB I

PENDAHULUAN

1.1 Latar Belakang

Keamanan informasi itu penting, terutama ketika menyangkut privasi seseorang yang tidak di otorisasi oleh pihak yang berwenang. Salah satu cara untuk mengamankan data adalah kriptografi atau penyandian teks.

Selain menjadi ilmu untuk mengamankan data, kriptografi adalah seni untuk menjaga kerahasiaan data dengan mengubahnya menjadi terenkripsi atau tersandi yang tidak bermakna dan hanya dapat diselesaikan oleh orang-orang yang memiliki kunci.

RSA (Rivest Shamir Adleman) merupakan salah satu teknik dalam kriptografi modern 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 kriptografi yang sulit dipecahkan. Dengan pesatnya perkembangan teknologi atau dengan se-iring waktu, perlu dilakukan sebuah trik untuk tetap menjadikan RSA sebagai modern kriptografi.

Berdasarkan hal tersebut, maka pada penilitian ini akan dilakukan "Pembangkitan Kunci *Private* Pada Enkripsi RSA Menggunakan Informasi Device".

1.2 Rumusan Masalah

Dalam melaksanakan tugas penelitian ini ada sejumlah masalah yang menjadi poin utama diskusi atua pembahasan, termasuk “Bagaimana Melakukan Pembangkitan Kunci *Private* Pada Enkripsi RSA Sesuai Informasi *Device*”.

1.3 Tujuan Penelitian

Dari rumusan masalah , tujuan dari penelitian ini adalah :

1. Menghasilkan kunci *private* yang tidak tetap.
2. Mempertahankan *CipherText* dan *plaintext* terhadap kunci yang berbeda // tidak bisa karena , ada kunci yang jika di faktorkan tidak dapat menerjemahkan beberapa cipher dan tentu kunci lama mampu / bisa men-dekripsi.
3. Menjadikan *CipherText* yang semula tidak rahasia menjadi rahasia.
4. Menjadikan *PlainText* yang semula rahasia menjadi tidak rahasia.
5. Kunci *private* tidak bisa di pakai dalam waktu tertentu dan hanya bisa digunakan 1x dekripsi.

1.4 Batasan Masalah

Agar tidak terjadi kesalahan persepsi dan tidak meluasnya pokok bahasan, maka penulis memberikan batasan-batasan masalah sebagai berikut:

1. Informasi *device* menggunakan waktu sekarang dan zona waktu yang digunakan adalah **GMT -11:00** sampai **GMT +13:00** .
2. *PlainText* dan *CipherText* menggunakan ASCII (bukan tunggal karakter atau *null*) dengan *encoding* (UTF-8)

3. Panjang kunci adalah 7 *bit max* (2 digit) sampai 14 *bit max* (3 digit)

1.5 Manfaat Penelitian

Penelitian yang dilakukan diharapkan dapat memberikan manfaat bagi pembaca dan penulis , termasuk :

1. Mengetahui algoritma RSA masih bertahan terhadap era perkembangan teknologi terbaru.
2. Tidak khawatir jika data atau teks telah di ketahui oleh orang yang tidak memiliki otorisasi.
3. Menambah pengetahuan, wawasan, dan pemahaman tentang algoritma RSA dan mengaplikasikan ilmu-ilmu yang didapat untuk dikembangkan lebih lanjut.
4. Diharapkan dapat memberi kemudahan dan bermanfaat untuk informasi secara akademis.

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*, 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 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* 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. 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, dan EIGamal.

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*.

2. 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.

T	L	I	M	BLOK 1
E	O	N	A	BLOK 2
K	G	F	S	BLOK 3
N	I	O	I	BLOK 4
O		R		BLOK 5
P=	TEKNOLOGI INFOMASI			
E=	TLIMEONAKGFSNIOIO R			

Gambar 2.1 Teknik *Blocking*

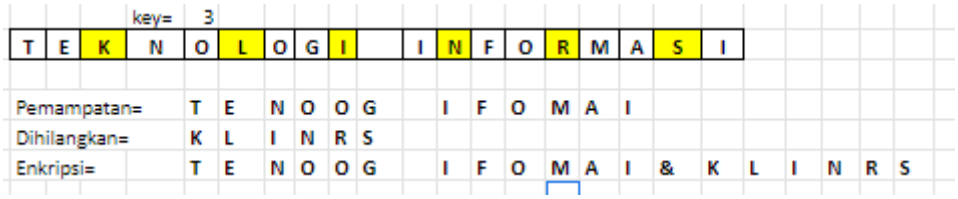
3. Teknik Ekspansi (Algoritma Ekspansi)

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".

4. Teknik Pemampatan (Algoritma Pemampatan)

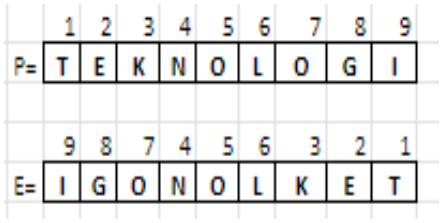
Teknik pemampatan adalah teknik penyandian dengan memampatkan isi teks. Hal ini dapat dilakukan dengan menghilangkan huruf tertentu pada susunan sesuai ketentuan, dan menyusunnya kembali di akhir hasil teks yang dimampatkan. Berikut adalah contoh teknik pemampatan.



Gambar 2.2 Teknik Pemampatan

5. 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

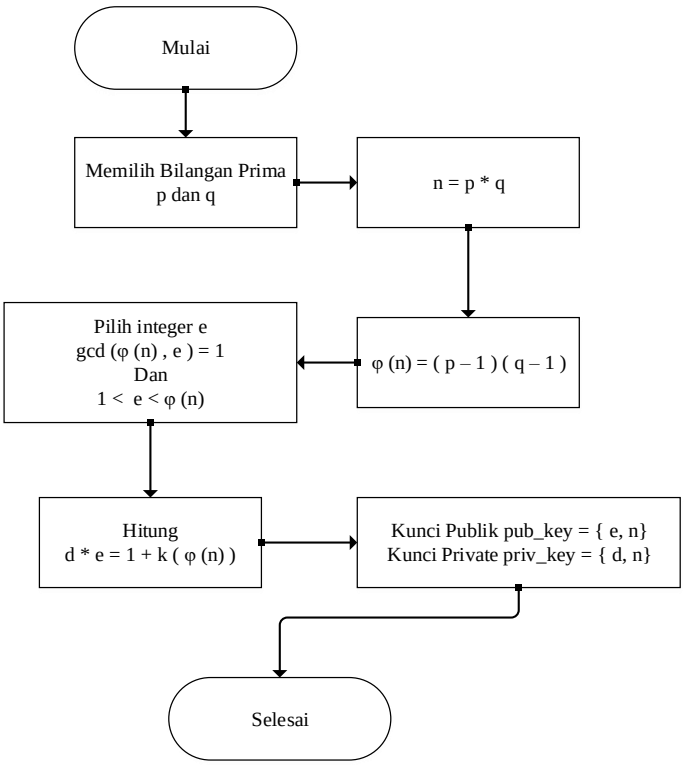
Telah dibahas di atas, salah satu implementasi kriptografi asimetris adalah Rivest Shamir Adleman (RSA). Langkah-langkah untuk untuk membangkitkan kunci RSA adalah:

1. 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.
2. Mencari nilai n dengan memanfaatkan persamaan 2.1.

   $n = p * q$……..……..……..……..…(2.1)
3. Mencari nilai ekuivalen dengan persamaan 2.2.

   $\phi(n) = (p-1) * (q-1)$ ……...……(2.2)
4. Memilih bilangan prima secara random antara 1 sampai $CC = \frac{\sum_{i=1}^{m}\sum_{j=1}^{n}[W(i,j)*W'(i,j)}{\sum_{i=1}^{m}\sum_{j=1}^{n}(W(i,j))^2}$ untuk mendapatkan kunci publik e.
5. Menghitung kunci private d dengan persamaan 2.3.

   $(e * d) mod \phi(n) = 1$ ……(2.3)
6. Pasangan kunci yaitu kunci publik (e, n) dan kunci private (d, n) telah dihasilkan.



Gambar 2.4 FlowChart Pembangkitan Kunci Algoritma RSA

4.2.2 Informasi *Device*

Informasi Device adalah komponen perangkat lunak yang mengizinkan sebuah sistem computer untuk berkomunikasi dengan sebuah perangkat keras. Informasi device memiliki cakupan yang begitu luas, salah satu diantara-nya adalah:

1. Waktu
2. Signal
3. Suhu

2.3.1 *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 :

$$MAE = \frac{1}{n}\sum_{i=0}^{n} |f_i - y_i| \quad \text{.....(2.4)}$$

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 :

$$MSE = \frac{1}{n}\sum_{i=0}^{n}(f_i - y_i)^2 \quad \text{.....(2.5)}$$

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.

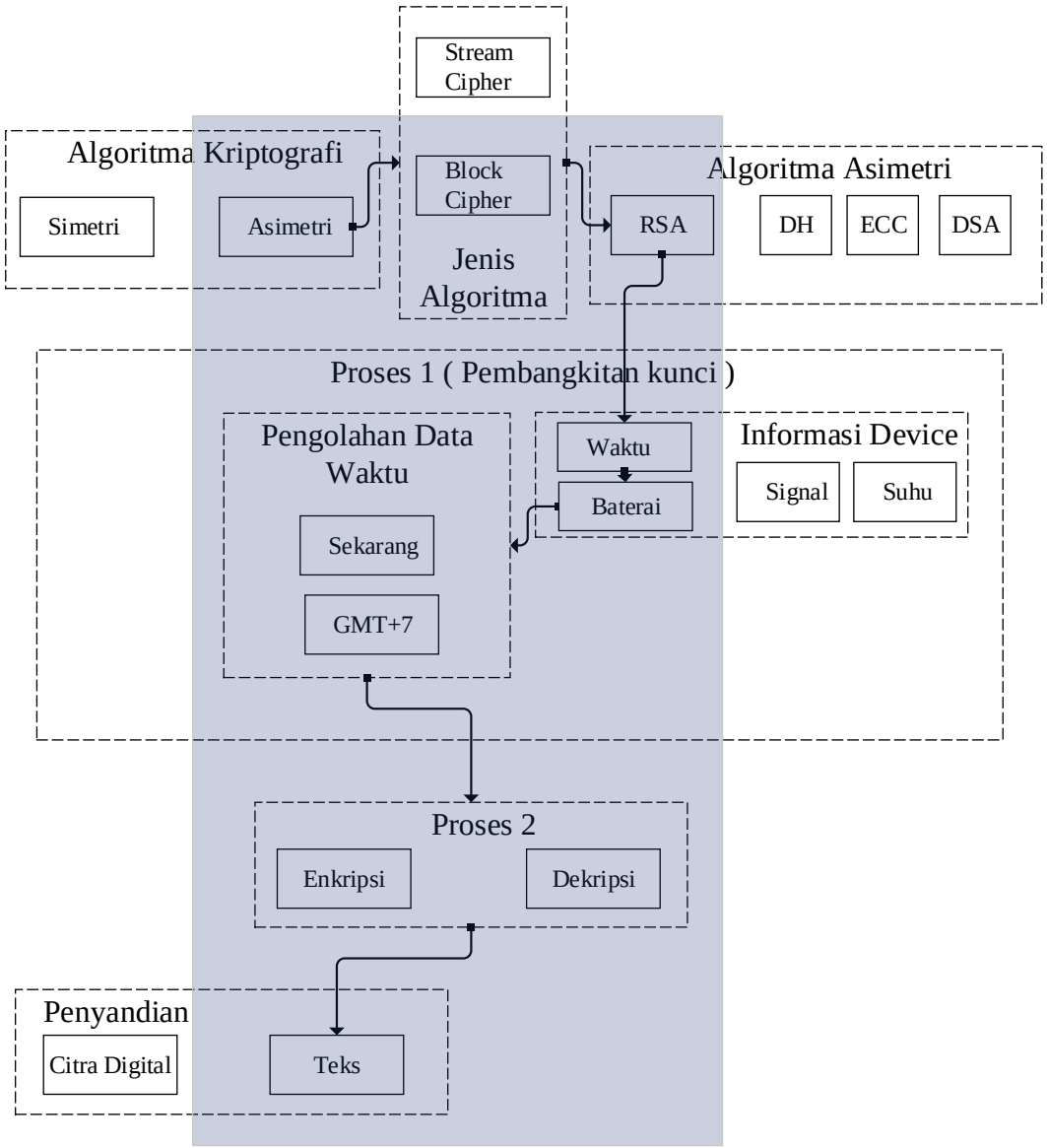
Dalam kasus klasifikasi biner, dimana hanya terdapat dua kelas dengan label kelas 0 dan 1, tidak ada perbedaan baik menggunakan MAE maupun MSE. Hal ini karena nilai *error* hanya mempunyai dua kemungkinan, 0 jika prediksi benar dan 1 jika prediksi kelas berbeda dengan kelas sebenarnya. Hasil kuadrat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

BAB III

METODE PENELITIAN

3.1 Kerangka Konsep Penelitian

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

3.1.1 Kriptografi

Didalam kriptografi terdapat dua jenis algoritma berdasarkan kuncinya yaitu:

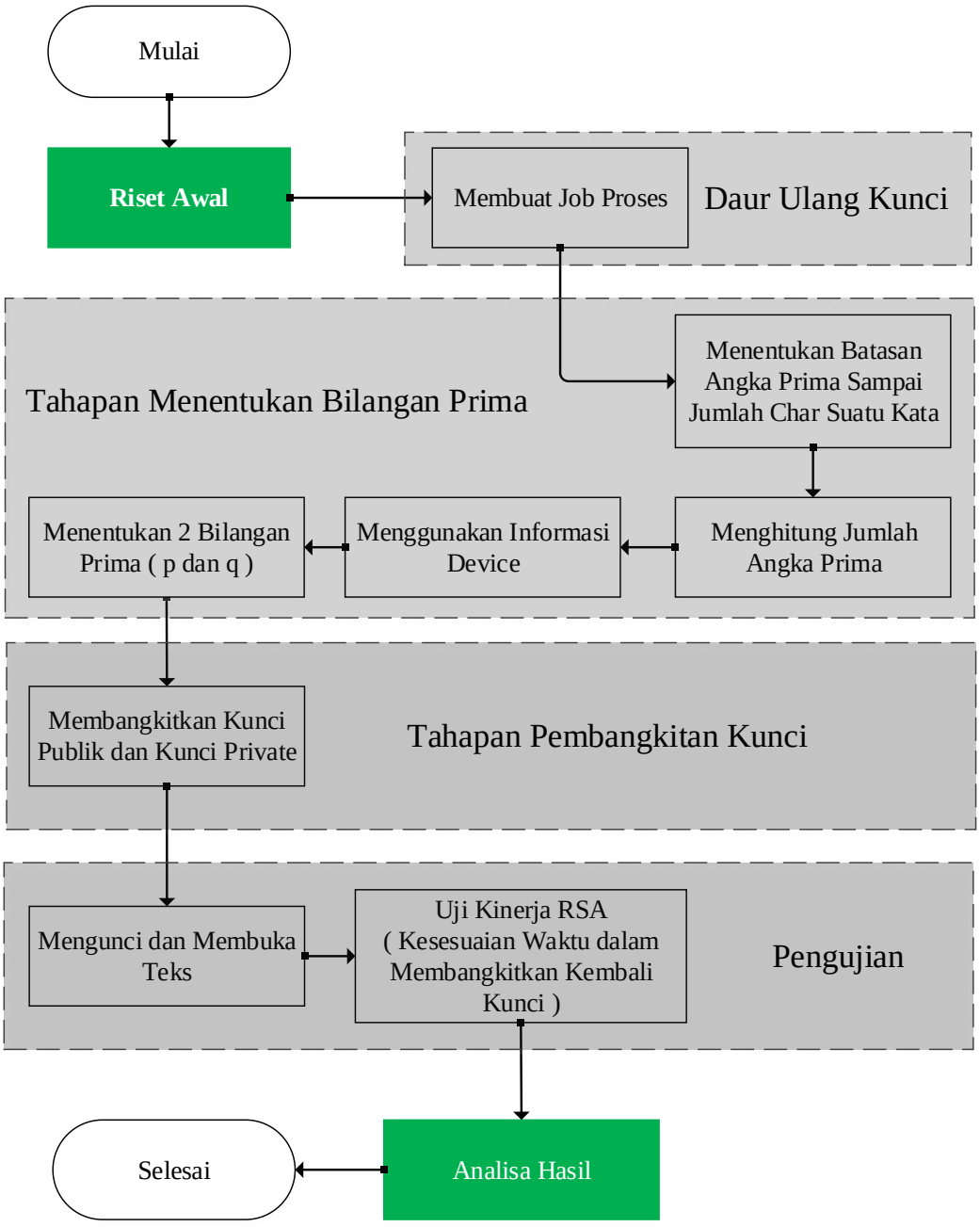
1. Algoritma Simetri
2. Algoritma Asimetri

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. Proses pembangkitan kunci private menggabungkan informasi device yaitu waktu dan baterai. Proses enkripsi dan dekripsi adalah jenis data teks.

3.2 Metodologi Penelitian



Gambar 3.2 Diagram Alir Metodologi Penelitian

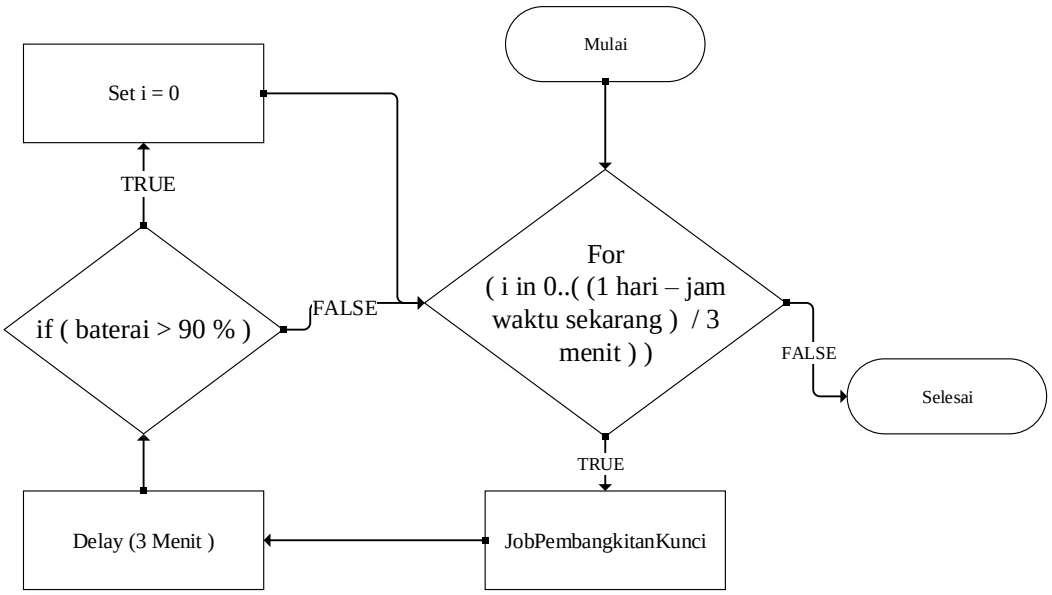
3.2.1 Riset Awal

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. Konsep penggunaan informasi *device*

3.2.2 Daur Ulang Kunci

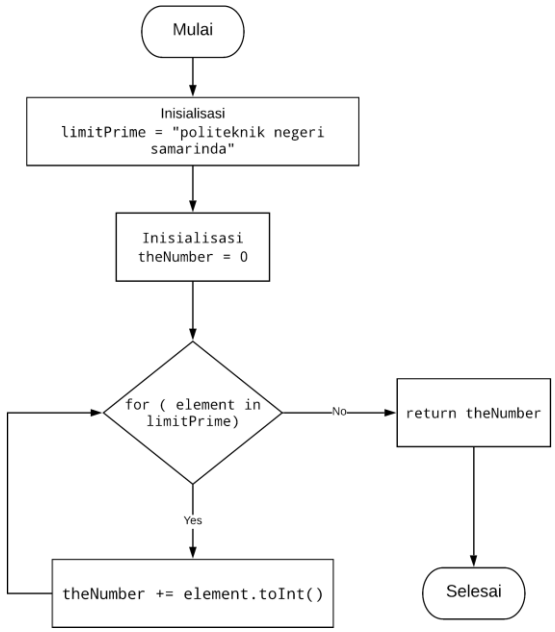
Membuat job proses (tempo) dimana kunci di daur ulang.



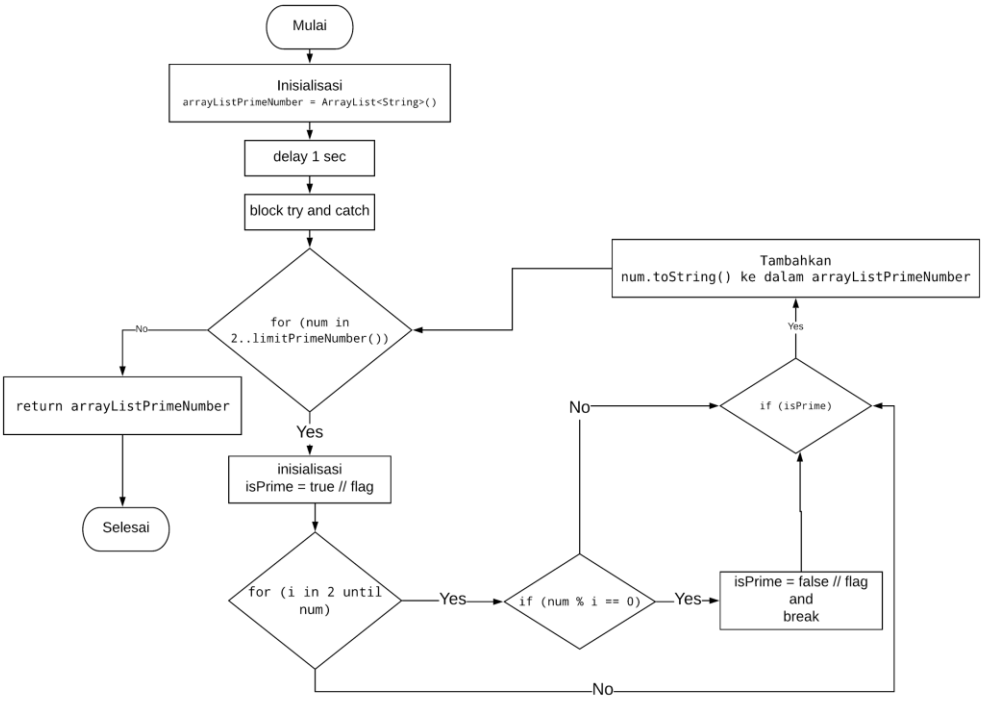
Gambar 3.2.1 FlowChart Daur Ulang Kunci

3.2.3 Tahapan Menentukan Bilangan Prima

Berdasarkan riset awal yang dilakukan, Tahapan menentukan bilangan prima adalah langkah lanjutan dalam poin utama tujuan penlitian.



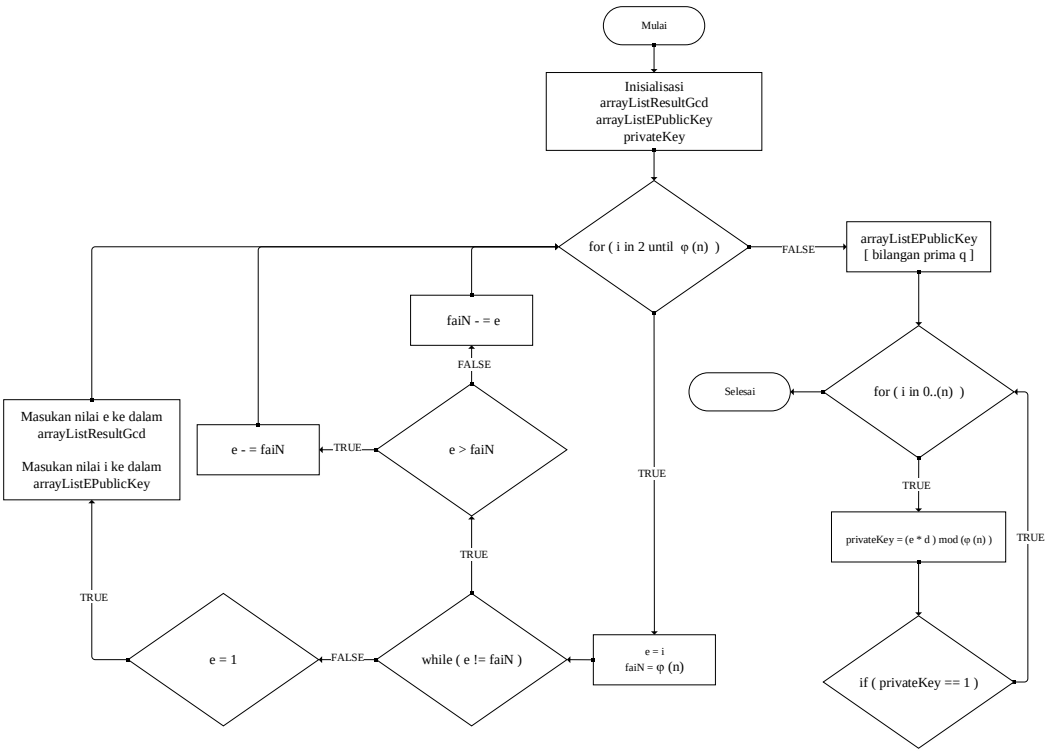
Gambar 3.2.2 FlowChart Pembangkit Batas Angka Prima



Gambar 3.2.3 FlowChart Hasil Pembangkit Batas Angka Prima

3.2.4 Tahapan Pembangkitan Kunci

Hasil kunci yang telah di tetapkan, di simpan sementara dalam device dan kunci di daur ulang berdasarkan informasi device yang digunakan.



Gambar 3.2.4 FlowChart Pembangkitan Kunci dengan Informasi Device

3.2.5 Pengujian

Melakukan enkripsi dan dekripsi sesuai dengan tahapan sebelumnya, yaitu pembangkitan kunci. Setelah itu menetapkan tempo daur ulang kunci berdasarkan penelitian terdahulu yang meng-kaji "*cryptoanalyze*" yang menggunakan algoritma RSA.

3.2.6 Analisa Hasil

Hasil yang diperoleh dari pengujian kemudian dianalisa terutama pada proses pembangkitan kunci private.

3.3 Variabel Penelitian

Fokus penelitian tugas akhir ini di tuangkan dalam variable yaitu Algoritma RSA yang menggunakan Informasi *Device* terhadap pembangkitan kunci *private*.

3.4 Waktu dan Tempat Penelitian

Peneliatian dilaksanakan pada bulan December 2019 sampai bulan Febuari 2020 di Politeknik Negeri Samarinda.

\

RENCANA JADWAL PENGERJAAN

NO	KEGIATAN	WAKTU											
		Dec-19				Jan-20				Feb-20			
		1	2	3	4	1	2	3	4	1	2	3	4
1	Pembuatan Proposal												
2	Persetujuan Proposal												
3	Studi Literatul												
4	Perancangan												
5	Pembangkitan Kunci Private												
6	Enkripisi dan Dekripsi												
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.