PEMBANGKITAN KUNCI PRIVAT PADA ENKRIPSI RSA MENGGUNAKAN INFORMASI PERANTI

LAPORAN 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

2020

Kata Pengantar

Puji syukur Alhamdulillah panjatkan kehadirat Allah SWT yang telah melimpahkan rahmatnya serta hidayahnya 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.

Harapannya 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, 16 Februari 2020

Yogi Arif Widodo

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

BAB I

PENDAHULUAN

1.1 Latar Belakang

RSA merupakan teknik kriptografi modern yang melewati batas paten selama 20 tahun, sehingga mudah dibaca secara bebas. Sulitnya memfaktorkan bilangan besar $n = p.q$ menjadi faktor prima (utama), serta perbedaan kunci dalam mengungkap teks maupun penyandian, membuat RSA menjadi salah satu teknik yang sulit dipecahkan. "Teknik Pemecahan Kunci Algoritma *Rivest Shamir Adleman* (RSA) dengan Metode *Kraitchick*". Penelitian tersebut menjadi kreativitas dalam meneliti bilangan konstanta atau orde p dan q, kesimpulan menghasilkan tentang efisiensi waktu pemfaktoran, selisih $p - q$ maupun faktor $(p - 1), (q - 1)$, dan panjang kunci (Muchlis dkk., 2017).

Tentu menimbulkan pertanyaan "keamanan sudah kuat, kenapa dimodifikasi lagi?" banyak sudah penelitian yang membahasnya, bisa dilihat menggunakan *dorking google* dengan kata kunci "*intext:'journal rsa" filetype:pdf site:ac.id*" hasilnya sekitar 5000 journal. Dengan begitu konsep RSA mulai dikenal, digunakan, dan terbongkar (Nisha & Farik, 2017).

Nilai p dan q hanya sering dikenal atau digunakan dalam pembangunan kunci publik dan kunci privat. Berdasarkan penelitian tadi, dapat diketahui bahwa nilai p dan q berperan penting dalam tingkat keamanan enkripsi algoritma RSA.

Ketika hak otorisasi dijatuhkan dalam informasi tertentu, memberikan pola yang merangkai konsep, Seperti waktu terus berjalan mengikuti masa sekarang,

tentu memiliki aspek krusial terhadap kombinasi angka atau bilangan yang dilakukan *simple* acak informasi ataupun posisinya.

Waktu merupakan sebuah informasi dengan konsep angka yang terus berjalan dan selalu berubah. Pada masa kini, informasi ini dapat dengan mudah di dapatkan dari perangkat peranti telepon genggam atau komputer.

Berdasarkan aspek tersebut, maka dilakukan penelitian "Pembangkitan Kunci Privat Pada Enkripsi RSA Menggunakan Informasi Peranti".

1.2 Rumusan Masalah

Dalam melaksanakan penelitian, masalah yang menjadi poin utama diskusi atau pembahasan, adalah "Bagaimana Melakukan Pembangkitan Kunci Privat Pada Enkripsi RSA Sesuai Informasi Peranti".

1.3 Tujuan Penelitian

Tujuan dari penelitian ini adalah:

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

1.4 Batasan Masalah

Agar persepsi penilitian tepat dan sesuai rumusan masalah, memerlukan batasan masalah sebagai berikut:

1. Informasi peranti menggunakan waktu.
    a. Waktu yang dipakai adalah sekarang
    b. Zona waktu adalah **GMT -11:00** sampai **GMT +13:00**.
2. *PlainText* (m) dan *CipherText* (c) menggunakan ASCII (bukan tunggal karakter atau *null*) dengan *encoding* (UTF-8).

3. 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 lebih berpola dalam pembangkitannya.
2. Melihat celah konsep mustahil, menjadi bisa atau telah stabil.
3. Lebih memperhatikan data, yang orang berangapan sepele.

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 diantaranya 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 memengaruhi adalah GCD(p-1, q-1), panjang kunci dan faktor prima (p-1), (q-1). (Muchlis dkk., 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 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 dkk., 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 dkk., 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 teks asli (*plaintext*) diubah menggunakan suatu kunci enkripsi menjadi teks acak yang sulit dibaca (*ciphertext*) dan hanya seseorang yang memiliki kunci dekripsi mudah membaca.

Kriptografi berdasarkan kunci yang digunakan, dapat dibagi menjadi simetris dan asimetris (Rani & Kaur, 2017). Kriptografi dikatakan simetris jika kunci yang digunakan untuk menyandikan *plaintext* adalah ekuivalen dengan kunci yang digunakan untuk memecahkan *ciphertext* (ini menjadikan kelebihannya). 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 dipecahkan tanpa kunci privat, sehingga keamanannya lebih terjaga. Contoh Kriptografi asimetris adalah RSA, DSA, dan EIGamal.

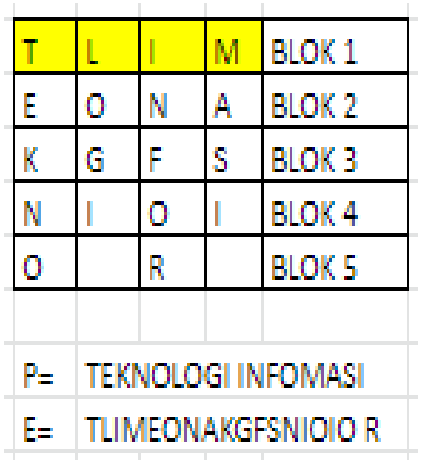
Selain berdasarkan kunci yang digunakan, kriptografi dibagi menjadi 5 berdasarkan tekniknya (Pabokory dkk., 2016). Kelima teknik itu adalah:

1. Teknik Substitusi (Algoritma Substitusi)

   Teknik substitusi adalah teknik penyandian teks dengan mengganti huruf yang ada dengan 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 membagi huruf teks menjadi beberapa kolom, lalu membacanya dalam satu blok sesuai dengan ketentuan yang ditetapkan. Contohnya ditunjukan oleh Gambar 2.1.



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*

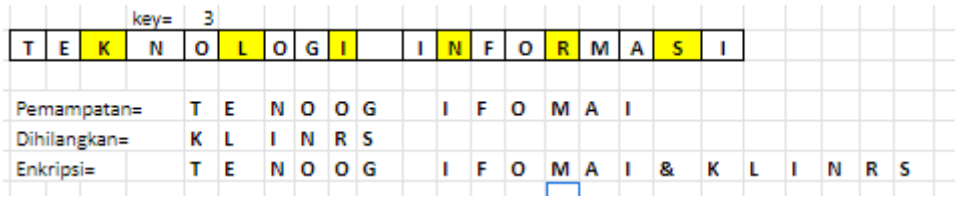
3. Teknik Ekspansi (Algoritma Ekspansi)

Teknik ekspansi adalah teknik penyandian dengan memanjangkan *plaintext* (m), dengan menambah huruf sesuai aturan tertentu adalah caranya. Salah satu contohnya adalah dengan meletakkan huruf pertama kata di akhir kata dan jika huruf pertama dari kata dalam m termasuk huruf konsonan, di tambahkan "i" di belakang kata hasil enkripsi. Tetapi jika huruf dari kata dalam m termasuk huruf vokal, ditambahkan "an" di belakang kata hasil enkripsi. Contohnya jika diberi *m,* "teknologi informasi". Maka hasil enkripsinya 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

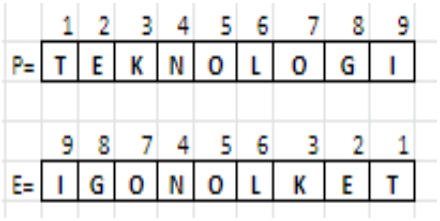
susunan sesuai ketentuan, dan menyusunnya kembali di akhir hasil teks yang dimampatkan. Berikut adalah contoh teknik pemampatan.



Gambar 2.2 Teknik Pemampatan

5. Teknik Permutasi (Algoritma Permutasi)

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



Gambar 2.3 Teknik Permutasi

Dengan beragam algoritma, 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 dianjurkan ($p \neq q$). (Zulfikar dkk., 2019) Sebaiknya bilangan yang besar agar tingkat keamanannya juga meningkat, rekomendasi prima adalah 100 digit (desimal), sehinga n mempunyai 200 digit lebih (Wulansari dkk., 2016).

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)

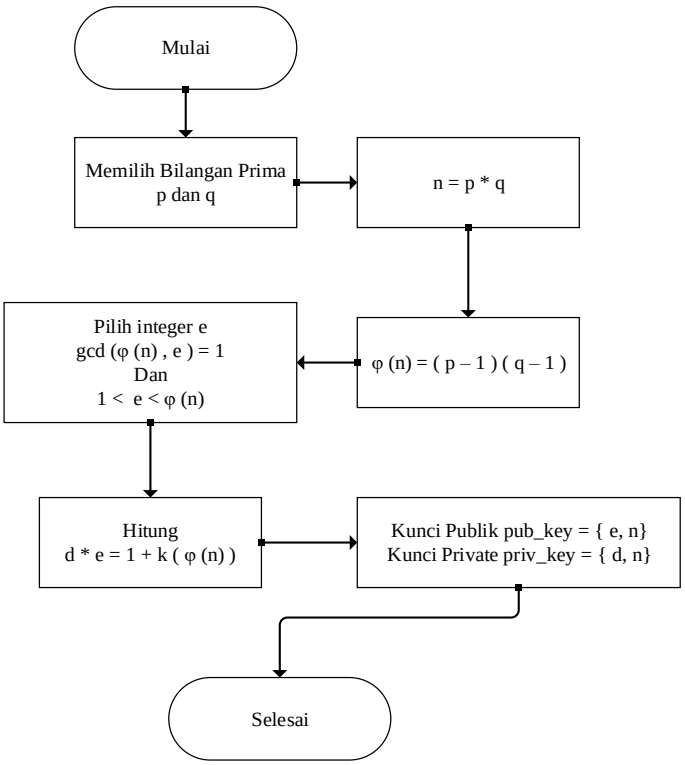
   Rekomendasi $Gcd(p-1, q-1)$ semakin besar maka semakin cepat pemfaktoran dan sebaliknya maka semakin lama (Muchlis dkk., 2017).

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 privat d dengan persamaan 2.3.

   $(e * d) mod \phi(n) = 1$ …… (2.3)

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



Gambar 2.4 *FlowChart* Pembangkitan Kunci Algoritma RSA

Untuk enkripsi $C \equiv P^e (mod\ n)$ dan dekripsi $\equiv C^e (mod\ n)$.

2.2.2 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 di antaranya adalah:

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

2.3.1 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 (Firmansyah, 2015). Teori ini merupakan hal yang mendasar untuk memahami algoritma kriptografi (Qorny, 2018).

2.3.2 Entropi dan Matrik

Entropi merupakan suatu parameter atau untuk mengukur tingkat keberagaman dari kumpulan data. Jika nilai dari entropi semakin besar, maka tingkat keberagaman suatu kumpulan data semakin besar (Kusuma dkk., 2018). Rumus untuk menghitung entropi sebagai berikut:

$$Entropi(S) = \sum_{i=1}^{m} \rho_i \log_2(\rho_i) \quad \text{.....(2.4)}$$

M = jumlah kelas klasifikasi

ρ_i = jumlah proporsi sampel (peluang) untuk kelas i

Sedangkan rumus untuk entropy masing-masing variabel adalah:

$$Entropi_A(S) = \sum_v \frac{|Sv|}{|S|} \text{Entropi(Sv)} \quad \text{.....(2.4)}$$

A = Variabel.

v = nilai yang mungkin untuk variable A.

|Sv| = Jumlah sampel untuk nilai v.

|S| = Jumlah sampel untuk seluruh sampel data.

Entropi(Sv) = Entropi untuk sampel yang memiliki nilai.

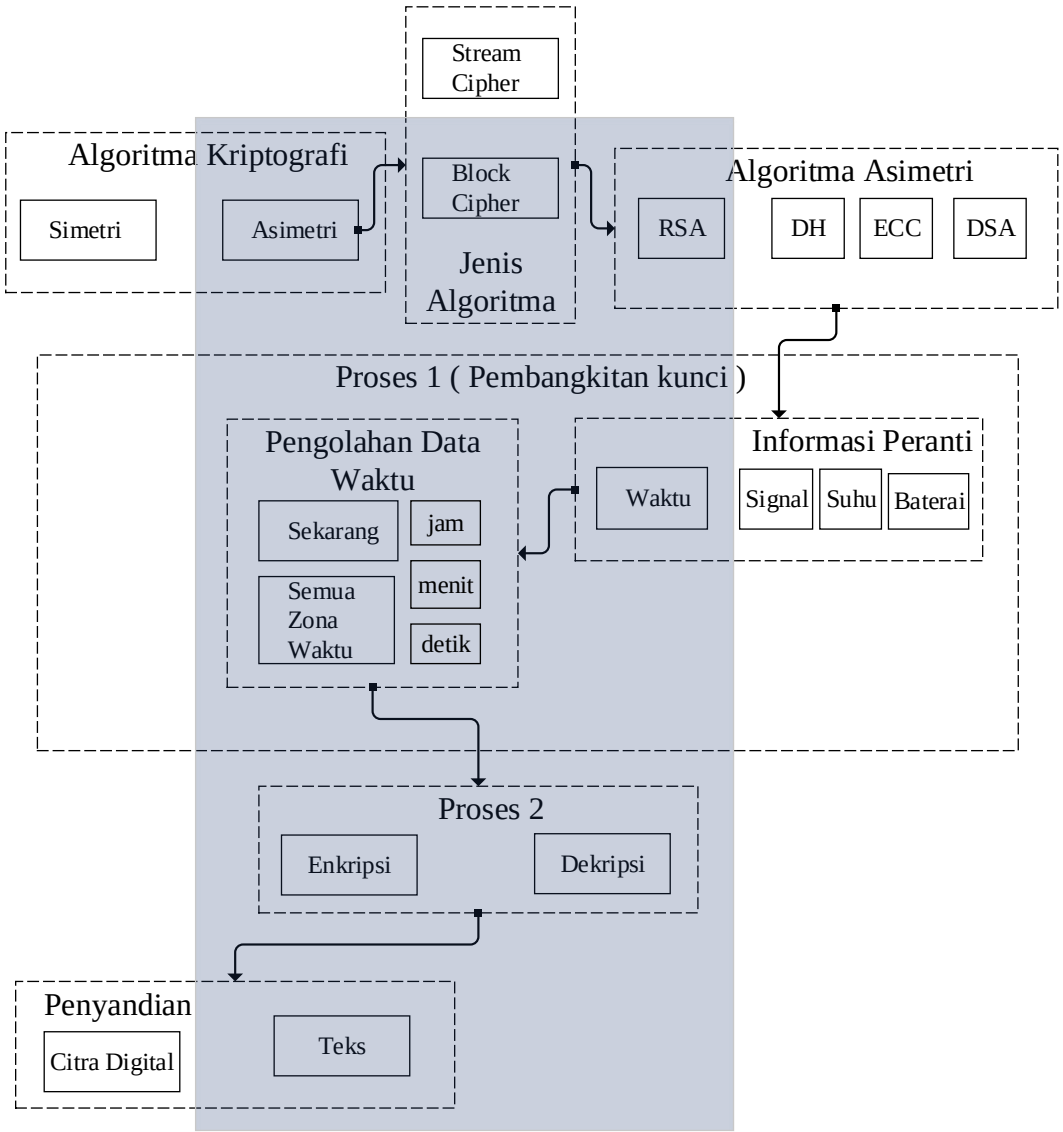
Ideal nilai entropi adalah 7,99902 (≈8) (Irfan & Prayudi, 2015). Matrik merupakan sekumpulan data baris dan kolom yang bisa dimainkan perhitungan atau aritmatika maupun logika (Qorny, 2018). Pada dasarnya hubungan entropi dan matrik adalah tentang dimensi, biasanya entropi menyangkut image proses, dimana matrik merepresentasikan gambar (Kusuma dkk., 2018).

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

Dalam kriptografi terdapat dua jenis algoritma berdasarkan kuncinya, yaitu:

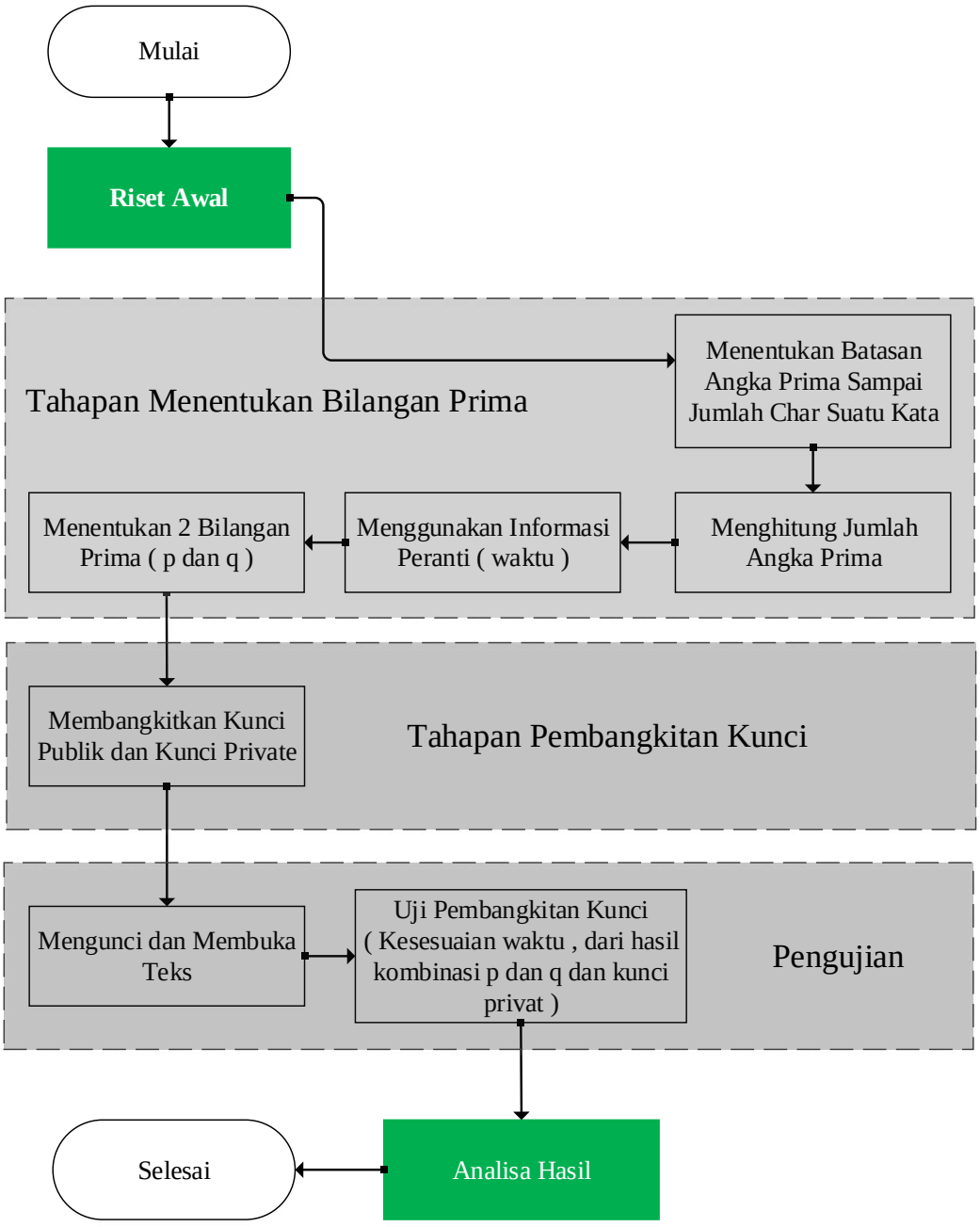
1. Algoritma Simetri
2. Algoritma Asimetri

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 banyaknya algoritma asimetri, yang digunakan adalah RSA dan jenis algoritma *cipher* adalah *block*. Proses pembangkitan kunci privat menggabungkan informasi peranti yaitu waktu. Proses enkripsi dan dekripsi adalah jenis data teks.

3.2 Metodologi Penelitian



Gambar 3.2 Diagram Alir Metodologi Penelitian

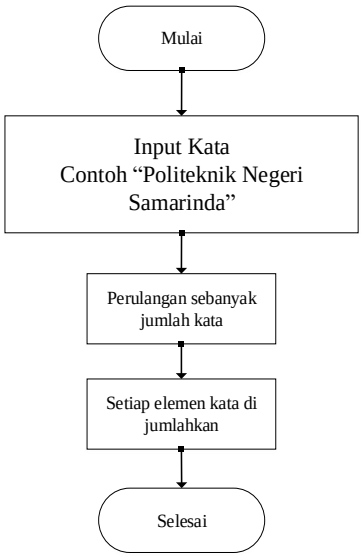
3.2.1 Riset Awal

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

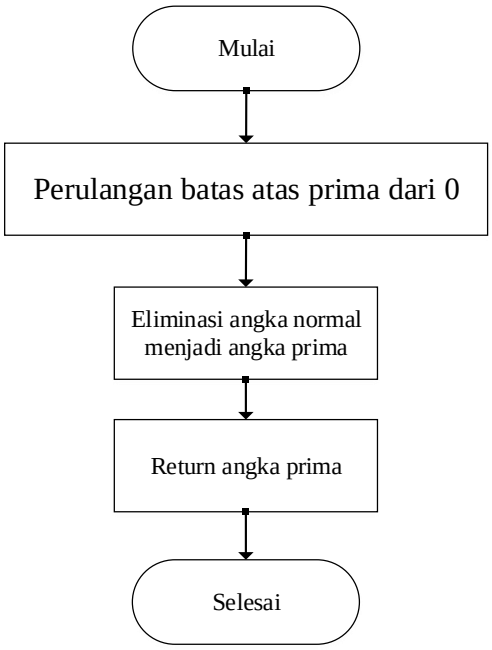
1. Konsep dasar Kriptografi
2. Mengetahui penggunaan informasi peranti
3. Landasan matematika (teori bilangan dan pemfaktoran bilangan bulat)
4. Algoritma *Rivest Shamir Adleman* (RSA)

3.2.2 Tahapan Menentukan Bilangan Prima

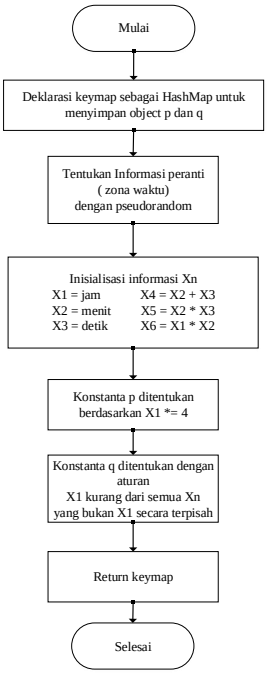
Tahapan menentukan bilangan prima adalah langkah lanjutan dalam poin utama tujuan penelitian berdasarkan informasi peranti yaitu waktu sekarang dan semua zona waktu yang ketentuanya posisinya berdasarkan *pseudorandom*. Ada 3 tahapan, yaitu mendapatkan batas atas prima, menghasilkan angka prima, dan menentukan konstanta atau orde p dan q.



Gambar 3.2.2 *FlowChart* Proses Pembangkit Batas Atas



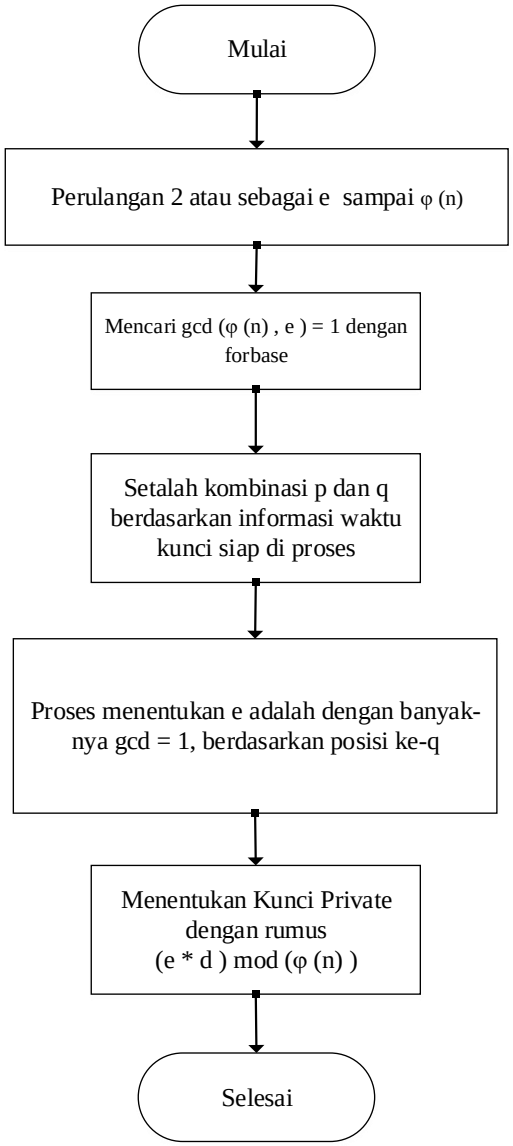
Gambar 3.2.3 *FlowChart* Proses Hasil Pembangkit Semua Angka Prima



Gambar 3.2.4 *FlowChart* Proses Terpilihnya konstanta atau orde P dan Q

3.2.3 Tahapan Pembangkitan Kunci

Tahapan pembangkitan kunci mengikuti pola pemilihan yang ditentukan dengan posisi secara *pseudorandom* berdasarkan informasi peranti. Pada proses pembangkitan kunci privat yaitu $e * d \, mod \, \varphi(n)$ dan $\mathrm{GCD}\,(\varphi\,(\mathrm{n})\,,\mathrm{e}\,) = 1$ merupakan nilai e yang pemilihannya adalah orde q.



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, dibandingkan dengan catatan nilai entropi semakin besar atau pola acak matrik.

3.2.5 Analisa Hasil

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

3.2.6 Variabel Penelitian

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

3.2.7 Waktu dan Tempat Penelitian

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

BAB IV
HASIL DAN PEMBAHASAN

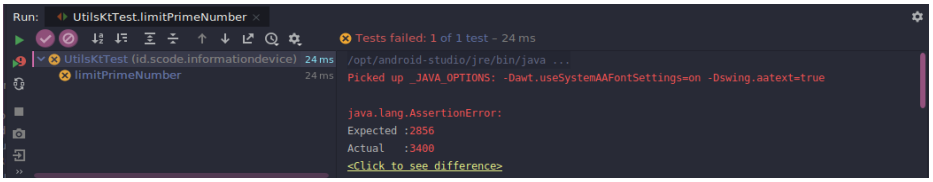
4.1 Hasil Menentukan Bilangan Prima

Sebelum mengkombinasikan waktu peranti, dan mengolahnya menjadi lebih berpola dalam pembangkitan kunci privat, bilangan prima yang digunakan, ditentukan sedemikian rupa oleh jumlah karakter dari suatu kata melalui proses input, sehingga cukup panjang untuk memfaktorkannya, dengan batasan yang lebih dari 3000 bilangan dan maksimal batasan adalah opsional, jika semakin tinggi maka proses eliminasi menambah sekian detik waktu. Hal tersebut juga menghasilkan angka-angka yang berbeda di setiap variabel (pada semua bilangan tanpa batasan), dalam hal ini menggunakan *Rivest Shamir Adleman* (RSA) sebagai acuan uji coba yaitu ordo atau konstanta p dan q, pada waktu sekarang dan zona berkondisikan random maupun bersamaan atau sebaliknya. Alur menentukan bilangannya, di atur dengan proses berikut:

4.1.1 Pembatasan Bilangan Prima

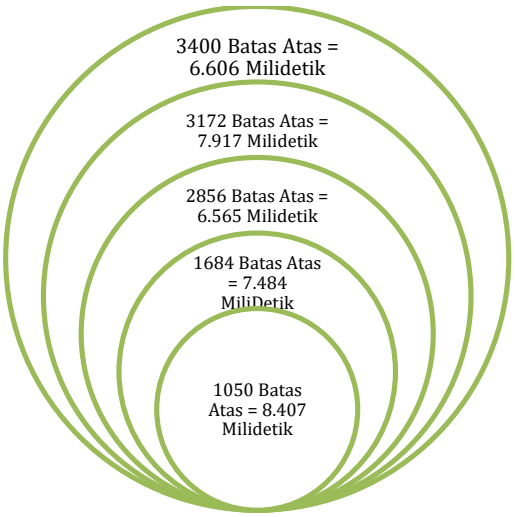
Pembatasan dimaksudkan menjaga ruang memori atau proses dalam menentukan bilangan normal ke prima (eliminasi angka bukan prima). *American Standard Code for Information Interchange* (ASCII) digunakan dalam masukan batasan. Sebagai contoh, kalimat ‘Politeknik Negeri Samarinda Tahun 2020’, setiap elemen atau karakter diubah menjadi *integer*, kemudian dijumlah secara *default* yaitu *ascending*, sehingga dihasilkan batas atas bernilai 3400. Pada Gambar 4.1.1.1 Hasil *JUnit Testing* Pengecekan Batas Atas Prima, uji coba batas atas dilakukan secara

komputer (dengan *unit testing*) terhadap *flowchart* program Gambar 4.1.1.3 *FlowChart* Program Pembangkit Batas Atas Angka Prima, bertujuan mengecek nilai 3400 adalah benar hasil dari contoh kalimat.



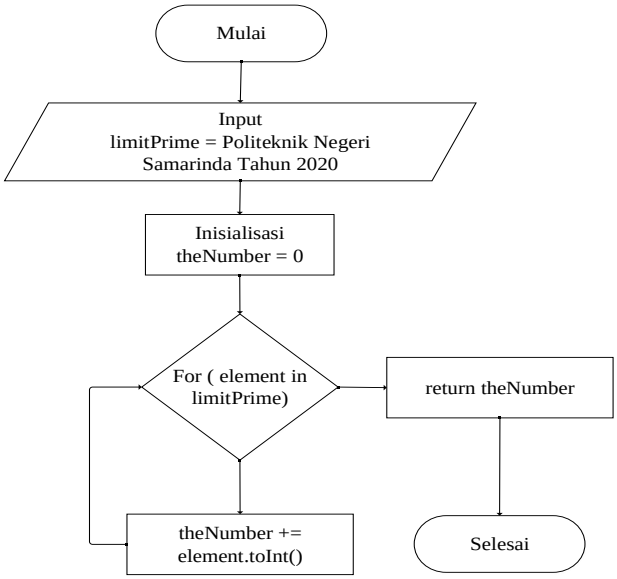
Gambar 4.1.1.1 Hasil *JUnit Testing* Pengecekan Batas Atas

Proses memasukan kalimat ASCII, memiliki aturan diatas batas nilai sekitar 2000 - 3000, bertujuan meluaskan rentang waktu berjalan pembangkitan angka prima menuju pada penggunaannya, sekitar 6.606 milidetik untuk contoh kalimat dan ilustrasi dijelaskan pada Gambar 4.1.1.2 Ilustrasi Hasil Pembangkitan Bilangan Atas, yang dilakukan uji coba dengan melihat waktu selesai *compiler*. Setiap tempo yang dihasilkan dipengaruhi oleh kondisi kecepatan peranti dalam memproses membaca program.



Gambar 4.1.1.2 Ilustrasi Hasil Pembangkitan Bilangan Atas.

Keseluruhan uji proses menghasilkan nilai yang logika (urut), tetapi saat peranti menjalankan banyak proses, menghasilkan rentang waktu yang berbeda. Logika yang berjalan dari Gambar 3.2.2 *FlowChart* Proses Pembangkit Batas Atas dan Gambar 4.1.1.2 Ilustrasi Hasil Pembangkitan Bilangan Atas, dimuat dalam *flowchart* program yang disajikan pada Gambar 4.1.1.3 *FlowChart* Program Pembangkit Batas Atas.



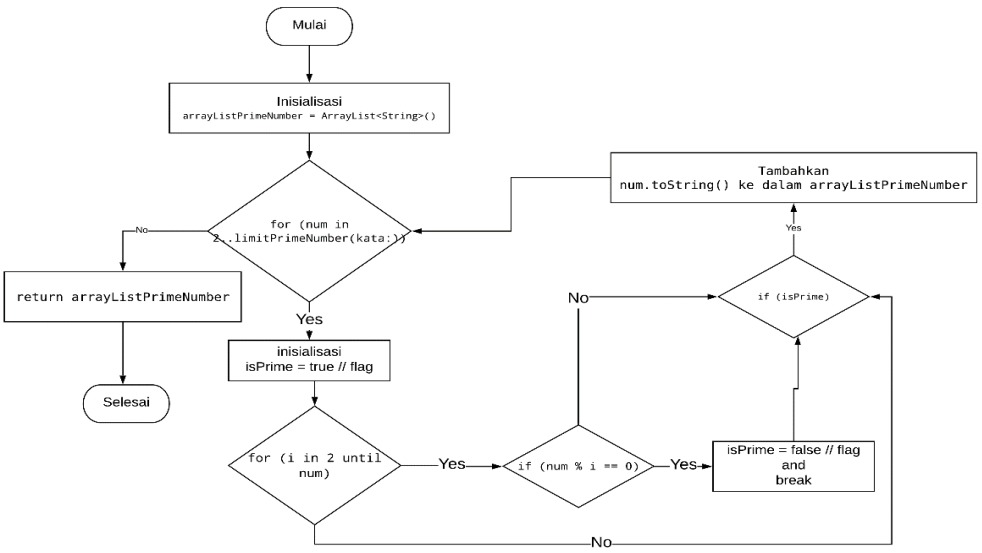
Gambar 4.1.1.3 *FlowChart* Program Pembangkit Batas Atas

4.1.2 Eliminasi Angka Bukan Prima

Eliminasi angka bukan prima yang dimaksud adalah mencari bilangan prima itu sendiri, dengan menyatakan proses menghasilkan bukan nol adalah benar dan sebaliknya adalah salah. Perhitungan rumus menggunakan sisa bagi, jika A = 3 dan nilai pembaginya (sisa bagi) B = 2, maka ditandai sebagai benar.

Pada pembatsan bilangan prima sebelumnya adalah 3400, dengan ketentuan sisa bagi, maka dihasilkan angka prima sebanyak 478, dan

rentang waktu sekitar 16.908 milidetik. Waktu ini mempengaruhi penggunaan informasi peranti sebelum terbangkitnya bilangan p dan q, sehingga waktu sekarang adalah **14:05:30 GMT+8**. Alur eliminasi sendiri memuat batas atas prima di dalam prosesnya, diperlihatkan pada Gambar 4.1.2.1 *FlowChart* Program Hasil Pembangkit Semua Angka Prima.



Gambar 4.1.2.1 *FlowChart* Program Hasil Pembangkit Semua Angka Prima

4.1.3 Zona waktu

Seluruh Zona waktu merupakan bagian dari informasi waktu yang digunakan. Greenwich Mean Time Zone (GMT) secara *default* adalah menyesuaikan waktu peranti dan hasil menentukan bilangan prima menggunakan Waktu Indonesia Tengah (WITA) dalam format **24 jam (HH:mm:ss)**.

Waktu Tengah Dunia					
GMT (-)				GMT (+)	
GMT-1	GMT-6			GMT+1	GMT+6
GMT-2	GMT-7			GMT+2	GMT+7
GMT-3	GMT-8			GMT+3	**GMT+8**
GMT-4	GMT-9			GMT+4	GMT+9
GMT-5	GMT-10			GMT+5	GMT+10
	GMT-11				GMT+11
					GMT+12
					GMT+13

Gambar 4.1.3.1 Daftar Waktu Indonesia Tengah

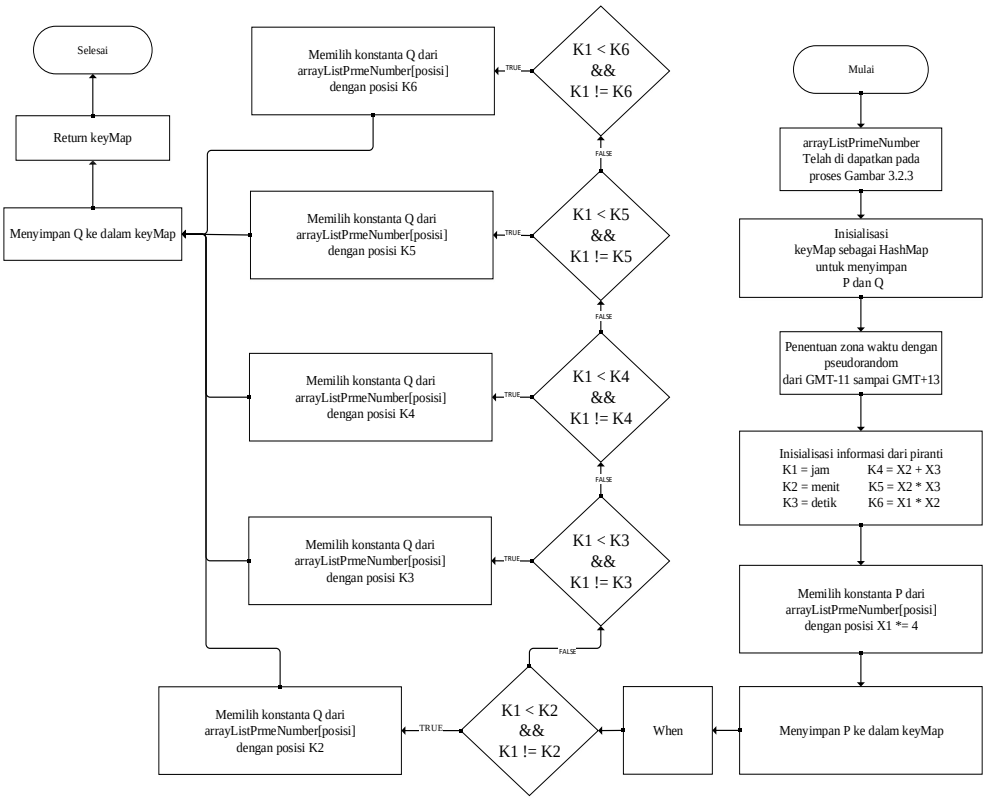
4.1.4 Pseudorandom

Random Number Generator (RNG) diimplementasi menggunakan *kotlin random* yang menghasilkan urutan angka *pseudo* atau simbol yang tidak dapat diprediksi. Seluruh zona waktu disimpan ke dalam *array string* yang telah disusun secara *ascending* dari minus (-) ke plus (+) dengan format *Extensible Markup Language* (XML).

Gambar 4.1.4.1 Proses *Pseudorandom* Zona Waktu

Pemilihan posisi berdasarkan keluaran dari nilai *integer* RNG, sehingga waktu sekarang adalah **10:05:31 GMT + 12** karena hasil nilai RNG adalah 22 dan dalam format **12 jam (hh:mm:ss)**.

4.1.5 P dan Q



Gambar 4.1.5.1 *FlowChart* Program Terpilihnya konstanta atau orde P dan Q

Nilai P dan Q adalah dua variable fokus dalam skema menggunakan informasi peranti (waktu). Nilai P dihasilkan dengan menghitung jam (hh) x 2 = 20 sebagai letak (posisi memilih) bilangan prima dalam daftar *array*, angka 2 merupakan bilangan sedemikian rupa untuk menghindari P < 10 sehingga nilai P = 73. Nilai Q memiliki aturan mirip dengan nilai P, tetapi memiliki 5 keputusan perhitungan dari 6 ketentuanya (K), yaitu:

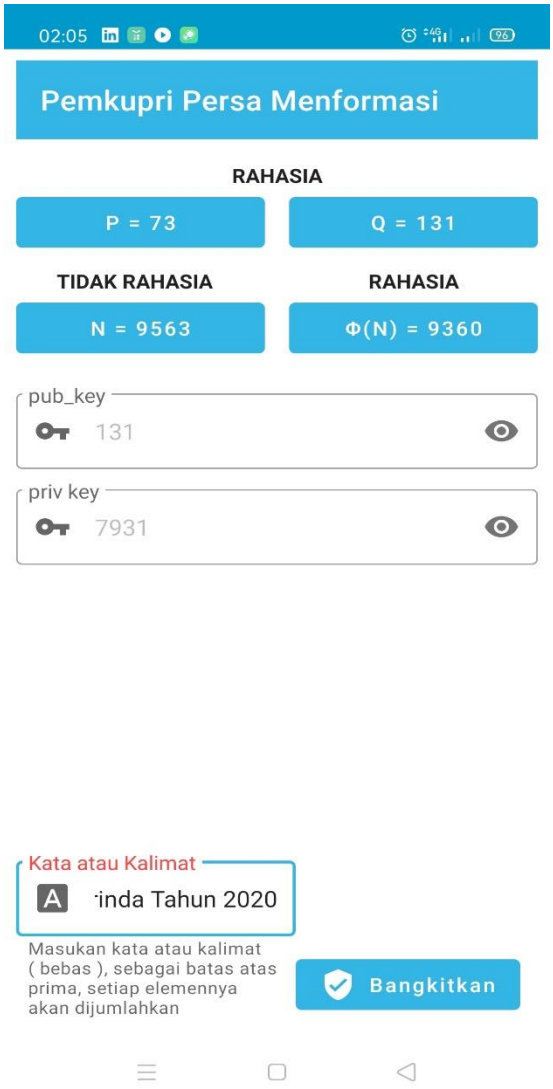
1. K1 merupakan posisi (P) sebelumnya
2. K2 adalah menit (mm)
3. K3 adalah detik (ss)

4. K4 adalah K2 + K3 (mm + ss)
5. K5 adalah K1 * K2 (P * mm)
6. K6 adalah K2 * K3 (mm * ss)

Keputusanya adalah ketika K1 < K (2 sampai 6) dan K1 ! = K (2 sampai 6), sehingga yang berjalan adalah keputusan ke 3, yaitu K3 dengan nilai 31 menghasilkan nilai Q = 131. Hasil *Greatest Common Divisor* (GCD) adalah 2 dimana hasil tersebut membuktikan nilai P dan Q atau (P – 1, Q – 1) memiliki waktu pemfaktoran yang tidak sebentar dan kedua variabel memiliki selisih yang cukup jauh sehingga lebih efisien.

4.2 Hasil Pembangkitan Kunci

Hasil *Greatest Common Divisor* (GCD) dari $(\varphi(n), e(i) = 1$ berjumlah sebanyak 2303, dimana i adalah 2 sampai 9360 ($\varphi(n)$). Data disimpan secara urut (*ascending*) posisinya ke dalam daftar *array*. Satu data diambil berdasarkan nilai Q = 131 sebagai posisinya yang dimana isi *array* menunjukan nilai yang persis secara kebetulan yaitu e = 131.



Gambar 4.2.1 Hasil Pembangkitan Kunci Pada Peranti *Android*

Nilai N atau $P * Q = 9563$ di definisikan menjadi rentang 1 sampai d, dimana $e * d \; mod \; \varphi(n)$ menghasilkan nilai 1, sehingga didapat $d = 7931$. Label rahasia merujuk pada besaran-besaran algoritma rsa dan kunci publik (pub_key) adalah e dan kunci privat (priv_key) adalah d.

4.3 Pengujian

Pengujian dilakukan dengan berbagai tahapan, pertama menggunakan 5 data pembangkitan kunci privat dengan eksperimen rentang waktu yang diambil secara 5 menit usai pembangkitan dan 2 data lainya secara tidak diperhitung. Pengujian kedua menggunakan 13 data dengan rentang waktu 5 menit secara aturan. Satu *PlainText* (m) sepanjang 242 berisi kode *American Standard Code for Information Interchange* (ASCII).

4.3.1 Pengujian Pertama

Tabel 4.3.1.1 Hasil Pengujian Pertama Enkripsi dan Dekripsi

PlainText (m) panjang ASCII m = 242	```Yogi Arif Widodo, [17.04.20 10:55]``` *assalamu'alaikum warrahmatullahi wabarakatuh* <!-- (CATATANBIASA~3986) Obat kehidupan adalah sederhana. Sederhana itu cara hidup. Cara hidup itu sederhana. #simpel-->				
Batas Atas Prima (BAP) 3400	Politeknik Negeri Samarinda Tahun 2020				
Rentang Waktu Awal Proses (HH : mm)	02:05:31 GMT +8	13:57:08 GMT +8	14:49:07 GMT +8	14:54:10 GMT +8	14:59:09 GMT +8
PEMBANGKITAN KE -	**1**	**2**	**3**	**4**	**5**
Rentang Waktu Setelah Proses Awal (hh : mm)	10:05:32 GMT + 12	14:57:09 GMT + 9	11:49:08 GMT + 5	09:54:11 GMT + 3	05:59:10 GMT - 1
P	73	47	83	67	31
Q	131	271	197	197	197
N ϕ (n)	9563 9360	12737 1240	16351 16072	13199 12936	6107 5880
pub_key (d) priv_key (e) *CipherText* (c)	131 7931 c1	227 383 c2	109 2949 c3	173 5309 c4	197 1373 c5
GCD (p - 1, q - 1)	2	2	2	2	2
GCD (ϕ (n) ,e) = 1, sebanyak	2303	3167	6719	3359	3359
Entropi Seluruh Nilai P	2.321928094887362				
Entropi Seluruh Nilai Q	1.370950594454668				
Entropi ASCII	4.814863028233948				
Entropi Blok *CipherText*	4.814863028233948				

Percobaan dilakukan dengan membatasi bilangan prima sampai jumlah seluruh elemen *string* dalam bentuk *integer* dari kalimat Batas Atas Prima (BAP), panjang kunci 2 *bit* sampai 14 *bit*, mengenkripsi m dan mendekripsi blok *cipherText* (c), memperhitungkan *Greatest Common Divisior* (GCD) dan entropi (m dan c) dalam bentuk *binary large object* (BLOB) atau semua data dalam bentuk *binary*.

Tabel 4.3.1.2 Hasil Kode ASCII *PlainText*

ASCII	010, 032, 032, 032, 032, 096, 096, 096, 089, 111, 103, 105, 032, 065, 114, 105, 102, 032, 087, 105, 100, 111, 100, 111, 044, 032, 091, 049, 055, 046, 048, 052, 046, 050, 048, 032, 049, 048, 058, 053, 053, 093, 096, 096, 096, 010, 032, 032, 032, 032, 042, 097, 115, 115, 097, 108, 097, 109, 117, 039, 097, 108, 097, 105, 107, 117, 109, 032, 119, 097, 114, 114, 097, 104, 109, 097, 116, 117, 108, 108, 097, 104, 105, 032, 119, 097, 098, 097, 114, 097, 107, 097, 116, 117, 104, 042, 010, 032, 032, 032, 032, 060, 033, 045, 045, 010, 032, 032, 032, 032, 032, 040, 067, 065, 084, 065, 084, 065, 078, 066, 073, 065, 083, 065, 126, 051, 057, 056, 054, 041, 010, 032, 032, 032, 032, 079, 098, 097, 116, 032, 107, 101, 104, 105, 100, 117, 112, 097, 110, 032, 097, 100, 097, 108, 097, 104, 032, 115, 101, 100, 101, 114, 104, 097, 110, 097, 046, 010, 032, 032, 032, 032, 083, 101, 100, 101, 114, 104, 097, 110, 097, 032, 105, 116, 117, 032, 099, 097, 114, 097, 032, 104, 105, 100, 117, 112, 046, 010, 032, 032, 032, 032, 067, 097, 114, 097, 032, 104, 105, 100, 117, 112, 032, 105, 116, 117, 032, 115, 101, 100, 101, 114, 104, 097, 110, 097, 046, 032, 035, 115, 105, 109, 112, 101, 108, 045, 045, 062, 010, 032, 032, 032, 032

Tabel 4.3.1.3 Hasil Enkripsi atau *ChiperText*

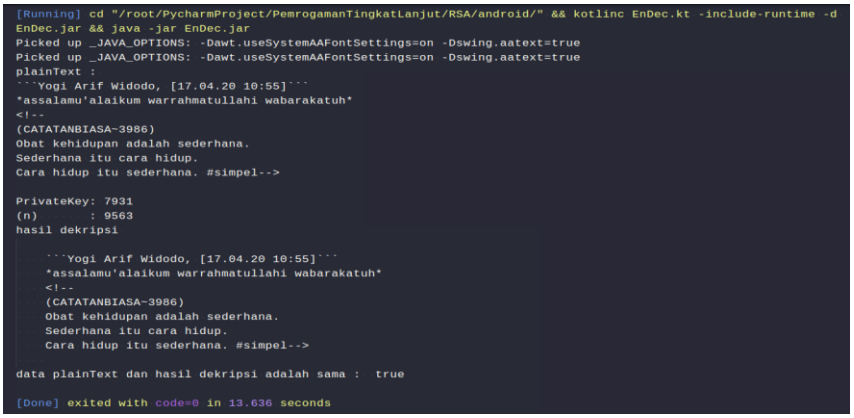
c1	0927, 6844, 6844, 6844, 6844, 4812, 4812, 4812, 4019, 4434, 9142, 6917, 6844, 8842, 2865, 6917, 5211, 6844, 4803, 6917, 8222, 4434, 8222, 4434, 4498, 6844, 3759, 5551, 5950, 1487, 8956, 0445, 1487, 4897, 8956, 6844, 5551, 8956, 2940, 2018, 2018, 7691, 4812, 4812, 4812, 0927, 6844, 6844, 6844, 6844, 1090, 4158, 1163, 1163, 4158, 5348, 4158, 7576, 4571, 6851, 4158, 5348, 4158, 6917, 2858, 4571, 7576, 6844, 1560, 4158, 2865, 2865, 4158, 8619, 7576, 4158, 0640, 4571, 5348, 5348, 4158, 8619, 6917, 6844, 1560, 4158, 0753, 4158, 2865, 4158, 2858, 4158, 0640, 4571, 8619, 1090, 0927, 6844, 6844, 6844, 6844, 4121, 1212, 5809, 5809, 0927, 6844, 6844, 6844, 6844, 8424, 4783, 8842, 3490, 8842, 3490, 8842, 7021, 0459, 073, 8842, 1000, 8842, 2091, 8697, 5690, 9095, 4246, 2792, 0927, 6844, 6844, 6844, 6844, 4926, 0753, 4158, 0640, 6844, 2858, 3900, 8619, 6917, 8222, 4571, 6924, 4158, 2206, 6844, 4158, 8222, 4158, 5348, 4158, 8619, 6844, 1163, 3900, 8222, 3900, 2865, 8619, 4158, 2206, 4158, 1487, 0927, 6844, 6844, 6844, 6844, 1000, 3900, 8222, 3900, 2865, 8619, 4158, 2206, 4158, 6844, 6917, 0640, 4571, 6844, 0623, 4158, 2865, 4158, 6844, 8619, 6917, 8222, 4571, 6924, 1487, 0927, 6844, 6844, 6844, 6844, 4783, 4158, 2865, 4158, 6844, 8619, 6917, 8222, 4571, 6924, 6844, 6917, 0640, 4571, 6844, 1163, 3900, 8222, 3900, 2865, 8619, 4158, 2206, 4158, 1487, 6844, 5275, 1163, 6917, 7576, 6924, 3900, 5348, 5809, 5809, 6219, 0927, 6844, 6844, 6844, 6844
c2	4165, 1572, 1572, 1572, 1572, 5364, 5364, 5364, 3904, 2570, 2634, 10926, 1572, 5276, 1161, 10926, 5856, 1572, 6214, 10926, 12168, 2570, 12168, 2570, 4646, 1572, 11696, 11944, 2754, 12313, 1505, 2065, 12313, 11193, 1505, 1572, 11944, 1505, 5145, 9818, 9818, 4088, 5364, 5364, 5364, 4165, 1572, 1572, 1572, 1572, 5079, 7010, 11539, 11539, 7010, 8635, 7010, 4444, 4739, 10735, 7010, 8635, 7010, 10926, 12216, 4739, 4444, 1572, 3863, 7010, 1161, 1161, 7010, 10322, 4444, 7010, 12117, 4739, 8635, 8635, 7010, 10322, 10926, 1572, 3863, 7010, 12585, 7010, 1161, 7010, 12216, 7010, 12117, 4739, 10322, 5079, 4165, 1572, 1572, 1572, 1572, 0607, 3397, 9817, 9817, 4165, 1572, 1572, 1572, 1572, 11196, 5861, 5276, 1616, 5276, 1616, 5276, 8386, 9196, 11491, 5276, 9425, 5276, 9844, 4407, 7314, 2822, 0554, 11708, 4165, 1572, 1572, 1572, 1572, 8951, 12585, 7010, 12117, 1572, 12216, 2716, 10322, 10926, 12168, 4739, 7062, 7010, 6278, 1572, 7010, 12168, 7010, 8635, 7010, 10322, 1572, 11539, 2716, 12168, 2716, 1161, 10322, 7010, 6278, 7010, 12313, 4165, 1572, 1572, 1572, 1572, 9425, 2716, 12168, 2716, 1161, 10322, 7010, 6278, 7010, 1572, 10926, 12117, 4739, 1572, 10619, 7010, 1161, 7010, 1572, 10322, 10926, 12168, 4739, 7062, 12313, 4165, 1572, 1572, 1572, 1572, 5861, 7010, 1161, 7010, 1572, 10322, 10926, 12168, 4739, 7062, 1572, 10926, 12117, 4739, 1572, 11539, 2716, 12168, 2716, 1161, 10322, 7010, 6278, 7010, 12313, 1572, 10981, 11539, 10926, 4444, 7062, 2716, 8635, 9817, 9817, 9661, 4165, 1572, 1572, 1572, 1572
c3	14223, 3457, 3457, 3457, 3457, 12387, 12387, 12387, 12541, 12793, 15422, 5704, 3457, 9499, 10871, 5704, 0145, 3457, 11313, 5704, 15508, 12793, 15508, 12793, 4035, 3457, 13073, 8531, 15261, 16313, 11790, 9464, 16313, 4413, 11790, 3457, 8531, 11790, 1707, 5181, 5181, 4761, 12387, 12387, 12387, 14223, 3457, 3457, 3457, 3457, 12583, 4783, 13666, 13666, 4783, 16221, 4783, 0515, 4500, 14225, 4783, 16221, 4783, 5704, 9994, 4500, 0515, 3457, 4380, 4783, 10871, 10871, 4783, 13954, 0515, 4783, 14013, 4500, 16221, 16221, 4783, 13954, 5704, 3457, 4380, 4783, 4973, 4783, 10871, 4783, 9994, 4783, 14013, 4500, 13954, 12583, 14223, 3457, 3457, 3457, 3457, 1070, 2974, 8488, 8488, 14223, 3457, 3457, 3457, 3457, 3240, 11825, 9499, 15937, 9499, 15937, 9499, 2318, 13293, 15989, 9499, 8632, 9499, 6222, 15301, 16002, 10513, 5452, 12566, 14223, 3457, 3457, 3457, 3457, 3544, 4973, 4783, 14013, 3457, 9994, 14405, 13954, 5704, 15508, 4500, 13887, 4783, 3265, 3457, 4783, 15508, 4783, 16221, 4783, 13954, 3457, 13666, 14405, 15508, 14405, 10871, 13954, 4783, 3265, 4783, 16313, 14223, 3457, 3457, 3457, 3457, 8632, 14405, 15508, 14405, 10871, 13954, 4783, 3265, 4783, 3457, 5704, 14013, 4500, 3457, 2119, 4783, 10871, 4783, 3457, 13954, 5704, 15508, 4500, 13887, 16313, 14223, 3457, 3457, 3457, 3457, 11825, 4783, 10871, 4783, 3457, 13954, 5704, 15508, 4500, 13887, 3457, 5704, 14013, 4500, 3457, 13666, 14405, 15508, 14405, 10871, 13954, 4783, 3265, 4783, 16313, 3457, 12944, 13666, 5704, 0515, 13887, 14405, 16221, 8488, 8488, 1733, 14223, 3457, 3457, 3457, 3457
c4	7659, 10982, 10982, 10982, 10982, 12566, 12566, 12566, 11899, 9726, 4873, 9879, 10982, 5214, 7453, 9879, 3423, 10982, 7555, 9879, 3925, 9726, 3925, 9726, 12339, 10982, 10650, 0839, 3568, 0940, 6463, 075, 0940, 0690, 6463, 10982, 0839, 6463, 2320, 9023, 9023, 3038, 12566, 12566, 12566, 7659, 10982, 10982, 10982, 10982, 0981, 2182, 5793, 5793, 2182, 10362, 2182, 11433, 12147, 6637, 2182, 10362, 2182, 9879, 3359, 12147, 11433, 10982, 6641, 2182, 7453, 7453, 2182, 7600, 11433, 2182, 1911, 12147, 10362, 10362, 2182, 7600, 9879, 10982, 6641, 2182, 1425, 2182, 7453, 2182, 3359, 2182, 1911, 12147, 7600, 0981, 7659, 10982, 10982, 10982, 10982, 10573, 12769, 11886, 11886, 7659, 10982, 10982, 10982, 10982, 6374, 6700, 5214, 7015, 5214, 7015, 5214, 3800, 4823, 8502, 5214, 033, 5214, 7853, 5461, 8019, 1962, 9741, 11166, 7659, 10982, 10982, 10982, 10982, 1725, 1425, 2182, 1911, 10982, 3359, 7331, 7600, 9879, 3925, 12147, 0831, 2182, 9584, 10982, 2182, 3925, 2182, 10362, 2182, 7600, 10982, 5793, 7331, 3925, 7331, 7453, 7600, 2182, 9584, 2182, 0940, 7659, 10982, 10982, 10982, 10982, 033, 7331, 3925, 7331,

	7453, 7600, 2182, 9584, 2182, 10982, 9879, 1911, 12147, 10982, 11183, 2182, 7453, 2182, 10982, 7600, 9879, 3925, 12147, 0831, 0940, 7659, 10982, 10982, 10982, 10982, 6700, 2182, 7453, 2182, 10982, 7600, 9879, 3925, 12147, 0831, 10982, 9879, 1911, 12147, 10982, 5793, 7331, 3925, 7331, 7453, 7600, 2182, 9584, 2182, 0940, 10982, 9453, 5793, 9879, 11433, 0831, 7331, 10362, 11886, 11886, 1623, 7659, 10982, 10982, 10982, 10982
c5	2177, 032, 032, 032, 032, 2657, 2657, 2657, 2650, 5036, 2270, 2863, 032, 2626, 4054, 2863, 3057, 032, 0284, 2863, 0297, 5036, 0297, 5036, 1226, 032, 5607, 4974, 5965, 2410, 1230, 3992, 2410, 3399, 1230, 032, 4974, 1230, 2619, 3205, 3205, 093, 2657, 2657, 2657, 2177, 032, 032, 032, 032, 3785, 3643, 3267, 3267, 3643, 2472, 3643, 3852, 6027, 4373, 3643, 2472, 3643, 2863, 5032, 6027, 3852, 032, 0316, 3643, 4054, 4054, 3643, 3847, 3852, 3643, 1889, 6027, 2472, 2472, 3643, 3847, 2863, 032, 0316, 3643, 6008, 3643, 4054, 3643, 5032, 3643, 1889, 6027, 3847, 3785, 2177, 032, 032, 032, 032, 5576, 0624, 4970, 4970, 2177, 032, 032, 032, 032, 2995, 5977, 2626, 3236, 2626, 3236, 2626, 3821, 3612, 3816, 2626, 4023, 2626, 0717, 2415, 0254, 0253, 1827, 2208, 2177, 032, 032, 032, 032, 1261, 6008, 3643, 1889, 032, 5032, 4435, 3847, 2863, 0297, 6027, 3461, 3643, 1292, 032, 3643, 0297, 3643, 2472, 3643, 3847, 032, 3267, 4435, 0297, 4435, 4054, 3847, 3643, 1292, 3643, 2410, 2177, 032, 032, 032, 032, 4023, 4435, 0297, 4435, 4054, 3847, 3643, 1292, 3643, 032, 2863, 1889, 6027, 032, 6009, 3643, 4054, 3643, 032, 3847, 2863, 0297, 6027, 3461, 2410, 2177, 032, 032, 032, 032, 5977, 3643, 4054, 3643, 032, 3847, 2863, 0297, 6027, 3461, 032, 2863, 1889, 6027, 032, 3267, 4435, 0297, 4435, 4054, 3847, 3643, 1292, 3643, 2410, 032, 3581, 3267, 2863, 3852, 3461, 4435, 2472, 4970, 4970, 062, 2177, 032, 032, 032, 032

Tabel 4.3.1.4 Hasil Probabilitas *Binary ChiperText*

c1	927=8, 6844=48, 4812=6, 4019=1, 4434=3, 9142=1, 6917=11, 8842=6, 2865=9, 5211=1, 4803=1, 8222=9, 4498=1, 3759=1, 5551=2, 5950=1, 1487=5, 8956=3, 445=1, 4897=1, 2940=1, 2018=2, 7691=1, 1090=2, 4158=28, 1163=5, 5348=6, 7576=4, 4571=9, 6851=1, 2858=3, 1560=2, 8619=10, 640=5, 753=2, 4121=1, 1212=1, 5809=4, 8424=1, 4783=2, 3490=2, 7021=1, 459=1, 73=1, 1000=2, 2091=1, 8697=1, 5690=1, 9095=1, 4246=1, 2792=1, 4926=1, 3900=8, 6924=4, 2206=4, 623=1, 5275=1, 6219=1
c2	4165=8, 1572=48, 5364=6, 3904=1, 2570=3, 2634=1, 10926=11, 5276=6, 1161=9, 5856=1, 6214=1, 12168=9, 4646=1, 11696=1, 11944=2, 2754=1, 12313=5, 1505=3, 2065=1, 11193=1, 5145=1, 9818=2, 4088=1, 5079=2, 7010=28, 11539=5, 8635=6, 4444=4, 4739=9, 10735=1, 12216=3, 3863=2, 10322=10, 12117=5, 12585=2, 607=1, 3397=1, 9817=4, 11196=1, 5861=2, 1616=2, 8386=1, 9196=1, 11491=1, 9425=2, 9844=1, 4407=1, 7314=1, 2822=1, 554=1, 11708=1, 8951=1, 2716=8, 7062=4, 6278=4, 10619=1, 10981=1, 9661=1
c3	14223=8, 3457=48, 12387=6, 12541=1, 12793=3, 15422=1, 5704=11, 9499=6, 10871=9, 145=1, 11313=1, 15508=9, 4035=1, 13073=1, 8531=2, 15261=1, 16313=5, 11790=3, 9464=1, 4413=1, 1707=1, 5181=2, 4761=1, 12583=2, 4783=28, 13666=5, 16221=6, 515=4, 4500=9, 14225=1, 9994=3, 4380=2, 13954=10, 14013=5, 4973=2, 1070=1, 2974=1, 8488=4, 3240=1, 11825=2, 15937=2, 2318=1, 13293=1, 15989=1, 8632=2, 6222=1, 15301=1, 16002=1, 10513=1, 5452=1, 12566=1, 3544=1, 14405=8, 13887=4, 3265=4, 2119=1, 12944=1, 1733=1
c4	7659=8, 10982=48, 12566=6, 11899=1, 9726=3, 4873=1, 9879=11, 5214=6, 7453=9, 3423=1, 7555=1, 3925=9, 12339=1, 10650=1, 839=2, 3568=1, 940=5, 6463=3, 75=1, 690=1, 2320=1, 9023=2, 3038=1, 981=2, 2182=28, 5793=5, 10362=6, 11433=4, 12147=9, 6637=1, 3359=3, 6641=2, 7600=10, 1911=5, 1425=2, 10573=1, 12769=1, 11886=4, 6374=1, 6700=2, 7015=2, 3800=1, 4823=1, 8502=1, 33=2, 7853=1, 5461=1, 8019=1, 1962=1, 9741=1, 11166=1, 1725=1, 7331=8, 831=4, 9584=4, 11183=1, 9453=1, 1623=1
c5	2177=8, 32=48, 2657=6, 2650=1, 5036=3, 2270=1, 2863=11, 2626=6, 4054=9, 3057=1, 284=1, 297=9, 1226=1, 5607=1, 4974=2, 5965=1, 2410=5, 1230=3, 3992=1, 3399=1, 2619=1, 3205=2, 93=1, 3785=2, 3643=28, 3267=5, 2472=6, 3852=4, 6027=9, 4373=1, 5032=3, 316=2, 3847=10, 1889=5, 6008=2, 5576=1, 624=1, 4970=4, 2995=1, 5977=2, 3236=2, 3821=1, 3612=1, 3816=1, 4023=2, 717=1, 2415=1, 254=1, 253=1, 1827=1, 2208=1, 1261=1, 4435=8, 3461=4, 1292=4, 6009=1, 3581=1, 62=1

Hasil enkripsi didefinisikan dalam variabel c[i] dimana i adalah proses ke (dari pembangkitan ke- (P-[i])). Ukuran probabilitas c[i] memiliki kesamaan dengan kode ASCII yaitu sebanyak 58 terhadap seluruh data.



Gambar 4.3.1.5 Hasil Pengujian Pertama Dekripsi *PlainText*

Masing-masing dekripsi pesan diuji dengan kunci yang sesuai untuk m berupa elemen panjang dan isinya menghasilkan kondisi *true*. Menggunakan pembangkitan pertama yang diperlihatkan pada Gambar 4.3.1.5 Hasil Pengujian Dekripsi *PlainText*.

4.3.2 Pengujian Kedua

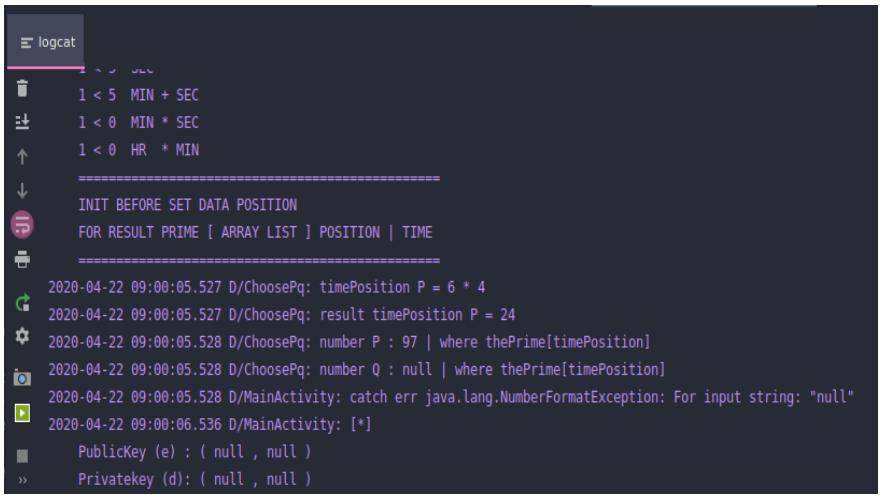
Pengujian kedua dibuat karena mendapti sebuah *bug* atau *crash* atau berupa *exception* posisi yaitu aritmatika waktu yang mengakibatkan *index out of bound* terhadap posisi Q.

RWAP (HH:mm:ss)	DATA	RWSPA (hh:mm:ss)	Pseudo RNG GMT POSISI	P	Q	GCD (p - 1, q - 1)
11:00:05 GMT + 8	1	05:00:06 GMT +2	12	73	3251	2
11:05:05 GMT +8	2	12:05:06 GMT +7	17	227	283	2
11:10:05 GMT +8	3	09:10:06 GMT -2	1	157	467	2
11:15:04 GMT +8	4	12:15:05 GMT -5	4	227	1087	2
11:20:05 GMT +8	5	10:20:06 GMT +9	19	179	1229	2
11:25:04 GMT +8	6	05:25:05 GMT +2	12	73	101	4
11:30:04 GMT +8	7	11:30:05 GMT +8	18	197	2221	4

11:35:04 GMT +8	8	03:35:05 GMT +4	14	41	151	10
11:40:05 GMT +8	9	08:40:06 GMT +11	21	137	179	2
11:45:10 GMT +8	10	03:45:12 GMT +4	14	41	199	2
11:50:05 GMT +8	11	08:50:06 GMT +11	21	137	233	8
11:55:04 GMT +8	12	01:55:04 GMT +6	16	11	263	2
12:00:04 GMT +8	13	04:00:05 GMT +4	14	59	3271	2
Entropi Seluruh Nilai P			3.085055102756477			
Entropi Seluruh Nilai Q			3.7004397181410926			

Gambar 4.3.2.1 Tabel Hasil Pengujian Kedua Pada orde P dan Q

Dengan menaikan perhitungan pada waktu pemilihan P (dimana hh * 4) dan pada orde Q ketika *index* posisi melampaui batas ukuran yang dibangkitkan, maka Q mengambil posisi akhir daftar *array* prima dikurang hh (ukuran *array* – hh).



Gambar 4.3.2.2 Hasil Pengujian Kedua Mengalami Null

Ketika Ketentuan (K) tidak terpenuhi mengakibatkan Q *null* dan melemparkan sebuah exception berupa *NumberFormatException*, sehingga pembangkitan kunci tidak berjalan semestinya saat menit (mm) adalah 0 dan

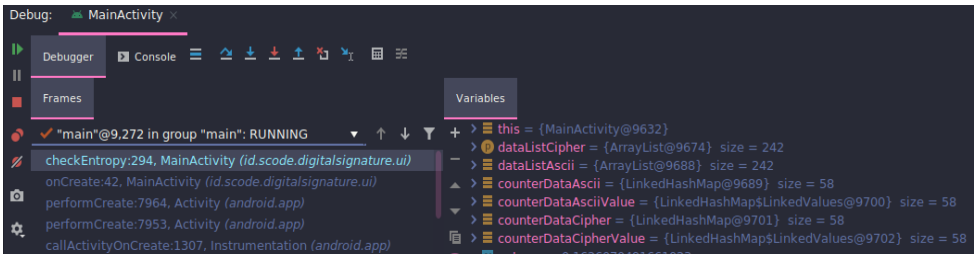
detik (ss) berapa di bawah P. Ketentuan *null* ditambahkan untuk menghindari hal tersebut dan nilai nya adalah posisi ukuran *array* – hh, seperti ketika menghindari *index out of bound*. Dekripsi pesan

4.4 Analisa Hasil P dan Q

Analisa hasil P dan Q dilakukan untuk melihat kunci privat sesuai (enkripsi dan dekripsi) dengan informasi peranti waktu yang berbeda. P dan Q dipilih berdasarkan nilai posisi secara acak (*pseudorandom*) serta waktu awal proses (HH:mm:ss) sampai perhitungan batas atas prima (hh:mm:ss) sehingga membuat P dan Q lebih tidak terduga dengan adanya 24 macam atau jenis *Greenwich Mean Time Zone* (GMT). Analisa memiliki 2 hasil yang saling berhubungan.

4.4.1 Analisa Hasil P dan Q Pengujian Pertama

Dari 5 data menghasilkan nilai entropi P = 2.321928094887362 (semua daftar bilangan adalah berbeda) dan Q = 1.370950594454668 (3 dari 5 bilangan adalah persis). Hasil *Greatest Common Divisor* (GCD) konstanta di angka 2. Variabel tersebut melakukan perhitungan algoritma *Rivest Shamir Adleman* (RSA) menghasilkan enkripsi berupa blok cipher (c) bernilai entropi 4.814863028233948 dari kode ASCII sepanjang 242 yang juga bernilai sama dengan hasil entropi c.



Gambar 4.4.1.1 Analisa Hasil Probabilitas ASCII dan *CipherText*

Daftar *binary* antara c dan ASCII memiliki probabilitas berjumlah 58 diperlihatkan pada Gambar 4.4.1.2 Analisa Hasil Probabilitas Blok *Cipher* dan Kode ASCII.

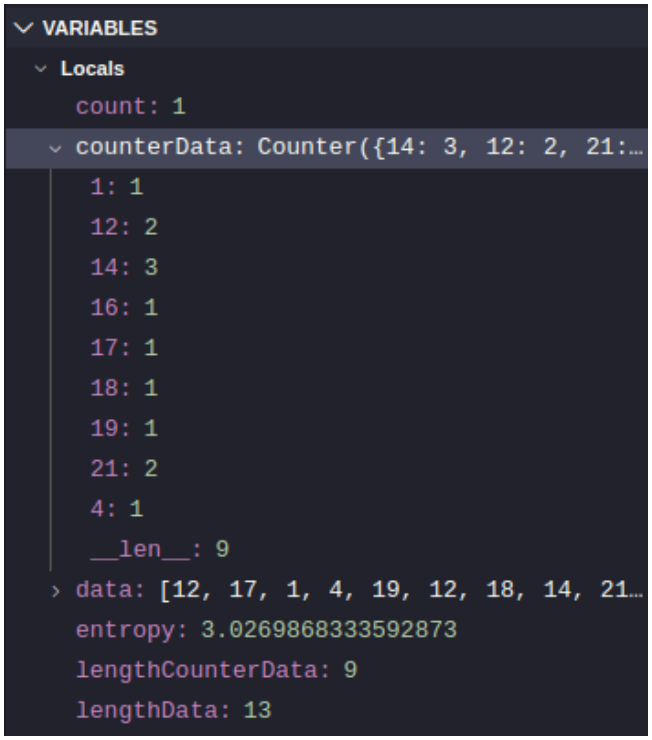
DATA	P	Q	P - Q
1	73	131	58
2	47	271	224
3	**83**	**197**	**114**
4	**67**	**197**	**130**
5	**31**	**107**	**76**
RATA-RATA			**120,4**

Gambar 4.4.1.2 Analisa Hasil Jarak Rentang Nilai P dan Q

Pembangkitan (data) P dan Q memiliki jarak rentang nilai rata-rata 120.4 (khusus pembangkitan setelah 5 menit bernilai rata-rata 269.3 dari 3 buah data) dan P selalu lebih kecil dari Q.

4.4.2 Analisa Hasil P dan Q Pengujian Kedua

Analisa hasil P dan Q Pengujian kedua, memiliki hasil Q yang tinggi ketika ketentuan tidak terpenuhi dengan begitu nilai Q mudah diperhitungkan namun telah diatasi dengan bergantung pada batas atas yang digunakan dan hasil konversi zona waktu sehingga membuat nilai P dan Q lebih tidak terduga walaupun dibangkitkan pada menit dan detik (mm:ss) adalah 0 atau dibawah P dan kondisi proses atau memori peranti yang digunakan.



Gambar 4.4.2.1 Analisa Hasil Entropi PRNG Zona Waktu Dalam 5 Menit

Pseudorandom Random Number Generate (PRNG) penentuan posisi zona waktu menghasilkan entropi 3.085055102756477 dari 13 data PRNG setiap 5 menit dalam kurung waktu 1 jam mendekati hasil nilai entropi 3.7004397181410926 sebagai acuan dari 13 data jika seluruhnya adalah acak. Hasil entropi pada text bernilai persis dengan hasil pengujian pertama yaitu 4.814863028233948.

BAB V PENUTUP

5.1 Kesimpulan

Penlitian dan percobaan yang telah dilakukan menghasilkan kesimpulan sebagai berikut:

1. Proses mendapatkan waktu (HH:mm:ss dan hh:mm:ss) sekarang yang diterapkan bergantung peranti yang digunakan, ketika peranti memiliki ruang *memory* pengunaan yang besar, mampu melakukan perhitungan dan proses lebih cepat (berbeda). Sehingga data waktu dan perhitungan membuat hasil P dan Q lebih efisien dengan melihat hasil $\mathrm{GCD}(P-1, Q-1)$ tidak terlalu besar dan rentang dua variabel itu sendiri.
2. Dari Analisa Hasil P dan Q
    a. Pengujian pertama dengan panjang kunci 2 *bit* sampai 14 *bit*, keduanya telah membangkitkan kunci privat yang mampu mendekripsi kode ASCII. Entropi (bagian yang terenkripsi) Blok *CipherText* menunjukan indikasi setengah ideal yaitu 4.814863028233948 dan probabilitas elemen *binary cipherText* berjumlah 58. P dan Q memiliki rentang jarak nilai rata-rata 269.3 dalam waktu 5 menit dan seluruh data memiliki rata-rata 120.4.
    b. Pengujian kedua dengan menaikan pemilihan P adalah hh * 4 dan ditambahkanya ketentuan Q adalah batas prima dikurang posisi P, menghasilkan P dan Q yang memiliki

kemungkinan rentang cukup jauh pada saat menit dan detik kecil antara 0 – 20 dan posisi P adalah puluhan atau lebih besar dari mm:ss. Kedua variabel menghasilkan GCD rata-rata adalah 2.

5.2 Saran

Asd

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

Firmansyah, F. F. 2015. Kajian matematis dan penggunaan bilangan prima pada algoritma kriptografi RSA (Rivest, Shamir, dan Adleman) dan algoritma kriptografi Elgamal [skripsi]. Malang (ID): Universitas Islam Negeri Maulana Malik Ibrahuim Malang.

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

Irfan, P., & Prayudi, Y. (2015). Penggabungan Algoritma Chaos dan Rivers Shamir Adleman (RSA) Untuk Peningkatan Keamanan Citra. *SNATI (Seminar Nasional Aplikasi Teknologi Informasi)*, D5.

Kusuma, E. J., Sari, C. A., Rachmawanto, E. H., & Setiadi, D. R. I. M. (2018). A combination of inverted LSB, RSA, and arnold transformation to get secure and imperceptible image steganography. *Journal of ICT Research and Applications*, *12*(2), 103–122. https://doi.org/10.5614/itbj.ict.res.appl.2018.12.2.1

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. http://jurnal.polgan.ac.id/index.php/sinkron/article/view/75

Nisha, S., & Farik, M. (2017). RSA Public Key Cryptography Algorithm A Review. *International Journal of Scientific & Technology Research*, *06*(07),

187–191.

Pabokory, F. N., Astuti, I. F., & Kridalaksana, A. H. (2016). Implementasi Kriptografi Pengamanan Data Pada Pesan Teks, Isi File Dokumen, Dan File Dokumen Menggunakan Algoritma Advanced Encryption Standard. *Informatika Mulawarman : Jurnal Ilmiah Ilmu Komputer*, *10*(1), 20. https://doi.org/10.30872/jim.v10i1.23

Qorny, M. W. A. 2018. Enkripsi dan Dekripsi Menggunakan Algoritma RSA dan Affine Cipher Dengan Metode Matriks [skripsi]. Malang (ID): Universitas Islam Negeri Maulana Malik Ibrahuim Malang.

Rani, S., & Kaur, H. (2017). Technical Review on Symmetric and Asymmetric Cryptography Algorithms. *International Journal of Advanced Research in Computer Science*, *8*(4), 182–186.

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.

Zulfikar, M. I., Abdillah, G., Komarudin, A., Informatika, J., & Sains, F. (2019). Kriptografi untuk Keamanan Pengiriman Email Menggunakan Blowfish dan Rivest Shamir Adleman (RSA). *Seminar Nasional Aplikasi Teknologi Informasi (SNATi) 2019*, *2*(1), 19–26.