PEMBANGKITAN KUNCI UNTUK PENENTUAN KONSTANTA P DAN Q YANG PRIMA BERDASARKAN INFORMASI PERANTI

TUGAS AKHIR

Oleh :

Yogi Arif Widodo
NIM. 17615006

KEMENTERIAN PENDIDIKAN DAN KEBUDAYAAN
POLITEKNIK NEGERI SAMARINDA
JURUSAN TEKNOLOGI INFORMASI
PROGRAM STUDI TEKNIK INFORMATIKA

SAMARINDA 2020

HALAMAN JUDUL

Inisial sebagai index daftar isi

Print terpisah

HALAMAN PERNYATAAN ORISINALITAS

Inisial sebagai index daftar isi
Print terpisah

HALAMAN PENGESAHAN PEMBIMBING

Inisial sebagai index daftar isi

Print terpisah

HALAMAN PERSETUJUAN PENGUJI

Inisial sebagai index daftar isi
Print terpisah

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 Untuk Penentuan Konstanta P dan Q yang Prima Berdasarkan Informasi 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, 07 September 2020

Yogi Arif Widodo

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

ABSTRAK

Jika difaktorkan hanya habis dibagi oleh angka 1 dan dengan dirinya sendiri disebut Bilangan Prima. Keunikanya selalu berbentuk antara 6k-1 atau 6k +1. Salah satu konsep atau metode berhubungan dengan bilangan yang prima dimiliki oleh Rivest Shamir Adleman (RSA), untuk pembangkitan kuncinya dibagi menjadi 2 buah pola yaitu variabel *p* dan *q*. Konstanta atau orde *p* dan *q* menjadi eksperimen aritmatika dalam kombinasi informasi peranti waktu pada *android mobile* dengan bentuk jam (HH), menit (mm) dan detik (ss). Greenwich Mean Time Zone (GMT) merupakan zona waktu informasi menjadikanya berpola determisitik menjadi probabilistik jika diolah menggunakan *pseudorandom* kemudian menghasilkan *index* waktu yang mengubah Zona Awal (ZA) 15:17:02 GMT + 8 ke Zona Lain (ZL) menjadi 10:17:03 GMT - 11. Waktu yang digunakan ketika terjadinya proses aritmatika yaitu ZL. HH berperan dalam pembentukan *p* sedangkan *q* dipengaruhi oleh mm dan ss dengan ketentuan sebagai *index* yang sedemikian rupa. Pembangkitan awal ditentukan dengan batas atas prima n = 512. Dengan teknik sederhana *naive solution* dimana 2 ke n – 1 menghasilkan *arrayListPrimeNumber* = 2,3,5,7,9..n. Kombinasi dan Aritmatika berhasil menentukan p = 179 dan q = 419. Hasil Entropi Enkripsi dari 4 sample (teks 1 = 4.035569614562073, teks 2 = 4.257107430057822, teks 3 = 3.77391380004984 dan teks 4 = 4.421087076196203) masing-masing menghasilkan nilai yang ekuivalen terhadap p dan q yang ditentukan dengan yang secara *default.* Hasil enkripsi dibantu dengan RSA dengan kunci 2 *bit* – 17 *bit*. Cara meningkatkan hasil Prima yang besar pada penelitian ini, dapat dilakukan dengan menaikan nilai *inisial* dan *n* yang ditetapkan pada rumus $P_{penentuan}$ dan $q_{penentuan}$. Seluruh proses, diuji keberhasilan program dengan pengecualian atau *Exception Handling*, hasilnya tidak ada *problem* pada *feedback monitoring* aplikasi android.

Kata kunci : *Bilangan Prima, Informasi Peranti Waktu, P dan Q*

ABSTRACT

If it is factored, it is only divisible by the number 1 and by itself it is called a prime number. The uniqueness is always in the form between 6k-1 or 6k +1. One of the concepts or methods related to prime numbers is owned by Rivest Shamir Adleman (RSA). The key generation is divided into 2 patterns, namely variables p and q. Constants or orders p and q become arithmetic experiments in a combination of time device information on an android mobile in the form of hours (HH), minutes (mm) and seconds (ss). Greenwich Mean Time Zone (GMT) is an information time zone making it a deterministic pattern to be probabilistic if processed using pseudorandom then producing a time index which changes the Initial Zone (ZA) 15:17:02 GMT + 8 to Other Zones (ZL) to 10:17: 03 GMT - 11. The time used when the arithmetic process occurs is ZL. HH plays a role in the formation of p while q is influenced by mm and ss provided that it is an index in such a way. Initial generation is determined with an upper limit of prime n = 512. With a simple naive solution technique where 2 to n - 1 results in arrayListPrimeNumber = 2,3,5,7,9..n. Combination and Arithmetic succeeded in determining p = 179 and q = 419. The results of the Encryption Entropy of 4 samples (text 1 = 4.035569614562073, text 2 = 4.257107430057822, text 3 = 3.77391380004984 and text 4 = 4.421087076196203) each yields a value equivalent to p and q which is specified by default. The results of the encryption are assisted by RSA with a key of 2 bits - 17 bits. How to increase the large Prima results in this study, can be done by increasing the initial value and n set in the formula $P_{penentuan}$ and $q_{penentuan}$. *The whole process, tested the success of the program with exception or Exception Handling, the result is that there are no problems in the android application monitoring feedback.*

Keywords*: Prime Number, Information Time Device, P and Q*

BAB I

PENDAHULUAN

1.1 Latar Belakang

Bilangan prima adalah bilangan yang hanya memiliki dua faktor: 1 dan bilangan itu sendiri. Satu-satunya bilangan prima bernilai genap hanyalah 2 (Cahyo Dhea Arokhman Yusufi, 2020). Setiap bilangan asli lebih dari 1 yang tidak prima disebut bilangan komposit (Harahap, 2019). Jika n adalah suatu bilangan komposit, maka n memiliki setidaknya 1 faktor prima yang nilainya tidak lebih dari $\sqrt{n}$.

Bilangan prima yang lebih besar dari 3 memiliki keunikan yang selalu berbentuk antara (Chiewchanchairat dkk., 2016) 6k-1 atau 6k +1 (Ferreira, 2017), dimana k adalah bilangan prima yang diketahui. Maka dari itu bilangan prima yang lebih dari 3 akan selalu memiliki antara dua bentuk tadi. Hasil selanjutnya didapat mengenai bilangan prima adalah bahwa bilangan prima ada tak hingga banyaknya (Meštrović, 2018; Sciences, 2016). Bilangan Prima merupakan bilangan bulat positif, sifat pembagiannya (Firmansyah, 2015) melahirkan konsep-konsep aritmatika *modulo*, dan salah satu konsep bilangan bulat yang digunakan dalam penghitungan komputer.

Pada penelitian (Sari, 2017) bilangan prima merupakan bilangan istimewa dalam Al-Qur'an karena definisi bilangan prima yaitu bilangan yang tidak bisa dibagi dengan bilangan lain kecuali satu dan bilangan itu sendiri yang menampilkan

sifat Allah yang tidak dapat dibagi dengan siapapun kecuali diri-Nya. Dengan ditemukannya bilangan prima, teori bilangan berkembang semakin jauh dan lebih mendalam. Banyak dalil dan sifat dikembangkan berdasarkan bilangan prima (Firmansyah, 2015), salah satunya adalah Kriptografi *Rivest Shamir Adleman* (RSA) yang memiliki 2 buah pola bilangan prima dan ditetapkan sebagai variabel p dan q untuk pembangkitan kunci RSA (Sylfania dkk., 2019), Selain itu setiap angka genap yang cukup besar dapat ditulis sebagai jumlah dari beberapa bilangan prima dan nomor lain yang merupakan produk dari dua bilangan prima (Kumari dkk., 2015).

Pada penilitian (TH & MB, 2017) Pengecualian atau *Exception Handling* merupakan cara bersih memeriksa kesalahan tanpa mengacaukan kode dan mampu menangkap pengecualian sebuah. Aritmatika salah satunya *NumberFormat Exception*. Klausa tangkapan diikuti blok coba (*try and catch*), setiap blok tangkapan merupakan pengecualian yang menangani jenis pengecualian.

Berdasarkan sifat Bilangan Prima, maka penelitian ini mengkombinasikan informasi peranti waktu jam, menit dan detik pada android mobile menjadi teknik penentuan konstanta p dan q juga memastikan ketentuan prosesnya terpenuhi dan menghasilkan pola tersendiri tanpa ada pengecualian sebagai tanda berhasilnya proses pada Pengujian dan Pembuktian terhadap Tahapan Penentuan Konstanta P dan Q Berdasarkan Informasi Peranti

1.2 Rumusan Masalah

Dalam melaksanakan penelitian, masalah yang menjadi poin utama diskusi atau pembahasan, adalah "Bagaimana Melakukan Pembangkitan Kunci Untuk Penentuan Konstanta P dan Q Yang Prima Berdasarkan Informasi Peranti".

1.3 Tujuan Penelitian

Tujuan dari penelitian ini adalah:

1. Memanfaatkan Informasi Peranti Waktu (jam, menit dan detik)
2. Memodifikasi Teknik Pembangkitan Kunci Untuk Penentuan Konstanta P dan Q Yang Prima
3. Memonitoring konsep informasi peranti waktu dengan *Exception Handling*, sebagai indikator berjalannya konsep yang dibuat.

1.4 Batasan Masalah

Adapun batasan masalah dalam penilitian sebagai berikut:

1. Informasi peranti menggunakan waktu jam, menit dan detik dan Zona waktu adalah **GMT -11:00** sampai **GMT +13:00**.
2. Panjang kunci *p* dan *q* adalah 7 *bit* (2 digit) sampai 14 bit (4 digit).

1.5 Manfaat Penelitian

Harapan penelitian yang dilaksanakan, dapat memberikan manfaat:

1. Kunci konstanta *p* dan *q* memiliki pola tambahan berdasarkan informasi waktu jam, menit dan detik dari peranti *mobile android*.
2. Dapat menjadi sumber referensi bagi pihak lain dalam menyusun karya ilmiah maupun penelitian yang berkaitan dengan judul pada penelitian.

BAB II

LANDASAN TEORI

2.1 Kajian Ilmiah

Hasil penelitian yang telah dilakukan para peneliti dapat dijadikan dasar atau kajian untuk mempermudah dalam melakukan penelitian. 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)

Dan mengambil konstanta p dan q sebagai acuan dari penelitian ini 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

Hubungan matematika dengan kriptografi sangat erat sekali, karena matematika adalah konsep dasar yang berhubungan dengan kriptografi terutama matematika diskrit (Firmansyah, 2015). Dalam bab 2 ini, akan menjelaskan konsep matematis yang melandasi pembentukan konstanta p dan q dengan algoritma bilangan prima, seperti teori bilangan bulat, keterbagian, sifat-sifat pembagian, algoritma euklid, aritmatika modulo, logaritma diskrit dan bilangan prima.

2.2.1 Teori Bilangan

Teori bilangan salah satunya bilangan prima dengan berbagai metode, banyak yang dapat dipelajari, namun masih sebatas bilangan prima dengan jumlah digit yang sederhana (kecil) misalnya 2, 3, 5, 7, 11, 17, 23, 29 dan seterusnya Sehingga metode untuk mendapatkan bilangan prima yang besar perlu dikupas lagi. (Harahap, 2019) mengeluarkan bilangan prima yang terbesar saat ini ditemukan oleh manusia adalah $2^{74207281}$-1 dengan jumlah 22.338.618 digit

Dalam pengertian yang ketat, kajian tentang sifat-sifat bilangan asli disebut dengan teori bilangan. Dalam pengertian yang lebih luas, teori bilangan mempelajari bilangan dan sifat-sifatnya. Sebagai salah satu cabang matematika, teori bilangan dapat disebut sebagai "aritmetika lanjut (*advanced aritmetics*)" karena terutama berkaitan dengan sifat-sifat bilangan asli. Teori bilangan merupakan dasar perhitungan dan menjadi salah satu teori yang mendasari pemahaman kriptografi, bilangan yang dimaksud hanyalah bilangan bulat (integer).

Berikut penjelasan mengenai bilangan bulat, keterbagian, algoritma pembagian, fungsi eular, bilangan prima, relatif prima, modulus dan *Greatest Common Divisor* (GCD).

1 Bilangan Bulat

Bilangan bulat positif yang lebih besar dari 1 dan hanya habis dibagi dirinya sendiri dan bilangan 1 disebut Bilangan Prima (Harahap, 2019). Bilangan bulat adalah bilangan yang tidak mempunyai pecahan desimal. Himpunan semua bilangan bulat yang dinotasikan dengan Z yang diambil dari kata Zahlen dari bahasa Jerman atau dinotasikan dengan I yang diambil dari huruf pertama kata Integer dari bahasa Inggris, adalah himpunan *... , −3, −2, − 1,0,1,2,3 ... +. Himpunan bilangan bulat dibagi tiga, yaitu bilangan bulat positif, yaitu bilangan bulat yang lebih besar dari nol yang dituliskan Z + , nol, dan bilangan bulat negatif, yaitu bilangan bulat yang lebih kecil dari nol yang dituliskan Z −. Himpunan bilangan bulat dilengkapi dengan dua buah operasi, yaitu operasi penjumlahan dan perkalian, dilambangkan (Z, +,·) membentuk suatu sistem matematika yang disebut gelanggang atau ring. Himpunan bilangan bulat berperan sangat penting dalam kriptografi karena banyak

algoritma kriptografi yang menggunakan sifat-sifat himpunan bilangan bulat dalam melakukan proses penyandiannya.

2 Keterbagian

Sifat-sifat yang berkaitan dengan keterbagian (*divisibility*) merupakan dasar pengembangan teori bilangan. Jika suatu bilangan bulat dibagi oleh suatu bilangan bulat yang lain, maka hasil pembagiannya adalah bilangan bulat atau bukan bilangan bulat.

3 Algoritma Pembagian

Jika a, b $\in$ Z dan a > 0, maka ada bilangan q, r $\in$ Z yang masing-masing tunggal sehingga b = qa + r dengan 0 r < a. Jika a$\nmid$b, maka r memenuhi ketidaksamaan 0 < r < a. Algoritma pembagian adalah suatu cara atau prosedur yang dapat dipakai untuk mendapatkan faktor persekutuan terbesar (FPB) (Fernanda, 2020).

4 Fungsi Euler (φ)

Fungsi Euler digunakan untuk menyatakan banyaknya bilangan bulat < n yang relatif prima terhadap n. Jika p adalah suatu bilangan prima, maka φ(p) = p - 1, Karena p adalah bilangan prima, maka setiap bilangan bulat positif kurang dari p relatife prima terhadap p. Ini berarti bahwa sistem residu tereduksi modulo p adalah himpunan {1, 2, 3,...,p - 1} yang mana seluruh anggotanya sebanyak (p - 1) sehingga φ(p) = p – 1.

5 Bilangan Prima

Bilangan bulat positif yang mempunyai aplikasi penting dalam ilmu komputer dan matematika diskrit adalah bilangan prima. Bilangan prima adalah bilangan bulat positif yang lebih dari 1 yang hanya habis dibagi oleh 1 dan dirinya 23 sendiri. Sifat pembagian pada bilangan bulat melahirkan konsep-konsep bilangan prima dan aritmetika modulo, dan salah satu konsep bilangan bulat yang digunakan dalam penghitungan komputer adalah bilangan prima. Dengan ditemukannya bilangan prima, teori bilangan berkembang semakin jauh dan lebih mendalam. Banyak dalil dan sifat dikembangkan berdasarkan bilangan prima. Bilangan prima juga memainkan peranan yang penting pada beberapa algoritma.
Jika p suatu bilangan bulat positif lebih dari 1 yang hanya mempunyai pembagi positif 1 dan p, maka p disebut bilangan prima. Jika suatu bilangan bulat q 1 bukan suatu bilangan prima, maka q disebut bilangan komposit. Untuk menguji apakah p merupakan bilangan prima atau bilangan komposit, dapat menggunakan cara yang paling sederhana, yaitu cukup membagi p dengan sejumlah bilangan prima, yaitu 2, 3, ... , bilangan prima √p. Jika p habis dibagi salah satu dari bilangan prima tersebut, maka p adalah bilangan komposit tetapi jika p tidak habis di bagi oleh semua bilangan prima tersebut, maka p adalah bilangan prima.

Solusi sederhana menentukan bilangan prima dalam deret bilangan dapat dilakukan dengan *naive solution* dimana $2\ ke\ n-1$ menghasilkan $arrayListPrimeNumber = 2,3,5..n$ dan n atau batas prima merupakan bilangan yang ditentukan. Solusi lain memiliki kebutuhan yang beragam atau

kompleks, sedangkan penelitian ini membutuhkan konsep yang sederhana dan fleksibel untuk diterapkan dalam berbagai konsep.

Beberapa fakta menarik tentang bilangan prima (*Prime Numbers - GeeksforGeeks*, n.d.)

1. Dua adalah satu-satunya bilangan prima genap.
2. Setiap bilangan prima dapat direpresentasikan dalam bentuk 6n + 1 atau 6n-1 kecuali 2 dan 3, di mana n adalah bilangan asli.
3. Dua dan Tiga hanyalah dua bilangan asli berurutan yang juga merupakan bilangan prima.
4. Dugaan Goldbach: Setiap bilangan bulat genap yang lebih besar dari 2 dapat diekspresikan sebagai jumlah dari dua bilangan prima.
5. Teorema Wilson: Teorema Wilson menyatakan bahwa bilangan asli p > 1 adalah bilangan prima jika dan hanya jika

$(p - 1)! \equiv -1 \bmod p$

ATAU $(p - 1)! \equiv (p - 1) \bmod p$

6. Teorema Kecil Fermat: Jika n adalah bilangan prima, maka untuk setiap a, 1 <= a <n,

$$an - 1 \equiv 1 \pmod n$$

ATAU

$$an - 1 \,\%\, n = 1$$

7. Teorema Bilangan Perdana: Probabilitas suatu bilangan yang dipilih secara acak n adalah bilangan prima berbanding terbalik dengan jumlah digitnya, atau dengan logaritma dari n.

8. Dugaan Lemoine: Setiap bilangan bulat ganjil yang lebih besar dari 5 dapat diekspresikan sebagai jumlah bilangan prima ganjil (semua bilangan prima selain 2 adalah ganjil) dan semiprime genap. Bilangan semiprima adalah hasil perkalian dua bilangan prima. Ini disebut dugaan Lemoine.

6 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). Dua buah bilangan bulat dan dikatakan relative prima. Jika FPB/GCD (x,) = 1.

Contohnya 20 dan 3 relatif prima sebab FPB (20, 3) = 1. Begitu juga 7 dan 11 relatif prima karena FPB (7, 11) = 1. Tetapi 20 dan 5 tidak relatif prima sebab FPB (20, 5) = 5 dan 1. Jika x dan relatif prima, maka terdapat bilangan bulat sehingga: x + n dan n sedemikian = 1.

Contohnya Bilangan 20 dan 3 adalah relatif prima karena FPB (20, 3) = 1, atau dapat ditulis: $2 \cdot 20 + (-13) \cdot 3 = 1$, dengan = 2 dan n = – 13. Tetapi 20 dan 5 tidak relatif prima karena FPB (20, 5) = $5 \neq 1$ sehingga 20 dan 5 tidak dapat dinyatakan dalam $20 + n \cdot 5 = 1$.

7 Modulus

Dalam matematika dan pemrograman komputer, operasi modulus adalah sebuah operasi yang menghasilkan sisa pembagian dari suatu bilangan terhadap bilangan lainnya. Dalam bahasa pemrograman operasi ini umumnya dilambangkan dengan simbol %, mod atau modulo, tergantung bahasa pemrograman yang digunakan.

Pada penelitian ini modulus digunakan karena operasi ini memiliki atau berhubungan dengan bilangan yang prima berdasarkan pada penilitian (Serdano dkk., 2019)

8 GCD

Greatest Common Divisor (GCD) atau sehari – hari kita sebut dengan Faktor Persekutuan Terbesar yaitu bilangan bulat N yang paling besar yang habis membagi dua buah bilangan bulat (Harahap, 2019). Misalnya dua buah bilangan bulat 12 dan 8.

12 habis dibagi oleh: 1, 2, 3, 4, 6, 12.

8 habis dibagi oleh: 1, 2, 4, 8.

Berdasarkan pembagian di atas maka dapat disimpulkan bahwa GCD dari 12 dan 8 adalah 4.

Contoh lainya:

1. GCD (24, 12) =12 (Artinya 12 merupakan bilangan terbesar yang membagi 24 dan 12)
2. GCD (24, 9)= 3 (Artinya 3 merupakan bilangan terbesar yang membagi 24 dan 9)

Cara yang digunakan pada penelitian ini dalam menemukan GCD atau dalam metode ini, bilangan bulat yang lebih kecil dikurangi dari bilangan bulat yang lebih besar, dan hasilnya diberikan ke variabel yang memiliki bilangan bulat yang lebih besar. Mencari GCD memiliki berbagai macam teknik dan berdasarkan konsep yang dipilih tidak menjadi masalah untuk menerapkan konsep salah satunya.

2.3 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.

Salah satu implementasi kriptografi asimetris adalah Rivest Shamir Adleman (RSA). Langkah-langkah (yang diteliti yaitu pada no 1 – 3 tepatnya konstanta p dan q) untuk membangkitkan kunci RSA adalah (Nisha & Farik, 2017):

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.

$$n = p * q \quad \text{(2.1)}$$

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).

Berdasarkan penilitian ini memberikan gagasan atau ide dalam eksperimen yang ditujukan pada pembangkitan kunci p dan q berdasarkan infomasi peranti yaitu waktu.

2.4 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).

Baterai adalah alat elektro kimia yang berfungsi untuk menyimpan tenaga listrik dalam bentuk tenaga kimia. Tenaga listrik yang tersimpan akan dialirkan untuk memberikan arus listrik. Daya baterai biasanya bernilai 1 – 100% yang terlihat pada ponsel contohnya.

Suhu adalah suatu besaran yang menunjukan derajat panas khususnya pada benda. Benda yang mempunyai panas maupun dingin, pada umumnya ponsel dilengkapi indikator derajat.

Sinyal adalah suatu besaran fisis yang berubah terhadap waktu, ruang, ataupun dapat berubah terhadap variabel bebas lainnya. Ponsel harus memiliki sebuah sinyal ketika melakukan komunikasi.

Waktu atau masa menurut Kamus Besar Bahasa Indonesia adalah seluruh rangkaian saat ketika proses, perbuatan, atau keadaan berada atau berlangsung. Dalam hal ini, skala waktu merupakan interval antara dua buah keadaan/kejadian, atau bisa merupakan lama berlangsungnya suatu kejadian

Pada penilitian ini menggunakan waktu, sebagai eksperimen dan memanfaatkan data jam menit dan detik yang menjadi 3 variabel fokus untuk penentuan *p* dan *q*.

2.5 *Kotlin* dan Aliran Kontrol

Kotlin adalah sebuah bahasa pemrograman dengan pengetikan statis yang berjalan pada Mesin Virtual Java ataupun menggunakan kompiler LLVM yang dapat pula dikompilasikan kedalam bentuk kode sumber JavaScript. Pengembang utamanya berasal dari tim developer dari JetBrains yang bermarkas di Rusia (*FAQ - Kotlin Programming Language*, n.d.).

Pada penelitian ini operasi dan pengujian menggunakan bahasa *kotlin* yang dikompilasi atau dijalankan oleh *mobile android*. Beberapa aliran kontrolnya terdapat *if*, *when*, *for* dan *while*. Semua aliran digunakan menangani aritmatika dan konsep yang dibuat sesuai kebutuhan.

2.6 *Exception Handling*

Memeriksa semua kemungkinan kesalahan atau yang disebut *Exception Handling* untuk setiap metode karena ini dapat membuat kode tidak dapat dipahami jika setiap pemanggilan metode memeriksa semua kemungkinan kesalahan sebelum menjalankan pernyataan berikutnya. Kelas *Throw* mampu menangani seluruh konsep pengecualian dan kesalahan. Tujuan utama dari mekanisme penanganan *Exception* adalah mendeteksi dan melaporkan "keadaan pengecualian" sehingga tindakan yang sesuai dapat diambil (Kumari dkk., 2015). Mekanisme tersebut menyarankan penggabungan kode penanganan kesalahan terpisah yang melakukan tugas berikut:

1. Menemukan masalah yaitu *Exception*
2. Menginformasikan bahwa telah terjadi kesalahan yaitu Pengecualian
3. Menerima informasi kesalahan yaitu Menangkap pengecualian
4. Ambil tindakan korektif, yaitu Menangani pengecualian Melempar

2.7 Shannon Entropy

Entropi merupakan konsep dasar yang dikemumakan pada teori informasi Shannon, ide ini diadopsi dari salah satu cabang ilmu fisika yaitu termodinamika. Dalam hal ini Entropi (H) digunakan untuk mengukur keacakan data (Rihartanto dkk., 2020) dimana terdapat suatu keadaan yang tidak dapat dipastikan kemungkinannya. Entropi timbul jika prediktabilitas/kemungkinan rendah (*low predictable*) dan informasi yang ada (*high information*). Entropi dihitung menggunakan formula entropi Shannon yang ditunjukkan pada Persamaan 2.6.1. Nilai entropi tertinggi yang dapat dicapai pada sebuah citra adalah 8, sementara

pada teks yang hanya menggunakan ASCII standar entropi tertinggi yang mungkin diperoleh adalah 7. Semakin tinggi nilai entropi menunjukkan tingkat keacakan yang semakin tinggi.

$$H(x) = -\sum_{i=1}^{n} P(x_i) log2\ P(x_i)$$

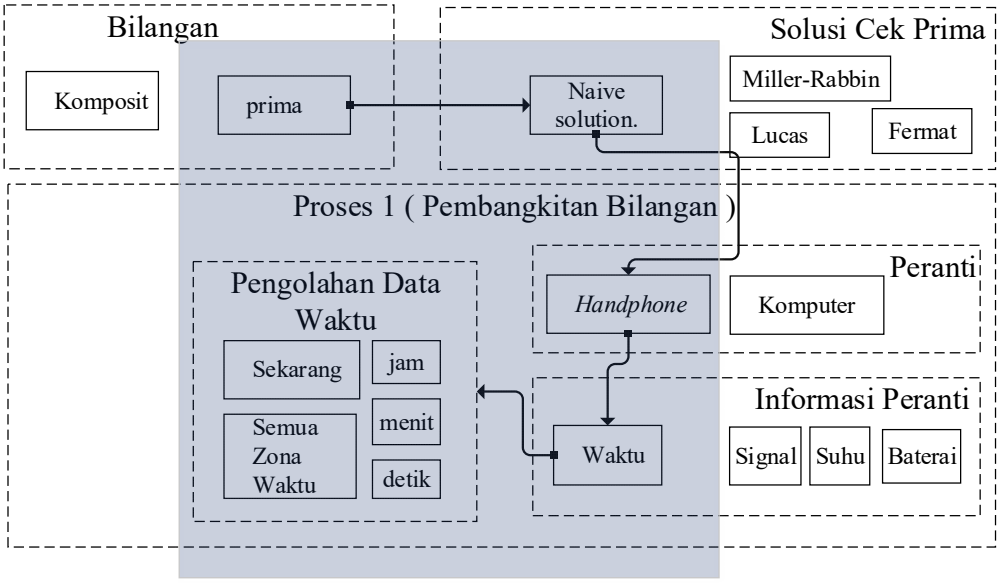
Dalam penelitian ini, entropi dihitung berdasarkan besarnya peluang jarak antar karakter dalam teks. Hasil entropi kemudian dibandingkan antara *p* dan *q* yang ditentukan secara *default* dengan *p* dan *q* yang ditentukan berdasarkan informasi peranti waktu.

BAB III

KERANGKA KONSEP DAN METODE PENELITIAN

3.1 Kerangka Konsep Penelitian

Kerangka konsep penelitian (teori atau konsep ilmiah yang digunakan sebagai dasar penelitian) menjelaskan hubungan atau gabungan alur sebagai ruang lingkup penelitian dan ruang lingkup ilmu



Gambar 3.1 Diagram Alur Kerangka Konsep Penelitian

Berdasarkan Gambar 3.1 diagram alur kerangka konsep penelitian dapat dijelaskan secara singkat.

1. Prima

Pada penelitian ini objek atau bahan yang diolah adalah Bilangan Prima. Dalam bilangan terdapat berbagai jenis bilangan, dua diantaranya yaitu:

a. Bilangan Komposit

b. Bilangan Prima

Bilangan prima berhubungan dekat dengan penilitian ini sebagai konsep pemilihan konstanta *p* dan *q*, dimana bilangan yang prima tidak hanya unik melainkan memiliki bentuk 6k-1 atau 6k +1.

2. Naive Solution

Solusi sederhana untuk mengecek bilangan kecil yang prima tepatnya dapat ditangani dengan *Naive Solution*. Macam-macam solusi lain yang mengenai bilangan prima lebih luas, diantaranya adalah:

a. Fermet

b. Miller-Rabbin

c. Solovay-Strassen

d. Lucas

3. Handphone

Pengujian ini didasarkan pada peranti yang pemrosesan aritmatikadilakukan dengan *handphone* yang dapat menghasilkan sebuah *metadata* atau informasi yang beragam sesuai kebutuhan yaitu waktu jam menit dan detik.

4. Informasi Peranti Waktu

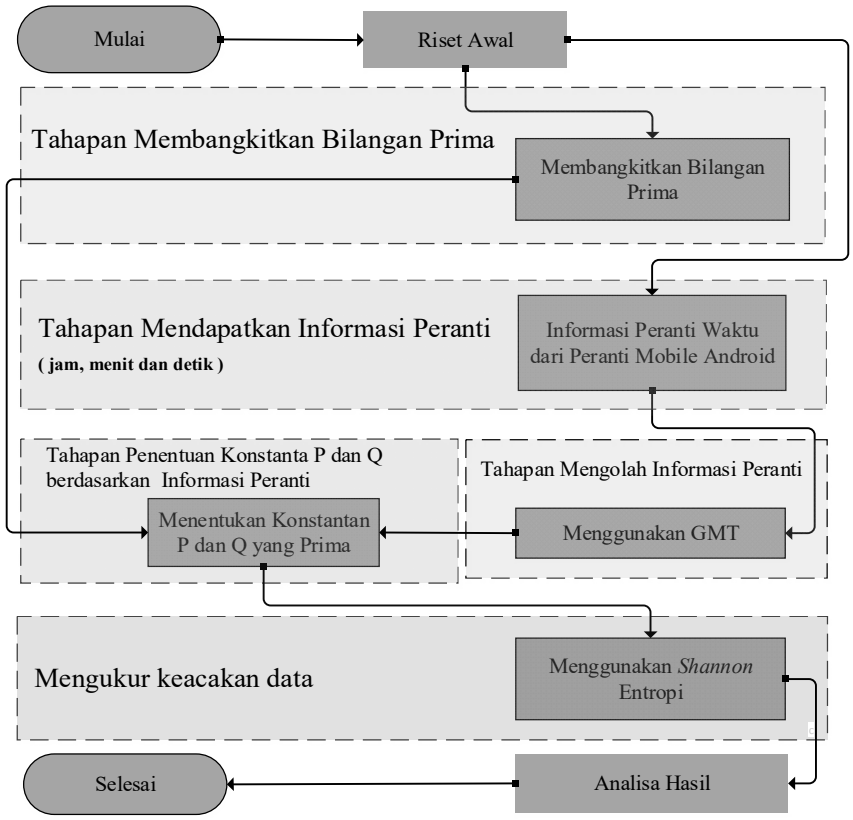
Waktu merupakan perhitungan masa dunia, dengan waktu dapat mengetahui kapan suatu hal terjadi. Khususnya proses aritmatika yang terjadi pada suatu perangkat atau peranti. Informasi ini dapat dengan mudah diperoleh dengan alat elektronik contohnya *handphone* atau komputer

5. Pengolahan Data Waktu

Waktu memiliki berbagai macam jenis yang dapat diolah sebagai konsep pemanfaatan nilainya, seperti jam menit dan detik ataupun zona waktu. Dengan begitu data waktu dapat dirancang sedemikian rupa untuk menghasilkan bilangan yang prima berdasarkan kejadian atau waktu yang diperoleh serta menjadikanya sebuah posisi dalam memilih bilangan yang prima.

3.2 Metodologi Penelitian

Metode Penelitian menjelaskan mengenai tahapan-tahapan pengerjaan dari penelitian yang dilakukan. Metode penelitian ini bertujuan agar penyelesaian penelitian ini tidak terlepas dari penggunaan metode yang dikerjakan.



Gambar 3.2 Diagram Alur Metodologi Penelitian

Pada Gambar 3.2, tahapan dari metodologi penelitian yang dilakukan dimulai pada riset awal, kemudian membangkitkan bilangan prima dan pada bagian alur kedua mendapatkan informasi peranti waktu , mengolah informasi waktu menggunakan GMT, setelah itu penentuan konstanta p dan q berdasarkan informasi perenti , mengukur keacakan data menggunakan *Shannon* entropi, terakhir adalah analisa hasil.

3.2.1 Riset Awal

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

1. Mengetahui fungsi konstanta *p* dan *q* yang prima
2. Mengetahui penggunaan informasi peranti waktu
3. Landasan matematika (teori bilangan dan pemfaktoran bilangan bulat)

3.2.2 Tahapan Membangkitkan Bilangan Prima

Membangkitkan Bilangan Prima dengan mengeliminasi angka bukan prima (TH & MB, 2017). Penerapanya sederhana akan dilakukan dengan *naive solution* dengan hasil yang tersimpan dalam *ArrayList* sehingga dapat diolah lebih lanjut berdasarkan informasi peranti.

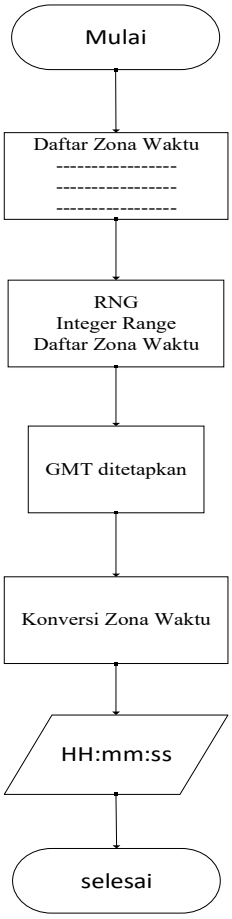
3.2.3 Tahapan Mendapatkan Informasi Peranti

Informasi Peranti yang didapatkan berupa 3 variabe yaitu jam, menit, dan detik. Proses mendapatkannya dibaca oleh peranti *Mobile Android*. Data waktu yang didapat bukan berupa nilai seperti 1594886148236 melainkan jam menit dan detik serta zona waktu sebagai contoh informasi yang dimaksud seperti 15:07:00 GMT +8.

3.2.4 Tahapan Mengolah Informasi Peranti

Informasi Peranti diolah kembali untuk menghasilkan informasi peranti yang probabilstik berdasarkan angka pseudorandom dari jumlah 24 zona waktu dalam artian 1 sampai 24, kemudian angkanya akan menentukan zona yang

terdaftar atau konversi terhadap data zona waktu yang telah didapatkan seperti yang diperlihatkan pada Gambar 3.2.4.



Gambar 3.2.4 Tahapan Mengolah Informasi Peranti Waktu

Perubahan zona sendiri merupakan proses, tujuanya mengkonsumsi sebuah waktu ketika mendapatkan informasi waktu itu sendiri sehingga menyerupai data yang probabilistik, pada intinya informasi yang akan dipakai bukan waktu dengan zona awal melainkan zona lain yang ditetapkan dari daftar zona secara pseudorandom.

3.2.3 Tahapan Penentuan Konstanta P dan Q Berdasarkan Informasi Peranti

Penentuan konstanta *p* dan *q* akan dilakukan berdasarkan informasi peranti dengan melihat syarat sebagai berikut:

1. Bilangan yang prima telah didapatkan dalam bentuk arrayListPrimeNumber hasilnya berdasarkan pada Tahapan Menentukan Bilangan Prima.
2. Informasi Peranti telah didapatkan dalam bentuk bagian dari waktu jam, menit dan detik.

Kemudian tahapan penentuan *p* dan *q* dapat diproses lebih lanjut dengan menggabungkan syaratnya, syarat dua akan menjadi posisi yang menjadikan syarat pertama menjadi outputnya sedemikian rupa, dimana *p* dipengaruhi oleh nilai jam sedangkan *q* dipengaruhi oleh menit dan detik.

3.2.4 Mengukur Keacakan Data

Mengukur keacakan data dilakukan dengan menggunakan Shannon entropi dihitung berdasarkan besarnya peluang jarak antar karakter dalam teks.

3.2.5 Analisa Hasil

Menganalisa hasil dan proses terpilihnya kunci p dan q yang dikaitkan dengan Hasil entropi enkripsi kemudian dibandingkan antara *p* dan *q* yang ditentukan secara *default* dengan *p* dan *q* yang ditentukan berdasarkan informasi peranti waktu.

3.2.6 Variabel Penelitian

Fokus penelitian tugas akhir ini dituangkan dalam variabel yaitu modifikasi konstanta atau orde *p* dan *q* yang prima berdasarkan waktu informasi peranti yaitu jam, menit dan detik.

3.2.7 Waktu dan Tempat Penelitian

Penelitian ini dilakukan di Jurusan Teknologi Informasi Politeknik Negeri Samarinda dengan waktu pengerjaan berdasarkan jadwal pengerjaan tugas akhir.

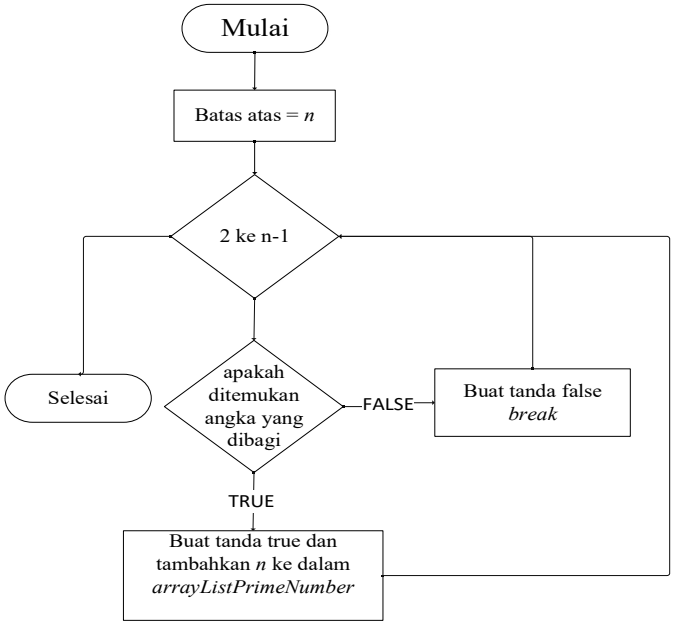
BAB IV

HASIL DAN PEMBAHASAN

4.1 Hasil Tahapan Membangkitkan Bilangan Prima

Membangkitkan Bilangan Prima dengan mengeliminasi angka bukan prima (TH & MB, 2017). Penerapanya sederhana dilakukan dengan *naive solution* sebagai berikut:

1. Ketika Melalui semua angka dari 2 ke *n*-1, maka setiap nomor periksa apakah ia membagi *n*.
2. Jika ditemukan angka yang dibagi, akan mengembalikan tanda *false*
3. Sebaliknya *true* dan simpan nilai *n* ke dalam *arrayListPrimeNumber*.



Gambar 4.1 FlowChart Proses Naive Solution

Tabel 4.1 Hasil Pembangkitan Bilangan Prima

arrayListPrimeNumber	prima	2	3	5	..	509
	size	1	2	3	..	97

Jadi pada penilitian ini *Naive Solution* membangkitkan bilangan yang prima sebanyak 97 dan bilanganya dimulai dari 2,3,5,7 sampai 509 seperti yang diperlihatkan pada Tabel 4.1

Nilai n telah ditentukan sebelumnya, *n* merupakan batas atas prima yang di atur dan bernilai 512. Jika *n* memiliki nilai yang lebih besar dari 512, maka memiliki tujuan menaikan nilai *inisial* pada rumus penentuan *p* dan *q* sehingga membangkitkan hasil prima yang cukup besar.

4.2 Hasil Tahapan Mendapatkan Informasi Peranti

Pada tahapan ini dilakukan ketika proses sebelumnya telah usai dikerjakan sehingga informasi yang didapat menyerupai aturan probabilistik. Informasi Peranti yang didapatkan memiliki 3 variabel yaitu jam, menit, dan detik dan Tambahan Zona Waktu. Proses mendapatkannya dibaca oleh peranti *Mobile Android* dengan fungsi yang sudah tersedia di *kotlin* menggunakan *Package Kotlin System*.

Data waktu yang didapat masih berupa nilai keseluruhan waktu 1594886148236, kemudian diformat menjadi (HH:mm:ss) untuk menjadikanya jam, menit dan detik. Dengan fungsi yang sudah tersedia di *kotlin* menggunakan *Open Class SimpleDateFormat.*

Maka hasil yang informasi peranti waktu yang didapatkan 15:17:02 dengan zona awal GMT +8.

4.3 Hasil Tahapan Mengolah Informasi Peranti

Informasi Peranti diolah kembali untuk menghasilkan informasi peranti yang probabilstik berdasarkan waktu jam, menit dan detik serta menggunakan *Greenwich Mean Time Zone* (GMT) sebagai pengubah Zona Awal ke Zona Lain. Seluruh zona waktu telah didefinisikan sebelumnya ke dalam *arrayTime* sebagai zona lain yang diperlihatkan pada Tabel 4.3

Tabel 4.3 Daftar Waktu Indonesia Tengah

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	

Pemilihan posisi atau *index* untuk *arrayTime* berdasarkan keluaran dari nilai *integer* oleh *sudorandom*, sebagai zona lain. Dengan fungsi yang sudah tersedia di kotlin menggunakan *Package Kotlin Random*.

Pada penelitian ini hasil nilai *sudoRandom* = 22, maka didapat *arrayTime* [*sudoRandom*] = GMT +12. Kemudian dilakukan konversi waktu sekarang 15:17:02 GMT +8 ke GMT -11 Dengan fungsi yang sudah tersedia di *kotlin* menggunakan *Open Class SimpleDateFormat* dan hasilnya akhir diperlihatkan pada Gambar 4.3

Gambar 4.3 Hasil Informasi Peranti Waktu

Informasi yang digunakan adalah zona lain, perubahan zona sendiri merupakan proses, tujuanya mengkonsumsi sebuah waktu ketika mendapatkan informasi waktu itu sendiri.

4.4 Hasil Tahapan Penentuan Konstanta P dan Q Berdasarkan Informasi Peranti

Berdasrakan penentuan yang telah dilakukan dengan melihat syarat sebagai berikut:

1 Bilangan yang prima telah didapatkan dalam bentuk *arrayListPrimeNumber* hasilnya diperlihatkan pada Gambar 3.

2. Informasi Peranti telah didapatkan dalam bentuk bagian dari waktu jam, menit dan detik. Hasilnya diperlihatkan pada Gambar 4.2.

Kemudian tahapan penentuan p dan q dapat diproses lebih lanjut dengan menggabungkan syaratnya, syarat dua telah menjadi posisi yang menjadikan syarat pertama menjadi outputnya sedemikian rupa, dimana p dipengaruhi oleh nilai jam sedangkan q dipengaruhi oleh menit dan detik sebagaimana tahapan berikut:

A. Menentukan Konstanta P yang Prima, penentuan ini sederhana, dengan menghitung persamaan 1.1 didapat *i = 40*.

($P_{penentuan}$……..…..……(1.1)

$$Pi = hh * inisial$$

Dimana :

Pi = *List Array* Ke-i

I = *Index arrayListPrimeNumber*

inisial = 4

hh = Informasi Peranti Waktu Jam

Maka didapatkan nilai *Pi* = 179. Jika *n* memiliki nilai yang lebih besar dari 4 misal 5 maka memiliki tujuan terbentuknya *p* yang prima cukup besar. Dengan *p* yang besar, memiliki kesempatan *Greatest Common Divisor* GCD(*p-1*, *q-1*) atau proses pemfaktoran yang memakan waktu lebih lama.

B. Menentukan Konstanta Q yang Prima, nilai *q* memiliki aturan mirip dengan nilai *p*, tetapi memiliki 2 keputusan perhitungan ($q_{keputusan}$) dari 2 ketentuanya ($q_{ketentuan}$).

($q_{ketentuan}$)……..…(2.1)

K1 = informasi peranti waktu menit

K2 = informasi peranti waktu detik

$(q_{keputusan})$……..…….……(2.2)

$$Qi = \begin{cases} inisial * (K1 * K2)\ mod\ q.size, & K1 < K2 \\ inisial * (K1 + K2)\ mod\ q.size, & K1 > K2 \end{cases}$$

Dimana:

Qi = *List Array* Ke-i

i = *Index arrayListPrimeNumber*

inisial = *4*

q.size = *arrayListPrimeNumber.size*

Dengan persamaan 2.1 dan 2.2 didapat K1 > K2 seperti yang diperlihatkan pada Tabel 4.4

Tabel 4.4 Hasil $(q_{keputusan})$ dan $(q_{ketentuan})$

informasi peranti waktu (HH:mm:ss)			10:17:03
arrayListPrimeNumber .size			97
inisial			4
index		Kondisi	
Qi	10	K1 < K2	*FALSE*
Qi	80	K2 > K1	*TRUE*
Hasil			
$q_{keputusan}$		*qQi*	419

Tahapan ini berhasil menentukan dan menghasilkan *Pi*=179 dan *Qi* = 419, sesuai ketentuan yang ditetapkan pada proses A dan B, selanjutnya nilai dan konsep yang dihasilkan memasuki Tahapan Mengukur Keacakan Data.

4.5 Hasil Mengukur Keacakan Data

Pengukuran keacakan data dilakukan pada hasil enkripsi dengan Shannon entropi dengan bantuan RSA (*Rivest Shamir Adleman*) dimana 2 bilangan prima *p* dan *q* telah ditentukan berdasarkan informasi peranti waktu yang diperlihatkan pada Tabel 4.5.1 dimana kunci yang digunakan merupakan data ke 12, 11, 10, dan 9 untuk teks uji 1, 2, 3, dan 4 yang diperlihatkan pada Tabel 4.5.2 sedangkan Tabel 4.5.3 dan Tabel 4.5.4 merupakan *p* dan *q* yang ditentukan secara umum atau default.

Pada Table 4.5.1 ataupun Tabel 4.5.3, Teks 1 berisi teks umum, teks 2 merupakan bahasa ingris, teks 3 adalah kalimat yang berulang, dan teks 3 memiliki huruf simbol seperti !@#$.

Hasil daripada entropi kemudian dibawa ke tahapan analisa hasil dengan membandingkan keacakan data yang didapat.

Tabel 4.5.1 Teks uji dan hasil enkripsi RSA dengan *p* dan *q* berdasarkan informasi peranti waktu

No	Teks Asli	Jumlah Karakter	Hasil Enkripsi	Entropi Enkripsi
1	“Ketahuilah, bahwa sesungguhnya kehidupan dunia ini hanyalah permainan dan suatu yang melalaikan, perhiasan dan bermegah-megah antara kamu serta berbangga-banggaan tentang banyaknya harta dan anak, seperti hujan yang tanam-tanamannya mengagumkan para petani; kemudian tanaman itu menjadi kering dan kamu lihat warnanya kuning kemudian menjadi hancur. Dan di akhirat (nanti) ada azab yang keras dan ampunan dari Allah serta keridhaan-Nya. Dan kehidupan dunia ini tidak lain hanyalah kesenangan yang menipu.”	512	剿?봠○ゐ罠慬東甒ᵛ罠慬　拦┤罠慬帰罠拦婧○婧東獘踫踫 東慬獘癇罠拦つ○慬甒群東磁罠獘拦群東獘甒罠拦甒獘甒拦慬罠獘癇罠ᵛ罠慬拦磁○▣砚罠甒獘罠獘罠拦群罠獘拦婧東罠ゐ東拦癇罠獘踫拦砚○ᵛ罠ᵛ罠甒つ罠獘　拦磁○▣慬甒罠婧罠獘拦群罠獘拦┤○▣砚○踫罠慬锁砚○踫罠慬拦罠獘ゐ罠▣罠拦つ罠ᑫ東拦婧○▣ゐ罠拦┤○▣┤罠獘踫踫罠锁┤罠獘踫踫罠罠獘拦ゐ○獘ゐ罠獘踫拦┤罠獘癇罠つ獘癇罠拦慬罠▣ゐ罠拦群罠獘拦罠獘罠つ　拦婧○磁○▣ゐ甒拦慬東ぶ罠獘拦癇罠獘踫拦ゐ罠獘罠砚锁ゐ罠獘罠砚罠獘獘癇罠拦砚ᑫ○獘踫罠踫東砚つ罠獘拦磁罠▣罠拦磁○ゐ罠獘甒鵬拦つ○砚東群甒罠獘拦ゐ罠獘罠砚罠獘拦甒ゐ東拦砚○獘ぶ罠群甒拦つ▣甒獘踫拦群罠獘拦つ罠砚東拦ᵛ甒慬罠ゐ拦帰罠▣獘罠獘癇罠拦つ東獘甒獘踫拦つ○砚東群甒罠獘拦砚○獘ぶ罠群甒拦慬罠獘　東▣釜拦ᑫ罠獘拦群甒拦罠つ慬甒▣罠ゐ拦　獘罠獘ゐ甒爆拦罠群罠拦罠涵罠├拦癇罠獘踫拦つ○▣罠婧拦群罠獘拦罠砚磁東獘罠獘拦群罠▣甒拦罰ᵂ罠慬拦婧○▣ゐ罠拦つ○▣甒群慬罠獘锁㬹癇罠釜拦ᑫ罠獘拦つ○慬甒群東磁罠獘拦群東獘甒罠拦甒獘甒拦ゐ甒群罠つ拦ᵛ罠甒獘拦慬罠獘癇罠ᵛ罠慬拦つ○婧○獘罠獘踫罠獘拦癇罠獘踫拦砚○獘甒磁東釜婠剿拦拦拦拦	4.035569614562073

2	"Know, that truly the life of this world is only a game and a neglect, adornment and boasting among you and boasting about the abundance of wealth and children, like rain whose crops amaze the peasants; Then the plant dries up and you see it is yellow and then crumbles. And in the hereafter (later) there will be harsh punishment and forgiveness from Allah and His good pleasure. And the life of this world is nothing but deceptive pleasures. "	451	嬸硃?駞鐓笹⁝??殌?⁝? r 䶢舫䶜⁝??ｒ⁝舫씴ｒ ⁝駞⁝??씴칅⁝鐓駞 r 舫訛⁝씴칅⁝駞?舫䶜⁝ 殌⁝ś殌夈ｒ⁝殌?訛⁝殌⁝?ｒś舫ｒ䳄?笹⁝殌訛駞 r ?夈ｒ??⁝殌?訛⁝剡駞殌칅?씴?ś⁝殌夈駞?ś ⁝䶜駞䶢⁝殌?訛⁝剡駞殌칅?씴?ś⁝殌剡駞䶢 ?⁝??ｒ⁝殌剡䶢?訛殌?䳄ｒ⁝駞⁝鐓ｒ殌舫??⁝ 殌?訛⁝䳄?씴舫訛 r ｒ?笹⁝舫씴吩ｒ⁝ r 殌씴? ⁝鐓?駞칅ｒ⁝䳄 r 駞鬡칅⁝殌夈殌銜ｒ⁝??ｒ⁝鬡 ｒ殌칅殌??칅?⁝?ｒ?⁝??ｒ⁝鬡舫殌??⁝訛 r 씴 ｒ칅⁝䶢鬡⁝殌?訛⁝䶜駞䶢⁝칅ｒｒ⁝씴?⁝씴칅⁝ 䶜ｒ舫舫駞鐓⁝殌?訛⁝??ｒ?⁝䳄 r 䶢夈剡舫ｒ 칅⁝ϱ?訛⁝씴?⁝??ｒ⁝?ｒ r ｒ殌?ｒ r ⁝歎舫殌?ｒ r ⁝??ｒ r ｒ⁝鐓씴舫舫⁝剡ｒ⁝?殌 r 칅?⁝鬡䶢 ?씴칅?夈ｒ??⁝殌?訛⁝駞 r ś씴珪ｒ?ｒ칅칅⁝ r 駞夈⁝ϱ舫舫殌?⁝殌?訛⁝FAX씴칅⁝ś駞駞訛⁝ 鬡舫ｒ殌칅䶢 r ｒ⁝ϱ?訛⁝??ｒ⁝舫씴ｒ⁝駞⁝?? 씴칅⁝鐓駞 r 舫訛⁝씴칅⁝?駞??씴?ś⁝剡䶢? ⁝訛ｒ䳄ｒ鬡?씴珪ｒ⁝鬡舫ｒ殌칅䶢 r ｒ칅⁝嬸⁝⁝ ⁝⁝	4.257107430057822

3	Politeknik Samarinda. Politeknik Samarinda.	512	Njꝏꝺꝺꝏ扎█扎ꟼNj?ㅆ扎 ꝺ?ꝏ ẻњ ǀ Nj ؤ Njꝏꝺꝺꝏ扎█扎ꟼNj?ㅆ扎 ꝺ?ꝏ ẻњ ǀ Nj Njꝏꝺꝺꝏ扎█扎ꟼNj?ㅆ扎 ꝺ?ꝏ ẻњ ǀ Nj Njꝏꝺꝺꝏ扎█扎ꟼNj?ㅆ扎 ꝺ њ?ꝏ ẻњ ǀ Nj Njꝏꝺꝺꝏ扎█扎ꟼNj?ㅆ扎 ꝺ њ ǀ ?ꝏ ẻ ǀ Nj Njꝏꝺꝺꝏ扎█扎ꟼNj?ㅆ扎 ꝺ њ ǀ Nj?ꝏ ẻNj ẻNjꝏꝺꝺꝏ扎█扎ꟼNj?ㅆ扎 ꝺ њ ǀ Nj?ꝏ ẻ ẻNjꝏꝺꝺꝏ扎█扎ꟼNj?ㅆ扎 ꝺ њ ǀ Nj?ꝏ ꝏ ẻNjꝏꝺꝺꝏ扎█扎ꟼNj?ㅆ扎 ꝺ њ ǀ Nj?ꝏ ?ꝏ ẻNjꝏꝺꝺꝏ扎█扎ꟼNj?ㅆ扎 ꝺ њ ǀ Nj? Nj?ꝏ ẻNjꝏꝺꝺꝏ扎█扎ꟼNj?ㅆ扎 ꝺ њ ǀ Nj ꝏNj?ꝏ ẻꝺꝺꝏ扎█扎ꟼNj?ㅆ扎 ꝺ њ ǀ Njꝏ Njꝏꝺ?ꝏ ẻꝺꝺꝏ扎█扎ꟼNj?ㅆ扎 ꝺ њ ǀ Nj Njꝏꝺ?ꝏ ẻꝺꝏ扎█扎ꟼNj?ㅆ扎 ꝺ њ ǀ Nj Njꝏꝺ?ꝏ ẻꝺꝏ扎█扎ꟼNj?ㅆ扎 ꝺ њ ǀ Nj Njꝏꝺ?ꝏ ẻꝺꝏ扎█扎ꟼNj?ㅆ扎 ꝺ њ ǀ Nj Njꝏꝺ?ꝏ ẻꝺꝏ扎█扎ꟼNj?ㅆ扎 ꝺ њ ǀ Nj Njꝏꝺ?ꝏ ẻꝺꝏ扎█扎ꟼNj?ㅆ扎 ꝺ њ ǀ Nj Njꝏꝺ?ꝏ ẻꝺꝏ扎█扎ꟼNj?ㅆ扎 ꝺ њ ǀ Nj Njꝏꝺꝺꝏ?ꝏ ẻꝺꝏ扎█扎ꟼNj?ㅆ扎 њ ǀ Nj █Njꝏꝺꝺꝏ扎?ꝏ ẻ扎█扎ꟼNj?ㅆ扎 њ ǀ Nj Njꝏꝺꝺꝏ扎█扎ꟼ?ꝏ ẻ扎ꟼNj?ㅆ扎 њ ǀ Nj ꝺꝺꝺꝺꝺꝺꝺꝺꝺؤNj?ㅆ扎	3.77391380004984

4	jika menggunakan simbol !@#$%^&*()_+{}:"><[];',/|~` apakah memiliki has1l perbandingan sama atau berbeda, belum diketahui karena sedang dicoba dan lihatlah disamping ini hasilnya jika menggunakan simbol ! dikeyboard sampai simbol ? dengan berdasarkan informasi peranti waktu yang digunakan dalam penentuan p dan q yang detailnya ada pada tahapan sebelumnya, ok! nb: fokus analisanya ada pada nilai keacakan data yang menggunakan shannon enteropi	451	卤鲨 侀羿怄焖碕蚯匱匱睖蚯羿侀羿蚯怄纤焖 ʁx ▯怄m調: 糅Ē標宥ᴍ嫱儥亩曦磯婪Ⅴ熠猓 ℊ 吠▯乀踇輥伏罐▯怄羿▯羿侀羿▯ ℊ 怄焖碕焖 ▯ 侀 怄▯ 羿纤ᵪ▯怄▯碕瑛 羿蚯隱 蚯匱羿蚯怄纤羿焖 羿怄羿侶羿睖怄 碕换 碕隱羿輥怄 碕▯睖焖 怄隱 侀碕侶羿▯ 睖ℊ怄侀羿瑛碕蚯羿怄纤碕隱羿蚯匱怄隱 ▯ ʁx 羿怄隱羿蚯怄▯ ▯羿侶▯羿▯ 怄隱 纤羿焖▯ 蚯匱怄 蚯 怄▯ ℊ 羿纤 ▯蚯賅羿怄鲨 侀羿怄焖碕蚯匱匱睖蚯 羿侀羿蚯怄纤 焖 ʁx怄m怄隱 侀碕賅 ʁx羿 瑛隱怄纤羿焖▯羿 怄纤 焖 ʁx▯怄缪怄隱碕 蚯匱羿蚯怄 碕瑛隱羿纤羿瑛侀羿蚯怄 蚯ᵪʁx 瑛焖羿纤 怄▯碕瑛羿蚯侶 怄鸟羿侀侶睖怄 賅羿蚯匱怄隱 匱睖蚯羿侀羿蚯怄隱羿▯羿焖 怄▯碕蚯碕蚯侶睖羿蚯怄▯怄隱羿蚯怄唬怄賅 羿蚯匱 怄隱碕侶羿 ▯蚯賅羿怄羿隱羿怄▯羿 隱羿怄侶羿▯ 羿▯羿蚯怄纤碕 碕 侀睖焖賅羿毦怄ʁx侀m怄 蚯 婪 怄ᵪʁx侀睖纤怄羿蚯羿 纤羿蚯賅羿怄 羿隱羿怄▯羿隱羿怄蚯 ▯羿 怄侀碕羿▯羿侀 羿蚯怄隱羿侶羿怄賅羿蚯匱怄焖碕蚯匱匱睖 蚯羿侀羿蚯怄纤▯ 羿蚯蚯ʁx蚯怄碕蚯侶碕瑛ʁx▯ 卤怄怄怄怄 ℊ	4.421087076196203

Tabel 4.5.2 Hasil Pembangkitan kunci selama 1 jam

DATA	*ZA* (HH:mm:ss)	*ZL* (hh:mm:ss)	*sudoRandom Zi*	*p*	*q*	kunci	
						publik	private
1	16:51:05 GMT + 8	06:51:07 GMT-6	5	97	167	121	4873
2	16:56:01 GMT +8	02:56:02 GMT-2	1	23	167	89	2421
3	17:01:01 GMT +8	03:01:02 GMT-2	1	41	23	27	163
4	17:06:01 GMT +8	14:06:02 GMT+11	21	269	137	73	32953
5	17:11:01 GMT +8	06:11:02 GMT-5	4	97	241	199	10999
6	17:16:01 GMT +8	12:16:02 GMT+13	23	227	367	227	17855
7	17:21:01 GMT +8	18:21:02 GMT+7	17	367	487	283	143935
8	17:26:01 GMT +8	14:26:02 GMT+11	21	269	53	35	11547
9	17:31:01 GMT +8	13:31:02 GMT+12	22	241	151	137	22073
10	17:36:01 GMT +8	04:36:02 GMT-3	2	59	263	117	11949

11	17:41:01 GMT +8	15:41:02 GMT+10	20	283	383	239	51383
12	17:46:01 GMT +8	11:46:02 GMT-10	9	197	503	225	20553
rata - rata panjang kunci publik dan privat 2 bit - 17 bit (2 digit - 5 digit)							

Tabel 4.5.3 Teks uji dan hasil enkripsi RSA dengan *p* dan *q* default

No	Teks Asli	Jumlah Karakter	Hasil Enkripsi	Entropi Enkripsi
1	“Ketahuilah, bahwa sesungguhnya kehidupan dunia ini hanyalah permainan dan suatu yang melalaikan, perhiasan dan bermegah-megah antara kamu serta berbangga-banggaan tentang banyaknya harta dan anak, seperti hujan yang tanam-tanamannya mengagumkan para petani; kemudian tanaman itu menjadi kering dan kamu lihat warnanya kuning kemudian menjadi hancur. Dan di akhirat (nanti) ada azab yang keras dan ampunan dari Allah serta keridhaan-Nya. Dan kehidupan	512	Þ$ḋzⱮ⁽ÖÎŘ.⍰ÖÎŘƵĠMÖÎŘ¬ÖÎƓϑⱮϑƆŭŭŘƆÖÎƓΨⱮŘ.ŭṢÖÎƆĠŭƆ.ÖÎĠ.Ɔ.ĠŘÖÎƆÖÎ⍰ÖÎŘƓṢⱮ ÖÎ.ƆÖÎƆĠŭÖÎƆƓϑÖÎ⁽ƓÖÎƆŭĠ ⱮⱮ ⱮŭÖÎŘ¿ ⱮŭÖÎŘĠÖÎƆ⁽ÖÎÖÎƓΨÖÎ ĠϑⱮ⁽ÖÎĠMⱮⱮMÖÎƆŭŭÖÎ¿MÖÎƆŭŭÖÎÖÎƆĠ⁽ⱮƆ⁽ÖÎƆŭĠMÖÎƆÖÎΨÖÎƆÖÎĠŘÖÎ⁽ÖÎĠüÖÎƆĠÖÎƆÖÎΨƵĠⱮⱮSⱮⱮ.⁽ĠŘƅ⁽ÖÎƆĠÖÎƆŭĠ⁽ÖÎƆÖÎ Ĺ⁽ÖÎƆÖÎ ÖÎƆƆÖÎĠ ⱮƆŭÖÎŭ ΨÖÎ ƆĠṢÖÎÖÎĠSⱮ⁽ÖÎƆ.ʷĠΨⱮⱮ ŭ.ÖÎƆĠ⁽ÖÎƆ ÖÎ ÖÎƆĠ⁽.Ġ ⱮƆƅ⁽ÖÎüⱮ.ĠΨⱮⱮ.ƆŭĠüÖÎƆĠ ΨÖÎ Ġ⍰.ŘÖÎ⁽Ġ¬ÖÎƆÖÎƆÖÎĠΨÖÎƆ.ƆŭĠΨⱮⱮ ŭ.ÖÎƆĠ ⱮƆƅ⁽ÖÎüⱮ.ĠŘÖÎƆ␣⍰ĠĹÖÎƆĠüⱮ.Ġ ÖÎΨÖÎŘ.ÖÎ⁽ĠĹƆÖÎƆ.⁽ÕĠÖÎüÖÎĠÖÎ⍰ ÖÎMĠÖÎƆŭĠΨⱮⱮÖÎϑüÖÎƆĠÖÎ ṢƆÖÎƆĠ ŭÖÎ.ĠⱮ⍰⍰ÖÎŘĠϑⱮ⁽ÖÎĠΨⱮⱮ.ŭŘÖÎÖÎƆ¿⍰ÖÎ ⍰ĠĹÖÎƆĠΨⱮⱮŘ.ŭṢÖÎƆĠüƆ.ÖÎĠ.Ɔ.Ġ⁽üÖÎΨⱮĠ⍰ÖÎ.ƆĠŘÖÎƆÖÎ⍰ÖÎŘĠΨⱮⱮϑⱮⱮƆÖÎƆŭÖÎ ƆĠÖÎƆŭĠ ⱮⱮƆ.Ṣ⍰ŕÞĠĠĠĠ	4.035569614562073
2	"Know, that truly the life of this world is only a game and a neglect, adornment and boasting among you and boasting about the abundance of wealth and children, like rain whose crops amaze the peasants; Then the plant dries up and you see it is yellow and then crumbles. And in the hereafter (later) there will be harsh punishment and forgiveness from Allah and His good pleasure. And the life of this world is nothing but deceptive pleasures. "	451	纂ὐ垴貉婪ㄐ柏茼鄄┌淅鄂茼鄄ơ涞▫招茼鄂┌⍰茼▫橞呖⍰茼婪呖茼鄄┌橞嫊茼ㄐ婪ơ▫闌茼橞嫊茼婪貉▫招茼淅茼显淅艚⍰茼淅貉闌茼淅茼貉⍰显▫⍰ **鄂柏**茼淅闌婪ơ**貉體**⍰**貉鄂**茼淅貉闌茼婪淅嫊鄄橞貉显茼淅艚婪**貉**显茼招婪涞茼淅貉闌茼婪淅嫊鄄橞貉显茼淅婪涞鄄茼鄄┌⍰茼淅涞貉闌淅貉‖⍰茼婪呖茼ㄐ⍰**淅▫鄂**┌茼淅貉闌茼‖┌橞▫闌ơ⍰**貉柏**茼▫橞曝⍰茼ơ**淅**橞貉茼ㄐ┌**婪**嫊⍰茼‖ơ**婪所**嫊茼淅艚淅瑎⍰茼鄄┌⍰茼所⍰**淅**嫊淅貉鄂嫊ǐ茼蝏┌⍰**貉**茼鄄┌⍰茼所▫**淅貉鄂**茼闌ơ橞⍰嫊茼涞所茼淅貉闌茼招婪涞茼嫊⍰⍰茼橞鄂茼橞嫊茼招▫▫**婪**ㄐ茼淅貉闌茼鄄┌⍰**貉**茼ㄧơ涞**體**▫⍰嫊靓茼帼貉闌茼橞貉茼鄄┌⍰茼┌⍰ơ⍰**淅**呖鄂⍰ơ茼λ▫**淅鄂**⍰ơ貢茼鄄┌⍰ơ⍰茼ㄐ橞▫▫茼⍰茼┌**淅**ơ嫊┌茼所涞貉橞嫊┌**體**⍰**貉鄂**茼淅貉闌茼呖婪ơ显橞掾⍰**貉**⍰嫊嫊茼呖ơ**婪體**茼帼▫▫**淅**┌茼淅貉闌茼箇橞嫊茼显婪婪闌茼所▫⍰**淅**嫊涞ơ⍰**靓**茼帼貉闌茼鄂┌⍰茼▫橞呖⍰茼婪呖茼鄄┌橞嫊茼ㄐ**婪**ơ▫闌茼橞嫊茼貉婪鄂┌橞貉显茼涞鄄茼闌⍰ ⍰**所鄂**橞掾⍰茼所▫⍰**淅**嫊涞ơ⍰嫊靓茼ὐ纂茼茼茼茼 ‖	4.257107430057822

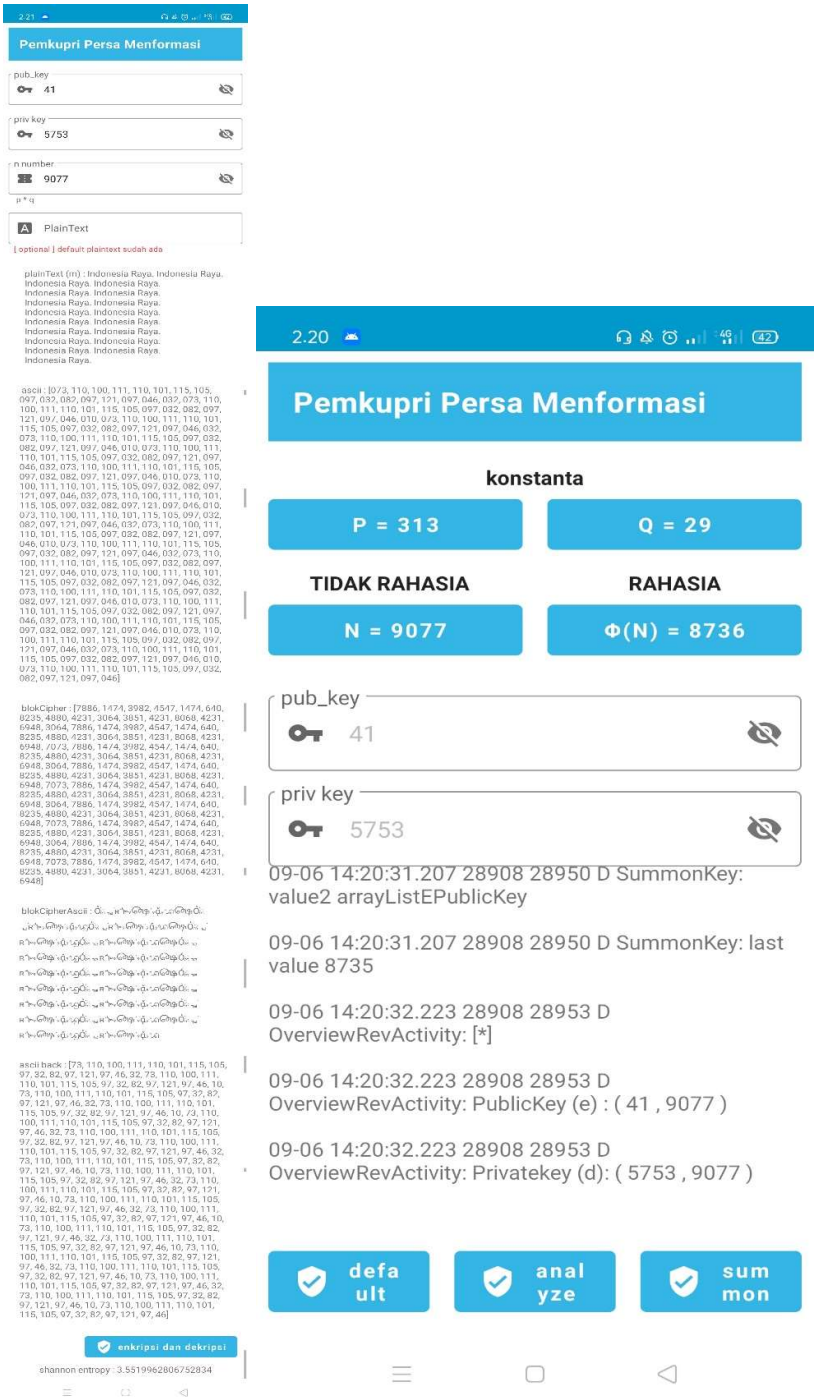
3	Politeknik Samarinda. Politeknik Samarinda.	512	睭瘦鋖芍ズ٩ ڬ茹ズڬ蠞⍰ۦ⁂ۦ豁ズ茹ۦپ鴧 蠞瘦鋖芍ズ٩ ڬ茹ズڬ蠞⍰ۦ⁂ۦ豁ズ茹ۦپ鴧 蠞瘦鋖芍ズ٩✠ڬ茹ズڬ蠞⍰ۦ⁂ۦ豁ズ茹ۦپ鴧 蠞瘦鋖芍ズ٩✠ڬ茹ズڬ蠞⍰ۦ⁂ۦ豁ズ茹ۦپ鴧 蠞瘦鋖芍ズ٩✠ڬ茹ズڬ蠞⍰ۦ⁂ۦ豁ズ茹ۦپ鴧 蠞瘦鋖芍ズ٩✠ڬ茹ズڬ蠞⍰ۦ⁂ۦ豁ズ茹ۦپ鴧 蠞瘦鋖芍ズ٩✠ڬ茹ズڬ蠞⍰ۦ⁂ۦ豁ズ茹ۦپ鴧 蠞瘦鋖芍ズ٩✠ڬ茹ズڬ蠞⍰ۦ⁂ۦ豁ズ茹ۦپ鴧 蠞瘦鋖芍ズ٩✠ڬ茹ズڬ蠞⍰ۦ⁂ۦ豁ズ茹ۦپ鴧 蠞瘦鋖芍ズ٩✠ڬ茹ズڬ蠞⍰ۦ⁂ۦ豁ズ茹ۦپ鴧 蠞瘦鋖芍ズ٩✠ڬ茹ズڬ蠞⍰ۦ⁂ۦ豁ズ茹ۦپ鴧 蠞瘦鋖芍ズ٩✠ڬ茹ズڬ蠞⍰ۦ⁂ۦ豁ズ茹ۦپ鴧 蠞瘦鋖芍ズ٩✠ڬ茹ズڬ蠞⍰ۦ⁂ۦ豁ズ茹ۦپ鴧 蠞瘦鋖芍ズ٩✠ڬ茹ズڬ蠞⍰ۦ⁂ۦ豁ズ茹ۦپ鴧 蠞瘦鋖芍ズ٩✠ڬ茹ズڬ蠞⍰ۦ⁂ۦ豁ズ茹ۦپ鴧 蠞瘦鋖芍ズ٩✠ڬ茹ズڬ蠞⍰ۦ⁂ۦ豁ズ茹ۦپ鴧 蠞瘦鋖芍ズ٩✠ڬ茹ズڬ蠞⍰ۦ⁂ۦ豁ズ茹ۦپ鴧 蠞瘦鋖芍ズ٩✠ڬ茹ズڬ蠞⍰ۦ⁂ۦ豁ズ茹ۦپ鴧 蠞瘦鋖芍ズ٩✠ڬ茹ズڬ蠞⍰ۦ⁂ۦ豁ズ茹ۦپ鴧 蠞瘦鋖芍ズ٩✠ڬ茹ズڬ蠞⍰ۦ⁂ۦ豁ズ茹ۦپ鴧 瘦鋖芍ズ٩ ✠ڬ茹ズڬ蠞⍰ۦ⁂ۦ豁ズ茹ۦپ鴧瘦 鋖芍ズ٩ ✠ڬ茹ズڬ蠞⍰ۦ⁂ۦ豁ズ茹ۦپ鴧瘦鋖 芍ズ٩ ڬ茹✠ズڬ蠞⍰ۦ⁂ۦ豁ズ茹ۦپ鴧睭蠞蠞 ✠ 蠞蠞蠞蠞蠞蠞 ✠	3.77391380004984

4	jika menggunakan simbol !@#$%^&*()_+{}:"><[];',/|~` apakah memiliki has1l perbandingan sama atau berbeda, belum diketahui karena sedang dicoba dan lihatlah disamping ini hasilnya jika menggunakan simbol ! dikeyboard sampai simbol ? dengan berdasarkan informasi peranti waktu yang digunakan dalam penentuan p dan q yang detailnya ada pada tahapan sebelumnya, ok! nb: fokus analisanya ada pada nilai keacakan data yang menggunakan shannon enteropi	451	uĐ¯ǫfŋĭҤƠøøƮǪǫƠfŋΣ¯ĭϢΎʂfŋ̈x≥¥ˈÂËĘȫwÔЮҷ -ҺČǿӿɵljˀϤȺŞËfŋƤǫҺfŋĭҤĭ¯ʂ¯ɔ¯fŋҔΣςʂfŋƤҤiϢ ƠŰ¯ƠǿƠfŋΣĭfŋπƮfŋϢҤiϢҤŰˀfŋϢҤʂƮĭfŋŰ¯ɔ ҤπҺƮ¯fŋǫiҤǪfŋΣҤŰƠøfŋŰ¯FΎϢfŋŰƠfŋʂ¯Ҕπʂ ҺfŋŰ¯ΣĭƤ¯Ơøfŋ¯Ơ¯fŋҔΣ¯ʂƠĮfŋĐ¯ǫfŋĭҤƠøøƮǪǫ ƠfŋΣ¯ĭϢΎʂfŋ̈fŋŰ¯ɔҤÏϢΎiŰfŋΣĭƤ¯fŋΣ¯ĭϢΎʂfŋvfŋ ŰҤƠǿƠfŋϢҤiŰΣiǫƠfŋ¯ƠɩΎiĭΣ¯fŋƤҤiƠπ¯fŋĿɔπ ƮfŋÏƠøfŋŰ¯øƮǪǫƠfŋŰʂĭfŋƤҤƠҤƠπƮƠfŋƤfŋŰƠ fŋNfŋÏƠøfŋŰҤπ¯ʂƠĮfŋŰfŋƤŰfŋπҔƤƠfŋΣҤϢҤ ʂƮĭƠĮˀfŋΎ̈ɔfŋƠϢҷfŋɩΎɔƮΣfŋǪʂ¯ΣƠĮfŋŰfŋƤŰfŋƠ¯ ʂ¯fŋɔҤFǫƠfŋŰπfŋÏƠøfŋĭҤƠøøƮǪǫƠfŋΣҔƠƠΎƠ fŋҤƠπҤiΎƤ¯ufŋfŋfŋfŋ	4.421087076196203

Tabel 4.5.4 Hasil Pembangkitan kunci secara umum atau default

DATA	*p*	*q*	kunci	
			publik	private
1	61	227	191	13631
2	53	331	301	5701
3	89	409	281	12905
4	257	137	71	14711
5	61	113	137	1913
6	229	211	221	33581
7	113	2	3	187

8	83	139	109	6229
9	7	173	125	677
10	127	389	275	30755
11	97	401	299	899
12	71	53	53	1717
rata - rata panjang kunci publik dan privat 2 bit - 17 bit (2 digit - 5 digit)				



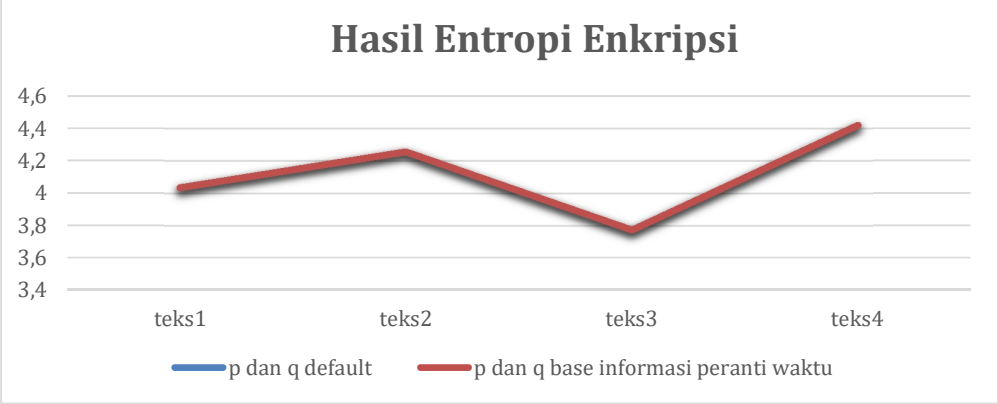
(2) (1)

Gambar 4.5 Tampilan Aplikasi Pembangkitan (2) dan Proses Enkripsi Dekripsi

(1)

4.6 Analisa Hasil

Berdasarkan Hasil Mengukur Keacakan Data, Pada Tabel 4.5.1 Hasil entropi enkripsi memiliki nilai yang ekuivalen terhadap Hasil entropi enkripsi pada



Gambar 4.6 Hasil Entropi Enkripsi

Tabel 4.5.3 dan Hasil seluruh teks uji pada p dan q *default* dengan p dan q *base* informasi peranti waktu jam menit detik memiliki hasil enkripsi yang berbeda seperti yang diperlihatkan pada Tabel 4.6.

Tabel 4.6 Perbandingan Hasil Enkripsi Teks 4

p dan q base informasi peranti	p dan q default
Hasil Enkripsi Teks 4	Hasil Enkripsi Teks 4
卤鲶 俐羿怄焚碕蚯匱匱睖蚯羿俐羿蚯怄纤 焚 ʁx ı怄m詷: 糅È標肓ʍ僆儥亘噶磏婪Ṽ熠獚吠⍰\ₒ踡輒伏 罐ᵍ⍰怄羿⍰羿俐羿⍰怄焚碕焚 ı 俐 怄⍰ 羿纤ₔ́ı怄⍰碕瑛 羿蚯隱 蚯匱羿蚯怄纤羿焚羿怄羿侶羿睖怄 碕瑛 碕隱羿輒怄 碕ı睖焚怄ᵍ隱ᵍ俐禽侶羿⍰ 睖ᵍ怄俐羿瑛碕蚯羿怄纤ᵍ碕隱羿蚯匱怄隱 ⍰ʁx 羿怄隱羿蚯 怄ı ⍰羿侶ı羿⍰怄隱 纤羿焚⍰ 蚯匱怄 蚯 怄⍰ 羿纤 ı蚯賅羿怄鲶 俐羿怄焚碕蚯匱匱睖蚯羿俐羿蚯怄纤 焚 ʁx ı怄m怄隱 俐碕賅ᵍʁx羿瑛隱怄纤羿焚⍰羿ᵍ 怄纤 焚 ʁx ı怄缪怄隱碕蚯匱羿蚯怄 碕瑛隱羿纤羿瑛俐羿蚯怄 蚯ᵍ ʁx瑛焚羿纤 怄⍰碕瑛羿蚯侶 怄鸟羿俐侶睖怄賅羿蚯匱怄 隱 匱睖蚯羿俐羿蚯怄隱羿ı羿焚怄⍰碕蚯碕蚯侶睖羿蚯怄⍰ 怄隱羿蚯怄ᵍ晚怄賅羿蚯匱怄隱碕侶羿 ı蚯賅羿怄羿隱羿怄 ᵍ ⍰羿隱羿怄侶羿⍰ 羿⍰羿蚯怄纤碕 碕ı睖焚蚯賅羿輒怄ᵍ俐m怄蚯 婪怄ₔ́ʁx俐 睖纤怄羿蚯羿ı 纤羿蚯賅羿怄羿隱羿怄⍰羿隱羿怄蚯 ı羿 怄俐碕羿⍰羿俐羿蚯怄隱羿侶羿怄賅羿蚯匱怄焚碕蚯匱匱睖 ᵍ ᵍ ᵍ 蚯羿俐羿蚯怄纤⍰ 羿蚯蚯ʁx蚯怄碕蚯侶碕瑛ʁx⍰ 卤怄怄怄怄 ᵍ	uÐ¯ɟɱjïHʊƠøøŢǪɟǫƠɱƩ¯ïƆƳʏsɱx̃ɟɣ¦ÂËĘȫwÔⱧOɥ- ɦČøжølj³ɥѦŞËɱƤɟǫȞɱjïHuï˜ş¯ɔ¯ɱȞʂƩçşɱƤHuiĢƠǖ¯ƠøƠɱʒĭɱɲţ ɱƓHuiƆHuǖ²ɱƓHuʂŢĭɱǖ¯ɔHuɲȞŢ¯ɱɟiHǪƠɱƩHǖƠøƥǖ¯FʏǪɟɱ ǖƠƒɲş¯ȞɲnʂȞɱǖ¯ʒĬᴾ¯Ơøɱ¯Ơ¯ɱȞʂƩ¯şƠ[ɱÐ¯ɟɱjïHʊƠøøŢǪɟǫƠɱƩ¯ï ƆƳʏşɱ̃ɱǖ¯ɔHuïƆƳʏiǖɱʒĬᴾ¯ɱƩ¯ïƆƳʏşɱvɱǖHʊƠøǫƠɱƓHuiǖʒiɟǫƠ ɱ¯Ơ'ʏiʒ¯ɱƤHuȷƠn¯ɱʟɔnŢɱ[Ơøɱǖ¯øŢǪɟǫƠɱǖʒĭɱƤHʊƠHʊƠnŢǫƠ ɱƤɱǖƠɱNɱ[ƠøɱǖHuɲ¯şƠ[ɱǖɱƤǖɱƤɱƩHƓHuşŢĭƠ[ˀɱƴ ɜɱƠƓɥɱʏƳɔŢƩɱǪʂ¯ʒƠ[ɱǖɱƤǖɱƠ¯ş¯ɱɔHuɟʒƠɱǖɲɱ[ƠøɱǖHu ƠøøŢǪɟǫƠɱƩȞƠƠƳƠɱHʊƠnHuiƳƤ¯uɱɱɱɱɱ

BAB V

PENUTUP

5.1 Kesimpulan

Penlitian dan percobaan yang telah dilakukan menghasilkan kesimpulan sebagai berikut:

1. Dari Analisa Hasil P dan Q

   A. Hasil *p* dan *q* yang dibangkitkan berukuran 2 *bit* sampai 17 bit, pembangkitan yang diketahui hanya waktu dalam 1 jam yaitu pada jam 16:51:05GMT+8 sampai dengan 17:46:01 GMT+8.

   B. Hasil proses kombinasi berdasarkan infomasi peranti waktu diuji keberhasilan program dengan *monitoring* pengecualian sehingga menghasilkan tidak ada *feedback* berupa pengecualian di seluruh pemrosesan.

2. Dari Analisa Hasil Entropi Enkripsi, didapat teks 1 = 4.035569614562073, teks 2 = 4.257107430057822, teks 3 = 3.77391380004984 dan teks 4 = 4.421087076196203. Enkripsi dilakukan dengan bantuan RSA (*Rivest Shamir Adleman*) yang proses didalamnya menghadirkan p dan q berdasarkan informasi peranti. Hasil seluruh teks memiliki nilai entropi yang ekuivalen dengan hasil entrop enkripsi rsa yang proses didalamnya (*p* dan *q*) ditentukan default.

5.2 Saran

Adapun saran pada penelitian ini sebagai berikut:

1. Efek *Avalanche*, dapat ditambahkan yang digunakan untuk menilai seberapa signifikan perubahan yang terjadi pada cipherteks karena adanya perubahan kecil, baik pada pesan maupun pada kunci. AE dihitung menggunakan Persamaan 8. AE dikatakan baik jika perubahan bit yang terjadi berkisar antara 45 % hingga 60 % (Sugiyanto & Hapsari, 2017). Semakin banyak bit yang berubah mengindikasikan bahwa algoritme enkripsi tersebut semakin sulit untuk dipecahkan.

$$AE = \frac{Jumlah\ bit\ yangberubah}{Jumlah\ bit\ cipherteks}\ 100\%$$

2. Eksperimen berdasarkan informasi peranti waktu dapat digunakan pada hasil enkripsi untuk modifikasi, dimana *block ciphertext* tertentu diputar atau dipindah berdasarkan nilai informasi peranti dan dikembalikan dengan menyimpan nilai informasi peranti ke dalam memory sementara atau dengan rumus tertentu.
3. Informasi peranti bisa menggunakan informasi selain waktu jam menit dan detik untuk kemudahan lainya tergantung pada peranti yang diterapkan.
4. Gunakan metode lain sebagai bantuan untuk menjadikan hasil p dan q menjadi kunci enkripsi.

DATAR PUSTAKA

Cahyo Dhea Arokhman Yusufi. (2020). *Heuristic - For Mathematical Olympiad Approach*. Math Heuristic. https://books.google.co.id/books?id=OJriDwAAQBAJ&pg=PA18&lpg=PA18&dq=6k+%2B+1+selalu+prima+?&source=bl&ots=aWNDfVbx9w&sig=ACfU3U3JQyCKsvq5_G4JUSbp8WKZhr_7Tw&hl=en&sa=X&ved=2ahUKEwiW9eXuhr_qAhUkheYKHfrHAJ4Q6AEwCnoECAoQAQ#v=snippet&q=prima&f=false

Chiewchanchairat, K., Bumroongsri, P., & Kheawhom, S. (2016). Improving fermat factorization algorithm by dividing modulus into three forms. *KKU Engineering Journal*, *40*(March), 131–138. https://doi.org/10.14456/kkuenj.2015.1

FAQ - Kotlin Programming Language. (n.d.). Diambil 15 Agustus 2020, dari https://kotlinlang.org/docs/reference/faq.html

Ferreira, J. W. P. (2017). The Pattern of Prime Numbers. *Applied Mathematics*, *08*(02), 180–192. https://doi.org/10.4236/am.2017.82015

Firmansyah, F. F. (2015). *Kajian matematis dan penggunaan bilangan prima pada algoritma kriptografi RSA (Rivest, Shamir, dan Adleman) dan algoritma kriptografi Elgamal [skripsi]*.

Harahap, M. K. (2019). *Membangkitkan Bilangan Prima Marsenne dengan metode Bilangan Prima Probabilistik Solovay – Strassen*. *1*(Oktober).

Kumari, J., Singh, S., & Saxena, A. (2015). *An Exception Monitoring Using Java*.

3(2), 12–18.

Meštrović, R. (2018). *Euclid's theorem on the infinitude of primes: a historical survey of its proofs (300 B.C.--2017) and another new proof*. http://arxiv.org/abs/1202.3670

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.

Prime Numbers - GeeksforGeeks. (n.d.). Diambil 15 Agustus 2020, dari https://www.geeksforgeeks.org/prime-numbers/?ref=lbp

Rihartanto, R., Ningsih, R. K., Gaffar, A. F. O., & Utomo, D. S. B. (2020). Implementation of vigenere cipher 128 and square rotation in securing text messages. *Jurnal Teknologi dan Sistem Komputer*, *8*(3), 201–209. https://doi.org/10.14710/jtsiskom.2020.13476

Sari, R. H. (2017). Apakah Integrasi Islam dapat Membudayakan Literasi Matematika ? *Seminar Matematika dan Pendidikan Matematika UNY*, 655–662.

Sciences, T. (2016). *Dirichlet ' s Theorem Related Prime Gap*. *10*, 305–310.

Serdano, A., Zarlis, M., Sawaluddin, & Hartama, D. (2019). Pengamanan Pesan Menggunakna Algoritma Hill Cipher Dalam Keamanan Komputer. *Jurnal*

Mahajana Informasi, *2*, 1–5.

Sugiyanto, S., & Hapsari, R. K. (2017). Pengembangan Algoritma Advanced Encryption Standard pada Sistem Keamanan SMS Berbasis Android Menggunakan Algoritma Vigenere. *Jurnal ULTIMATICS*, *8*(2), 131–138. https://doi.org/10.31937/ti.v8i2.528

Sylfania, D. Y., Juniawan, F. P., Laurentinus, L., & Pradana, H. A. (2019). SMS Security Improvement using RSA in Complaints Application on Regional Head Election's Fraud. *Jurnal Teknologi dan Sistem Komputer*, *7*(3), 116–120. https://doi.org/10.14710/jtsiskom.7.3.2019.116-120

TH, A., & MB, B. (2017). The Unique Natural Number Set and Distributed Prime Numbers. *Journal of Applied & Computational Mathematics*, *06*(04). https://doi.org/10.4172/2168-9679.1000368

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.