PEMBANGKITAN KUNCI YANG DIGUNAKAN 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

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 yang Digunakan 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, 2020

Yogi Arif Widodo

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

NOTASI

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 √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 Yang Digunakan 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 Yang Digunakan 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

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

1. Informasi peranti menggunakan waktu jam, menit dan detik.
    a. Waktu yang dipakai adalah sekarang
    b. 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

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 (Muhsetyo, 1997:1).

Teori bilangan merupakan dasar perhitungan dan menjadi salah satu teori yang mendasari pemahaman kriptografi, khususnya sistem kriptografi kunci publik. Bilangan yang dimaksud hanyalah bilangan bulat (integer).

2.2.2 Bilangan Bulat

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.

2.2.3 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.

2.2.4 Algoritma Pembagian

Jika a, b ∈ Z dan a > 0, maka ada bilangan q, r ∈ Z yang masing-masing tunggal sehingga b = qa + r dengan 0 r < a. Jika a∤b, maka r memenuhi ketidaksamaan 0 < r < a.

2.2.5 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 padalah himpunan {1, 2, 3,...,p - 1} yang mana seluruh anggotanya sebanyak (p - 1) sehingga φ(p) = p – 1.

2.2.6 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 (Munir, 2012:200). 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.

Definisi 2.8

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 $\sqrt{p}$. 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.

2.2.7 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 (Respatiadi, 2013).

Contoh:

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.

Contoh:

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 . $20 + n \cdot 5 = 1$.

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.

   $n = p * q$…….……..…….. (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 $CC = \frac{\sum_{i=1}^{m}\sum_{j=1}^{n}[W(i,j)*W\prime(i,j)}{\sum_{i=1}^{m}\sum_{j=1}^{n}(W(i,j))^2}$ 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.

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

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).

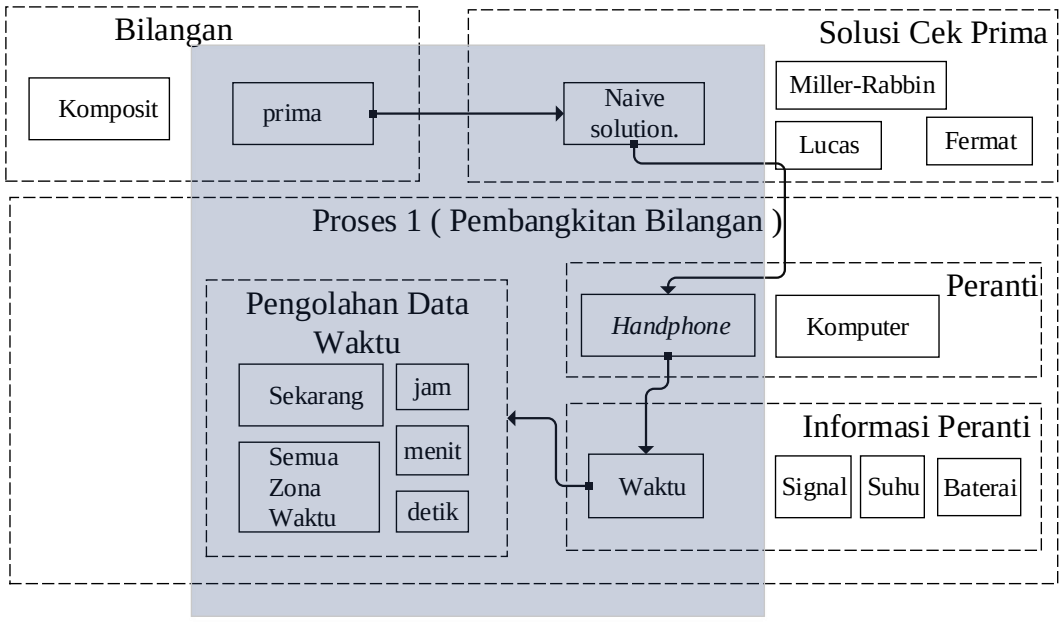
4. Baterai (voltase, daya atau persen dan lainnya).

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 aritmatika dilakukan dengan *handphone* yang dapat menghasilkan sebuah *metadata* atauu informasi yang beragam.

4. Informasi Peranti Waktu

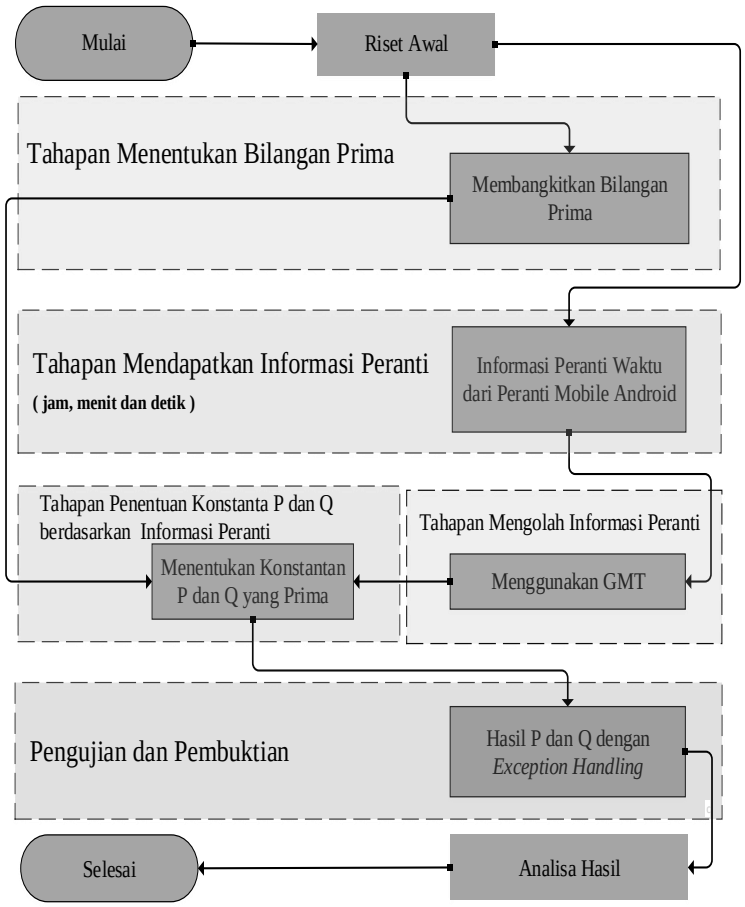
Waktu merupakan perhitungan masa dunia, dengan waktu dapat mengetahui kapan suatu hal terjadi. Khususnya proses aritmatika yang terjadi pada suatu perangkat atau peranti. Informasi ini dapat dengan mudah diperoleh dengan alat elektronik contohnya *handphone* atau komputer

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.

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 menentukan atau 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 , pengujian dan pembuktian, dan 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* denga hasil yang tersimpan dalam *ArrayList*.

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 angka akan menentukan zona yang terdaftar atau konversi terhadap data zona waktu yang telah didapatkan Perubahan zona

sendiri merupakan proses, tujuanya mengkonsumsi sebuah waktu ketika mendapatkan informasi waktu itu sendiri.

3.2.3 Tahapan Penentuan Konstanta P dan Q Berdasarkan Informasi Peranti

Penentuan akan dilakukan 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, Sekilas syarat dua akan menjadi posisi yang menjadikan syarat pertama menjadi outputnya sedemikian rupa.

3.2.4 Pengujian dan Pembuktian

Pengujian dilakukan dengan monitoring konsep menggunakan *Exception Handling* atau pengecualian sehingga akan membuktikan kombinasi peranti berhasil dilakukan dalam memilih konstanta *p* dan *q* yang prima jika tidak ada pengecualian yang dihasilkan.

3.2.5 Analisa Hasil

Menganalisa hasil dan proses terpilihnya kunci p dan q yang akan dikaitkan dengan GCD(*p-1, q-1*) dan rentang diantara keduanya dengan pembangkitan selama 1 jam dan membanding seluruh hasilnya berdasarkan proses kombinasi 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.

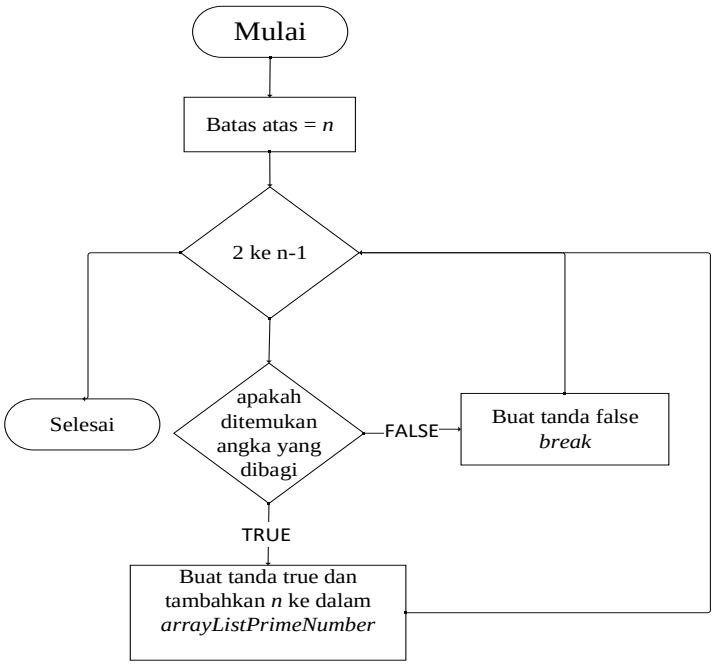
BAB IV

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 1.1 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 1.1

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 Gambar 4.2

Tabel 2.1 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 4.2 Hasil Zona Awal dan Zona Lain

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

Penentuan 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 2 syaratnya dimana ditentukan variabel $arrayListPrimeNumber = p = q$ untuk menghasilkan prima yang deterministik dari informasi peranti yang probabilistik, dilakukan sebagai 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, q) 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 3.1

Tabel 3 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 yang telah diuji pada Pengujian dan Pembuktian.

4.5 Pengujian dan Pembuktian

asda

4.6 Analisa Hasil

Hasil p dan q yang dibangkitkan berdasarkan informasi peranti waku jam, menit dan detik merupakan bilangan prima yang rata-rata menghasilkan panjang p dan q sebanyak 7 bit sampai 14 bit selama uji pembangkitan sebanyak 12 kali dalam tempo waktu setiap 5 menit dalam 1 jam dan benar p dan q adalah bagian dari bilangan prima berdasarkan uji primalitas sederhana dengan naive solution yang diperlihatkan pada Gambar 9 yang tidak jauh berbeda dengan Gambar 6.

Gambar 9. Potongan Kode Kotlin Cek Prima Naive Solution

Hasil kombinasi informasi peranti waktu jam, menit dan detik, memberikan pola sedemikian rupa terhadap hasil p dan q, dengan bantuan informasi berupa nilai yang digunakan sebagai posisi atau index dan telah dibuktikan penentuan dalam ketentuan p dan q dengan monitoring Exception Handling yang diperlihatkan pada Gambar 7, rumusnya telah berfungsi untuk setiap bilangan yang dibangkitkan atau ditentukan.

Ujianalisis Seluruh P dan Q Rentang 5 Menit Zona Awal(ZA) Zona Lain(ZL) Zona Index(Zi)

Tabel 4 Hasil Pembangkitan P dan Q

setiap 5 menit

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

Hasil pada penilitian [14] membuktikan bahwa bahasa pemrograman kotlin dapat mengurangi waktu kompilasi, waktu eksekusi dan dapat meningkatkan keringkasan. Maka berdasarkan hal tersebut kemampuan konsep sederhana ini menjadi efisien.

Gambar 4.2.1 Hasil Pembangkitan Kunci Pada Peranti *Android*

Nilai N atau $P * Q = 9563$ didefinisikan 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.

Matematikawan membuktikan bahwa bilangan prima terbesar itu tidak ada, bilangan prima 'terbesar' ditemukan, yaitu 277.232.917 – 1 yang diketahui pada Juli 2018 (*Untuk Apa Mencari Bilangan Prima Terbesar? - Anak Bertanya*, n.d.) diatasnya masih ada. Proses pembatasan prima mengkonsumsi sebuah waktu yang berhubungan dengan tahapan pengolahan informasi peranti yaitu jam, menit dan detik.

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 modus GCD 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.

Wicaksono, L. 2013. 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.

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

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.

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.

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

Untuk Apa Mencari Bilangan Prima Terbesar? - Anak Bertanya. (n.d.). Diambil 18 Juni 2020, dari https://anakbertanya.com/untuk-apa-mencari-bilangan-prima-terbesar/

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.