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

**1) Yogi Arif Widodo, 2) Mulyanto, S.Kom., M.Cs., dan 3)Bedi Suprapty, S.Kom., M.Kom.**

1,2,3)Program Studi, Teknik Informatika, Politeknik Negeri Samarinda

1,2,3)Jl. Cipto Mangun Kusumo Sungai Keledang – Samarinda - Indonesia

E-mail : *yogirenbox33@gmail.com, Penulis dua, dst…*

**ABSTRAK**

*Rivest* *Shamir* *Adleman* (RSA) merupakan teknik kriptografi modern yang melewati batas paten selama 20 tahun, sehingga mudah dibaca secara bebas. Sulitnya memfaktorkan bilangan besar menjadi faktor prima, serta perbedaan kunci dalam mengungkap teks maupun penyandian, membuat RSA menjadi salah satu teknik yang sulit dipecahkan. Bilangan konstanta atau orde *p* dan *q* menjadi eksperimen perhitungan menggunakan informasi peranti yaitu 24 zona waktu dengan format HH:mm:ss dan hh:mm:ss menghasilkan rentang 3000 lebih di waktu tertentu dan GCD kedua variable adalah 2. Pembangkitan tempo kelipatan 5 dalam menit selama kurung waktu 1 jam, menghasilkan entropi *p*, *q*, konversi *Greenwich* *Mean* *Time* *Zone* (GMT) = , dan ideal acuan data uji adalah . Kesesuaian waktu HH dan hh dipengaruhi oleh *pseudorandom*, mm konstanta dan ss adalah proses. Penerapan kunci privat RSA berhasil mendekripsi blok *cipher* (*c*) ke kode *American Standard Code for Information Interchange* (ASCII) bukan tunggal karakter atau null dengan *encoding* (UTF-8) dan lama prosesnya bergantung paling utama pada nilai p dan q yang dihasilkan oleh ketentuan, kemudian kondisi kecepatan baca peranti. Hasil GMT dipengaruhi oleh proses membatasi atas prima. Butuh sekitar 239.797 *miliseconds* (ms) untuk entropi ke 242 kode ASCII dengan menjadikan teks awal (8.083 ms nya adalah ASCII ke c) dan 1 sampai 2 detik untuk pembangkitan hingga kunci privat dimana p = 59 dan q = 3271.

**Kata Kunci: Bilangan Prima, Informasi Peranti Waktu, P dan Q , *Android* *Mobile***

***ABSTRACT***

*Rivest Shamir Adleman (RSA) is a modern cryptographic technique that exceeds the patent limit for 20 years, making it easy to read freely.*

***Keyword: Prime Number, Information Time Device, P and Q, Android Mobile***

### PENDAHULUAN

Bilangan prima adalah bilangan yang hanya memiliki dua faktor: 1 dan bilangan itu sendiri. Satu-satunya bilangan prima bernilai genap hanyalah 2 [1]. Kemudian akan muncul pertanyaan mengenai apakah 1 bilangan prima? tentu saja tidak. 1 hanya memiliki 1 faktor pembagi. Kita tidak menghitung 1 sebanyak dua kali. , maka *n* selalu memiliki setidaknya 1 faktor prima. Setiap bilangan asli lebih dari 1 yang tidak prima disebut bilangan komposit. Jika n adalah suatu bilangan komposit, maka n memiliki setidaknya 1 faktor prima yang nilainya tidak lebih dari . Bilangan prima > 3 memiliki keunikan yang selalu berbentuk antara 6k-1 atau 6k +1. Setiap bilangan hanya memiliki 6 bentuk: 6k - 2,6k - 1,6k, 6k+1 ,6k + 2,6k +3. Tapi perhatikan bahwa 6k -2,6k, 6k +2 selalu genap. Sedangkan 6k +3 adalah kelipatan 3. 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. Hal ini mungkin terkesan sangat jelas tapi tidak semua orang bisa membuktikan pernyataan ini. Berdasarkan sifat bilangan prima maka penilitian ini menggabungkan informasi peranti waktu pada *android* *mobile* menjadi teknik penentuan konstanta *p* dan *q* juga memastikan bilangan prima yang didapat adalah benar prima.

### METODE

Berdasarkan pendahuluan, pembangkitan dan menentukan konstanta *p* dan *q* yangprima maka penelitian menggunakan informasi peranti dapat digambarkan dalam bentuk diagram alir metode penelitian.



Gambar 1. Diagram Alir Metode Penelitian

***Kerangka Konsep Penelitian***

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

 Gambar 3. Kerangka Konsep Penelitian

Bilangan Prima merupakan bilangan bulat positif, sifat pembagiannya [2] melahirkan konsep-konsep aritmetika modulo, dan salah satu konsep bilangan bulat yang digunakan dalam penghitungan komputer. Dengan ditemukannya bilangan prima, teori bilangan berkembang semakin jauh dan lebih mendalam. Banyak dalil dan sifat dikembangkan berdasarkan bilangan prima.

Pada penelitian [3] 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.

### HASIL

Hasil proses tahapan menentukan bilangan prima, mendapatkan informasi peranti, mengolah informasi peranti dan penentuan konstanta p dan q berdasarkan informasi peranti, pengujian dan pembuktian dan analisa hasil menggunakan perangkat *visual* *studio* *code*, *android* *studio*, dan *android* *mobile*.

***Tahapan Menentukan Bilangan Prima***

Tahapan ini memiliki 2 langkah yakni Menentukan Batasan Angka Atas Prima Sampai Jumlah Suatu *Char* dan Membangkitkan Bilangan Prima.

1. Menentukan Batasan Angka Prima Sampai Jumlah Suatu *Char*, Misalnya dari kalimat “Politeknik Negeri Samarinda Tahun 2020” Diuraikan menjadi kode *ASCII* yang diperlihatkan pada Tabel 1.

Tabel 1 Hasil Karakter ke *ASCII*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| *char* | P | o | … | n |
| *ASCII* | 80 | 111 | … | n |

Kemudian dengan persamaan 1.1 didapat totalnya = 3400.

..………….….…(1.1)

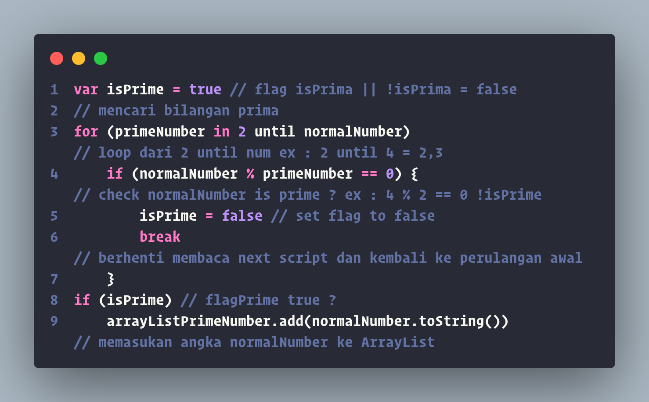
dimana :

Total = Batas Atas Prima

Ui = Nilai Karakter Pada *ASCII*

Matematikawan membuktikan bahwa bilangan prima terbesar itu tidak ada, Pada Juli 2018 bilangan prima ‘terbesar’ ditemukan, yaitu 277.232.917 – 1 yang diketahui [4]. Proses pembatasan prima mengkonsumsi sebuah waktu yang berhubungan dengan tahapan pengolahan informasi peranti jam, menit dan detik.

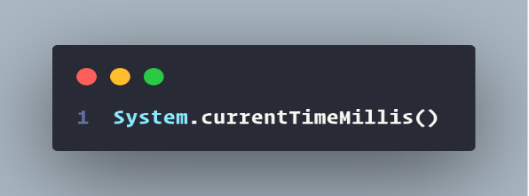
1. Membangkitkan Bilangan Prima dengan mengeliminasi angka bukan prima [5]. misalnya, jika A = 3 dan nilai pembaginya (sisa bagi) B = 2, maka ditandai sebagai prima sebaliknya bukan prima. Hasil rentang 1 sampai 3400 membangkitkan 478 angka prima (jumlah angka yang prima) didefinisikan *arrayListPrimeNumber*.



Gambar 3. Potongan Kode Membangkitkan Bilangan Prima dengan *Naive Solution*

***Tahapan Mendapatkan Informasi Peranti***

Informasi Peranti yang didapatkan memiliki 3 variabe yaitu jam, menit, dan detik. Proses mendapatkannya dibaca oleh peranti *Mobile* *Android* dengan fungsi yang sudah tersedia di kotlin yang diperlihatkan pada Gambar 4.



Gambar 4. Potongan Kode Mendapatkan Informasi Peranti Waktu Sekarang

Data waktu yang didapat masih berupa nilai keseluruhan waktu yang kemudian diformat menjadi (HH:mm:ss) untuk menjadikanya jam, menit dan detik.

Dengan fungsi yang sudah tersedia di kotlin, dapat digunakan *syntax* sebagai berikut :

Maka didapatkan waktu sekarang 06:05:30 dengan zona awal GMT +8 sebagai Informasi Peranti.

***Tahapan Mengolah Informasi Peranti***

Informasi Peranti diolah kembali untuk menghasilkan informasi peranti yang probabilstik berdasarkan waktu jam, menit dan detik menggunakan *Greenwich Mean Time Zone* (GMT) sebagai pengubah.

Seluruh zona waktu telah didefinisikan sebelumnya ke dalam *arrayTime* sebagai zona lain.



Gambar 4 Daftar Waktu Indonesia Tengah

Pemilihan posisi atau *index* untuk *arrayTime* berdasarkan keluaran dari nilai *integer* oleh *sudorandom*, sebagai zona lain.

Dengan fungsi yang sudah tersedia di kotlin, dapat digunakan syntax sebagai berikut :

Maka hasil nilai *sudoRandom* = 22.

Sehingga didapat *arrayTime* [*sudoRandom*]= GMT +12.

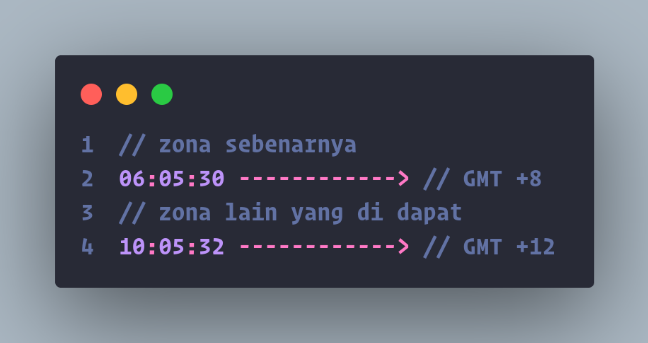
Kemudian dilakukan konversi waktu sekarang 06:05:30 GMT +8 ke GMT +12 yang diperlihatkan pada Gambar 5 dan Gambar 6.

.



Gambar 5. Potongan Kode Konversi Zona Waktu

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



Gambar 5. Hasil Zona Awal dan Zona Lain

***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 5.

Kemudian menentukan *p* dan *q* dimana untuk menghasilkan prima yang deterministik dari informasi peranti yang probabilistik:

* 1. Menentukan Konstanta P yang Prima penentuan ini sederhana, dengan menghitung persamaan 1.1 didapat *indexP* = 20.

(………..….……………(1.1)

Dimana :

hh = informasi peranti waktu jam

n = 2

Maka didapat nilai *p*[*indexP*] = 73.

Jika n memiliki nilai yang lebih besar dari 2 , misal 3 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.

* 1. Menentukan Konstanta Q yang Prima nilai *q* memiliki aturan mirip dengan nilai *p*, tetapi memiliki 5 keputusan perhitungan () dari 6 ketentuanya ().

()…………………..…(2.1)

K1 = *p*

K2 = informasi peranti waktu menit

K3 = informasi peranti waktu detik

K4 = K2 + K3

K5 = K1 \* K2

K6 = K2 \* K3

()…………….……….(2.2)

Dimana :

K[n] = *arrayListPrimeNumber* [n]

jml prima = *arrayListPrimeNumber.size*

Dengan persamaan 2.1 dan 2.2 didapat K[n] = K[31] = *indexQ*.

Maka didapat nilai *q*[*indexQ*] = 131.

Tahapan ini berhasil menentukan dan menghasilkan *p* = 73 dan *q* = 131 sesuai ketentuan yang ditetapkan dan telah diuji pada pengujian primalitas dengan naive solution dan pembuktian kombinasi dengan informasi peranti dengan metode pemilihan.

***Pengujian dan Pembuktian***

Pengujian telah dilakukan terhadap hasil *p* dan *q* dengan *naive* *solution*, selain untuk cek bilangan prima sederhana terhadap *p* dan q*,* juga bisa digunakan sebagai pembangkit bilangan prima.

Diketahui:

*p* = 73

*q* = 131

(*Naive*S*olution*)………………………......(3.1)

Dimana :

n = *p atau q*

Maka dengan persamaan 3.1 didapat hasilnya adalah benar atau *true* untuk *p* dan *q*, Hasilnya diperlihat pada Gambar x. Persamaan 3.1 sama dengan yang diperlihatkan pada Gambar 3.

Pembuktian terhadap persamaan 2.1 dan 2.2 telah dilakukan dengan

NaiveHasilnya kedua konstanta p dan q benar merupakan bilangan prima. Naive solution merupakan hal yang sederhana yang cocok digunakan untuk p dan q yang bernilai

berbagai tahapan metode pemilihan untuk membuktikan pernyataan pembangkitan prima dan kombinasi informasi peranti waktu jam, menit dan detik.

proses pembuktian dilakukan sebagai berikut [1]:

1. Mengumpulkan semua fakta yang ada dari permasalahan.

2. Mengaitkan semua fakta-fakta yang terkumpul dan melihat hal menarik apa yang bisa di dapat. Biasanya dalam proses ini kita cuman mengaitkan satu dua fakta, dan fakta-fakta lain digunakan selanjutnya.

3. Menentukan tujuan. Tentukan apa yang

harus dicapai(syarat cukup untuk mengatakan terbukti), untuk membuktikan nilai kebenaran permasalahan.

4. Pemilihan strategi.

5. Eksekusi.

6.Penarikan kesimpulan.

signifikan kemungkinan terjadi ketika terjadi proses yang berlebihan atau kondisi baca peranti itu sendiri. Pada tahapan selanjutnya dua variabel ini menghasilkan sesuatu yang berbeda. // analisah hasil later will move

Hasil *Greatest Common Divisor* (GCD) = 2, menunjukan waktu pemfaktoran semakin lama [6]. //masuk analisa hasil later edit

*array* – hh).

Ketika Ketentuan (K) tidak terpenuhi mengakibatkan *q* *null* dan melemparkan sebuah *NumberFormatException*, pembangkitan kunci tidak berjalan semestinya saat menit (mm) adalah 0 dan detik (ss) berapa di bawah nilai P. Sehingga ketentuan *null* ditambahkan untuk menghindari hal tersebut dan nilai nya adalah posisi ukuran *array* – hh, seperti ketika menghindari *index out of bound*

***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 X.

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*, rumusnya telah berfungsi untuk setiap bilangan yang dibangkitkan atau ditentukan.

### KESIMPULAN

Penlitian dan percobaan terhadap rancangan dan pengujian yang telah dilakukan menghasilkan kesimpulan sebagai berikut:

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, mempengaruhi data waktu.

melakukan perhitungan dan proses lebih cepat (berbeda). Sehingga data waktu dan perhitungan membuat hasil *p* dan *q* lebih efisien dengan melihat hasil tidak terlalu besar dan rentang dua variabel itu sendiri.

### DAFTAR PUSTAKA

[1] Cahyo Dhea Arokhman Yusufi, *Heuristic - For Mathematical Olympiad Approach*. Jakarta: Math Heuristic, 2020.

[2] F. F. Firmansyah, “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, 2015.

[3] R. H. Sari, “Apakah Integrasi Islam dapat Membudayakan Literasi Matematika ?,” *Semin. Mat. dan Pendidik. Mat. UNY*, hal. 655–662, 2017.

[4] “Untuk Apa Mencari Bilangan Prima Terbesar? - Anak Bertanya.” [Daring]. Tersedia pada: https://anakbertanya.com/untuk-apa-mencari-bilangan-prima-terbesar/. [Diakses: 18-Jun-2020].

[5] A. TH dan B. MB, “The Unique Natural Number Set and Distributed Prime Numbers,” *J. Appl. Comput. Math.*, vol. 06, no. 04, 2017, doi: 10.4172/2168-9679.1000368.

[6] B. S. Muchlis, M. A. Budiman, dan D. Rachmawati, “Teknik Pemecahan Kunci Algoritma Rivest Shamir Adleman (RSA) dengan Metode Kraitchik,” *SinkrOn*, vol. 2, no. 2, hal. 49–64, 2017.