

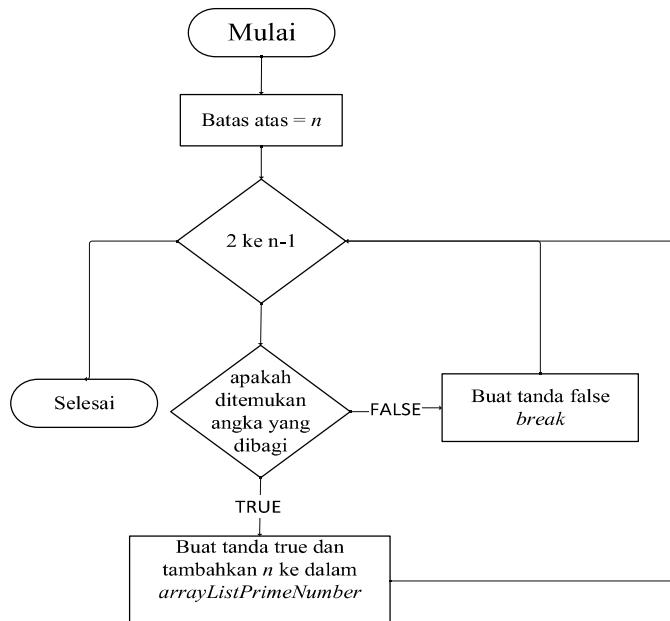
BAB IV

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

<i>arrayListPrimeNumber</i>	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 diatur 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

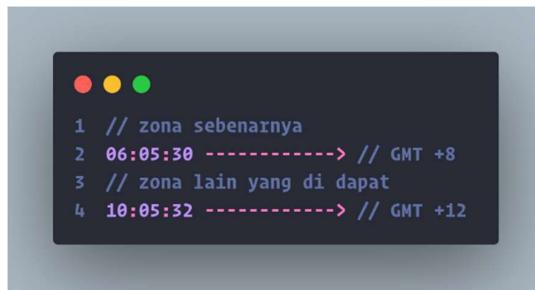
Informasi Peranti diolah kembali untuk menghasilkan informasi peranti yang probabilistik berdasarkan waktu jam, menit dan detik serta menggunakan *Greenwich Mean Time Zone* (GMT) sebagai pengubah Zona Awal ke Zona Lain. Seluruh zona waktu telah didefinisikan sebelumnya ke dalam *arrayTime* sebagai zona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



```

1 // zona sebenarnya
2 06:05:30 -----> // GMT +8
3 // zona lain yang di dapat
4 10:05:32 -----> // GMT +12

```

Gambar 4.3 Hasil Informasi Peranti Waktu

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

4.4 Hasil Tahapan Penentuan Konstanta P dan Q Berdasarkan Informasi Peranti

Berdasarkan 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:

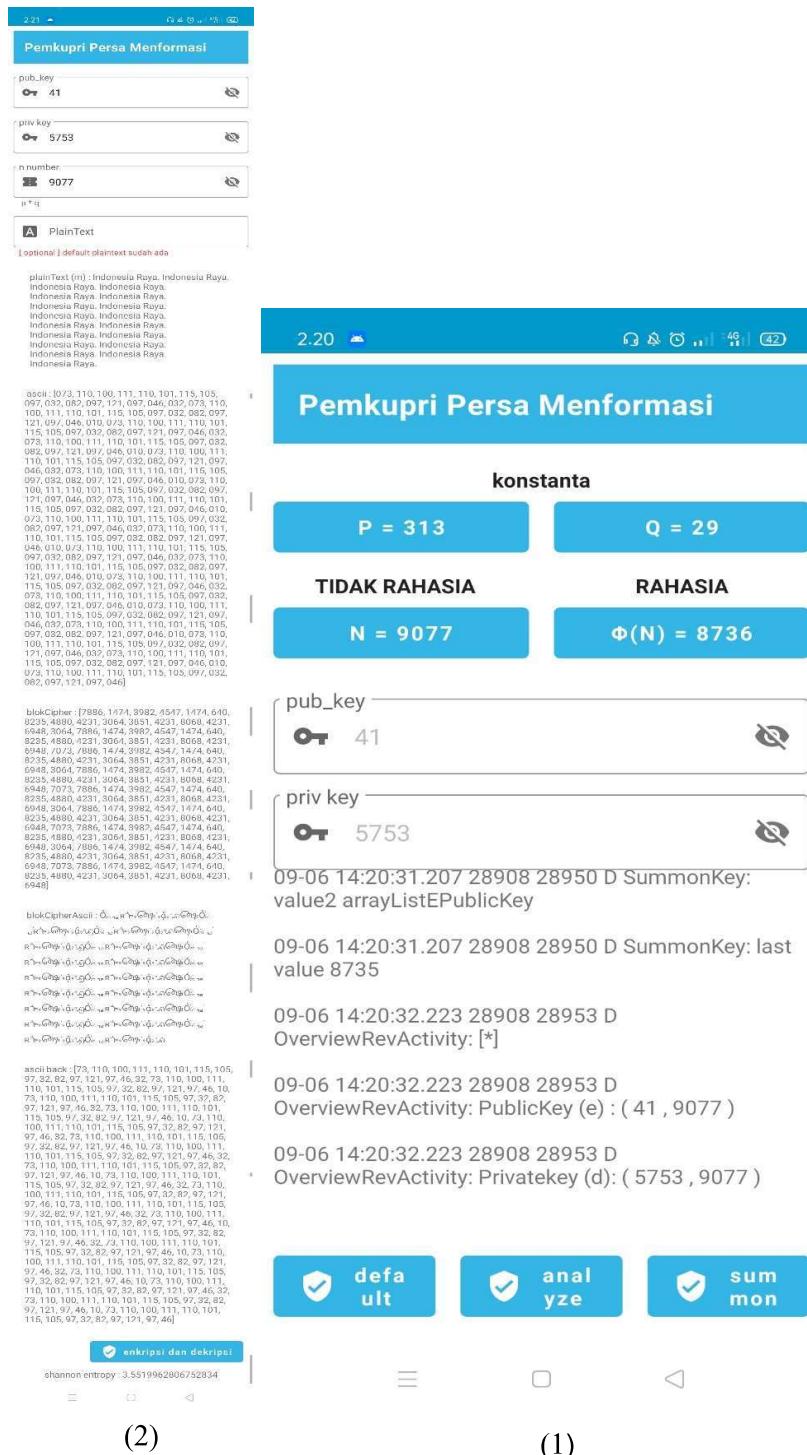
11	17:41:01 GMT +8	15:41:02 GMT+10	20	283	383	239	51383
12	17:46:01 GMT +8	11:46:02 GMT-10	9	197	503	225	20553
rata - rata panjang kunci publik dan privat 2 bit - 17 bit (2 digit - 5 digit)							

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	DATA FROM RSA ENCRYPTION	4.03556914562073

No	Teks Asli	Jumlah Karakter	Hasil Enkripsi	Entropi Enkripsi
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	DATA FROM RSA ENCRYPTION	4.257107430057822

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)				



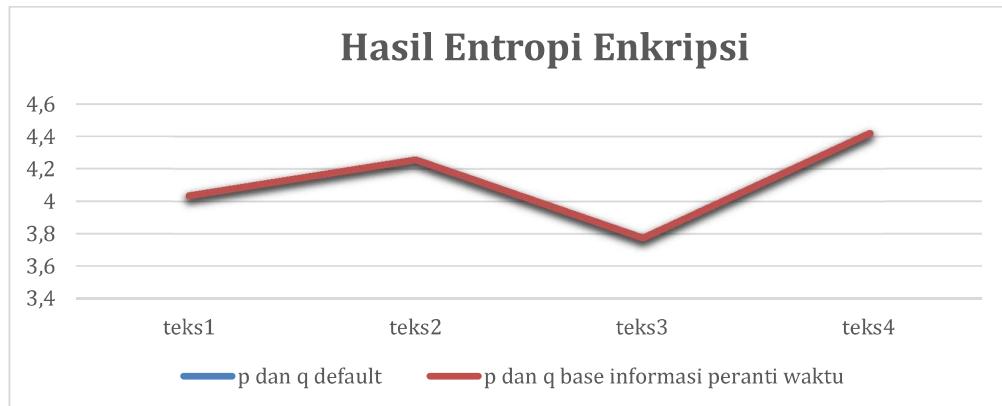
Gambar 4.5 Tampilan Aplikasi Pembangkitan (2) dan Proses Enkripsi Dekripsi

(1)

(2)

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