RABIT : Jurnal Teknologi dan Sistem Informasi Univrab
Volume xx No. xx | Januari xxx : Hal :xx-xx
ISSN CETAK : 2477-2062
ISSN ONLINE : 2502-891X

PEMBANGKITAN KUNCI PRIVAT PADA ENKRIPSI RSA MENGGUNAKAN INFORMASI PERANTI

[1)] Yogi Arif Widodo, [2)] Mulyanto, S.Kom., M.Cs., dan seterusnya [3)] …[4)] ….
[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 $n = p.q$ 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 $p =$ 3.085055102756477, $q =$ 3.7004397181410926, konversi *Greenwich Mean Time Zone* (GMT) = 3.085055102756477, dan ideal acuan data uji adalah 3.7004397181410926. Kesesuaian waktu HH dan hh dipengaruhi oleh *pseudorandom*, mm ketetapanya 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 $c =$ 4.814863028233948 ke 242 kode ASCII dengan $n =$ 192989 menjadikan teks awal (8.083 ms nya adalah ASCII ke c) dan 1 sampai 2 detik untuk pembangkitan hingga kunci privat.

Kata Kunci: Kunci Privat, RSA, Informasi Peranti, GMT, entropi.

ABSTRACT
Rivest Shamir Adleman (RSA) is a modern cryptographic technique that exceeds the patent limit for 20 years, making it easy to read freely. The difficulty of factoring large numbers n = p.q into prime factors, as well as key differences in revealing texts and encoding, makes RSA a difficult technique to solve. The constant numbers or the order p and q become experimental calculations using device information that is 24 time zones with the format HH: mm: ss and hh: mm: ss produces a range of 3000 more at a given time and the second variable GCD is 2. Generating a multiple of 5 in minutes during 1 hour brackets, entropy yields p = 3.085055102756477, q = 3.7004397181410926, Greenwich Mean Time Zone (GMT) conversion = 3.085055102756477, and the ideal reference test data is 3.7004397181410926. The suitability of HH and HH times is influenced by pseudorandom, mm constant constant and ss is the process. The application of the RSA private key succeeded in decrypting the cipher block (c) to the American Standard Code for Information Interchange (ASCII) instead of single character or null with encoding (UTF-8) and the duration of the process depends primarily on the p and q values generated by the provisions, then the device's read speed condition. GMT results are influenced by the upper limit limiting process. It takes about 239,797 miliseconds (ms) for entropy c = 4.814863028233948 to 242 ASCII code with n = 192989 making the initial text (8083 ms is ASCII to c) and 1 to 2 seconds for generation to private key.

Keyword: *Private Key, RSA, Device Information, GMT, entropy.*

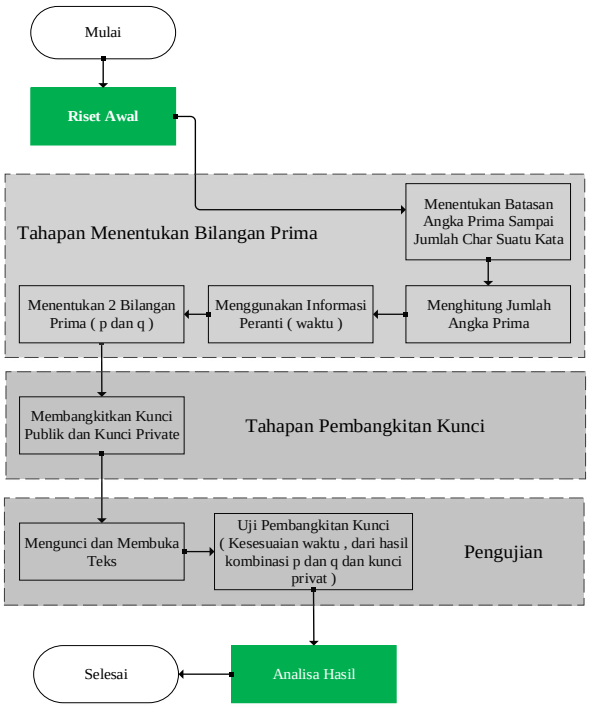
PENDAHULUAN

"Teknik Pemecahan Kunci Algoritma *Rivest Shamir Adleman* (RSA) dengan Metode *Kraitchick*". Penelitian tersebut menjadi kreativitas dalam meneliti bilangan konstanta atau orde p dan q, kesimpulan menghasilkan tentang efisiensi waktu pemfaktoran, selisih $p - q$ maupun faktor $(p-1), (q-1)$, dan panjang kunci [1]. Tentu menimbulkan pertanyaan "keamanan sudah kuat, kenapa dimodifikasi lagi?" banyak sudah penelitian yang membahasnya, bisa dilihat menggunakan *dorking google* dengan kata kunci "*intext:'journal rsa" filetype:pdf site:ac.id*" hasilnya sekitar 5000 journal. Dengan begitu konsep RSA mulai dikenal,

digunakan, dan terbongkar [2]. Nilai *p* dan *q* hanya sering dikenal atau digunakan dalam pembangunan kunci publik dan kunci privat. Berdasarkan penelitian tadi, dapat diketahui bahwa nilai *p* dan *q* berperan penting dalam tingkat keamanan enkripsi algoritma RSA. Ketika hak otorisasi dijatuhkan dalam informasi tertentu, memberikan pola yang merangkai konsep, Seperti waktu terus berjalan mengikuti masa sekarang, tentu memiliki aspek krusial terhadap kombinasi angka atau bilangan yang dilakukan *simple* acak informasi ataupun posisinya. Waktu merupakan sebuah informasi dengan konsep angka yang terus berjalan dan selalu berubah. Pada masa kini, informasi ini dapat dengan mudah di dapatkan dari perangkat peranti telepon genggam atau komputer.

METODE

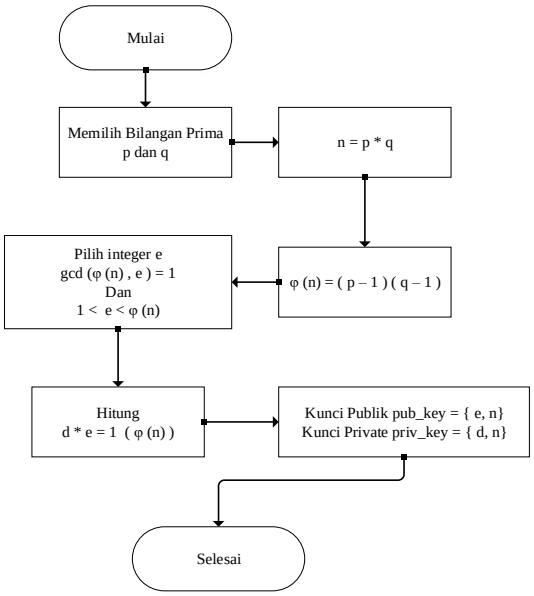
Metode yang digunakan yaitu Kriptografi Rivest Shamir Adleman (RSA).



Gambar 1. Diagram Alir Metode Penelitian

Algoritma RSA sangat bergantung pada dua variabel p dan q dimana variable ini di gunakan untuk membangkitkan kunci asimetris [3].

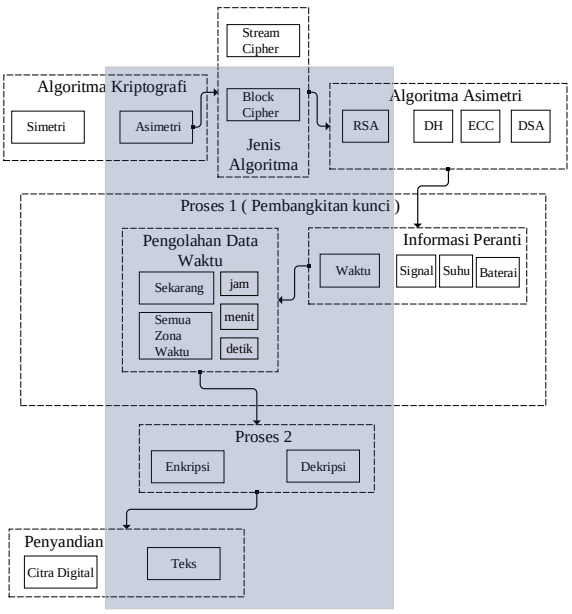
Pembangkitan kunci RSA diperlihatkan pada Gambar 2 [2].



Gambar 2. *FlowChart* Poses Pembangkitan Kunci RSA

Kerangka Konsep Penelitian

Kerangka konsep penelitian (teori atau konsep ilmiah yang digunakan sebagai dasar penelitian) menjelaskan hubungan atau gabungan atau modifikasi proses pembangkitan kunci RSA sebagai ruang lingkup penelitian dan ruang lingkup ilmu pengetahuan.



Gambar 3. Kerangka Konsep Penelitian

HASIL

Hasil proses tahapan menentukan bilangan prima, pembangkitan kunci, pengujian, dan analisa hasil menggunakan perangkat visual studio code, android studio, dan android mobile. Pengujian akhir dilakukan optimasi program, proses pembangkitan kunci privat 2x lebih cepat, P dan Q menjadikan fungsi delay menjadi acuan informasi peranti waktu dan zona waktu diproses tertentu dan bervariasi oleh kondisi perangkat saat pembangkitan.

Tahapan Menentukan Bilangan Prima

American Standard Code for Information Interchange (ASCII) digunakan dalam masukan batasan. Sebagai contoh, kalimat 'Politeknik Negeri Samarinda Tahun 2020', setiap elemen atau karakter diubah menjadi *integer*, kemudian dijumlah secara *default* yaitu *ascending*, sehingga dihasilkan batas atas bernilai 3400. Terdapat 5 proses untuk nilai *p* dan *q*:

a. Menentukan Batasan Angka Prima Sampai Jumlah Suatu *Char* Suatu Kata, sekitar 1 - 6.606 milidetik, waktu yang dibutuhkan.
b. Menghitung Jumlah Angka Prima dengan mengeliminasi angka bukan prima yaitu proses menghasilkan bukan nol adalah benar dan sebaliknya adalah salah. Perhitungan rumus menggunakan sisa bagi, jika A = 3 dan nilai pembaginya (sisa bagi) B = 2, maka ditandai sebagai benar. Waktu sekarang adalah 14:05:30 GMT+8 dan hasilnya 478 prima.
c. Menggunakan Informasi Peranti (Waktu), Greenwich Mean Time Zone (GMT) secara *default* menyesuaikan waktu peranti dan hasil menentukan bilangan prima menggunakan Waktu Indonesia Tengah (WITA) dalam format 24 jam (HH:mm:ss) dan diganti menjadi format 12 jam (hh:mm:ss) setelah *pseudorandom* dijalankan. Seluruh zona waktu disimpan ke dalam *array string* yang telah disusun secara *ascending* dari minus (-) ke plus (+) dengan format *Extensible Markup Language* (XML).

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

Gambar 4 Daftar Waktu Indonesia Tengah

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

$$val\ stateZoneTime = (listZoneTime.indices).random()$$

Pemilihan posisi berdasarkan keluaran dari nilai *integer* RNG, sehingga waktu sekarang adalah 10:05:31 GMT + 12 dengan hasil nilai RNG adalah 22**.**

d. Menentukan 2 Bilangan Prima (p dan q), Nilai *p* dihasilkan dengan menghitung jam (hh) x 2 = 20 sebagai letak (posisi memilih) bilangan prima dalam daftar *array*, angka 2 merupakan bilangan sedemikian rupa untuk menghindari $p < 10$ sehingga nilai $p = 73$. Nilai *q* memiliki aturan mirip dengan nilai *p*, tetapi memiliki 5 keputusan perhitungan dari 6 ketentuanya (K), yaitu:
   0. K1 merupakan posisi (*p*)
   1. K2 adalah menit (mm)
   2. K3 adalah detik (ss)
   3. K4 adalah K2 + K3 (mm + ss)
   4. K5 adalah K1 * K2 (*p* * mm)
   5. K6 adalah K2 * K3 (mm * ss)

Keputusanya adalah ketika K1 < K (2 sampai 6), K1 ! = K (2 sampai 6). K[*null*] berisi ukuran prima – K1, Hasilnya adalah keputusan ke 3, yaitu K3 dengan nilai 31 menghasilkan nilai *q* = 131. Hasil *Greatest Common Divisor* (GCD) adalah 2, menunjukan waktu pemfaktoran semakin lama [1].

Hasil Tahapan Pembangkitan Kunci

Fokus kombinasi informasi peranti untuk p dan q adalah penerapan kunci privat sebagai dekripsi teks yang dirancang oleh kunci publik sebagai acuan uji hasil. Sehingga hasilnya adalah sebuah kombinasi informasi peranti waktu untuk p dan q, menghasilkan kunci publik mengunci teks hingga privat mampu membuka teks enkripsi standar yaitu entropi 4 – 5 bukan ideal *encrypted* 7,99902 (≈8) [4], yang difokuskan pada kunci privat dalam hal ini dekripsi

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

Nilai N atau $p * q = 9563$ di definisikan menjadi rentang 1 sampai d, dimana $e * d = 1\ mod\ \varphi(n)$ 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, yang diperlihatkan pada Gambar 5.

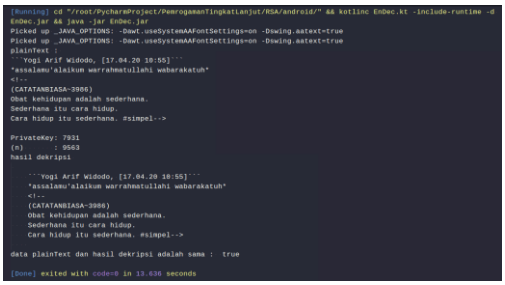
Gambar 5 Hasil Pembangkitan Kunci

Pengujian

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

a. Mengunci dan Membuka Teks, Pengujian pertama, panjang kunci 2 *bit* sampai 14 *bit*, mengenkripsi m dan mendekripsi blok *cipherText* (c), memperhitungkan *Greatest Common Divisior* (GCD) dan entropi (m dan c) dalam bentuk *binary large object* (BLOB) atau semua data dalam bentuk *binary*. Hasil enkripsi didefinisikan dalam variabel c[i] dimana i adalah proses ke (dari pembangkitan ke- (*p*-[i])). Ukuran probabilitas c[i] memiliki kesamaan dengan kode ASCII yaitu sebanyak 58 terhadap seluruh data, yang diperlihatkan pada Tabel 1, 1.2 dan 1.3.

Masing-masing dekripsi pesan diuji dengan kunci yang sesuai untuk m berupa elemen panjang dan isinya menghasilkan kondisi *true* yang diperlihatkan pada Gambar 6.



Gambar 6 Hasil Pengujian Pertama Dekripsi *PlainText*

b. Pengujian kedua menghindari sebuah *bug* atau *crash* atau berupa *exception* posisi yaitu aritmatika waktu yang mengakibatkan *index out of bound* terhadap posisi *q* yang diperlihatkan pada Tabel 2.

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

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*.

Tabel 1 Hasil Pengujian Pertama Enkripsi dan Dekripsi

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

Tabel 1.1 Hasil Kode ASCII *PlainText*

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

Tabel 1.2 Hasil Probabilitas *Binary ChiperText*

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

Tabel 2 Hasil Pengujian Kedua Pada orde P dan Q

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

11:30:04 GMT +8	7	11:30:05 GMT +8	18	197	2221	4
11:35:04 GMT +8	8	03:35:05 GMT +4	14	41	151	10
11:40:05 GMT +8	9	08:40:06 GMT +11	21	137	179	2
11:45:10 GMT +8	10	03:45:12 GMT +4	14	41	199	2
11:50:05 GMT +8	11	08:50:06 GMT +11	21	137	233	8
11:55:04 GMT +8	12	01:55:04 GMT +6	16	11	263	2
12:00:04 GMT +8	13	04:00:05 GMT +4	14	59	3271	2
Entropi Seluruh Nilai *p*						3.085055102756477
Entropi Seluruh Nilai *q*						3.7004397181410926

c. Uji Pembangkitan Kunci

Uji Pembangkitan kunci dilakukan untuk melihat kunci privat yang dibangkitkan oleh *p* dan *q* memiliki ciri waktu sesuai yaitu HH:mm:ss terhadap hh:mm:ss masing-masing konstanta atau berbeda, perubahan zona waktu dipengaruhi secara probabilistik oleh *pseudorandom*. Dengan mencocokan entropi (tingkat data acak/kompresi/*encrypted*). Dapat dilihat rumus entropi sebagai berikut

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

Tabel 3 Uji Pembangkitan Kunci pada Hasil Pengujian Pertama Enkripsi dan Dekripsi

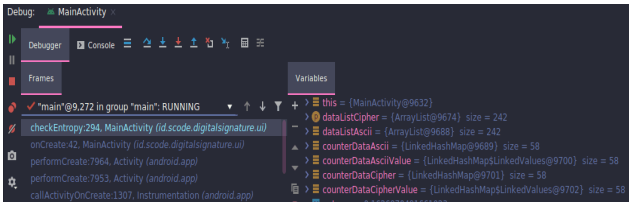
Rentang Waktu Awal Proses (RWAP) (HH : mm)	02:05:31 GMT +8	13:57:08 GMT +8	14:49:07 GMT +8	14:54:10 GMT +8	14:59:09 GMT +8
PEMBANGKITAN KE -	1	2	3	4	5
Rentang Waktu Setelah Proses Awal (RWSPA) (hh : mm)	10:05:32 GMT + 12	14:57:09 GMT + 9	11:49:08 GMT + 5	09:54:11 GMT + 3	05:59:10 GMT - 1
P	73	47	83	67	31
Q	131	271	197	197	197
Entropi RWAP	2.2516291673878226				
Entropi RWSPA	2.2516291673878226				

Uji awal memiliki acuan bervariasi HH untuk hh, mm konstanta, ss adalah proses pembangkitan dan diuji kembali pada tahap kedua, yang memiliki acuan konstanta HH, yaitu 2.2516291673878226 dan menghasilkan persis oleh ciri waktu yang berbeda untuk masing-masing data maupun keseluruhan.

Analisa Hasil

Analisa hasil *p* dan *q*, dipilih berdasarkan nilai posisi secara acak (*pseudorandom*) serta waktu awal proses (HH:mm:ss) sampai perhitungan batas atas prima (hh:mm:ss) sehingga membuat *p* dan *q* lebih tidak terduga dengan adanya 24 macam atau jenis *Greenwich Mean Time Zone* (GMT). Analisa memiliki 2 hasil yang saling berhubungan. Dari 5 data menghasilkan nilai entropi P = 2.321928094887362 (semua daftar bilangan adalah berbeda) dan *q* = 1.370950594454668 (3 dari 5 bilangan adalah persis). Hasil *Greatest Common Divisor* (GCD) konstanta di angka 2. Variabel tersebut

melakukan perhitungan algoritma *Rivest Shamir Adleman* (RSA) menghasilkan enkripsi berupa blok cipher (c) bernilai entropi 4.814863028233948 dari kode ASCII sepanjang 242 yang juga bernilai sama dengan hasil entropi c. Daftar *binary* antara c dan ASCII memiliki probabilitas berjumlah 58 diperlihatkan pada Gambar 7.



Gambar 7 Analisa Hasil Probabilitas ASCII dan *CipherText*

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

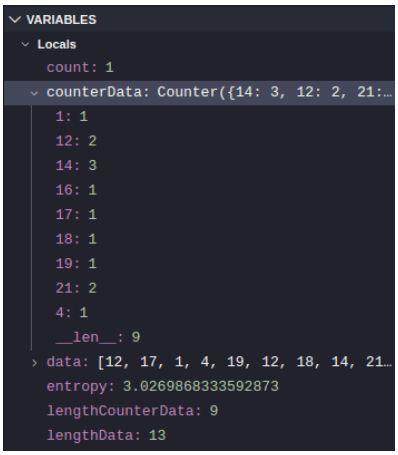
Tabel 4 Analisa Hasil Jarak Rentang Nilai P dan Q

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

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

Pseudorandom Random Number Generate (PRNG) penentuan posisi zona waktu menghasilkan entropi 3.085055102756477 dari 13 data PRNG setiap 5 menit dalam kurung waktu 1 jam mendekati hasil nilai entropi 3.7004397181410926 sebagai acuan dari 13 data waktu jika seluruhnya adalah acak untuk mengetahu :

1. tingkat keberagaman suatu kumpulan data semakin besar [5]
2. merepresentasikan jumlah informasi yang terkandung di dalam [6].



Gambar 8 Analisa Hasil Entropi PRNG Zona Waktu Dalam 5 Menit

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, mampu melakukan perhitungan dan proses lebih cepat (berbeda). Sehingga data waktu dan perhitungan membuat hasil *p* dan *q* lebih efisien dengan melihat hasil GCD $(p-1, q-1)$ tidak terlalu besar dan rentang dua variabel itu sendiri.

Pengujian pertama dengan panjang kunci 2 *bit* sampai 14 *bit*, keduanya telah membangkitkan kunci privat yang mampu

mendekripsi kode ASCII. Entropi Blok *CipherText* 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.

Pengujian kedua dengan menaikan pemilihan *p* adalah hh * 4 dan ditambahkanya ketentuan *q* adalah batas prima dikurang posisi *p*, menghasilkan *p* dan *q* yang memiliki kemungkinan rentang cukup jauh pada saat menit dan detik kecil antara 0 – 20 dan posisi *p* adalah puluhan atau lebih besar dari mm:ss. Kedua variabel menghasilkan GCD rata-rata adalah 2.

DAFTAR PUSTAKA

[1] 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.

[2] S. Nisha dan M. Farik, "RSA Public Key Cryptography Algorithm A Review," *Int. J. Sci. Technol. Res.*, vol. 06, no. 07, hal. 187–191, 2017.

[3] M. A. Zainuddin dan D. I. Mulyana, "Penerapan Algoritma Rsa Untuk Keamanan Pesan Instan Pada Perangkat Android," *J. CKI SPOT*, vol. 9, no. 2, hal. 105–114, 2016.

[4] P. Irfan dan Y. Prayudi, "Penggabungan Algoritma Chaos dan Rivers Shamir Adleman (RSA) Untuk Peningkatan Keamanan Citra," *SNATI (Seminar Nas. Apl. Teknol. Informasi)*, hal. D5, 2015.

[5] E. J. Kusuma, C. A. Sari, E. H. Rachmawanto, dan D. R. I. M. Setiadi, "A combination of inverted LSB, RSA, and arnold transformation to get secure and imperceptible image steganography," *J. ICT Res. Appl.*, vol. 12, no. 2, hal. 103–122, 2018, doi: 10.5614/itbj.ict.res.appl.2018.12.2.1.

[6] A. B. W. P dan E. Subkhiana, "Ekstraksi Ciri Entropy Untuk Pengenalan Pola Wajah Menggunakan Fuzzy Rule Base," vol. 2, no. 2, hal. 35–42, 2016.