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

(maksimal 15 Kata, Memberi Gambaran Penelitian Yang Telah Dilakukan, Huruf Kapital, Times New Roman, Font 12, Spasi 1, Bold)

[1)] Yogi Arif Widodo, [2)] Penulis Kedua, dan seterusnya [3)] …[4)] ….
(Times New Roman, Font 11, Bold, spasi 1, Nomor Urut Penulis)
[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…*
(Times New Roman, Font 10,spasi 1, nomor urut email)

ABSTRAK (Times New Roman 10, spasi 1, dibuat dalam dua bahasa indonesia)
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. Dengan begitu konsep RSA mulai dikenal, digunakan, dan terbongkar. Bilangan konstanta atau orde p dan q menjadi eksperimen perhitungan menggunakan informasi peranti yaitu 24 zona waktu secara *pseudorandom* 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. 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 mili detik (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 *(*Times New Roman 10, spasi 1, dibuat dalam bahasa inggris *tulisan cetak miring / italic)*
Rivest Shamir Adleman (RSA) is a modern cryptographic technique that exceeds patent limits 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. That way the concept of RSA began to be known, used, and uncovered. Constant numbers or order p and q become experimental calculations using device information that is 24 time zones in pseudorandom 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 tempo multiples of 5 in minutes for 1 hour brackets, entropy p = 3.085055102756477, q = 3.7004397181410926, Greenwich Mean Time Zone (GMT) conversion = 3.085055102756477, and the ideal test data reference is 3.7004397181410926. The application of the RSA private key successfully decrypts 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. It takes about 239,797 milliseconds (ms) for entropy c = 4.814863028233948 to 242 ASCII codes with n = 192989 making the initial text (where 8083 ms is ASCII to c) and 1 to 2 seconds for generation to private key.

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

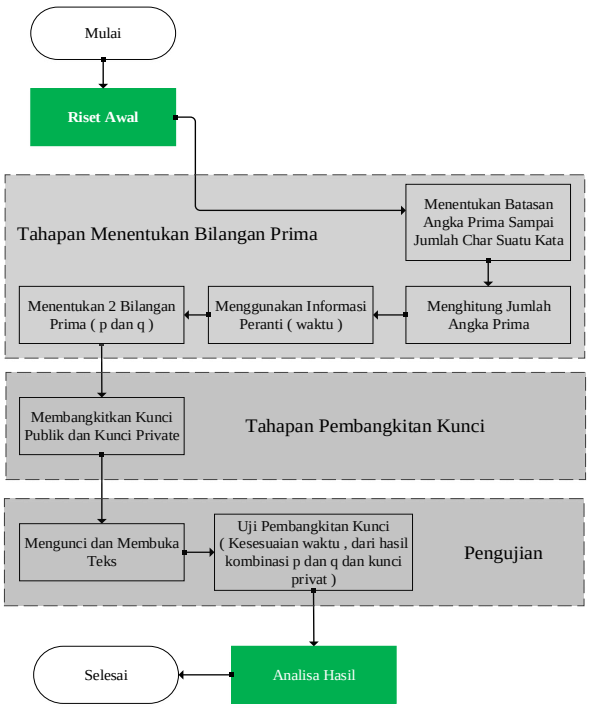
PENDAHULUAN

"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

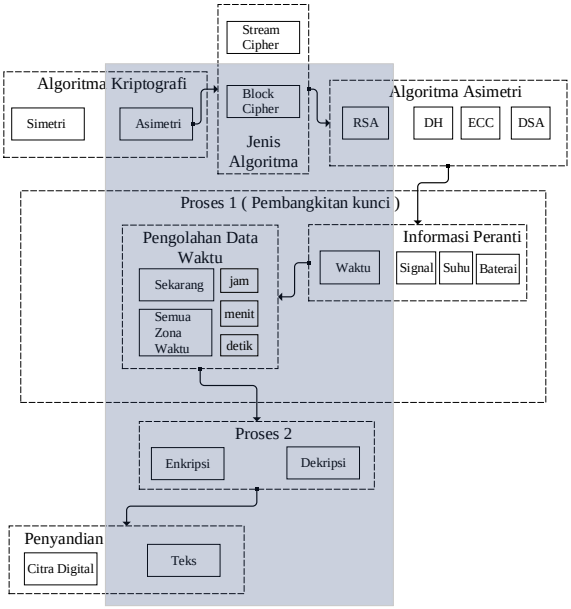
Metode yang digunakan yaitu Kriptografi Rivest Shamir Adleman (RSA).



Gambar 1. Diagram Alir Metode Penelitian

Kerangka Konsep Penelitian

Kerangka konsep penelitian (teori atau konsep ilmiah yang digunakan sebagai dasar penelitian) menjelaskan hubungan antara ruang lingkup penelitian dan ruang lingkup ilmu pengetahuan.



Gambar 2. Kerangka Konsep Penelitian

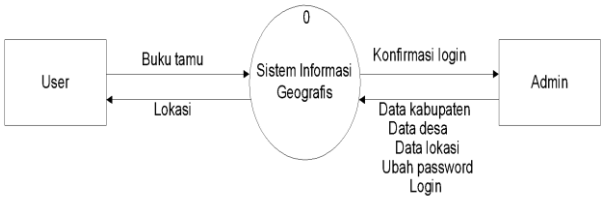
HASIL

Hasil proses tahapan menentukan bilangan prima, pembangkitan kunci, pengujian, dan analisa hasil menggunakan perangkat visual studio code, android studio, dan peranti android.

Perancangan Proses

Diagram konteks memberikan gambaran seluruh elemen sistem. Terdapat dua entitas luar yaitu :

a. *user*, sebagai pengguna sistem dan dapat melihat info peta keramba. Pada *user* terdapat beberapa aliran data, yaitu data lokasi dan data buku tamu.
b. Admin sebagai pengolah sistem, pada admin terdapat aliran data yaitu, data login, data lokasi, data desa dan data kabupaten

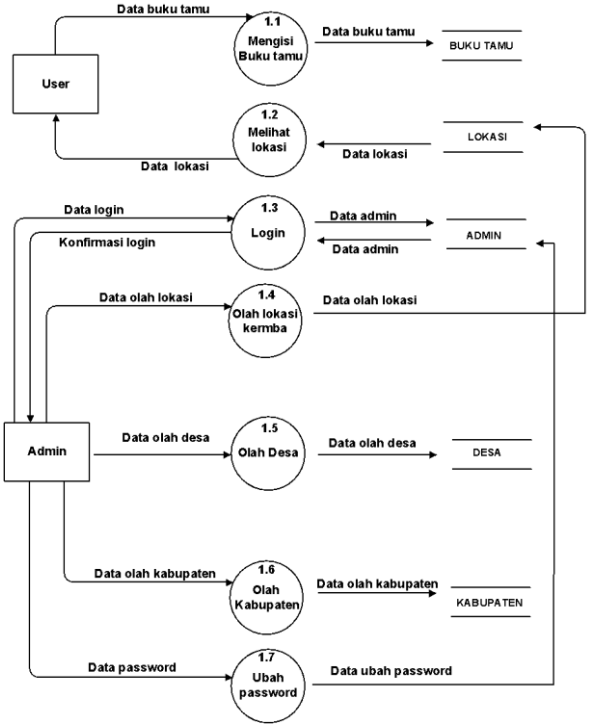


Gambar 2. Diagram Konteks

Gambar 3. DFD Level 1

DFD Level 1

Pada proses sistem informasi geografis keramba ikan berbasis web ini, terdiri dari 2 proses untuk *user* yaitu, buku tamu dan peta keramba dan 6 proses untuk admin yaitu, login, olah peta keramba, olah kecamatan, olah desa dan ubah *password*. Dapat dilihat pada gambar 3.



Implementasi

Tabel 1. Tabel Pengolahan Data

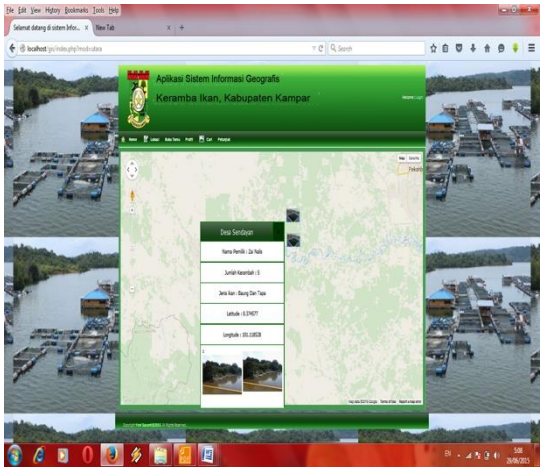
No	Koordiat	Lokasi	alamat	ket
1				
2				
3				
4				
5				
6				
7				
8				
9				
10				

Ikuti bentuk dan penamaan tabel seperti di atas, tabel tanpa garis vertikal, jika tabel terlalu banyak kolom maka boleh menggunakan margin 1 kolom saja untuk tabel tersebut seperti contoh table 2 dibawah ini

Tabel 2. Pengolahan Data

No	NIM	Nama	Alamat	Ttgl	Umur	semeter	sks	Nama	Alamat

Untuk gambar jangan memasukkan gambar dengan resolusi yang terlalu tinggi, gunakan resolusi yang rendah namun gambar tetap terlihat jelas dan dapat di baca,



Gambar 4. Halaman Lokasi

KESIMPULAN

Penlitian dan percobaan 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 (Menggunakan Mendeley atau sejenisnya dengan style **IEEE**,*)*

[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.

DVD

[1] Holm, Narator, dan J. Fullerton-Smith, Produser, How to Build a Human [DVD]. London: BBC; 2002.

Rekaman Suara

[2] D. Fisher, Penulis, dan T. Baker, Presenter, Doctor Who dan the Creature From the Pit [Perekaman suara]. Bath, Inggris: Buku Audio BBC, 2009.

Rekaman video

[3] Rogers, Penulis dan Direktur, Grrls di TI [Videorecording]. Bendigo, Vic. : Video Education Australasia, 1999.

Video YouTube / Vimeo

[4] RK. "Meja bantuan Abad Pertengahan dengan terjemahan bahasa Inggris," YouTube, 26 Februari 2007 [File video]. Tersedia: http://www.youtube.com/watch?v=pQHX-SjgQvQ. [Diakses: 28 Januari 2014].

Bab atau Artikel dalam Buku yang Diedit

[5] Rezi dan M. Allam, "Teknik dalam pemrosesan array melalui transformasi," dalam Sistem Kontrol dan Dinamis, Vol. 69, Sistem Multidemsional, C. T. Leondes, Ed. San Diego: Academic Press, 1995, hlm. 133-180.

Buku: Penulis Tunggal

[6] W.-K. Chen, Jaringan Linear dan Sistem. Belmont, CA: Wadsworth, 1993, hlm. 123-135

Buku: Dua atau Lebih Penulis

[7] U. J. Gelinas, Jr., S. G. Sutton, dan J. Fedorowicz, Proses Bisnis dan Teknologi Informasi. Cincinnati: Pembelajaran Barat Daya / Thomson, 2004.

Buku: Organisasi sebagai Penulis

[8] Bank Dunia, Teknologi Informasi dan Komunikasi: Strategi kelompok Bank Dunia. Washington, DC: Bank Dunia, 2002.

Buku: Instansi Pemerintah sebagai Penulis

[9] Australia. Departemen Kejaksaan Agung, Tinjauan Agenda Digital, 4 Vol. Canberra: Departemen Kejaksaan Agung, 2003.

Buku: Tidak Ada Pengarang

[10] Kamus Oxford untuk Komputer, edisi ke-5. Oxford: Oxford University Press, 2003.

Buku: Editor

[11] D. Sarunyagate, Ed., Laser. New York: McGraw-Hill, 1996.

Buku: Edisi Berbeda

[12] K. Schwalbe, Manajemen Proyek Teknologi Informasi, edisi ke-3. Boston: Teknologi Kursus, 2004.

Laporan Ilmiah / Teknis

[13] K. E. Elliott dan C.M. Greene, "Protokol adaptif lokal," Argonne National Laboratory, Argonne, Prancis, Tech. Rep. 916-1010-BB, 1997.

Makalah Konferensi dalam Cetak

[14] L. Liu dan H. Miao, "Pendekatan berbasis spesifikasi untuk menguji atribut polimorfik," dalam Metode Formal dan Rekayasa Perangkat Lunak: Proc. dari Int 6. Conf. tentang Metode Teknik Formal, ICFEM 2004, Seattle, WA, USA, 8-12 November 2004, J. Davies, W. Schulte, M. Barnett, Eds. Berlin: Springer, 2004. hlm. 306-19.

Makalah Konferensi dari Internet

[15] J. Lach, "SBFS: Sistem file berbasis steganografi," di Proc. dari Int 1 2008. Conf. pada Teknologi Informasi, IT 2008, 19-21 Mei 2008, Gdansk, Polandia [Online]. Tersedia: IEEE Xplore, http://www.ieee.org. [Diakses: 10 September 2010].

Prosiding Konferensi

[16] TJ van Weert dan RK Munro, Eds., Informatika dan Masyarakat Digital: Masalah sosial, etika dan kognitif: IFIP TC3 / WG3.1 & 3.2. Buka Konflik tentang Masalah Sosial, Etis dan Kognitif dari Informatika dan TIK, 22-26 Juli 2002, Dortmund, Jerman. Boston: Kluwer Academic, 2003.

E-book

[17] L. Bass, P. Clements, dan R. Kazman, Arsitektur Perangkat Lunak dalam Praktek, edisi ke-2. Reading, MA: Addison Wesley, 2003. [Online] Tersedia: Safari e-book.

Bab dari buku elektronik

[18] D. Kawecki, "Persiapan bahan bakar," dalam Masalah Teknik Pembakaran untuk Sistem Bahan Bakar Padat, B.G. Miller dan D. Tillman, Eds. Boston, MA: Academic Press, 2008, 199-240. [Online] Tersedia: Referex.

Artikel dari Ensiklopedia Elektronik

[19] G. S. Thompson dan M. P. Harmer, "komposit keramik berskala nano," dalam Ensiklopedia Bahan: Sains dan Teknologi, K. H. J. Buschow, R. W. Cahn, M. C. Flemings, B. Ilschner, E.J. Kramer, S. Mahajan, dan P. Veyssière, Eds. Amsterdam: Elsevier, 2001, hlm. 5927-5930. [On line]. Tersedia: ScienceDirect.

Artikel Jurnal dari Database Teks Lengkap

[20] H. Ayasso dan A. Mohammad-Djafari, "Pemulihan dan Penggabungan Gambar NDT Bersama Menggunakan Gauss-Markov-Potts Model Sebelumnya dan Komputasi Bayesian Variasi," Transaksi IEEE tentang Pengolahan Gambar, vol. 19, tidak. 9, hlm. 2265-77, 2010. [Online]. Tersedia: IEEE Xplore, http://www.ieee.org. [Diakses 10 September 2010].

Artikel Jurnal dari Internet

[21] P. H. C. Eilers dan J. J. Goeman, "Meningkatkan scatterplots dengan kepadatan yang dihaluskan," Bioinformatika, vol. 20, tidak. 5, hlm. 623-628, Maret 2004. [Online]. Tersedia: www.oxfordjournals.org. [Diakses 18 September 2004].

Dokumen Elektronik

[22] Lembaga Standar Telekomunikasi Eropa, “Penyiaran Video Digital (DVB): Pedoman pelaksanaan untuk layanan terestrial DVB; aspek transmisi, ”Lembaga Standar Telekomunikasi Eropa, ETSI TR-101-190, 1997. [Online]. Tersedia: http://www.etsi.org. [Diakses: 17 Agustus 1998].

Publikasi Pemerintah

[23] Australia. Departemen Pendidikan, Ketenagakerjaan dan Hubungan Tempat Kerja, Survei tentang Perubahan Kesadaran dan Pemahaman Sains, Teknik dan Teknologi: Laporan temuan. Canberra: Departemen; 2008. [Online]. Tersedia: http://www.dest.gov.au/NR/rdonlyres/241263CF-8585-4EEC-B104-C947C6C18029/23713/SurveyonChangesinawarenessunderstandingofSET.pdf. [Diakses: 7 September 2010].

Seluruh Situs Internet

[24] J. Geralds, "Sega Mengakhiri Produksi Dreamcast," vnunet.com, para. 2, 31 Januari 2001. [Online].

Tersedia: http://nl1.vnunet.com/news/1116995. [Diakses: 12 September 2004].

Artikel Jurnal di Cetak: Judul disingkat

[25] G. Liu, K. Y. Lee, dan H. F. Jordan, "TDM dan TWDM de Bruijn jaringan dan shufflenet untuk komunikasi optik," IEEE Trans. Comp., Vol. 46, hlm. 695-701, Juni 1997.

Artikel Jurnal di Cetak: Judul lengkap

[26] J. R. Beveridge dan E. M. Riseman, "Seberapa mudah mencocokkan model garis 2D menggunakan pencarian lokal?" Transaksi IEEE pada Analisis Pola dan Kecerdasan Mesin, vol. 19, hlm. 564-579, Juni 1997.

Tesis yang tidak diterbitkan

[27] M. W. Dixon, "Penerapan jaringan saraf untuk menyelesaikan masalah perutean di jaringan komunikasi," Ph.D. disertasi, Murdoch Univ., Murdoch, WA, Australia, 1999.

Tesis yang Diterbitkan

[28] M. Lehmann, Akses Data dalam Sistem Manajemen Workflow. Berlin: Aka, 2006.

Tesis dari Database Teks Lengkap

[29] F. Sudweeks, Pengembangan dan Kepemimpinan dalam Kelompok Kolaborasi yang Dimediasi Komputer. PhD [Disertasi]. Murdoch, WA: Murdoch Univ., 2007. [Online]. Tersedia: Program Tesis Digital Australasia

*Hapus tulisan ini dan semua tulisan yang berwana abu-abu/*gray*