RSA ENCRYPTION BASED ON RSA-ELGAMAL KEY GENERATION FOR ASCII TEXT DATA

Diajukan Sebagai Syarat Untuk Menyelesaikan
Pendidikan Program Strata-1 Pada
Jurusan Teknik Informatika

Oleh :

Ricardo
NIM : 09021281419132

Jurusan Teknik Informatika
FAKULTAS ILMU KOMPUTER UNIVERSITAS SRIWIJAYA
2019

LEMBAR PENGESAHAN TUGAS AKHIR

RSA Encryption Based on RSA-ElGamal Key Generation for ASCII Text Data

Oleh :

RICARDO
NIM : 09021281419132

Palembang,

Pembimbing I,	Pembimbing II,
Drs. Megah Mulya, M.T	Alfarissi, M.Comp.Sc
NIP. 196602202006041001	NIP. 198512152014041001

Mengetahui,
Ketua Jurusan Teknik Informatika

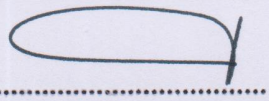
Rifkie Primartha, M.T
NIP. 197706012009121004

TANDA LULUS UJIAN SIDANG TUGAS AKHIR

Pada hari Selasa, 23 Juli 2019 telah dilaksanakan ujian sidang tugas akhir oleh Jurusan Teknik Informatika Fakultas Ilmu Komputer Universitas Sriwijaya.

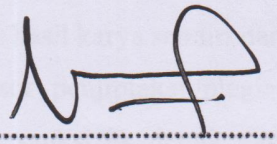
Nama : Ricardo
NIM : 09021281419132
Judul : RSA Encryption Based on RSA-ElGamal Key Generation for ASCII Text Data

1. Pembimbing I



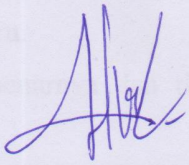
Drs. Megah Mulya, M.T
NIP. 196602202006041001

2. Pembimbing II



Alfarissi, M.Comp.Sc
NIP. 198512152014041001

3. Penguji I

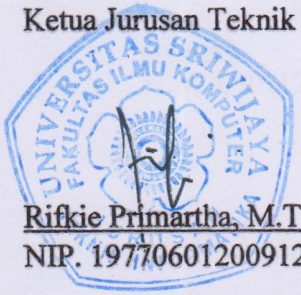


Alvi Syahrini Utami, M.Kom
NIP. 197812222006042003

4. Penguji II

Muhammad Ali Buchari, M.T
NIP. 198803302019031007

Mengetahui,
Ketua Jurusan Teknik Informatika,



Rifkie Primartha, M.T
NIP. 197706012009121004

HALAMAN PERNYATAAN

Yang bertanda tangan di bawah ini:

Nama	: Ricardo
NIM	: 09021281419132
Program Studi	: Teknik Informatika Bilingual
Judul Skripsi	: RSA Encryption Based on RSA-ElGamal Key Generation for ASCII Text Data

Hasil Pengecekan Software *iThenticate/Turnitin* : **9%**

Menyatakan bahwa Laporan Projek saya merupakan hasil karya sendiri dan bukan hasil penjiplakan/plagiat. Apabila ditemukan unsur penjiplakan/plagiat dalam laporan projek ini, maka saya bersedia menerima sanksi akademik dari Universitas Sriwijaya sesuai dengan ketentuan yang berlaku.

Demikian, pernyataan ini saya buat dengan sebenarnya dan tidak ada paksaan oleh siapapun.

Palembang,

Ricardo
NIM. 09021281419132

KATA PENGANTAR

Puji syukur kepada Tuhan Yang Maha Esa atas berkat dan rahmat-Nya yang telah diberikan kepada Penulis sehingga dapat menyelesaikan Tugas Akhir ini dengan baik. Tugas akhir ini disusun untuk memenuhi salah satu syarat guna menyelesaikan pendidikan program Strata-1 pada Fakultas Ilmu Komputer Program Studi Teknik Informatika di Universitas Sriwijaya.

Untuk selanjutnya penyusun mengucapkan banyak terima kasih kepada pihak-pihak yang telah membantu dalam penyelesaian skripsi ini, yaitu :

1. Dekan Fakultas Ilmu Komputer Universitas Sriwijaya, Jaidan Jauhari, S.Pd., M.T.
2. Ketua Jurusan Teknik Informatika Universitas Sriwijaya, Rifkie Primartha, M.T.
3. Orang tua, Vredy Tan dan Nelly, Saudara Kenedy, Saudari Meilinda dan seluruh keluarga besar yang selalu mendoakan, motivasi, menasehati, serta memberikan dukungan, baik moral maupun material.
4. Pembimbing I, Drs. Megah Mulya, M.T dan pembimbing II, Alfarissi, M.Comp.Sc yang telah membimbing, mengarahkan dan memberikan motivasi dalam proses perkuliahan dan pengerjaan Tugas Akhir.
5. Supervisor yang telah membimbing penulis dalam menyelesaikan Projek Sarjana Muda (PSM 1) di Universiti Teknologi Malaysia, Dr. Mazleena Salleh.
6. Penguji I, Alvi Syahrini Utami, M.Kom dan penguji II, Muhammad Ali Buchari, M.T yang telah memberikan masukan dan ilmu pengetahuan kepada penulis.
7. Dosen Program Studi Teknik Informatika Fakultas Ilmu Komputer Universitas Sriwijaya.
8. Staf Tata Usaha yang telah membantu dalam kelancaran proses administrasi dan akademik selama masa perkuliahan.
9. Teman-teman IF Reguler dan Bilingual, yang selalu berjuang bersama dalam menempuh ilmu.
10. Senior di jurusan Informatika dan teman dekat dari penulis yang telah menemani kehidupan penulis, tempat berbagi cerita, serta menjadi pendengar setia dalam keluh kesah penulis.
11. Semua pihak yang tidak dapat penulis sebutkan satu-persatu yang telah banyak membantu dan berperan bagi penulis terutama dalam penyelesaian tugas akhir ini, terima kasih banyak atas semuanya.

Palembang,

Penulis

DAFTAR ISI

Halaman

BAB III METODOLOGI PENELITIAN

BAB IV PENGEMBANGAN PERANGKAT LUNAK

DAFTAR GAMBAR

Halaman

DAFTAR TABEL

Halaman

DAFTAR LAMPIRAN

Halaman

RSA ENCRYPTION BASED ON RSA-ELGAMAL KEY GENERATION FOR ASCII TEXT DATA

By :

Ricardo

09021281419132

ABSTRACT

The increasing number of users of Internet services, the more data that needs to be secured. One way to get the secure data is through an encryption process. Because RSA keys are very large and requires a long time in key generation, it requires a method which is effective and simple to implement in the key generation process. Method ElGamal which uses a key size smaller than RSA is selected, so that it can speed up RSA key generation. This research uses RSA and ElGamal methods for RSA key generation. In this study obtained average yield of key generation computing time from RSA-ElGamal 1358 bits and RSA 2048 bits are 1831877422 ns and 3389572767 ns, respectively. That result obtained from this study are expected to be useful for takers a decision for the RSA cryptosystem in the future.

Keywords : *Key Generation*, *Encryption*, *RSA*, *ElGamal*.

Palembang,

Supervisor I,

Drs. Megah Mulya, M.T
NIP. 196602202006041001

Supervisor II,

Alfarissi, M.Comp.Sc
NIP. 198512152014041001

Approve,
Chairman of Informatics Engineering Department

Rifkie Primartha, M.T
NIP. 197706012009121004

RSA ENCRYPTION BASED ON RSA-ELGAMAL KEY GENERATION FOR ASCII TEXT DATA

Oleh :

Ricardo

09021281419132

ABSTRAK

Semakin meningkat jumlah pengguna layanan Internet, maka semakin banyak data yang perlu diamankan. Salah satu cara untuk mendapatkan data yang aman adalah melalui proses enkripsi. Karena kunci RSA yang sangat besar dan membutuhkan waktu yang lama dalam *key generation*, maka dibutuhkan metode yang efektif dan sederhana untuk diterapkan dalam proses *key generation*. Metode ElGamal yang menggunakan ukuran kunci yang lebih kecil dari RSA dipilih, sehingga dapat mempercepat RSA *key generation*. Penelitian ini menggunakan metode RSA dan ElGamal untuk RSA *key generation*. Pada penelitian ini didapat hasil rata-rata waktu komputasi *key generation* dari RSA-ElGamal 1358 bit dan RSA 2048 bit berturut-turut 1831877422 ns dan 3389572767 ns. Hasil yang didapatkan dari penelitian ini diharapkan dapat berguna bagi para pengambil keputusan untuk kriptosistem RSA pada masa yang akan datang.

Kata kunci: *Key Generation*, Enkripsi, RSA, ElGamal.

Palembang,

Pembimbing I,

Drs. Megah Mulya, M.T
NIP. 196602202006041001

Pembimbing II,

Alfarissi, M.Comp.Sc
NIP. 198512152014041001

Mengetahui,
Ketua Jurusan Teknik Informatika

Rifkie Primartha, M.T
NIP. 197706012009121004

BAB I

PENDAHULUAN

1.1 Pendahuluan

Bab ini membahas mengenai latar belakang penelitian *RSA Encryption Based on RSA-ElGamal Key Generation for ASCII Text Data* yang akan dibahas secara umum dan singkat pada latar belakang.

1.2 Latar Belakang

Keamanan informasi adalah praktik untuk mencegah akses informasi yang tidak sah. Bidang perhatian utama dari keamanan informasi adalah kerahasiaan, otentikasi, integritas, penolakan, dan ketersediaan. Kriptografi adalah salah satu topik studi dalam keamanan informasi. Kriptografi memiliki pengaruh besar dalam banyak aplikasi dunia nyata, seperti perdagangan elektronik, kartu pembayaran berbasis chip, mata uang digital, kata sandi komputer, dan komunikasi militer.

Berdasarkan waktu, kriptografi dibagi menjadi dua kategori: klasik dan modern. Kriptografi klasik terutama difokuskan pada pesan enkripsi. Kriptografi klasik didasarkan pada transposisi dan subtitusi sandi. Di sisi lain, kriptografi modern memiliki fokus yang sama dengan keamanan informasi. Kriptografi modern didasarkan pada matematika, termasuk kompleksitas komputasi, dan teori bilangan. Berdasarkan kuncinya, kriptografi modern dibagi menjadi dua kategori: simetris dan asimetris. Kriptografi simetris memiliki kunci yang sama untuk

pengirim dan penerima. Kriptografi asimetris menggunakan kunci yang berbeda tetapi berhubungan secara matematis.

Kriptografi asimetris sering didasarkan pada kompleksitas komputasi teori bilangan seperti faktorisasi bilangan bulat dan logaritma diskrit. RSA adalah salah satu kriptografi asimetris berdasarkan faktorisasi bilangan bulat, sedangkan ElGamal didasarkan pada logaritma diskrit. Dalam penelitian ini, diterapkan enkripsi RSA berdasarkan RSA-ElGamal *key generation* untuk data teks ASCII.

Kriptografi kunci publik memiliki kelemahan dalam kecepatan karena pertukaran antara efisiensi dan keamanan (Mahajan & Singh, 2014). Pada saat itu, penulis RSA menyarankan bilangan prima yang digunakan untuk membangkitkan kunci memiliki panjang lebih dari 100 digit (330 bit) (Rivest et al., 1978). Bilangan prima p dan q harus besar sehingga tidak efisien bagi siapa pun untuk memfaktorisasi $n = p \times q$ (Rivest et al., 1978). Semakin besar bilangan prima, semakin tidak efisien untuk memfaktorisasi n, tetapi semakin lambat untuk membangkitkan kunci. Di sisi lain, membangkitkan kunci dengan bilangan prima kecil akan mempercepat perhitungan, tetapi akan lebih mudah bagi *cryptanalyst* untuk memfaktorisasi n. Oleh karena itu, dibutuhkan pengukuran waktu komputasi *key generation* dengan ukuran kunci yang berbeda untuk melihat pengaruh panjang kunci terhadap waktu untuk *key generation*.

Pada 2016, Iswari mengklaim bahwa perhitungannya untuk *key generation* RSA yang dimodifikasi menggunakan 256 bit lebih cepat daripada RSA dengan 1024 bit dengan mempertahankan faktor keamanan. Saat ini, banyak peneliti menyarankan bahwa ukuran kunci yang digunakan untuk menghasilkan kunci RSA

harus setidaknya 2048 bit. Karena itu, panjang kunci juga perlu ditingkatkan untuk mengikuti standar keamanan.

Cryptool, sebuah perangkat lunak untuk enkripsi, menunjukkan bahwa RSA biasanya menghasilkan *ciphertext* hanya dalam format angka seperti: desimal, biner, oktal, dan heksadesimal. Tetapi pengguna menginginkan *ciphertext* dalam bentuk ASCII. Pesan yang ditampilkan sebagai karakter ASCII akan meningkatkan keamanan pesan. Mengubah karakter ASCII ke angka itu mudah, tetapi bagaimana cara mengubah angka besar menjadi ASCII? Beberapa karakter dalam ASCII direpresentasikan sebagai angka dalam dua digit dan sisanya dalam tiga digit. Misalnya, 'H' direpresentasikan sebagai 72, 'i' direpresentasikan sebagai 105, dan '!' Direpresentasikan sebagai 33, jadi "Hi!" Dikonversi menjadi 7210533, tetapi tidak ada karakter ASCII yang diwakili bilangan desimal yang lebih dari 3 *digit*, bahkan dengan membagi jumlah *digit*, juga tidak mungkin dilakukan karena jumlah *digit* tidak sama untuk setiap karakter ASCII. Lebih lanjut, teks harus direpresentasikan sebagai angka desimal sekecil mungkin, sehingga enkripsi akan lebih efisien. Oleh karena itu, *encoding* pesan sebelum dan sesudah enkripsi akan meningkatkan waktu komputasi untuk mendekripsi *ciphertext.*

1.3 Rumusan Masalah

Rumusan permasalahan yang diselesaikan dalam penelitian ini adalah sebagai berikut:

1. Bagaimana mekanisme *key generation* RSA – ElGamal untuk enkripsi dan dekripsi text ASCII?

2. Bagaimana hasil dari pengaruh panjang kunci yang berbeda pada *key generation* RSA – ElGamal?

1.4 Tujuan Penelitian

Tujuan penelitian ini adalah mengetahui pengaruh panjang kunci yang berbeda terhadap waktu komputasi *key generation* RSA – ElGamal.

1.5 Manfaat Penelitian

Manfaat dari penelitian ini adalah sebagai berikut:

1. Memahami RSA dan ElGamal sebagai metode kriptografi;
2. Mampu menerapkan teknik *key generation*, enkripsi dan dekripsi RSA – ElGamal pada data teks ASCII;
3. Hasil penelitian dapat digunakan untuk referensi dalam penelitian lainnya yang sejenis yang menggunakan RSA dan ElGamal dan teks ASCII.

1.6 Batasan Masalah

Batasan masalah pada penelitian ini adalah sebagai berikut:

1. Metode *key generation* yang digunakan adalah RSA dan ElGamal.
2. Enkripsi dan dekripsi dilakukan dengan metode RSA.

1.7 Sistematika Penulisan

Penyusunan skripsi ini disusun dengan sistematika penulisan sebagai berikut:

BAB I. PENDAHULUAN

Bab ini membahas mengenai latar belakang, perumusan masalah, tujuan penelitian, manfaat penelitian, batasan masalah, dan sistematika penulisan.

BAB II. KAJIAN LITERATUR

Pada bab ini akan membahas dasar-dasar teori yang akan digunakan dalam penelitian, seperti pengetahuan dasar tentang kriptografi dan metode yang akan digunakan dalam proses *key generation*, enkripsi dan dekripsi.

BAB III. METODOLOGI PENELITIAN

Pada bab ini akan dibahas mengenai unit penelitian, tahapan yang akan dilaksanakan pada penelitian ini, tahapan proses secara umum, metode pengembangan perangkat lunak, teknik pengujian dan manajemen proyek penelitian.

BAB IV. PENGEMBANGAN PERANGKAT LUNAK

Pada bab ini membahas mengenai analisis dan perancangan perangkat lunak yang akan digunakan sebagai alat penelitian. Dimulai dari pengumpulan dan analisa kebutuhan, rancangan dan konstruksi perangkat lunak serta pengujian untuk memastikan semua kebutuhan pengembangan perangkat lunak sesuai dengan dengan kebutuhan. Penyusunan pada bab ini memiliki kerangka penulisan dengan fase-fase dan elemen-elemen pengembangan perangkat lunak bersifat berorientasi objek.

BAB V. HASIL DAN ANALISA PENELITIAN

Pada bab ini diuraikan hasil pengujian berdasarkan langkah-langkah yang telah direncanakan. Tabel hasil pengujian serta analisisnya disajikan sebagai basis dari kesimpulan yang akan diambil dalam penelitian ini.

BAB VI. KESIMPULAN DAN SARAN

Pada bab ini berisi kesimpulan dari semua uraian-uraian pada bab-bab sebelumnya dan juga saran-saran yang diharapkan berguna untuk pengembangan selanjutnya.

1.8 Kesimpulan

Penelitian mengenai *key generation* akan dilakukan dengan metode RSA – ElGamal untuk enkripsi dan dekripsi data teks ASCII menggunakan metode RSA. Tujuannya adalah untuk mengembangkan perangkat lunak yang mampu mengenkripsi dan dekripsi data teks ASCII.

DAFTAR PUSTAKA

Abubakar, A., Jabaka, S., Tijjani, B. I., Zeki, A., Chiroma, H., Usman, M. J., … Mahmud, M. (2014). Cryptanalytic Attacks on Rivest, Shamir, and Adleman (RSA) cryptosystem: Issues and Challenges. *Journal of Theoretical and Applied Information Technology*, *61*(1), 37–43.

Boneh, D. (1999). Twenty Years of Attacks on the RSA Cryptosystem. *Notices of the American Mathematical Society*, *46*(2), 203–213.https://doi.org/10.1.1.525.7995

Diffie, W., & Hellman, M. E. (1976). Multiuser Cryptographic Techniques. *Proceedings of the June 7-10, 1976, National Computer Conference and Exposition on - AFIPS '76*, 109. https://doi.org/10.1145/1499799.1499815

ElGamal, T. (1985). A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms. *Advances in Cryptology*, *196*, 10–18. https://doi.org/10.1007/3-540-39568-7_2

Gaithuru, J. N., Bakhtiari, M., Salleh, M., & Muteb, A. M. (2016). A Comprehensive Literature Review of Asymmetric Key Cryptography Algorithms for Establishment of the Existing Gap. *2015 9th Malaysian Software Engineering Conference, MySEC 2015*, 236–244. https://doi.org/10.1109/MySEC.2015.7475227

Iswari, N. M. S. (2017). Key Generation Algorithm Design Combination of RSA and ElGamal Algorithm. *Proceedings of 2016 8th International Conference on Information Technology and Electrical Engineering: Empowering Technology for Better Future, ICITEE 2016*. https://doi.org/10.1109/ICITEED.2016.7863255

Mahajan, S., & Singh, M. (2014). Analysis of RSA Algorithm Using GPU. *International Journal of Network Security & Its Applications (IJNSA)*, *6*(4), 13–28. https://doi.org/10.5121/ijnsa.2014.6402

Meier, A. V. (2005). The ElGamal Cryptosystem, 1–13.

Menezes, A., van Oorschot, P., & Vanstone, S. (1996). Handbook of Applied Cryptography. *Annals of Physics*, *19964964*, 258. https://doi.org/10.1201/9781439821916

Ramanjaneya Reddy, N., Reddy, P. C., & Padmavathamma, M. (2016). Study the

Impact of Carmichael Function on RSA (pp. 752–756). https://doi.org/10.1007/978-981-10-3433-6_90

Rivest, R. (1990). *Cryptology*.

Rivest, R., Shamir, A., & Adleman, L. (1978). A Method for Obtaining Digital Signatures and Public-key Cryptosystems. *Communications of the ACM*, *21*(2), 120–126. https://doi.org/10.1145/359340.359342

Steef, A., A, A., & M. N, S. (2015). RSA Algorithm With a New Approach Encryption and Decryption Message Text by ASCII. *International Journal on Cryptography and Information Security*, *5*(3/4), 23–32. https://doi.org/10.5121/ijcis.2015.5403