DESAIN DAN IMPLEMENTASI ALGORITMA KRIPTOGRAFI RSA PADA TELKOM BOJONEGORO UNTUK MENINGKATKAN KEAMANAN SISTEM JARINGAN

SKRIPSI

Digunakan Sebagai Syarat Maju Ujian Diploma IV

Politeknik Negeri Malang

Oleh:

DIMAS WAHONO NIM. 1541183011

PROGRAM STUDI TEKNIK INFORMATIKA

JURUSAN TEKNOLOGI INFORMASI

POLITEKNIK NEGERI MALANG

JULI 2020

DESAIN DAN IMPLEMENTASI ALGORITMA KRIPTOGRAFI RSA PADA TELKOM BOJONEGORO UNTUK MENINGKATKAN KEAMANAN SISTEM JARINGAN

SKRIPSI

Digunakan Sebagai Syarat Maju Ujian Diploma IV

Politeknik Negeri Malang

Oleh:

DIMAS WAHONO NIM. 1541183011

PROGRAM STUDI TEKNIK INFORMATIKA

JURUSAN TEKNOLOGI INFORMASI

POLITEKNIK NEGERI MALANG

JULI 2020

HALAMAN PENGESAHAN

DESAIN DAN IMPLEMENTASI ALGORITMA KRIPTOGRAFI RSA PADA TELKOM BOJONEGORO UNTUK MENINGKATKAN KEAMANAN SISTEM JARINGAN

Disusun oleh:

DIMAS WAHONO NIM. 1541183011

Laporan Akhir ini telah diuji pada tanggal 30 Juli 2020

Disetujui oleh:

1. Penguji I : Dr. Eng. Rosa Andrie Asmara, ST., MT.
   NIP. 19801010 200501 1 001 .....
2. Penguji II : Eka Larasati Amalia, ST., M.T.
   NIP. 19880711 201504 2 005 .....
3. Pembimbing I : Yuri Ariyanto, S.Kom., M.Kom
   NIP. 19800716 201012 1 002 .....
4. Pembimbing II : Vipkas Al Hadid Firdaus, S.T, M.T
   NIP. 19910505 201903 1 029 .....

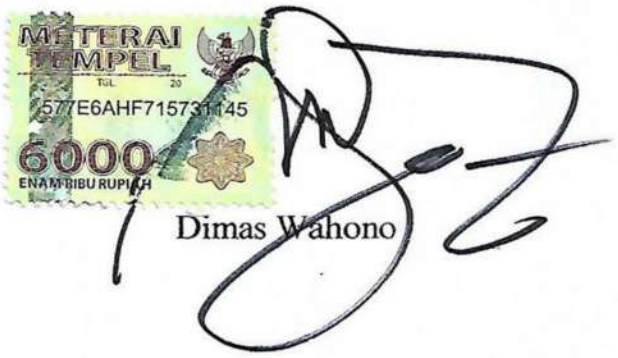
Mengetahui,

Ketua Jurusan Teknologi Informasi	Ketua Program Studi Teknik Informatika
Rudy Ariyanto, S.T., M.Cs.	Imam Fathur Rozi, ST., MT.
NIP. 19711110 199903 1 002	NIP. 19840610 200812 1 004

HALAMAN PERNYATAAAN

Dengan ini saya menyatakan bahwa Skripsi ini tidak terdapat karya yang pernah diajukan untuk memperoleh gelar kesarjanaan di suatu Perguruan Tinggi, dan sepanjang pengetahuan saya juga tidak terdapat karya atau pendapat yang pernah ditulis atau diterbitkan oleh orang lain, kecuali yang secara tertulis diacu dalam naskah ini dan disebutkan dalam daftar pustaka.

Malang, 30 Juli 2020



Dimas Wahono

ABSTRAK

Wahono, Dimas. "Desain dan Implementasi Algoritma Kriptografi RSA pada Telkom Bojonegoro Untuk Meningkatkan Keamanan Sistem Jaringan". **Pembimbing**: **(1) Yuri Ariyanto,S.Kom.,M.Kom. (2) Vipkas Al Hadid Firdaus, S.T, M.T**

Skripsi, Program Studi Teknik Informatika, Jurusan Teknologi Informasi, Politeknik Negeri Malang, 2020.

Pada suatu organisasi pasti terdapat suatu dokumen yang bersifat rahasia, dokumen yang bersifat rahasia tersebut perlu dibuatkan sistem penyimpanan dan pengirimannya agar tidak terbaca oleh orang-orang yang tidak bertanggung jawab. Dokumen yang perlu diamankan adalah dokumen-dokumen penting dan bersifat rahasia, baik dokumen tersebut tersimpan sebagai *file* di dalam komputer pribadi maupun *file* yang dikirim melalui *Public network*. Untuk menyimpan dokumen tersebut agar benar-benar aman. Permasalahan ini juga mendasari persoalan keamanan data penting seperti persaingan bisnis dan strategi bisnis dalam hal pemasaran pada Telkom Bojonegoro yang membutuhkan keamanan informasi dalam hal penyampaian data.

Berdasarkan permasalahan tersebut aplikasi "Desain dan Implementasi Algoritma Kriptografi RSA pada Telkom Bojonegoro untuk Meningkatkan Keamanan Sistem Jaringan" dirancang dan diimplementasikan untuk membangun sistem yang dapat mengirim *file* data penting secara aman melalui jaringan *public* khususnya pada Telkom Bojonegoro. dikembangkan menggunakan model sistem pengamanan dengan proses enkripsi dan dekripsi dengan menerapkan metode Algoritma kriptografi RSA *(Rivest-Shamir-Adleman)* sebagai pengamanan *file* pada *Transport Layer* TCP/IP untuk jaringan *publik* maupun lokal menjadi pilihan yang tepat sesuai kebutuhan dari algoritma yang lain sehingga amat sulit untuk ditembus oleh hacker.

Kata Kunci: RSA *(Rivest-Shamir-Adleman)* , Kriptografi, Algoritma, Keamanan Sistem Jaringan, keamanan Informasi.

ABSTRACT

Wahono, Dimas. *"Desain dan Implementasi Algoritma Kriptografi RSA pada Telkom Bojonegoro Untuk Meningkatkan Keamanan Sistem Jaringan".* ***Advisors: (1) Yuri Ariyanto,S.Kom.,M.Kom. (2) Vipkas Al Hadid Firdaus, S.T, M.T.***

Thesis, Informatics Engineering Study Program, Department of Information Technology, State Polytechnic of Malang, 2020.

In an organization there must be a document that is confidential, confidential documents that need to be made storage and shipping systems so that it is not read by people who are not responsible. Documents that need to be secured are important and confidential documents, both documents are stored as files on a personal computer or files sent through the Public Network. To save the document to be really safe. This problem also underlies important data security issues such as business competition and business strategy in terms of marketing at Telkom Bojonegoro which requires information security in terms of data delivery.

Based on these problems the application "Design and Implementation of the RSA Cryptographic Algorithm in Telkom Bojonegoro to Improve Network Security System" is designed and implemented to build a system that can send important data files safely through public networks, especially at Telkom Bojonegoro. developed using a security system model with the encryption and decryption process by applying the RSA (Rivest-Shamir-Adleman) cryptographic Algorithm method as file security at the Transport Layer TCP / IP for public and local networks to be the right choice according to the needs of other alogarithms to be penetrated by hackers.

Keywords: *RSA (Rivest-Shamir-Adleman), Cryptography, Algorithms, Network System Security, Information Security.*

KATA PENGANTAR

Puji Syukur penulis panjatkan kehadirat Allah SWT atas segala rahmat dan hidayah-Nya penulis dapat menyelesaikan laporan akhir dengan judul "DESAIN dan IMPLEMENTASI ALGORITMA KRIPTOGRAFI RSA pada TELKOM BOJONEGORO untuk MENINGKATKAN KEAMANAN SISTEM JARINGAN". Skripsi ini penulis susun sebagai persyaratan untuk menyelesaikan studi program Diploma IV Program Studi Teknik Informatika, Jurusan Teknologi Informasi, Politeknik Negeri Malang.

Penyusun laporan kegiatan ini terselenggara berkat bantuan dan dorongan dari berbagai pihak, untuk itu pada kesempatan ini penulis mengucapkan terimakasih kepada:

1. Allah SWT yang selalu memberikan kelancaran dalam melakukan pengerjaan skripsi ini.
2. Bapak Rudy Ariyanto, ST., M.Cs., selaku ketua jurusan Teknologi Informasi.
3. Bapak Imam Fathur Rozi, ST., MT., selaku ketua program studi Teknik.
4. Bapak Yuri Ariyanto,S.Kom.,M.Kom., selaku pembimbing pertama.
5. Bapak Vipkas Al Hadid Firdaus, S.T, M.T., selaku pembimbing kedua.
6. Kedua orang tua yang selalu mendoakan agar Skripsi ini lancar hingga akhir.
7. Seluruh PT.TELKOMINDONESIA (BOJONEGORO) yang telah membantu selama melakukan observasi dan seluruh pihak yang telah membantu dan mendukung lancarnya pembuatan Skripsi dari awal hingga akhir yang tidak dapat kami sebutkan satu persatu.

Demikian laporan ini dibuat. Atas perhatian, kerjasama dan bantuan dari semua pihak penulis ucapkan terima kasih.

Malang, Juli 2020

Dimas Wahono

DAFTAR ISI

Halaman

DAFTAR GAMBAR

Halaman

DAFTAR TABEL

Halaman

DAFTAR LAMPIRAN