ANALISIS DAN PERANCANGAN ENKRIPSI DOKUMEN MENGGUNAKAN METODE RIVEST SHAMIR ADLEMAN (RSA) BERBASIS WEB

SKRIPSI

diajukan oleh

SUPRIYANTO

17.11.1680

PROGRAM SARJANA
PROGRAM STUDI INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS AMIKOM YOGYAKARTA
YOGYAKARTA
2022

ANALISIS DAN PERANCANGAN ENKRIPSI DOKUMEN MENGGUNAKAN METODE RIVEST SHAMIR ADLEMAN (RSA) BERBASIS WEB

SKRIPSI

diajukan oleh

SUPRIYANTO

17.11.1680

PROGRAM SARJANA
PROGRAM STUDI INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS AMIKOM YOGYAKARTA
YOGYAKARTA
2022

PERSETUJUAN

SKRIPSI

ANALISIS DAN PERANCANGAN ENKRIPSI DOKUMEN MENGGUNAKAN METODE RIVEST SHAMIR ADLEMAN (RSA) BERBASIS WEB

yang dipersiapkan dan disusun oleh

Supriyanto

17.11.1680

telah disetujuai oleh Dosen Pembimbing Skripsi

pada tanggal 23 Agustus 2022

Dosen Pembimbing,

Joko Dwi Santoso, M.Kom
NIK. 190302181

PENGESAHAN

SKRIPSI

ANALISIS DAN PERANCANGAN ENKRIPSI DOKUMEN MENGGUNAKAN METODE RIVEST SHAMIR ADLEMAN (RSA) BERBASIS WEB

yang dipersiapkan dan disusun oleh

Supriyanto

17.11.1680

telah dipertahankan di depan Dewan Penguji
pada tanggal 23 Agustus 2022

Susunan Dewan Penguji

Nama Penguji	**Tanda Tangan**
Joko Dwi Santoso, M.Kom **NIK. 190302181**	_____
Sri Ngudi Wahyuni, S. T., M.Kom **NIK. 190302060**	_____
Rini Indrayani, S. T., M.Kom **NIK. 190302417**	_____

Skripsi ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana Komputer

DEKAN FAKULTAS ILMU KOMPUTER

Hanif Al Fatta, S.Kom., M.Kom
NIK. 190302096

PERNYATAAN KEASLIAN SKRIPSI

HALAMAN PERNYATAAN KEASLIAN SKRIPSI

Yang bertandatangan di bawah ini,

Nama mahasiswa : Supriyanto
NIM : 17.11.1680

Menyatakan bahwa Skripsi dengan judul berikut:

ANALISIS DAN PERANCANGAN ENKRIPSI DOKUMEN MENGGUNAKAN METODE RIVEST SHAMIR ADLEMAN (RSA) BERBASIS WEB

Dosen Pembimbing : Joko Dwi Santoso, M. Kom

1. Karya tulis ini adalah benar-benar ASLI dan BELUM PERNAH diajukan untuk mendapatkan gelar akademik, baik di Universitas AMIKOM Yogyakarta maupun di Perguruan Tinggi lainnya.
2. Karya tulis ini merupakan gagasan, rumusan dan penelitian SAYA sendiri, tanpa bantuan pihak lain kecuali arahan dari Dosen Pembimbing.
3. Dalam karya tulis ini tidak terdapat karya atau pendapat orang lain, kecuali secara tertulis dengan jelas dicantumkan sebagai acuan dalam naskah dengan disebutkan nama pengarang dan disebutkan dalam Daftar Pustaka pada karya tulis ini.
4. Perangkat lunak yang digunakan dalam penelitian ini sepenuhnya menjadi tanggung jawab SAYA, bukan tanggung jawab Universitas AMIKOM Yogyakarta.
5. Pernyataan ini SAYA buat dengan sesungguhnya, apabila di kemudian hari terdapat penyimpangan dan ketidakbenaran dalam pernyataan ini, maka SAYA bersedia menerima SANKSI AKADEMIK dengan pencabutan gelar yang sudah diperoleh, serta sanksi lainnya sesuai dengan norma yang berlaku di Perguruan Tinggi.

Yogyakarta, 23 Agustus 2022

Yang Menyatakan,

Supriyanto

PERSEMBAHAN

Puji Syukur penulis panjatkan kepada Allah SWT, yang telah memberikan kesehatan, rahmat dan hidayah, sehingga penulis masih diberikan kesempatan untuk menyelesaikan skripsi ini, sebagai salah satu syarat untuk mendapatkan gelar kesarjanaan. Walaupun jauh dari kata sempurna, namun penulis bangga telah mencapai pada titik ini, yang akhirnya skripsi ini bisa terselesaikan. Skripsi ini saya persembahkan untuk :

1. Kedua orang tua Bapak Suparwo dan Ibu Sularni terimakasih atas doa, semangat, motivasi, pengorbanan, nasehat serta kasih sayang yang tidak pernah henti sampai saat ini.
2. Adikku & Kakakku semuanya, terimakasih telah menjadi penyemangat dalam mengerjakan tugas akhir ini.
3. Untuk keluarga besar saya terimakasih untuk dukungan dan doa atas terselesaikannya skripsi ini.
4. Dosen Pembimbing Pak Joko Dwi Santoso yang sudah membimbing serta memberi masukan dan saran selama ini, sehingga saya dapat menyelesaikan skripsi ini.
5. Sahabat Bajuri Squad, Nanik, Felly, Nur, Qhosim, Bambang, Dias, Ulin, Arpin, Dimas, Mondy yang telah memberikan masukan, saran, motivasi dan bimbingan dalam mengerjakan skripsi ini.
6. Sahabat Skripsi Sulis, Riska, Bayu, Mas Umar yang sudah memberikan masukan, semangat, saran, bimbingan dalam mengerjakan skripsi ini.
7. Semua teman-teman Informatika IF12 Angkatan 2017.
8. Kepada semua teman-teman, saudara yang tidak bisa saya sebutkan satu persatu, saya persembahkan skripsi ini untuk kalian semua.

KATA PENGANTAR

Segala puji dan syukur bagi Allah atas ridho-Nya, penulis dapat menyelesaikan skripsi ini dengan baik. Penyusunan penelitian ini dapat selesai dengan lancar karena tidak lepas dari bantuan berbagai pihak. Untuk itu saya ucapkan terima kasih sebesar-besarnya kepada :

1. Bapak Prof. Dr. M. Suyanto, MM. selaku Rektor Universitas Amikom Yogyakarta
2. Bapak Hanif Al Fatta, S.Kom., M.Kom. selaku Dekan Fakultas Ilmu Komputer Universitas Amikom Yogyakarta
3. Bapak Joko Dwi Santoso, M.Kom selaku dosen pembimbing yang telah memberikan bimbingan dan masukan dalam melakukan penelitian
4. Bapak dan Ibu Dosen Universitas AMIKOM Yogyakarta yang telah banyak memberikan ilmunya selama masa studi.
5. Kedua orang tua saya yang telah memberi berbagai macam bantuan baik secara dorongan doa,motivasi, moral dan materi.
6. Semua pihak yang tidak dapat disebutkan satu-persatu yang telah membantu saya untuk menyelesaikan penelitian.

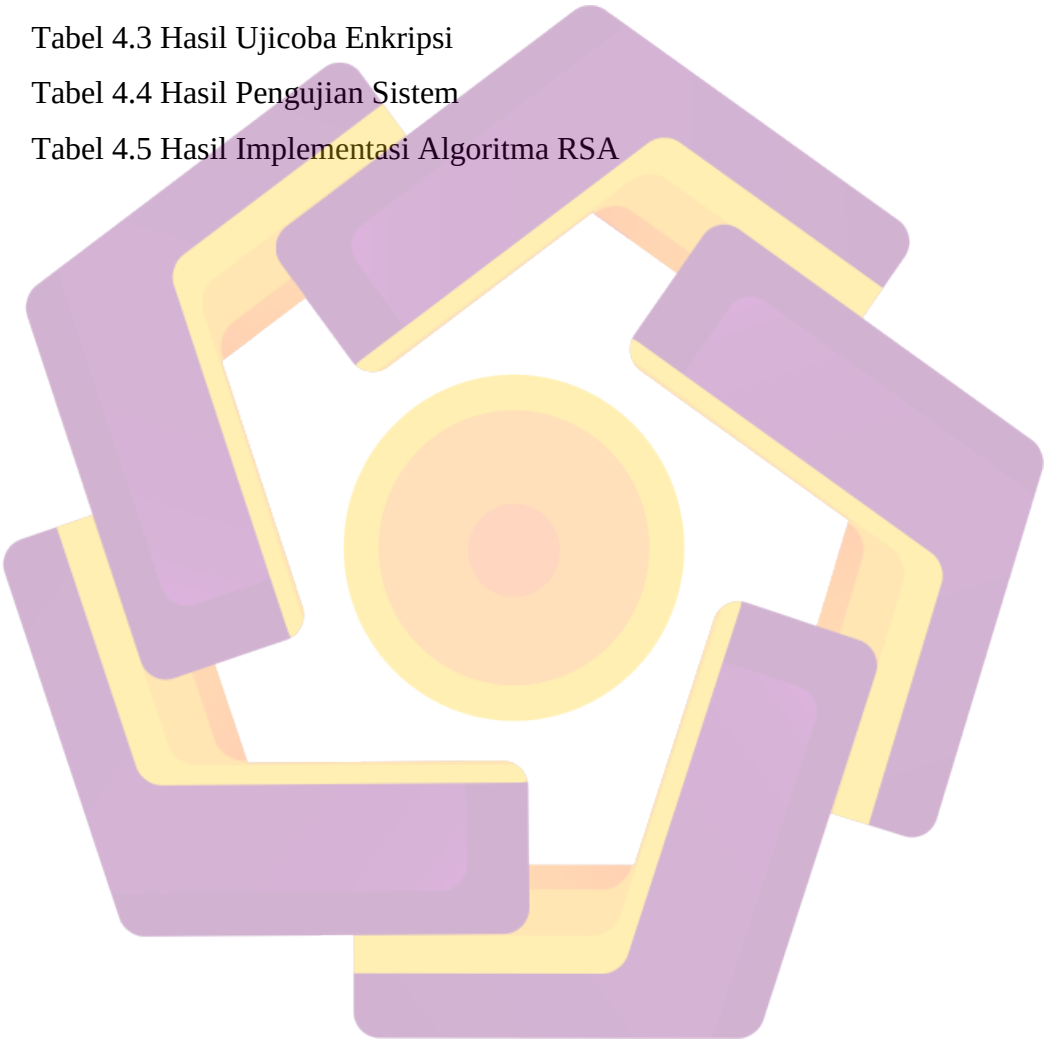
Penulis tentunya menyadari bahwa skripsi ini masih banyak kekurangan dan kelemahannya. Oleh karena itu penulis berharap kepada semua pihak agar dapat menyampaikan kritik dan saran yang membangun untuk menambah kesempurnaan skripsi ini. Namun penulis tetap berharap skripsi ini akan bermanfaat bagi semua pihak yang membacanya.

Yogyakarta, 28 Agustus 2022

Penulis

DAFTAR ISI

DAFTAR TABEL

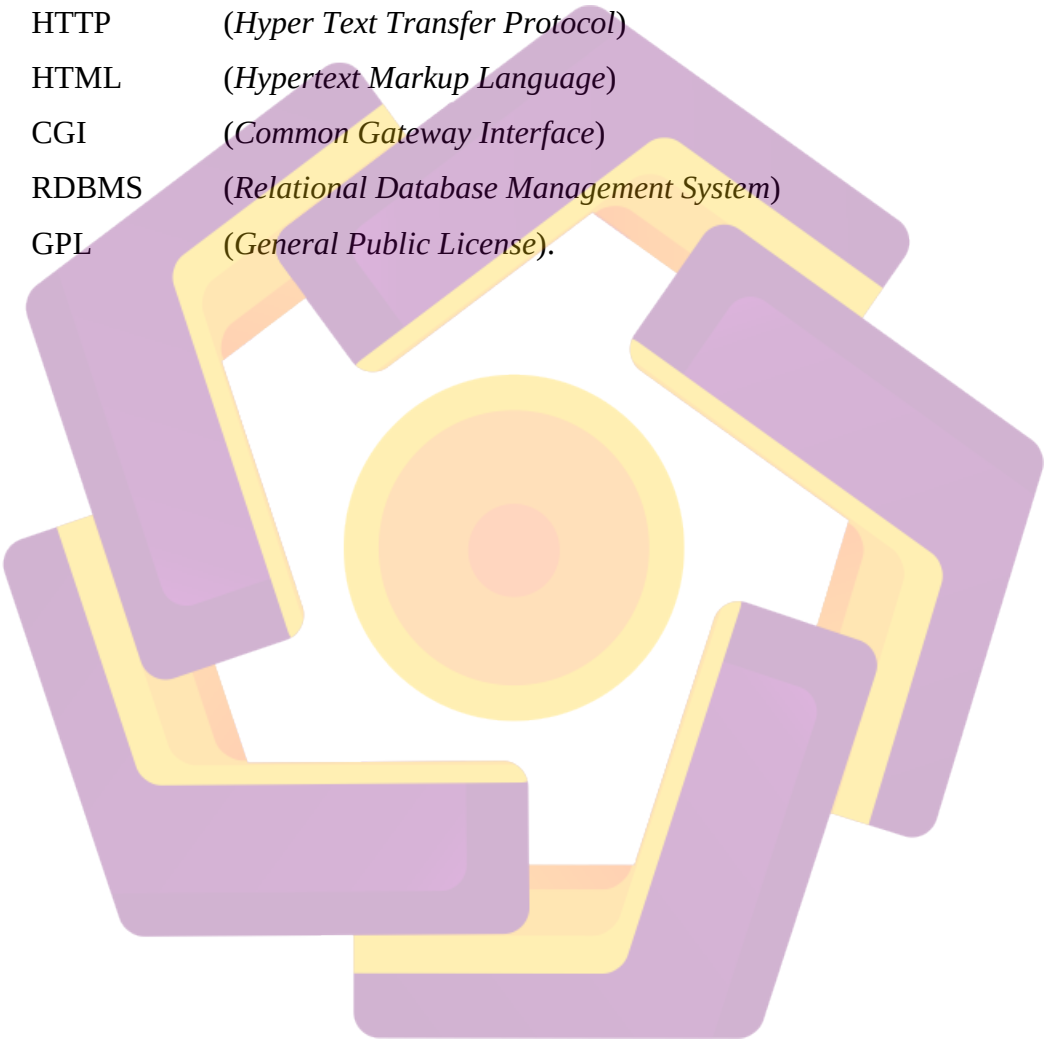


DAFTAR GAMBAR

DAFTAR LAMPIRAN

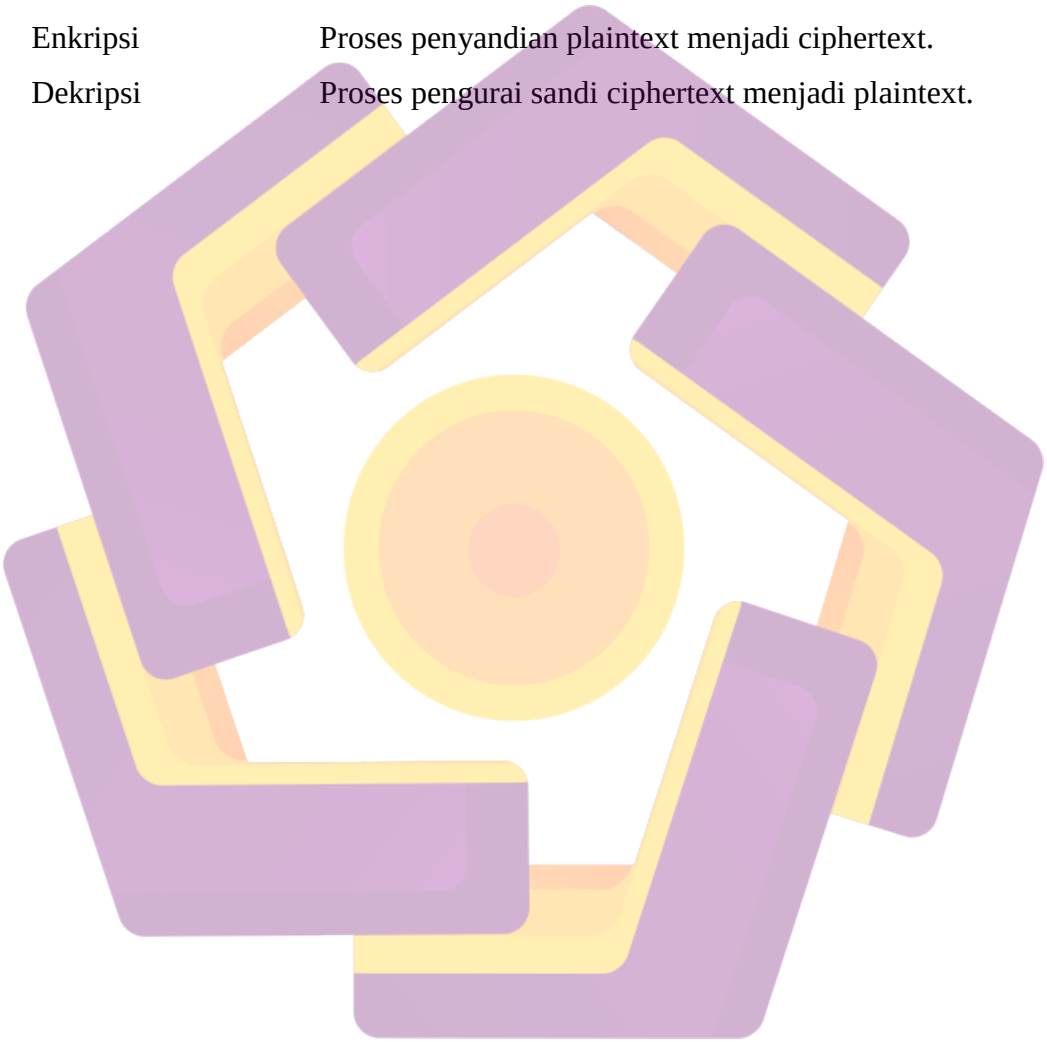
DAFTAR LAMBANG DAN SINGKATAN

RSA	(*Rivest Shamir Adleman*)
MIT	(*Massachusetts Institute of Technology*).
ASCII	(*American Standard Code for Information Interchange*)
HTTP	(*Hyper Text Transfer Protocol*)
HTML	(*Hypertext Markup Language*)
CGI	(*Common Gateway Interface*)
RDBMS	(*Relational Database Management System*)
GPL	(*General Public License*).



DAFTAR ISTILAH

Ciphertext	Pesan tersembunyi atau rahasia
Plaintext	Pesan teks asli
Generate Key	Proses pembangkitan kunci publik dan kunci privat
Enkripsi	Proses penyandian plaintext menjadi ciphertext.
Dekripsi	Proses pengurai sandi ciphertext menjadi plaintext.



INTISARI

Dengan adanya internet, semua orang bisa saling berkomunikasi dan bertukar informasi dengan mudah dan cepat. Beberapa aspek penting dalam proses pertukaran data atau informasi yaitu: kerahasiaan, integritas data, autentikasi dan non-repudiasi. Namun terkadang aspek tersebut kurang diperhatikan, sehingga Salah satu akibat yang timbul dari hal ini semakin banyaknya pencurian data terhadap suatu dokumen yang bersifat rahasia.

Salah satu upaya untuk menjaga keamanan dan kerahasiaan data yaitu dengan metode kriptografi. Kriptografi merupakan ilmu yang digunakan untuk menjaga kerahasiaan data. RSA adalah salah satu algoritma yang menggunakan konsep kriptografi kunci publik (Asimetri) yaitu kunci yang digunakan untuk mengenkripsi berbeda dengan kunci yang digunakan untuk mendekripsi).

Aplikasi dibangun dalam lingkungan bahasa pemrograman PHP. Dari hasil pengujian membuktikan sistem kriptografi RSA berhasil mengenkripsi dan mendekripsi dokumen berekstensi .pdf, sistem memiliki keterbatasan nilai p dan q yaitu dalam rentang bilangan prima 11-101 semakin besar bilangan prima yang dipilih akan membutuhkan waktu yang lama dalam pembangkitan kunci. Harapannya aplikasi bisa dionlinekan sehingga bisa digunakan secara luas.

Kata Kunci: Kriptografi, RSA, Enkripsi, Dekripsi, PHP.

ABSTRACT

With the internet, everyone can communicate with each other and exchange information easily and quickly. Several important aspects in the process of exchanging data or information are: confidentiality, data integrity, authentication and non-repudiation. However, some of these aspects are not paid attention to, so that one of the consequences arising from this is the increasing number of data theft of a confidential document.

One of the efforts to maintain data security and confidentiality is the cryptographic method. Cryptography is a science used to maintain the confidentiality of data. RSA is an algorithm that uses the concept of public key cryptography (asymmetry), i.e. the key used to encrypt is different from the key used to decrypt.

Applications built in the PHP programming language environment. The test results prove that the RSA cryptography system successfully encrypts and decrypts documents with .pdf extension, the system has limited p and q values, namely in the prime number range 11-101 the larger the prime number chosen, the longer it will take to generate the key. The hope is that the application can be online so that it can be used widely.

Keyword: *Cryptography, RSA, Encryption, Decryption, PHP.*